Мистецтво залишатися непоміченим

Kevin Mitnick
with Robert Vamosi

The art of invisibility

The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data

Foreword by Mikko Hypponen

Little, Brown and Company
New York · 2017

Кевін Митник
за участю Роберта Вемосі

Мистецтво залишатися непоміченим

Хто ще читає ваші імейли?

З передмовою Мікко Гюппонена

Переклала з англійської
Олександра Асташова

«Наш формат»
Київ · 2019

УДК 004.73/.77:342.738](0.062)
М66

Митник Кевін, Вемосі Роберт
М66 Мистецтво залишатися непоміченим. Хто ще читає ваші імейли? / пер. з англ. Олександра Асташова. — К. : Наш формат, 2019. — 280 с.
ISBN 978-617-7730-39-1 (паперове видання)
ISBN 978-617-7730-40-7 (електронне видання)

Щодня кількість інтернет-даних про кожну людину зростає в геометричній прогресії. Тому хоч би якою привабливою була ілюзія конфіденційності, ми аж ніяк не є невидимками для світу. Навіть якщо ви не публічна особа, по той бік екрана знають, що ви їли на обід. За вами може шпигувати будь-хто і будь-що, навіть офісний принтер.

Однак від цього можна захиститися. У цій книжці колишній хакер Кевін Митник разом із журналістом Робертом Вемосі доступно розповідає, як залишатися непоміченим в інтернеті, дає поради, яких паролів краще не використовувати та як запобігти викраденню особистих даних.

УДК 004.73/.77:342.738](0.062)

Перекладено за виданням: Kevin Mitnick, Robert Vamosi. *The art of invisibility. The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data* (NY, Little, Brown and Company, 2017, ISBN 978-0-316-38050-8)

This edition published by arrangement with Little, Brown and Company, New York, New York, USA.

Головна редакторка *Олеся Дубчак*. Літературна редакторка *Ярослава Панкєєв*. Коректорка *Анастасія Ушинська*. Верстальник *Назар Матлах*. Технічна редакторка *Ірина Щепіна*. Художня редакторка *Оксана Гадзай*. Дизайнерка обкладинки *Валерія Печеник*. Відповідальна за випуск *Ілона Замоцна*.

Надруковано в Україні видавництвом «Наш формат» у типографії «Антологія». Підписано до друку 10.10.2019. Замовлення № 39-10-19. Тираж 2500 прим. Термін придатності необмежений. ТОВ «НФ», пров. Алли Горської, 5, м. Київ, Україна, 01032, тел. (044) 222-53-40, pub@nashformat.ua. Свідоцтво ДК № 4722 від 19.05.2014. Висновок Держ. сан.-епідем. експертизи № 05.03.02-04/51017 від 16.11.2015.

Науково-популярне видання

ISBN 978-617-7730-39-1 (паперове видання)
ISBN 978-617-7730-40-7 (електронне видання)

Моїй люблячій матері Шеллі Джафф і бабусі Рібі Вартанян

Передмова

Кілька місяців тому я натрапив на давнього друга, якого не бачив ще зі школи. За чашечкою кави ми вирішили надолужити кілька останніх десятиліть і поговорити про роботу. Приятель розповів, що займається поширенням і підтримкою сучасного медичного обладнання; я ж,зі свого боку, про двадцять п'ять років роботи у сфері інформаційної безпеки й конфіденційності. Мої слова про конфіденційність викликали в нього лиш легкий смішок. «Певен, усе це супер-пупер круто, — відповів він, — але тут мені хвилюватися нічого. Урешті-решт, я ж не злочинець. Я не роблю нічого поганого. Мені байдуже, якщо хтось буде спостерігати за тим, що я роблю в інтернеті».

Мене вкрай розчарували слова давнього друга і його аргументи щодо того, чому конфіденційність безглузда. Розчарували, бо я чув ці доводи й раніше. Купу разів. І далі чую від людей, які щиро вірять, що приховувати їм нічого. Щиро вірять, що захищатися треба лише злочинцям. Щиро вірять, що лише терористи використовують шифрування. Щиро вірять, що нам не треба захищати свої права. Ні. Треба. Конфіденційність не просто торкається наших прав — вона сама є правом. Одним з основних прав людини, визнаних Загальною декларацією прав людини ООН 1948 року.

Якщо конфіденційність потребувала захисту ще в далекому 1948-му, то що вже казати про сьогодні. Урешті-решт, ми — перше покоління в історії людства, за яким можна стежити так пильно. Спостерігати за кожним кроком нашого цифрового життя. Так чи інакше дізнаватися про кожне наше слово. Ми навіть добровільно носимо на собі «жучки», чомусь називаючи їх «смартфонами».

Завдяки інтернет-моніторингу можна легко дізнатися, які книжки ми купуємо, які новини читаємо і які шматки з цих новин вподобали. Куди подорожуємо і з ким. Хворіємо, сумуємо чи збуджені. Загалом сучасний моніторинг збирає всі ці дані з комерційною метою. Адже компанії, які пропонують безкоштовні послуги, якось мають перетворити їх на мільярдні прибутки. У цьому й полягає цінність профілювання інтернет-користувачів у масових масштабах. Проте існує й більш цілеспрямований моніторинг — той, який проводять вітчизняні та зарубіжні уряди.

Цифрові комунікації дали державним установам змогу провадити масове спостереження, однак вони ж озброїли й нас. Ми здатні захистити себе такими інструментами, як шифрування, безпечне зберігання даних і дотримання основних принципів операційної безпеки (OPSEC). Нас просто треба навчити, як робити це правильно.

Що ж, навчальний посібник уже у вас у руках. Я дуже радий, що Кевін таки знайшов час поділитися своїми знаннями з мистецтва невидимості. Урешті-решт, він експерт у темі, а ця книжка — відмінний ресурс. Неодмінно

прочитайте її і скористайтеся отриманою інформацією. Захистіть себе і свої права.

Повернемося до кафе, де після чашечки кави ми з другом попрощалися й розійшлися. Я побажав йому успіхів і знову зникнув з радарів. Але я й досі іноді згадую його слова: «Мені байдуже, якщо хтось буде спостерігати за тим, що я роблю в інтернеті». Що ж, друже, можливо, тобі і нічого приховувати. Але необов'язково щось приховувати, щоб це довелося захищати.

Мікко Гюппонен

Мікко Гюппонен — директор із досліджень у компанії F-Secure. Він — єдиний, хто виступив і на хакерському DEF CON, і на конференції TED.

Вступ

Час зникнути

Майже за два роки після того, як співробітник Booz Allen Hamilton Едвард Сноуден уперше оприлюднив секретні матеріали Агентства національної безпеки (АНБ), комік Джон Олівер вийшов з опитуванням на Таймс-сквер у Нью-Йорку в рамках свого шоу на каналі HBO. Питання до перехожих були простими. Хто такий Едвард Сноуден? І що він зробив?[1]

Кадри, що вийшли в ефір, вражали: ніхто не знав. І навіть якщо хтось таки пригадував ім'я, що зробив Сноуден (і чому), він і гадки не мав. Потрапивши до АНБ, Едвард Сноуден скопіював тисячі таємних державних документів, які згодом передав журналістам для оприлюднення. Олівер міг би завершити свою рубрику про конфіденційність і спостереження на цій сумній ноті (виявляється, навіть роки галасу в ЗМІ не змусили американців перейматися внутрішнім шпигунством уряду), але комік пішов іншим шляхом. Він вилетів до Росії, де зараз мешкає Сноуден у вигнанні, щоб взяти особисте інтерв'ю[2].

Найперше, що Олівер запитав Сноудена в Москві, було: «Чого ви сподівалися цим досягти?». Сноуден пояснив, що хотів показати світові правду про АНБ, яке збирало дані майже на всіх. Коли Олівер увімкнув йому уривки опитування на Таймс-сквер, де перехожі одне за одним зізнавалися, що знати не знають про Сноудена, той відповів: «Що ж, усіх проінформувати неможливо».

Чому ж ми так погано проінформовані в питаннях конфіденційності, які порушував Сноуден та інші поборники? Чому нам чхати на те, що державні установи прослуховують наші телефони, читають імейли і навіть повідомлення? Можливо, тому, що АНБ не втручається в наше життя безпосередньо. Не явно. *Не відчутно.*

Однак того дня на Таймс-сквер Олівер дізнався й те, що американцям таки не чхати на конфіденційність, якщо це зачіпає їх особисто. Окрім запитань про Сноудена, комік ставив і загальні запитання щодо конфіденційності. Наприклад, коли він розповідав про секретну (і на сто відсотків вигадану) урядову програму, яка відстежує всі оголені фото, щойно їх відправляють по інтернету, реакція серед жителів Нью-Йорка була одностайна: вони демонстрували відкритий протест. Один перехожий навіть зізнався, що сам нещодавно надіслав таку світлину.

Усі опитувані погодилися, що громадяни США мають право ділитися по інтернету чим завгодно (навіть фотографією пеніса) у приватному порядку. Що й намагався донести Сноуден.

Виявляється, вигадана урядова програма відстеження оголених фото не така вже й вигадана. Сноуден пояснив Оліверові, що компанії на зразок Google мають фізичні сервери у всьому світі, тож навіть звичайне повідомлення від чоловіка дружині (яке, між іншим, може містити оголені світлини) у межах

одного американського міста цілком імовірно спочатку потрапляє на зарубіжний сервер. А позаяк дані вийшли за межі США, хай і на наносекунду, АНБ може озброїтися «Патріотичним актом»[3] і вилучити повідомлення чи імейл (зокрема й непристойну світлину), бо технічно вони надійшли до країни з іноземного джерела. Сноуден стверджує, що звичайні американці потрапили в тенета антитерористичних законів, які мали захистити країну після трагедії 11 вересня, а насправді розв'язали руки урядові, що тепер шпигує майже за всіма громадянами.

Здавалося б, регулярні новини про витік даних та урядові «шпигунські» програми мають обурити нас до нестями. Здавалося б, події розгортаються так стрімко (за якихось кілька років), що свіжі рани мають спонукати нас протестувати на вулиці. Але все навпаки. Купа людей (і навіть деякі з тих, хто зараз читає цю книжку) уже певною мірою примирилися з тим, що за всіма нашими діями — телефонними дзвінками, повідомленнями, імейлами, активністю в соцмережах — можуть спостерігати.

І це розчаровує.

Можливо, ви не порушили жодних законів. Живете собі тихим, середньостатистичним життям, такі непримітні серед гігантського натовпу інтернет-користувачів. Але повірте мені: ви — не невидимка. Принаймні поки що.

Я обожнюю фокуси. І недарма: кажуть, що хакерові таки не завадить хоч якась спритність рук. Певно, усі бачили фокус зі зникненням предмета? Секрет у тому, що предмет насправді не зникає і не стає невидимим — він просто ховається десь на задньому плані: за завісою, у рукаві, у кишені. Бачимо ми його чи ні, він однак там.

Те саме відбувається і з купою особистих даних, які невпинно збираються і зберігаються, хоча ми цього навіть не помічаємо. Більшість із нас і гадки не має, як легко знайти цю інформацію і де її шукати. Ми її не бачимо, тож вважаємо себе невидимими для колишніх, батьків, навчальних закладів, начальників, навіть уряду.

Однак якщо знати, де шукати, можна знайти будь-яку інформацію. Про будь-кого.

Я часто виступаю з промовами. І байдуже, наскільки велика аудиторія: завжди є одна людина, яка намагається заперечити вищезгаданий факт. Якось після такого виступу сумніви висловила одна вкрай скептична журналістка.

Пам'ятаю, як ми сиділи за окремим столиком у барі готелю в одному американському мегаполісі. Саме тоді вона і заявила мені, що ніколи не була жертвою витоку даних. Через юний вік у неї майже нема майна на власне ім'я, а отже, у реєстрах є мінімум записів. Вона ніколи не розголошує особистих даних у статтях і соцмережах — усе суто професійно. Вона вважала себе невидимкою. Тож я попрохав дозволу розшукати її номер соціального страхування та інші особисті дані в інтернеті. Хоча й неохоче, дівчина погодилася.

За тим самим столиком я зайшов на сайт для приватних детективів, до яких належу і я через свою роботу у сфері хакерських розслідувань у всьому світі. Я вже знав ім'я журналістки, тож спитав у неї лише адресу (хоча можна було і без цього: адресу легко знайти на іншому сайті). Уже за кілька хвилин я знав її номер соціального страхування, місто народження і навіть дівоче прізвище матері. Знав усі місця, з яких вона телефонувала додому, і всю історію її мобільних номерів. Дівчина шоковано втупилася в екран і врешті-решт визнала, що вся інформація більш-менш правдива.

Сайт, яким я скористався, доступний лише перевіреним компаніям чи особам. Щомісяця він стягує фіксовану, але невелику плату плюс додаткові витрати на пошук інформації. Також час від часу мене перевіряють стосовно законної мети для проведення конкретного пошуку. Але базову інформацію можна знайти фактично за копійки. І все це абсолютно законно.

Ви коли-небудь заповнювали онлайн-форму? Надсилали інформацію до школи чи іншого закладу, який зберігає її в інтернеті? Чи, може, подавали заяву на розгляд судової справи через сайт? Якщо так, то вітаю: ви добровільно передали особисту інформацію третій стороні, яка може робити з нею що завгодно. Існує ймовірність того, що деякі з цих даних (ба навіть усі) вже в мережі і доступні компаніям, які заробляють на тому, що збирають особисту інформацію по всьому інтернету. Установа Privacy Rights Clearinghouse називає понад 130 таких компаній, які мають на вас «досьє» (і байдуже, правдиве воно чи ні)[4].

І не забувайте про дані, які ви в інтернет добровільно не завантажуєте, але які все одно зберігаються в архівах приватних та урядових компаній: інформація про те, кому ми пишемо чи телефонуємо, що шукаємо в мережі, що купуємо (як у звичайних, так і в інтернет-магазинах) і куди подорожуємо (хай там як: на машині чи пішки). Кількість даних на кожного з нас зростає з кожним днем у геометричній прогресії.

Вважаєте, що хвилюватися вам нічого? Повірте мені: дарма. Сподіваюся, що наприкінці книжки ви будете достатньо проінформовані й готові покласти цьому край.

Усі ми живемо з ілюзією конфіденційності. І жили так, мабуть, десятиліттями.

У певну мить нам стає некомфортно від того, який необмежений доступ до нашого особистого життя має уряд, робота, керівники, вчителі, батьки. Але позаяк цей доступ розширюється поступово, позаяк ми самі приймаємо кожну нову цифрову дрібницю без огляду на її втручання в приватне життя, повернути час назад стає дедалі важче. Тим паче, хто добровільно відмовиться від своїх електронних іграшок?

Небезпека цифрового спостереження полягає не в тому, що дані збирають (із цим ми мало що здатні зробити), а в тому, що з ними роблять опісля.

Уявіть, що надто завзятий прокурор може зробити з вашим товстим досьє необробленої інформації за кілька років. Дані, зібрані сьогодні (і часто поза

контекстом), житимуть вічно. Навіть член Верховного суду США Стівен Браєр погоджується, що «важко здогадатися заздалегідь, які ваші слова чи дії видадуться (прокуророві) актуальними в контексті конкретного розслідування і коли»[5]. Інакше кажучи, ваше фото в нетверезому стані на фейсбуці — найменша з проблем.

Усе ще вважаєте, що вам нічого приховувати? Впевнені? В одній переконливій статті для журналу Wired відомий дослідник кібербезпеки Моксі Марлінспайк зазначає, що федеральним злочином у США може стати навіть дрібниця. Наприклад, звичайний невеличкий лобстер[6]. «Байдуже, купили ви його в магазині чи хтось подарував, живий він чи мертвий, знайшли ви його після того, як той помер із природних причин, чи вбили під час самозахисту. Ви можете сісти у в'язницю через лобстера»[7]. Суть у тому, що існує купа незначних і маловідомих законів, які ви можете порушити, навіть про це не підозрюючи. А цифровий слід, що веде до доказів, доступний кожному всього в кілька кліків.

Конфіденційність — річ складна. Вона не є універсальною. В усіх нас різні причини якоюсь інформацією вільно ділитися з незнайомцями, а якусь залишати приватною. Може, ви просто не хочете, щоб друга половинка знала про вас кожну дрібницю. Може, хочете відокремити особисте життя від роботи. А може, дійсно боїтеся, що уряд за вами шпигує.

У кожного свій сценарій, тож жодна з порад у книжці не підійде на всі випадки життя. Позаяк наше ставлення до конфіденційності досить складне і, як наслідок, унікальне, ми зануримося в найголовніше — те, що зараз відбувається з таємним збором даних. А ви вже самі зможете вирішувати, що пасуватиме до вашої ситуації.

Як мінімум, ця книжка розкриє вам способи зберігання конфіденційності в цифровому світі і запропонує рішення, на які ви можете пристати чи не пристати. Оскільки конфіденційність — справа особиста, ступінь невидимості теж коливатиметься від людини до людини.

Ця книжка доведе вам, що спостерігають абсолютно за кожним: вдома чи на вулиці, у кафе чи в машині по дорозі на роботу. Ваш комп'ютер, телефон, автомобіль, домашня сигналізація, навіть холодильник — усе це потенційні точки доступу до приватного життя.

Але не хвилюйтеся, я не збираюся лише лякати вас. Я також розповім, що робити з відсутністю конфіденційності, яка зараз уже стала нормою.

Книжка навчить вас:

- шифрувати і надсилати захищені імейли;
- захищати дані надійним паролем;
- приховувати реальну IP-адресу в публічних місцях;
- убезпечувати комп'ютер від стеження;
- захищати свою анонімність;
- тощо.

А тепер приготуйтеся опановувати мистецтво невидимості.

1 https://www.youtube.com/watch?t=33&v=XEVlyP4_11M.

2 Перш ніж дістати дозвіл на проживання в Росії, Сноуден вирушив у Гонконг. Опісля він подавав прохання на політичний притулок у Бразилії та інших країнах і не виключав можливості повернутися до США за умови справедливого суду.

3 «Патріотичний акт» — федеральний закон, ухвалений у США в жовтні 2001 року, який дає урядові й поліції широкі повноваження для нагляду за громадянами. Ухвалено після терористичного акту 11 вересня 2001 року. — *Прим. пер.*

4 http://www.reuters.com/article/2011/02/24/idUSN2427826420110224.

5 https://www.law.cornell.edu/supct/html/98-93.ZD.html.

6 https://www.law.cornell.edu/uscode/text/16/3372.

7 http://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/.

Розділ 1

Ваш пароль можна зламати!

День праці 2014-го для Дженніфер Лоуренс видався не з легких. Лауреатка премії «Оскар», як і ще купа голлівудських зірок, прокинулася того ранку під новини, що їхні особисті фото — деякі й в оголеному вигляді — уже гуляли по всьому інтернету.

Знайдіть хвилинку і подумки прогляньте всі фото, що зберігаються у вас на комп'ютері, у телефоні, на пошті. Певен, більшість із них — абсолютно безневинні. Вам однаково, якщо весь світ побачить світлини заходів сонця, милі сімейні знімки, може, навіть жартівливі селфі в непрезентабельному вигляді. Але чи готові ви поділитися всіма фото? Що ви відчуєте, якщо раптом усі вони опиняться в інтернеті? Можливо, не в усіх особисті фото — самі непристойнощі, але вони все одно особисті. Ми маємо право вирішувати, коли і з ким ділитися ними, і чи варто взагалі. Однак із хмарними сервісами ми втрачаємо вибір.

Того року історія Дженніфер Лоуренс заполонила майже всі новини святкового дня. Інцидент був частиною кампанії під назвою #TheFappening — масштабного витоку оголених і напівоголених світлин Ріанни, Кейт Аптон, Кейлі Куоко, Едріанн Каррі і ще майже трьох сотень знаменитостей — переважно жінок, — телефони яких якось дистанційно зламали. Очевидно, що купа людей щиро зацікавилася фотографіями. Але для багатьох це стало тривожним нагадуванням про те, що таке може трапитися і з ними.

То як зловмисники дістали доступ до особистих світлин Дженніфер Лоуренс та інших зірок?

Позаяк усі ці знаменитості мали айфони, перші припущення крутилися навколо масового витоку даних із iCloud — сервісу хмарного зберігання даних для користувачів продукції Apple. Коли на девайсі закінчується пам'ять, у вас є змога зберігати всі нові фото, файли, музику та ігри на серверах Apple за невеличку щомісячну плату. Для пристроїв на платформі Android існує схожий сервіс від Google.

Хоча Apple зазвичай публічно не коментує проблеми безпеки, компанія заперечила помилку з їхнього боку. Apple оприлюднила заяву, у якій назвала інцидент «вузько спрямованою атакою на акаунти, паролі та питання безпеки» і додала, що «жоден із випадків, які ми розглянули під час розслідування, не став наслідком зламу систем Apple, зокрема й iCloud чи Find my iPhone»[8].

Перші світлини з'явилися на хакерському форумі, що славиться викраденими фотографіями[9]. Там же зародилося активне обговорення інструментів цифрової експертизи, якими скористалися для викрадення фото.

Дослідники, слідчі та правоохоронні органи користуються цими інструментами, щоб отримати дані з девайсів чи хмарних сховищ підозрюваних у злочині. Але, ясна річ, на цьому функції інструментів не закінчуються.

В обговореннях часто фігурувала програма Elcomsoft Phone Password Breaker (EPPB), яка дає правоохоронним органам і державним установам змогу дістати доступ до акаунтів iCloud і продається відкрито. Вона — лиш один із багатьох інструментів, але на форумі про неї говорили найбільше. Для доступу через EPPB потрібні логін і пароль в iCloud, однак для завсідників форуму це взагалі не проблема. Якраз напередодні Дня праці 2014-го хтось запостив на популярному репозиторії коду (Github) інструмент під назвою iBrute — механізм для зламу паролів, призначений спеціально для викрадення даних із iCloud.

Озброївшись iBrute та EPPB, будь-хто може видати себе за жертву зламу й завантажити повну резервну копію даних з її iCloud на свій девайс. Функція корисна, якщо ви, наприклад, змінюєте телефон. І на руку зловмисникові, який бачить абсолютно все, що ви будь-коли зберігали на айфоні. А це — набагато більше файлів, аніж можна знайти в iCloud жертви.

Консультант із цифрової експертизи та дослідник інформаційної безпеки Джонатан Здзіарски розповів Wired, що після перевірки вкрадених фото Кейт Аптон припускає можливість використання iBrute та EPPB. Доступ до відновленої резервної копії айфону дає зловмисникові купу особистої інформації, якою можна скористатися для шантажу[10].

У жовтні 2016-го тридцятишестирічний Раян Коллінз з Ланкастера, штат Пенсильванія, був засуджений до вісімнадцяти місяців позбавлення волі за «несанкціонований доступ до захищеного комп'ютера з метою отримання інформації» під час цього зламу. Йому було висунуто звинувачення в незаконному доступі до більш як сотні акаунтів Apple та Google[11].

Щоби захистити свій iCloud та інші інтернет-акаупти, варто видумати надійний пароль. Здавалося б, логічно. Але за роки роботи тестувальником на проникнення (спеціаліст, якому платять за злам комп'ютерних мереж і пошук вразливих місць) я зустрів купу людей — навіть директорів величезних корпорацій, — які надто ледачі, щоби друкувати складний пароль. Приміром, генеральний директор Sony Entertainment Майкл Лінтон поставив на внутрішній акаунт пароль «sonyml3». Я навіть не здивувався, що його імейл зламали й поширили листи на весь інтернет: зловмисники дістали адміністративний доступ до кожного куточка компанії.

Однак робочими акаунтами ваше життя не обмежується: особисті дані також потребують захисту паролем. Ясна річ, складний пароль не зупинить хакерські програми на зразок oclHashcat (інструмент для зламу паролів, який використовує графічні процесори для швидкого підбору варіантів), але сповільнить процес настільки, що зловмисник може переключитися на легший об'єкт.

Логічно припустити, що деякими паролями, опублікованими після зламу соцмережі Ashley Madison у липні 2015-го, жертви користуються і поза сайтом. Приміром, для банківських рахунків чи навіть на робочих комп'ютерах. Зі списку в 11 мільйонів оприлюднених паролів найпопулярнішими виявилися

«123456», «12345», «password», «DEFAULT», «123456789», «qwerty», «12345678», «abc123» та «1234567»[12]. Якщо ви побачили свій пароль у списку, то ви маєте всі шанси стати жертвою крадіжки даних, бо найпоширеніші варіанти фігурують ледь не в усіх програмах для зламу паролів, які можна легко завантажити з інтернету. На сайті haveibeenpwned.com завжди можна перевірити, чи ламали колись ваш акаунт.

У XXI столітті ми здатні на більше. Набагато більше. Із довжелезними і складними комбінаціями літер і цифр. Якщо зараз вам це видається важким, то ось автоматичний і ручний способи створити пароль.

Найпростіший підхід — узагалі не видумувати пароль і віддати процес у руки автоматизації. Існує декілька цифрових менеджерів паролів, які не лише надійно зберігають їх і вводять в один клік, а й здатні згенерувати новий і безпечний пароль для кожного сайту.

Але майте на увазі: тут є дві проблеми. Перша: менеджери паролів завжди використовують для доступу єдиний майстер-пароль. Якщо хтось заразить ваш комп'ютер шкідливим ПЗ, яке вкраде базу даних паролів і майстер-пароль через кілоґінґ (процес, коли шкідливе ПЗ записує кожне натиснення клавіші), то кінець грі. Зловмисник дістане доступ до всіх ваших паролів. Працюючи тестувальником на проникнення, іноді я підміняв менеджер паролів модифікованою версією, яка пересилає майстер-пароль мені (якщо це менеджер паролів із відкритим вихідним кодом). Це можна зробити, діставши адміністративний доступ до мережі клієнта. Після таких маніпуляцій усі конфіденційні паролі опиняються в нас у руках. Інакше кажучи, ми використовуємо менеджер паролів як чорний хід до скарбниці.

А друга проблема досить очевидна: якщо втрачаєте майстер-пароль, то втрачаєте всі паролі. Зрештою, це не так страшно. Завжди можна скинути паролі на всіх сайтах вручну. Але якщо у вас море акаунтів, то це перетвориться на справжню тяганину.

Однак, попри всі ці недоліки, наступних порад буде цілком достатньо, щоб убезпечити ваші паролі.

Перше правило: парольні фрази (не паролі!) повинні бути довгими — принаймні 20–25 символів. Довільні символи — наприклад, ek5iogh#skf&skd — найкращий варіант. На жаль, людському мозку важко запам'ятати довільну послідовність, тому на допомогу приходить менеджер паролів. Це набагато краще, ніж видумувати пароль самостійно. Я віддаю перевагу менеджерам паролів із відкритим кодом, як от Password Safe чи KeePass, які зберігають усі дані локально на вашому комп'ютері.

Ще одне важливе правило: ніколи не використовуйте один і той самий пароль для двох різних акаунтів. Знаю, це важко. Зараз у нас стоїть пароль на кожній дрібниці. Тож дозвольте менеджерові паролів генерувати і зберігати надійні, унікальні паролі.

Але навіть якщо у вас надійний пароль, технології все ще здатні взяти верх. Існують програми підбору пароля на зразок John the Ripper — безкоштовної програми з відкритим кодом, яку будь-хто може завантажити і встановити свої параметри конфігурації[13]. Наприклад, користувач сам вказує, скільки знаків підбирати, чи враховувати спеціальні символи, чи використовувати іноземні алфавіти тощо. John the Ripper та аналогічні програми підбирають символи за наборами правил, що надзвичайно ефективні для зламу паролів. Тобто пробує всі можливі комбінації цифр, літер і символів за встановленими параметрами, поки не зламає пароль. На щастя, мало хто з нас перейшов дорогу цілій державі з майже необмеженим часом і ресурсами. Зазвичай це друга половинка, родич чи розлючений знайомий, який, зіткнувшись з паролем у двадцять п'ять символів, не матиме часу й ресурсів на успішний злам.

Є ще один варіант. Скажімо, ви не хочете мати справи з менеджером паролів, і у вас є супернадійна фраза. Я вас порадую: можете її записати. Але в жодному разі не пишіть «Bank of America: 4the1sttimein4ever». Це буде надто очевидно. Краще зашифруйте назву банку кодовим словом на зразок «матрац» (бо раніше гроші часто зберігали під матрацом) і напишіть «4the1st». Зверніть увагу, я не дописав фрази. Це і не треба. Ви вже й так знаєте решту. А хтось може і не знати. Якщо зловмисники знайдуть роздрукований список обірваних паролів, то будуть украй спантеличені — принаймні попервах. Цікава історія: якось я вечеряв у товариша — не останньої людини в Microsoft. Ми сиділи за столом разом із його дружиною і дитиною, обговорюючи безпеку паролів. Раптом дружина товариша підвелася й підійшла до холодильника. Виявилося, вона записала всі свої паролі на аркуші паперу і прикріпила його до дверей холодильника магнітом. Мій друг просто похитав головою, а я мимоволі усміхнувся. Записувати паролі — не найкраще рішення, але забути якийсь складний пароль, який використовуєш раз на століття, — ще гірше.

Деякі сайти — наприклад, ваш інтернет-банк — блокують користувачів після кількох (зазвичай трьох) невдалих спроб ввести пароль. Не всі сайти так роблять, але навіть якщо подібна функція є, зловмисники із John the Ripper чи oclHashcat працюють не так. (До речі, oclHashcat розподіляє процес зламу між кількома графічними процесорами, тому є потужнішим за John the Ripper). До того ж хакери насправді не вводять кожен потенційний пароль.

Скажімо, у вас стався витік даних, серед яких опинилися логіни та паролі. Однак паролі, отримані в результаті зламу, — це якась тарабарщина.

Як же ж це допоможе зламати ваш акаунт?

Коли ви вводите пароль, — щоб розблокувати ноутбук, увійти на сайт тощо, — цей пароль проходить через односторонній алгоритм — геш-функцію. Це не те саме, що й шифрування. Шифрування — процес двосторонній, бо ви можете шифрувати і дешифрувати дані за наявності ключа. Геш же — це відбиток пальця, який відповідає за конкретний рядок символів. Якщо говорити загалом,

односторонні алгоритми є незворотними. Або принаймні зробити це дуже і дуже важко.

Тобто в базі даних паролів на вашому комп'ютері, телефоні чи у хмарному сховищі зберігається не пароль «MaryHadALittleLamb123$», а його геш — певна послідовність цифр і літер. Ця послідовність — токен[14] вашого пароля[15].

Саме геші, а не паролі, крадуть із захищеної пам'яті комп'ютера в процесі зламу системи чи витоку даних. Отримавши геші паролів, хакер може спробувати зламати їх загальнодоступними програмами (як от John the Ripper чи oclHashcat) й дістати реальний пароль. Можна зробити це або грубою силою (тобто перебирати всі можливі буквено-цифрові комбінації), або пробувати кожне слово з якогось списку — наприклад, словника. Опції John the Ripper та oclHashcat допомагають зловмисникам модифікувати цей список за різними наборами правил. Приміром, за принципом «літспіку», коли система замінює літери цифрами, як от у «к3в1н м17н1к». Таке правило перетворить усі варіанти пароля на комбінації літспіку. Подібні методи уможливлюють набагато ефективніший злам паролів, аніж грубою силою. Спочатку зламуються прості й поширені паролі; на складніші ж потрібно вже більше часу (хоча швидкість зламу залежить від кількох чинників). Маючи на руках програму для зламу, ваш логін і геш пароля хакери можуть дістати доступ навіть до кількох акаунтів і спробувати отримати пароль на сайтах, прив'язаних до вашої імейл-адреси чи іншого ідентифікатора.

Загалом, що більше символів містить ваш пароль, то більше часу знадобиться програмі на зразок John the Ripper, щоб перебрати всі можливі комбінації. Нові покоління процесорів стають дедалі швидшими, а отже, часу на те, щоб підібрати шести- і навіть восьмизначний пароль, потрібно дедалі менше. Ось чому я раджу створювати паролі на 25 і більше символів.

Після того як створите собі надійні паролі — і всюди різні, — нікому їх не кажіть. Вам здається це доволі очевидним? Опитування, проведені в Лондоні й інших великих містах, показали, що люди часто видають паролі в обмін на якусь дрібницю — ручку чи навіть шоколадку[16]. Якось мій товариш поділився паролем від Netflix із дівчиною.

Це здавалося логічним. Таким собі актом довіри: тепер вона могла сама вибирати фільм, який вони подивляться разом. Але розділ рекомендацій був захаращений стрічками на основі фільмів, які він дивився з колишньою дівчиною. Приміром, «Джинси-талісман» — не той фільм, який би він вибрав добровільно. І нова дівчина це прекрасно розуміла.

Так, в усіх нас є колишні. А якщо нема, то це навіть якось підозріло. Але жодна дівчина не хоче бачити «сліди» тих, хто був до неї.

Якщо вже захищаєте паролем свої онлайн-сервіси, то варто подумати і про особисті девайси. У більшості з нас є ноутбуки чи стаціонарні комп'ютери. Можливо, зараз ви вдома одні, але як щодо чергових гостей? Не боїтеся, що хтось із них дістане доступ до ваших файлів, фото та ігор звичайним порухом

мишки за робочим столом? І ще одна повчальна історія про Netflix: ще в часи, коли Netflix переважно розсилав фільми на DVD по пошті, моїх знайомих вирішили розіграти. Якось вони влаштували вдома вечірку й забули вийти з акаунта Netflix у браузері. Наступного дня пара знайшла купу непристойних другосортних фільмів у черзі і ще стільки ж у поштовій скриньці.

Захистити паролем свій робочий комп'ютер ще важливіше. Пригадайте, скільки разів вас смикали з робочого місця на раптову нараду. Хтось міг проходити повз ваш стіл і побачити таблицю з бюджетом на наступний квартал. Або прочитати всі ваші імейли. Ба навіть гірше: якщо у вас нема захищеного паролем скрінсейвера, який вмикається за кілька секунд бездіяльності, коли вас нема на робочому місці тривалий час (відійшли на обід чи довгу нараду), хтось може просто сісти й написати імейл від вашого імені. Чи навіть змінити цифри в бюджеті на наступний квартал.

Зараз видумали безліч креативних способів цьому запобігти, як-от програми для блокування екрана, які через блютуз перевіряють, перебуваєте ви поряд із комп'ютером чи ні. Інакше кажучи, якщо ви відійдете в туалет разом із телефоном, то він зникне із блютуз-зони комп'ютера і екран негайно заблокується. Аналогічні програми існують навіть для блютуз-браслетів і розумних годинників.

Захистити паролем інтернет-акаунти — це половина справи. Якщо хтось справді вкраде ваш девайс, особливо з відкритими акаунтами, то ці паролі не допоможуть. З усіх девайсів пароль потрібно ставити насамперед на мобільні, бо їх найлегше вкрасти чи загубити. І все ж опитування журналу Consumer Reports показало, що 34 % американців не захищають свої мобільні девайси жодним паролем, навіть простим чотиризначним PIN-кодом на екрані блокування[17].

У 2014 році в місті Мартінес, штат Каліфорнія, один поліцейський зізнався у викраденні оголених світлин зі смартфона підозрюваного в керуванні автомобілем у нетверезому стані. А це — явне порушення четвертої поправки до Конституції США, яка є частиною Білля про права[18]. Зокрема, четверта поправка забороняє безпідставний обшук та арешт без ордера, виданого суддею і підкріпленого достатньою причиною: наприклад, працівник правоохоронних органів має зазначити, з якою метою хоче дістати доступ до вашого телефона.

Якщо ваш телефон досі не захищений паролем, відірвіться на хвилинку і зробіть це. Я серйозно.

Існують три основні способи захистити свій телефон незалежно від системи — Android, iOS чи щось інше. Найпоширеніший — звичайний кодовий пароль, тобто коротка послідовність цифр, яку ви вводите на екрані блокування смартфона. Забудьте про код за замовчуванням — не полінуйтеся залізти в налаштування і вручну введіть щось надійніше. Можна навіть семизначний код (наприклад, старий номер телефону, яким користувалися в дитинстві). Чотирьох цифр замало.

Деякі мобільні пристрої дають змогу використовувати в коді ще й літери. Знову ж таки, робіть пароль не менш як на сім символів. Сучасні смартфони відображають цифри й літери на одній клавіатурі, тож переключатися не доведеться.

Ще один варіант блокування — візуальний. У 2008-му телефони на базі Android почали оснащувати так званими графічними ключами. На екрані з'являються дев'ять крапок, які ви можете з'єднати будь-яким довільним способом. Ця послідовність з'єднання і стає вашим паролем. Здавалося б, геніально. Величезний діапазон можливих комбінацій робить вашу послідовність незламною. Однак людська природа бере верх. У 2015-му на конференції PasswordsCon дослідники повідомили, що учасники експерименту скористалися лише кількома з можливих 140 704 комбінацій графічного ключа[19]. Що ж це за такі передбачувані варіанти? Зазвичай перша літера імені. Дослідження також показало, що люди схильні більше користуватися центральними точками й ігнорувати кути. Візьміть це до уваги, коли будете видумувати свій графічний ключ.

І, нарешті, біометричне блокування. Apple, Samsung та інші відомі виробники тепер дають змогу своїм користувачам розблоковувати телефон сканером відбитка пальця. Однак майте на увазі, що технологія не цілком надійна. Із випуском Touch ID усі, певно, сподівалися, що Apple перевершать сканери від інших фірм на ринку. Але для дослідників стало сюрпризом те, що з айфоном працювали старі фокуси: наприклад, зняття відбитка пальця з чистої поверхні за допомогою дитячої присипки та скотча.

Також деякі смартфони використовують фронтальну камеру для розпізнавання обличчя власника. Але і цю технологію можна обдурити за допомогою чіткої роздрукованої фотографії користувача.

Загалом біометрика сама собою вразлива до зламу. В ідеалі, вона повинна бути лиш одним з етапів автентифікації. Прикладіть палець чи усміхніться на камеру, потім введіть PIN-код чи пароль. Так ви зможете захистити свій смартфон.

А що як ви створили надійний пароль, але забули його записати? Скидання пароля — це справжнє спасіння, коли не можеш дістати доступ до акаунта, яким рідко користуєшся... але й легка мішень для потенційних зловмисників. Наші профілі в соцмережах, розкидані по всьому інтернету, — лазівка для хакерів. Скинувши паролі, вони легко можуть дістати доступ до наших імейлів та інших сервісів.

Одну таку атаку широко висвітлювали в пресі: зловмисники дізнавалися чотири останні цифри номера кредитки жертви, а потім зверталися до адміністрації сервісу з проханням змінити імейл авторизації, називаючи як доказ ці чотири цифри. Так, вони могли змінити пароль на власний без відома законного користувача.

Якось 2008-го студент Університету Теннессі Девід Кернелл вирішив перевірити, чи зможе дістати доступ до особистого імейлу на Yahoo кандидата у

віце-президенти Сари Пейлін[20]. Кернелл міг би вгадати пароль, але не знав, чи заблокує сайт доступ до акаунта через кілька невдалих спроб. Тож він скористався функцією скидання пароля, що, за його словами, «елементарно»[21].

Певен, усі ми отримували від друзів і приятелів дивні імейли з посиланнями на зарубіжні порносайти, а згодом дізнавалися, що їхні акаунти зламали. Привласнення імейлів часто трапляється через ненадійність паролів, які або дізнаються через витік даних, або скидають.

Коли ви створюєте акаунт в електронній пошті чи на сайті банку, часто вас можуть попрохати відповісти на так звані «секретні» питання. Зазвичай їх три. Нерідко вам випаде меню зі списком запропонованих питань, щоб ви могли вибрати собі щось до смаку. Здебільшого вони дуже і дуже очевидні.

Де ви народилися? У якій школі вчилися? У якому університеті? І старе добре «дівоче прізвище матері» — знамените секретне запитання ще з 1882-го[22]. Пізніше я розповім, як компанії можуть нарити в інтернеті вашу особисту інформацію і відповісти на стандартні запитання завиграшки. Кілька хвилин пошуків — і у вас непогані шанси успішно пройти всі секретні запитання будь-якого користувача.

Лише нещодавно ці запитання почали якось вдосконалювати. Наприклад, «у якому штаті народився ваш дівер/шурин?» — запитання досить специфічне, але чесна відповідь на нього може бути справою досить ризикованою. За мить поясню чому. І все ж більшість так званих «секретних» запитань усе ще не складніші за «де народився ваш батько?».

Коли відповідаєте на такі запитання, намагайтеся уникати найбільш очевидних варіантів зі списку. Навіть якщо сайт пропонує лиш банальні запитання, підійдіть до процесу творчо: ніхто не зобов'язує писати вас банальні відповіді. Додайте трохи кмітливості. Приміром, ваш провайдер мультимедіа цікавиться, який ваш улюблений колір. А що як це тутті-фрутті? Хто про це здогадається? Це ж колір, так? Усе, що ви напишете у відповіді, автоматично стане «правильною» відповіддю на секретне запитання.

Якщо даєте креативну відповідь, краще запишіть собі кудись і її, і саме запитання та сховайте в надійне місце (або просто збережіть усе це в менеджері паролів). Коли вам знадобиться зателефонувати в службу технічної підтримки, оператор може поставити вам одне із секретних запитань. Тому тримайте аркуш під рукою, у гаманці або використовуйте одні й ті самі відповіді на різних сайтах, щоб запам'ятати, що на запитання «де ви народилися?» варто відповісти «в лікарні». Такий простий фокус зіб'є з пантелику зловмисників, що назбирали на вас досьє в інтернеті і безуспішно вводять щось на зразок «Колумбус, штат Огайо».

А от чесно відповідати на специфічні секретні запитання — додатковий ризик: так ви видаєте ще більше особистої інформації, ніж було до цього в інтернеті. Наприклад, чесну відповідь на запитання «у якому штаті народився ваш дівер/шурин?» сайт, якому ви повідомляєте цю інформацію, може просто

продати. А зловмисники вже поєднають її з наявними даними чи заповнять прогалини у вашому досьє. Наприклад, на основі простої відповіді можна зробити висновок, що ви перебуваєте або перебували в шлюбі і у вашого теперішнього чи колишнього чоловіка або дружини є брат, що народився у вказаному штаті, чи сестра, одружена з чоловіком із цього штату. Забагато додаткової інформації в простому питанні, еге ж? З іншого боку, якщо у вас нема дівера чи шурина, сміливо видумуйте кмітливу відповідь. Напишіть щось на зразок «Пуерто-Рико». Це зіб'є з пантелику будь-якого зловмисника, що збирає на вас досьє. Що більше обманних маневрів ви зробите, то менш помітними станете в мережі.

Відповідаючи на відносно специфічні запитання, завжди оцінюйте цінність сайту. Наприклад, інтернет-банку можна довірити додаткову інформацію про себе, а от провайдеру мультимедіа — навряд чи. Також звертайте увагу на політику конфіденційності сайту: не полінуйтеся пошукати уточнення, чи може він надавати зібрану інформацію третій стороні.

Щоб скинути пароль пошти Сари Пейлін, знадобилася її дата народження, індекс і відповідь на секретне запитання: «Де ви вперше зустріли свого чоловіка?». Дату народження і поштовий індекс дізнатися було дуже легко (тоді Пейлін була губернатором Аляски). Із секретним запитанням усе було трохи складніше, але Кернелл і на нього знайшов відповідь. У своїх інтерв'ю Сара Пейлін не раз казала, що чоловік був її шкільним коханням. Тож логічно, що відповіддю на секретне запитання було «школа».

Угадавши відповідь, Кернелл зміг скинути пароль її імейлу на Yahoo й поставити свій. Так він зміг проглянути всі її особисті листи й розмістити скріншот поштової скриньки на хакерському сайті. Пейлін не мала доступу до власного імейлу, доки не скинула пароль ще раз[23].

Дії Кернелла були незаконними. Він порушив закон «Про боротьбу з комп'ютерним шахрайством і зловживанням» і був визнаний винним за двома статтями: випереджальне перешкоджання правосуддю шляхом знищення документів (кримінальний злочин) і несанкціонований доступ до комп'ютера (проступок). У 2010-му він був засуджений до одного року й одного дня у в'язниці та ще трьох років перебування під наглядом[24].

Якщо ви повторили долю Пейлін, і ваш імейл зламали, спершу варто змінити пароль... Здогадалися як? Правильно, скинувши його ще раз. Придумайте новий і більш надійний пароль, скориставшись моїми порадами. А тепер відкрийте теку «Надіслані» і подивіться, що написали від вашого імені. Є шанс знайти купу спаму, надісланого відразу кільком людям чи навіть усьому списку контактів. Тепер ви розумієте, чому друзі завалювали вас спамом усі ці роки: їхню пошту просто зламали.

А ще перевірте, чи не додав хтось свій імейл до вашого акаунта: якщо зловмисник дістав доступ до вашої пошти, то може ввімкнути функцію пересилання на свій акаунт. Тобто ви так само бачитимете свої листи, але їх

зможе проглядати і зловмисник. Якщо хтось додав свій імейл до вашого акаунта, одразу його видаліть.

Паролі та PIN-коди вважаються заходами безпеки, але, як ви вже переконалися, їх можна вгадати. Інша ж справа зі складними паролями та двофакторною автентифікацією (2ФА). Останню Apple запровадили у своїх сервісах iCloud після інциденту з оголеними фото Дженніфер Лоуренс та інших зірок.

Що ж таке 2ФА?

Для автентифікації на сайті або в застосунку[25] потрібно виконати щонайменше дві з трьох умов. Зазвичай це те, що ви маєте; те, що знаєте; те, що є частиною вас. Мати ви можете банківську картку з магнітною смугою або чипом; знати — PIN-код чи відповідь на секретне запитання. А до біометричної перевірки входять сканування відбитків пальців, розпізнавання обличчя, голосу тощо. Що більше умов виконає користувач, то більше шансів, що він — той, за кого себе видає.

Якщо це здається вам чимось новим, то ви помиляєтеся. Уже понад сорок років ми стикаємося з 2ФА, навіть цього не усвідомлюючи.

Наприклад, коли користуємося банкоматом. Як? У вас є картка, видана банком (те, що ви маєте), і PIN-код (те, що ви знаєте). Коли ви комбінуєте їх, то машина розуміє, що ви хочете дістати доступ до рахунку, закріпленого за карткою. У деяких країнах банкомати мають додаткові засоби автентифікації, як-от розпізнавання обличчя або відбитка долоні. Це вже називається багатофакторною автентифікацією (БФА).

Такий принцип працює й в інтернеті. Більшість фінансових і медичних установ, а також комерційні імейли та акаунти в соцмережах мають функцію 2ФА. У цьому випадку ви знаєте свій пароль і маєте смартфон. Доступ через телефон вважається зовнішнім каналом, бо девайс ніяк не під'єднаний до вашого комп'ютера. Якщо ви користуєтеся 2ФА, зловмисники не зможуть дістати доступ до захищених так акаунтів без вашого телефона в руці. Скажімо, у вас пошта на Gmail. Щоб увімкнути 2ФА, сервіс попрохає вас додати свій номер телефону. Для верифікації особи Google надішле на цей номер SMS із шестизначним кодом. Вводячи цей код на сайті Gmail, ви підтверджуєте, що цей комп'ютер і номер телефону тепер зв'язані.

Тепер, якщо хтось спробує змінити пароль вашого акаунта з іншого комп'ютера чи телефона, вам надійде про це повідомлення. Сайт дозволить зберегти зміни, лише якщо ввести правильний код верифікації.

Хоча і тут є «але». За словами дослідників зі Symantec, якщо ви таки підтвердите свою особу через SMS, хтось, хто знає ваш номер телефону та основи соціальної інженерії, може вкрасти код скидання захищеного пароля просто з-під носа[26].

Скажімо, я хочу зламати ваш імейл і не знаю пароля. Але знаю ваш номер телефону, бо його легко знайти в ґуґлі. У такому випадку я можу подати запит на

скидання пароля від вашої поштової скриньки, у результаті чого на ваш телефон надійде SMS із кодом, позаяк ви увімкнули 2ФА. Усе цілком надійно, так? Не кваптеся з висновками.

Нещодавня атака на телефон політичного активіста Дерея Маккессона показала, що зловмисники можуть скористатися послугою заміни SIM-карти від вашого мобільного оператора[27]. Інакше кажучи, вони можуть вкрасти ваш номер телефону й отримувати ваші повідомлення — приміром, SMS від Google з кодом для скидання пароля від пошти Маккессона, захищеного двофакторною автентифікацією. Це набагато ефективніше, ніж умовляти вас самостійно озвучити новий пароль із SMS. Хоча й цей фішинговий трюк усе ще працює.

Під час фішингової атаки я не побачу коду верифікації, який надіслав вам імейл-провайдер, тож мені доведеться прикинутися цим провайдером і видурити у вас код. За кілька секунд після SMS від, скажімо, Google я (як зловмисник) надсилаю вам ще одне SMS із текстом: «Google виявив підозрілу активність на вашому акаунті. Щоб припинити несанкціонований доступ, будь ласка, уведіть у відповідь на це повідомлення код, який отримали на телефон».

І так, дійсно, вам щойно надійшло від Google повідомлення з робочим кодом верифікації. А ви через неуважність можете його мені переслати. Якщо я встигну дізнатися код за шістдесят секунд, то зможу зайти на сторінку скидання пароля і, замінивши його своїм, привласнити ваш імейл. Чи будь-який інший акаунт.

Позаяк код у SMS ніяк не зашифрований і може бути вкрадений описаним способом, для більш надійної 2ФА раджу завантажити застосунок Google Authenticator з Google Play чи iTunes. Цей застосунок генеруватиме унікальний код доступу щоразу, як ви заходитимете на сайт із двофакторною автентифікацією. Жодних SMS. Застосунок генерує шестизначний код, який синхронізується з механізмом автентифікації сайту і дозволяє увійти. Однак в айфонах Google Authenticator зберігає «зерно» одноразових паролів у Keychain із налаштуванням «Лише для цього пристрою». Тобто якщо ви створите резервну копію айфону, щоб відновити його на новому пристрої через зміну чи втрату старого, коди з Google Authenticator не перенесуться, а скидати їх — ще та халепа. Раджу вам роздрукувати екстрені коди на випадок, якщо захочете змінити телефон. Однак з допомогою інших застосунків, як-от 1Password, можна робити резервні копії і відновлювати «зерна» одноразових паролів, тож тут проблеми нема.

Якщо ви зареєстрували свій пристрій і заходите на захищений сайт саме з нього, щоразу буде генеруватися новий код доступу. Але в більшості застосунків можна відмітити прапорцем «Довіряти цьому комп'ютеру протягом 30 днів», навіть якщо ви зі своїм ноутбуком чи телефоном перебуваєте в іншому місці. Проте, якщо спробуєте зайти з іншого пристрою (приміром, з комп'ютера вашого чоловіка чи дружини), вам доведеться пройти додаткову автентифікацію. Тож завжди тримайте телефон під рукою, тим паче якщо користуєтесь 2ФА.

Ви, мабуть, читаєте про ці заходи безпеки й запитуєте: а які ж поради я даю тим, хто здійснює в інтернеті фінансові операції?

За 100 доларів на рік ви можете придбати надійний антивірус і брандмауер і встановити їх аж на три комп'ютери. Коли ви «ходите» в інтернеті, можете випадково клікнути на рекламний банер, що містить шкідливе ПЗ. Або відкрити імейл із вірусом. Так чи так, якщо ви часто сидите в інтернеті, то без антивірусу (або з поганим антивірусом, який не здатен усе вловити) рано чи пізно заразите комп'ютер.

Рекомендую витратити приблизно 200 доларів і придбати собі хромбук[28]. Я обожнюю айпади, але вони недешеві. А хромбук так само простий у використанні, як і айпад, хіба що коштує значно дешевше.

Я ось до чого веду: вам потрібен додатковий пристрій виключно для фінансових операцій (а може, і для медичних). Програми встановлюються не на сам хромбук, а на акаунт Gmail, тобто браузер вам буде потрібен лише для серфінгу в інтернеті.

А тепер активуйте 2ФА на бажаному сайті, щоб він міг розпізнати хромбук. Завершивши всі свої операції з банком чи лікарнею, відкладіть хромбук до наступного разу, коли вам знадобиться поповнити рахунок чи записатися на прийом до лікаря.

Забагато клопоту? Так і є. Ви позбавите себе зручності перевіряти свій банківський рахунок будь-де і будь-коли. Але в результаті шанс, що хтось заволодіє вашими фінансовими даними, буде мінімальним. Якщо ви користуєтеся на хромбуці лише двома-трьома застосунками і заходите лише на сайт банку та лікарні із закладок, то спіймати «троян» чи інший вірус майже неможливо.

* * *

То до чого ми з вами дійшли? По-перше, варто створювати надійні паролі й нікому їх не розголошувати. По-друге, вмикати 2ФА, де це можливо. А в наступних розділах ми дізнаємося, як банальні повсякденні дії залишають повсюди цифрові відбитки і як цього уникнути.

---

8 https://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html.

9 https://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html.

10 http://www.wired.com/2014/09/eppb-icloud/.

11 https://www.justice.gov/usao-mdpa/pr/lancaster-county-man-sentenced-18-months-federal-prison-hacking-apple-and-google-e-mail.

12 http://arstechnica.com/security/2015/09/new-stats-show-ashley-madison-passwords-are-just-as-weak-as-all-the-rest/.

13 http://www.openwall.com/john/.

14 Токенізація — технологія, яка підміняє реальні конфіденційні дані випадковою комбінацією символів — цифровим токеном. Використовується для захисту номерів кредитних карток, номерів соціального страхування тощо. — *Прим. пер.*

15 Приклад токена «MaryHadALittleLamb123$» можна отримати на http://www.danstools.com/md5-hash-generator/.

16 http://news.bbc.co.uk/2/hi/technology/3639679.stm.

17 http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

18 http://www.mercurynews.com/california/ci_ 26793089 /warrant-chp-officer-says-stealing-nude-photos-from.

19 http://arstechnica.com/security/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns/.

20 http://www.knoxnews.com/news/local/official-explains-placing-david-kernell-at-ky-facility-ep-406501153-358133611.html.

21 http://www.wired.com/2008/09/palin-e-mail-ha/.

22 http://fusion.net/story/62076/mothers-maiden-name-security-question/.

23 http://web.archive.org/web/20110514200839/http://latimesblogs.latimes.com/webscout/2008/09/4chans-half-hac.html.

24 http://edition.cnn.com/2010/CRIME/11/12/tennessee.palin.hacking.case/.

25 Прикладне програмне забезпечення, що використовують для редагування тексту, відтворення медіа тощо. — *Прим. ред.*

26 http://www.symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access.

27 https://techcrunch.com/2016/06/10/how-activist-deray-mckessons-twitter-account-was-hacked/.

28 Хромбук (від англ. chromebook) — різновид нетбука. При цьому програми не встановлюються на жорсткий диск, а перебувають на дата-серверах і доступні через браузер Chrome. — *Прим. ред.*

Розділ 2

Хто ще читає ваш імейл?

Якщо ви схожі на мене, то щоранку перевіряєте імейл, щойно розплющили очі... і водночас думаєте, хто ще читає ваші листи? Повірте, це не параноя. Якщо ви користуєтеся веб-поштою на зразок Gmail чи Outlook 365, відповідь досить очевидна і зовсім невтішна.

Навіть якщо ви видалите імейл, щойно прочитали його з комп'ютера чи телефона, це необов'язково підчистить усі дані. Десь-таки збережеться копія. Веб-пошта працює на основі хмарних технологій, тож щоб дістати до неї доступ із будь-якого пристрою в будь-який час, резервні копії просто необхідні. Наприклад, якщо ви користуєтеся Gmail, то копії кожного вхідного та надісланого листа з вашої скриньки зберігаються на серверах Google у всьому світі. Те саме і з мейл-клієнтами від Yahoo, Apple, AT&T, Comcast, Microsoft і навіть внутрішньої системи у вас на роботі. Хостингова компанія може в будь-яку мить переглянути будь-який ваш лист. Теоретично це потрібно для блокування вірусів... але по факту треті особи можуть дістати доступ до вашого імейлу з інших, менш благородних і більш корисливих причин.

Мало хто захоче, щоби його листи читав хтось, окрім одержувача. Тому в нас існують закони для захисту як паперової пошти, що доставляється через Поштову службу США, так і електронної. Але на практиці заради принад імейлу нам доводиться йти на певний компроміс. Усі знають, що Yahoo (як і аналогічні сервіси) пропонує веб-мейл послуги безкоштовно, а прибутки отримує з реклами. Але ви навряд чи намагалися пов'язати ці два факти й подумати, як це впливає на вашу конфіденційність.

А от Стюарт Даймонд із Північної Каліфорнії таки задумався. Якось його осінило, що реклама у верхньому правому кутку в його поштовій скриньці на Yahoo не випадкова: вона відповідала змісту надісланих та отриманих листів. Наприклад, якщо я писав у листі про майбутню ділову поїздку в Дубай, рекламний блок пропонував мені авіаквитки, готелі й туристичні маршрути в ОАЕ.

Зазвичай цю деталь ретельно прописано в умовах використання сайту, на які ми автоматично погоджуємося, навіть не читаючи. Ніхто ж не хоче бачити рекламу, яка не відповідає нашим інтересам, так? Позаяк листи подорожують між різними поштовими скриньками Yahoo, компанія має повне і логічне право проглядати зміст імейлів, щоб краще підібрати рекламу й заблокувати спам і віруси.

Однак Даймонд разом із земляком Девідом Саттоном помітили, що зміст листування між їхніми скриньками на Yahoo та імейлами інших веб-мейл сервісів також впливає на рекламу. Тобто компанія читала всі їхні листи, а не лише ті, що подорожували між внутрішніми серверами.

На основі цієї закономірності 2012 року ці двоє подали колективний позов проти Yahoo від імені їхніх 275 мільйонів користувачів і висловили побоювання стосовно дій компанії, що фактично прирівнюються до незаконного шпигування.

Чи поклало це край проблемі? Ні.

Колективні позови мають період досудового пред'явлення й розгляду доказів і період зустрічних дій з обох сторін. У цьому випадку перший етап розтягнувся майже на три роки. У червні 2015-го суд Сан-Хосе, штат Каліфорнія, постановив, що позивачі мають достатньо підстав для розгляду групового позову, і що люди, які надсилали чи отримували листи через сервіс Yahoo з 2 жовтня 2011 року — дати подання першого клопотання, — можуть приєднатися до позову відповідно до закону «Про збережені повідомлення». Крім того, власники поштової скриньки будь-якого іншого веб-мейл сервісу, що проживають у Каліфорнії, теж можуть подати позов відповідно до закону «Про вторгнення в приватне життя». Справа все ще перебуває на розгляді.

Ще один позов із приводу конфіденційності пошти — цього разу проти Google — подали 2014-го. Компанія випадково оприлюднила інформацію про процес проглядання листів й одразу спробувала її видалити чи відредагувати, але так і не змогла. У позові ставилося питання про те, що саме може проглядати Google. За словами позивачів, серед яких було і кілька медіа-гігантів (зокрема й USA Today), Google якоїсь миті зрозумів, що зміст збереженої кореспонденції — це далеко не вся потенційно корисна інформація. У позові стверджувалося, що компанія перейшла до практики проглядання не лише заархівованої пошти, що зберігається на серверах Google, а й листів під час передавання.

Деякі компанії навіть намагалися таємно проглядати імейли з власною метою. Одна така гучна історія трапилася в Microsoft: компанія зізналася, що проглянула пошту користувача Hotmail, який підозрювався у створенні піратської копії їхнього ПЗ. Це здійняло справжній галас, і Microsoft пообіцяла, що буде віддавати подібні справи на розгляд правоохоронних органів.

І така тенденція не обмежується особистим імейлом. Якщо ви надсилаєте лист через внутрішню мережу на роботі, IT-відділ теж може його проглянути та заархівувати. Саме айтішники та їхнє керівництво вирішують, пропустити підозрілий імейл через власні сервери чи залучити правоохоронні органи. До підозрілих відносять листи з комерційною таємницею чи сумнівними матеріалами на зразок порнографії. Також імейли сканують щодо вірусів. Якщо IT-відділ проглядає та архівує ваші листи, то повинен попереджувати вас про свою політику, щоразу як ви входите в систему. Однак більшість компаній цього не робить.

Дехто може примиритися зі скануванням листів стосовно вірусів чи навіть задля реклами. Однак треті особи, що читають нашу кореспонденцію і використовують знайдену в ній інформацію, — це вже занадто. (Звісно ж, якщо не йдеться про дитячу порнографію)[29].

Тож щоразу, як надсилаєте імейл, — хай би яким дріб'язковим він був, хай би як ви його видаляли зі скриньки — існує величезна ймовірність, що весь текст і зображення ретельно просканують і збережуть. Може, не назавжди, але точно надовго. (Деякі компанії ведуть політику короткочасного зберігання, але цілком можна припустити, що більшість зберігає імейли тривалий час).

Тепер, коли ви знаєте, що уряд і компанії читають ваші листи, найменше, що ви можете зробити, — ускладнити їм завдання.

Більшість веб-мейл служб користуються шифруванням для повідомлень під час передавання. Однак коли служби пересилають повідомлення між поштовими серверами, шифрування іноді вимикається, а ваш лист стає вразливим. Наприклад, на роботі ваш начальник має доступ до імейл-системи компанії. Щоб стати непоміченим, вам доведеться зашифрувати повідомлення, тобто заблокувати їх так, щоби розблокувати і прочитати міг лише одержувач. Що таке шифрування? Це — код.

Елементарний приклад шифрування — шифр Цезаря: кожна літера заміняється іншою, зсунутою за алфавітом на певну кількість позицій. Якщо, приміром, зсув дорівнює 2, то за шифром Цезаря «а» стає «в», «в» стає «д», «я» стає «б» тощо. Якщо за подібною схемою зашифрувати моє ім'я, «Кевін Митник» перетвориться на «Мжґйп Ойфпйм»[30].

Ясна річ, більшість сучасних систем шифрування набагато надійніші, ніж звичайний шифр Цезаря. Тобто теоретично зламати їх набагато складніше. Усі типи шифрування об'єднує одне: щоби зашифрувати і дешифрувати повідомлення, потрібен ключ. Симетричне шифрування передбачає, що для цих двох процесів потрібен один і той самий ключ. Однак симетричні ключі важко передавати, коли дві сторони незнайомі чи контактують лише по інтернету, а не наживо.

Тому більшість імейл-сервісів користуються асиметричним шифруванням. У цьому випадку я маю згенерувати два ключі: закритий ключ, який залишається на моєму девайсі і який я нікому не розголошую, і відкритий ключ, який я можу вільно розмістити в інтернеті. Ці два ключі різняться, але математично пов'язані.

Наприклад, Боб хоче надіслати Еліс захищений імейл. Він шукає відкритий ключ Еліс в інтернеті чи питає його в неї особисто, а потім зашифровує своє повідомлення цим ключем. Лист залишатиметься зашифрованим, допоки Еліс — і тільки Еліс! — не введе пароль до закритого ключа і не розблокує зашифроване повідомлення.

То як же ж працює шифрування вмісту вашої поштової скриньки?

Найпопулярніший метод імейл-шифрування — PGP. Технологія не безкоштовна. Вона є продуктом корпорації Symantec. Але її розробник, Філ Цимерман, створив і версію з відкритим кодом — OpenPGP. Оце вже безкоштовно. Є також і третій варіант — GnuPG, створений Вернером Кохом.

Так само безкоштовний. Плюс у тому, що всі три програми — інтероперабельні, тобто основний набір функцій буде однаковим незалежно від версії PGP.
Коли Едвард Сноуден вирішив оприлюднити конфіденційні дані, вкрадені в АНБ, йому знадобилася допомога однодумців, розкиданих у всьому світі. Звучить парадоксально, але йому треба було зникнути з радарів, залишаючись водночас в інтернеті. Він мав стати невидимкою.

Навіть якщо ви не збираєтеся розголошувати державні таємниці, непогано було б зробити свої листи конфіденційними. Своїм прикладом Сноуден та інші продемонстрували, що зробити це непросто, але за належних зусиль цілком можливо.

Для спілкування зі спільниками Сноуден скористався власним імейлом від компанії Lavabit. Однак шлях електронної пошти — не прямий відрізок із двома кінцями: перш ніж потрапити у скриньку одержувача, імейл може пройти через кілька серверів у всьому світі. Сноуден розумів, що його повідомлення може прочитати будь-яка людина, що зможе перехопити його на цьому шляху.

Тож Сноудену довелося виконати складний маневр, щоб створити дійсно безпечний, анонімний і повністю зашифрований канал зв'язку з поборницею конфіденційності і режисеркою Лорою Пойтрас, яка на той час щойно зняла документальний фільм про життя інформаторів. Сноуден прагнув зашифрувати листування з нею, однак її відкритий ключ знали одиниці. Він виявився не таким вже й відкритим.

Щоб відшукати її ключ, Сноудену довелося зв'язатися із третьою стороною — Майком Лі з організації Electronic Frontier Foundation, що бореться за конфіденційність у мережі. Відкритий ключ Лі можна було знайти в інтернеті, і, якщо вірити словам з інтернет-журналу Intercept, він мав відкритий ключ Пойтрас. Лі сказав, що спершу має дізнатися в Лори, чи дозволить вона передати ключ. Пойтрас погодилася[31].

На той час ані Лі, ані Пойтрас і гадки не мали, хто прохав у них відкритий ключ. Сноуден написав їм із конспіративного імейлу, а не з особистого. І тут виникла проблема: якщо ви не так часто користуєтеся PGP, то іноді можете забути прикласти ключ до важливих листів. Це й трапилося зі Сноуденом. Він забув вказати власний відкритий ключ, щоб Лі міг відповісти.

Позаяк жодного безпечного способу зв'язатися із загадковим незнайомцем не було, Лі довелося відповісти Сноудену текстовим, незашифрованим імейлом, щоб попрохати в нього відкритий ключ.

Тобто Лі зіграв роль довіреної третьої особи. Із власного досвіду можу сказати, що перевіряти справжність співрозмовника в захищеній бесіді неабияк важливо, і краще робити це через спільного приятеля. Вам треба переконатися, що ви спілкуєтеся з другом, а не вовком в овечій шкурі.

Я знаю, чому це так важливо, бо й сам колись прикидався іншою людиною. Тоді співрозмовники не поставили під сумнів мою особу чи мій відкритий ключ, що було лише на руку. Якось мені знадобилося було зв'язатися з Ніллом

Кліфтом — аспірантом у галузі органічної хімії британського Університету Лідса, якому вдалося знайти вразливі місця в операційній системі VMS від Digital Equipment Corporation. Я попрохав Кліфта надіслати мені всі «дірки» в системі безпеки, які він описав DEC. Для цього довелося прикинутися співробітником компанії.

Тож спершу я надіслав Кліфту імейл, де назвався таким собі Дейвом Гатчінсом. Незадовго до цього я телефонував Кліфтові від імені Деррелла Пайпера з відділу розробки VMS, тож в імейлі (від Гатчінса) зазначив, що Пайпер хотів би полистуватися з Кліфтом щодо теми проекту. В імейл-системі DEC я знайшов переписку між Кліфтом і справжнім Пайпером, тож моє прохання звучало цілком правдоподібно. Після цього я надіслав хлопцю листа з підробленої імейл-адреси Пайпера.

Щоб переконати Кліфта, що все по-справжньому, я навіть запропонував увімкнути PGP-шифрування, щоби всілякі Кевіни Митники не змогли прочитати наші імейли. Уже незабаром Кліфт і «Пайпер» обмінялися відкритими ключами для зашифрованої бесіди, яку «Пайпер», тобто я, спокійно міг прочитати. Помилка Кліфта була в тому, що він не поставив під сумнів особу Пайпера. Тож коли вам несподівано телефонують з банку й запитують номер соціального страхування чи іншу особисту інформацію, скиньте виклик і перетелефонуйте в банк самостійно. Ніколи не знаєш, хто по той бік слухавки чи екрана.

З огляду на важливість таємниці, яку збирався оприлюднити Сноуден, йому з Пойтрас не можна було користуватися звичайними імейлами. Чому ні? Їхні особисті акаунти містили унікальні деталі, як-от конкретні інтереси чи списки контактів, які могли видати їхню особу. Тому Сноуден і Пойтрас створили нові.

І тут виникла проблема: а як вони дізнаються нові імейл-адреси одне одного? Якщо обидві сторони є абсолютно анонімними, як вони знатимуть, хто є хто і кому можна довіряти? Скажімо, як Сноудену виключити можливість того, що АНБ чи інші служби видають свій імейл за нову адресу Пойтрас? Відкриті ключі — це довжелезний набір символів. Не можна просто так зателефонувати за захищеною лінією і зачитати ключ. Потрібно зашифроване листування.

Тож вони знову завербували Майка Лі як довірену особу, яка підтвердить їхні нові анонімні імейли. Спершу свій новий відкритий ключ Пойтрас передала Лі. Однак ключі PGP-шифрування досить довгі (не як число пі, але теж немаленькі), а за імейлом Лі, знову ж таки, могли стежити. Тому він узяв відкритий ключ Пойтрас, скоротив його до сорока перших символів і виклав у твітер.

Іноді, щоб стати непомітним, доводиться користуватися чимось дуже і дуже помітним.

Тепер Сноуден міг анонімно проглянути твіт Лі й порівняти скорочений ключ із тим, що отримав у імейлі. Якби вони були неоднакові, Сноуден зрозумів би, що отриманий лист — підробка, і цьому імейлу довіряти не можна. Хто знає, а раптом по той бік екрана сидить АНБ.

На щастя, вони були однакові.

Переконавшись у тому, хто вони є в інтернеті і в житті, Сноуден і Пойтрас були майже готові почати анонімне, захищене імейл-листування. Сноуден нарешті надіслав Пойтрас зашифрований імейл, у якому підписався як «Citizenfour», або «Громадянин чотири». Згодом це ім'я стало назвою її оскароносного документального фільму про кампанію Сноудена за права на недоторканність приватного життя.

Здавалося б, кінець історії. Тепер вони можуть безпечно спілкуватися через зашифровані імейли. Але ні. Це був лише початок.

У 2015-му, на хвилі терактів у Парижі, уряди різних країн почали обговорювати можливість створення лазівок чи інших способів дешифрувати імейли, повідомлення та дзвінки — нібито для боротьби з іноземними терористами. Ясна річ, це порушує саму мету шифрування. Але, як ви ще побачите, урядам необов'язково розшифровувати зміст ваших імейлів, щоб дізнатися, з ким ви переписуєтеся і як часто.

Раніше я вже згадував, що мета шифрування — закодувати повідомлення так, щоби розкодувати його могла лише людина з правильним ключем. Те, наскільки легко чи важко буде зламати ваш код без ключа, залежить від надійності математичних алгоритмів і довжини ключа.

Сучасні алгоритми шифрування — відкриті. Ними можна користуватися[32]. А от приватних криптосистем із закритим ключем варто остерігатися. Відкриті алгоритми вже безліч разів перевірили на міцність: користувачі навмисно намагалися їх зламати. Якщо алгоритм із відкритим ключем слабшає чи ламається, він вважається застарілим, а на зміну приходять нові, сильніші алгоритми. Старі варіанти все ще існують, але їх не радять використовувати.

Переважно ключі перебувають під вашим особистим контролем, а отже, як ви вже здогадалися, управління ними — пріоритетне завдання. Якщо ви самостійно генеруєте ключ шифрування, то ви, і лише ви, матимете його на своєму девайсі. А от якщо компанія проводить шифрування (наприклад, «у хмарі») за вас, то вона може залишити собі ключ після того, як передасть його вам. Проблема полягає в тому, що суд може зобов'язати компанію передати ключ правоохоронним чи державним органам — навіть без ордера. Тож раджу спершу прочитати політику конфіденційності й дізнатися, кому належатимуть ключі.

Якщо шифруєте повідомлення — імейл, SMS чи дзвінок — користуйтеся наскрізним шифруванням. Так ваше повідомлення не можна буде прочитати, поки воно не досягне адресата. При наскрізному шифруванні ключ для розкодування маєте лише ви й одержувач. Жодних операторів зв'язку, власників сайту та розробників застосунку, до яких за інформацією про вас звертаються правоохоронні й державні органи. Як дізнатися, чи пропонує той чи той сервіс наскрізне шифрування?

Заґуґліть список «наскрізне шифрування телефонних дзвінків». Якщо вашого застосунку чи сервісу там нема, то краще виберіть щось інше.

Звучить надто складно? Так і є. Однак існує кілька PGP-плагінів для браузерів Chrome та Firefox, які зроблять шифрування простішим. Наприклад, Mailvelope, який обережно й грамотно поводиться з відкритими та закритими ключами. Просто введіть парольну фразу, на основі якої хочете створити відкритий і закритий ключ. Тепер щоразу, як писатимете електронне повідомлення одержувачеві, який має відкритий ключ, плагін пропонуватиме вам надіслати цій людині зашифрованого листа[33].

* * *

Однак навіть якщо ви зашифруєте імейл за допомогою PGP, невеличка, але інформаційно цінна частка все ще доступна всім і кожному. У спробі відхреститися від слів Сноудена уряд США неодноразово заявляв, що не читає сам зміст наших листів, у цьому випадку PGP-шифрування, і не дасть прочитати. Вони лиш збирають метадані.

Що ж таке «метадані електронної пошти»? Це — дані про те, від кого й кому прямує лист, а також IP-адреси всіх серверів, через які пройшов цей лист на шляху до одержувача. Також сюди входить графа «Тема», яка іноді може частково розкривати зміст зашифрованого повідомлення. Метадані — рудимент з епохи зародження інтернету, але він усе ще присутній у кожному вхідному та надісланому імейлі. Просто сучасні «читачі» імейлів приховують цю інформацію від широкого загалу[34].

Хоч би яку програму для PGP-шифрування ви взяли, вона не зашифрує метадані, тобто графи «Кому», «Від кого», «Тема» та інформацію про мітки часу. Вони залишаються в тексті листа, навіть якщо ви цього і не бачите. І треті особи все ще можуть проглянути ваші метадані. Вони знають, що такого-то дня ви відправили імейл такій-то людині, через два дні відправили їй ще один імейл тощо.

Здавалося б, не біда. Вони ж не читають сам імейл, а вас не хвилюють транспортні деталі, як-от адреса серверів і мітки часу. Але ви не повірите, скільки можна дізнатися лише з одного маршруту та частоти імейлів.

У дев'яностих, коли мені ще не доводилося грати у схованки із ФБР, я проводив так званий аналіз метаданих телефонних записів. Почав я з того, що зламав лос-анджелеського мобільного оператора PacTel Cellular і дістав детальний звіт про дзвінки інформатора, який оповіщав ФБР про мою діяльність.

Детальні звіти дуже схожі на вищезгадані метадані: у них зазначається час дзвінка, набраний номер, тривалість розмови і частота виклику цього номера. Усе це — дуже корисна інформація.

Проглянувши історію дзвінків, які надходили через PacTel Cellular на стаціонарний телефон інформатора, я зміг дізнатися, з яких мобільних номерів йому телефонують. Спираючись на виставлені цим номерам рахунки за зв'язок, я зміг встановити їхню належність до відділу боротьби з посадовими злочинами ФБР, який працює за межами Лос-Анджелесу. Також кілька номерів належали

внутрішнім відомствам: лос-анджелеському офісові ФБР, прокуратурі та державним установам. Деякі з розмов були досить тривалими. І досить частими.

Щоразу як ФБР перевозило інформатора на іншу конспіративну квартиру, я діставав новий номер стаціонарного телефону, бо агенти телефонували на нього відразу після повідомлення на пейджер інформатора. А через номер стаціонарного телефону я вже дізнавався реальну адресу: доводилося трохи погратися в соціальну інженерію і прикинутися співробітником Pacific Bell — телефонної компанії, яка обслуговувала нову квартиру.

Соціальна інженерія — це метод зламу на основі маніпуляції, обману та психологічного впливу з метою змусити людину виконати певні дії. У такий спосіб у нас часто виманюють конфіденційну інформацію. У цьому випадку я знав внутрішні номери телефонної компанії і міг видати себе за технічного співробітника. До того ж я володів потрібною термінологією та професійним жаргоном — украй цінними інструментами для отримання конфіденційної інформації.

Тож хай метадані електронної пошти і не розкривають змісту листа, вони все одно містять досить цінні з погляду конфіденційності дані.

Якщо ви подивитеся на метадані будь-якого нещодавнього імейлу, то знайдете IP-адреси всіх серверів, через які пройшло ваше повідомлення, перш ніж потрапити до адресата. Кожен сервер, як і кожен користувач в інтернеті, має унікальну IP-адресу — набір цифр, який вираховується на основі вашої країни та інтернет-провайдера. IP-адреса поділяється на блоки залежно від країни, на підблоки залежно від інтернет-провайдера і далі за типом послуги: інтернет-модем, кабель чи мобільний. Якщо ви придбали собі статичний IP, то він буде прив'язаний до вашого акаунта користувача та домашньої адреси. Якщо ж ні, то ваша зовнішня IP-адреса щоразу генеруватиметься на основі купи адрес, що належать вашому провайдерові. Наприклад, IP-адреса відправника, який надсилає вам імейл, має такий вигляд: 27.126.148.104. Це — штат Вікторія, Австралія.

А от якщо це буде 175.45.176.0, що говорить про Північну Корею, то вашу поштову скриньку можуть відправити на урядову перевірку. Державні установи США захочуть дізнатися, чому ви листуєтеся з кимось із Північної Кореї, навіть якщо тема листа — «З днем народження».

Можливо, сама собою адреса серверів не така вже й цікава. А от частота контакту — це вже щось. Тим паче в поєднанні з такими деталями, як місця розташування відправника й одержувача. На цьому етапі вже можна будувати певні припущення. Приміром, метадані телефонних дзвінків (тривалість, час доби тощо) можуть немало сказати про психічне здоров'я людини. Вечірній дзвінок на гарячу лінію з питань домашнього насильства тривалістю в десять хвилин чи нічний виклик із Бруклінського мосту на гарячу лінію для самогубць на двадцять хвилин можуть бути дуже показовими. У Дартмутському коледжі навіть розробили застосунок, який перевіряє користувацькі дані щодо стресу,

депресії та самотності. Дослідження показало, що активність в інтернеті залежить навіть від оцінок в університеті[35].

Усе ще не бачите в метаданих загрози? Програма Immersion («Занурення») з MTI здатна на основі метаданих встановити стосунки між відправником та одержувачем кожного імейлу, що зберігається у вашій скриньці. Нею користуються, щоб візуально підрахувати, хто для вас важить найбільше. Програма навіть виводить графік, де показано, як зростає й падає важливість конкретної особи для вас із плином часу. Хоча ви прекрасно розумієте свої стосунки зі співрозмовниками, побачити це в графічному вигляді — досить повчальний досвід. Ви можете навіть не уявляти, як багато пишете людям, яких майже не знаєте, і як мало тим, яких знаєте близько. З Immersion ви можете вирішити, чи варто завантажувати дані, а також видалити всю інформацію, щойно програма побудує графік[36].

За словами Сноудена, АНБ та інші служби збирають метадані наших імейлів, повідомлень і дзвінків. Але ж уряд не може зібрати дані на всіх і кожного... чи може? Технічно, ні. Однак з 2001 року спостерігається різкий стрибок щодо «законного» збирання інформації.

Відповідно до Акту про негласне спостереження з метою зовнішньої розвідки 1978 року (FISA), Суд із нагляду за зовнішньою розвідкою США (FISC) контролює всі запити щодо ордерів на спостереження за іноземними особами в Сполучених Штатах. Те, що між правоохоронними органами та громадянами стоятиме судовий наказ, на перший погляд, досить логічний крок. Але на практиці все інакше. Лише 2012-го з 1856 запитів суд задовольнив усі 1856. Тобто така процедура — лише формальність[37]. Після того як суд видасть дозвіл, правоохоронні органи можуть змусити будь-яку приватну компанію видати всі дані на вас. Звісно ж, якщо вони все ще не зробили цього добровільно.

Щоби стати в цифровому світі по-справжньому невидимим, вам доведеться піти трохи далі звичайного шифрування повідомлень.

Приховайте реальну IP-адресу. Вона — ваша точка дотику до інтернету, ваш відбиток пальця. IP здатен видати ваше місцеперебування (аж до домашньої адреси) та інтернет-провайдера.

Приховайте інформацію про апаратне та програмне забезпечення. Деякі сайти збирають інформацію про ваше ПЗ та «залізо», щойно ви на них заходите. Кілька трюків — і можна легко дізнатися, чи встановлена у вас та чи та програма, приміром, Adobe Flash. Браузер же видає сайтові вашу операційну систему, її версію, а іноді й інформацію про те, які ще програми відкрито у вас зараз.

Захистіть свою анонімність. Установлення фактів у мережі — справа не з легких. Дуже важко довести, що ви були за комп'ютером, коли трапилася та чи та подія. Але якщо ви пройдетеся перед камерою в Starbucks чи придбаєте там лате по картці перед тим, як зайти в інтернет з їхнього вай-фаю, це можна буде пов'язати з вашими діями в мережі.

Отже, щоразу за під'єднання до інтернету відповідає певна IP-адреса[38]. Це досить проблематично, якщо ви намагаєтеся бути непомітними в інтернеті: ви можете змінити ім'я (або взагалі його не вказувати), але IP все одно видаватиме ваше місцеперебування, провайдера та особу людини, що сплачує за інтернет (якою можете бути ви). Усі ці крихти інформації зберігаються серед метаданих електронної пошти і можуть вказати на вас особисто. Будь-яке спілкування в інтернеті (необов'язково навіть по електронній пошті) може допомогти ідентифікувати вас на основі IP-адреси вашого роутера вдома, на роботі чи в товариша.

Ясна річ, IP-адреси в імейлах можна підробити. Наприклад, скористатися проксі-сервером, тобто не справжнім IP, а чужою адресою. Так імейл буде надходити з начебто іншого місця. Проксі — це як перекладач: ви кажете текст перекладачеві, а він передає його іншомовній людині. Хіба що тут повідомлення не змінюється. Так людина, яка надсилає повідомлення з Північної Кореї, може скористатися проксі-сервером у Китаї чи навіть Німеччині.

Замість того щоб самому створювати проксі-сервер, можна звернутися до так званого анонімного ремейлера, який маскує справжній IP вашого імейлу за вас. Анонімний ремейлер просто замінює адресу відправника перед тим, як переслати лист вказаному одержувачеві, який теж може відповісти через ремейлер. Це — найпростіший варіант.

Існують різні варіації ремейлерів. Наприклад, деякі ремейлери типів I і II не дають змоги відповідати на лист; вони призначені лиш для одностороннього листування. А от сервери типу III, що працюють за стандартом Mixminion, пропонують повний спектр послуг: відповідь, пересилання та шифрування. Якщо вибираєте цей спосіб анонімного листування, обов'язково поцікавтеся, до якого типу належить ваш ремейлер.

Ще один спосіб приховати реальну IP-адресу — цибулева маршрутизація (Tor), якою і скористалися Сноуден і Пойтрас.

Програму з відкритим вихідними кодом Tor розробила Дослідницька лабораторія Військово-морських сил США ще 2004-го, вона призначалася для військовослужбовців, яким необхідно було приховувати своє місцеперебування під час пошуків в інтернеті. Відтоді програма поширилася на весь світ. Tor — знахідка для людей, що живуть за жорстокого режиму й потерпають від цензури в ЗМІ та інших сферах життя, і тих, хто хоче зробити свій пошук в інтернеті конфіденційним. Tor безкоштовний, і його може завантажити будь-хто і будь-де. Навіть ви.

Як Tor працює? Він змінює звичну схему доступу до сайту.

Зазвичай, щоби зайти в інтернет, ви відкриваєте браузер і вводите адресу потрібного сайту. На цей сайт надсилається запит, і вже через кілька мілісекунд ваш браузер отримує відповідь у вигляді веб-сторінки. Сайт уже знає (через IP-адресу), який у вас інтернет-провайдер і навіть де ви перебуваєте, зіставивши місцеперебування вашого провайдера й затримку хопів[39] між вашим девайсом і

сайтом. Наприклад, якщо ваш девайс показує, що ви нібито перебуваєте в США, але час і кількість хопів, за які ваш запит досягає сайту, не відповідають локації, то деякі сайти (особливо сайти з іграми) запідозрять вас у фальсифікації.

Коли ви робите це через Tor, то пряма лінія між вами й сайтом викривляється додатковими вузлами, і кожні десять секунд цей ланцюжок вузлів видозмінюється, не перериваючи вашого зв'язку із сайтом. Ці численні вузли, що з'єднують вас із сайтом, нагадують шари цибулини. Інакше кажучи, якщо хтось захоче простежити маршрут від сайту до вас, то в нього не вийде, бо цей маршрут постійно змінюється. Якщо зв'язок між вашими точками входу й виходу якось не спливе на поверхню, з'єднання вважається анонімним.

Якщо ви використовуєте Tor, ваш запит на відкриття сторінки — скажімо, mitnicksecurity.com — надходить не до самого сервера сайту, а до вузла Tor. Щоб заплутати шлях ще більше, цей вузол передає запит іншому вузлу, а той вже сайтові mitnicksecurity.com. Тож маємо вхідний вузол, проміжний вузол і вихідний вузол. Якщо я захочу подивитися, хто відвідав мій сайт, то побачу лише IP-адресу та інформацію з вихідного вузла (останнього в ланцюжку), а не вашого вхідного (першого в ланцюжку). Ви можете налаштувати Tor так, щоб він створював вихідні вузли в конкретній країні — наприклад, Іспанії — або навіть призначити конкретний вузол виходу в якомусь Гонолулу.

Щоб скористатися Tor, вам доведеться завантажити модифікований браузер Firefox із сайту Tor (torproject.org). Завжди шукайте офіційний браузер, сумісний з вашою оперативною системою, і лише на сайті проекту Tor. Не варто завантажувати його зі сторонніх ресурсів. Для систем на базі Android підійде Orbot — безкоштовний застосунок від Tor у Google Play, який одночасно шифрує ваш трафік і приховує IP-адресу[40]. Для девайсів із системою iOS (айпад, айфон) офіційним є браузер Onion Browser, який можна завантажити з iTunes.

Ви, напевно, думаєте: чому б їм не зробити всередині Tor імейл-сервер? А вони й зробили. Сервіс Tor Mail розмістили на сайті, доступному лише для користувачів Tor-браузерів. Однак ФБР вилучило сервер у справі, що до нього жодного стосунку не мала, і в такий спосіб дістало доступ до всіх зашифрованих імейлів у Tor Mail. Ця повчальна історія демонструє: навіть коли здається, що ваша інформація в абсолютній безпеці, це не так[41].

Хоча й Tor спирається на спеціальну мережу, через нього все одно можна зайти у звичайний інтернет, просто сторінки будуть завантажуватися повільніше. Однак додатково до інтернету Tor дає вам доступ до цілого всесвіту сайтів, які так просто не знайти — так званої «темної мережі», або даркнету. Адреси цих сайтів не схожі на звичні нам: замість «com» вони мають закінчення «onion». Деякі з цих прихованих сайтів пропонують товари та послуги, що вважаються нелегальними; деякі ж — цілком законні сайти, створені людьми в країнах із жорстким режимом.

Однак варто зазначити, що в Tor є кілька недоліків:

- ви не контролюєте вихідних вузлів, які можуть перебувати під

контролем урядових чи правоохоронних органів[42];
- при бажанні, вас усе ще можна ідентифікувати й зібрати на вас інформацію[43];
- Tor дуже повільний.

Якщо попри це ви все ще захочете завантажити Tor, виділіть для нього окремий девайс. Заходьте в інтернет через звичайний браузер з одного ноутбука, а через Tor — з іншого (наприклад, придбайте мінікомп'ютер Raspberry Pi й установіть на нього Tor). Якщо хтось зламає ваш комп'ютер, то однак не зможе дістатися транспортного рівня Tor, позаяк той установлений на іншому пристрої[44].

Як я вже казав, у випадку Сноудена та Пойтрас спілкуватися просто через зашифровані імейли було не дуже безпечно. Створивши новий відкритий ключ для анонімного імейлу, Пойтрас могла надіслати його на попередню адресу Сноудена. Але якби хтось проглядав той акаунт, вона б скомпрометувала свою нову пошту. Головне правило: тримайте свої анонімні акаунти подалі від усього, що може вказати на вашу справжню особу.

Щоб стати невидимим, доведеться почати з чистого аркуша. Для нових контактів використовуйте лиш нову безпечну пошту. Застарілі імейл-акаунти можуть несподівано вивести на інші частини вашого життя: друзів, хобі, роботу. Створюючи новий імейл для таємного спілкування, використовуйте Tor, щоб IP-адресу, з якої реєструється новий акаунт, не можна було ніяк пов'язати з вами.

Створити анонімну імейл-адресу важко, але можливо. Існує немало безпечних мейл-клієнтів. Але краще вибирайте безкоштовні: якщо ви заплатите, то залишите фінансовий слід. І ще невелика проблема: Gmail, Microsoft, Yahoo та інші сервіси вимагають від вас номер телефону, щоб підтвердити особу. Ясна річ, реальний номер давати не можна, бо він може вказати на ваше реальне ім'я та адресу. Непоганий варіант — телефонний номер Skype, якщо сервіс підтримує не лише SMS-автентифікацію, а й голосову. Однак і тут вам знадобиться вже готовий імейл і подарункова картка, щоб зареєструвати номер у Skype[45]. Якщо думаєте, що передплачений телефон сам собою захистить вашу анонімність, то помиляєтеся. Якщо ви хоч раз скористаєтеся таким телефоном для дзвінка, пов'язаного з реальним життям, то викрити вашу особу буде лише справою часу.

Краще придбайте одноразовий телефон. Дехто вважає, що одноразовими телефонами користуються лише терористи, сутенери й наркоторговці, але вони стануть у пригоді і в цілком законних цілях. Наприклад, одна бізнес-журналістка переключилася на одноразові телефони, коли все її сміття перерили приватні детективи, яких найняли Hewlett-Packard у спробі дізнатися, хто «зливає» важливу інформацію щодо ради директорів. Відтоді вона розмовляла зі своїм інформатором лише по цьому одноразовому телефону, бо так детективам було важче відстежити її дзвінки[46]. А ще телефон, який не потребує контракту (або акаунта в Google чи Apple, якщо вже на те пішло), може подарувати трохи спокою дівчині, яка уникає жорстокого колишнього.

Одноразові телефони мають обмежений доступ в інтернет або взагалі його не мають. Вони створені переважно для дзвінків та обміну повідомленнями або імейлами — для декого більше і не треба. Але одноразовий телефон можна прив'язати до ноутбука і спокійно сидіти з нього в інтернеті. (У розділі 7 я розповім, як на ноутбуці змінити адресу управління доступом до середовища (MAC), щоб одноразовий телефон сприймався як новий пристрій, щоразу як ви прив'язуєте його до комп'ютера).

Однак придбати одноразовий телефон анонімно — завдання не з легких. Ваші дії в реальному світі можуть допомогти ідентифікувати вас у світі віртуальному. Але ж я можу придбати одноразовий телефон і сто хвилин на розмови у Walmart за готівку. Хто про це дізнається? Багато хто.

Почнемо з того, як я дістався до Walmart. Замовив убер? Узяв таксі? Усі ці записи може вилучити суд.

Я міг би поїхати на власній машині, але правоохоронні органи встановили автоматичну технологію розпізнавання номерних знаків на великих парковках для пошуку зниклих і вкрадених автомобілів, а також людей, на арешт яких є ордер. Записи системи розпізнавання може вилучити суд.

Навіть якщо я піду у Walmart пішки, на вході моє обличчя засвітиться на кількох камерах безпеки, а це відео теж може вилучити суд.

Гаразд. Припустимо, я відправлю до магазину когось замість себе. Когось, кого я навіть не знаю. Може, безхатька, якого я найняв на вулиці. Він зайде у Walmart та придбає телефон і кілька передплачених карток за готівку. Це — найбезпечніший варіант. З «кур'єром» я домовлюся зустрітися пізніше десь подалі від магазину — це допоможе фізично дистанціюватися від фінансової операції. Однак і в цьому плані найслабше місце — людина. Чи можете ви їй довіряти? Якщо пообіцяєте заплатити зверху більше за вартість телефона, то безхатько, найімовірніше, із радістю доставить вам девайс.

Для активації передплаченого телефона треба або зателефонувати у службу підтримки мобільного оператора, або активувати його на сайті провайдера. Щоб уникнути запису дзвінка «з метою підвищення якості послуг», краще проводьте активацію в інтернеті. Зробити це в Tor-браузері через відкриту Wi-Fi мережу після зміни MAC-адреси — найменше, що ви можете зробити для конфіденційності. Уся інформація, яку ви вказуєте на сайті, має бути вигаданою. Для графи «Адреса» загуґліть і скопіюйте адресу будь-якого готелю. Дату народження й PIN-код придумайте такі, щоби згадати, якщо доведеться зв'язуватися зі службою підтримки в майбутньому.

Є й імейл-сервіси, які не потребують верифікації. А якщо ви не переховуєтеся від влади, то під час реєстрації акаунта, скажімо, в Google підійде і номер у Skype. Але для наочності уявіть таку ситуацію: ви приховали IP-адресу через Tor, створили Gmail-акаунт, який не має нічого спільного з реальним номером телефону, після чого Google відправив вам на телефон код верифікації чи подзвонив. Тепер у вас є акаунт на Gmail, який майже неможливо відстежити.

Отже, ми маємо анонімний імейл на знайомому й популярному сервісі. А також можемо надсилати більш-менш безпечні листи, де IP-адреса завдяки Tor прихована (хоча у вас все ще нема контролю над вихідними вузлами), а зміст завдяки PGP не може прочитати ніхто, крім одержувача.

Зверніть увагу, що для збереження анонімності акаунта в нього можна заходити лише через Tor — так вашу реальну IP-адресу до нього ніхто не прив'яже. Крім того, ніколи нічого не шукайте в інтернеті, поки не вийдете з анонімного акаунта: ви можете ненавмисно заґуґлити щось пов'язане з вашою реальною особою. Навіть погоду не перевіряйте, бо вкажете на своє місце перебування[47]. Як бачите, щоб стати непомітним і залишатися непомітним, потрібна шалена витримка й постійна увага. Однак непомітність того варта.

Ось те, що вам просто необхідно закарбувати: тримайте в голові всі способи, якими вас можна ідентифікувати, навіть якщо використовуєте кілька описаних заходів безпеки. Якщо ж користуєтеся всіма, будьте уважні кожного разу, як заходите в анонімний акаунт. Кожного. Без винятків.

Також варто повторити, що наскрізне шифрування — метод, який порівняно зі звичайним шифруванням не дасть прочитати ваше повідомлення, поки воно не досягне адресата — дуже і дуже важливе. Крім того, наскрізним шифруванням можна користуватися і з іншою метою (приміром, для зашифрованих дзвінків і миттєвих повідомлень), про що й поговоримо у двох наступних розділах.

---

29 Якщо вам цікаво, зображення сексуального насильства над дітьми ідентифікуються Національним центром для зниклих і експлуатованих дітей. У такий спосіб автоматичні системи сканування від Google та інших пошуковиків відрізняють ці фотографії від непорнографічних. Див. http://www.dailymail.co.uk/news/article-2715396/Google-s-email-scan-helps-catch-sex-offender-tips-police-indecent-images-children-Gmail-account.html.

30 http://www.braingle.com/brainteasers/codes/caesar.php.

31 https://theintercept.com/2014/10/28/smuggling-snowden-secrets/.

32 Наприклад, список можна зайти за посиланням: https://en.wikipedia.org/wiki/Category:Cryptographic_algorithms.

33 Mailvelope працює з Outlook, Gmail, Yahoo Mail і ще кількома мейл-клієнтами. Див. https://www.mailvelope.com/.

34 Щоб проглянути метадані у вашому Gmail-акаунті, відкрийте його, клікніть на три крапки у верхньому правому кутку листа. Серед опцій («Відповісти», «Переслати» тощо) буде графа «Показати оригінал». У Apple Mail потрібно вибрати лист, потім Вигляд>Повідомлення>Усі заголовки. В Yahoo натисніть «Більше», потім «Переглянути повний заголовок». Така функція є і в інших мейл-клієнтах.

35 http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-privacy.

36 https://immersion.media.mit.edu/.

37 http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubberstamp-for-government-requests.

38 Можете заґуґлити «IP-адреса» й дізнатися власний IP на момент запиту.

39 Хоп — назва процесу передавання мережевого пакета між вузлами мережі. Зазвичай використовується для визначення «відстані» між вузлами. — *Прим. пер.*

40 https://play.google.com/store/apps/details?id=org.torproject.android.

41 http://www.wired.com/threatlevel/2014/01/tormail/.

42 https://www.theguardian.com/technology/2014/oct/28/tor-users-advised-check-computers-malware.

43 http://arstechnica.com/security/2014/07/active-attack-on-tor-network-tried-to-decloak-users-for-five-months/.

44 Щодо інформації про ПЗ Tor на Raspberry Pi можете звернутися, приміром, до порталу: https://github.com/grugq/PORTALofPi.

45 https://www.skype.com/en/features/online-number/.

46 http://www.newyorker.com/magazine/2007/02/19/the-kona-files.

47 Знову ж таки, краще не користуватися великими імейл-провайдерами на зразок Google. Тут я використовую цей приклад для наочності.

Розділ 3

Прослуховування для чайників

Ледь не щодня ви проводите з телефоном у руці. Годинами балакаєте, переписуєтеся, лазите в інтернеті. А чи знаєте ви, як цей телефон працює?

Стільниковий зв'язок, закладений в основу наших мобільних девайсів, — бездротовий і залежить від стільникових веж, або базових станцій. Для підтримки зв'язку мобільні телефони мають передавач, який постійно надсилає сигнали до найближчої станції або станцій. Рівень зворотного радіосигналу від станцій до передавача має вигляд на телефоні як позначка з певною кількістю «паличок». Нема паличок — нема сигналу.

Щоб захистити особу абонента, в основу роботи передавачів закладено міжнародний ідентифікатор користувача мобільного зв'язку (IMSI), простіше кажучи — унікальний номер, закріплений за вашою SIM-картою. Ця практика бере початок із часів, коли стільниковим операторам уперше знадобилася інформація, яка станція вас обслуговує і коли ви в роумінгу (тобто користуєтеся станціями інших операторів). Перша частина IMSI-номера ідентифікує оператора мобільного зв'язку, друга — ваш мобільний телефон.

Правоохоронні органи розробили пристрої, які видають себе за базові станції стільникового зв'язку і призначені для перехоплення голосових і текстових повідомлень. Також наші представники закону і спецслужби користуються пристроями для визначення IMSI-номерів (див. розділ 13). IMSI ідентифікується миттєво — менш ніж за секунду — і абсолютно непомітно. Зазвичай перехоплювачами IMSI користуються на масових мітингах, особливо коли учасники активно закликають інших приєднатися: так правоохоронні органи знатимуть, хто був присутній.

Подібні пристрої також іноді використовують у застосунках із прокладання маршрутів, щоб зібрати звіт про рух на дорозі. Тут уже потрібен не сам IMSI-номер, а інформація про те, як швидко ваш телефон рухається з однієї базової станції чи точки на карті до іншої. Час, за який сигнал телефона переміщується з однієї станції до іншої, визначає завантаженість дороги: червона, жовта чи зелена[48].

Ваш мобільний телефон під'єднується відразу до кількох базових станцій, тільки-но вмикається. Найближча станція обробляє дзвінки, повідомлення чи пошук в інтернеті. Якщо ви рухаєтеся, то сигнал телефона рухається разом із вами і перемикається на найближчу вежу, не перериваючи зв'язку. Інші вежі поблизу перебувають у режимі очікування, тож якщо ви переміщуєтеся з точки А в точку Б і найближчою стає вже інша станція, передавання сигналу відбувається плавно і не припиняє дзвінка.

Якщо коротко, то ваш телефон випромінює сигнал з унікальним номером, який реєструється у стільникових вежах поблизу. Якщо хтось продивиться логи

конкретної станції, то отримає тимчасові ідентифікатори користувачів мобільного зв'язку (TMSI) усіх людей на певній території в певний момент часу, навіть якщо вони наразі нікому не телефонують. Правоохоронні органи мають право вилучити в операторів мобільного зв'язку ці дані, зокрема внутрішню інформацію про конкретних абонентів.

Зазвичай логи базової станції інформації дають небагато: лиш те, що певна людина проходила повз і її телефон «зчепився» з певною стільниковою вежею в режимі очікування. Якщо в цей момент із телефона здійснювався дзвінок чи передавалася інформація, у логах буде запис про цей дзвінок і його тривалість.

А от через логи кількох базових станцій можна визначити, де перебуває користувач. Більшість мобільних девайсів зчіпляються з більш як трьома станціями одночасно. Якщо продивитися логи з усіх цих веж і визначити відносну силу кожного зчеплення, можна досить точно вирахувати місце розташування телефона користувача. Тобто смартфон, який ви кожного дня тягаєте в себе в кишені, по суті є «жучком».

Як же ж захиститися від стеження?

У контракті з оператором мобільного зв'язку треба вказати ім'я, адресу та номер соціального страхування. Крім того, потрібна перевірка вашого банківського рахунку, щоб переконатися, що ви зможете платити щомісяця за послуги. Якщо підписуєте контракт із комерційним оператором, то цього не уникнути.

Одноразовий телефон — непоганий варіант. Передплачений телефон, який можна змінювати досить часто (скажімо, щомісяця чи навіть щотижня), робить ваш слід не таким помітним. Ваш TMSI буде з'являтися в логах базових станцій і відразу зникати. Телефон аж ніяк не вкаже на вашу реальну особу, якщо ви придбали його таємно. Передплачені телефони також реєструються на абонентські облікові записи. Ваш IMSI завжди буде прив'язаний до певного абонента. Тож ваша анонімність залежить лише від того, наскільки непомітно ви придбали одноразовий телефон.

Ну, добре. Припустимо, ви змогли провернути купівлю одноразового телефона так, щоб її не можна було пов'язати з вами. Приміром, скористалися порадою в минулому розділі й попрохали придбати девайс за готівку незнайому людину. Тепер цей телефон неможливо відстежити? Можна.

Ось вам повчальна історія: якось у 2007-му контейнер із екстазі на 500 мільйонів доларів зник із порту в австралійському Мельбурні. Власник контейнера і відомий наркоторговець, Пет Барбаро, дістав із кишені один із дванадцяти телефонів і подзвонив місцевому журналістові Ніку Маккензі, який проводив журналістське розслідування у справі і знав Пета під фальшивим ім'ям Стен.

Опісля Барбаро написав Маккензі вже з іншого одноразового телефона, намагаючись дістати інформацію про перебіг розслідування щодо контейнера. Забіжу наперед і скажу, що це не спрацювало.

Попри поширене переконання, одноразові телефони не є цілком анонімними. Згідно із законом США «Про допомогу та сприяння провайдерів телекомунікаційних послуг правоохоронним органам» (CALEA), інформація про всі IMSI-номери одноразових телефонів так само доступна, як і дані про номери контрактних абонентів. Інакше кажучи, правоохоронні органи можуть знайти в логах одноразовий телефон так само легко, як і зареєстрований. Так, IMSI-номер не вкаже на вашу реальну особу. Але за нього це може зробити схема використання.

В Австралії, де такого закону не існує, представники закону стежили за купою телефонів Барбаро більш традиційними методами. Наприклад, вони могли помітити в логах дзвінок з його особистого номера, а за кілька секунд — ще один дзвінок чи повідомлення з одноразового телефона, який зареєструвала та сама станція. Згодом на основі інформації про те, що ці IMSI-номери зазвичай реєструє та сама станція, можна зробити висновок, що вони належать одній особі.

Проблема Барбаро полягала в тому, що хоч би яким телефоном він скористався — особистим чи одноразовим, — сигнал реєструвала одна й та сама базова станція, якщо Барбаро не рухався з місця. Дзвінки з одноразового мобільного завжди йшли поряд із дзвінками з особистого телефона. Останній був зареєстрований в оператора на справжнє ім'я, а отже, особу Барбаро можна було легко встановити і відстежити. Завдяки тому, що схема повторювалася з різними станціями, правоохоронні органи змогли завести на Барбаро серйозну справу, а влада — засудити його за постачання однієї з найбільших партій екстазі в історії Австралії.

Маккензі після цього сказав: «З того дня, як телефон задзвонив у мене в кишені, а "Стен" ненадовго увійшов у моє життя, я чітко усвідомив: байдуже, наскільки людина обережна. Вона завжди залишає слід»[49].

Звісно ж, можна користуватися лише одноразовим телефоном. Тоді вам доведеться час від часу анонімно купувати додаткові хвилини за передплачені картки чи біткоїни, що можна зробити через відкриту Wi-Fi мережу після зміни MAC-адреси на бездротовій мережевій карті (див. розділ 7), перед цим переконавшись, що не потрапили в поле зору камер. Або, як я вже казав, можете найняти незнайомця, який придбає в магазині за готівку передплачений телефон і кілька карток поповнення[50]. Це буде дорожче і не так зручно, але так ви отримаєте анонімний телефон.

Хоча мобільні телефони й здаються нам сучасним винаходом, технології стільникового зв'язку вже більше ніж сорок років. Вона, як і дротяні стаціонарні телефони, працює на застарілих технологіях, які можуть поставити під загрозу нашу конфіденційність.

Із кожним поколінням стільникові телефони отримували нові фупкції, спрямовані в основному на ефективніше передавання даних. Телефони першого покоління, або 1G, були розроблені ще на початку 1980-х. Перші 1G-мережі та

телефони були аналоговими й використовували безліч тепер уже застарілих мобільних стандартів. У 1991 році широкому загалу презентували цифрову мережу другого покоління (2G), яка спиралася на два стандарти: глобальну систему мобільного зв'язку (GSM) і множинний доступ із кодовим розділенням каналів (CDMA). Також на практиці було реалізовано службу коротких повідомлень (SMS), неструктуровані дані додаткових служб (USSD) та інші прості протоколи зв'язку, якими й досі користуються. Зараз ми на етапі 4G/LTE і вже рухаємося до 5G.

Незалежно від того, яким поколінням користується той чи той оператор зв'язку (2G, 3G, 4G чи 4G/LTE), в основі однак лежить головний міжнародний сигнальний протокол — система сигналізації. Протокол системи сигналізації (наразі версія 7) разом з іншими протоколами не дає дзвінку перерватися, коли ви їдете по автостраді й перемикаєтеся з однієї базової станції на іншу. А ще його використовують для спостереження. По суті, система сигналізації 7 (SS7) робить усе, пов'язане з дзвінком, а саме:

- проводить з'єднання для дзвінка;
- перериває з'єднання, коли дзвінок завершується;
- стягує оплату за дзвінок з відповідного абонента;
- відповідає за управління додатковими функціями, як-от переадресація виклику, відображення імені й номера абонента, що здійснює вхідний дзвінок, режим конференції та інші служби інтелектуальної мережі;
- відповідає за дзвінки на безкоштовні (800 та 888) й платні (900) номери;
- надає бездротові послуги, зокрема ідентифікацію абонента й оператора та мобільний роумінг.

Виступаючи на щорічному Всесвітньому конгресі хакерів у Берліні, Тобіас Енґель (засновник Sternraute) та Карстен Ноль (головний науковий співробітник у Security Research Labs) заявили, що можуть не лише визначити місцеперебування будь-якого абонента в будь-якому куточку світу, а й прослуховувати їхні дзвінки. А якщо в момент дзвінка прослухати його неможливо, вони могли записати зашифровану розмову й текст для подальшого дешифрування.

З погляду безпеки, ви взагалі незахищені. Енґель і Ноль зазначили, що, хоча розвинені країни Північної Америки та Європи інвестують мільярди доларів у створення безпечних і конфіденційних 3G та 4G мереж, вони все ще спираються на SS7 як основний протокол.

SS7 відповідає за встановлення зв'язку, виставлення рахунків та обмін інформацією. Тобто якщо ви зламаєте SS7, то можете маніпулювати дзвінком. Завдяки SS7 зловмисники можуть під'єднатися до розмов у Європі чи США через невеличкого оператора, скажімо, у Нігерії. «Це як забарикадувати головні двері, коли задні відкриті навстіж», — пояснив Енґель.

Дослідники протестували спосіб, яким зловмисник за допомогою функції переадресації та SS7 може переадресувати вихідні дзвінки жертви на свій телефон і під'єднатися до розмови в режимі конференції. Так хакер може прослуховувати дзвінки будь-кого в будь-якому куточку світу.

Ще один спосіб — установити радіоантени, які ловитимуть усі дзвінки та повідомлення на конкретній ділянці. А для зашифрованих 3G-дзвінків зловмисник може за допомогою SS7 дістати відповідний ключ дешифрування.

«І все це автоматизовано — варто лиш кнопку натиснути, — сказав Ноль. — Як на мене, змога записувати й дешифрувати будь-яку мережу має величезний шпигунський потенціал. А це спрацювало з кожним оператором, якого ми намагалися зламати»[51]. І він перерахував майже всіх великих операторів у Північній Америці та Європі — приблизно двадцять штук.

Ноль та Енґель також виявили, що можуть установити, де перебуває будь-який абонент через SS7-функцію миттєвого запиту абонентської інформації. Принаймні могли, поки функцію не скасували на початку 2015-го. Однак операторам усе ще потрібно якось стежити за територіальним розташуванням своїх абонентів, тож у SS7 залишилися функції, через які можна здійснювати дистанційне спостереження. Хоча варто зазначити, що більшість операторів таки полагодили деякі очевидні діри в безпеці, на які вказали Ноль та Енґель в оприлюдненому дослідженні.

Здавалося б, шифрування саме собою здатне захистити конфіденційність наших розмов, адже, починаючи з 2G, усі GSM-дзвінки шифруються. Однак перші спроби шифрувати дзвінки у 2G були визнані слабкими й неефективними. На жаль, ціна переходу на 3G-мережі для деяких операторів зв'язку виявилася непомірною, тож дехто використовував недосконалий 2G майже до 2010 року.

Улітку 2010-го команда дослідників на чолі з Нолем взяла всі можливі ключі шифрування 2G/GSM-мереж, провела розрахунки й оформила результати в так звану «райдужну таблицю» — список попередньо прорахованих паролів, чи ключів. Вони оприлюднили її, щоб показати операторам зв'язку у всьому світі, наскільки ненадійним є 2G-шифрування на основі GSM. Завдяки таблиці будь-який блок даних (голосових чи текстових) між джерелом і пунктом призначення, відправлений через 2G/GSM-мережу, можна дешифрувати за кілька хвилин[52]. Хід досить радикальний, але команда вважала його необхідним: побоювання, які Ноль висловив операторам на словах, залишилися непочутими. Показавши на практиці, як можна зламати шифрування 2G/GSM, вони так чи так змусили операторів щось змінити.

Важливо зазначити, що 2G все ще використовують, а оператори зв'язку розглядають можливість продажу доступу до старих 2G-мереж для пристроїв «інтернету речей» (некомп'ютерні пристрої, які мають доступ до інтернету, як-от телевізор і холодильник), які не потребують регулярного передавання даних. Якщо це трапиться, доведеться розробляти пристрої з наскрізним шифруванням, бо 2G-шифрування, як ви зрозуміли, саме собою слабке.

Ясна річ, прослуховування існувало ще задовго до створення мобільних телефонів.

Кошмар журналістки Аніти Буш розпочався вранці 20 червня 2002 року, коли вона прокинулася під нервовий стук сусіда у двері. Виявилося, хтось всадив кулю в лобове скло її автомобіля, припаркованого на під'їзній доріжці. Ба більше: на капоті незнайомець залишив троянду, дохлу рибу й записку з одним словом: «Стоп»[53]. Згодом вона дізналася, що її телефони прослуховували. І далеко не правоохоронні органи.

Те, що прострілене вікно вкупі з мертвою рибою нагадувало сцену з дешевого голлівудського фільму про гангстерів, мало пояснення. Досвідчена журналістка вже кілька тижнів проводила позаштатне дослідження для Los Angeles Times про зростання впливу організованої злочинності в Голлівуді. На той час вона працювала над статтею про Стівена Сіґала і його колишнього партнера по бізнесу Юліуса Нассо, якого звинувачували у змові з нью-йоркською мафією з метою вимагання грошей у Сіґала[54].

Після записки на машині Буш отримала низку телефонних повідомлень. Невідомий чоловік заявляв, що хоче поділитися інформацією про Сіґала. Пізніше журналістка дізналася, що «інформатора» найняв Ентоні Пеллікано — колишній приватний детектив із Лос-Анджелеса, якого на час інциденту з Буш ФБР уже підозрювало в незаконному прослуховуванні, підкупі, крадіжці особистих даних і перешкоджанні правосуддю. Пеллікано встановив жучок у домашній телефон Буш і в такий спосіб дізнався, що вона пише статтю в газету про його клієнтів. Дохла риба на машині була попередженням.

Здебільшого термін «прослуховування» пов'язаний лише з телефонними дзвінками, але закони про прослуховування в США охоплюють ще й стеження за імейлом і миттєвими повідомленнями. Тут я зосереджуся на традиційному прослуховуванні, що стосується стаціонарних телефонів.

Раніше пристрій для прослуховування вмонтовували у дріт стаціонарних телефонів. У ті часи кожна телефонна компанія мала низку комутаторів, які слугували своєрідними жучками. Тобто в кожної такої компанії були спеціальні пристрої, які техніки під'єднували до конкретного номера телефону в мейнфреймі в головному офісі. Також було додаткове обладнання для прослуховування, яке приєднували до пристрою і використовували для стеження. Однак сьогодні ці методи вважаються застарілими: усі телефонні компанії мають виконувати технічні вимоги, передбачені CALEA.

Хоча більшість зараз переключилася на мобільні телефони, купа людей і досі користуються дротяними телефонами, а деякі пристали на технологію VoIP — інтернет-телефонію, яка часто йде комплектом із кабельним телебаченням чи інтернетом.

Однак правоохоронні органи таки мають можливість прослуховувати ваші дзвінки. Байдуже, через фізичний комутатор у телефонній компанії чи цифровий.

Закон CALEA 1994 року вимагає від виробників телекомунікацій та операторів зв'язку модифікувати своє обладнання, щоб правоохоронні органи мали змогу прослуховувати лінію. Тож теоретично, дзвінки будь-якого стаціонарного телефона в США можна перехопити. Також, відповідно до CALEA, для доступу до прослуховування потрібен відповідний ордер, який видають лише правоохоронні органи. Звичайним громадянам заборонено вести прослуховування, а отже, Ентоні Пеллікано незаконно стежив за Анітою Буш та іншими. Список його жертв прослуховування охоплює таких голлівудських зірок, як Сільвестер Сталлоне, Девід Керрадайн і Кевін Нілон.

До цього списку потрапила і моя подруга Ерін Фінн, бо її колишній хлопець став одержимий і хотів стежити за кожним її кроком. Позаяк її телефонну лінію прослуховували, я теж мимоволі став жертвою, коли їй телефонував. І найкумедніша частина епопеї: оператор AT&T сплатив мені штраф у тисячу доларів у рамках урегулювання колективного позову, тому що Пеллікано прослуховував мої дзвінки Фінн. Досить іронічно, бо наступного разу вже я прослуховував їхніх абонентів. Хіба що мета Пеллікано була більш зловмисною за мою: він намагався залякати свідків, щоб ті давали потрібні йому свідчення чи не давали їх взагалі.

У 1990-х прослуховування могли встановити лише технічні працівники телефонних компаній. Тож Пеллікано (чи хтось із його людей) мав завербувати когось у PacBell, щоб той установив прослуховування на телефонній лінії Буш і Фінн. Техніки змогли «врізати» в потрібні лінії додаткові телефони і встановити їх в офісі Пеллікано в Беверлі-Гіллз. Так не потрібно нічого встановлювати в електромонтажну коробку чи вивідний щиток приватного будинку або житлового комплексу, хоча можливий і такий варіант[55].

Якщо ви читали попередню мою книжку «Привид у дротах» (Ghost in the Wires), то пам'ятаєте таку історію. Якось я поїхав з батьківської квартири в Калабасасі до Лонг-Біч, щоб установити прослуховування на телефонну лінію Кента — друга мого покійного брата. Його смерть від передозування викликала в усіх багато питань. Мені здавалося, що Кент був якось до цього причетний, хоча пізніше виявилося, що він не має до смерті брата жодного стосунку. Спершу треба було проникнути в технічне приміщення під багатоквартирним будинком, де жив Кент, потім — дізнатися, який кабель веде до телефона Кента. Для цього довелося увімкнути всі навики соціальної інженерії й подзвонити в телефонну компанію GTE, прикинувшись їхнім працівником. Виявилося, що його дроти проходять геть через інший будинок. Тож уже в другому технічному приміщенні я врешті-решт врізав свій мікрокасетний пристрій для запису з голосовою активацією в його телефонну лінію у вивідному щитку (звідки ведуть телефонні дроти до кожної квартири).

Тепер щоразу, як Кент комусь телефонував, я міг записувати двосторонню розмову без його відома. Хоча тут варто зазначити, що запис можна було зробити в режимі реального часу, а ось прослухати — ні. Тож кожного дня,

десять днів поспіль, доводилося годину їхати до будинку Кента і слухати там записи, шукаючи будь-яке згадування про брата. На жаль, нічого з цього не вийшло. Кілька років по тому я дізнався, що, найімовірніше, до смерті брата причетний мій дядько.

Враховуючи те, з якою легкістю ми з Пеллікано втрутилися в чужі телефонні розмови, виникає запитання: а як же ж стати непомітним зі стаціонарним телефоном, який потенційно вразливий до спостереження? Ніяк. Принаймні якщо у вас нема спеціального обладнання. Для справжніх параноїків існують дротяні телефони, які самі шифрують розмову[56]. Такі телефони розв'язують проблему перехоплення приватних дзвінків, але тільки якщо вони є в обох співрозмовників: інакше розмову легко прослухати[57]. Для решти ж є ще кілька способів убезпечити себе від прослуховування.

Перехід від дротяної до цифрової телефонії лиш спростив процес спостереження. Зараз установити прослуховування на цифрову телефонну лінію можна дистанційно — комутатор просто створює другий, паралельний потік даних. Жодного додаткового обладнання. А ще так набагато важче зрозуміти, що лінія прослуховується: зазвичай про прослуховування дізнаються випадково.

Незабаром після літніх Олімпійських ігор 2004 року в Афінах грецьке відділення Vodafone видалило фальшиве ПЗ, яке працювало в стільниковій мережі компанії понад рік. Правоохоронні органи можуть перехоплювати всі голосові й текстові дані в будь-якій стільниковій мережі через систему дистанційного керування RES — цифровий аналог традиційного прослуховування. Коли суб'єкт під наглядом робить дзвінок із мобільного, RES створює другий потік даних, який спрямовується безпосередньо до співробітника правоохоронних органів.

Фальшиве ПЗ, знайдене в грецькому Vodafone, під'єднувалося до їхньої системи RES, тобто хтось, окрім представників закону, міг слухати розмови абонентів. У цьому випадку прослуховувалися розмови урядовців. Під час Олімпійських ігор деякі країни (як-от США та Росія) для дзвінків державного рівня використовували власні приватні системи комунікації, а от політики й бізнесмени інших країн спілкувалися через зламану систему Vodafone.

Розслідування показало, що в цей час прослуховувалися розмови грецького прем'єр-міністра і його дружини, мера Афін, місцевого комісара Європейського Союзу, а також членів міністерств національної оборони, закордонних справ, торгового флоту і юстиції. Інші телефони на прослуховуванні належали членам правозахисних організацій, антиглобалізаційних груп, правлячої партії «Нова демократія», командному складу Військово-морських сил Греції, а також активістам руху за мир і греко-американському співробітникові посольства Сполучених Штатів в Афінах[58].

Шпіонаж міг би тривати і далі, якби Vodafone не запросила представників з Ericsson, які поставляли обладнання для системи RES, у зв'язку з іншою скаргою: збої доставлення SMS-повідомлень чомусь відбувалися частіше, ніж зазвичай.

Продіагностувавши проблему, Ericsson повідомила Vodafone про знайдене фальшиве ПЗ.

На жаль, за більш ніж десять років ми так і не дізналися, хто за цим стояв. Або чому. Або як часто таке трапляється. Крім того, Vodafone підлила масла у вогонь і сама завалила розслідування[59]. Основні файли логів, що стосувалися злочину, кудись зникли, а фальшиву програму відразу видалили із системи, чим попередили злочинців і дали їм змогу замести сліди. Зазвичай під час проведення кримінального розслідування виявлене шкідливе ПЗ не чіпають.

Інцидент із Vodafone — тривожне нагадування про те, наскільки вразливі наші мобільні телефони до прослуховування. Однак способи уникнути цього все ж таки є.

Окрім мобільних і стаціонарних телефонів, існує й третій варіант, про який я вже згадував мимохідь: IP-телефонія, або VoIP. VoIP чудово підходить для будь-якого бездротового пристрою, у якому не закладено функції дзвінків, як-от iPod Touch. Це навіть більше схоже на серфінг в інтернеті, аніж на класичний дзвінок. Стаціонарні телефони працюють завдяки дротам, мобільні — через стільникові вежі. А от VoIP просто передає ваш голос по дротовому інтернету чи вай-фаю. Також VoIP працює на мобільних девайсах (приміром, ноутбуках і планшетах) незалежно від того, передбачений у них стільниковий зв'язок чи ні.

Звичайні користувачі та цілі компанії з метою економії переходять на систему VoIP, яку тепер пропонують нові провайдери та старі кабельні компанії. VoIP працює через той самий коаксіальний кабель, призначений для потокового відео та високошвидкісного інтернету.

Добре те, що телефонні системи VoIP використовують шифрування, зокрема дескриптори безпеки SDP або SDES. Погано те, що SDES — не дуже надійна річ.

Проблема частково полягає в тому, що ключі шифрування SDES не можна передати через безпечний криптографічний протокол SSL/TLS, і ключ доводиться відправляти у відкритому вигляді. Позаяк замість асиметричного шифрування тут використовується симетричне, відправник має якось передати згенерований ключ одержувачу, щоб той розшифрував дзвінок.

Припустимо, Боб хоче зателефонувати Еліс, яка живе в Китаї. VoIP Боба на основі шифрування SDES генерує новий ключ для дзвінка, який він якось має відправити Еліс, щоб її VoIP-девайс розшифрував його дзвінок, і вони могли поговорити. SDES пропонує такий варіант: Боб надсилає ключ своєму провайдерові, той передає його провайдерові Еліс, а він уже — самій Еліс.

Бачите недолік? Пам'ятаєте, що я говорив про наскрізне шифрування в минулому розділі? Розмова конфіденційна лише за умови, що її може розшифрувати тільки одержувач. Однак SDES відправляє ключ Боба його провайдерові, а той ще одному, якщо провайдер у Еліс інший. Схожу ситуацію маємо зі Skype та Google Voice: із кожним новим дзвінком генерується новий ключ, однак відправляються ці ключі Microsoft та Google. Надто людно для приватної розмови.

На щастя, є способи зашифрувати VoIP наскрізно. Застосунок Signal від Open Whisper Systems є безкоштовною VoIP-системою з відкритим вихідним кодом для мобільних телефонів, яка забезпечує справжнє наскрізне шифрування як на iOS, так і на Android[60].

Головна перевага Signal у тому, що розпоряджаються ключами лише співрозмовники. Жодних третіх осіб. Як і для SDES, із кожним дзвінком генеруються нові ключі, однак зберігаються вони лише на пристроях користувачів. Позаяк CALEA забезпечує доступ до будь-яких записів дзвінків, правоохоронні органи можуть прослуховувати лінію, але почують вони лиш нерозбірливий зашифрований трафік. А ключів в Open Whisper Systems — некомерційної організації, яка розробляє Signal, — просто нема, тому ордер не допоможе. Ключі існують лише на девайсах, що здійснюють між собою дзвінок, а щойно він завершується, ключі сеансу видаляються.

Зараз CALEA не поширюється на кінцевого користувача та його девайси.

Думаєте, що програма шифрування розрядить вам батарею на телефоні? Так, але зовсім трохи. Signal використовує push-повідомлення, як і застосунки на зразок WhatsApp і Telegram. Тобто ви лише бачите виклик під час надходження, що скорочує витрати батареї. Як на Android, так і на iOS застосунок спирається на аудіо-кодеки та алгоритми буфера мобільної мережі, і шифрування, знову ж таки, не надто виснажує батарею під час розмови.

Додатково до наскрізного шифрування Signal теж використовує пряму секретність (PFS). Що таке PFS? Це система, яка трохи видозмінює ключі для кожного дзвінка, тож якщо в когось-таки вийшло зламати ваш зашифрований дзвінок і ключ до нього, наступні дзвінки залишаться в безпеці. Усі PFS-ключі спираються на єдиний первинний ключ, однак навіть якщо зловмисник якось дістане один із ключів, доступу до ваших наступних розмов у нього не буде.

---

48 Ви можете відмовитися від надання особистих даних для подібних сервісів на Android. Відкрийте Налаштування>Google>Пошук, Асистент і Voice>Облікові записи та конфіденційність і там відключіть обмін даних для маршрутів. У користувачів Apple подібної можливості нема, але в майбутніх версіях iOS можуть реалізувати функцію планування маршруту залежно від того, де в цей час перебуває ваш телефон.

49 http://www.abc.net.au/news/2015-07-06/nick-mckenzie-speaks-out-about-his-brush-with-the-mafia/6596098.

50 Краще купувати картки поповнення за допомогою біткоїнів.

51 https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/.

52 http://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/.

53 http://www.latimes.com/local/la-me-pellicano5mar05-story.html.

54 http://www.nytimes.com/2008/03/24/business/media/24pellicano.html.

55 https://www.hollywoodreporter.com/thr-esq/anthony-pellicanos-prison-sentence-vacated-817558.

56 http://www.cryptophone.de/en/products/landline/.

57 https://www.kickstarter.com/projects/620001568/jackpair-safeguard-your-phone-conversation/posts/1654032.

58 http://spectrum.ieee.org/telecom/security/the-athens-affair.

59 http://bits.blogs.nytimes.com/2007/07/10/engineers-as-counterspys-how-the-greek-cellphone-system-was-bugged/.

60 https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms.

Розділ 4
Без шифру як без зброї

Якщо хтось просто зараз візьме ваш розблокований телефон, то дістане доступ до вашого імейлу, акаунтів у соцмережах і навіть профілю в Amazon. На відміну від ноутбуків і ПК, на телефонах не потрібно щоразу заходити в сервіси: після авторизації мобільні застосунки постійно залишаються відкритими. Також у телефоні зберігаються ваші фотографії, музика і SMS-повідомлення, які зловмисник так само отримає на блюдечку, якщо заволодіє вашим незаблокованим телефоном.

У 2009 році Деніела Лі з Лонґв'ю, штат Вашингтон, заарештували за підозрою в продажі наркотиків[61]. Поки він перебував під вартою, поліція перевірила його незахищений паролем телефон і відразу ж знайшла кілька текстових повідомлень, пов'язаних із наркотиками. Одна така зачіпка вела до особи на ім'я Зі-Джон.

У SMS ішлося: «У мене 130 зі 160, що винен із минулого вечора». Згідно зі свідченнями в суді, поліція Лонгв'ю не просто прочитала повідомлення Зі-Джона, а й відповіла на нього, організувавши наркоугоду. Прикинувшись Лі, поліція надіслала з його телефона SMS Зі-Джону й запитала, чи «потрібно більше». Той написав: «Ага, можна». Коли Зі-Джон (справжнє ім'я — Джонатан Роден) з'явився на зустрічі, його заарештували за спробу придбати героїн.

Поліція також знайшла в телефоні ще одну переписку й арештувала Шона Деніела Гінтона за аналогічною схемою[62].

Обидва чоловіки подали на апеляцію, і 2014-го за сприяння Американського союзу захисту громадянських свобод Верховний суд штату Вашингтон скасував вироки Родена і Гінтона, позаяк поліція порушила право підсудних на недоторканність приватного життя.

Судді штату Вашингтон заявили, що якби Лі першим побачив повідомлення від Родена й Гінтона або поліцейські відповіли їм «Деніела зараз нема», це кардинально змінило б хід обох справ. «Текстові повідомлення можуть містити таку саму особисту інформацію, що й телефонні дзвінки, запечатані листи й інші традиційні форми спілкування, які історично були надійно захищені відповідно до законодавства Вашингтона», — написав суддя Стівен Ґонсалес у справі Гінтона[63].

Судді постановили, що право на недоторканність приватного життя охоплює не лише еру паперових листів, а й цифрову епоху. У США правоохоронним органам забороняється відкривати запечатаний паперовий лист без дозволу одержувача. Право на недоторканність приватного життя є юридичним критерієм і показником того, чи виконуються вимоги щодо захисту конфіденційності в рамках четвертої поправки до Конституції США. Наразі невідомо, чим керуватимуться суди в ухваленні майбутніх рішень і чи враховуватимуть цей правовий критерій.

Технологія текстових повідомлень, відома як «служба коротких повідомлень» (скорочено — SMS), з'явилася ще 1992 року. Усі стільникові телефони — навіть фічерфони (тобто звичайні телефони, а не смартфони) — дають змогу обмінюватися короткими повідомленнями. Однак ці повідомлення незавжди потрапляють одразу до адресата. SMS-повідомлення, як і електронні листи, спочатку надходять до Центру служби коротких повідомлень (SMSC) — елемента мобільної мережі, призначеного для зберігання, пересилання й доставлення SMS. Через що іноді вони надходять із затримкою в кілька годин.

«Рідні» мобільні повідомлення (тобто ті, які надсилаються безпосередньо з телефона, а не через окремий застосунок) проходять через SMSC мобільного оператора, який може їх тимчасово зберігати. Оператори начебто зберігають SMS-повідомлення протягом кількох днів, а потім вони залишаються лиш у пам'яті телефонів, які їх надсилають і приймають. Обсяг пам'яті для зберігання повідомлень залежить від моделі телефона. Однак усе це на словах. Думаю, що мобільні оператори в США зберігають повідомлення незалежно від того, що розповідають людям[64].

Сумніви щодо заяв мобільних операторів не безпідставні. У документах, які оприлюднив Сноуден, ідеться про тісний зв'язок між АНБ і принаймні одним оператором — AT&T. Журнал Wired запевняє, що 2002 року (незабаром після трагедії 11 вересня) АНБ звернулося до AT&T з пропозицією створити потаємні кімнати в кількох офісах оператора: одну в Бриджтоні, штат Міссурі, і ще одну на вулиці Фолсом у центрі Сан-Франциско. Згодом додалися й інші міста, зокрема Сіетл, Сан-Хосе, Лос-Анджелес і Сан-Дієго. Мета таких потаємних кімнат — пропускати весь трафік мобільного інтернету, імейлу і телефонів через спеціальний фільтр ключових слів. Невідомо, чи входили сюди SMS-повідомлення, але логічно припустити, що так. Невідомо і те, як вплинули на це дії Сноудена, і чи існує десь подібна практика й досі[65].

Один випадок підказує, що ні.

У чемпіонаті Американської футбольної конференції 2015 року, яка передувала Суперболу XLIX, розгорівся конфлікт навколо перемоги команди «Нью-Інґленд Петріотс» над «Індіанаполіс Колтс» з рахунком 45:7. Приводом для дискусій стало питання, чи навмисно команда переможців не до кінця накачала свої м'ячі. Національна футбольна ліга має суворі вимоги щодо накачування м'ячів, а після плей-оффу виявилося, що м'ячі від команди «Нью-Інґленд Петріотс» не відповідали критеріям. Головне місце в розслідуванні посіли SMS-повідомлення від їхнього зіркового квотербека, Тома Бреді.

Публічно Бреді заперечив свою причетність. І це могли б підтвердити повідомлення, які від надсилав та отримував до та після гри. Однак у день зустрічі зі слідчими Бреді раптом з'явився з новеньким телефоном. Того, яким він користувався з листопада 2014-го до 6 березня 2015-го, у нього вже не було. Як він пізніше заявив, старий телефон зламався, а всі дані на ньому, зокрема й повідомлення, зникли. У результаті Національна футбольна ліга ухвалила рішення відсторонити Бреді на чотири гри, яке згодом було скасовано в суді[66].

«Протягом цих чотирьох місяців Бреді надіслав і отримав приблизно десять тисяч повідомлень, які зараз із пристрою вилучити вже неможливо, — заявили представники Ліги. — Після слухання апеляції представники пана Бреді надали лист від мобільного оператора, який підтвердив, що надіслані чи отримані SMS-повідомлення зі зламаного телефона відновити неможливо»[67].

Тож якщо оператор Тома Бреді підтвердив, що всі повідомлення зникли, а оператори начебто не зберігають у себе SMS-повідомлень, єдиний спосіб зберегти їх — створити резервну копію телефона в хмарі. Якщо скористаєтеся сервісом від вашого оператора (чи навіть Google або Apple), компанія матиме доступ до ваших повідомлень. Найімовірніше, у Тома Бреді не було часу зробити резервну копію старого телефона перед тим, як придбати новий.

Конгрес не торкався проблеми зберігання даних загалом і мобільних зокрема. Але в останні роки він розглядає варіант змусити мобільних операторів архівувати повідомлення і зберігати їх протягом двох років. В Австралії таке ввели 2015 року, тож нам залишається лиш спостерігати, як це працюватиме там.

То як зберегти конфіденційність текстових повідомлень? Не користуйтеся вбудованим сервісом, який пропускає повідомлення через вашого оператора. Краще встановіть сторонній застосунок. Який?

Щоб приховати свою особу в інтернеті й насолоджуватися ним анонімно, доведеться довіритися певним програмам і сервісам. А довіритися їм на всі сто важко. Загалом розробники програм із відкритим вихідним кодом і некомерційні організації є найнадійнішими, бо без перебільшення тисячі очей розкладають код по поличках і відмічають усе, що здається підозрілим чи слабким. Якщо ж вам потрібне приватне ПЗ, доведеться так чи інакше повірити розробникові на слово.

Зазвичай в оглядах програмного забезпечення ви не знайдете нічого, окрім інформації про те, як працюють окремі функції. Оглядачі кілька днів тестують програму і пишуть про свої враження. По суті, вони не користуються ПЗ і не можуть сказати, як воно працює в довгостроковій перспективі. Вони лиш пишуть про перші спостереження.

Крім того, оглядачі ніколи не скажуть вам, чи можна довіряти ПЗ. Вони не перевіряють аспекти конфіденційності та безпеки. А той факт, що програму розробляє відома компанія, ще не гарантує надійності. Навпаки, краще обережно ставитися до гучних брендів, які здатні прищепити нам оманливе відчуття безпеки. Не варто вірити розробникові на слово.

Ще в 1990-х, коли мені треба було зашифрувати ноутбук на Windows 95, я вибрав тепер уже неіснуючу утиліту від Norton під назвою Norton Diskreet. Пітер Нортон — справжній геній. Його перша комп'ютерна утиліта автоматизувала процес відновлення файлів. У 1980-х, коли ще мало хто розбирався в командних рядках, він уже створював купу чудових системних утиліт. Але згодом він продав компанію Symantec, і писати програми від його імені став хтось інший.

Коли я купував Diskreet (який вже більше не підтримується), 56-бітне DES-шифрування (DES означає «стандарт шифрування даних») було інновацією і найнадійнішим алгоритмом. Для порівняння, зараз ми користуємося 256-бітним AES-шифруванням (AES означає «прогресивний стандарт шифрування даних»). Із кожним додатковим бітом шифрування кількість ключів злітає по експоненті, а що більше ключів, то надійніше. 56-бітне DES-шифрування вважалося першим словом у безпеці, поки його не зламали 1998 року[68].

Однак мені кортіло дізнатися, чи зможе Diskreet приховати мої дані. Та ще й створити проблеми ФБР, якщо вони заволодіють моїм ноутбуком. Придбавши програму, я одразу зламав Symantec і знайшов вихідний код програми[69]. Проаналізувавши принципи його роботи, я виявив, що Diskreet використовує з 56-бітного ключа лише тридцять бітів. Решта мала вигляд просто купи нулів[70]. Це було навіть гірше за сорок біт, які було дозволено експортувати за межі США.

Що це означало на практиці? АНБ, правоохоронні органи, зловмисник із швидким комп'ютером — майже будь-хто міг зламати Diskreet набагато швидше, ніж заявляли розробники, позаяк 56-бітного шифрування там не було і в помині. Але компанія рекламувала продукт як програму з 56-бітним шифруванням. Тож я вирішив скористатися чимось іншим.

Чи могли про це дізнатися звичайні клієнти? Ні.

Хоча й такі соцмережі, як фейсбук, снепчат та інстаґрам, популярні серед підлітків, за даними niche.com, SMS-повідомлення все одно мають більший попит[71]. Нещодавнє дослідження показало, що кожного дня повідомленнями користуються 87 % підлітків, тоді як другим за популярністю фейсбуком — лише 61 %. Дівчата в середньому надсилають 3952 SMS-повідомлення на місяць, а хлопці — приблизно 2815[72].

Добре те, що всі сучасні популярні месенджери шифрують повідомлення під час надсилання й отримання, тобто захищають так звані «дані в русі». Погано те, що незавжди це шифрування надійне. У 2014 році дослідник Пол Хурегі з фірми інформаційної безпеки Praetorian виявив, що шифрування WhatsApp можна обійти і провести «атаку посередника» (MitM), коли зловмисник перехоплює і читає повідомлення між жертвою та її співрозмовником. «АНБ би сподобалося», — зазначив Хурегі[73].

На час написання книжки WhatsApp удосконалив своє шифрування і зробив його наскрізним як на iOS, так і на Android. А його материнська компанія Facebook ввела подібне шифрування на свій месенджер із 900 мільйонами користувачів. Хоча й ця функція не є автоматичною і «Секретні розмови» треба вмикати вручну[74].

Однак найгірше трапляється з архівованими даними, або «даними в стані спокою». Більшість мобільних месенджерів не шифрує заархівовані дані — ні на вашому телефоні, ні в сторонній системі. Застосунки на зразок AIM, BlackBerry Messenger і Skype зберігають ваші повідомлення в незашифрованому вигляді. Тобто провайдер може їх проглядати (якщо вони зберігаються в хмарі) і використовувати для налаштування реклами. Ба більше: якщо вашим телефоном заволодіють правоохоронні органи (або хакери-злочинці), вони також зможуть прочитати всі ваші повідомлення.

Ще одна проблема — термін зберігання даних, який ми згадували вище. Як довго дані в стані спокою залишаються «в спокої»? Як довго застосупки на зразок AIM і Skype зберігають архіви з вашими повідомленнями в незашифрованому вигляді? Microsoft, яка придбала Skype, каже: «Skype використовує миттєве сканування миттєвих повідомлень і SMS, щоб: а) визначити потенційний спам та/або б) визначити посилання, які раніше були відмічені як спам, спроба шахрайства чи фішингу». На перший погляд, звичайний процес сканування щодо шкідливого ПЗ. Те саме, що відбувається з нашими імейлами. Проте далі політика конфіденційності каже нам: «Skype зберігатиме вашу інформацію стільки, скільки потрібно для: 1) виконання будь-якої з Цілей (які визначені в статті 2 цієї Політики конфіденційності) або 2) дотримання чинного законодавства, нормативних вимог і відповідних постанов компетентних судів»[75].

Звучить уже не так безневинно? «Стільки, скільки треба» — це ж скільки?

Програма AOL Instant Messenger (скорочено AIM), імовірно, є першим сервісом миттєвих повідомлень, яким ми з вами скористалися. Він на ринку вже давно. Спершу AIM розробляли для стаціонарних ПК, він мав вигляд маленького спливаючого вікна в правому нижньому кутку робочого столу. Сьогодні він доступний ще й у формі мобільного застосунку. Але з погляду конфіденційності AIM викликає деякі питання. По-перше, месенджер архівує всі ваші повідомлення. По-друге, він, як і Skype, сканує зміст цих повідомлень. І по-третє, AOL зберігає ваші повідомлення у «хмарі», якщо раптом ви захочете переглянути історію діалогу з іншого пристрою[76].

Позаяк ваша переписка в AOL не зашифрована і доступна з будь-якого пристрою, бо зберігається в «хмарі», правоохоронні органи чи хакери можуть легко дістати копію. Наприклад, мій акаунт в AOL зламав якийсь аматор під ніком «Вірус», якого насправді звуть Майкл Нівз[77]. Трохи соціальної інженерії (що означає додзвонитися AOL і мило побалакати) — і він дістав доступ до їхньої внутрішньої клієнтської бази даних під назвою «Мерлін». Там він змінив мою імейл-адресу на ту, що була прив'язана до його акаунта. Після цих маніпуляцій він зміг скинути мій пароль і прочитати всі колишні повідомлення. У 2007-му Нівзу висунули звинувачення в чотирьох кримінальних злочинах і одному проступку за злам «внутрішніх комп'ютерних мереж і баз даних AOL, зокрема облікових записів клієнтів, адрес та інформації про кредитні картки».

Якось представники правозахисної організації EFF сказали: «Найкращі логи — відсутність логів». В AOL логи є.

Вважається, що нерідні месенджери шифрують повідомлення, але це шифрування необов'язково надійне чи навіть пристойне. На що звертати увагу? Шифрування має бути наскрізним, тобто ключі повинні бути лише у вас і співрозмовника. Без третіх осіб. Однак перевірте, чи не заражені ці два телефони вірусом, бо інакше жодне шифрування не допоможе.

Існує три основних типи месенджерів:

- месенджери взагалі без шифрування, тобто будь-хто може прочитати ваші повідомлення;
- месенджери із шифруванням, але не наскрізним, тобто повідомлення можуть перехопити треті особи, які володіють ключами шифрування (приміром, компанія-власник застосунку);
- месенджери з наскрізним шифруванням, тобто треті особи не можуть прочитати ваші повідомлення, бо ключі зберігаються лише у вас і співрозмовника.

На жаль, найпопулярніші месенджери на зразок AIM не дуже приватні. Навіть такі застосунки, як Whisper і Secret, не гарантують повної конфіденційності. Whisper позиціонує себе як анонімну соцмережу, якою користуються мільйони, але дослідники знайшли прогалини в її анонімності. Whisper стежить за своїми користувачами, а особи користувачів Secret іноді спливають на поверхню.

Telegram — ще один месенджер із шифруванням і популярна альтернатива WhatsApp, яка підтримується на Android, iOS і Windows. Хоча й тут існує спосіб, як зламати сервери Telegram і дістати доступ до важливих даних[78]. А ще в Telegram виявилося досить легко відновити зашифровані повідомлення, навіть якщо їх видалили з телефона[79].

Що ж, ми виключили всі очевидні варіанти. Що залишається? Та куна всього. Коли вибираєте застосунок в App Store чи Google Play, шукайте щось на основі OTR — протоколу наскрізного шифрування вищого рівня, що використовується для обміну повідомленнями. І він таки є в низці застосунків[80].

У вашому ідеальному месенджері теж має бути пряма секретність (PFS). Якщо пам'ятаєте, ця система довільно генерує нові ключі для кожної сесії, щоб не скомпрометувати пристрій наступного разу. Тобто якщо один ключ зламають, прочитати через нього наступні повідомлення буде неможливо.

Отже, існує кілька застосунків одночасно і з OTR, і з PFS.

ChatSecure — безпечний застосунок для обміну повідомленнями для Android та iOS[81]. Окрім того, у ньому є функція так званого «пінінгу сертифіката». Тобто на вашому телефоні зберігається сертифікат, що посвідчує «особу» девайса. Під час кожного контакту із серверами ChatSecure сертифікат на вашому телефоні порівнюється із сертифікатом на цих серверах. Якщо ці сертифікати не збігаються, сесія припиняється. І ще один бонус: ChatSecure шифрує і логи переписки, що зберігаються на телефоні, тобто дані в стані спокою[82].

Напевно, найкращим варіантом з відкритим вихідним кодом можна назвати Signal від Open Whisper Systems, який працює на iOS та Android (див. розділ 3).

А ще як варіант розгляньте месенджер Cryptocat. Його можна встановити на iPhone і більшість головних браузерів ПК, однак для телефонів на Android він недоступний[83].

На час написання книжки проект Tor, який розробляє Tor-браузер (див. розділ 2), щойно випустив Tor-месенджер. Як і браузер, месенджер анонімізує вашу IP-адресу, тобто ваші повідомлення стає важко відстежити (але зверніть увагу, що тут, як і в Tor-браузері, вихідні вузли вам непідконтрольні). Миттєві повідомлення захищені наскрізним шифруванням. Як і всі розробки Tor, застосунок спершу здається важким в управлінні, але ви отримуєте дійсно конфіденційну переписку[84]. Наскрізне шифрування пропонують і деякі платні застосунки. Єдине зауваження: їхнє ПЗ є приватним, а отже, безпечність і цілісність застосунків неможливо підтвердити без незалежного огляду. Приміром, Silent Phone пропонує наскрізне шифрування для повідомлень. Хоча й застосунок створює певні логи, робиться це з метою поліпшення сервісу. Ключі шифрування зберігаються лише на телефонах, а отже, уряд і правоохоронні органи не можуть змусити розробника видати їм ключі жодного з користувачів.

Що ж, ми трохи поговорили про те, як шифрувати дані в русі і дані в стані спокою за допомогою наскрізного шифрування, PFS і OTR. А як щодо браузерів? Імейлів? Паролів?

---

61 http://caselaw.findlaw.com/wa-supreme-court/1658742.html.

62 http://courts.mrsc.org/mc/courts/zsupreme/179wn2d/179wn2d0862.htm.

63 http://www.komonews.com/news/local/Justices-People-have-right-to-privacy-in-text-messages-247583351.html.

64 http://www.democracynow.org/2016/10/26/headlines/project_hemisphere_at_ts_secret_program_to_spy_on_americans_for_profit.

65 http://www.wired.com/2015/08/know-nsa-atts-spying-pact/.

66 http://espn.go.com/nfl/story/_/id/13570716/tom-brady-new-england-patriots-wins-appeal-nfl-deflategate.

67 https://www.bostonglobe.com/sports/2015/07/28/tom-brady-destroyed-his-cellphone-and-texts-along-with/ZuIYu0he05XxEeOmHzwTSK/story.html.

68 DES почасти зламали тому, що він шифрував дані лиш раз. Натомість AES використовує тришарове шифрування і є надійнішим, навіть якщо не враховувати кількість бітів.

69 Розробник уже не підтримує Diskreet.

70 https://twitter.com/kevinmitnick/status/346065664592711680. А за цим посиланням можна знайти більш технічне пояснення 32-бітного DES-шифрування: https://www.cs.auckland.ac.nz/~pgut001/pubs/norton.txt.

71 http://www.theatlantic.com/technology/archive/2014/06/facebook-texting-teens-instagram-snapchat-most-popular-social-network/373043/.

72 http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015.

73 http://www.forbes.com/sites/andygreenberg/2014/02/21/whatsapp-comes-under-new-scrutiny-for-privacy-policy-encryption-gaffs/.

74 https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/.

75 https://community.skype.com/t5/Security-Privacy-Trust-and/Skype-to-Skype-call-recording/td-p/2064587.

76 https://www.eff.org/ru/deeplinks/2011/12/effs-raises-concerns-about-new-aol-instant-messenger-0.

77 http://www.wired.com/2007/05/always_two_ther/.

78 http://venturebeat.com/2016/08/02/hackers-break-into-telegram-revealing-15-million-users-phone-numbers/.

79 http://www.csmonitor.com/World/Passcode/2015/0224/Private-chat-app-Telegram-may-not-be-as-secretive-as-advertised.

80 https://otr.cypherpunks.ca/.

81 https://chatsecure.org/.

82 https://guardianproject.info/apps/chatsecure/.

83 https://crypto.cat/.

84 https://getconfide.com/.

Розділ 5
Абракадабра!

У квітні 2013-го колишній двадцятидвохрічний таксист із Квінсі Гайрулложон Матанов зустрівся за вечерею із друзями — двома братами. Чоловіки обговорювали нагальні теми, зокрема й нещодавній інцидент на фінішній лінії Бостонського марафону, де хтось залишив кілька рисоварок, набитих цвяхами, порохом і таймерами. Від вибуху загинуло три людини, ще понад двісті — поранені. Пізніше цих двох братів — Тамерлана та Джохара Царнаєвих — визнали головними підозрюваними у справі. Хоча Матанов заявив, що нічого не знав про теракт, одразу після зустрічі із правоохоронними органами він видалив історію браузера зі свого ПК. Ця начебто безвинна дія обернулася для нього звинуваченнями в суді[85].

Через видалення історії браузера звинуватили і студента Девіда Кернелла, який зламав імейл-акаунт Сари Пейлін. Лякає те, що, поки Девід не почистив браузера, не запустив дефрагментації диска й не видалив завантажених фото Пейлін, його ніхто не підозрював. Я веду до того, що в США, виявляється, видаляти щось із комп'ютера — незаконно. Прокурори хочуть бачити всю історію вашого браузера.

Законові, за яким засудили Матанова й Кернелла, уже понад п'ятнадцять років. У Сенаті його називають законом «Про реформу відкритих акціонерних товариств і захист інвесторів», у Палаті представників — законом «Про корпоративну й аудитну звітність і відповідальність», а народ називає законом Сарбейнса—Окслі 2002 року. Законопроект було прийнято з огляду на порушення в унравлінні енергетичної компанії Enron, яка водила за ніс інвесторів та уряд США. Слідчі у справі Enron виявили, що на початку розслідування компанія видалила купу даних, чим завадила прокурорам дізнатися, що саме відбувалося всередині організації. У результаті сенатор Пол Сарбейнс (демократ від Меріленду) та представник Майкл Окслі (республіканець від Огайо) ініціювали ухвалення закону, який накладає низку вимог, спрямованих на збереження даних. Одна з них — заборона на видалення історії браузера.

За обвинувальним актом суду присяжних, Матанов почистив історію в браузері Google Chrome вибірково, видаливши лише дані за конкретний період, а саме за тиждень, до якого входило й 15 квітня 2013 року[86]. Офіційно його звинуватили за двома статтями: «1) Знищення, зміна і фальсифікація записів, документів і матеріальних об'єктів у федеральному розслідуванні та 2) матеріально хибні, фіктивні й обманні заяви у федеральному розслідуванні, що стосується міжнародного та внутрішнього тероризму»[87]. Його засудили до тридцяти місяців в'язниці.

Раніше до положення закону Сарбейнса—Окслі до історії браузера зверталися рідко — як стосовно компаній, так і приватних осіб. Справа Матанова — гучний виняток, справа національної безпеки. Однак саме після цього винятку прокурори усвідомили потенціал положення й почали користуватися ним частіше.

Отже, не можна заборонити проглядати свої імейли, миттєві повідомлення й прослуховувати дзвінки. Не можна видалити історію браузера на законних підставах. То як же себе захистити? Почнемо з того, що взагалі не варто цю історію збирати.

Такі браузери, як Mozilla Firefox, Google Chrome, Safari та Internet Explorer чи Edge від початку містять альтернативний спосіб анонімного пошуку як на традиційному ПК, так і на мобільному девайсі. Для кожної сесії браузер відкриватиме нове вікно, яке не фіксуватиме ваші пошукові запити чи відкриті сайти. Закрийте приватне вікно браузера — і всі сліди сесії зникнуть з вашого комп'ютера чи телефона. Плата за конфіденційність — неможливість повернутися до закритого сайту, якщо ви перед цим не додали його в закладки. У приватному вікні нема історії. Принаймні не на вашому девайсі.

Якщо вже почуваєтеся невловимим із приватним вікном у Firefox чи в режимі інкогніто у Chrome, не кваптеся з висновками. Ваші запити все ще проходять через сервери інтернет-провайдера, який може перехопити будь-яку незашифровану інформацію. Зокрема й ваші імейли. Якщо ж заходите на сайт із шифруванням, провайдер отримує метадані: куди ви заходили і коли.

Коли інтернет-браузер (як на стандартному ПК, так і на телефоні) намагається відкрити сайт, насамперед він встановлює, чи використовує сайт шифрування і яке саме. Цей протокол передавання даних відомий вам як «http». Він прописаний перед адресою сайту, тобто звичайний URL має вигляд як http://www.mitnicksecurity.com. Іноді навіть і «www» не потрібно.

Якщо ви заходите на сайт із шифруванням, протокол трохи видозмінюється: замість «http» у вас буде «https». Тепер посилання матиме вигляд як https://www.mitnicksecurity.com. Цей протокол більш надійний і пропонує наскрізне шифрування, але тільки якщо ви з'єднуєтеся із сайтом безпосередньо. Існує купа мереж доправлення й поширення контенту (CDN), які кешують сторінки, щоб клієнт міг швидше їх відкрити незалежно від свого місця розташування, а отже, між вами і сайтом з'являється посередник.

І зверніть увагу: якщо ви не вийшли зі своїх акаунтів у Google, Yahoo чи Microsoft, вони можуть записувати ваш трафік на комп'ютері чи телефоні. У такий спосіб вони створюють ваш профіль поведінки в інтернеті, щоб краще налаштовувати таргетовану рекламу. Найпростіший спосіб цього уникнути — щоразу виходити з перерахованих акаунтів. Заходьте лиш тоді, коли вони вам потрібні.

А ще в телефонах є браузери за замовчуванням. Обходьте їх десятою дорогою. Ці міні-версії повноцінних ПК-браузерів — лайно. Їм не вистачає елементів

безпеки й захисту конфіденційності. Наприклад, в айфони вбудовано Safari, однак нескладно зайти в App Store і завантажити мобільну версію Chrome чи Firefox, заточену під мобільне середовище. Хоча в нових телефонах на Android браузер Chrome вже йде за замовчуванням. Принаймні всі мобільні браузери мають режим анонімного пошуку.

А от якщо у вас Kindle Fire, просто так установити Firefox чи Chrome через Amazon не вийде. Доведеться піти на хитрощі і вручну встановити ці застосунки через амазонівський рідний браузер Silk. Щоб завантажити Firefox на Kindle Fire, відкрийте Silk і перейдіть на сайт Mozilla FTP. Натисніть «Go» і виберіть файл із розширенням «apk».

У приватному режимі не створюються тимчасові файли, а отже, історія браузера не зберігається на вашому ноутбуці чи телефоні. Чи можуть треті особи все ще побачити ваші дії на сайті? Так, якщо ці дії не зашифрувати. Для цього компанія Electronic Frontier Foundation і створила плагін для браузерів HTTPS Everywhere[88]. Плагін підходить для Firefox і Chrome на ПК і для Firefox на Android. На час написання книжки версії для iOS поки що не існує. Але HTTPS Everywhere дає відчутну перевагу. У перші секунди з'єднання сайт і браузер «обговорюють», який тип безпеки вибрати. Вам потрібна пряма секретність (PFS), про яку ми говорили в минулому розділі. Однак не всі сайти користуються PFS. І не всі «обговорення» приходять до PFS, навіть якщо такий варіант можливий. А от HTTPS Everywhere здатен забезпечити вам «https», де це можливо, навіть якщо сайт не користується PFS.

І ще один критерій для безпечного з'єднання: у кожного сайту має бути сертифікат — гарантія від третьої сторони, що, приміром, сайт Bank of America є дійсно сайтом Bank of America, а не підробкою. Сучасні браузери співпрацюють з такими третіми сторонами — центрами сертифікації — для постійного оновлення списків. Якщо ви намагаєтеся зайти на сайт без належної сертифікації, ваш браузер повинен попередити вас і запитати, чи достатньо ви довіряєте цьому сайтові. Вам вирішувати, заходити на нього чи ні. Якщо ви не знаєте сайту, то варто утриматися.

Окрім того, типів сертифікатів в інтернеті безліч. Є навіть рівні сертифікатів. Найпоширеніший сертифікат, з яким ви стикаєтеся повсякчас, визначає лиш те, чи належить доменне ім'я тому, хто запросив сертифікат через імейл-верифікацію. Цей «хтось» може бути ким завгодно, але байдуже: він має сертифікат, який приймає ваш браузер. Та сама історія і з другим популярним типом сертифікатів — організаційним. Це означає, що сайт поширює сертифікат на всі сайти під тим самим доменом. Тобто всі піддомени сайту mitnicksecurity.com матимуть той самий сертифікат.

А от найнадійніший рівень верифікації — сертифікат із розширеною верифікацією. У сайтів із подібним сертифікатом частина URL є зеленою (тоді як зазвичай вона сіра). Клікнувши на адресу (https://www.mitnicksecurity.com), ви побачите додаткові відомості про сертифікат і його власника — зазвичай це

місто і штат сервера, на якому розміщено сайт. Це є підтвердженням того, що компанія, якій належить URL, — цілком законна і була засвідчена довіреним центром сертифікації.

Переймаєтеся, що браузер на телефоні відстежує ваше місцеперебування? Здивуєтеся, але браузер на традиційному ПК робить те саме. Як?

Пам'ятаєте, як я казав, що метадані електронної пошти містять IP-адреси всіх серверів, через які проходить лист на шляху до вас? Логічно, що IP у листі від вас може вказати на вашого інтернет-провайдера і звузити ваше можливе місцеперебування до конкретної географічної області.

Під час першого входу, який запитує ваші геодані (як-от сайти з прогнозом погоди), браузер повинен запитати, чи ви хочете поділитися цією інформацією із сайтом. Можна і погодитися: так у вас буде краще налаштована реклама. Наприклад, на washingtonpost.com ви бачитимете бізнес-оголошення у власному місті, а не в самому Вашингтоні.

Не знаєте, чи пропонував вам браузер вибір раніше? Спробуйте протестувати це на сторінці benwerd.com/lab/geo.php. Подібні тестові сайти демонструють, чи відправляє ваш браузер інформацію про місцеперебування. Якщо таки відправляє, а ви хочете залишитися непоміченим, вимкніть цю функцію. На щастя, це можливо. У Firefox в адресному рядку надрукуйте «about:config», прокрутіть вниз до «geo» і змініть налаштування на «disable». Збережіть зміни. У Chrome відкрийте Налаштування>Розширені>Веб-контент>Місцеперебування і змініть «Запитувати дозволу, перш ніж надавати доступ (рекомендується)» на «Заблоковано». Це відключить геолокацію в Chrome. Подібні функції є і в інших браузерах.

Можна заради жарту підробити свою геолокацію. Якщо хочете відправити сайту хибні координати (скажімо, Білого дому), встановіть у браузері Firefox плагін Geolocator. У Google Chrome можна зробити це через вбудовану функцію емуляції геолокації. Відкрийте Chrome і натисніть Ctrl+Shift+I у Windows чи Cmd+Option+I на Mac — вам відкриється Панель інструментів веб-розробника. У консольному вікні знайдіть три вертикальні точки у правому верхньому кутку, клікніть, виберіть More tools>Sensors. Знизу вам відкриється вкладка Sensors, і ви зможете вибрати конкретну широту й довготу. Можна ввести координати відомої пам'ятки або точку посеред океану — сайт усе одно не буде знати, де ви перебуваєте насправді.

В інтернеті можна приховати не лише геолокацію, а й IP-адресу. Раніше я казав про Tor, який рандомізує IP-адресу, що показується сайтові, на який ви заходите. Але не всі сайти відкриваються у Tor. Приміром, фейсбук донедавна блокувався. Для сайтів, які не приймають запити Tor, можна скористатися проксі.

Відкритий проксі — це сервер-посередник між вами й інтернетом. У розділі 2 я проводив аналогію між проксі-сервером і перекладачем: ви повідомляєте текст перекладачеві, він передає його іншомовній людині, але повідомлення не

змінюється. Якщо пам'ятаєте, про проксі я говорив як про спосіб надіслати імейл із ворожої країни, прикинувшись громадянином безпечної держави.

Скористатися проксі-сервером можна і для того, щоб дістати доступ до веб-сайтів із географічною прив'язкою, наприклад, якщо живете в країні, яка обмежує доступ до ґуґл-пошуку. Або, можливо, вам треба приховати свою особу, щоб завантажити незаконний або захищений авторським правом контент через BitTorrent.

Однак проксі-сервери не є невразливими. Якщо користуєтеся проксі, то не забувайте, що кожен браузер треба вручну налаштувати на роботу із проксі. І навіть найкращі проксі-сайти визнають, що Flash чи JavaScript хитрими трюками можуть вирахувати ваш справжній IP, через який ви під'єднуєтеся до самого проксі-сервера. Ви можете знизити вірогідність таких трюків, заблокувавши чи обмеживши в браузері використання Flash і JavaScript. Але найкращий спосіб запобігти свавіллю JavaScript — скористатися плагіном HTTPS Everywhere.

Існує купа платних проксі-сервісів, але обов'язково читайте політику конфіденційності компанії, продуктом якої збираєтеся скористатися. Звертайте увагу на принципи шифрування даних у русі й можливість передавання особистої інформації правоохоронним та урядовим органам.

Є й безкоштовні проксі, але як плату за користування вам доведеться терпіти нескінченний потік безглуздої реклами. Особисто я раджу утримуватися від безкоштовних проксі. На конференції DEF CON 20 мій товариш і експерт з інформаційної безпеки Чема Алонсо презентував експеримент: він створив проксі-сервер і, в надії привернути увагу поганих хлопців, виклав його IP-адресу на xroxy.com. Уже за кілька днів п'ять тисяч людей користувалися його безкоштовним, «анонімним» проксі. На жаль, більшість з них провертала через сервер афери.

Однак є й позитив: через цей проксі Алонсо міг легко заразити комп'ютери аферистів вірусом і стежити за їхніми діями. Так він і вчинив, скориставшись BeEF — фреймворком для експлуатації браузера. Також у хід пішла користувацька угода, на яку люди самі й погодилися. Так Алонсо дістав можливість проглядати імейли, що проходили через проксі-сервер, щодо злочинної діяльності. Мораль тут така: безкоштовний сир лише в мишоловці. Ви все одно так чи інакше заплатите.

Якщо ви користуєтеся проксі з протоколом https, правоохоронні органи або державні установи бачитимуть лише IP-адресу проксі-сервера, а не ваші дії на веб-сайтах — ця інформація буде зашифрована. Як я вже згадував, звичайні сайти з протоколом http не шифруються, тож раджу встановити HTTPS Everywhere (так, це моя відповідь на більшість проблем із конфіденційністю браузера).

Для зручності користувачі часто синхронізують налаштування браузера на різних пристроях. Наприклад, при вході в браузер Chrome чи Chromebook ваші вкладки, закладки, історія й інші налаштування браузера синхронізуються за

допомогою облікового запису Google. Ці параметри завантажуються автоматично щоразу, як ви відкриваєте Chrome на комп'ютері чи телефоні. Щоб вибрати, що саме треба синхронізувати, перейдіть на сторінку налаштувань браузера Chrome. Панель інструментів Google дає вам повний контроль над управлінням і видаленням синхронізованих даних з акаунта. Переконайтеся, що конфіденційна інформація не синхронізується автоматично. Mozilla Firefox теж має опцію синхронізації.

Мінус у тому, що якщо зловмисник якось змусить вас зайти у свій акаунт Google в нього в браузері, то зможе завантажити собі всю вашу історію пошуку. Уявіть, що ваш друг зайшов у свій акаунт з вашого комп'ютера. Уся його історія, закладки тощо відразу синхронізуються. Тепер ви можете проглянути його історію пошуку й купу іншої інформації в себе на комп'ютері. А якщо ви увійдете в синхронізований акаунт через пристрій у громадському місці й забудете вийти, наступний користувач отримає вашу історію та закладки. Якщо це трапиться в Google Chrome, то навіть ваш Google Календар, YouTube та інші елементи акаунта Google стануть загальнодоступними. Якщо користуєтеся загальним комп'ютером, не забувайте виходити з облікових записів.

Ще один недолік синхронізації — усі взаємопов'язані пристрої будуть показувати однаковий контент. Якщо ви живете один, то байдуже. Але якщо поділитеся з кимось акаунтом в iCloud, готуйтеся до проблем. Наприклад, батьки, які дозволяють своїм дітям використовувати сімейний iPad, можуть ненавмисно дозволити їм проглядати дорослі матеріали[89].

У крамниці Apple в Денвері, штат Колорадо, місцевий менеджер по роботі з клієнтами Еліот Родрігес зареєстрував свій новий планшет на колишній акаунт в iCloud. За мить усі його фотографії, тексти, музика й відео висвітилися на новому планшеті. Це добряче заощадило час, бо йому не довелося вручну копіювати це на нові девайси. Він мав доступ до даних незалежно від того, яким пристроєм користувався.

За кілька років Еліот вирішив віддати свій застарілий планшет восьмирічній донечці. І те, що планшет був з'єднаний з усіма іншими пристроями Еліота, попервах здавалося йому плюсом. На новому планшеті він бачив кожен новий застосунок, що його донька завантажувала на свій пристрій. Іноді вони навіть ділилися сімейними світлинами. Але потім Еліот вирушив до Нью-Йорка, куди часто їздив у справах.

Не подумавши, Еліот зробив на айфон кілька фото зі своєю нью-йоркською коханкою, деякі з них досить... інтимні. Зображення з його айфону автоматично синхронізувалися з айпадом його дочки в Колорадо. І, ясна річ, донька запитала маму про жінку, яка була з татком. Думаю, не варто казати, що вдома на Еліота чекала серйозна розмова.

А ще виникає проблема з подарунками на день народження. Якщо у вас в родині зв'язані пристрої чи синхронізовані акаунти, майбутній іменинник може натрапити на історію пошуку й дізнатися, що ви йому подаруєте. Чи навіть

гірше: що ви збиралися йому подарувати. Ще одна проблема конфіденційності із сімейними комп'ютерами чи планшетами. Елементарний спосіб цього уникнути — зареєструвати кілька користувачів, що досить просто зробити на Windows. Залишіть собі права адміністратора, щоб ви могли реєструвати додаткові акаунти для членів родини і встановлювати потрібні програми. Усі користувачі будуть заходити у свій обліковий запис із власним паролем і матимуть доступ лише до власних файлів, закладок та історій браузера.

Apple має схожу функцію в операційних системах OS X, однак часом деякі забувають розділити простір iCloud. А часом ми ні в чому не винні і технології нас просто підводять.

Після багатьох років легковажних романів лос-анджелеський телевізійний продюсер Ділан Монро нарешті знайшов «ту саму» і вирішив спробувати серйозні стосунки. Вони з нареченою з'їхалися, і він без задньої думки під'єднав майбутню дружину до свого акаунта в iCloud.

Коли створюєш родину, зробити для всіх її членів єдиний акаунт — це логічний крок, невід'ємна частина спільного проживання. Так можна обмінюватися відео, документами й музикою з вашою другою половинкою. Нинішньою другою половинкою. Яка не захоче бачити ваше цифрове минуле.

Іноді сервіси автоматичного хмарного резервного копіювання на зразок iCloud перетворюються на віртуальне горище, де ми роками збираємо фотографії, тексти й музику. Про дещо з цього ми успішно забуваємо, наче про вміст старих коробок у підвалі.

Світлини — це наші візуальні спогади. А другі половинки вже багато поколінь знаходять ці забуті коробки, повні листів і фотографій. Але цифрове середовище, де можна без проблем зберігати тисячі фото високої якості, — проблема масштабніша. Раптово старі спогади Ділана (а деякі з них дуже особисті) огорнули його у вигляді світлин, що тепер мирно спочивали в телефоні та планшеті його нареченої.

Довелося викинути деякі меблі, бо на фото Ділан займався коханням з іншими жінками на отому дивані, отому столі і в цьому ліжку. Довелося відмовитися від деяких ресторанів, бо наречена відмовлялася йти в місце, де на фото Ділан сидить з іншою за тим столиком чи в цьому кутку.

Ділан обожнював наречену й покірливо виконував усі забаганки і навіть пішов на грандіозну жертву: продав будинок одразу після весілля. І все тому, що він синхронізував айфони.

І от ще цікава проблема із «хмарами». Навіть якщо ви видалите історію браузера на ПК, ноутбуці чи мобільному пристрої, копія історії пошуку залишиться в «хмарі». А із серверів компанії історію видалити трохи складніше. І набагато складніше заборонити її зберігання. Ось вам приклад того, як таємний збір даних без належного контексту можна хибно витлумачити пізніше. Навіть невинні пошукові запити можуть пустити все під укіс.

Одного ранку наприкінці літа 2013 року, усього за кілька тижнів після вибуху на Бостонському марафоні, чоловік Мікеле Каталано побачив, як три чорних позашляховики під'їхали до їхнього будинку на Лонг-Айленді. Коли він вийшов на вулицю привітатися з поліцейськими, вони попросили документи і показали дозвіл обшукати будинок. Приховувати чоловікові було нічого, тож він їх впустив. Хоча й не розумів, у чому річ. Квапливо оглянувши кімнати, федеральні агенти перейшли до допиту.

«Хто-небудь у цьому будинку шукав інформацію про скороварки?»

«Хто-небудь у цьому будинку шукав інформацію про рюкзаки?»

Мабуть, історія ґуґл-пошуку родини Каталано потягнула за собою попереднє розслідування Департаменту внутрішньої безпеки. Імовірно, протягом кількох тижнів після вибуху на Бостонському марафоні правоохоронні органи стежили за пошуком в інтернеті і відмічали деякі результати, які в поєднанні натякали на тероризм. За дві години із сім'ї Каталано зняли будь-які потенційні звинувачення. Пізніше Мікеле написала про цей досвід на сайті Medium як попередження: те, що ви шукаєте сьогодні, може обернутися зовсім іншим боком завтра[90].

У статті Каталано зауважила, що слідчі проігнорували її пошукові запити на зразок «Що мені, в біса, робити з кіноа?» чи «Алекса Родріґеза вже дискваліфікували?». Шукала вона скороварки лише для того, щоб якось зварити те кіноа. А рюкзак? Рюкзак шукав собі її чоловік.

Принаймні один пошуковик — Google — створив кілька інструментів конфіденційності, що допомагають вибирати, якою інформацією ви бажаєте поділитися[91]. Наприклад, ви можете відключити персоналізоване відстеження реклами, щоб, якщо ви ґуґлите Патагонію (регіон у Південній Америці), вас не завалило рекламою турів у Південну Америку. Ви також можете повністю відключити історію пошуку або вийти з Gmail, YouTube чи будь-якого іншого акаунта в Google під час пошуку в інтернеті.

Навіть якщо ви вийшли з акаунтів у Microsoft, Yahoo чи Google, ваша IP-адреса все ще прив'язана до кожного запиту пошукової системи. Один зі способів уникнути цього — використовувати проксі для ґуґлу startpage.com чи пошуковик DuckDuckGo.

DuckDuckGo вже є опцією за замовчуванням у Firefox і Safari. На відміну від Google, Yahoo і Microsoft, у DuckDuckGo нема можливості створити акаунт, а розробник заявляє, що ваш IP не реєструється за замовчуванням. А ще компанія підтримує власний вузол виходу в Tor, тобто ви можете користуватися DuckDuckGo у Tor-браузері без лаґів[92].

Позаяк DuckDuckGo не відстежує ваших дій, нові результати пошуку не будуть фільтруватися минулими. Більшість людей цього не знає, але результати, які вам видає Google, Yahoo і Bing, фільтруються на основі того, що ви шукали на цих сайтах раніше. Наприклад, якщо пошуковик побачить, що часто відвідуєте сайти про здоров'я, він почне фільтрувати пошук і піднімати вверх

результати, пов'язані зі здоров'ям. Чому? Тому що нам ліньки перейти на другу сторінку результатів пошуку. Є навіть такий жарт: якщо хочете сховати труп у надійному місці, спробуйте другу сторінку пошуку в ґуґлі.

Можливо, дехто оцінить зручність того, що не треба прокручувати нецікаві результати. Але так ви, по суті, дозволяєте пошуковикові вирішувати за вас, що вам цікаво, а що — ні. З якого боку не поглянь, цензура. DuckDuckGo теж фільтрує результати пошуку, але за темою, а не минулою історією пошуку.

У наступному розділі я детальніше розповім про спроби веб-сайтів розсекретити вашу особу і те, як зробити серфінг в інтернеті анонімним.

---

85 https://www.techdirt.com/articles/20150606/16191831259/according-to-government-clearing-your-browser-history-is-felony.shtml

86 http://www.cbc.ca/news/trending/clearing-your-browser-history-can-be-deemed-obstruction-of-justice-in-the-u-s-1.3105222.

87 http://ftpcontent2.worldnow.com/whdh/pdf/Matanov-Khairullozhon-indictment.pdf.

88 https://www.eff.org/https-everywhere%20.

89 http://www.tekrevue.com/safari-sync-browser-history/.

90 http://www.theguardian.com/commentisfree/2013/aug/01/government-tracking-google-searches.

91 https://myaccount.google.com/intro/privacy.

92 http://www.fastcompany.com/3026698/inside-duckduckgo-googles-tiniest-fiercest-competitor.

Розділ 6
Гра у схованки

Будьте обережні з пошуками в інтернеті. За вашою поведінкою онлайн стежать не лише пошуковики, а й самі сайти. Здавалося б, навіщо сайтам розголошувати про вас особисту інформацію? Але дослідження 2015 року показало, що «70 % сайтів із питань здоров'я містять інформацію про конкретні стани, лікування та хвороби в URL»[93].

Інакше кажучи, якщо я зайду на сайт WebMD і введу в пошук «грибок стопи», то ця фраза в зашифрованому вигляді з'явиться в URL сторінки, який відображається в адресному рядку браузера. А отже, будь-хто — мій браузер, інтернет-провайдер, оператор зв'язку — знатиме, що я шукаю інформацію про грибок стопи. Плагін HTTPS Everywhere, звісно ж, зашифрує зміст сайту, якщо той підтримує https, але URL він зашифрувати не зможе. Навіть у Electronic Frontier Foundation зазначають, що https не призначений для того, щоб приховувати інформацію про відвідувані сайти.

Крім того, дослідження показало, що 91 % сайтів, пов'язаних зі здоров'ям, роблять запити третім сторонам. Процес вбудовано в саму сторінку, і робиться запит на крихітні зображення (які можуть навіть не відображатися на сторінці браузера). Так стороннім сайтам надходить інформація про те, що ви відвідуєте конкретну сторінку. Забийте в пошук «грибок стопи» — і десь зо двадцять різних сайтів (від фармацевтичних компаній до Facebook, Pinterest, Twitter і Google) знатимуть про це швидше, ніж браузер встигне завантажити результати пошуку. Тепер усім їм відомо, що ви шукали інформацію про грибок стопи[94].

І треті сторони скористаються цим, щоб краще налаштувати на вас рекламу. А якщо ви ще й акаунт на сайті маєте, то вони можуть отримати ще й вашу імейл-адресу. Але не хвилюйтеся. Зараз я навчу вас, як цього уникнути.

У дослідженні медичних сайтів 2015 року серед топ-10 третіх сторін фігурували такі компанії: Google, comScore, Facebook, AppNexus, AddThis, Twitter, Quantcast, Amazon, Adobe та Yahoo. Деякі з них — comScore, AppNexus та Quantcast — вимірюють веб-трафік, як і Google. З усіх вищеперерахованих компаній Google, Facebook, Twitter, Amazon, Adobe та Yahoo шпигують за вашими діями в комерційних цілях. Отож згодом у вас у браузері може вискакувати реклама щодо лікування грибка стопи.

Також у дослідженні згадано Experian та Axiom, що, по суті, є звичайними сховищами даних, які намагаються зібрати якомога більше інформації на кожну людину. Яку вони потім продають. Пам'ятаєте нашу бесіду про секретні питання та креативні відповіді? Компанії на зразок Experian та Axiom часто збирають і обробляють такі питання, доповнюючи ваш інтернет-профіль. Ці профілі є цінними для маркетологів, які хочуть налаштувати рекламу своїх продуктів на цільову аудиторію.

Як це працює?

Незалежно від того, вводите ви URL вручну або через пошуковик, кожен сайт в інтернеті має ім'я хоста та числову IP-адресу (деякі сайти існують тільки у формі числової адреси). Але цю числову адресу ви майже ніколи не бачите. Ваш браузер приховує її, перетворюючи ім'я хоста сайту (скажімо, Google) на певну адресу через службу доменних імен (DNS). Наприклад, у Google вона має такий вигляд: https://74.125.224.72/. DNS схожа на всесвітню телефонну книгу, яка містить ім'я хоста й відповідну числову адресу сервера сайту, на який ви намагаєтеся зайти. Введіть «google.com» в адресний рядок браузера — і DNS надішле запит на сервер https://74.125.224.72. І от ви вже бачите знайомий білий екран з написом Google над порожнім рядком пошуку. Загалом так працюють усі веб-браузери. На практиці ж усе трохи складніше.

Після того як сайт ідентифікувався за числовою адресою, він відправляє інформацію назад до вашого браузера, щоб той зміг «побудувати» веб-сторінку, яка з'являється у вас перед очима. Коли сторінка повертається у ваш браузер, ви бачите всі очікувані деталі: інформацію, яку шукали, пов'язані з нею зображення і посилання на інші розділи сайту. Але часто в браузер повертаються й деталі, що надсилають запити на додаткові зображення, або скрипти, на інші сайти. Деякі (ба майже всі) із цих скриптів мають функцію відстеження і в більшості випадків вам просто не потрібні.

Майже будь-яка цифрова технологія створює метадані, і, як ви вже здогадалися, браузери не є винятком. Сайти, які ви відвідуєте, можуть навіть отримати інформацію про конфігурацію вашого комп'ютера. Приміром, яка у вас стоїть операційна система і версія браузера, які додаткові модулі і програми (приміром, продукти від Adobe) встановлено в момент пошуку. А ще інформацію про «залізо», як-от роздільна здатність екрана та ємність вбудованої пам'яті.

У нас уже шостий розділ. Якщо вам здається, що ви вже достатньо зробили для непомітності в інтернеті, то так і є. Але завжди можна зробити ще більше.

Не полінуйтеся зайти на сайт panopticlick.com. Ця розробка Electronic Frontier Foundation може визначити, наскільки поширена (чи унікальна) у вас конфігурація браузера порівняно з іншими, проаналізувавши операційну систему ПК чи телефона та встановлені плагіни. Інакше кажучи, вам скажуть, чи є у вас плагіни, що обмежують чи захищають інформацію, яку Panopticlick намагається витягнути з вашого браузера.

Якщо panopticlick.com видасть вам зліва велике число (скажімо, шестизначне), то ви досить унікальні: подібні налаштування браузера трапляються в одному зі ста тисяч комп'ютерів. Мої вітання. А от якщо результат невеликий (приміром, менше за тризначне число), то налаштування вашого браузера досить поширені. Такі є вже в одного з кількох сотень. А це означає, що якщо я захочу налаштувати на вас рекламу чи заразити вірусом, мені

не доведеться надто напружуватися, бо налаштування вашого браузера досить банальні[95].

Здавалося б, поширена конфігурація — ключ до невидимості. Ви — частина натовпу. Ви не виділяєтеся. Але, з технічного погляду, ви даєте зловмисникам зелене світло. Хакер не хоче надто напружуватися. Уявіть, що ви — крадій. Перед вами два будинки: один із зачиненими дверима, інший — з відчиненими. Який пограбуєте? Якщо хакер знає, що у вас типові налаштування, то логічно буде припустити, що із заходами безпеки у вас теж проблеми.

Я розумію, що несподівано перестрибнув із маркетологів, які стежать за вашими діями в інтернеті, на зловмисників, які можуть вкрасти особисту інформацію. Це зовсім різні речі. Маркетологи збирають дані, щоб показувати на сайтах прибуткову й ефективну рекламу. Без реклами деякі сайти просто не зможуть існувати. Але і маркетологи, і хакери, і навіть уряд намагаються дістати інформацію, якою ви не хочете ділитися, тож усі вони часто фігурують разом у дискусіях про вторгнення в приватне життя.

Один зі способів залишити звичні налаштування, але й уберегти себе від інтернет-шпигунства — скористатися віртуальною машиною (VM; див. розділ 16) — операційною системою (на зразок Mac OS X), що працює поверх звичайної Windows. Можна встановити собі продукт від VMware і запускати через нього іншу операційну систему. А коли завершите роботу, просто вийдіть з програми. Операційна система і всі ваші дії всередині системи зникнуть, а збережені файли так і залишаться там, де ви їх зберегли.

І ще дещо спільне між «мирними» маркетологами і злочинними хакерами: усі вони збирають інформацію про відвідувачів сайту через так звані однопіксельні зображення, чи веб-маячки. Ці зображення розміром 1×1 піксель схожі за принципом роботи на порожні спливаючі вікна і вбудовуються в саму сторінку. Хоча й зображення невидиме, воно здатне надсилати запити стороннім сайтам, які її там розмістили. Внутрішній сервер записує IP-адресу сайту, який намагався відобразити це зображення. Так однопіксельне зображення на медичному сайті може сповістити фармацевтичну компанію про те, що я шукав інформацію про лікування грибка стопи.

Дослідження 2015 року, про яке я згадував на початку розділу, показало, що майже половина сторонніх запитів просто відкривають спливаючі вікна без жодного контенту. Ці порожні вікна непомітно генерують http-запити до сторонніх хостів з метою відстеження. Але цього можна уникнути, заборонивши браузерові відкривати спливаючі вікна (що позбавить вас ще й від набридливої реклами).

Майже третина всіх сторонніх запитів складається з коротких рядків коду — файлів JavaScript, які зазвичай відповідають за анімацію на веб-сторінці. Сайт, на який ви намагаєтеся зайти, ідентифікує комп'ютер переважно за IP-адресою, яка посилає запит на файл JavaScript.

Але сайти можуть стежити за вашими діями в інтернеті і без однопіксельного зображення чи порожнього спливаючого вікна. Наприклад, якщо Amazon дізнається, що останнім ви відвідали медичний сайт, то запропонує вам продукти для здоров'я вже на власному сайті. Як Amazon дізнається? Просто продивиться запити браузера і знайде останній сайт, який ви відвідали.

Amazon робить це через сторонні реферери — текст у запиті на веб-сторінку, який повідомляє новій сторінці, звідки надійшов запит. Приміром, якщо я читаю статтю на Wired, натрапляю в ній на посилання й переходжу по ньому, новий сайт буде знати, що перейшов я зі сторінки wired.com. Здогадуєтеся, як це може вплинути на вашу конфіденційність?

Щоб уникнути цього, ви можете перейти на бажаний сайт через ґуґл, щоб цей сайт не знав, де ви були до цього. Але не думаю, що сторонні реферери — це якась величезна проблема, якщо ви не намагаєтеся приховати свою особу. Це ще один приклад компромісу між зручністю (швидкий перехід на наступний сайт) і невидимістю (завжди переходити через google.com).

Mozilla Firefox пропонує один з найкращих засобів захисту від стороннього стеження за допомогою плагіна NoScript[96]. Цей застосунок ефективно блокує майже все, що вважає шкідливим для вашого комп'ютера і браузера, а саме Flash і JavaScript. Ясна річ, плагіни безпеки змінюють зовнішній вигляд веб-сторінки не на краще, але завжди можна включити певні функції чи вибрати, яким сайтам довіряти.

Величезний плюс NoScript полягає в тому, що він прибирає з веб-сторінки всю рекламу і, звичайно ж, сторонні реферери. Але в результаті сторінка буде дещо порожньою порівняно з оригінальною версією. Однак, якщо вам ну дуже потрібне те Flash-відео у верхньому лівому кутку сторінки, можна дозволити відображення цього конкретного елемента, заблокувавши все інше. Або, якщо ви цілком довіряєте сайтові, можете дозволити завантаження всіх елементів на цій сторінці тимчасово або на постійній основі (наприклад, на сайті інтернет-банку).

А от для Chrome є ScriptBlock[97], який дає змогу блокувати запуск скриптів на веб-сторінці. Чудовий варіант для дітей, які можуть натрапити на сайт, що містить спливаючу рекламу контенту для дорослих.

Блокування потенційно небезпечних (і, звичайно ж, шкідливих для конфіденційності) елементів веб-сторінок убереже ваш комп'ютер від шкідливих програм, що засипають вас рекламою. Приміром, вам доводилося помічати оголошення на головній сторінці Google? Річ у тому, що на головній сторінці Google оголошень бути не може. Якщо ви їх бачите, то, найімовірніше, ваш комп'ютер і браузер заразили. Клікати по такій сторонній рекламі небезпечно: вона може містити «троян» (кілоґер, який записує кожне натиснення клавіші) чи інші віруси. А навіть якщо нічого небезпечного в цій рекламі нема, від кількості кліків залежить дохід рекламодавців. Що більше людей вони обманюють, то більше грошей заробляють.

Але якими чудовими не були б NoScript і ScriptBlock, заблокувати все вони не здатні. Для повного захисту браузера від загроз можна встановити Adblock Plus. Єдина проблема полягає в тому, що Adblock усе записує — ще одна програма, яка відстежує історію серфінгу попри режим приватного перегляду. Однак у цьому випадку плюси (блокування потенційно небезпечних оголошень) перевершують мінуси (компанія бачить ваші дії в інтернеті).

Ще один корисний плагін називається Ghostery. Він доступний як для Chrome, так і для Firefox. Ghostery ідентифікує всі трекери веб-трафіка (наприклад, DoubleClick і Google AdSense), через які сайти стежать за вашою активністю. Як і NoScript, Ghostery дає вам повний контроль над тим, які трекери блокувати, а які дозволяти. На сайті розробника написано: «Блокування трекерів не допустить їх запуску у вашому браузері, що допоможе запобігти відстеженню ваших поведінкових даних. Але майте на увазі, що деякі трекери — потенційно корисні, як-от віджети у стрічці соцмереж чи браузерні ігри. Блокування може вплинути на сайти, які ви відвідуєте, непередбачувано». Тобто деякі сайти не будуть працювати з увімкненим Ghostery. На щастя, його можна відключити для конкретного сайту[98].

Блокування відстеження на сайтах через плагіни — лише половина справи. Раджу ще й заплутати потенційних хакерів різними адресами електронної пошти для різних цілей. У розділі 2 ми говорили про створення анонімних імейлів для анонімного спілкування. Однак кілька акаунтів електронної пошти — непогана ідея і для щоденного використання. Це вас не сховає — просто зробить менш цікавим для третіх сторін. З погляду конфіденційності, кілька імейл-профілів в інтернеті — безпечніше, ніж одна-єдина адреса. Якщо хтось захоче зібрати на вас цифрове досьє, завдання буде дуже непростим.

Припустимо, ви хочете щось купити в інтернеті. Можна створити імейл лише для покупок. А ще можна замовляти все, що купуєте через цей імейл, на відділення служби доставлення, а не домашню адресу. І купувати все з передплаченої подарункової картки, яку час від часу поповнюватимете.

Так продавець бачитиме лиш додатковий імейл, адресу відділення перевізника й подарункову картку, яку ви можете викинути будь-якої миті. Якщо в цій компанії колись станеться витік даних, зловмисники не матимуть ні вашого основного імейлу, ні реальної адреси, ні номера банківської картки.

Дистанціюватися від інтернет-покупок — непоганий спосіб захистити конфіденційність.

А ще можна створити додаткову адресу електронної пошти для соцмереж. Її можна використовувати і як «публічну» адресу, на яку вам писатимуть незнайомці і малознайомі люди. Плюс в тому, що, знову ж таки, вони не зможуть про вас надто багато дізнатися. Принаймні це буде непросто. Ви можете додатково захистити себе, зареєструвавши кожен імейл на унікальне ім'я — варіацію справжнього імені або цілком вигадане.

Але будьте обережні, якщо вибрали перший варіант. Приміром, не варто писати чи натякати на своє друге ім'я. Навіть щось таке безневинне, як JohnQDoe@xyz.com уже каже нам, що у вас є друге ім'я і воно починається з Q. Ось вам приклад того, як можна розголосити особисту інформацію без потреби. Не забувайте, що вам треба злитися з натовпом, а не привертати до себе увагу.

Якщо використовуєте слово або фразу, не пов'язану з іменем, робіть її більш відстороненою. Приміром, за адресою snowboarder@xyz.com ім'я ми ваше не вгадаємо, а от хобі — цілком. Вибирайте щось більш загальне, як-от silverfox@xyz.com[99].

Ясна річ, вам потрібен і особистий імейл. Ним можна ділитися лише з близькими друзями і сім'єю. Але безпека конфіденційності дає непогані бонуси: додатковий імейл для інтернет-покупок убереже вас від тонни спаму на особисту адресу.

Мобільні телефони не застраховані від корпоративного стеження. Влітку 2015 року один уважний дослідник зловив операторів AT&T і Verizon на тому, що вони додавали спеціальний код до кожного запиту веб-сторінки через мобільний браузер. І це не міжнародний ідентифікатор користувача мобільного зв'язку IMSI, про який я говорив у розділі 3, а унікальний ідентифікаційний код, який надсилається з кожним запитом веб-сторінки. Так званий унікальний ідентифікаційний заголовок (UIDH) є тимчасовим серійним номером, за яким рекламодавці ідентифікують вас в інтернеті. Дослідник дізнався про все це, бо налаштував свій мобільний телефон на створення логів веб-трафіка (що мало хто робить). У цих логах він і помітив додаткові дані, що з'являлися в клієнтів Verizon і, як потім виявилося, AT&T[100].

Проблема в тому, що клієнтам про цей додатковий код не повідомили. Наприклад, за тими, хто завантажив мобільний браузер Firefox і встановив плагіни конфіденційності, однак користувався послугами AT&T або Verizon, усе одно стежили через коди UIDH.

Завдяки UIDH-кодам Verizon і AT&T могли скористатися вашим веб-трафіком або для створення профілю вашої мобільної активності в інтернеті для рекламодавців, або щоб згодом продати ці дані.

AT&T тимчасово припинили цю практику... поки що[101]. Verizon же перетворили це на опцію, від якої користувач може відмовитися[102]. Але будьте уважні: не відмовляючись, ви автоматично даєте Verizon згоду.

Навіть якщо вимкнути JavaScript, сайт усе одно може надіслати вашому браузерові текстовий файл із даними — так званий «cookie». Cookie можуть зберігатися тривалий час. Вони є фрагментами тексту, які надсилаються веб-сайтом і зберігаються в браузері користувача для відстеження стану сеансу (наприклад, які товари лежать у кошику) чи навіть автентифікації користувача. Уперше cookie-файлами скористалися Netscape. Попервах вони призначалися для створення віртуальних кошиків та електронної комерції. Cookie-файли зазвичай зберігаються в браузері на ПК і мають термін дії, хоча термін цей може

становити й кілька десятиліть. Чи є cookie небезпечними? Ні. Принаймні не самі собою. Проте cookie постачають третім сайтам інформацію про ваш акаунт і пріоритети, як-от улюблені міста на сайті прогнозу погоди чи улюблені авіакомпанії на туристичному сайті. Якщо такий сайт уже створив cookie-файл, то наступного разу, як ваш браузер під'єднається до нього, сайт вас «згадає» і, можливо, навіть привітається. Якщо ж це сайт електронної комерції, він може запам'ятати ваші останні покупки.

По суті, cookie-файли зберігають цю інформацію не на вашому ПК чи мобільному девайсі. Як і стільникові телефони, що використовують IMSI як проксі, cookie-файли містять проксі для даних, що зберігаються на серверах сайту. Коли ваш браузер завантажує веб-сторінку з прикріпленим cookie-файлом, додаткові дані про вас витягуються із самого сайту.

Cookie-файли не лише зберігають ваші налаштування сайту, а й надають цьому сайтові цінні дані для стеження. Наприклад, якщо ви є потенційним клієнтом компанії і колись ввели адресу електронної пошти або іншу інформацію, щоб завантажити собі інформаційну брошуру, імовірно, сайт уже відправив вашому браузерові cookie-файл, який відповідає інформації про вас у системі управління відносинами з клієнтами (CRM) компанії — скажімо, Salesforce або HubSpot. Тепер щоразу, як ви заходитимете на сайт цієї компанії, вас ідентифікуватимуть через cookie в браузері, й інформація про сеанс запишеться в CRM.

Cookie-файли є сегментованими, тобто зазвичай сайт А не бачить вміст cookie-файлу для сайту Б. Бувають винятки, але в цілому інформація зберігається окремо й досить безпечно. Однак, з погляду конфіденційності, cookie шкодять вашій непомітності.

Дістати доступ до cookie-файлів можна лише всередині одного домену, але рекламні агентства навчилися обходити цю проблему, завантажуючи cookie-файли, що відстежують вашу активність на кількох сайтах, які є частиною більшої мережі. Хоча загалом cookie одного сайту не можуть дістати доступ до cookie-файлів іншого, а сучасні браузери дають користувачеві можливість контролювати cookie. Наприклад, якщо ви сидите в інтернеті в режимі інкогніто чи приватному режимі, у вас у браузері не зберігатиметься ні історія відвідування цього сайту, ні cookie-файли цієї сесії. Однак якщо у вас був cookie-файл із попереднього відвідування, він однак працюватиме в приватному режимі. З іншого боку, у звичайному режимі перегляду можна час від часу вручну частково або повністю видаляти cookie за минулі роки.

Хоча маю попередити, що видалення всіх cookie-файлів незавжди доцільно.

Вибіркове видалення cookie-файлів випадкових сайтів, які вам уже не цікаві, допоможе позбавитися зайвих слідів в інтернеті. Якщо ви зайдете на ці сайти ще раз, вони вас не «впізнають». Але, приміром, вводити щоразу своє місто на сайті прогнозу погоди — сізіфова праця. Cookie-файл легко би розв'язав цю проблему.

Видалити cookie може через спеціальне доповнення або через налаштування браузера, де зазвичай є опція видалити один або кілька (чи навіть усі) cookie-файли. Тож ви можете визначати долю ваших cookie-файлів для кожного конкретного випадку.

Деякі рекламодавці використовують cookie для спостереження за тим, скільки часу ви проводите на сайтах, де вони розмістили свої оголошення. Деякі навіть записують інформацію про ваші відвідування попередніх сайтів — так званих сайтів реферера. Видаляйте ці cookie-файли відразу. Як їх вирізнити? Шукайте файли з назвами сайтів, які ви ніколи не відвідували. Наприклад, замість «CNN» cookie-файл реферера називатиметься «Ad321». Також розгляньте варіант з інструментом для очищення cookie, як-от CCleaner, який спростить управління файлами.

Однак існують й такі cookie, на які ваші рішення взагалі не впливають. Вони називаються «супер-cookie» й зберігаються в системі комп'ютера, а не в самому браузері. Супер-cookie дістають доступ до налаштувань сайту й даних відстеження незалежно від того, який у вас браузер (сьогодні — Chrome, завтра — Firefox). Ці супер-cookie треба постійно видаляти з браузера, бо інакше ваш ПК намагатиметься відтворити cookie з пам'яті щоразу, як ви заходитимете на конкретний сайт.

Є два види файлів супер-cookie, які зберігаються поза межами браузера і які можна видалити: Flash від Adobe і Silverlight від Microsoft. В обох видів необмежений термін придатності. Ізазвичай безпечніше їх видалити[103].

Але це все квіточки порівняно з cookie від Семі Камкара, який прославився створенням комп'ютерного вірусу для MySpace під назвою «Семі». Свій новий винахід хакер називає «evercookie», що, по суті, є дуже стійкими cookie-файлами[104]. Чому ж вони такі стійкі? Камкар зміг запрограмувати cookie зберігатися в максимально можливій кількості систем усередині Windows. Поки одне з місць зберігання cookie-файлів залишається недоторканим, evercookie намагатиметься відновити себе скрізь[105]. Тож простого видалення evercookie-файлів з cookie-кеша браузера буде недостатньо. Це як боротися з казковим драконом: відріжеш одну голову — виросте інша. Щоб позбутися від evercookie-файлів раз і назавжди, треба видалити їх із усіх місць.

Якщо прикинути, скільки cookie-файлів зберігається у вашому браузері, і помножити їх на кількість потенційних місць зберігання на вашому ПК, то зрозумієте, що роботи тут на півдня.

Однак за нашою діяльністю в інтернеті стежать не лише сайти та мобільні оператори. Фейсбук уже давно став всюдисущим, вийшовши за межі звичайної соцмережі. Ви можете зареєструватися на фейсбуці і використовувати свій акаунт для входу в куну інших застосунків.

Наскільки така практика поширена? Один маркетинговий звіт показує, що аж 88 % користувачів у США заходили на сайт або в мобільний застосунок через існуючий акаунт соцмережі на зразок фейсбука, твітера чи Google+[106].

Зручність ця називається OAuth — протокол автентифікації, який дозволяє сайтові довіряти вам, навіть якщо ви не вводите пароль. І зручність ця має як плюси, так і мінуси. З одного боку, ви урізаєте шлях і швидко дістаєте доступ до нових сайтів, використовуючи існуючий пароль у соціальних мережах. З іншого ж, це дає соцмережі змогу збирати інформацію про вас для маркетингового профілю. За звичайних умов вона знає лиш те, що ви зайшли на її сайт, а з OAuth — усі сайти й компанії, де ви пройшли автентифікацію через акаунт соцмережі. З OAuth ми обмінюємо конфіденційність на комфорт.

Фейсбук, мабуть, найбільш «клейкий» з усіх соціальних медіа-платформ. Вихід із фейсбука може перекрити вашому браузерові доступ до самої соцмережі і її веб-застосунків. Крім того, фейсбук вбудовує трекери для моніторингу активності користувачів, які працюють, навіть якщо ви вийшли з фейсбука. Вони зчитують таку інформацію, як ваше місцеперебування, які сайти ви відвідуєте, куди заходите на цих сайтах, ваше ім'я користувача у фейсбуці. Організації із захисту конфіденційності висловили стурбованість наміром Facebook почати відстежувати інформацію з деяких веб-сайтів і застосунків, які відвідують користувачі, заради більш точної реклами.

Річ у тому, що фейсбукові, як і ґуґлу, потрібні дані про вас. Може, вони і не скажуть цього просто в лоб, але обхідними шляхами цю інформацію таки здобудуть. Якщо ви зв'яжете свій акаунт у фейсбуці з іншими сервісами, платформа отримає інформацію про вас і ці застосунки. Приміром, якщо ви користуєтеся фейсбуком для входу в інтернет-банк, то соцмережа знає, де ви зберігаєте гроші. І якщо хтось потрапить у ваш акаунт на фейсбуці, він матиме доступ до всіх інших веб-сайтів, пов'язаних із цим обліковим записом. Так, і до банківського рахунку теж. Власноруч створити собі ахіллесову п'яту — сумнівна ідея. Не полінуйтеся заходити у фейсбук лише тоді, коли вам потрібна соцмережа, і реєструватися у кожному застосунку окремо. Хоч це і буде на кілька секупд довше.

Крім того, Facebook свідомо вирішив ігнорувати сигнал «Не відстежувати», який посилає Internet Explorer, бо він не має «жодного галузевого консенсусу»[107]. Трекери Facebook представлені в класичних формах: cookie-файли, JavaScript, однопіксельні зображення і фрейми. Вони дають цільовим рекламодавцям доступ до cookie-файлів і трекерів браузера для просування продуктів, послуг і реклами як на фейсбуці, так і за його межами.

На щастя, існують розширення для браузерів, які блокують сервіси від Facebook на сторонніх сайтах, наприклад, Disconnect Facebook для Chrome[108] і Facebook Privacy List для Adblock Plus (який працює і у Firefox, і в Chrome)[109]. Мета всіх цих плагінів — дати вам контроль над інформацією, якою ви ділитеся з фейсбуком та іншими соцмережами, що пристібають вас до заднього сидіння й беруть кермо у свої руки. Враховуючи те, що Facebook знає про своїх 1,65 мільярда користувачів, компанія поводиться ще досить милосердно... поки що[110].

Як і Google, Facebook має просто тонни даних, якими досі не скористався. Але це зовсім не означає, що цей день ніколи не настане.

Ще більш кричущими і ще більш паразитичними за cookie-файли можна вважати панелі інструментів. Бувало таке, що у вашому браузері з'являлися додаткові панелі інструментів з написом Yahoo, McAfee, Ask чи будь-якою іншою назвою будь-якої іншої компанії? Ви можете навіть не пам'ятати, як вони там опинилися. І ніколи ними не користуватися. І не знати, як їх видалити.

Додаткові панелі інструментів відволікають вашу увагу від основної панелі в браузері. Рідна панель інструментів дає змогу самому вибрати пошукову систему за замовчуванням, а от паразитична спрямує вас на власний пошуковий сайт, де результати можуть аж по швах тріщати від спонсорського контенту. Саме це і трапилося з Ґері Мором — мешканцем Західного Голлівуду, який одного дня знайшов у себе панель від ask.com і жодного способу її видалити. «Це як непроханий гість, який нікуди не збирається йти», — прокоментував Мор[111]. Якщо у вас раптом з'явилася друга чи третя панель інструментів, імовірно, ви завантажили нове ПЗ або оновили старе. Наприклад, якщо на вашому ПК стоїть Java, її розробник Oracle за замовчуванням установить вам панель інструментів, якщо ви вручну від цього не відмовитеся. Клікаючи по сторінці завантаження чи оновлення, ви, напевно, не помітили крихітного прапорця, який за замовчуванням висловлював вашу згоду на встановлення панелі інструментів. У цьому нема нічого протизаконного: ви дійсно дали згоду, хай і просто забули відмовитися від автоматичного установлення. Але ця панель інструментів дає змогу іншій компанії відстежувати ваші дії в інтернеті і, можливо, навіть замінити вашу пошукову систему за замовчуванням на власну службу.

Найкращий спосіб позбавитися панелі інструментів — видалити її так само, як і звичайну програму з ПК. Але для деяких надто стійких і паразитичних панелей доведеться завантажити спеціальну програму для видалення, а сам процес видалення зможе переслати рекламним агентам стільки інформації, що вони будуть здатні перевстановити вам панель.

Під час установлення нового програмного забезпечення або оновлення старого уважно придивляйтеся до всіх прапорців. Якщо відмовитеся від панелей інструментів від самого початку, зможете уникнути купи клопоту.

То що як ви вже користуєтеся браузером у приватному режимі, маєте NoScript, HTTPS Everywhere і періодично видаляєте з браузера cookie-файли та сторонні панелі інструментів? Ви в безпеці, так? Ні. Вас усе ще можна відстежити.

Сайти кодують за допомогою так званої мови розмітки гіпертекстових документів, або HTML. У поточній версії, HTML5, запропоновано купу нових функцій. Деякі з них прискорили смерть таких супер-cookie, як Silverlight і Flash, що просто чудово. Однак HTML5 — свідомо чи ні — дав зелене світло новим технологіям відстеження.

Однією з них можна вважати цифровий відбиток із використанням Canvas — неймовірний і досить моторошний онлайн-інструмент для відстеження. Такий

цифровий відбиток спирається на елемент HTML5 під назвою «Canvas», що призначений для малювання простого зображення. От і все. Малювання зображення відбувається в браузері, невидиме для користувача і займає всього частку секунди. Але результат бачить сайт.

Ідея полягає в тому, що ваше «залізо», у поєднанні з ПЗ, малюватиме унікальне зображення (наприклад, ряд різнокольорових фігур), яке перетворюється на унікальний номер, подібний до пароля.

Опісля цей номер зіставляється з усіма випадками, коли він реєструвався на інших веб-сайтах. І вже на основі цього (кількості місць, де з'являвся цей номер) можна створити ваш профіль відвідувань сайтів. Такий цифровий відбиток допомагає ідентифікувати ваш браузер щоразу, коли ви повертаєтеся на конкретний сайт, навіть якщо ви видалили всі cookie-файли або взагалі заборонили їх. Позаяк сайт використовує елемент, вбудований у сам HTML5[112].

Цифровий відбиток із використанням Canvas знімається автоматично. Не треба нічого клікати, нікуди переходити. Достатньо просто відкрити веб-сторінку. На щастя, є плагіни для браузера, які можуть заблокувати цей процес: для Firefox існує CanvasBlocker[113], а для Google Chrome — CanvasDefender[114]. Tor навіть вбудував у свій браузер подібну технологію[115].

Що ж, ви встановили всі ці плагіни й дотримуєтеся всіх моїх рекомендацій. Ну, тепер ви вже в повній безпеці, так? Ще ні.

Такі фірми, як Drawbridge, Tapad і Crosswise зробили крок уперед на ниві інтернет-стеження. Вони стверджують, що можуть відстежувати ваші дії на кількох девайсах і знати про сайти, на які ви заходите лише з телефона чи планшета.

Почасти це є результатом самонавчання машин і їхньої цікавої логіки. Наприклад, якщо мобільний девайс і звичайний ПК часто заходять на один і той самий сайт з одного IP, то існує вірогідність, що вони належать одній людині. Припустимо, на роботі ви через телефон шукаєте щось конкретне з одягу в інтернет-магазині. Повернувшись ввечері додому, ви заходите на той сайт через ПК... і знаходите цей самий одяг у розділі «нещодавно проглянуто». І вишенька на торті: ви купуєте цей предмет одягу через ПК. Усе це лиш зміцнює зв'язок між вашим комп'ютером і телефоном, а що більше таких збігів, то більше ймовірності, що обидва девайси належать одній людині. Лише один Drawbridge стверджує, що 2015-го зв'язав 1,2 мільярда користувачів і 3,6 мільярда девайсів[116].

Звісно ж, Google теж таким займається. Як і Apple. Як і Microsoft. Телефони на Android вимагають користуватися Google-акаунтом. Девайси від Apple — ідентифікатором Apple ID. Байдуже, смартфон у вас чи ноутбук: будь-який веб-трафік з будь-якого девайса прив'язується до певного користувача. А останні операційні системи від Microsoft вимагають зареєструвати внутрішній акаунт для завантаження застосунків і зберігання фотографій та документів у «хмарі».

Різниця в тому, що Google, Apple і Microsoft дають змогу частково або повністю відключити збір даних і видалити всі зібрані дані. У Drawbridge, Crosswise і Tapad ці процеси трохи заплутані або взагалі відсутні.

Хоча проксі чи Tor — зручні способи приховати своє справжнє місцеперебування, вони ж можуть стати причиною цікавих проблем — ба навіть неприємних наслідків. Іноді онлайн-відстеження є виправданим, особливо в боротьбі з фінансовим шахрайством. Наприклад, за кілька днів до того, як Едвард Сноуден оприлюднив матеріали, він захотів створити сайт для підтримки прав людини в інтернеті. Однак у нього не виходило заплатити хосту за реєстрацію сайту кредиткою.

Тоді він все ще користувався справжнім ім'ям, справжнім імейлом і особистою кредиткою (поки не став міжнародним злочинцем). Але Сноуден користувався і Tor-браузером, який іноді видає кредитним компаніям попередження про шахрайство, коли ті хочуть перевірити вашу особу, а частина наданої вами інформації не відповідає тому, що вони бачать. Якщо, приміром, у вашому акаунті сказано, що ви живете в Нью-Йорку, то чому ваш вихідний вузол Tor запевняє, що зараз ви в Німеччині? Така невідповідність геолокації часто сигналізує про спробу шахрайства і запускає додаткову перевірку. Ясна річ, кредитні компанії відстежують нас в інтернеті. Вони знають усі наші покупки. Вони знають, на що ми підписані. Вони знають, коли ми залишаємо країну. І вони знають, коли ми робимо інтернет-покупку з нового девайса.

За словами Майка Лі з EFF, коли Сноуден обговорював урядові секрети з Лорою Пойтрас і репортером The Guardian Ґленном Ґринвальдом у готельному номері в Гонконзі, у той же час він переписувався з техпідтримкою DreamHost — інтернет-провайдера з Лос-Анджелеса. Мабуть, Сноуден запевнив DreamHost, що перебуває за кордоном і не довіряє місцевим інтернет-компаніям, тому й користується Tor-браузером. Урешті-решт, DreamHost провів платіж через Tor[117].

Один зі способів уникнути цієї проблеми з Tor — налаштувати файл конфігурації torrc на використання вихідних вузлів у власній країні. Цього кредитним компаніям має вистачити. З іншого боку, постійне використання одних і тих самих вихідних вузлів може з часом вас викрити. Дехто припускає, що урядові установи контролюють певні вихідні вузли, тож змінювати їх час від часу не завадило б.

Ще один спосіб анонімної оплати — віртуальна валюта біткоїн. Як і більшість валют, його курс коливається залежно від довіри людей.

Bitcoin — це алгоритм, за допомогою якого люди створюють (або, як кажуть профі, майнять) власну валюту. Але якби все було так легко, цим би займалися всі, кому не ліньки. Обчислювальний процес є досить інтенсивним, а на створення одного біткоїну йде купа часу. До того ж кількість біткоїнів завжди обмежена, і це, як і довіра споживачів, теж впливає на його вартість.

Кожен біткоїн має криптографічний підпис, який свідчить про оригінальність та унікальність валюти. Транзакцію з таким криптографічним підписом можна простежити до самого біткоїна, але те, як ви дістали валюту, можна приховати (приміром, створити надійну анонімну електронну пошту і зареєструвати на неї біткоїн-гаманець через мережу Tor).

Біткоїни можна придбати відкрито чи анонімно — через інтернет за допомогою передплачених подарункових карток або через біткоїн-банкомат, за яким не стежать камери. Існує купа нюансів спостереження, які потенційно можуть розкрити вашу справжню особу, тож під час вибору способу купівлі варто враховувати всі ризики. Опісля біткоїни можна покласти в так званий біткоїн-міксер. Міксер бере трохи біткоїн-валюти в мене, трохи у вас, трохи в інших власників — абсолютно випадкових людей — і змішує все це разом. У вас на рахунку залишається повна вартість біткоїнів мінус невелика плата за те, що міксер перемішує валюту й видає вам зовсім інший криптографічний підпис. Це робить систему дещо анонімною.

Приміром, ви змогли придбати біткоїни. Де їх тепер зберігати? Позаяк біткоїн-банків не існує, а валюта не є фізичною, вам потрібен анонімно зареєстрований біткоїн-гаманець. Далі в книжці ви знайдете детальну інструкцію того, як це зробити.

Припустимо, ви купили й поклали біткоїн у гаманець. Як тепер ним скористатися? Біржі допомагають інвестувати в біткоїн і обмінювати його на інші валюти, як-от долари США, чи купувати товари на сайтах, як-от Amazon. Скажімо, у вас є один біткоїн вартістю 618 доларів. Якщо вам потрібно придбати товар за 80 доларів, то після транзакції певна частина вартості залишиться у вас на рахунку. Зніметься лише частина біткоїна відповідно до курсу обміну валют.

Транзакції підтверджуються в публічному реєстрі — блокчейні — та ідентифікуються за IP-адресою. Але, як ми вже переконалися, IP можна змінити чи підробити. І хоча продавці потихеньку приймають біткоїни, плата за транзакцію, яку зазвичай виплачує продавець, тепер лежить на покупцеві. Крім того, на відміну від кредиток, біткоїни не можна повернути, а платіж не можна скасувати.

Біткоїнів можна мати на рахунку стільки ж, скільки і звичайної валюти. Але, незважаючи на абсолютний успіх (брати Вінклвосс, які судилися з Марком Цукерберґом за ідею Facebook, є основними інвесторами в біткоїн), були в історії валюти й масштабні невдачі. У 2004 році токійська біткоїн-біржа Mt.Gox оголосила про банкрутство після заяви про те, що її біткоїни вкрали. Були й інші повідомлення про крадіжку на біткоїн-біржах, але їхні рахунки, на відміну від більшості банківських рахунків у США, не застраховані.

Хоча й спроби введення віртуальної валюти робилися ще давно, саме біткоїн став стандартом анонімної інтернет-валюти. Так, система поки що не ідеальна, але є чудовим варіантом для прихильників конфіденційності.

Що ж, ви приховали IP-адресу через Tor, зашифрували імейли й повідомлення через PGP і Signal. Уже почуваєтеся невидимкою? Зачекайте, я ще не розповів про апаратне забезпечення, яке може як видати вас з головою, так і сховати в інтернеті.

---

93 https://timlibert.me/pdf/Libert-2015-Health_Privacy_on_Web.pdf.

94 Цей неофіційний тест під час написання книжки показав, що плагін Ghostery в браузері Chrome у відповідь на пошук інформації про грибок стопи заблокував 21 запит від партнерів Mayo Clinic і 20 від партнерів WebMD.

95 Щоб отримати детальнішу інформацію про те, які дані витікають із вашого браузера, зайдіть на: http://browserspy.dk/.

96 https://noscript.net/.

97 https://chrome.google.com/webstore/detail/scriptblock/hcdjknjpbnhdoabbngpmfekaecnpajba?hl=en.

98 https://www.ghostery.com.

99 Snowboarder (з англ.) — сноубордист; silverfox (з англ.) — срібна лисиця. — *Прим.пер.*

100 http://www.wired.com/2014/10/verizons-perma-cookie/.

101 http://www.pcworld.com/article/2848026/att-kills-the-permacookie-stops-tracking-customers-internet-usage-for-now.html.

102 http://www.verizonwireless.com/support/unique-identifier-header-faqs/.

103 http://www.brighthub.com/computing/smb-security/articles/59530.aspx.

104 http://en.wikipedia.org/wiki/Samy_Kamkar

105 https://github.com/samyk/evercookie.

106 http://venturebeat.com/2015/07/14/consumers-want-privacy-yet-demand-personalization/.

107 http://www.businessinsider.com/facebook-will-not-honor-do-not-track-2014-6.

108 https://chrome.google.com/webstore/detail/disconnect-facebook-pixel/nnkndeagapifodhlebifbgbonbfmlnfm/.

109 https://facebook.adblockplus.me/.

110 https://zephoria.com/top-15-valuable-facebook-statistics/.

111 http://www.latimes.com/business/la-fi-lazarus-20150417-column.html.

112 https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block#.

113 https://addons.mozilla.org/en-us/firefox/addon/canvasblocker/.

114 https://chrome.google.com/webstore/detail/canvas-defender/obdbgnebcljmgkoljcdddaopadkifnpm/.

115 https://trac.torproject.org/projects/tor/ticket/6253.

116 https://www.technologyreview.com/s/538731/how-ads-follow-you-from-phone-to-desktop-to-tablet/.

117 https://theintercept.com/2014/10/28/smuggling-snowden-secrets/.

Розділ 7
Грабіж серед білого дня

Кошмар почався в інтернеті, а завершився в «реалі», коли агенти ФБР узяли штурмом будинок у передмісті Блейна, штат Міннесота. Агенти мали лише IP-адресу, пов'язану із завантаженням дитячої порнографії та навіть загрозою вбивства віце-президента Джо Байдена. Звернувшись до інтернет-провайдера, який обслуговував цей IP, ФБР отримало фізичну адресу користувача. Таке можна було успішно провернути в ті дні, коли всі були під'єднані до модемів чи маршрутизаторів. Тоді будь-яку IP-адресу можна було фізично простежити до ПК.

Але сьогодні більшість людей удома має Wi-Fi. Завдяки бездротовому зв'язку можна вільно переміщатися з мобільним девайсом по будинку і не втрачати доступу до інтернету. Але якщо не захистити мережу, сусіди теж отримають доступ до сигналу. Ось чому федеральні агенти з Міннесоти увірвалися не в той будинок. Потрібен був сусідній.

У 2010 році Баррі Вінсент Ардольф визнав себе винним у хакерстві, крадіжці особистих даних, зберіганні дитячої порнографії та погрозах віце-президентові Байдену. Згідно із судовим протоколом, тяганина між Ардольфом і його сусідом почалася, коли сусід (який насправді був адвокатом; ім'я не називають) подав у поліцію заяву, що Ардольф нібито «непристойно торкнувся й поцілував малюка адвоката в губи»[118].

Після чого Ардольф скористався IP-адресою Wi-Fi роутера сусіда і зареєстрував облікові записи в Yahoo та MySpace на ім'я жертви. Саме через ці фальшиві акаунти Ардольф намагався очорнити адвоката й виставити його злочинцем.

Тепер інтернет-провайдери часто вбудовують у домашні роутери додаткові можливості[119]. Деякі з них, як от Comcast, мають додаткову відкриту Wi-Fi мережу для гостей, над якою у вас обмежений контроль. Наприклад, ви можете лише увімкнути її та вимкнути. Про це варто знати. Хтось може припаркувати фургон біля вашого будинку і під'єднатися до вашої безкоштовної бездротової мережі. Платити за це вам не доведеться, але якщо другим сигналом користуються надто інтенсивно, можна помітити невелике зниження швидкості основного сигналу. Ви можете відімкнути Xfinity Home Hotspot Comcast, якщо впевнені, що вашим гостям ніколи не знадобиться безкоштовний доступ до вашого домашнього інтернету[120].

Хоча вбудовані функції й полегшують знайомство з новими технологіями, часто такі широкосмугові роутери слабко захищені і можуть спричинити проблеми. Приміром, незахищена бездротова мережа може забезпечити цифрову точку входу у ваш будинок, як це трапилося з Ардольфом. Хоча

зловмисники в такий спосіб ваші файли навряд чи отримають, вони все одно можуть підкинути вам проблем.

Ардольф був далеко не комп'ютерним генієм. У суді він зізнався, що не розумів різниці між WEP-шифруванням, яким користувався сусід, і WPA-шифруванням, яке вважається набагато надійнішим. Він просто розлютився.

І це лиш одна-єдина причина, чому варто не полінуватися і подбати про безпеку власної домашньої бездротової мережі. Ви ніколи не знаєте, коли розгніваний сусід спробує «налаштувати» ваш Wi-Fi проти вас.

Але навіть якщо хтось скористається вашою бездротовою мережею з поганою метою, ви все одно відносно захищені. EFF повідомляє, що федеральні судді відхилили позови правовласників проти BitTorrent, бо відповідачі успішно ухилилися від звинувачень, заявивши, що хтось інший скачав фільми через їхні бездротові мережі[121]. У EFF кажуть, що IP-адреса не є особою, а отже, користувачі не можуть нести відповідальність за дії інших осіб, що користуються їхнім вай-фаєм[122].

Якщо ж комп'ютерна експертиза знімає обвинувачення з невинної людини, вай-фаєм якої скористалися зі злочинною метою — як це було з адвокатом із Міннесоти, — навіщо тоді всі ці складнощі?

Навіть якщо ви користуєтеся аналоговим модемом, що працює через телефонну лінію, чи кабельним ASM-роутером (які виробляють переважно Cisco та Belkin), проблем із ПЗ і конфігурацією все одно не уникнути.

По-перше, завантажте останню версію прошивки (ПЗ, установлене на апаратне забезпечення). Це можна зробити через екран конфігурації роутера (див. нижче) або пошукати оновлення для конкретної марки й моделі на сайті виробника. Робіть це якомога частіше. Найпростіший спосіб оновлювати прошивку роутера — щороку купувати нову. Це може коштувати дорого, але гарантує вам найновішу і найкращу прошивку. По-друге, поновіть параметри конфігурації роутера. Жодних налаштувань за замовчуванням.

Але почнемо з імені мережі. Хіба це важливо? Ще б пак. Ім'я мають абсолютно всі роутери — як маршрутизатор від вашого провайдера, так і з найближчого супермаркету. Усі бездротові маршрутизатори за замовчуванням транслюють те, що називається ідентифікатором SSID[123]. Зазвичай SSID складається з назви та моделі роутера, як-от «Linksys WRT54GL». Якщо ви продивитеся список доступних Wi-Fi мереж у вашому районі, то зрозумієте, що я маю на увазі.

Назва SSID за замовчуванням може приховати те, з якого будинку чи квартири йде сигнал, і водночас допомагає будь-якому перехожому дізнатися точну марку й модель вашого роутера. Чим це небезпечно? Ця людина може знати вразливість цієї моделі і скористатися нею.

То як же змінити ім'я роутера й оновити прошивку?

Дістати доступ до маршрутизатора легко — через браузер. Якщо у вас нема інструкцій до власного роутера, в інтернеті знайдеться безліч сайтів із поясненнями, що саме ввести в адресний рядок, щоб під'єднатися безпосередньо

до домашнього роутера[124]. Ввівши локальну URL-адресу (не забувайте, вам потрібна саме адреса роутера, а не інтернет), ви побачите екран входу. Який вводити логін і пароль?

Виявляється, в інтернеті є список логінів за замовчуванням[125]. Наприклад, у Linksys поле з логіном порожнє, а пароль — «admin». Думаю, ви прекрасно розумієте, що варто негайно змінити пароль за замовчуванням, щойно відкриєте екран конфігурації маршрутизатора. Раджу дотримуватися порад щодо створення надійних та унікальних паролів, про які ми говорили в розділі 1, чи скористатися менеджером паролів.

Не забудьте зберегти пароль у менеджері паролів або десь записати, бо, ймовірно, знадобиться він вам не так часто. Якщо раптом забули пароль (серйозно, не думаю, що ви кожного дня заходитиме на сторінку конфігурації роутера), не турбуйтеся. На самому роутері є кнопка скидання, яка відновить налаштування за замовчуванням. Але після апаратного скидання вам доведеться повторно ввести всі параметри конфігурації, про які йтиметься нижче. Тож краще запишіть налаштування маршрутизатора або зробіть скріншоти і роздрукуйте їх. Вони стануть у пригоді, якщо буде потрібно переналаштувати роутер.

Пропоную вам змінити «Linksys WRT54GL» на щось безневинне — приміром, «HP Inkjet» — щоб незнайомці не здогадалися, з якого будинку йде сигнал Wi-Fi. Я часто пишу щось загальне, як-от назву житлового комплексу чи навіть ім'я сусіда.

Також є спосіб повністю приховати SSID, тобто сторонні не побачать вашої мережі у своєму списку найближчих бездротових мереж.

Коли зайдете в основні налаштування конфігурації роутера, зверніть увагу на кілька деталей безпеки. Зазвичай вони не ввімкнені за замовчуванням. До того ж не все бездротове шифрування однакове і не всі роутери його підтримують.

Найпоширеніший стандарт бездротового шифрування WEP абсолютно марний. Навіть не розглядайте його як варіант. WEP ламають із року в рік. Тільки старі роутери і пристрої все ще пропонують його як застарілий варіант. Краще виберіть щось із нових, більш надійних стандартів шифрування, як-от WPA. Або навіть WPA2 — він ще більш захищений.

Якщо вмикаєте шифрування на маршрутизаторі, то девайси, що під'єднуються до нього, теж повинні відповідати налаштуванням шифрування. Більшість нових пристроїв автоматично розпізнає тип шифрування, але на старих моделях, як і раніше, доводиться вказувати рівень шифрування вручну. Завжди вибирайте максимальний рівень. Ступінь захисту вимірюється за найслабшою ланкою, тому переконайтеся, що максимальне шифрування прописано навіть на найстаріших девайсах.

Якщо вмикаєте WPA2, то, під'єднуючи до мережі ноутбук чи мобільний пристрій, доведеться також налаштувати їх на WPA2, хоча й деякі нові операційні системи розпізнають тип шифрування автоматично. Сучасні

операційні системи на телефонах і ПК виводять вам список усіх Wi-Fi мереж, доступних поблизу. Ваш SSID (який тепер називається «HP Inkjet») має з'явитися в списку ближче до верху. Значок замка навпроти доступних Wi-Fi мереж (які зазвичай вишиковуються в список за силою сигналу) вказує, які мережі вимагають пароль (у вас обов'язково повинен бути замок).

У списку доступних під'єднань виберіть ваш ідентифікатор SSID. Вам запропонують увести пароль — раджу зробити його не менш як на п'ятнадцять символів. Або скористатися менеджером паролів для складнішого ланцюжка. Щоб під'єднатися до захищеного паролем Wi-Fi, доведеться ввести цей пароль принаймні один раз на всіх ваших девайсах. Тож менеджер паролів незавжди найкращий, особливо коли треба запам'ятати пароль і ввести його самостійно. Усі пристрої, зокрема «розумний» холодильник і цифрове телебачення, прийматимуть той пароль, який ви ввели під час налаштування шифрування роутера. Увести його доведеться на кожному девайсі, який має доступ до домашнього або робочого Wi-Fi, але зробити це доведеться лиш раз. Звісно ж, якщо ви не змінюватимете пароль мережі чи сам пристрій.

Можна піти ще далі й дозволити доступ до Wi-Fi мережі лише пристроям, які ви самі вкажете. Це називається «білий» список. Так ви відкриєте доступ конкретним девайсам (білий список) і забороните його всім іншим (чорний список). Для цього потрібно ввести адресу управління доступом до середовища вашого пристрою, або MAC-адресу. Тож якщо раптом придбаєте новий телефон, доведеться додавати його до списку MAC-адрес маршрутизатора, перш ніж під'єднатися до мережі[126]. Ця адреса є унікальною для кожного пристрою: перші три набори символів (байт) — це код виробника, а останні три є унікальним кодом продукту. Маршрутизатор відхилить будь-який пристрій, MAC-адреса якого відсутня в списку. Проте хакерський інструмент під назвою Aircrack-ng може дістати й розшифрувати MAC-адресу пристрою під'єднаного користувача, після чого зловмисник підробить її і під'єднається до роутера. Обійти фільтрацію MAC-адрес не так уже й важко.

Дізнатися MAC-адресу вашого девайса теж відносно легко. Якщо у вас Windows, натисніть «Пуск» або «Пошук», уведіть «CMD», клікніть на «Командний рядок» і надрукуйте «IPCONFIG». Комп'ютер видасть вам довгий список даних, серед яких буде і MAC-адреса. Вона складається з дванадцяти шістнадцяткових символів, де кожних два символи розділені двокрапкою. З продуктами Apple все ще простіше. Натисніть значок Apple, виберіть «Системні налаштування», далі — «Мережа». Потім натисніть на мережевий пристрій на лівій панелі і перейдіть у Додатково> Апаратура, де і побачите MAC-адресу. На деяких старих продуктах Apple процедура така: значок Apple>Системні налаштування>Мережі>Ethernet. На айфоні MAC-адресу можна знайти за ланцюжком Налаштування>Загальні>Про цей пристрій і вибрати «Адреса Wi-Fi». Якщо телефон на базі Android, відкрийте Налаштування>Про телефон>Стан

і знайдіть рядок «MAC-адреса Wi-Fi». Шлях може змінюватися залежно від пристрою й моделі.

Тепер, коли маєте двадцятизначні MAC-адреси всіх своїх девасів, дозвольте роутерові надавати доступ лише цим адресам і блокувати все інше. Але тут є кілька недоліків. Якщо ваш гість захоче під'єднатися до домашньої мережі, доведеться вирішувати, дати йому один із власних пристроїв із паролем чи просто відключити фільтрацію MAC-адрес через екран конфігурації маршрутизатора. Крім того, іноді може знадобитися змінити MAC-адресу пристрою (див. розділ 8), і тоді ви вже не зможете під'єднатися до мережі Wi-Fi з обмеженим доступом вдома чи на роботі. На щастя, перезавантаження пристрою в більшості випадків відновлює вихідну MAC-адресу.

Щоб зробити під'єднання будь-якого нового пристрою до домашнього роутера елементарним, організація Wi-Fi Alliance — група компаній, що мають на меті популяризувати Wi-Fi технології, — розробила захищене налаштування Wi-Fi (WPS). WPS рекламують як простий — дуже простий — спосіб надійно налаштувати мобільний пристрій вдома або на роботі. Але на практиці до надійності тут далеко.

Зазвичай WPS має вигляд звичайної кнопки на маршрутизаторі. Можна також натрапити на технологію у формі PIN-коду і «зв'язку на невеликих відстанях» (NFC). Простіше кажучи, ви активуєте функцію WPS, і вона з'єднує роутер із будь-якими новими пристроями, які є у вас вдома чи на роботі, автоматично синхронізуючи їх для роботи з мережею Wi-Fi.

Звучить круто. Але якщо роутер розташований у «доступному» місці — скажімо, у вітальні, — будь-хто може натиснути кнопку WPS й увійти у вашу домашню мережу.

А можна обійтися і без особистої присутності. Зловмисник може просто підібрати PIN-код від вашого WPS. Імовірно, це затягнеться на кілька годин, але спосіб усе ще дієвий. Єдиний спосіб від нього захиститися — негайно вимкнути функцію WPS на маршрутизаторі.

Ще один спосіб атаки на WPS, відомий як Pixie Dust. Атака — офлайнова і працює лише з деякими марками чипів, як-от Ralink, Realtek і Broadcom, допомагає хакерам отримати паролі від бездротових роутерів. Інструмент — дуже простий і може дістати доступ до пристрою за лічені секунди чи години, залежно від складності вибраного чи згенерованого PIN-коду до WPS[127]. Наприклад, одна з таких програм — Reaver — може зламати маршрутизатор із підтримкою WPS за кілька годин.

Загалом, раджу вимикати WPS. Увести пароль від мережі на кожному новому мобільному пристрої не так уже й важко.

Що ж, за допомогою шифрування і надійних паролів ви захистили свою Wi-Fi мережу від втручання. Тепер ніхто не зможе потрапити у вашу домашню мережу? Не зовсім.

Коли десятикласника Блейка Роббінса викликали в кабінет директора в приміській школі у Філадельфії, він і гадки не мав, що його покарають за «неналежну поведінку»... вдома. Шкільний округ Нижній Меріон у передмісті Філадельфії видав усім старшокласникам, включно з Роббінсом, нові макбуки для навчання. Однак шкільний округ забув повідомити учням, що програмне забезпечення, призначене для відновлення ноутбука в разі його втрати, могло ще й шпигувати за 2300 учнями, поки вони перебували в полі зору веб-камери.

У чому ж звинуватили Роббінса? Зловживання таблетками. Сім'я Роббінсів через свого адвоката довела, що хлопець просто їв цукерки-драже, сидячи за домашньою роботою.

Чому навколо цього піднявся такий галас?

Шкільний округ стверджує, що активував протикрадіжне ПЗ лише після того, як один із ноутбуків украли. Протикрадіжна програма працює так: якщо хтось з учнів повідомляє, що його ноутбук вкрали, школа може увійти на сайт ПЗ і отримати зображення з веб-камери вкраденого ноутбука і звук із мікрофона. Після чого адміністратор школи може стежити за ноутбуком і за потреби робити знімки. У такий спосіб девайс можна знайти й повернути, а винного ідентифікувати і покарати. Проте в цьому випадку були підозри, що керівництво школи користується функцією для спостереження за учнями вдома.

Веб-камера на шкільному макбуці Роббінса зробила сотні фотографій — на деяких із них хлопець спав у своєму ліжку. Але це ще квіточки: згідно зі свідченнями в суді, у школі знайшли тисячі світлин з іншими учнями, подеколи «частково роздягненими». Ніхто б і далі цього не помічав, якби Роббінс не отримав догану за те, що нібито скоїв удома.

Роббінс разом із колишнім учнем Джалілом Хасаном — у школи було приблизно п'ятсот знімків його самого і чотириста знімків екрана комп'ютера, де видно всю його активність в інтернеті і сайти, які він відвідав, — подали в суд на шкільний округ. Роббінс отримав 175 тисяч доларів, Хасан — 10 тисяч[128]. Також округ заплатив майже півмільйона доларів на покриття юридичних витрат хлопців, а загалом виплатив через свого страховика приблизно 1,4 мільйона доларів.

Шкідливе ПЗ із легкістю може активувати веб-камеру й мікрофон на ПК без вашого відома. Те саме і з мобільними пристроями. У цьому випадку це було зроблено навмисно, але зазвичай все по-іншому. Елементарне рішення — заклеїти веб-камеру непрозорою стрічкою, поки нею не користуєтеся.

Восени 2014 року Софі Кертіс, репортер лондонської газети Telegraph, отримала по електронній пошті запит на контакт у лінкдін, який начебто надійшов від колеги з газети. Такі імейли Софі отримувала ледь не щодня, а професійна етика не дозволяла відхилити запит від колеги, тож вона його прийняла. За кілька тижнів Софі отримала іншого електронного листа — цього разу від організації анонімних інформаторів, яка мала от-от розсекретити документи. Як журналістку, яка займалася групами на зразок Anonymous і WikiLeaks й

отримувала такі листи раніше, тема її зацікавила. До імейлу був прикріплений начебто стандартний файл, тож Софі його відкрила.

І відразу зрозуміла, що щось не так. Windows Defender — програма безпеки, яка вбудована в саму систему Windows, — почала видавати попередження за попередженням. Вони ледь не заполонили весь робочий стіл.

Клікнувши на прикріплений файл, що здавався досить безневинним, Кертіс припустилася поширеної помилки. Запевнивши журналістку, що в документі міститься цікава інформація, зловмисник змусив її завантажити файл, який розпакувався в кілька інших файлів, так хакер узяв її комп'ютер під повний контроль. Шкідливе ПЗ навіть сфотографувало її на власну веб-камеру. На світлині жінка намагається зрозуміти, як її могли так обдурити, з виразом повного розчарування на обличчі.

Насправді Кертіс прекрасно знала, хто її зламав. За кілька місяців до того вона як експеримент найняла тестувальника на проникнення. Так, когось на зразок мене. Приватні особи і компанії наймають професійних хакерів, які проникають у їхню мережу, щоб виявити слабкі місця. Щодо Кертіс процес розтягнувся на кілька місяців.

Особисто я завжди починаю роботу зі спроб знайти якомога більше інформації про клієнта. Певний час я вивчаю його життя і звички. Відстежую пости у твітері, на фейсбуці і так, навіть у лінкдін. Те саме зробив і тестувальник Софі Кертіс. Серед усіх її вхідних повідомлень заховався один особливий імейл — перший, відправлений тестувальником. Він знав, що вона працює журналісткою і досить відкрита до спілкування з невідомими особами. Пізніше Кертіс написала, що тоді отримала повідомлення від людини, яка начебто хотіла дати інтерв'ю для майбутньої статті, але відсутність контексту змусила його проігнорувати. Але Софі була вражена тим, яке дослідження провів тестувальник і його колеги: «Через твітер вони дістати мій робочий імейл, інформацію про місця, де я часто буваю, та нашу регулярну вечірню зустріч із журналістами. По задньому плану однієї з фотографій у твітері вони змогли дізнатися, яким мобільним телефоном я користувалася і які цигарки курив мій наречений (це була стара фотографія), а також те, що йому подобаються велосипеди»[129]. Будь-яка з цих деталей могла б послугувати основою для наступного імейлу.

А ще на конференції DEF CON 2016 анонсували новий інструмент на основі штучного інтелекту, який аналізуватиме твіти жертви й генеруватиме фішинговий імейл, спираючись на її особисті інтереси[130]. Тому будьте обережні під час переходу на посилання у твітері.

Зазвичай уся інформація — у дрібницях: якийсь своєрідний коментар, якась унікальна штука на фото десь за вами на полиці, якась фірмова футболка з табору — усе це видає важливу особисту інформацію, якою ви ніколи не поділилися б із будь-ким. Ці дрібниці здаються нам безвинними, але що більше

деталей зловмисник про вас дістане, то більше в нього шансів змусити вас відкрити файл, прикріплений до листа, і прибрати до рук ваш онлайн-світ.

Кертіс попереджає, що команда тестувальників на цьому зупинилася, але якби вони були справжніми злочинцями, такі ігри могли б тривати ще довго. Хакери дістали б доступ до її акаунтів у соцмережах, робочої мережі в Telegraph, навіть фінансових рахунків. І, найімовірніше, провернули б вони це так, що Кертіс ніколи про це і не дізналася б: більшість атак не відразу запускають Windows Defender чи антивірус. Деякі зловмисники можуть місяцями чи навіть роками контролювати ваш комп'ютер, перш ніж ви здогадаєтеся, що вас зламали. І така історія не лише з комп'ютерами: імейл-атаку можна провести і на хакнутому айфоні чи смартфоні на Android.

Хоча Google та інші імейл-сервіси сканують ваші повідомлення щодо шкідливих програм і поширення порнографії (а також для збору рекламних даних), щодо шахрайства їх перевіряють незавжди. Як і конфіденційність — стандарт, який у кожного свій, — шахрайство теж важко оцінити. Ми незавжди розпізнаємо його, навіть якщо воно лежить просто на поверхні.

У Кертіс у підробленому імейлі із запитом на лінкдіні містився крихітний піксель — малесенька крапка зображення, невидима для очей. На зразок тої, що використовують сайти для відстеження ваших дій в інтернеті. І ця крихітна крапка посилає сигнал дистанційному серверу відстеження (який може бути в будь-якій точці світу) про те, коли ви відкрили електронний лист, як довго він залишався відкритим і на якому пристрої його відкрили. А ще повідомляє, що ви зробили з імейлом: зберегли, переслали чи видалили. Крім того, якби атака тестувальників на проникнення була справжньою, зловмисник міг би включити в лист посилання на підроблену сторінку лінкдін. Ця сторінка була б як дві краплі води схожа на справжню, хіба що зберігалася б на іншому сервері десь за кордоном.

Для рекламодавця такий баг — шанс зібрати інформацію про потенційного клієнта (і в перспективі завести на нього профіль). Для зловмисника ж — можливість дістати технічні відомості, потрібні для розроблення наступної атаки, зокрема й способу проникнути в комп'ютер. Якщо ви використовуєте стару версію браузера, то такі баги стають вірогіднішими.

Так другий електронний лист Кертіс від тестувальників містив додаток — стиснутий документ, запрограмований скористатися вразливістю ПЗ, яке відкриває цей формат файлу (наприклад, Adobe Acrobat). Коли йдеться про шкідливі програми, більшість людей уявляє собі комп'ютерні віруси початку 2000-х, коли один заражений імейл розсилав інші заражені імейли всім у списку контактів. Зараз такі масові атаки втрачають популярність, почасти через зміни в програмному забезпеченні електронної пошти. Сьогодні найнебезпечніші віруси діють набагато тонше і часто націлені на конкретну особу. Як це трапилося із Софі Кертіс. Тестувальники на проникнення скористалися

особливою формою фішингу — так званим «цільовим фішингом», розрахованим лише на певну людину.

Фішинг вважається шахрайством з метою отримання конфіденційної інформації, як-от імен користувачів, паролів, даних кредитної картки чи банківського рахунку. Так обдурили не одного фінансового директора, змусивши перевести величезні суми, бо «генеральний директор» схвалив транзакцію. Зазвичай фішинговий імейл чи повідомлення вимагає від вас щось зробити, наприклад, клікнути на посилання чи відкрити прикріплений файл. У випадку з Кертіс метою було показати, як легко завантажити у ваш комп'ютер вірусну програму.

Однією з найвідоміших фішингових схем стала операція «Аврора», у рамках якої фішинговий лист надіслали китайським працівникам Google.

Зловмисники націлилися заразити комп'ютери в Китаї, щоб дістати доступ до внутрішньої мережі в штаб-квартирі Google в Маунтін-В'ю, штат Каліфорнія. Урешті-решт, хакери опинилися небезпечно близько до вихідного коду пошуковика Google. І таке трапилося не лише з Google. Компанії на зразок Adobe теж повідомили про подібні вторгнення. У результаті Google ненадовго припинив свою діяльність у Китаї[131].

Запити з лінкдін і фейсбука присипляють нашу пильність. Ми довіряємо цим сайтам, тому іноді автоматично починаємо довіряти й імейлам від них. Проте підробити таке повідомлення може будь-хто. У реальному житті нам не так складно розпізнати, коли хтось носить фальшиві вуса, перуку чи говорить фальшивим голосом. У нас закладені еволюційні інстинкти, що віками допомагали виявляти обман, навіть про це не замислюючись. Однак в інтернеті ці інстинкти безсилі. Принаймні в більшості з нас. Софі Кертіс — журналістка. Її робота — бути допитливою і скептичною, іти за зачіпками й перевіряти факти. Вона могла б легко переглянути список співробітників Telegraph і дізнатися, що такої людини в штаті не існує, а імейл, імовірно, — підробка. Але вона цього не зробила. Як і не зробила б більшість із нас.

Фішингом зловмисник усі ваші дані не дістане, але крихти таки виманить — це й буде приманкою. Наприклад, фішер може надіслати імейл із чотирма останніми цифрами вашої кредитки, щоб підкупити довіру й витягнути з вас ще більше інформації. Іноді вам можуть надіслати неправильні чотири цифри і попрохати виправити. Не робіть цього. Узагалі ніяк не реагуйте на фішера. Не відповідайте на жодні запити щодо особистої інформації, навіть якщо вони здаються надійними. Краще зв'яжіться з особою чи компанією, що нібито подала запит, окремим імейлом (якщо у вас є імейл-адреса) або через SMS (якщо у вас є номер мобільного телефону).

Найнебезпечніша фішинг-атака — та, яка вашими ж руками дає зловмисникові повний контроль над вашим комп'ютером. Саме цим я й займаюся в соціальній інженерії. Збір особистих даних — теж популярна лінія

атаки, під час якої виманюють логін і пароль користувача, але реальна небезпека цільового фішингу — у повному доступі до комп'ютера та мережі жертви.

* * *

А що як ви таки потрапили на вудочку і в результаті втратили всі дані — особисті фотографії, конфіденційні документи — із зараженого ПК чи телефона? Таке трапилося з мамою письменниці Аліни Сімон. Авторка написала в New York Times статтю про те, як важко було боротися її непідкованій у технологіях матері з досвідченим ворогом, що скористався так званою програмою-вимагачем[132].

У 2014 році інтернет накрила хвиля шкідливих програм-шантажистів, націлених як на корпорації, так і окремих людей. Приміром, вірус Cryptowall шифрує весь жорсткий диск і блокує всі файли, поки ви не заплатите зловмисникові за ключ для розблокування. Якщо у вас нема повної резервної копії, весь вміст ПК чи мобільного пристрою буде недоступний, поки ви не заплатите викупу.

Не хочете платити? На екран монітора виводять повідомлення від вимагача, де йдеться про те, що ключ для розблокування файлів буде знищений через такий-то час. Часто додають і годинник зворотного відліку. Якщо ви не встигаєте заплатити, термін іноді продовжують, але з кожним разом ціна збільшується.

Як уберегтися від цього? Зазвичай не варто натискати на прикріплені до імейлів файли (якщо відкриваєте їх не через Google Quick View чи Google Docs). Але є й інші способи заразити вас Cryptowall: приміром, банерна реклама на сайтах. Навіть звичайний перегляд сторінки із зараженим рекламним банером може заразити ваш ПК. Ось де дійсно знадобиться плагін для видалення реклами на зразок Adblock Plus.

Протягом перших шести місяців 2015 року Центр скарг на інтернет-злочинність ФБР (IC3) зареєстрував майже тисячу випадків зараження Cryptowall 3.0: втрати, за оцінками, становили приблизно 18 мільйонів доларів. Ця цифра охоплює виплачені викупи, витрати на IT-відділи й ремонтні майстерні, а також втрачений заробіток. У деяких випадках зашифровані файли містять особисту інформацію, таку як номери соціального страхування, що вже відносить атаку до витоку даних, а це — ще більше фінансових втрат.

Хоча ключ для розблокування файлів завжди можна придбати за фіксовану плату від п'ятисот до тисячі доларів, жертви зазвичай намагаються позбутися вірусу по-іншому. Наприклад, самостійно зламати шифрування. Це спробувала й мати Сімон. Коли вона нарешті зателефонувала доньці, часу вже майже не було.

Ледь не кожен, хто намагається зламати шифрування вимагачів, ловить облизня. Шифрування є дійсно сильним, а злам вимагає потужніших комп'ютерів і більше часу, ніж має більшість людей. Тож зазвичай жертви платять. За словами Сімон, управління шерифа округу Діксон, штат Теннессі, у

листопаді 2014 року заплатило викуп, щоб розблокувати 72 тисячі звітів з аутопсії, заяв свідків, фотографій з місця злочину й інших документів.

Часто хакери вимагають оплату в біткоїнах, що не під силу середньостатистичному громадянинові[133]. Як я вже згадував, біткоїн — децентралізована, однорангова віртуальна валюта, тож у більшості людей просто нема біткоїн-гаманців.

Від початку і до кінця статті Сімон нагадує читачам, що вони ніколи не повинні платити викуп, хоча сама врешті-решт так і вчинила. Зараз ФБР радить людям, чиї комп'ютери спіймали вірус, просто заплатити. Джозеф Бонаволонта, помічник керівника програми ФБР із кібер- і контррозвідки в Бостоні, зізнається: «Чесно кажучи, ми часто радимо людям просто заплатити викуп». За його словами, навіть ФБР не може зламати надскладний шифр вимагачів. До того ж люди платять настільки стабільно, що ціна в 500 доларів не змінюється вже багато років[134]. Пізніше ФБР виступило із заявою, що рішення заплатити викуп чи звернутися до фахівців з інформаційної безпеки цілком і повністю залежить від постраждалої сторони.

Мати Сімон, яка в житті не купувала жодних застосунків, зателефонувала дочці об одинадцятій вечора лиш для того, щоб з'ясувати, як платити віртуальною валютою. Сімон сказала, що таки знайшла біткоїн-банкомат на Мангеттені, з якого після збою програмного забезпечення й виклику в службу техпідтримки врешті-решт зробила платіж. На той час один біткоїн за курсом коштував трохи більше ніж 500 доларів.

Незалежно від того, вимагають хакери оплату в біткоїнах чи валюті, вони все одно залишаються інкогніто. Хоча технічно можна відстежити обидва способи оплати. Транзакції, проведені в інтернеті за участю біткоїнів, можна пов'язати з особою покупця, але це складно. Питання в тому, хто витрачатиме час і зусилля на боротьбу з такою злочинністю?

У наступному розділі я розповім, що може статися, якщо під'єднатися до інтернету через громадський Wi-Fi. З погляду конфіденційності, анонімність публічних Wi-Fi мереж — приваблива, але перестрахуватися однак доведеться.

118 http://www.computerworld.com/article/2511814/security0/man-used-neighbor-s-wi-fi-to-threaten-vice-president-biden.html.

119 http://www.computerworld.com/article/2476444/mobile-security-comcast-xfinity-wifi-just-say-no.html.

120 http://customer.xfinity.com/help-and-support/internet/disable-xfinity-wifi-home-hotspot/.

121 BitTorrent є сервісом потокового відео, що поширює фільми, деякі з них викладають не власники авторських прав.

122 http://blog.privatewifi.com/why-six-strikes-could-be-a-nightmare-for-your-internet-privacy/.

123 Також існує базовий набір обслуговування (BSS), який забезпечує основу стандарту 802.11 WLAN (бездротової локальної мережевої зони). Кожен BSS або ESS (розширений набір обслуговування) ідентифікується SSID.

124 http://www.techspot.com/guides/287-default-router-ip-addresses/.

125 http://www.routeripaddress.com/.

126 MAC-адреси авторизованих пристроїв легко виявити через тест на проникнення Wireshark.

127 https://www.pwnieexpress.com/blog/wps-cracking-with-reaver.

128 http://www.wired.com/2010/10/webcam-spy-settlement/.

129 http://www.telegraph.co.uk/technology/internet-security/11153381/How-hackers-took-over-my-computer.html.

130 https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter.pdf.

131 http://www.wired.com/2010/01/operation-aurora/.

132 http://www.nytimes.com/2015/01/04/opinion/sunday/how-my-mom-got-hacked.html.

133 http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/.

134 https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/.

Розділ 8

Віру на максимум, довіру на мінімум

Коли телефони лише почали з'являтися в домівках, їх під'єднували дротами й часто ставили на видне місце в затишну нішу. Друга лінія взагалі вважалася ознакою статусу. У гонитві за конфіденційністю на вулицях паралельно виростали громадські телефонні будки. Навіть таксофони у вестибюлях готелів були обладнані звуковими перегородками, щоб створити ілюзію приватності.

З появою мобільних телефонів це відчуття конфіденційності зникло без сліду. Для нас не рідкість іти вулицею й чути, як хтось голосно розповідає особисту драму чи — навіть гірше — диктує номер кредитки. І чують це всі, хто проходить повз. У вирі культури відкритості й обміну інформацією ми повинні ретельно фільтрувати те, що добровільно кажемо світу.

Бо іноді світ слухає.

Припустимо, вам подобається працювати, сидячи в кафе за рогом (сам іноді так роблю). У кафе є безкоштовний Wi-Fi. Це ж прекрасно, так? Не хочу вас засмучувати, але ні. Громадський Wi-Fi створювався не для інтернет-банків чи електронної комерції, а просто для зручності. Тому надійністю тут і не пахне. Але не всі прогалини в безпеці мають технічний характер. Дещо залежить і від вас[135].

Як зрозуміти, що ви під'єдналися до громадського Wi-Fi? Найімовірніше, вам не потрібно буде вводити пароль. Щоб продемонструвати, як важко сховатися в громадській Wi-Fi мережі, дослідники з антивірусної компанії F-Secure створили власну точку доступу, або хот-спот. Експеримент проводили на двох різних локаціях у центрі Лондона — у кафе та в громадському місці. Результати були приголомшливими.

У першому експерименті дослідники встановили свій хот-спот у кафе у жвавій частині міста. Коли відвідувачі отримували список доступних мереж, точка доступу від F-Secure здавалася ідеальним варіантом — сильний сигнал і вхід без пароля. Під час під'єднання клієнтам у браузері вилазив банер з умовами використання. Можливо, ви натрапляли на таке десь у місцевій кав'ярні. Зазвичай на банері прописано, що ви можете і не можете робити, користуючись мережею, але в цьому випадку за безкоштовний Wi-Fi експериментатори вимагали пожертвувати первістком чи домашнім улюбленцем. Шестеро людей погодилися з цими умовами[136].

Чесно кажучи, мало хто читає дрібний шрифт: усі ми просто хочемо якомога швидше опинитися в інтернеті. І все ж хоча б очима пробіжіться по умовах. Пізніше F-Secure заявили, що ні вони, ні їхні адвокати нічого не збираються робити з дітьми чи домашніми тваринами. Акцент тут стояв на тому, яку особисту інформацію дістають треті сторони через громадський Wi-Fi. Вдома ваша бездротова мережа зашифрована через WPA2 (див. розділ 7), тож якщо

хтось вирішить за вами шпигувати, ваших дій в інтернеті він не побачить. Але коли ви користуєтеся відкритим громадським Wi-Fi в кафе чи аеропорту, ваш трафік як на долоні.

Усе ще не розумієте, у чому проблема? Ви не знаєте, хто сидить по той бік з'єднання. У цьому випадку дослідницька група F-Secure знищила зібрані дані з етичних міркувань, але злочинці навряд чи вчинять так само. Вони продадуть вашу адресу електронної пошти компаніям, які розсилають спам із набридливою рекламою чи вірусом. Чи навіть вивудять деталі для фішингової атаки з незашифрованих імейлів.

У другому експерименті група встановила хот-спот на балконі в безпосередній близькості від Вестмінстерського палацу — штаб-квартири лейбористської і консервативної партій та Національного агентства по боротьбі зі злочинністю. За тридцять хвилин до експериментальної безкоштовної точки доступу під'єдналося десь 250 осіб. У більшості з них спрацювало автоматичне з'єднання на телефоні. Інакше кажучи, вони не вибирали мережу свідомо — за них усе вирішив девайс.

Зупинимося на цьому докладніше. Спочатку треба зрозуміти, як і чому ваші мобільні пристрої автоматично під'єднуються до мережі Wi-Fi.

І ПК, і мобільні пристрої завжди пам'ятають останні кілька мереж, до яких під'єднувалися, — як громадських, так і приватних. Це зручно. Так вам не треба постійно під'єднуватися до точки доступу Wi-Fi, приміром, удома чи на роботі. Однак на цьому зручності закінчуються. Буває так, що ви заходите в кафе, де ніколи раніше не були, а телефон уже приєднується до Wi-Fi. Чому це погано? Тому що під'єднатися ви можете зовсім не до мережі кафе.

Імовірно, мобільний пристрій знайшов точку доступу, яка відповідає профілю, що вже є в списку останніх під'єднань. Вас може насторожити той факт, що телефон під'єднався до Wi-Fi в абсолютно незнайомому місці... але що як ви надто захоплені якоюсь грою і не надасте цьому особливого значення?

Як працює автоматичне під'єднання Wi-Fi? У минулому розділі я вже згадував, що можна під'єднати собі провайдера Comcast й отримати безкоштовний, незашифрований публічний SSID під назвою Xfinity. Можливо, ваш пристрій колись уже під'єднувався до такої мережі[137]. Але звідки ви знаєте, що цю бездротову точку доступу під назвою Xfinity транслює не отой хлопець із ноутбуком за дальнім столиком?

Припустимо, ви під'єдналися до фальшивого Wi-Fi того дивного хлопця, а не до мережі кафе. Доступ до інтернету у вас все одно буде, тож гру на телефоні переривати не доведеться. Однак кожен пакет незашифрованих даних, які ви надсилаєте й отримуєте через інтернет, цей підозрілий тип бачитиме через підроблений хот-спот.

А якщо він потрудився налаштувати підроблений хот-спот, то, найімовірніше, перехоплює ваші пакети за допомогою якоїсь безкоштовної програми на зразок Wireshark. Нею я користуюся в роботі тестувальника на проникнення. Вона дає

змогу бачити всю мережеву активність, що відбувається навколо. Я бачу IP-адреси сайтів, до яких під'єднуються люди, і як довго вони сидять на цих сайтах. Якщо з'єднання не зашифровано, то перехоплення трафіку є законним, позаяк він апріорі доступний громадськості. Наприклад, як IT-адміністратор я хотів би бачити активність у своїй мережі.

Можливо, підозрілий тип за дальнім столиком просто спостерігає за вами і не втручається в трафік. А може, якраз активно цим і займається. Що відкриває перед ним кілька можливостей.

Можливо, він перенаправляє ваше з'єднання на проксі-сервер, який вбудовує у бразуер кілоґґер на основі Javascript. Так, коли ви зайдете на Amazon, усі натискання клавіш на сайті запишуться. Хто знає, може, хакеру заплатили за збір ваших облікових даних — логіну й пароля. Не забувайте, що на Amazon та інших торгових сайтах може міститися інформація про вашу кредитку.

Майже на кожному публічному вистуні я проводжу демонстрацію того, як можна перехопити логін і пароль жертви, щойно вона під'єднається до мого підробленого хот-споту. Позаяк я стаю посередником між жертвою і веб-сайтом, то легко можу вмонтувати в процес JavaScript, який висвітить користувачу на екрані фальшиве оновлення Adobe. Якщо жертва його встановить, комп'ютер заразиться вірусом. Суть у тому, щоб змусити вас установити підроблене оновлення й дістати повний контроль над комп'ютером.

Якщо хлопець за дальнім столиком втручається в трафік, це називається «атакою посередника». Зловмисник пересилає ваші пакети реальному сайту через проксі, а дорогою перехоплює дані чи щось у них додає.

Будь-хто може ненавмисно під'єднатися до фальшивої мережі Wi-Fi. Як від цього вберегтися? Зазвичай, ноутбук спершу виконує пошук найкращої бездротової мережі й під'єднується до неї лиш після вашого вибору. Але деякі ноутбуки і мобільні пристрої автоматично вирішують, до якої мережі під'єднатися. Це було зроблено з метою полегшити вам пересування з телефоном з одного місце в інше. Але, як я вже казав, зручна функція має недоліки.

За словами представників Apple, їхні продукти автоматично під'єднуються до мереж за пріоритетом у такому порядку:

1. Остання приватна мережа, до якої приєднався пристрій.
2. Інша приватна мережа.
3. Хот-спот.

На щастя, на ноутбуках можна видалити непотрібні Wi-Fi мережі: наприклад, мережу готелю, у якому ви зупинялися у відрядженні минулого літа. У Windows ви можете зняти прапорець з «Підключатися автоматично» поруч із назвою мережі перед під'єднанням. Або перейдіть у Панель управління>Центр управління мережами і загальним доступом і клацніть на ім'я мережі. Натисніть на «Властивості бездротової мережі» і зніміть прапорець з «Підключатися

автоматично, коли ця мережа в радіусі дії». На комп'ютерах Mac перейдіть у розділ «Системні налаштування», потім — «Мережа», виберіть Wi-Fi на панелі зліва і натисніть «Додатково». Потім зніміть прапорець із «Запам'ятати мережі, до яких підключався цей комп'ютер». Також можете вручну видалити мережі, вибравши ім'я й натиснувши мінус під ним.

Мобільні девайси на Android і iOS також мають функцію видалення непотрібних мереж Wi-Fi. На айфоні чи айподі перейдіть у «Налаштування», виберіть «Wi-Fi», клацніть значок «і» поруч з ім'ям мережі і виберіть «Забути цю мережу». На Android зайдіть у «Налаштування», виберіть «Wi-Fi», далі — стрілочку вбік і «Видалити мережу».

Якщо вам треба зробити щось конфіденційне далеко від дому, краще скористайтеся мобільним інтернетом замість бездротової мережі в аеропорту чи кафе. Під'єднатися до телефона з мобільним інтернетом з іншого пристрою можна через USB, блютуз або Wi-Fi. Якщо вибираєте Wi-Fi, переконайтеся, що у вас стоїть WPA2. Ще один варіант — придбати портативний хот-спот для подорожей. Зверніть увагу, що це не зробить вас непомітними, однак усе краще, ніж громадський Wi-Fi. Але якщо вам потрібно захистити дані від оператора мобільного зв'язку (скажімо, завантажити якусь особисту електронну таблицю), тоді раджу скористатися HTTPS Everywhere або протоколом SFTP. SFTP підтримує програма Transmit на Mac і застосунок Tunnelier на Windows.

Віртуальна приватна мережа (VPN) — такий собі безпечний «тунель», який поширює на ваш пристрій приватну мережу (з дому, офісу чи VPN-провайдера) поверх громадської мережі. Можете пошукати VPN-провайдерів у Google і придбати сервіс десь за 60 доларів на рік. Будь-яка мережа в кафе, аеропорту чи інших громадських місцях, яким не можна довіряти, є громадською. Але за допомогою VPN ви можете перетворити тунель із громадської мережі на приватну і безпечну. Усе, що ви робите всередині VPN, захищено шифруванням, позаяк весь ваш інтернет-трафік тепер захищений мережею поверх громадської мережі. Ось чому важливо користуватися послугами VPN-провайдера, якому можна довіряти: він може проглянути ваш трафік. Якщо ви скористаєтеся VPN у кафе, той підозрілий хлопець за дальнім столиком побачить лиш те, що ви під'єдналися до VPN-сервера. І все. Усі ваші дії і сайти, на які ви заходите, повністю приховані за куленепробивним шифруванням.

Однак ви все одно заходитимете в інтернет з IP-адреси, яку можна простежити до вас, — приміром, IP вдома чи на роботі. Тож VPN не гарантує повної невидимості. Не забувайте: ваш VPN-провайдер знає вашу вихідну IP-адресу. Про те, як зробити з'єднання повністю конфіденційним, поговоримо трохи пізніше (див. розділ 14).

Багато компаній під'єднують своїх працівників до VPN, щоб ті могли перейти з громадської мережі (тобто інтернету) до приватної внутрішньої корпоративної мережі. А як щодо простих смертних?

Є багато платних VPN-сервісів. Але як дізнатися, чи можна їм довіряти? В основі VPN лежить технологія IPsec, яка автоматично охоплює PFS (пряму секретність; див. розділ 3). Але не всі сервіси (навіть корпоративні) правильно її налаштовують. Приміром, OpenVPN — технологія з відкритим вихідним кодом, яка охоплює PFS. Здавалося б, логічно, що коли продукт заявляє, що використовує OpenVPN, він автоматично використовує й PFS. На практиці так буває незавжди. Інколи продукт може й не налаштувати OpenVPN належно. Переконайтеся, що сервіс точно пропонує вам PFS.

Одним із недоліків є те, що VPN коштують дорожче, ніж проксі[138]. Також платними VPN одночасно користується купа людей, тож вони можуть працювати повільно чи навіть не давати вам доступу до сервісу, бо вільних серверів просто немає. У такому випадку доводиться чекати, поки наплив людей спаде. Ще одна неприємність — інколи Google під час спроби зайти в пошуковик видаватиме вам капчу (запит ввести символи, які ви бачите на екрані), бо хоче переконатися, що ви людина, а не бот. І ще одне: якщо ваш VPN-провайдер зберігає логи, ознайомтеся з політикою конфіденційності. Переконайтеся, що компанія не зберігає вашого трафіку або логів під'єднань (навіть у зашифрованому вигляді) і не передає даних правоохоронним органам. Цю інформацію можна знайти в умовах користування й політиці конфіденційності. Якщо вони надають інформацію правоохоронним органам, то точно зберігають логи.

Пасажири авіакомпаній, які користуються інтернет-сервісами на борту літака (наприклад, GoGo), ризикують так само, як і в Starbucks чи залі очікування, а VPN тут — не варіант. Позаяк GoGo й аналогічні сервіси мають блокувати Skype та інші програми голосових викликів, вони зупиняють передавання UDP-пакетів, що сповільнює більшість VPN-сервісів, які користуються протоколом UDP за замовчуванням. Але VPN на основі протоколу TCP, замість UDP, — наприклад, TorGuard або ExpressVPN — значно підвищить продуктивність. Обидва сервіси дають змогу користувачеві вибрати протокол самостійно.

Ще одна проблема з VPN — політика конфіденційності. Незалежно від того, користуєтеся ви платними VPN чи корпоративним, ваш трафік подорожує мережею провайдера. Тому важливо не забувати https, щоб провайдер не міг прочитати змісту ваших повідомлень[139]. Якщо ви працюєте в офісі, найімовірніше, компанія видасть вам VPN для дистанційної роботи. У застосунку на ПК потрібно ввести ім'я користувача й пароль (те, що ви знаєте). Також застосунок містить ідентифікаційний сертифікат, доданий вашим IT-відділом (те, що ви маєте), або відправляє контрольне повідомлення на телефон, виданий компанією (знову те, що ви маєте). Програма може проводити всі три перевірки — так звану багатофакторну автентифікацію.

Тепер можете спокійно сидіти в Starbucks або залі очікування в аеропорту і працювати, наче користуєтеся приватним інтернет-сервісом. Але не варто в

такий спосіб вирішувати особисті справи, як-от оплата з особистого рахунку. Шифруйте подібні сеанси через HTTPS Everywhere.

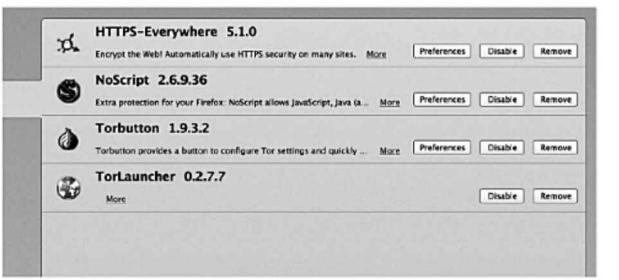
Єдиний спосіб довіряти VPN-провайдеру — анонімність від самого початку. Якщо справді хочете стати непомітним, ніколи не користуйтеся інтернет-з'єднанням, яке можна пов'язати з вашою особою (тобто мережею вдома, на роботі, у друзів, з готельного номера, зарезервованого на ваше ім'я, тощо). Мене зловили, коли в 1990-х ФБР відстежило сигнал мобільного телефона до моєї схованки в Ралі, штат Північна Кароліна. Тож якщо тікаєте від влади, ніколи не чіпайте особисту інформацію на одноразовому пристрої в місці, яке можна пов'язати з вами. Якщо хочете анонімності, одноразовий телефон у жодному разі не повинен бути пов'язаним із вашим реальним життям. Жодні метадані не мають вказувати на вашу особу.

А ще на мобільний девайс можна встановити VPN. В інтернеті багато інформації про те, як це робити на пристроях Apple[140] та на базі Android[141].

Якщо ви дотримуєтеся всіх порад, які були перераховані в книжці досі, то вже більш захищені, ніж середньостатистичний громадянин. Імовірно, більшій частині вашого інтернет-трафіку не загрожують прослуховування чи маніпуляції зловмисників.

Те саме і з вашими акаунтами в соцмережах. Усі сеанси на фейсбуці захищені https. Перевіряєте пошту? Google теж переключився на https. Як і більшість мейл-клієнтів і сервісів обміну миттєвими повідомленнями. Найбільші сайти — Amazon, eBay, Dropbox — тепер теж пристали на https.

Щоб стати невидимим, завжди краще «нашаровувати» рівні безпеки. Ризик розкрити свій трафік у громадській мережі знижується з кожним таким шаром. Наприклад, із громадського Wi-Fi під'єднайтеся до платного VPN-сервісу, а звідти ввімкніть розширення Tor і HTTPS Everywhere, установлені за замовчуванням у браузері Firefox.



Так усе, що ви робите в інтернеті, точно буде зашифрованим, а вас — складно відстежити.

Скажімо, ви просто хочете перевірити погоду — жодних фінансових операцій чи конфіденційних справ. І робите ви це через особистий ноутбук за межами домашньої мережі. Це ж безпечно, так? Почасти. Все ще доведеться потурбуватися про кілька нюансів.

По-перше, вимкніть Wi-Fi. Серйозно. Купа людей залишають Wi-Fi на ноутбуках увімкненим, навіть коли він їм не потрібен. Згідно з документами, опублікованими Едвардом Сноуденом, Канадський Центр безпеки комунікацій (CSEC) може ідентифікувати мандрівників, що летять через канадські аеропорти, просто перехопивши їхні MAC-адреси. Це можна провернути з будь-яким пристроєм, який виконує пошук бездротових пристроїв. Навіть якщо ви не під'єднуєтеся до мережі, MAC-адресу все одно можна перехопити. Тож якщо Wi-Fi вам не потрібен, вимкніть його[142]. Ми з вами вже переконалися, що заради зручності часто жертвуєш конфіденційністю та безпекою.

Досі ми ледве торкалися такої важливої проблеми, як MAC-адреса. Вона є унікальною для будь-якого девайса... але не фіксованою. Її можна змінити.

Наведу вам приклад.

У розділі 2 я розповів про PGP-шифрування електронної пошти. Але що як ви не хочете возитися з усім цим чи одержувач не має відкритого ключа PGP? Існує ще один таємний спосіб обміну повідомленнями електронною поштою: папка «Чернетки» в спільній електронній скриньці.

Так колишній директор ЦРУ Девід Петреус обмінювався повідомленнями з коханкою Полою Бродвелл — авторкою його біографії. Скандал розгорівся після того, як Петреус припинив стосунки й помітив, що хтось слав його другові листи з погрозами. Коли ФБР взялося за розслідування, виявилося, що саме Бродвелл слала погрози. Як і романтичні листи Петреусу[143].

Цікаво, що листувалися Бродвелл і Петреус, не надсилаючи імейли, а залишаючи їх у чернетках «анонімної» поштової скриньки. Так лист не проходить через інші сервери на шляху до одержувача. Менше шансів, що імейл перехоплять. А якщо хтось і дістане доступ до скриньки, докази можна легко знищити, заздалегідь видаливши листи й очистивши кошик.

А ще Бродвелл заходила в «анонімну» пошту з окремого комп'ютера. І ніколи не користувалася домашньою IP-адресою. Це було б занадто очевидно. Заради листування вона знімала номери в різних готелях.

Хоча Бродвелл доклала чимало зусиль,щоб приховатися, невидимкою вона так і не стала. За словами New York Times, «позаяк імейл відправника був зареєстрований анонімно, для встановлення особи слідчим довелося провести криміналістичну експертизу і перевірити, у які ще акаунти електронної пошти заходили з цієї адреси комп'ютера»[144].

Імейл-провайдери на зразок Google, Yahoo і Microsoft зберігають записи входу в пошту понад рік. Сюди входять й усі IP-адреси, з яких користувач входив у систему. Наприклад, якщо ви робите це через громадський Wi-Fi у Starbucks, IP-адреса вкаже на місцерозташування кав'ярні. Зараз у США правоохоронним органам дозволяється вилучати в імейл-провайдерів записи входу, маючи звичайну повістку — жодного суду.

А це означає, що в слідчих була інформація про місцеперебування кожної IP-адреси, через яку заходили в цю поштову скриньку. Потім вони зіставили дані з

логами Wi-Fi роутерів, які зареєстрували MAC-адресу пристрою Бродвелл у цих місцях[145].

З безмежними ресурсами ФБР (справа була гучна, бо Петреус на той час був директором ЦРУ), агенти змогли проглянути логи роутерів у кожному готелі і помітити, що MAC-адреса Бродвелл постійно фігурувала в цих логах. Окрім того, у зазначені дати Бродвелл заселялася в кожен із цих готелів. І от що зацікавило слідчих: хоча вона входила в ці анонімні акаунти електронної пошти, жодних імейлів вона не надсилала.

Під час приєднання до бездротової мережі роутер автоматично записує MAC-адресу вашого комп'ютера. MAC-адреса — це як серійний номер вашої мережевої плати. Щоб стати невидимим, перед під'єднанням до будь-якої бездротової мережі треба змінити MAC-адресу на ту, яку не можна пов'язати з вами. Щоб залишатися невидимим, потрібно змінювати MAC-адресу щоразу, як під'єднуєтеся до Wi-Fi. Так ваші інтернет-сеанси ніяк на вас не вкажуть. Також важливо в цей час не заходити в особисті акаунти — це підірве вашу анонімність.

Процес зміни MAC-адреси залежить від вашої операційної системи: Windows, Mac OS X, Linux, Android чи iOS[146]. Кожен раз, як під'єднуєтеся до громадської (або приватної) мережі, не забудьте змінити MAC-адресу. Не хвилюйтеся, після перезавантаження звична адреса повернеться на місце.

Припустимо, у вас нема ноутбука, а вийти в інтернет таки треба. Доведеться скористатися громадським комп'ютером десь у кафе, бібліотеці чи навіть бізнес-центрі елітного готелю. Як можна себе захистити?

Коли я йду в похід, то дотримуюся правила «не залишати слідів»: місце відпочинку на природі повинне мати такий самий вигляд, як і до того, коли я приїхав. Те саме можна сказати і про публічні комп'ютерні термінали. Коли ви підете, ніхто не повинен здогадатися, що ви там були.

Особливо це актуально на торговельних виставках. Якось я відвідав щорічну виставку Consumer Electronics Show і примітив цілий ряд громадських ПК, де учасники, гуляючи територією заходу, могли перевірити електронну пошту. Таке було навіть на міжнародній конференції з інформаційної безпеки RSA в Сан-Франциско. Купа загальнодоступних терміналів у громадських місцях — жахлива ідея з низки причин.

По-перше, комп'ютери — орендовані. Ними користуються лише час від часу. Звісно ж, їх можуть почистити, а операційну систему перевстановити, але хто знає?

По-друге, на них відкрито права адміністратора, а отже, будь-який учасник конференції може встановити туди будь-яке програмне забезпечення. Зокрема й шкідливі програми на зразок кілоґерів, які можуть запам'ятати ваш логін і пароль. У сфері безпеки ми наполягаємо на принципі «найменших привілеїв», коли машина надає користувачеві лише мінімально потрібний доступ. Вхід у громадський термінал на правах системного адміністратора (що часто

встановлено за замовчуванням) порушує принцип найменших привілеїв і збільшує ризик того, що ви зараз користуєтеся комп'ютером зі шкідливим ПЗ. Єдиний вихід — переконатися, що ви працюєте в гостьовому акаунті з обмеженими функціями.

Але раджу взагалі ніколи не довіряти громадським ПК. Припустимо, що людина, яка користувалася комп'ютером перед вами, встановила шкідливе ПЗ — навмисно чи несвідомо. Якщо ви зайдете в Gmail із громадського термінала, на якому встановлено кілоґер, третя сторона матиме ваш логін і пароль. Якщо хочете зайти в інтернет-банк, забудьте про це. І забезпечте собі 2ФА на кожному сайті, щоби зловмисник не міг видати себе за вас навіть з вашим логіном і паролем. Двофакторна автентифікація значно знизить імовірність злому акаупта, якщо хтось дізнається ваш логін і пароль.

Мене щиро вражає, скільки людей користуються громадськими ПК на комп'ютерних конференціях на зразок CES і RSA. Висновок: якщо ви на виставці, користуйтеся мобільним телефоном чи планшетом, особистим хот-спотом або потерпіть до дому чи до готелю. Якщо потрібно вийти в інтернет далеко від дому або роботи, скористайтеся смартфоном. Якщо ж кров з носа потрібен громадський термінал, у жодному разі не входьте в особисті акаунти, навіть у пошту. Приміром, якщо шукаєте ресторан, відкривайте лише ті сайти, які не потребують перевірки автентичності, як-от Yelp. Якщо користуєтеся громадськими терміналами майже на постійній основі, заведіть собі електронну пошту лише для громадських комп'ютерів і поставте переадресацію листів зі «справжніх» скриньок, коли поїхали у відрядження. Вимкніть функцію, щойно повернетеся додому. Це зводить до мінімуму кількість інформації, яку можна вилучити з «одноразової» адреси.

Також переконайтеся, що сайти, на які ви заходите з публічного термінала, мають https в URL-адресі. Якщо позначки https нема (або якщо є, але ви підозрюєте, що хтось туди її помістив обманним шляхом, щоб приспати вашу пильність), намагайтеся не вводити на таких сайтах конфіденційної інформації з цього термінала.

Припустимо, ви зайшли на цілком безпечну URL-адресу з https. На сторінці входу знайдіть вікно з написом «Запам'ятати мене». Зніміть прапорець. Причина очевидна: це не ваш особистий комп'ютер. Ним користуються й інші люди. Якщо сайт вас запам'ятає, на терміналі з'явиться cookie-файл. Ви ж не хочете, щоби наступна людина зайшла у ваш імейл і надіслала лист від вашого імені?

Повторюся, але не заходьте в акаунти на фінансових або медичних сайтах із громадського ПК. Якщо таки входите в акаунт (Gmail чи будь-який інший), обов'язково виходьте з нього, коли закінчите роботу. Можна ще перестрахуватися і якомога швидше змінити пароль уже з особистого комп'ютера чи телефона. Можливо, вдома ви й не виходите з акаунтів, але не забувайте робити цього на чужих комп'ютерах.

Після того як відправили імейл (або знайшли в інтернеті те, що хотіли) і вийшли з системи, зітріть історію браузера, щоби наступна людина не змогла дізнатися, куди ви заходили. За можливості видаліть усі cookie-файли. І переконайтеся, що не завантажили особисті файли на комп'ютер. Якщо таки завантажили, спробуйте видалити файли з робочого столу або папки із завантаженнями.

Але просто видалити файл недостатньо. Після видалення очистіть ще й кошик. Хоча і так ви все одно не позбудетеся файлу повністю: за бажанням, я можу відновити файл після того, як ви підете. На щастя, більшість людей так не вміє, і зазвичай вам вистачить простого видалення й очищення кошика.

Усіх правил просто необхідно дотримуватися, якщо хочете залишитися непомітним у громадському терміналі.

---

135 Важливо зазначити, що громадський Wi-Fi відкритий і доступний не в усіх куточках світу. Наприклад, у Сінгапурі, щоб скористатися громадським Wi-Fi за межами готелю або McDonald's, треба зареєструватися. Місцеві жителі повинні мати сінгапурський номер мобільного телефону, а туристи — надати свої паспорти в місцеві органи влади, щоб отримати дозвіл.

136 https://f-securecybersecurity.co.za/dangers-public-wifi-crazy-things-people-use/.

137 http://dnlongen.blogspot.com/2015/05/is-your-home-router-spying-on-you.html.

138 Існує безліч нюансів, які потрібно знати, вибираючи VPN-провайдер. Див. https://torrentfreak.com/anonymous-vpn-service-provider-review-2015-150228/3/.

139 Один з варіантів комерційного VPN — канадська компанія TunnelBear. Вона заявляє, що «TunnelBear НЕ зберігає вихідні IP-адреси користувачів під час під'єднання до нашого сервісу і тому ідентифікувати користувачів за IP-адресами наших серверів неможливо. Крім того, ми не можемо надати інформацію про застосунки, сервіси чи веб-сайти, якими користуються наші клієнти, позаяк TunnelBear НЕ зберігає цю інформацію». https://www.tunnelbear.com/privacy-policy/.

140 http://www.howtogeek.com/215730/how-to-connect-to-a-vpn-from-your-iphone-or-ipad/.

141 http://www.howtogeek.com/135036/how-to-connect-to-a-vpn-on-android/?PageSpeed= noscript.

142 http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881.

143 http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9673429/David-Petraeus-ordered-lover-Paula-Broadwell-to-stop-emailing-Jill-Kelley.html.

144 http://www.nytimes.com/2012/11/12/us/us-officials-say-petraeuss-affair-known-in-summer.html.

145 https://www.wired.com/2012/11/gmail-location-data-petraeus/.

146 http://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/?PageSpeed=noscript.

Розділ 9

Приватності не існує. Змиріться[147]

Якось колишньому розробникові відомого антивірусу Джону Макафі майнула думка розпочати блог... поки він тікав від влади Белізу. Повірте на слово: якщо ви намагаєтеся зникнути з радарів, блог — найгірша ідея. Ви обов'язково припуститеся помилки.

Макафі — розумний чоловік. Він збив статки на світанку Кремнієвої долини, ставши першопрохідцем антивірусних досліджень. Потім він продав компанію й усі активи в США і приблизно чотири роки — з 2008-го до 2012-го — жив у Белізі, на віллі біля моря. В останні роки уряд Белізу тримав Макафі під постійним наглядом, час від часу обшукуючи віллу і звинувачуючи його у створенні приватної армії й торгівлі наркотиками.

Макафі заперечував це і казав, що, навпаки, завжди боровся з наркобаронами на острові. Наприклад, подарував дрібному торговцеві маріхуаною телевізор із пласким екраном за умови, що той припинить торгувати. А також зупиняв на дорозі машини, у яких, за його припущеннями, їхали наркоторговці[148].

Але Макафі таки мав лабораторію з виготовлення наркотиків, проте не рекреаційних. Він стверджував, що створює нове покоління «корисних» препаратів. Звідси його постійна підозра, що всі машини з іноземними номерами — шпигуни з фармацевтичних компаній на зразок GlaxoSmithKline. Згодом він заявив, що рейди місцевої поліції — теж справа рук фармацевтичних компаній.

Охороняли майно Макафі кілька людей зі зброєю й одинадцять собак. Сусід за два будинки від нього, Ґреґ Фолл, регулярно скаржився владі на гавкіт собак ночами. В один із вечорів листопада 2012 року кількох собак Макафі отруїли. Того самого тижня Фолла застрелили. Чоловіка знайшли на підлозі власного будинку, обличчям у калюжі крові.

Влада Белізу не без підстав назвала Макафі підозрюваним у справі. Як пише Макафі у своєму блозі, коли економка сказала йому, що поліція хоче поговорити, він одразу зник. Став утікачем.

Але не блог врешті-решт вивів правоохоронні органи на Макафі. А звичайне фото. Яке навіть не він опублікував.

Дослідник інформаційної безпеки Марк Лавлесс (більш відомий у вузьких колах як Simple Nomad) помітив фотографію Макафі у твітері журналу Vice на початку грудня 2012 року. На світлині редактор Vice стоїть поруч із Макафі на фоні тропіків — може, десь у Белізі, а може, деінде.

Лавлесс знав, що цифрові фотографії містять багато інформації про те, коли, де і як були зроблені. Дослідник вирішив подивитися, яку цифрову інформацію містить це фото. Усі цифрові світлини містять так званий EXIF — метадані фотографії. Зазвичай це нудні деталі, як-от рівень насиченості кольору для

точного відтворення на екрані чи принтері. Але деякі камери додають сюди ще й точну широту й довготу місця, де було зроблено фотографію.

Світлину Макафі з редактором Vice було зроблено на iPhone 4S, а деякі стільникові телефони мають автоматично ввімкнену геолокацію. Лавлессу пощастило: зображення у твітері містило точне місцеперебування Джона Макафі, який, як виявилося, ховався в сусідній Гватемалі.

Пізніше в блозі Макафі написав, нібито підробив дані (що малоймовірно), а згодом узагалі повідомив про свій намір розкрити місцеперебування. Імовірно, йому просто набридло.

Якщо коротко, поліція Гватемали затримала Макафі й заборонила покидати країну. Згодом чоловік захворів, його госпіталізували і врешті-решт дозволили повернутися в Сполучені Штати.

Вбивство Ґреґа Фолла все ще не розкрито. Макафі зараз мешкає в Теннессі, а 2015 року вирішив балотуватися на пост президента і впроваджувати більш «кіберлояльну» політику уряду США. Зараз веде блог, але не так регулярно.

Припустимо, ви — молодий, амбітний джихадист і пишаєтеся тим, що отримали місце в новенькому військовому штабі ІДІЛ. Що зробите спершу? Звісно ж, дістанете смартфон і зробите селфі. Ба навіть краще: разом із фото свого задоволеного обличчя на фоні нового військового об'єкта опублікуєте кілька слів про очманіле обладнання.

А на іншій півкулі розвідники авіабази Гарлбарт Філд у Флориді прочісують соцмережі й роздивляються фотографії. «Щось знайшов», — каже один із них. І через кілька годин три «розумних» бомби залишають від новенької, блискучої військової бази саме попелище[149]. І все через селфі[150].

Ми незавжди думаємо про те, що ховається в кадрі звичайного селфі. У театрі й кіно це називається «мізансцена» й приблизно перекладається з французької як «те, що є на сцені». Ви можете сфотографувати метушливий міський пейзаж із Всесвітнім торговим центром із вікна власної квартири. Навіть фотографія десь за містом (наприклад, степ, що тягнеться аж до самого горизонту) містить цінну інформацію про те, де ви мешкаєте. Візуальні орієнтири завжди дають крихітні підказки про місце людині, якій кортить вас знайти.

Що ж стосується молодого джихадиста, то «на сцені» був військовий штаб.

А от у метаданих селфі ховалися точні довгота й широта, тобто геолокація місця, де було зроблено фотографію. Генерал Гоук Карлайл — голова Бойового командування Повітряних сил США — підрахував, що з часу першої публікації селфі до повного знищення штаб-квартири минуло всього двадцять чотири години.

За метаданими, що містяться у ваших фотографіях, вас можна легко знайти. Дані EXIF цифрового зображення містять дату і час, коли було зроблено знімок, марку і номер моделі камери, а також довготу і широту місця, де ви зробили знімок, якщо на пристрої активовано геолокацію. За цими даними американські військові знайшли штаб-квартиру ІДІЛ у пустелі. За цими самими даними Марк

Лавлесс знайшов Джона Макафі. Дістати доступ до метаданих ваших світлин і документів може будь-хто: необхідна програма вже встановлена в Apple OS X; для Windows можна завантажити FOCA, для Linux — Metagoofil.

Іноді на вашу геолокацію вказує не фото, а сам застосунок. Улітку 2015 року наркобарон Хоакін «Ель Чапо» Ґусман утік із мексиканської в'язниці і відразу ж зник. Але ненадовго. За два місяці після втечі з Альтіплано — мексиканської в'язниці з максимальним рівнем безпеки — двадцятидев'ятирічний син Ель Чапо, Хесус Альфредо Ґусман Салазар, опублікував у твітері фото. Хоча обличчя чоловіків за обіднім столом Салазара закриті смайликами, статура людини зліва дуже схожа на Ель Чапо.

І підпис під фото: «Серпень уже тут, і ти знаєш, з ким його проведеш». Твіт також містив дані геолокації — Коста-Рика. Імовірно, син Ель Чапо не зміг вимкнути автоматичну функцію в застосунку на смартфоні[151].

Навіть якщо серед ваших родичів немає злочинця-втікача, все одно не варто забувати, що цифрова чи візуальна інформація, прихована у фотографіях (іноді на самій поверхні), може розповісти багато нового й обернутися зброєю проти вас.

Геолокація — не найстрашніше, що можуть розкрити фотографії в інтернеті. Якщо скористатися певними програмами, вони здатні вказати на вашу особисту інформацію.

У 2011 році Алессандро Аквісті, дослідник з Університету Карнеґі—Меллона, висунув просту гіпотезу: «Я хотів перевірити, чи можна дізнатися номер соціального страхування будь-якого перехожого по обличчю». З'ясувалося, що можна[152]. Зробивши безневинне фото студента-волонтера на веб-камеру, Аквісті з командою отримали достатньо інформації й розкопали його особисті дані.

Лише уявіть: ви можете сфотографувати людину на вулиці і спробувати ідентифікувати її через програму розпізнавання облич. Так, програма може кілька разів видати помилкові результати, які здатна підтвердити лише сама людина. Але є ймовірність, що одне ім'я випадатиме частіше за інші.

«Зараз відбувається змішання онлайнових та офлайнових даних, а ваше обличчя — це канал, зв'язок між двома світами, — сказав Аквісті сайту Threatpost. — Думаю, що урок тут досить невеселий. Ми повинні змиритися з тим, що саме уявлення про недоторканність приватного життя руйнується з кожним днем. Ми вже не інкогніто на вулиці чи в натовпі. Поєднання технологій підриває наше природне очікування конфіденційності».

У рамках дослідження Аквісті з командою зупиняли студентів у кампусі Університету Карнеґі—Меллона і просили їх пройти онлайн-опитування. Веб-камера на ноутбуці робила знімок кожного студента, коли той проходив опитування, і фотографія негайно завантажувалася в програму розпізнавання облич. Після завершення кожного опитування на екрані з'являлося кілька фотографій із соцмереж. За словами Аквісті, 42 % студентів було правильно ідентифіковано, а фотографії на екрані відповідали їхнім світлинам у фейсбуці.

Якщо ви користуєтеся фейсбуком то, напевно, знаєте про його технологію розпізнавання облич. Коли ви завантажуєте фото на сайт, фейсбук намагається відмітити на ньому людей, що вже є у вас в друзях. Але технологія частково під вашим контролем. У налаштуваннях фейсбука можна ввімкнути оповіщення, якщо хтось відмічає вас на фото, і залишити чи прибрати мітку. Також можете дозволити публікацію фото на вашій стіні або в хроніці лише після схвалення.

Щоб приховати фотографії з вами, відкрийте свій акаунт і перейдіть у розділ «Налаштування конфіденційності». Тут є кілька варіантів, зокрема приватна хроніка, доступна лише вам. Але фейсбук поки що не дає можливості заборонити людям відмічати вас без дозволу.

Такі компанії, як Google та Apple, теж мають технологію розпізнавання обличчя, вбудовану в деякі з їхніх затосунків, приміром, Google Photo чи iPhoto. Думаю, варто залізти в параметри цих застосунків і максимально обмежити функції розпізнавання. Досі Google не підключав цю технологію до фупкції пошуку зображень (маленький значок камери у вікні пошуку Google). Ви можете завантажити будь-яке зображення, і ґуґл знайде його, якщо воно є в інтернеті. Але він не буде намагатися знайти інші фотографії з цією самою людиною чи людьми. Google не раз публічно заявляв, що, даючи змогу ідентифікувати незнайомців за обличчям, «перетинає моторошну межу»[153].

Проте деякі репресивні уряди цю межу перетнули. Траплялися випадки, коли протестувальників на антиурядових мітингах фотографували й викладали світлини в інтернет. І це вже не технологія розпізнавання облич — це краудсорсинг процесу ідентифікації. Крім того, у деяких штатах США правоохоронні органи користуються базами даних автотранспортних управлінь для ідентифікації підозрюваних у кримінальних справах. Але все це — операції державного рівня. На що ж здатен один-єдиний дослідник?

Аквісті та його колеги хотіли дізнатися, скільки інформації про людину можна знайти в інтернеті за звичайним фото. Для цього вони скористалися технологією розпізнавання обличчя під назвою Pittsburgh Pattern Recognition, або PittPatt, яка зараз належить Google. Алгоритмами PittPatt користуються різноманітні компанії з безпеки й державні установи. Незабаром після придбання технології Google оголосив про свої наміри: «Як ми вже говорили цього року, ми не збираємося впроваджувати технологію розпізнавання облич у пошуковик, доки не створимо надійний алгоритм для підтримання конфіденційності. Поки що ми його не створили»[154]. Будемо сподіватися, що компанія триматиме слово.

У дослідженні Аквісті скористався алгоритмами PittPatt на основі завантажених з фейсбука фотографій. Враховувалися лише «придатні для пошуку» профілі, тобто такі, на яких добровольці з Карнегі—Меллон розмістили власні фото разом із крихтами особистої інформації. Дослідники порівняли базу даних відомих облич із «анонімними» на популярному сайті знайомств. У результаті змогли ідентифікувати 15 % нібито анонімних цифрових серцеїдів.

Але найбільш моторошний експеримент полягав у зіставленні обличчя людини з її номером соціального страхування. Для цього Аквісті з командою шукали у фейсбуці профілі з датою і місцем народження. Ще 2009 року та сама група дослідників довела, що цієї інформації достатньо, щоб отримати номер соціального страхування людини (номери соціального страхування генеруються за усталеною формулою, а з 1989 року видаються в день народження або близько до дати, тож вгадати останні чотири цифри номера вже простіше)[155].

Після деяких розрахунків дослідники надіслали добровольцям ще одне опитування з першими п'ятьма цифрами їхнього орієнтовного номера соціального страхування, прорахованими алгоритмом. Більшість студентів підтвердили, що цифри правильні[156].

Б'юся об заклад, від деяких фото в соціальних мережах ви б з радістю позбавилися. Однак, найімовірніше, позбавитися від них до кінця ви не зможете, навіть якщо видалите з акаунта. Щойно ви публікуєте щось у соціальній мережі, це щось перестає бути вашим. Тепер це щось належить соцмережі. І ви на це самі погодилися, приймаючи умови надання послуг.

Якщо ви користуєтеся популярним застосунком Google Photos, то навіть видаливши фото, ви від нього не позбавитеся. Деякі користувачі помітили, що зображення зберігаються навіть після видалення застосунку з телефона. Чому? Бо щойно зображення потрапляє в хмару, воно припиняє залежати від застосунку, а отже, інші програми все ще мають до нього доступ і відображають видалене зображення[157].

І це може вийти за рамки віртуального життя. Припустимо, ви опублікували якийсь дурний підпис під світлиною людини, яка працює в компанії, куди ви тепер намагається влаштуватися. Або запостили фото з кимось, про кого краще не знати теперішній другій половинці. Хоча акаунт ваш особистий, дані цілком і повністю належать соцмережі.

Ви, ймовірно, ніколи навіть і не намагалися прочитати умови надання послуг сайтів, на яких розміщуєте особисті дані, повсякденне життя, думки, історії, нарікання, скарги тощо. Або сайтів, де робите покупки, граєте або вчитеся щодня чи навіть щогодини. Більшість соцмереж вимагають від користувачів під час реєстрації погодитися з правилами та умовами сайту. Цікаво, що ці умови часто містять положення, які дають сайтам право зберігати дані, отримані від користувачів, і навіть ділитися ними з третіми особами.

Facebook уже роками привертає увагу своєю політикою зберігання даних, зокрема складністю видалення акаупта. І в цьому компанія не самотня. Безліч сайтів містять в умовах використання ідентичні шматки, які, імовірно, під час реєстрації вас відстрахають і змусять закрити сторінку. Ось вам приклад з фейсбука, від 30 січня 2015 року:

> *Вам належить право власності на весь контент, який ви поширюєте у Facebook, і ви можете контролювати його поширення згідно з вашими налаштуваннями конфіденційності та застосування. Крім того:*

1. Щодо контенту, який є об'єктом прав інтелектуальної власності, наприклад, фотографії та відеозаписи (IP-контент), ви надаєте нам наступний дозвіл згідно з вашими налаштуваннями конфіденційності та застосування: ви надаєте нам невиключну, з правом передавання та субліцензування, без виплати роялті, глобальну ліцензію на використання будь-якого IP-контенту, який ви поширюєте на Facebook або у зв'язку з ним (IP-ліцензія). IP-ліцензія припиняє свою дію, коли ви видаляєте свій IP-контент чи обліковий запис, якщо ви не поширили його для інших користувачів, які його не видалили[158].

Інакше кажучи, Facebook має право використовувати все, що ви розміщуєте на сайті, де і як захоче. Він навіть може продати вашу фотографію, вашу рецензію, ваш пост — усе, що ви публікуєте, — і заробити на цьому, не виплативши вам ані копійки. Він може скористатися вашими коментарями, критикою, думками, наклепом (якщо ви таке пишете) й будь-якими особистими даними про ваших дітей, начальника чи кохану людину, які ви хоч раз опублікували на сайті. І необов'язково анонімно: якщо ви зареєстровані під справжнім ім'ям, ним Facebook теж може скористатися.

А це означає, що опубліковані вами світлини на фейсбуці можуть раптом опинитися на інших сайтах. Щоб дізнатися, чи не розлетілися по інтернету якісь небажані фото, скористайтеся пошуком за зображенням у ґуґлі. Для цього натисніть на маленьку іконку камери у вікні пошуку Google і завантажте будь-яку фотографію з жорсткого диска. За кілька секунд ви побачите всі копії цього зображення в інтернеті. Теоретично, якщо це ваша особиста світлина, ви повинні знати всі джерела з результатів пошуку. Але якщо хтось опублікував ваше фото без дозволу, варіантів у вас обмаль.

Пошук за зображенням обмежений тим, що опубліковано. Інакше кажучи, якщо десь в інтернеті є подібна, але не ідентична фотографія, ґуґл її не знайде. Так, він знайде обрізані версії вашого зображення, але вихідне фото повинно бути тим самим.

Якось на мій день народження друзі хотіли подарувати мені марку з моїм зображенням. Однак у компанії stamps.com досить сувора політика проти використання зображень засуджених осіб. Моє фото відхилили. Найімовірніше, вони закинули його в інтернет і знайшли десь у базі Кевіна Митника, засудженого за злочин.

Наступного року подруга спробувала ще раз, відправивши більш ранню фотографію й фальшиве ім'я. Фото було зроблено задовго до того, як я став «популярним». Подруга була впевнена, що цю світлину ще ніхто в інтернет не завантажував. І знаєте що? Це спрацювало. Другу фотографію з молодшим мною схвалили. Це наочно демонструє обмеження в технології пошуку зображень.

Але повернемося трохи назад. Якщо пошук усе ж видасть вам ваші фото, які б ви не хотіли бачити в інтернеті, варіантів у вас не так багато.

Спочатку зв'яжіться із сайтом. Більшість сайтів має адресу електронної пошти для скарг у форматі «abuse@[назва сайту].com». Можете також зв'язатися з веб-

майстром сайту за адресою «admin@[назва сайту].com». Поясніть, що ви є власником зображення і не даєте дозволу на його публікацію. Більшість веб-майстрів без зайвих нарікань видалять зображення. Якщо ж це не спрацювало, можете подати заяву на основі Закону «Про авторське право в цифрову епоху» (DMCA) за адресою «DMCA@[назва сайту].com».

Але будьте обережні. Неналежний запит DMCA може потягнути за собою неприємності, тож спершу проконсультуйтеся з юристом. Якщо все ще не можете позбутися фото, беріть ще вище і звертайтеся до провайдера сайту (Comcast, GoDaddy чи інша компанія). Але більшість сайтів почне ворушитися вже на етапі із запитом DMCA.

А що ще є у вашому профілі в соцмережах, окрім фотографій? Ви б не стали ділитися всім на світі з людиною, що сидить поруч з вами в метро, правда? Так само не бажано виставляти забагато особистої інформації на публічні сайти. Ніколи не знаєш, хто прочитає твій профіль. А щойно інформація потрапить в інтернет, її вже не позбутися. Ретельно зважуйте все, що хочете написати в профілі — необов'язково заповнювати всі порожні клітинки, як на екзамені. Навпаки, пишіть якомога менше інформації.

А ще можна створити спеціалізований профіль у соцмережі. Брехати не варто — просто подавайте факти дещо розпливчасто. Наприклад, якщо виросли в Атланті, напишіть, що дитинство провели «в південно-східних Сполучених Штатах» або просто «я з півдня».

Також подумайте про «безпечну» — тобто вигадану — дату народження, щоб приховати особисту інформацію ще краще. Але записуйте десь собі всі «безпечні» дати народження, бо іноді вони знадобляться для підтвердження особи в техпідтримці чи для відновлення профілю після блокування.

Після створення або налаштування профілів присвятіть кілька хвилин параметрам конфіденційності на кожному сайті. Наприклад, на фейсбуці необхідно ввімкнути елементи управління конфіденційністю, зокрема й перевірку міток. Відключити «Пропонувати фото друзям». Відключити «Друзі можуть відмічати мене в місцях».

Діти з акаунтами у фейсбуці, мабуть, найбільш вразливі. Вони зазвичай заповнюють усі порожні поля, які знайдуть, навіть сімейний стан. Або безвинно вказують назви своїх шкіл, імена вчителів, номери автобусів, якими вони їдуть на заняття щоранку. Хоча й діти не часто вказують номер свого будинку, іноді трапляється і таке. Батьки повинні підтримувати з дітьми дружні стосунки, стежити за тим, що вони публікують, і заздалегідь обговорювати, що можна розповідати, а що — ні.

Анонімність не означає, що ви не можете без остраху ділитися фактами з особистого життя, але в усьому має бути здоровий глузд. У цьому випадку — це виставити розумні налаштування конфіденційності в соцмережах і періодично до них повертатися, бо політика конфіденційності часто змінюється. Й іноді

зовсім не на краще. Приберіть справжню і навіть «безпечну» дату народження. Або принаймні приховайте її від «друзів», яких не знаєте особисто.
От візьмемо пост на зразок «Пані Санчес — найкраща вчителька!». Наступний пост може бути про якийсь ярмарок у початковій школі Аламо. Трохи поґуґливши, ми дізнаємося, що пані Санчес викладає у п'ятому класі в початковій школі Аламо. Логічний висновок: власник цього акаунта — дитина приблизно десяти років.

Незважаючи на попередження Спілки споживачів та інших організацій тим, хто публікує особисту інформацію в мережі, люди продовжують це робити. Не забувайте, щойно інформація з'явиться у відкритому доступі, треті особи можуть легко нею скористатися. І цілком законно[159].

А ще пам'ятайте, що ніхто не змушує вас розміщувати особисту інформацію. Ви можете розповісти стільки, скільки захочете. Іноді доводиться вказувати певну інформацію, але в більшості випадків ви самі вирішуєте, чим хочете поділитися і в яких масштабах. Вам треба встановити власний рівень конфіденційності і прийняти той факт, що будь-яка викладена в інтернет інформація залишиться там назавжди.

Щоб допомогти вам краще контролювати цей аспект, у травні 2015-го Facebook запустив новий інструмент для перевірки конфіденційності[160]. Але попри всі ці інструменти майже тринадцять мільйонів користувачів Facebook 2012 року повідомили Спілці споживачів, що ніколи не користувалися інструментами конфіденційності чи навіть не чули про них. А 28 % користувачів діляться всіма або майже всіма постами на стіні з аудиторією, ширшою за коло друзів. Але характерно й те, що 25 % опитуваних сфальсифікували інформацію у профілі, щоби захистити свою конфіденційність. З 2010 року ця цифра зросла на 10 %[161]. Що ж, ми хоча б учимося.

Хай ви і маєте повне право розміщувати неточну інформацію про себе, майте на увазі: у Каліфорнії незаконно видавати себе за іншу людину в інтернеті. Ви не можете прикидатися іншою особою. А Facebook реалізує політику, яка не дасть вам змоги створити акаунт на чуже ім'я.

Таке якось сталося і зі мною. Мій акаунт заблокували, бо Facebook звинуватив мене в присвоєнні особи Кевіна Митника. У той час на фейсбуці було дванадцять Кевінів Митників. Ситуацію виправили, лиш коли CNET опублікували історію про те, як фейсбук заблокував реального Кевіна Митника[162].

Однак є безліч причин, чому людям може знадобитися вигадане ім'я. Якщо для вас це важливо, то знайдіть соцмережу, яка дає змогу постити анонімно чи під іншим ім'ям. Однак подібні сайти ніколи не зрівняються з масштабами фейсбука.

Будьте обережні з тим, кого додаєте в друзі. Якщо ви бачилися з людиною віч-на-віч — чудово. Якщо людина є другом когось, кого ви знаєте, — теж нехай. Але якщо отримали запит від незнайомої людини, подумайте двічі. Хоча ви й

можете видалити з друзів будь-кого і будь-якої миті, все одно в людини буде шанс побачити весь ваш профіль. Лише кілька секунд — усе, що потрібно зловмисникові, щоби втрутитися у ваше життя. Раджу приховати на фейсбуці всю особисту інформацію, бо в соцмережах часто трапляються атаки, *навіть з боку друзів*. До того ж друзі завжди можуть репостнути ваші дані, до яких мають доступ, без вашої згоди чи відома.

Наведу приклад. Якось мене хотів найняти один хлопець, який став жертвою вимагання. Він познайомився з дивовижною дівчиною на фейсбуці і почав відправляти їй свої оголені фото. Це тривало деякий час. А потім ця «жінка» (яка, імовірно, була якимось хлопцем з Нігерії) попрохала надіслати їй чотири тисячі доларів. Що хлопець і зробив. Зв'язався він зі мною після того, як йому наказали відправити ще чотири тисячі, інакше його оголені фотографії розішлють усім його друзям на фейсбуці, включно з батьками. Він відчайдушно хотів знайти вихід із ситуації. Я сказав йому, що єдиний реальний варіант — розповісти родині або почекати й подивитися, чи перейде вимагач від загроз до дії. Я порадив йому не платити: якщо хлопець надсилатиме гроші, вимагач ніколи не зупиниться.

Соцмережі можна зламати й «законним» способом. Хтось може подружитися з вами, щоб дістати доступ до людини у вас в друзях. Правоохоронні органи можуть шукати інформацію про підозрюваного, який якось із вами пов'язаний. Таке трапляється.

За даними організації Electronic Frontier Foundation, федеральні слідчі вже роками користуються соціальними мережами для пасивного спостереження. У 2011 році EFF оприлюднили навчальний курс для співробітників Служби внутрішніх доходів США на тридцять вісім сторінок (на основі закону «Про свободу інформації»), яким ті начебто користувалися для проведення досліджень у соцмережах[163]. Хоча федеральні агенти за законом не можуть прикидатися кимось іншим, у друзі до вас напроситися вони можуть цілком законно. Так вони дістануть доступ до всіх ваших постів (якщо не прибрати це в налаштуваннях конфіденційності) і всіх ваших друзів. EFF продовжує вивчати питання конфіденційності, пов'язані з новою формою спостереження правоохоронних органів.

Іноді корпорації стежать за вами, коли ви публікуєте в соцмережах щось для них «небажане». Навіть таке невинне, як коментар про шкільний іспит.

Для одного учня такий твіт обернувся проблемами. Коли Елізабет Джуїтт, адміністраторка регіональної середньої школи Вотчунг у Воррені, штат Нью-Джерсі, отримала лист від компанії-видавця іспиту, вона радше здивувалася, аніж занервувала. Її просто вразило те, що така велика корпорація як Pearson Education спостерігає за твітерами звичайних учнів. Неповнолітні мають певну конфіденційність і свободу дій щодо публікацій у соцмережах. Але учням (як у школі, так і в коледжі чи університеті) потрібно усвідомити: усе, що вони

роблять в інтернеті, може побачити будь-хто. Що ж трапилося в цій ситуації? Один із учнів Джуїтт нібито виклав у твітер матеріал із тесту.

Насправді ж він твітнув питання про питання. Не фото сторінки з іспиту — усього лише кілька слів. Трапилося це під час загального тесту в штаті Нью-Джерсі від Товариства оцінки готовності до коледжу і кар'єри (PARCC). Твіт опублікували приблизно о третій дня — уже задовго після того, як учні в окрузі пройшли тест. Адміністраторка поговорила з батьками учня, який запостив твіт, і той його видалив. Доказів списування не було. Твіт (зміст якого не розголошують) був суб'єктивним коментарем, а не проханням допомогти з відповіддю.

Але нова правда про Pearson Education занепокоїла громадськість. «Міністерство освіти повідомило, що Pearson Education контролює всі соціальні мережі під час іспиту PARCC», — написала своїм колегам Джуїтт в імейлі, який місцевий журналіст опублікував без її дозволу. У листі Джуїтт підтвердила, що Pearson Education виявили ще три подібні випадки й передали їх на розгляд місцевого відділу Міністерства освіти.

Хоча не лише Pearson Education моніторять соцмережі щодо крадіжки інтелектуальної власності, їхні дії порушують певні питання. Як, наприклад, компанія виявила особу учня лише за його акаунтом у твітері? У статті для New York Times компанія заявляє: «Якщо хтось ділиться інформацією про іспит за межами класної кімнати — хай то в приватній розмові чи в інтернеті, — ми вважаємо це витоком даних. Знову ж таки, наша мета — забезпечити справедливе тестування для всіх учнів. Кожен заслуговує скласти іспит на рівних умовах»[164].

Через посадових осіб у Массачусетсі, де також проводять тест PARCC, журналісти New York Times дізналися, що Pearson Education таки зіставляють твіти про іспит зі списками зареєстрованих на тест учнів. Pearson Education відмовилися коментувати цю заяву.

Штат Каліфорнія споконвіку проглядав соціальні мережі під час щорічного іспиту STAR (Стандартизоване тестування та перевірка успішності). У 2013-му, коли тест востаннє проводився у штаті, каліфорнійський відділ Міністерства освіти назвав 242 школи, чиї учні розміщували пости в соцмережах під час проведення іспиту. Лише в шістнадцяти йшлося про питання чи відповіді тесту[165].

«Цей інцидент підкреслив масштаби спостереження за учнями — як всередині, так і за межами шкільного середовища, — заявила Елана Зейде, дослідниця з питань конфіденційності в Інституті інформаційного права Нью-Йоркського університету. — Зазвичай соціальні медіа є окремою від школи територією. Пости у твітері можна порівняти з особистими розмовами за стінами школи. Тож стеження Pearson Education більше схоже на шпигунство за розмовами в транспорті, аніж у шкільних коридорах»[166].

Проте дослідниця продовжує: «Акцент повинен зміститися з особистих інтересів на ширші наслідки інформаційної практики. Школи й освітні організації не повинні клеймити батьків як ненависників прогресу лише тому, що ті не можуть чітко сформулювати, яку шкоду нові практики несуть їхній дитині. Батьки, своєю чергою, мають зрозуміти, що школи не можуть задовольнити всі їхні вимоги конфіденційності, позаяк на карту поставлено колективні інтереси, що впливають на всю систему освіти».

Твітер зі своїм традиційним лімітом у 140 символів глибоко проникнув у наше життя, збираючи безліч крихітних деталей про наш побут. У політиці конфіденційності сайт чесно визнає, що збирає і зберігає особисту інформацію через різні сайти, застосунки, SMS-повідомлення, API (прикладний програмний інтерфейс) та інші сторонні ресурси. Якщо люди користуються твітером, вони погоджуються на збір, передавання, зберігання, розкриття й інше використання особистої інформації. Щоб створити акаунт у твітері, треба вказати власне ім'я, ім'я користувача, пароль і адресу електронної пошти. Одну адресу можна зв'язати лише з одним акаунтом у твітері.

Ще одна проблема з конфіденційністю у твітері стосується витоку твітів — приватних постів, які раптом опублікували для широкого загалу. Таке трапляється, коли друзі користувача з приватним акаунтом ретвітнути або скопіювали закритий твіт і розмістили його у себе в публічному акаунті. А щойно твіт став публічним, сховати його вже не можна.

У твітері небезпечно ділитися особистою інформацією, особливо якщо ваші твіти є публічними (за замовчуванням). Не пересилайте жодних адрес, телефонів, номерів кредитних карток і номерів соціального страхування[167]. Якщо треба поділитися з кимось конфіденційною інформацією, скористайтеся особистими повідомленнями для розмови з конкретною особою. Але майте на увазі, що навіть особисті твіти й повідомлення можуть раптом стати публічними.

Для сьогоднішньої молоді — так званого «покоління Z» — фейсбук і твітер уже стали минулим століттям. Нове покоління прив'язане до телефонів із WhatsApp (який, за іронією долі, тепер належить Facebook), Snapchat (не належить Facebook), а також Instagram та Instagram Stories (знову Facebook). Завдяки цим застосункам можна постити фото й відео.

Інстаґрам — це застосунок для обміну фотографіями й відео, такий собі фейсбук для молодшої аудиторії. З його допомогою можна підписуватися на користувачів, ставити лайки і відправляти повідомлення. В інстаґрама також є умови надання послуг, а компанія жваво реагує на прохання прибрати контент, захищений авторським правом.

Снепчат (може, тому, що він не належить Facebook) найдивніший із цієї трійки. Застосунок збудував репутацію на тому, що допомагає відправляти фотографії, які самознищуються. Світлини живуть недовго — десь дві секунди.

Достатньо, щоб одержувач встиг їх побачити. На жаль, двох секунд достатньо і для того, щоб швиденько зробити скріншот і зберегти фото.

Взимку 2013 року дві неповнолітні старшокласниці з Нью-Джерсі сфотографувалися оголеними і відправили фото хлопцеві з їхньої школи в снепчаті. Дівчата були впевнені, що зображення автоматично видалиться через дві секунди після перегляду. Принаймні в цьому їх запевнила компанія.

Проте хлопець знав, як зробити скріншот повідомлення в снепчаті, який потім завантажив собі в інстаґрам. А інстаґрам не видаляє фотографії через дві секунди. Зайве казати, що фото оголених дівчат розвірусилося, і адміністраторові школи довелося звертатися до батьків інших учнів із проханням видалити фото з телефонів дітей, щоб не нарватися на звинувачення в зберіганні дитячої порнографії. Неповнолітніх учасників інциденту не могли засудити за злочин через вік, тому призначили дисциплінарні заходи в шкільному окрузі[168].

І не лише дівчата надсилають оголені фото хлопчикам. У Британії чотирнадцятирічний хлопчик відправив свою оголену світлину дівчині з його школи через снепчат, знову ж таки сподіваючись, що зображення зникне за кілька секунд. Однак дівчина зробила скріншот... решту історії ви вже знаєте. За даними BBC, і хлопчика, і дівчинку внесуть до бази даних сексуальних злочинців, хоча й не можуть притягнути їх до відповідальності через юний вік[169].

Як і вотсап зі своєю суперечливою функцією розмиття зображень, снепчат, незважаючи на обіцянки, насправді не видаляє фото. У 2014 році Snapchat навіть погодився зі звинуваченнями Федеральної торгової комісії в тому, що компанія збрехала користувачам про повідомлення, що зникають, які, за твердженнями федерального агентства, можна зберегти чи відновити[170]. У політиці конфіденційності снепчата також зазначено, що компанія не відстежує геолокації вашого пристрою і не має жодного доступу до цієї інформації, але Федеральна торгова комісія також заперечила ці заяви[171].

Усі онлайн-сервіси дозволяють реєструватися лише користувачам, яким виповнилося тринадцять років. Ось чому під час реєстрації у вас запитують дату народження. Але ви можете легко заприсягтися, що вам більше тринадцяти років. Або вісімнадцяти. Байдуже, ви ж не під присягою. Батьки, які помітили, що їхня десятирічна дитина має акаунт у снепчаті чи фейсбуці, можуть звернутися з проханням видалити обліковий запис. Але є і батьки, які дозволяють дітям користуватися соцмережами і самі змінюють їхню дату народження. Ці дані стають частиною профілю дитини. Раптово вашій десятирічній дитині виповнюється чотирнадцять, а сайт починає видавати їй рекламу, орієнтовану на дітей старшого віку. І не забувайте, що кожен імейл і кожна фотографія, яку розмістить дитина на сайті, залишиться там назавжди.

А ще снепчат передає своєму провайдерові з аналітики інформацію про геолокацію користувачів Android, отриману через Wi-Fi і стільникові бази. Якщо у вас айфон і ви вводите свій номер телефону для пошуку друзів, снепчат

зберігає імена та номери усіх контактів у телефонній книзі без вашого відома або згоди, хоча й iOS запросить дозвіл при першому запиті. Якщо прагнете до справжньої конфіденційності, раджу спробувати інший застосунок.

У Північній Кароліні старшокласникові і його дівчині висунули звинувачення в зберіганні оголених фотографій неповнолітніх, хоча й фотографували вони самі себе і за обопільною згодою. Дівчині висунули два звинувачення в сексуальній експлуатації неповнолітнього: одне за зйомку, інше — за зберігання фотографій. Якщо не брати до уваги моральний бік питання, висновок такий: у Північній Кароліні підлітки не мають права фотографувати себе ж в оголеному вигляді і зберігати ці фото. У поліції дівчина одночасно значиться і як жертва, і як злочинець.

Хлопцеві висунули аж п'ять звинувачень: по два за кожне селфі плюс одне за зберігання фото дівчини. Йому загрожує до десяти років ув'язнення і статус сексуального злочинця до кінця життя. І все через те, що сфотографував себе голим і зберіг фотографію, яку надіслала йому його ж дівчина[172].

Коли мені в школі подобалася дівчина, я просто запрошував її на побачення. Сьогодні ж доводиться викладати інформацію про себе в інтернет, щоб люди могли заздалегідь про вас почитати і вирішити. Але будьте обережні.

Якщо ви зареєстровані на сайті знайомств і заходите на нього з чужого або громадського комп'ютера, завжди виходьте з акаунта. Я не жартую. Навряд чи вам захочеться, щоб хтось натиснув у браузері кнопку «Назад» і побачив вашу анкету. Або змінив її. Крім того, не забудьте зняти прапорець із «Запам'ятати мене» при вході в систему. Інакше хтось інший зможе зайти у ваш акаупт із чужого комп'ютера.

Скажімо, у вас із людиною перше побачення. Може друге. Мало хто може розкусити людину на першій чи другій зустрічі. А після того як ваша пасія додасть вас у друзі у фейсбуці, твітері чи в будь-якій іншій соцмережі, вона дістане доступ до всіх ваших друзів, фотографій, інтересів... усе може полетіти шкереберть за мить.

Що ж, ми розглянули онлайн-сервіси. А як щодо мобільних застосунків?

Застосунки для знайомств можуть транслювати вашу геолокацію, при чому часто за замовчуванням. Приміром, вам сподобався хтось у вашому місті: через застосунок ви можете дізнатися, чи поблизу ця людина. Мобільний застосунок для знайомств Grindr дає дуже точну інформацію про місцеперебування для своїх користувачів... занадто точну.

Дослідники Колбі Мур і Патрік Вордл із компанії з кібербезпеки Synack змогли підробити запити в Grindr, щоб стежити за пересуваннями по місту конкретних людей. Також виявилося, що якщо стежити за тією самою людиною з трьох акаунтів, можна деталізувати карту і точніше визначити, де перебуває жертва в конкретний час[173].

Можливо, застосунки для знайомств — це не ваше. Але навіть акаунт у Yelp для пошуку ресторану дає стороннім компаніям інформацію про вашу стать, вік

і місцеперебування. Налаштування за замовчуванням дозволяють програмі відправляти інформацію назад до ресторану: приміром, ваш заклад продивлялася жінка, тридцять один рік, Нью-Йорк. Однак завжди можна зайти в налаштування і вибрати «Основне» — так визначатиметься лише ваше місто (на жаль, відключити цю функцію повністю неможливо)[174]. Думаю, найкращий вихід — не реєструвати акаунт і користуватися Yelp анонімно.

Що стосується геолокації, не зайвим буде перевірити, чи не транслює раптом якийсь застосунок ваше місцеперебування. Зазвичай цю функцію можна відключити — в окремому застосунку або повністю на телефоні[175].

І ще: перш ніж погодитися на завантаження будь-якого застосунку на Android, завжди спершу прогляньте дозволи. Зробити це можна в Google Play: відкрийте сторінку застосунку, натисніть «Докладніше» і знайдіть «Дозволи». Якщо вам не подобаються дозволи або здається, що в розробника програми занадто багато контролю, не завантажуйте застосунок. Apple про свої застосунки аналогічної інформації не надає: замість цього запит на кожен дозвіл вискакує в міру потреби. Якщо чесно, мені більше подобаються пристрої на iOS, бо операційна система завжди надсилає запит перед розкриттям приватної інформації, як-от мої дані геолокації. Крім того, iOS набагато безпечніша, ніж Android, якщо ви не робили джейлбрейк. Ясна річ, заможні зловмисники можуть придбати експлойти для будь-якої операційної системи на ринку, але експлойти для iOS коштують дуже дорого — понад мільйон доларів[176].

147 Перефразована цитата американського бізнесмена Скотта Макнілі: «У вас все одно жодної приватності. Змиріться». — *Прим. пер.*

148 http://www.wired.com/2012/12/ff-john-mcafees-last-stand/.

149 http://defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/.

150 http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-privacy.

151 http://www.dailymail.co.uk/news/article-3222298/Is-El-Chapo-hiding-Costa-Rica-Net-closes-world-s-wanted-drug-lord-hapless-son-forgets-switch-location-data-Twitter-picture.html.

152 https://threatpost.com/how-facebook-and-facial-recognition-are-creating-minority-report-style-privacy-meltdown-080511/75514.

153 http://www.forbes.com/sites/kashmirhill/2011/08/01/how-face-recognition-can-be-used-to-get-your-social-security-number/2/.

154 http://searchengineland.com/with-mobile-face-recognition-google-crosses-the-creepy-line-70978.

155 Robert Vamosi, When Gadgets Betray Us: The Dark Side of Our Infatuation with New Technologies (New York: Basic Books, 2011).

156 http://www.forbes.com/sites/kashmirhill/2011/08/01/how-face-recognition-can-be-used-to-get-your-social-security-number/.

157 https://techcrunch.com/2015/07/13/yes-google-photos-can-still-sync-your-photos-after-you-delete-the-app/.

158 https://www.facebook.com/legal/terms.

159 http://www.consumerreports.org/cro/news/2014/03/how-to-beat-facebook-s-biggest-privacy-risk/index.htm.

160 http://www.forbes.com/sites/amitchowdhry/2015/05/28/facebook-security-checkup/.

161 http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm.

162 http://www.cnet.com/news/facebook-will-the-real-kevin-mitnick-please-stand-up/.

163 http://www.eff.org/files/filenode/social_network/training_course.pdf.

164 http://bits.blogs.nytimes.com/2015/03/17/pearson-under-fire-for-monitoring-students-twitter-posts/.

165 http://www.washingtonpost.com/blogs/answer-sheet/wp/2015/03/14/pearson-monitoring-social-media-for-security-breaches-during-parcc-testing/.

166 http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0513/Is-student-privacy-erased-as-classrooms-turn-digital.

167 https://motherboard.vice.com/en_us/article/78857e/so-were-sharing-our-social-security-numbers-on-social-media-now.

168 http://pix11.com/2013/03/14/snapchat-sexting-scandal-at-nj-high-school-could-result-in-child-porn-charges/.

169 http://www.bbc.co.uk/news/uk-34136388.

170 https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

171 http://www.informationweek.com/software/social/5-ways-snapchat-violated-your-privacy-security/d/d-id/1251175.

172 http://fusion.net/story/192877/teens-face-criminal-charges-for-taking-keeping-naked-photos-of-themselves/.

173 http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-privacy.

174 http://fusion.net/story/141446/a-little-known-yelp-setting-tells-businesses-your-gender-age-and-hometown/?utm_source=rss&utm_medium=feed&utm_campaign=/author/kashmir-hill/feed/.

175 На айфоні чи айпаді зайдіть у Налаштування>Конфіденційність>Служби геолокації і знайдіть список усіх застосунків, що підтримують геолокацію. Наприклад, можна вручну відключити геолокацію на Facebook Messenger. Прокрутіть до «Facebook Messenger» і встановіть для сервісів геолокації варіант «Ніколи». На пристроях на базі Android відкрийте застосунок Facebook Messenger, натисніть значок «Налаштування» (у формі шестерні) у правому верхньому кутку, прокрутіть до «Нові повідомлення включають вашу геолокацію за замовчуванням» і зніміть прапорець. Узагалі на Android доведеться вручну відключати геолокацію на всіх застосунках (якщо сам застосунок дозволяє). Немає єдиного налаштування.

176 https://blog.lookout.com/blog/2016/08/25/trident-pegasus/.

Розділ 10

Фітнес незавжди приносить користь

Якщо ви (як і всі ми) завжди і всюди тягаєте із собою мобільний телефон, то забудьте про невидимість. За вами спостерігають, навіть якщо відстеження геолокації на телефоні не увімкнене. Приміром, якщо у вас на айфоні iOS 8.2 чи більш рання версія, Apple відключатиме GPS у режимі польоту. Але якщо ви оновили версію, без додаткових маніпуляцій з вашого боку, GPS залишиться ввімкненим навіть у режимі польоту[177]. Щоб з'ясувати, наскільки мобільний оператор проникнув у повсякденне життя, відомий німецький політик Мальте Шпіц подав позов проти оператора, і суд Німеччини зобов'язав компанію віддати всі записи. Їх обсяг просто вражає. Протягом якихось шести місяців вони отримували інформацію про місцеперебування політика 85 тисяч разів, а також відстежували кожен вхідний і вихідний дзвінок, номер телефону співрозмовника і тривалість розмови. Інакше кажучи, вони отримували метадані з телефона Шпіца. І стосувалося це не лише дзвінків: SMS-повідомлення також потрапили під приціл[178].

Шпіц зв'язався і з іншими організаціями, попрохавши їх обробити й оприлюднити його дані. Одна з компаній щодня писала звіти на зразок того, що наведено нижче. Місце проведення ранкової зустрічі Партії зелених визначили за широтою й довготою, зазначеними в записах телефонної компанії.

Понеділок, 12 жовтня 2009 року

Ранок: чотиригодинна зустріч ради директорів Партії зелених у штаб-квартирі в Берліні, розташованій за адресою: Platz vor dem Neuen, Tor 1.

1 вхідний дзвінок
10 вихідних дзвінків
Загальний час розмов: 0 годин 33 хвилини 24 секунди

16 вхідних повідомлень
14 вихідних повідомлень

Тривалість інтернет-під'єднання:
16 годин 40 хвилин 54 секунди

Активність Мальте Шпіца за 12 жовтня 2009 року

На основі цих даних інша організація створила анімовану карту, яка показує пересування Шпіца всією Німеччиною, вона оновлюється щохвилини і миготить щоразу, як Шпіц отримує чи робить дзвінок. Дивовижний рівень деталізації повсякденного життя[179].

Ясна річ, ситуація зі Шпіцом не є унікальною і не обмежується кордонами Німеччини. Це просто яскравий приклад того, які дані отримує ваш мобільний оператор. Дані, якими можна скористатися в суді.

У 2015 році в Апеляційному суді США розглядали справу на основі аналогічних записів із мобільного телефона. У справі фігурували двоє крадіїв, які пограбували банк, магазин, кілька ресторанів швидкого харчування і ювелірну крамницю в Балтиморі. Отримавши від оператора Sprint дані про геолокацію телефонів головних підозрюваних за попередній 221 день, поліція змогла пов'язати злочинців із цілою серією пограбувань — як за відносною близькістю пограбованих місць, так і за близькістю до цих місць підозрюваних[180].

Ще одна справа, під юрисдикцією Окружного суду США в Північному окрузі штату Каліфорнія, теж стосувалася «історичної інформації про місцеперебування стільникового телефона» в базах Verizon і AT&T (уточнювати деталі злочину не буду). За словами Американської спілки захисту громадянських свобод, яка подала експертний висновок у справі, ці дані свідчать про «майже безперервний запис місцеперебування і переміщення людини». Коли федеральний суддя нагадав про конфіденційність користування мобільними телефонами у штаті Каліфорнія, федеральний прокурор запропонував абонентам, «які дбають про свою конфіденційність, взагалі не носити з собою телефонів або їх вимикати». Слова з офіційного звіту.

Це безпосередньо порушує наше право на захист від необґрунтованих обшуків за четвертою поправкою. Більшість людей навіть не здогадається якось пов'язати телефон у кишені зі стеженням уряду, але в наші дні саме так усе й відбувається. Зверніть увагу, що ні Verizon, ні AT&T, ні Sprint не роз'яснюють клієнтам у політиці конфіденційності масштаби відстеження геолокації. AT&T взагалі заявили в листі Конгресу від 2011 року, що зберігають стільникові дані протягом п'яти років «на випадок спорів щодо оплати послуг»[181].

А ще дані геолокації зберігають не лише оператори, а й сервіси. Наприклад, у вашому Google-акаунті зберігаються всі дані геолокації на Android. Якщо ж у вас айфон, не хвилюйтеся: Apple теж має доступ до даних. Щоб запобігти переглядові інформації на самому девайсі і резервному копіюванню в «хмару», періодично видаляйте дані геолокації зі смартфона. На Android перейдіть у Налаштування > Google >Місцеперебування >Видалити історію місцеперебування. А от з iOS все не так просто: доведеться трохи попітніти. Перейдіть у Налаштування>Конфіденційність>Служби геолокації, прокрутіть вниз до «Системних служб», потім — до «Часто відвідувані місця», а там уже натисніть «Очистити нещодавню історію».

Якщо ця функція Google у вас не відключена, на основі даних геолокації можна реконструювати ваш маршрут. Наприклад, більшу частину дня ви провели в одному місці, але видно періодичні сплески руху — зустрічі з клієнтами чи обід десь поблизу роботи. Лякає те, що варто комусь дістати доступ до вашого акаунта в Google чи Apple — і він зможе визначити, де ви живете і хто ваші друзі. Або принаймні вивчити ваш розпорядок дня. І все це на основі інформації про те, де ви проводите більшу частину часу.

* * *

Думаю, ви зрозуміли, що навіть звичайна прогулянка загрожує вам стеженням. Приміром, ви про це знаєте і свідомо залишили мобільний телефон вдома. Це ж має вирішити проблему, так? Почасти.

Чи носите ви якийсь фітнес-браслет, приміром, від Fitbit, Jawbone UP або Nike+ FuelBand? Якщо ні, то, можливо, розумний годинник від Apple, Sony або Samsung? Якщо у вас на руці якийсь із цих девайсів, то вас усе ще можна відстежити. Ці пристрої та відповідні застосунки призначені для запису вашої активності, часто на основі GPS. Тож байдуже, транслюється ця інформація відразу чи обробляється пізніше: за вами все ще можна спостерігати.

Слово «підгляд» (sousveillance), придумане захисником конфіденційності Стівом Манном, є каламбуром від слова «нагляд» (surveillance). Англійський варіант походить з французької: слово «sur» означає «над», «sous» — «під». Так, «підгляд» означає, що за вами спостерігають не зверху (інші люди або камери безпеки), а знизу, через крихітні пристрої, які ми всюди тягаємо із собою і, може, навіть носимо на тілі.

Фітнес-трекери й розумні годинники записують біометричні дані на зразок серцевого ритму, кількості пройдених кроків, навіть температури тіла. В App Store можна знайти безліч самостійних розробок для відстеження самопочуття через телефони й годинники. Та сама історія і з Google Play. І — який сюрприз! — ці застосунки запрограмовані передавати всі дані компанії. Нібито для того, щоб зібрати докупи інформацію для вас же, але вони можуть і поширити дані. Іноді навіть без вашої згоди.

Наприклад, учасники велоперегонів Амджен Тур у Каліфорнії 2015 року могли стежити за тим, хто їх обійшов, а після заїзду написати їм повідомлення. Трохи моторошно, коли незнайомець починає говорити про якийсь ваш рух під час гонки, який ви навіть не пам'ятаєте.

Таке сталося і зі мною. Дорогою з Лос-Анджелеса до Лас-Вегаса мене підрізав хлопець на BMW. Він розмовляв по телефону й раптово перешикувався в мій ряд за кілька сантиметрів від мене, налякавши мене до чортиків. Він ледве не вбив нас обох.

Я схопив телефон і зателефонував в автотранспортне управління, видавши себе за правоохоронця. Вони пробили його номери по базі й видали мені ім'я, адресу та номер соціального страхування. Потім я зателефонував операторові Airtouch Cellular, прикинувшись їхнім співробітником, і попросив пошукати за номером соціального страхування його обліковий запис. Ось як мені вдалося отримати його номер мобільного.

Уже за п'ять хвилин після того, як цей дурень мене підрізав, я до нього додзвонився. Я все ще тремтів від злості і волав у слухавку: «Слухай сюди, йолопе! Ти мене підрізав п'ять хвилин тому і майже не вбив нас обох. Я з автотранспортного управління, і якщо ти ще хоч раз викинеш такий фінт, я заберу в тебе водійське посвідчення!».

Він, мабуть, досі ламає голову над тим, як незнайомий хлопець просто в дорозі дістав його номер. Сподіваюся, дзвінок достатньо його налякав, і той став керувати уважніше. Але ніколи не знаєш напевно.

Однак що посієш, те й пожнеш. Якось мій мобільний акаунт у AT&T зламали методами соціальної інженерії якісь хакери-недоучки. Вони зателефонували в магазин AT&T і видали себе за співробітників іншого фірмового магазину. Хакери змогли переконати адміністратора скинути адресу електронної пошти від мого акаунта в AT&T, після чого змогли спокійно змінити пароль і дістати доступ до всіх моїх реквізитів, включно з рахунками!

Під час велоперегонів гонщики користувалися застосунком Strava Flyby, щоб за замовчуванням ділитися особистими даними з іншими користувачами застосунку. В інтерв'ю з Forbes Ґарет Неттлтон, директор міжнародного маркетингу в Strava, заявив: «Strava є відкритою платформою, яка допомагає спортсменам стати частиною всесвітнього співтовариства. Однак конфіденційність наших спортсменів для нас дуже важлива, тож ми вжили всіх заходів, щоб спростити для користувачів управління їхньою приватністю»[182].

Strava пропонує розширені налаштування конфіденційності, які дають вам змогу регулювати, хто може і не може бачити ваш серцевий ритм. Ви також можете встановити для застосунку конфіденційні зони, щоб інші користувачі не змогли дізнатися, де ви живете чи працюєте. Під час туру Амджен Тур у Каліфорнії користувачі могли вимкнути функцію Flyby: так усі їхні дії позначалися як «приватні».

Інші фітнес-трекери й відповідні застосунки мають подібний захист конфіденційності. Вам може здаватися, що якщо ви професійно велоспортом не займаєтеся і нікого на доріжці для бігунів біля роботи підрізати не збираєтеся, то й захист вам не потрібний. Що в цьому страшного? Але в інтернет через застосунок можуть потрапити й інші ваші повсякденні дії, іноді досить приватного характеру. А це вже створює певні проблеми.

Сам собою запис сну чи ходьби по сходах, особливо якщо це робиться з оздоровчою метою (приміром, щоб зменшити внески за медичне страхування), навряд чи поставить під загрозу вашу конфіденційність. Однак якщо поєднати ці дані з іншими, вимальовується цілісна картина. І вона може розповісти про вас більше, ніж вам хотілося б.

Один власник фітнес-трекера переглянув свої онлайн-дані і зауважив значне підвищення частоти серцевих скорочень щоразу, коли займався сексом[183]. І справді, компанія Fitbit якось мимохідь перерахувала список дій, які регулярно реєструються. Серед них був і секс. Хоча дані були анонімними, їх все одно можна було знайти через ґуґл, поки компанія не почала отримувати скарги і не прибрала функцію[184].

Хтось може подумати: «Ну й що тут такого?». Ваша правда: сама собою інформація не дуже цікава. Але якщо поєднати дані серцевого ритму із, скажімо, даними геолокації, стає не до жартів. Журналістка сайту Fusion Кашмір Гілл припустила найгірший сценарій для даних Fitbit: «А що як страхові компанії поєднають дані вашої активності з даними геолокації GPS і дізнаються не лише те, коли у вас, ймовірно, був секс, але й де? Чи може медична страхова компанія вирахувати клієнта, який протягом тижня займався сексом у кількох місцях, і присвоїти цій людині профіль вищого медичного ризику, спираючись на її потенційно безладні статеві стосунки?»[185].

З іншого боку, даними Fitbit успішно користуються в судах для доведення або спростування позовів, які неможливо підтвердити інакше. Якщо брати найяскравіші випадки, то якось дані Fitbit допомогли довести, що жінка збрехала про зґвалтування[186].

За словами жінки, яка звернулася до поліції Ланкастера, штат Пенсильванія, вона прокинулася приблизно опівночі, коли на неї заліз незнайомець. Також вона стверджувала, що намагалася звільнитися і в боротьбі втратила Fitbit-браслет. Коли поліція знайшла браслет, а жінка дозволила зчитати дані, девайс розповів зовсім іншу історію. Насправді жінка не лягала спати і просто гуляла всю ніч. За даними місцевого телеканалу, жінку звинуватили в хибних свідченнях поліції і фальсифікації доказів: вона перевернула меблі й підкинула ніж на «місце злочину», щоб виставити себе жертвою зґвалтування[187].

А ще трекерами можна скористатися для підкріплення заяв про інвалідність. Канадська юридична фірма скористалася даними трекера активності, щоби довести тяжкі наслідки виробничої травми клієнта. Клієнт надав записи компанії Vivametrica, яка збирає дані з портативних пристроїв і порівнює їх із даними активності і здоров'я населення загалом. Дані Fitbit демонстрували помітне зниження активності клієнта. «Раніше нам доводилося покладатися лише на медичні аналізи, — сказав Forbes Саймон Мюллер із фірми McLeod Law у Калґарі. — Тепер же ми бачимо триваліші періоди активності протягом дня. У нас є точні дані»[188].

Навіть якщо у вас нема фітнес-трекера, розумний годинник на зразок Galaxy Gear від Samsung може так само поставити під загрозу вашу конфіденційність. Якщо ви отримуєте на свій зап'ясток швидкі повідомлення (SMS, імейли, телефонні дзвінки), інші також можуть їх прочитати або прослухати.

Останнім часом спостерігається ще й стрімке зростання популярності GoPro — крихітної камери, яка прикріплюється до шолома чи панелі приладів автомобіля і записує на відео ваші дії. Але що трапиться, якщо ви забудете пароль до мобільного застосунку GoPro? Ізраїльський дослідник позичив у свого друга GoPro і відповідний застосунок, але не спитав пароля. Застосунок GoPro, як і електронна пошта, дає змогу скинути пароль. Однак процедура зміни пароля (яку згодом змінили) мала прогалини. Під час скидання пароля GoPro відправляв на ваш імейл посилання, що вело до ZIP-файлу, який треба було завантажити на SD-карту девайса. Відкривши отриманий ZIP-файл, дослідник знайшов текстовий документ із назвою «Налаштування», який містив бездротові дані користувача, зокрема SSID і пароль, через який GoPro з'єднується з інтернетом. Виявилося, що якщо замінити в посиланні номер 8605145 на якийсь інший (скажімо, 8604144), можна дістати доступ до даних конфігурації чужого GoPro, де містяться паролі.

Можна сміливо стверджувати, що тема конфіденційності в Америці почалася (або принаймні стала популярною) наприкінці XIX століття з компанії Eastman Kodak. До того часу фотографія була складним, трудомістким і вкрай незручним мистецтвом, що вимагало спеціалізованого обладнання (камера, світло, темна кімната) й обмежувало пересування (люди позували лише в студіях). А потім з'явився Kodak і презентував портативну й відносно доступну камеру. Перша серія розійшлася по 25 доларів — сучасні 100 баксів з урахуванням інфляції. Згодом компанія розробила нову камеру Brownie, яка коштувала лише долар. Обидві камери були призначені для зйомки поза приміщенням. Такі собі портативні комп'ютери чи мобільні телефони тих часів.

Раптово люди зіткнулися з тим, що будь-хто з камерою на пляжі чи в громадському парку може захопити їх у кадр. Треба було завжди мати вигляд на всі сто. Завжди бути обережним. «Змінилося не лише ставлення до фотографії, а й ставлення до об'єкта фотографії, — каже Брайан Волліс, колишній головний куратор Міжнародного центру фотографії. — Доводилося влаштовувати "театральні" вечері та дні народження»[189].

Думаю, ми дійсно поводимося інакше, коли за нами спостерігають. Коли ви під прицілом камери, то намагаєтеся мати якомога кращий вигляд, на весь свій максимум. Хоча, звісно ж, є й такі, кому начхати.

Поява фотографії також вплинула на ставлення до приватного життя. Тепер вашу погану поведінку могли несподівано зафіксувати на камеру. Так, сьогодні в автомобілях у нас відеореєстратори, а на поліцейських — портативні камери. Тож якщо ми порушимо закон, усе це зафіксують на відео. Так, сьогодні ви можете сфотографувати перехожого і через програму розпізнавання облич знайти його сторінку на фейсбуці. Так, сьогодні в нас є селфі.

Але 1888 року постійний ризик потрапити під приціл камери був шокуючою, тривожною дивиною. Газета Hartford Courant одразу забила тривогу: «Мирні громадяни тепер не можуть розважитися, не ризикуючи бути спійманими на гарячому. Не боячись того, що фотографії розлетяться серед їхніх дітей у недільній школі. А молодий хлопець, який хоче помилуватися з дівчиною, пливучи на човні річкою, тепер повинен постійно ховатися під парасолькою»[190].

Декому не сподобалися зміни. У 1880-х у США кілька жінок розбили в потязі чужу камеру, бо не хотіли, щоб власник їх фотографував. У Великобританії кілька хлопців об'єдналася в групу й пішли патрулювати пляжі, погрожуючи всім, хто намагався сфотографувати жінок після купання.

У 1890-х Семюел Воррен і Луї Брендайс (який згодом отримав роботу у Верховному суді США) у спільній статті написали, що «миттєві фотографії та видавці газет вторглися у священні кордони приватного й сімейного життя». Вони заявили, що законодавство США повинно офіційно визнати недоторканність приватного життя і накласти відповідальність за будь-яке вторгнення в нього, стримавши поширення таємної фотографії[191]. Такі самі закони згодом прийняли в кількох штатах.

Уже кілька поколінь виросло на відчутті загрози миттєвих фотографій. Хтось пам'ятає полароїди? А тепер нам доводиться боротися з повсюдністю фотографії. Хоч би куди ви пішли, завжди є ризик потрапити на відео, хочете ви цього чи ні. І його зможе побачити будь-хто, у будь-якій точці світу.

Конфіденційність у нашому житті — суцільне протиріччя. З одного боку, ми її невимовно цінуємо, вважаємо правом і бачимо невід'ємною частиною свободи та незалежності. Хіба те, що ми робимо в себе вдома, за зачиненими дверима, не має залишатися приватним? З іншого боку, люди — істоти допитливі. І тепер у нас є всі можливості задовольнити цікавість нечуваними раніше способами.

Ніколи не замислювалися, що там за парканом через дорогу, на задньому дворі сусіда? Відповідь вам майже у 100 % випадків дадуть сучасні технології. Компанії на зразок 3D Robotics чи CyPhy зробили безпілотні дрони доступними будь-якому середньостатистичному громадянинові (приміром, у мене є дрон DJI Phantom 4). Дрони — це невеликі літальні апарати з дистанційним управлінням, значно складніші за модельки, що ви купували в дитинстві у RadioShack. Майже всі вони оснащені крихітними відеокамерами. Дрони дають вам можливість побачити світ із нового ракурсу. Деякими можна взагалі управляти зі смартфона.

Особисті дрони — новий рівень підглядання. Майже ніщо не сховається від ваших очей, коли ви здатні парити в десятках метрів над землею.

Дрони зараз широко використовуються в страховій сфері. Лише уявіть: ви — страховий аджестер, і вам потрібно оцінити стан майна, яке ви збираєтеся застрахувати. З дроном ви здатні кружляти навколо будинку, візуально оглядаючи місця, до яких раніше у вас доступу не було, і фіксуючи на камеру всі недоліки, які помітите. З дроном ви отримуєте ракурс, який раніше був доступний лише з гелікоптера.

Ми ж з вами тепер можемо шпигувати за сусідами: просто запустіть дрон над чужим будинком і подивіться вниз. Можливо, у сусіда є басейн. Можливо, сусід любить купатися голяка. Ми зайшли в глухий кут: прагнемо до приватності у власних будинках і на власній території, але тепер ця приватність під питанням. Приміром, Google маскує обличчя, номерні знаки й іншу особисту інформацію в Google Street View і Google Earth... але сусід із дроном усе це перекреслює (хоча можна ввічливо попрохати його не літати над вашим подвір'ям). Особистий дрон із камерою — це як Google Earth і Google Street View в одному флаконі.

Однак законом це певною мірою регулюється. Наприклад, Федеральне управління цивільної авіації США забороняє, щоб дрон покидав поле зору оператора, літав надто близько до аеропортів і на висоті понад встановлений рівень[192]. Є застосунок під назвою B4UFLY, який вкаже вам, куди може літати ваш дрон[193]. А через поширення комерційних дронів кілька штатів ухвалили закони, що частково або повністю обмежують їх використання. У Техасі звичайні громадяни не можуть керувати дронами, хоча є й винятки (приміром, агенти з нерухомості). Найбільш ліберальне ставлення до дронів, мабуть, у Колорадо, де цивільні особи можуть вільно запускати своїх дронів у небо.

Уряд США як мінімум повинен зобов'язати любителів дронів реєструвати свої іграшки. У Лос-Анджелесі, де я живу, хтось влетів дроном у лінії електропередач у Західному Голлівуді, неподалік від перехрестя вулиці Ларрабі й бульвару Сансет. Якби дрон був зареєстрований, правоохоронці могли б легко визначити, хто наробив проблем семистам мешканцям і десяткам працівників енергетичної компанії, які гарували вночі кілька годин поспіль, щоб відновити живлення району.

Чимало магазинів хочуть знати про своїх клієнтів якомога більше. Один із дієвих способів зібрати інформацію — IMSI-перехоплювач (див. розділ 13). Коли ви заходите до магазину, перехоплювач чіпляє дані з вашого телефона і якось вираховує номер мобільного. З цією інформацією система здатна проглянути купу баз даних і створити ваш профіль. А ще магазини активно користуються технологією розпізнавання облич. Уявіть собі всюдисущу версію того консультанта, що вітає вас на вході до Walmart.

Думаю, у недалекому майбутньому я чутиму «Привіт, Кевіне» від консультантів на кожному кроці. Навіть якщо до цього я в їхньому магазині ніколи не був. Персоналізація шопінгу — ще одна, хоча і ледве помітна, форма нагляду. Ми вже не здатні робити покупки анонімно.

У червні 2015 року Конгрес ухвалив Акт «Про свободу США» — доопрацьовану версію «Патріотичного акту» з новими положеннями про конфіденційність. Але не минуло й двох тижнів, як дев'ять організацій із захисту конфіденційності споживачів, які активно лобіювали прийняття акта, уже встигли розчаруватися в кількох великих ритейлерах і виступили з вимогою обмежити використання технологій розпізнавання обличчя[194].

На порядку денному стояло питання про те, чи повинні в споживачів запитувати дозвіл перед скануванням. Звучить розумно, але жодна з торгових компаній, які брали участь у переговорах, на це не пристала. За їхніми словами, якщо покупець зайшов у їхній магазин, вони мають повне право його просканувати й ідентифікувати[195].

Може, деякі й не проти такої уваги до їхньої персони, але багатьох це просто виб'є з колії. Ритейлери ж дивляться на це по-іншому. У такий спосіб магазини намагаються зловити крадіїв. Якщо люди зможуть відмовитися від спостереження, то злодії неодмінно скористаються цим правом. А от із автоматичною технологією розпізнавання облич крадіїв зі стажем ідентифікують просто на вході в магазин.

Що думають покупці? Приміром, у Британії сім із десяти респондентів вважають технологію розпізнавання в магазині «занадто моторошною»[196]. А в США деякі штати (приміром, Іллінойс) взяли на себе процес збору і зберігання біометричних даних[197]. Це потягнуло за собою низку судових позовів. Приміром, мешканець Чикаго подав у суд на Facebook, бо не давав сайтові дозволу на розпізнавання його обличчя на чужих фотографіях[198].

Технологією розпізнавання облич користуються для того, щоб ідентифікувати людину по фотографії. Але що як ви вже знаєте людину на фото і просто хочете простежити, що вона «відмітилася» в потрібному місці? От вам ще одне потенційне використання технології.

Моше Ґріншпан є генеральним директором Face-Six — ізраїльської компанії з офісом у Лас-Вегасі, яка займається технологією розпізнавання обличчя. Їхня програма Churchix дуже популярна серед церков, які стежать за відвідуванням своїх прихожан через камери. Програма допомагає визначити, які прихожани відвідують церкву нерегулярно, а які стабільно, щоб спонукати перших приходити частіше, а других — жертвувати більше грошей церкві.

Розробники Face-Six кажуть, що вже як мінімум тридцять церков у всьому світі користуються їхнім ПЗ. Потрібно лиш завантажити фотографії прихожан у високій якості — і система буде стежити за ними під час служб та інших соціальних подій.

Коли журналісти Fusion запитали Ґріншпана, чи розповідають церкви своїм прихожанам про стеження, той відповів: «Не думаю. Ми закликаємо церкви повідомляти це прихожанам, але навряд чи вони нас слухаються»[199].

Якось Джонатан Зіттрейн — директор Дослідницького центру інтернету й суспільства імені Беркманів при Гарвардській школі права — жартома припустив, що на людей треба вішати тег «nofollow»[200] — такий самий, як і на деякі веб-сайти.[201] Це б убезпечило людей, які не хочуть потрапляти в бази даних облич для розпізнавання. З цією метою Національний інститут інформатики в Японії розробив так званий «конфіденційний візор». Окуляри продаються приблизно за 240 доларів і випромінюють світло, яке сприймають лише камери. Фоточутливе світло закриває очі й перешкоджає розпізнаванню вашого обличчя. За словами перших тестувальників, окуляри працюють у 90 % випадків. Єдиний нюанс у тому, що ними не скористаєшся за кермом чи на велосипеді. Та й мають вони не надто модний вигляд. Але в громадському місці окуляри ідеально захищають ваше право на приватне життя[202].

Тож на вулиці ваша конфіденційність може опинитися під загрозою. Думаєте, у машині, вдома чи на роботі безпечніше? Та де там! У наступних розділах я поясню чому.

---

177 GPS в останніх версіях iOS можна вимкнути так: http://smallbusiness.chron.com/disable-gps-tracking-iphone-30007.html.

178 https://gigaom.com/2013/07/08/your-metadata-can-show-snoops-a-whole-lot-just-look-at-mine/.

179 http://www.zeit.de/datenschutz/malte-spitz-data-retention.

180 https://www.washingtonpost.com/local/public-safety/federal-appeals-court-that-includes-va-md-allows-warrantless-tracking-of-historical-cell-site-records/2016/05/31/353950d2-2755-11e6-a3c4-0724e8e24f3f_story.html.

181 http://fusion.net/story/177721/phone-location-tracking-google-feds/?utm_source=rss&utm_medium=feed&utm_campaign=/author/kashmir-hill/feed/.

182 http://www.forbes.com/sites/andyrobertson/2015/05/19/strava-flyby/?ss=future-tech.

183 http://fusion.net/story/119745/in-the-future-your-insurance-company-will-know-when-youre-having-sex/?utm_source=rss&utm_medium=feed&utm_campaign=/author/kashmir-hill/feed/.

184 http://thenextweb.com/insider/2011/07/04/details-of-fitbit-users-sex-lives-removed-from-search-engine-results/.

185 http://fusion.net/story/119745/in-the-future-your-insurance-company-will-know-when-youre-having-sex/?utm_source=rss&utm_medium=feed&utm_campaign=/author/kashmir-hill/feed/.

186 http://www.engadget.com/2015/06/28/fitbit-data-used-by-police/.

187 http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/.

188 http://www.theguardian.com/technology/2014/nov/18/court-accepts-data-fitbit-health-tracker.

189 http://www.smithsonianmag.com/innovation/invention-snapshot-changed-way-we-viewed-world-180952435/?all&no-ist.

190 https://books.google.com/books?id=SlMEAAAAMBAJ&pg=PA158&lpg=PA158&dq=%22The+kodak+has+added+a+new+terror+to+the+picnic%22&source=bl&ots=FLtKbYGv6Y&sig=YzE2BisTYejb1pT3vYhR2QlS3Cg&ved=0CCAQ6AEwAA#v=onepage&q=%22The%20koda&f=false.

191 http://www.smithsonianmag.com/innovation/invention-snapshot-changed-way-we-viewed-world-180952435/?no-ist=&page=2.

192 https://www.faa.gov/uas/media/Part_107_Summary.pdf.

193 https://www.faa.gov/uas/where_to_fly/b4ufly/.

194 http://www.slate.com/articles/technology/future_tense/2015/06/facial_recognition_privacy_talks_why_i_walked_out.html.

195 http://www.extremetech.com/mobile/208815-how-facial-recognition-will-change-shopping-in-stores.

196 http://www.retail-week.com/innovation/seven-in-ten-uk-shoppers-find-facial-recognition-technology-creepy/5077039.article.

197 http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

198 http://arstechnica.com/business/2015/06/retailers-want-to-be-able-to-scan-your-face-without-your-permission/.

199 http://fusion.net/story/154199/facial-recognition-no-rules/?utm_source=rss&utm_medium=feed&utm_campaign=/author/kashmir-hill/feed/.

200 Тег вказує пошуковим системам на те, що не потрібно переходити за посиланням й індексувати конкретну сторінку. — *Прим. пер.*

201 https://www.youtube.com/watch?v=NEsmw7jpODc.

202 http://motherboard.vice.com/read/glasses-that-confuse-facial-recognition-systems-are-coming-to-japan.

Розділ 11

Жучки на колесах

Дослідникам Чарлі Міллеру і Крісові Валашеку вже не раз доводилося відкривати автомобілі. Якось ці двоє відкрили «Тойоту пріус», однак до машини довелося підключитися напряму, сидячи на задньому сидінні. А от влітку 2015-го Міллерові й Валашеку вдалося перехопити керування «Джипа черокі», коли той мчав зі швидкістю 112 кілометрів за годину по шосе в Сент-Луїсі. Але в машині їх не було. Вони змогли керувати автомобілем дистанційно[203].

За кермом «Джипа» таки був водій — журналіст Wired Енді Ґрінберг. Дослідники заздалегідь попередили Ґрінберга: «Хоч би що сталося, не панікуй». Завдання виявилося не з легких. Навіть для хлопця, який знав, що його машину відкриють.

«Раптом перестав працювати акселератор, — згодом написав про це Ґрінберг. — Я відчайдушно тиснув на педаль газу, але оберти все збільшувалися. Спочатку автомобіль втратив половину швидкості, а потім узагалі ледь сунувся. Тоді я якраз виїхав на довжелезну естакаду. Звернути було просто нікуди. Експеримент уже не здавався таким веселим».

Після інциденту на дослідників посипалася критика їхніх «нерозумних» і «небезпечних» дій. «Джип» Ґрінберга був на громадській дорозі, а не на трасі для випробувань, тож на час написання цієї книжки правоохоронні органи штату Міссурі все ще висувають звинувачення проти Міллера, Валашека і навіть Ґрінберга.

Про дистанційний злам дискутують уже роками, однак саме експеримент Міллера і Валашека привернув увагу автопрому. Байдуже, було це лише спробою похизуватися чи повноцінним дослідженням. Головне, що експеримент змусив виробників автомобілів серйозно задуматися про кібербезпеку... і чи варто заборонити злам автомобілів на рівні закону[204].

Раніше дослідники вже доводили, що можуть перепрограмувати протокол управління транспортним засобом, перехопивши і проаналізувавши трафік GSM або CDMA, який надсилає ваш бортовий комп'ютер автовиробникові. Дослідники змогли обдурити систему управління, блокуючи та розблоковуючи двері автомобіля через SMS-повідомлення. Дехто в такий спосіб узагалі дістав можливість дистанційно завести машину. Але Міллер і Валашек стали першими, хто зміг отримати повний дистанційний контроль над автомобілем[205]. І вони стверджують, що так можуть керувати машинами навіть в інших штатах.

Думаю, найгучнішим результатом експерименту Міллера—Валашека стало відкликання понад 1,4 мільйона «Крайслерів» через проблеми програмування — перше таке відкликання в історії. А ще Chrysler негайно призупинили під'єднання незахищених автомобілів до телематичної мережі Sprint, через яку автомобілі обмінювалися зібраними даними з виробником у режимі реального

часу. На DEF CON 23 Міллер і Валашек заявили, що легко могли перехопити контроль транспортними засобами й в інших штатах, але розуміли, що це неетично. Замість цього вони з Ґрінбергом провели підконтрольний експеримент у рідному місті Міллера.

У цьому розділі я розповім, наскільки наші машини, потяги і мобільні додатки для пошуку вдалого маршруту уразливі до кібератак. Не кажучи вже про численні загрози конфіденційності, на які наражають нас власні автомобілі. Коли журналістка BuzzFeed Джоана Буйян приїхала до нью-йоркського офісу Uber на самому убері, на неї вже чекав генеральний менеджер Джош Морер. «А ось і ви, — привітався він із айфоном у руках. — Я тут стежив за вашим маршрутом». Не дуже вдалий початок інтерв'ю, яке тепер торкнулося ще й конфіденційності споживачів[206].

До статті Буйян, яка вийшла в листопаді 2014 року, мало хто за межами Uber знав про God View — інструмент, який відстежує місцеперебування тисяч водіїв і їхніх клієнтів у режимі реального часу.

Як я вже казав, застосунки час від часу запитують у користувачів різні дозволи, зокрема й право доступу до даних геолокації. Застосунок Uber пішов ще далі: він запитує ваше приблизне (через Wi-Fi) і точне (через GPS) місцеперебування, доступ до контактів, а також не дозволяє телефонові «заснути» (щоб стежити за тим, де ви перебуваєте).

Буйян заявила Морерові, що не давала компанії дозволу стежити за нею в будь-який час і в будь-якому місці. Насправді ж, давала. Просто не помітила цього. Дозвіл прописано в користувацькій угоді, яку вона прийняла під час завантаження застосунку на телефон. Після інтерв'ю Морер надіслав Буйян імейл із логами її нещодавніх поїздок на убері.

Uber збирає особисте досьє на кожного клієнта, записуючи кожну поїздку. Погана ідея, якщо база даних недостатньо захищена. Шпигуни всіх мастей — від уряду США до китайських хакерів — злітаються на базу даних Uber як мухи на мед[207].

У 2015 році компанія підкорегувала політику конфіденційності, і зовсім не на користь споживачів[208]. Uber тепер збирає дані геолокації всіх користувачів із США, навіть якщо застосунок працює у фоновому режимі, а супутниковий і стільниковий зв'язок вимкнено. Uber заявив, що для відстеження користувачів офлайн використовуватиме Wi-Fi та IP-адреси. А отже, застосунок Uber — мовчазний шпигун на вашому телефоні. До того ж компанія так і не пояснила, навіщо їй потрібна ця фупкція[209].

Як і те, навіщо потрібен God View. Хоча в політиці конфіденційності компанії прописано: «Uber має сувору політику, яка забороняє всім співробітникам на всіх рівнях доступ до даних клієнта чи водія. Єдиним винятком є обмежений перелік законних дій в інтересах бізнесу».

Законні дії можуть охоплювати моніторинг акаунтів, що підозрюються в шахрайстві, і розв'язання проблем із водіями (наприклад, втрачене з'єднання).

Очевидно, що сюди не входить стеження за маршрутом журналістів.

Думаєте, Uber дає клієнтам право видалити трекінгову інформацію? Аж ніяк. А тепер здогадайтеся, що трапиться, якщо ви видалите застосунок із телефона? Правильно, нічого. Дані все ще зберігатимуться в Uber[210].

Згідно з новою політикою конфіденційності Uber теж може збирати інформацію про вашу адресну книгу. Якщо у вас айфон, зайдіть у налаштування і змініть дозвіл для обміну контактами. А от із телефоном на Android це вже не спрацює.

Представники Uber заявили, що зараз компанія не збирає даних про контакти. Однак збір даних усе ще прописаний у політиці конфіденційності, під якою вже підписалися поточні користувачі й підпишуться нові. Компанія може знову ввімкнути функцію в будь-який момент, а ви навіть поскаржитися не зможете.

God View — це те, що змушує мене сумувати за старими, добрими таксі. Раніше ви просто ловили машину, казали пункт призначення і платили готівкою після приїзду. Інакше кажучи, поїздка була майже анонімною.

З появою ледь не всюдисущих кредиток на початку XXI століття повсякденні транзакції стали простежуватися, тож і поїздки на таксі перестали бути конфіденційними. Можливо, у конкретного таксиста чи транспортної компанії даних про поїздку і нема, але вони точно є у вашого банку. Ще в 1990-х я працював приватним детективом і міг відстежити маршрут цілі, проглянувши транзакції за кредиткою. Відкриваєш звіт — і от уже бачиш, що минулого тижня ви взяли таксі в Нью-Йорку і заплатили 54 долари за поїздку.

Приблизно з 2010-го таксі почали користуватися GPS. Тепер перевізник знає ваше місце посадки і висадки, ціну поїздки й іноді навіть номер кредитної картки, з якої ви заплатили. Нью-Йорк, Сан-Франциско й інші міста, які підтримують рух відкритих даних в уряді, збирають і оприлюднюють цю анонімну інформацію для аналізу. Жодних реальних імен. Це ж не може вам зашкодити, так?

У 2013 році Ентоні Токар, на той час старшокурсник Північно-Західного університету, стажувався в компанії під назвою Neustar. До його обов'язків входив аналіз анонімних метаданих, оприлюднений державною транспортною комісією Нью-Йорка. Сюди входили записи про кожну поїздку таксі з автопарку за попередній рік, номер автомобіля, час і місце посадки та висадки, ціна поїздки, сума чайових, а також анонімні (гешовані) версії ліцензії таксиста і номер «медальйону»[211]. Сам собою набір даних не дуже цікавий. На жаль, геш у цьому випадку можна відносно легко розшифрувати[212].

Однак якщо поєднати ці оприлюднені дані з іншими джерелами, можна отримати цілісну картину. Приміром, Токар зміг визначити, куди і звідки минулого року їздили на таксі такі знаменитості, як Бредлі Купер і Джессіка Альба. Як йому це вдалося?

Дані геолокації вже були в нього на руках, тому місця посадки й висадки Токар знав. Тепер треба було визначити, хто був усередині[213]. Для цього хлопець поєднав метадані транспортної комісії і фото зі звичайних інтернет-таблоїдів — баз даних папараці.

Лише подумайте. Папараці часто фотографують знаменитостей, коли ті сідають чи виходять з нью-йоркських таксі. І на фото часто потрапляє унікальний номер медальйона, який завжди прикріплений до машини на видному місці. Так, наприклад, номер таксі на світлині Бредлі Купера можна зіставити з оприлюдненими даними про місця посадки і висадки, вартість проїзду і чайові.

На щастя, не всіх нас переслідують папараці. Але це не означає, що наш маршрут неможливо відстежити. Приміром, ви не їздите на таксі. Чи є інші способи визначити вашу геолокацію? Ще б пак. Навіть якщо ви користуєтеся громадським транспортом.

Якщо ви добираєтеся на роботу автобусом, електричкою чи поромом, то зовсім не губитеся серед натовпу. Ба навіть навпаки. Транспортні системи експериментують з мобільними застосунками й технологіями зв'язку на невеликих відстанях (NFC), щоб ставити мітки на пасажирів громадського транспорту. Технологія NFC працює з радіосигналом малого радіуса дії, який часто потребує фізичного контакту. З NFC більше не потрібно нишпорити по кишенях у пошуку готівки: достатньо встановити собі платіжну систему на зразок Apple Pay, Android Pay чи Samsung Pay.

Припустимо, ваш телефон підтримує NFC і має застосунок від вашого місцевого транспортного управління. До застосунку потрібно прив'язати ваш банківський рахунок чи кредитку, щоб спокійно сісти на будь-який автобус, електричку чи пором і не хвилюватися, що у вас нема грошей на рахунку. Якщо номер вашої кредитки не зашифрований токеном, то транспортне управління зможе дізнатися, хто ви є. Заміна номера картки токеном — нова опція, яку пропонують Apple, Android і Samsung. Так продавець (у цьому випадку, транспортне управління) має лише ваш токен, а не справжній номер кредитки. У найближчому майбутньому токени мінімізують інциденти з витоком даних кредитних карток, бо зловмисникам знадобляться вже дві бази даних: токенів і реальних номерів кредитних карток, прив'язаних до токенів.

А що як ваш телефон не підтримує NFC? Скажімо, ви користуєтеся проїзним, як-от CharlieCard у Бостоні, SmarTrip у Вашингтоні, Clipper у Сан-Франциско тощо. Через токени проїзні передають турнікету інформацію про те, що на вашому рахунку достатньо грошей для оплати проїзду на автобусі, метро чи поромі. Однак токени шифрують лише одну сторону транзакції. Сам проїзний містить на магнітній смузі лише номер рахунку, а не інформацію про кредитку. А от якщо зламають бази даних транспортного управління, то ваша банківська інформація опиниться під загрозою. Крім того, деякі транспортні системи вимагають онлайн-реєстрації, щоб мати змогу відправляти вам імейли. Тобто в

разі зламу розкриється ще й адреса вашої електронної пошти. Так чи інакше, якщо ви платите за проїзний карткою, а не готівкою, то забудьте про анонімні поїздки[214].

Усе це на руку правоохоронним органам.

Оскільки компанії, що випускають проїзні картки, приватні, а не державні, вони можуть встановлювати будь-які правила щодо даних. І можуть розкривати їх не лише правоохоронним органам, а й адвокатам у цивільних справах (якщо, приміром, ваша колишня пасія вирішила вас переслідувати).

Тож якщо продивитися логи транспортного управління, можна напевно дізнатися, хто і о котрій зайшов до станції метро. Однак логи не покажуть, на який потяг сіла ваша ціль, особливо якщо станція поєднує кілька ліній. Що ж, цю «проблему» може розв'язати ваш телефон, який укаже на конкретний потяг і ваше місцеперебування.

Як? Цим питанням зайнялися дослідники з Нанкінського університету в Китаї. Вони взялися вивчити маленьку деталь, яка є в кожному телефоні — акселерометр. Цей крихітний чип відповідає за орієнтацію вашого пристрою в просторі: приміром, тримаєте ви його вертикально чи горизонтально. Ці чипи настільки чутливі, що дослідники вирішили спиратися в розрахунках лише на дані з акселерометрів. І вони таки змогли точно визначити, на який потяг сів користувач.

Більшість ліній метро має повороти, які впливають на акселерометр. А ще немаловажною є відстань між зупинками, яка коливається від станції до станції. Точність прогнозів дослідників підвищувалася з кожною новою зупинкою. Вчені стверджують, що їхній метод точний на 92 %.

Припустимо, ви їдете на роботу на своєму автомобілі старої моделі. Ви почуваєтеся невидимкою. Один із мільйона автомобілів на завантаженій дорозі. Може, ви й праві. Але сучасні технології — навіть якщо вони не мають стосунку до вашої машини — вбивають анонімність. Найімовірніше, ваш автомобіль, що летить на повній швидкості автострадою, все ще можна відстежити. Нелегко, але можна.

У Сан-Франциско муніципальне транспортне управління почало використовувати систему автоматичної оплати проїзду FasTrak, що дає змогу легко перетнути будь-який із восьми платних мостів Затоки, як спосіб стежити за автомобілями з передавачем FasTrak у всьому місті. Пристрої для зчитування передавачів в автомобілях (схожі на ті, що стоять на платних мостах) установили на численних парковках Сан-Франциско. Тепер якщо ви надто довго кружляєте в пошуках вільного місця, пристрої це фіксують. Але міську владу цікавлять не ваші пересування, а завантаженість парковок. Більшість із них обладнані електронними лічильниками, і якщо парковка популярна, з вас можуть зняти більше грошей. Місцева влада здатна дистанційно регулювати тарифи на різних паркувальних майданчиках: приміром, підвищувати ціну там, де відбувається масштабний захід.

Крім того, 2014 року чиновники вирішили взагалі прибрати працівників із мосту Золоті ворота, тож тепер усі — навіть туристи — зобов'язані платити за проїзд в електронному вигляді чи за рахунком, який надсилають поштою. Звідки влада знає, куди надсилати рахунок? Вони фотографують ваш номерний знак, коли ви перетинаєте платну зону: схожі камери стоять на проблемних перехрестях і ловлять правопорушників, що їздять на червоне світло. Зараз технологія дедалі частіше з'являється на паркувальних майданчиках і житлових під'їзних доріжках.

Поліція щодня опосередковано відстежує пересування вашого автомобіля за допомогою автоматичної системи розпізнавання номерних знаків (ALPR). Ваш номерний знак можуть сфотографувати і зберігати місяцями чи навіть роками — залежить від політики відділу поліції. Камери ALPR сканують і зчитують номери всіх автомобілів, що проїжджають повз, незалежно від того, зареєстрований автомобіль на злочинця чи ні.

Насамперед ALPR нібито використовують для виявлення викрадених автомобілів, злочинців у розшуку і як частину системи оповіщення про викрадення дітей. Технологія складається з трьох камер, прикріплених на даху патрульного автомобіля і під'єднаних до екрана комп'ютера всередині машини. Ця система пов'язана з базою даних Міністерства юстиції, яка містить інформацію про номерні знаки викрадених автомобілів і транспортних засобів, пов'язаних зі злочинами. Якщо поліцейська машина рухається, ALPR може просканувати до 60 номерних знаків за секунду. Якщо відсканований номер збігається з номером у базі даних, поліцейський отримує візуальне та звукове попередження.

Wall Street Journal вперше висловив стурбованість технологією розпізнавання номерних знаків 2012 року[215]. Але в противників ALPR виникають питання радше не до самої системи, а до того, як довго зберігаються дані і чому деякі правоохоронні органи не розголошують інформацію навіть власникові автомобіля, який відстежують. Система перетворилася на сумнівний інструмент, за допомогою якого поліція може стежити за вашим місцеперебуванням.

«Автоматичні зчитувачі номерних знаків — це хитрий спосіб відстеження водіїв. Якщо ці дані збирати докупи протягом тривалого часу, можна намалювати докладну картину життя конкретної людини», — зазначає Беннет Штайн, учасник Проекту зі свободи слова, конфіденційності та технологій від Американської спілки захисту громадянських свобод (ACLU)[216].

Один мешканець Каліфорнії подав запит на доступ до державного реєстру: його занепокоїла кількість фотографій його номерного знака — більше ніж сто. Більшість фото було зроблено на мостах та в інших громадських місцях. Проте на одній світлині він із дочками виходив із сімейної машини, припаркованої на власній під'їзній доріжці. Зауважте: чоловіка *ні в чому* не підозрювали. Згодом ACLU отримала документи, які доводять: навіть управління генерального

юрисконсульта ФБР ставить під сумнів використання ALPR через відсутність послідовної державної політики[217].

На жаль, вам не треба подавати запит на доступ до державного реєстру, щоб отримати інформацію з систем ALPR. За даними EFF, фотографії з більш як ста камер ALPR висять у відкритому доступі в інтернеті. Усе, що вам потрібно, — це звичайний браузер. Перш ніж оприлюднити інформацію, EFF скооперувалася з правоохоронними органами, щоб припинити витік даних. Виявилося, помилки в конфігурації мають не лише ці сто камер — набагато більше. EFF закликала правоохоронні органи у всій країні прибрати або закрити доступ до того, що опубліковано в інтернеті. Але, на час написання книжки, при правильному запиті в пошуковику ви все ще можете знайти фото номерних знаків із купи камер. Один дослідник за тиждень знайшов понад 64 тисячі фотографій номерних знаків і відповідних даних про місцеперебування автомобіля[218].

Можливо, у вас нема власного автомобіля, тож ви його час від часу орендуєте. Тут уже точно забудьте про непомітність, враховуючи всю особисту та фінансову інформацію, яку ви подаєте для оренди. Ба навіть більше: зараз майже всі прокатні автомобілі мають GPS. Я точно знаю. Дізнався на власному гіркому досвіді.

Коли автосалон тимчасово позичає вам автомобіль, поки ваш на техобслуговуванні, зазвичай ви погоджуєтеся не виїжджати на ньому за кордони штату. Автосалонові потрібно тримати автомобіль у тому штаті, де ви його позичили. Правило стосується переважно їхньої страховки, не вашої.

Таке сталося і зі мною. Я привіз машину до салону Lexus у Лас-Вегасі на техобслуговування, і вони дали мені тимчасовий автомобіль. Було пізно, автосалон уже закривався, а співробітник мене квапив, тож я швидко підписав документи, навіть не читаючи. Незабаром я вирушив на виступ у Північну Каліфорнію, у район Затоки. Коли співробітник салону зателефонував мені щодо рекомендацій, він запитав:

— А ви де?

Я відповів:

— Сан-Рамон, Каліфорнія.

— Так-так, саме там ми і бачимо машину.

А потім відчитав мене за те, що я виїхав на машині за межі штату. Імовірно, у нашвидкуруч підписаних документах ішлося про те, що автомобіль повинен залишатися в межах Невади.

Коли ви орендуєте чи позичаєте автомобіль, з'являється спокуса під'єднати свій бездротовий пристрій до мультимедійного центру, щоб слухати власну музику. Але тут одразу ж виникають проблеми з конфіденційністю. Автомобіль не ваш. Що ж трапиться з вашими даними мультимедіа після того, як ви повернете автомобіль у прокат?

Перш ніж під'єднати девайс до чужого автомобіля, ретельно вивчіть мультимедійну систему. Можливо, зайшовши в налаштування блютуз

смартфона, ви побачите список пристроїв та/або імен попередніх користувачів. Добряче подумайте, чи хочете опинитися в цьому списку.

Інакше кажучи, коли віддаєте машину, ваші дані не зникають. Треба видаляти їх вручну.

Думаєте, що поганого в тому, щоб поділитися улюбленою музикою з іншими? Те, що ділитеся ви не лише музикою. Коли більшість телефонів під'єднуються до мультимедійного центру, вони автоматично завантажують ваші контакти в систему автомобіля: можливо, ви захочете зробити голосовий виклик за кермом, а зберігання контактів в автомобілі спростить процес. Проблема лише в тому, що машина не ваша.

«Коли я беру автомобіль напрокат, — каже Девід Міллер, директор служби безпеки Covisint, — останнє, що я зроблю, — це під'єднаю свій телефон. Він самовільно завантажує всі мої контакти. Якщо хтось колись під'єднувався до автомобіля, який ви орендували, можете зайти в систему і знайти його контакти».

Та сама проблема виникає під час продажу машини. Сучасні автомобілі дають вам доступ до цифрового світу просто за кермом. Хочете перевірити твітер? Хочете опублікувати пост на фейсбуці? Будь ласка. Із кожним днем автомобілі дедалі більше нагадують ПК і мобільний телефон «в одному флаконі». Тож не дивно, що з них також доведеться видалити персональні дані перед продажем.

З роботою у сфері безпеки звикаєш думати на кілька кроків наперед, навіть у побуті. «Роками я крок за кроком пов'язую свій автомобіль з особистим життям, — каже Міллер. — Але що як за п'ять років мені доведеться його продати? Як я можу відв'язати його від власного життя? Я не хочу, щоб покупець зміг проглянути всіх моїх друзів на фейсбуці. Треба провести деініціалізацію. Людей, що крутяться у сфері безпеки, набагато більше цікавлять вразливості в процесі деініціалізації, а не ініціалізації»[219].

Непогано було б мати змогу захистити автомобіль паролем, як і звичайний телефон. Але, на час написання книжки, досі не існує механізму, який допоможе поставити пароль на мультимедійну систему. Крім того, видалити всі контакти, що назбиралися в автомобілі за довгі роки, теж нелегко: процес залежить від виробника, марки і моделі. Можливо, у майбутньому це зміниться. Можливо, хтось винайде кнопку, яка моментально видаляє весь профіль користувача з автомобіля. А поки що залишається лиш зайти після продажу машини в інтернет і змінити паролі від усіх соцмереж.

Певно, найкращим прикладом комп'ютера на колесах є «Тесла» — надсучасний і наскрізь електронний автомобіль. У червні 2015 року Tesla досягла небувалої відмітки: її автомобілі у всьому світі разом проїхали понад мільярд миль[220].

У мене також «Тесла». Автомобіль чудовий, але з огляду на складні приладові панелі та постійний стільниковий зв'язок, виникають певні запитання щодо того, які дані збирає компанія.

Коли ви купуєте «Теслу», вам пропонують підписати форму згоди. У вас є можливість вирішити, чи буде Tesla отримувати інформацію про ваш автомобіль через бездротову систему зв'язку. Увімкнути чи вимкнути обмін особистими даними з Tesla можна через сенсорний екран на приладовій панелі. Але більшість людей вірять у те, що їхні дані допоможуть Tesla вдосконалити автомобілі в майбутньому.

Згідно з політикою конфіденційності Tesla, для аналізу роботи транспортного засобу компанія може збирати інформацію про ідентифікаційний номер автомобіля, швидкість, покази одометра, використання батареї, історію заряду акумулятора, функціонування електронних систем, версію ПЗ, мультимедійну систему, а також дані про безпеку (включно з інформацією про подушки безпеки, звичайні гальма, електронну гальмівну систему тощо). Tesla додає, що може збирати цю інформацію особисто (наприклад, під час чергового техобслуговування) або дистанційно.

Це те, що написано в політиці конфіденційності.

На практиці ж вона в будь-який час може визначити місцеперебування і стан машини. У ЗМІ Tesla не розголошує, які дані в реальному часі вона насправді збирає і як їх використовує. Як і Uber, Tesla знає все про кожен свій автомобіль та його місцеперебування в будь-яку мить.

Якщо це вас турбує, можете зв'язатися з Tesla і відмовитися від телематичної програми. Але так ви відмовляєтеся ще й від автоматичних оновлень програмного забезпечення, які охоплюють виправлення прогалин у безпеці і нові функції.

Звісно ж, профі у сфері безпеки зацікавилися Tesla. Незалежний дослідник інформаційної безпеки Нітеш Дханджані виділив кілька проблем. Хоча він згоден зі мною в тому, що «Тесла модел S» — відмінний автомобіль і фантастична інновація, Дханджані зауважив досить слабку систему однофакторної автентифікації при віддаленому доступі до систем автомобіля[221]. Сайт і застосунок Tesla не обмежують кількість невдалих спроб входу в акаунт користувача, тобто зловмисник, теоретично, може зламати пароль грубою силою. Отже, будь-яка стороння особа (за умови, що вона зламала ваш пароль) може зайти у ваш акаунт і дізнатися місцеперебування вашого автомобіля через прикладний програмний інтерфейс Tesla. А ще ця людина може дистанційно увійти в застосунок Tesla й отримати контроль над системами автомобіля: кондиціонером, фарами тощо.

На час написання книжки більшість проблем, які виявив Дханджані, Tesla вже виправила. Але ситуація чудово демонструє, скільки ще треба зробити сучасним автовиробникам, щоб випускати дійсно безпечні автомобілі. Самої наявності застосунку для віддаленого запуску й перевірки стану автомобіля замало. Він повинен бути безпечним. Нещодавно Tesla додала в застосунок функцію під назвою Summon, яка дає змогу автомобілю автоматично виїхати з гаража чи припаркуватися в тісному місці. У майбутньому завдяки Summon

машина зможе сама забрати вас із будь-якої точки країни. Як у старому серіалі «Лицар доріг».

У відповіді на негативний відгук у New York Times Tesla продемонструвала свою всюдисущість повною мірою. Журналіст Джон Бродер заявив, що його «Тесла модел S» зламалася в найнедоречніший момент посеред дороги. У своєму блозі Tesla спростувала цю заяву й оприлюднила дані, які ставили під сумнів історію Бродера. Наприклад, Tesla зазначила, що Бродер їхав зі швидкістю від 105 до 130 кілометрів за годину з середньою температурою в салоні 22 градуси за Цельсієм[222]. Згідно з Forbes, «реєстратори даних автомобіля фіксували температурні параметри в салоні, рівень заряду батареї протягом усієї поїздки, швидкість автомобіля похвилинно, а також точний маршрут — зокрема й той факт, що журналіст намотував кола парковкою, поки акумулятор не сів»[223].

Телематичні функції є логічним додатком до чорних ящиків, якими тепер треба оснащувати всі автомобілі, випущені в США після 2015 року. Але чорні ящики в машинах — зовсім не новинка. Коренями вони сягають ще 1970-х, коли водіям уперше представили подушки безпеки. Тоді в результаті зіткнень люди зазнавали від подушок безпеки небезпечних для життя травм. Деякі навіть гинули. Якби машини не були оснащені подушками безпеки, деякі пасажири сьогодні могли б бути живі. Щоб удосконалити систему, інженерам потрібні були дані про роботу подушок до і після аварії, які фіксувалися модулями датчиків і діагностики. Проте донедавна водії так і не знали, що якісь там датчики записують інформацію про роботу їхнього автомобіля.

Через різкі зміни гравітації, чорні ящики в автомобілях (як і в літаках) записують лиш останні кілька секунд гравітаційного маневру, як-от раптове прискорення, зміна крутного моменту чи різке гальмування.

Думаю, що скоро ці чорні ящики будуть збирати набагато більше даних і передавати їх бездротовим зв'язком у режимі реального часу. Лише уявіть: у майбутньому дані, зібрані за останніх 3–5 днів, зберігатимуться в самому транспортному засобі чи «хмарі». Замість того щоб намагатися описати дивний тріскіт, який ви чуєте, коли автомобіль розганяється до 60 кілометрів за годину, можна просто дати механікові доступ до записаних даних. Питання в тому, хто ще матиме до них доступ? Навіть Tesla визнає, що доступ до їхніх баз даних мають треті сторони.

А що як третя сторона — ваш банк? Якщо він має угоду з вашим автовиробником, то міг би стежити за наявністю аварій і ухвалювати відповідне рішення про надання вам кредиту на авто. Те саме може зробити і ваш медичний страховик. Чи навіть автостраховик. Можливо, уряду варто прописати в законах, хто може отримати дані про ваш автомобіль і як ви можете зберегти їх конфіденційність.

Сьогодні ви вже нічого не вдієте, але в майбутньому на це варто звернути увагу.

Припустимо, у вас не «Тесла». Але інші виробники теж мають різні застосунки, які уможливлюють дистанційно відчиняти двері автомобіля, запускати двигун чи навіть проводити певну діагностику. Один дослідник довів, що сигнал — між автомобілем, «хмарою» і застосунком — можна зламати. А це дає змогу легко відстежити потрібний автомобіль, розблокувати двері, увімкнути гудок, сигналізацію і навіть контролювати двигун. Хакер здатен робити все, що заманеться. Хіба що завести і викрасти машину не зможе: для цього все ще потрібен ключ. Хоча нещодавно я знайшов спосіб вимкнути брелок від «Тесли» і заблокувати машину. Через невеличкий передавач із частотою 315 МГц можна перервати сигнал від брелока, й автомобіль не зрушить з місця.

На DEF CON 23 Семі Камкар — дослідник інформаційної безпеки, який 2005-го прославився своїм комп'ютерним вірусом для MySpace під назвою «Семі», — презентував власну розробку під назвою OwnStar, яка підроблює сигнал відомої транспортної мережі. Приміром, такий пристрій може відкрити автомобіль від General Motors із системою безпеки OnStar. Пристрій необхідно розмістити на бампері чи знизу бажаного автомобіля або вантажівки. Девайс підміняє собою бездротову точку доступу автомобіля, і телефон водія автоматично прив'язується до нової, фальшивої точки (за умови, що телефон водія до цього був прив'язаний до справжньої точки доступу). Коли жертва запускає мобільний застосунок OnStar на iOS або Android, OwnStar краде особисті дані водія через недолік у системі. «Щойно ви під'єдналися до моєї мережі і відкрили застосунок, ваш автомобіль став моїм», — заявив Камкар[224].

Отримавши облікові дані для входу в RemoteLink (ПЗ, на якому працює OnStar), зловмисник може знайти ваш автомобіль на переповненій парковці за звуком розблокування (біп-біп), відкрити його і вкрасти щось цінне. А потім зняти пристрій з бампера. Досить елегантно: нема жодних ознак грубого зламу. Власник і страхова компанія будуть довго битися над тим, що ж таки сталося.

Дослідники виявили, що стандарти «під'єднаних» до мережі автомобілів, призначені для поліпшення руху на дорогах, теж можна відстежити. Сигнали «автомобіль-автомобіль» (V2V) та «автомобіль-інфраструктура» (V2I), разом відомі як V2X, змушують автомобілі передавати повідомлення зі швидкістю десять разів на секунду через спектр Wi-Fi на частоті 5,9 гГц, відомий як 802.11p.[225]

На жаль, ці дані надсилаються в незашифрованому вигляді. Так і повинно бути: коли автомобіль летить на великій швидкості, навіть мілісекундна затримка для розшифровки сигналу може призвести до аварії. Тому розробники зупинили вибір на відкритому, незашифрованому передаванні даних. Але вони запевняють, що сигнал не містить жодної особистої інформації, навіть номерного знака. Проте, щоб сигнал не змогли підробити, кожне повідомлення підкріплюється цифровим підписом. А цифрові підписи, надіслані з наших смартфонів (приміром, IMEI — серійний номер мобільного телефону), уже можна простежити до зареєстрованого власника транспортного засобу.

Джонатан Петі, один з авторів дослідження, пояснив Wired: «Ваш автомобіль каже: "Мене звуть Еліс, ось моя геолокація, ось моя швидкість і ось мій маршрут". І це почують усі навколо... А потім вони скажуть: "Еліс стверджувала, що була вдома, а сама поїхала в аптеку, а після цього — у клініку штучного запліднення", щось таке... Сторонні можуть отримати забагато особистої інформації про водія»[226].

Петі розробив систему вартістю приблизно тисяча доларів, яка може перехоплювати сигнали V2X. За його підрахунками, невелике місто може покрити датчиками всю територію приблизно за мільйон доларів. Замість того щоб тримати куну поліції, місто буде ідентифікувати водіїв і (що важливіше) їхні звички за датчиками.

Національна адміністрація безпеки дорожнього руху та європейські уряди висунули таку пропозицію: змінювати сигнал 802.11p — «псевдонім» автомобіля — кожні п'ять хвилин. Проте це не зупинить затятого зловмисника: він просто встановить більше датчиків, які встигнуть ідентифікувати автомобіль до і після зміни сигналу. Тобто варіантів уникнути ідентифікації транспортного засобу дуже мало.

«Зміна "псевдоніма" не зупиняє стеження. Лише його пом'якшує, — стверджує Петі. — Однак це все одно захищає конфіденційність... Ми хочемо показати, що без цього захисту вас зможуть легко відстежити в будь-якій точці».

«Під'єднання» автомобіля до інтернету — зручна функція: так виробники за потреби можуть миттєво виправляти баги програмного забезпечення. На час написання книжки, Volkswagen[227], Land Rover[228] і Chrysler[229] зіткнулися з масштабними вразливостями ПЗ. Проте лише кілька автовиробників, як-от Mercedes, Tesla та Ford, розсилають оновлення на всі свої автомобілі «по повітрю». Решті все ще доводиться ходити за ними в магазин.

Якщо думаєте, що Tesla і Uber, які стежать за кожним вашим рухом, — це якось моторошно, то безпілотні автомобілі налякають вас ще більше. Як і шпигунські жучки в нас у кишенях (це я про телефони), безпілотники будуть знати, куди ми їдемо і навіть де перебуваємо зараз, щоб завжди бути напоготові. Google та інші компанії запропонували цікавий сценарій майбутнього: у великих містах більше не буде парковок і гаражів, бо автомобіль кружлятиме навколо, поки не знадобиться. А можливо, ми підемо іншим сценарієм, де приватна власність відійшла в минуле, а люди сідають у той автомобіль, що опинився поряд.

Наші смартфони вже більше схожі на традиційні ПК, ніж на колишні дротові телефони. Та сама доля чекає і на безпілотні автомобілі. Вони будуть автономними комп'ютерами, здатними ухвалювати самостійні миттєві рішення на дорозі, навіть якщо відрізані від власної мережі. Через стільниковий зв'язок вони зможуть отримувати доступ до різноманітних хмарних сховищ і збирати в режимі реального часу інформацію про дорожній рух, дорожні роботи та прогноз погоди від Національної метеорологічної служби.

Зараз ці оновлення вже доступні для деяких звичайних автомобілів. Але, за прогнозами, до 2025 року більшість автомобілів будуть «під'єднаними» до інших автомобілів, до служб технічної допомоги на дорогах. Імовірно, що значний відсоток становитимуть безпілотники[230]. Уявіть, у що виллється програмна помилка в безпілотному автомобілі.

А ще кожна ваша поїздка на таксі буде десь записуватися. Вам обов'язково знадобиться застосунок — щось типу ПЗ від Uber, — зареєстрований на ваше ім'я і телефон. Застосунок буде записувати всі ваші подорожі і, ймовірно, витрати на них, якщо вони проведені по прив'язаній картці. І ці записи можна буде дістати (якщо не в Uber, то в банку) й пред'явити в суді. А ще програми розроблятимуть, найімовірніше, приватні компанії, тож уже вони вирішуватимуть, ділитися вашою особистою інформацією з правоохоронними органами чи ні.

Ласкаво прошу в майбутнє.

Сподіваюся, що на час виходу книжки влада вже посилить обмеження (або хоча б натякне на посилення в найближчому майбутньому) щодо виробництва «під'єднаних» автомобілів і протоколів їхнього зв'язку. Замість того щоб користуватися загальноприйнятими стандартами безпеки програмного й апаратного забезпечення, автомобільна промисловість — як і медична промисловість та деякі інші — намагається винайти колесо. Ніби за останні сорок років ми не дізналися нічого нового про мережеву безпеку. А ми дізналися. І краще б виробники пристали на наявні передові практики, замість того щоб вдавати, наче вони роблять щось радикально нове й унікальне. Не роблять. На жаль, злам коду автомобіля є набагато небезпечнішим, аніж звичайний збій ПК із синім екраном смерті. У машині це може покалічити чи навіть вбити людину. На час написання книжки щонайменше один водій загинув у тестовому режимі автопілота в «Теслі». Досі невідомо, стали причиною несправні гальма чи помилка в рішенні ПЗ автомобіля[231].

Читаючи це, ви, напевно, уже ніколи не схочете виходити з дому. Не кваптеся з висновками. У наступному розділі я розповім, як домашні гаджети слухають і записують усе, що ми робимо за зачиненими дверима. І тут уже треба боятися зовсім не уряду.

---

203 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

204 Це безглуздо. Просто забороняючи, ми не доб'ємося того, що явище зникне. А це вимальовує небезпечний сценарій, у якому хакнуті машини все ще можуть зашкодити іншим водіям.

205 https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/.

206 http://www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy.

207 http://www.theregister.co.uk/2015/06/22/epic_uber_ftc/.

208 http://nypost.com/2014/11/20/uber-reportedly-tracking-riders-without-permission/.

209 https://www.uber.com/legal/usa/privacy.

210 http://fortune.com/2015/06/23/uber-privacy-epic-ftc/.

211 http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-privacy.

212 https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1.

213 http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/.

214 Можете зайти в офіс транспортного управління й придбати проїзний за готівку, але це виллється в купу витраченого часу і лекцію про те, що для купівлі краще скористатися дебетовою чи кредитною карткою.

215 http://www.wsj.com/articles/SB10000872396390443995604578004723603576296.

216 https://www.aclu.org/blog/free-future/internal-documents-show-fbi-was-wrestling-license-plate-scanner-privacy-issues.

217 http://www.wired.com/2015/05/even-fbi-privacy-concerns-license-plate-readers/.

218 Серед джерел були: управління шерифа округу Сент-Таммані, управління шерифа округу Джефферсон та управління поліції Кеннера в штаті Луїзіана; управління поліції Гаялії у Флориді; Університет при Південно-Каліфорнійському управлінні громадською безпекою.

219 http://www.forbes.com/sites/robertvamosi/2015/05/04/dont-sell-that-connected-car-or-home-just-yet/.

220 https://www.washingtonpost.com/blogs/the-switch/wp/2015/06/24/tesla-says-its-drivers-have-traveled-a-billion-miles-and-tesla-knows-how-many-miles-youve-driven/.

221 http://www.dhanjani.com/blog/2014/03/curosry-evaluation-of-the-tesla-model-s-we-cant-protect-our-cars-like-we-protect-our-workstations.html.

222 http://www.teslamotors.com/blog/most-peculiar-test-drive.

223 http://www.forbes.com/sites/kashmirhill/2013/02/19/the-big-privacy-takeaway-from-tesla-vs-the-new-york-times/.

224 http://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/.

225 http://spectrum.ieee.org/cars-that-think/transportation/advanced-cars/researchers-prove-connected-cars-can-be-tracked.

226 http://www.wired.com/2015/10/cars-that-talk-to-each-other-are-much-easier-to-spy-on/.

227 https://grahamcluley.com/2013/07/volkswagen-security-flaws/.

228 https://grahamcluley.com/2015/07/land-rover-cars-bug/.

229 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

230 http://www.forbes.com/sites/robertvamosi/2015/03/24/securing-connected-cars-one-chip-at-a-time/.

231 http://www.nytimes.com/2016/07/30/business/tesla-faults-teslas-brakes-but-not-autopilot-in-fatal-crash.html.

Розділ 12

Ваш дім — не ваша фортеця

Ще кілька років тому ніхто й уваги не звертав на домашні термостати. В усіх був звичайнісінький механічний терморегулятор, який підтримував у будинку комфортну температуру. Але прогрес не стоїть на місці. Спочатку термостати стали електронними. Потім компанія Nest вирішила дати вам можливість керувати електронним термостатом через онлайн-застосунок. Уже зрозуміли, до чого я веду?

В одному негативному амазонівському відгуку на розумний термостат із підтримкою Wi-Fi від Honeywell користувач із ніком General написав, що після розлучення колишня дружина забрала будинок, собаку й накопичувальний пенсійний рахунок, але в нього залишився пароль від термостата Honeywell. Коли вона з новим хлопцем виїхала за місто, General зміг підвищити температуру до максимуму і знизити її, перш ніж вони повернуться: «Лише уявіть, які в них будуть рахунки за світло. Від самої думки посміхаюся»[232].

На конференції з інформаційної безпеки Black Hat USA 2014 дослідники продемонстрували кілька способів, якими можна зламати прошивку термостата Nest[233]. Варто зауважити, що більшість способів передбачають фізичний доступ до приладу, тобто хтось таки має прокрастися до будинку і встановити на термостат USB-порт. Деніел Бентелло, незалежний дослідник інформаційної безпеки й один із чотирьох експериментаторів, сказав: «Термостат — це комп'ютер, на який не можна встановити антивірус. Тим паче, у термостатах є лазівка, якою зловмисники можуть скористатися, щоб оселитися у вашому будинку назавжди. Це — найнепомітніший жучок»[234].

Команда дослідників показала відео, у якому вони почаклували над інтерфейсом термостата Nest (зробили його схожим на об'єктив камери HAL 9000[235]) й завантажили купу нових функцій. Цікаво, що вони не змогли відключити функцію автоматичної звітності, тож команді довелося розробити для цього програму самостійно[236]. Цей інструмент відрізає потік даних, що надсилаються в Google — материнську компанію Nest.

Пізніше Зоз Куссіас із Nest прокоментував презентацію на порталі VentureBeat: «Усі пристрої з апаратним забезпеченням — від ноутбуків до смартфонів — можна хакнути. Така проблема не лише в нас. Тут йдеться про фізичний джейлбрейк, який потребує фізичного доступу до розумного термостата Nest. Якщо хтось таки прокрадеться у ваш будинок, то, імовірно, він установить власні жучки чи вкраде коштовності. Джейлбрейк не загрожує нашим серверам або зв'язку з ними. І, наскільки нам відомо, до жодних наших девайсів не можна дістати доступ дистанційно. Безпека клієнтів вкрай важлива для нас, і в пріоритеті в нас увага до дистанційної вразливості. Для вас

найнадійніший варіант — установити камеру Dropcam Pro, яка дасть можливість стежити за будинком, коли ви не вдома»[237].

З появою інтернету речей такі компанії, як Google, прагнуть колонізувати нові терени. Заволодіти платформами, на яких працюють інші продукти. Тобто прагнуть, щоб пристрої, розроблені іншими компаніями, були під'єднані саме до їхніх сервісів. Приміром, Google володіє як Dropcam, так і Nest, але він хоче під'єднати до Google-акаунтів й інші девайси інтернету речей, як-от розумні лампочки і радіоняні. Плюс для Google в тому, що так вони отримають більше чистих даних про ваші звички (такі наміри ледь не в усіх гігантів індустрії: Apple, Samsung, навіть Honeywell).

У своєму інтерв'ю експерт із комп'ютерної безпеки Брюс Шнайер сказав про інтернет речей таке: «Це схоже на комп'ютерну галузь періоду 1990-х: ніхто не переймається безпекою, ніхто не випускає оновлень, ніхто нічого не знає. Усе це дуже погано. Рано чи пізно це виллється у катастрофу... Буде з'являтися дедалі більше вразливостей, зловмисники будуть цим користуватися, а жодного способу припинити це просто не існуватиме»[238].

Щоб довести це, влітку 2013-го репортерка Кашмір Гілл провела журналістське розслідування й спробувала себе в ролі хакера-аматора. Через ґуґл-пошук вона знайшла просту фразу, яка дала їй змогу керувати деякими пристроями системи розумного дому Insteon. Кашмір дістала доступ до контролера — центрального пристрою, який зв'язує систему з мобільним застосунком чи інтернетом напряму. Через застосунок люди можуть контролювати освітлення у вітальнях, замикати двері або регулювати температуру в домі. Через інтернет власник може управляти будинком, поки, скажімо, перебуває у відрядженні.

Але Гілл продемонструвала, що через інтернет до контролера може під'єднатися і зловмисник. Для цього журналістка зв'язалася з Томасом Гетлі — абсолютно незнайомим чоловіком з Орегону — і попрохала дозволу перевірити теорію на ньому.

Із власного будинку в Сан-Франциско Гілл змогла ввімкнути і вимкнути світло в будинку Гетлі, що стояв приблизно за тисячу кілометрів від Тихоокеанського узбережжя. А ще Гілл могла б дістати доступ до його джакузі, вентиляторів, телевізорів, водяних насосів, дверей гаража і камер відеоспостереження, якби вони були під'єднані до системи.

Проблема полягала в тому, що вся інформація про будинок Гетлі була доступна в Google (зараз Insteon це вже виправили). Ба навіть гірше: на той час інформація не була захищена паролем, а отже, будь-хто міг контролювати будь-який контролер Insteon, дані про який містяться в інтернеті. На роутері Гетлі стояв пароль, але його можна було обійти, знайшовши безпосередній порт Insteon, що і зробила Гілл.

«Будинок Томаса Гетлі був одним із восьми будинків, до яких я змогла дістати доступ, — пише вона. — В інтернеті можна знайти купу конфіденційної

інформації: не лише про пристрої, під'єднані до розумного дому, а й про часовий пояс власника (разом із найближчим великим містом до його будинку), IP-адреси і навіть імена дітей (мабуть, батьки хотіли дистанційно контролювати перегляд програм малюками). Щонайменше у трьох випадках інформації було достатньо для того, щоб пов'язати розумні будинки в інтернеті з їхньою геолокацією в реальному житті. Переважно назви систем були загальними, але в одному випадку замість назви вказали реальну адресу, яку я простежила до будинку в Коннектикуті»[239].

Приблизно в той самий час аналогічну проблему виявив дослідник інформаційної безпеки Нітеш Дханджані. Зокрема Дханджані вивчав систему освітлення Philips Hue, яка дає власникові змогу регулювати колір і яскравість лампочки з телефона. Лампочка має діапазон у 16 мільйонів кольорів.

Дханджані виявив, що достатньо встановити простий скрипт на ПК у домашній мережі, щоб викликати розподілену атаку на відмову в обслуговуванні, або DDoS-атаку[240]. Інакше кажучи, з такою лампочкою він міг загасити світло в будь-якій кімнаті. Коли користувач намагався перезапустити лампочку, вона знову миттєво згасала. І тривало це доти, доки код скрипта «сидів» у комп'ютері.

Дханджані зауважив, що так можна організувати серйозні проблеми для цілої офісної будівлі чи житлового будинку. Код вимкне всі лампочки, і постраждалі будуть раз за разом дзвонити в місцеву комунальну службу й дивуватися, що жодного відключення електроенергії в їхньому районі не було.

Але розумні девайси з доступом в інтернет вразливі не лише до DDoS-атак. Ще їх можна зламати і приєднати до ботнету — цілої армії заражених пристроїв, які управляються з одного контролера і можуть брати участь у DDoS-атаках на інші системи. У жовтні 2016 року компанія під назвою Dyn, яка опікується інфраструктурою DNS для інтернет-гігантів на зразок Twitter, Reddit і Spotify, добряче постраждала від однієї з таких атак. Мільйони користувачів зі східної частини США не могли дістати доступ до кількох великих сайтів, бо не було зв'язку із DNS-серверами компанії.

Винуватцем виявився «хробак» під назвою Mirai — вірус, який прочісує інтернет у пошуку незахищених пристроїв інтернету речей, як-от камери відеоспостереження, роутери, відеореєстратори та радіоняні, а потім зламує, щоб скористатися ними в майбутніх атаках. Зламує він девайс шляхом звичайного підбору пароля. Якщо атака пройшла успішно, пристрій приєднується до ботнету, де на нього чекають інструкції. Тепер за допомогою короткої команди оператор ботнету може доручити кожному пристрою — а їх у мережі сотні тисяч чи навіть мільйони — відправити дані на цільовий сайт і затопити його інформацією, змусивши перейти в автономний режим.

Хоча й самі DDoS-атаки як явище викорінити вам не вдасться, сховати свій пристрій від ботнетів таки можна. Насамперед змініть пароль на такому

пристрої на щось складне. А якщо ж ваш девайс уже заразили, зазвичай перезавантаження повинно видалити шкідливий код.
Комп'ютерні скрипти можуть взяти контроль і над іншими системами розумного будинку.

Якщо у вас вдома немовля, то напевно є і радіоняня. Такий девайс — мікрофон, камера або два в одному — допомагає батькам стежити за дитиною, навіть якщо вони перебувають не в дитячій кімнаті. На жаль, через радіоняню за вашими дітьми можете спостерігати не лише ви.

Аналогові радіоняні працюють на застарілій бездротовій частоті в діапазоні 43–50 МГц. Уперше ці частоти ввели в 1990-х для бездротових телефонів. Тоді будь-хто з дешевим сканером радіочастот міг легко перехопити телефонні дзвінки без відома жертви.

І навіть сьогодні хакер може виявити частоту конкретної аналогової радіоняні через аналізатор спектра, а потім перетворити сигнал на аудіо через різні схеми демодуляції. Вистачить і поліцейського сканера з магазину електроніки. Уже не раз до суду потрапляли справи про те, як сусіди з радіонянями однакової марки налаштовувалися на однакову частоту й підслуховували одне одного. У 2009 році Вез Денков із Чикаго подав до суду на виробників відеоняні Summer Infant Day & Night, стверджуючи, що через неї його сусід підслуховував приватні розмови[241].

Існують ще й цифрові радіоняні. Через них загалом теж можна шпигувати, але вони мають кращу систему безпеки і більше параметрів конфігурації. Наприклад, ви можете оновити прошивку девайса (програмне забезпечення чипа) відразу після покупки. Також не забудьте змінити ім'я користувача та пароль за замовчуванням.

Але й тут ви можете зіткнутися з пристроями, які не контролюєте взагалі. Нітеш Дханджані виявив, що бездротова радіоняня Belkin WeMo використовує в застосунку токен, який після встановлення на телефон і під'єднання до домашньої мережі залишається активним і доступним з будь-якої точки світу. Скажімо, ви погодилися посидіти з новонародженою племінницею, і брат пропонує вам завантажити собі на телефон застосунок Belkin через його домашній Wi-Fi (якщо пощастить, захищений паролем WPA2). Тепер у вас є доступ до радіоняні вашого брата з будь-якого куточка країни, ба навіть планети.

Дханджані зауважує, що таким недоліком може похизуватися купа зв'язаних девайсів інтернету речей. Ці пристрої припускають, що всім іншим пристроям у локальній мережі можна довіряти за замовчуванням. Якщо в майбутньому домашні мережі будуть об'єднувати більше ніж двадцять або навіть тридцять девайсів, модель безпеки доведеться змінювати. Позаяк усім пристроям у мережі можна довіряти, то лазівка в будь-якому з них — радіоняні, лампочці, термостаті — дасть зловмисникові дистанційний доступ до мережі вашого розумного будинку і шанс дізнатися більше про ваші особисті звички.

Задовго до появи мобільних застосунків люди користувалися пультами дистанційного керування. А ще до цього — підходили до телевізора і крутили коліщатко щоразу, як треба було перемикнути канал. Чи додати гучності. Можливо, деякі цього вже навіть і не згадають. Сьогодні ж ми можемо керувати телевізором голосом, навіть не встаючи з диванів. Так, це зручно. Але чи замислювалися ви про те, що телевізор постійно нас слухає? Хоча б для того, щоб почути команду «ввімкнути».

Перші пульти дистанційного керування працювали на батарейках, лише по прямій лінії й за допомогою інфрачервоного світла. Пульт випромінював певну послідовність спалахів, ледь видимих людському окові, але добре видимих (знову ж таки, лише по прямій лінії) приймачу на телевізорі. Як вимкнений телевізор розумів, що ви хочете його ввімкнути? Дуже просто: інфрачервоний датчик на телевізорі завжди був увімкнений, у режимі очікування. Тож щойно пульт випромінював певну послідовність інфрачервоних світлових імпульсів, датчик їх приймав і «будив» телевізор.

З роками почали з'являтися телевізори з дистанційним керуванням на бездротовому сигналі. Стояти просто перед телевізором уже не було потреби: ви могли увімкнути його з-за рогу чи взагалі з іншої кімнати. Знову ж таки, телевізор постійно перебував у режимі очікування, чекаючи на відповідний сигнал.

Пропустимо мобільні застосунки — і от ми вже на етапі телевізорів із голосовим управлінням. Кінець пультам, які особисто я регулярно десь гублю. Замість цього просто потрібно сказати щось безглузде на зразок «телевізор, увімкнися» або «привіт, телевізор» — і ось він уже працює. Як за помахом чарівної палички.

Навесні 2015 року дослідники інформаційної безпеки Кен Мунро і Девід Лодж захотіли перевірити, чи слухають голосові телевізори Samsung розмови в кімнаті, навіть коли вимкнені. Виявляється, цифрові телевізори дійсно нічого не роблять у неактивному стані, і це обнадіює. Але щойно ви дасте їм просту команду на зразок «привіт, телевізор», вони відразу ввімкнуть запис голосу і записуватимуть усе, поки ви його знов не вимкнете. А тепер питання: чи зможете ви не промовити жодного слова, поки працює телевізор?

Певен, що ні. Злякаю вас ще більше: усе, що говоримо (і що записується) після команди «привіт, телевізор», не шифрується. І якщо я під'єднаюся до вашої домашньої мережі, то зможу підслуховувати всі ваші розмови, поки працює телевізор.

Девайс постійно вас слухає не просто так: він повинен чути будь-які додаткові команди, як-от «збільш гучність», «перемкни канал» або «вимкни звук». І все це чудово... за винятком того, що голосові команди спочатку потрапляють на сунутник, а вже потім — до самого телевізора. І позаяк потік даних незашифрований, я можу провести «атаку посередника» і вставити в цей потік

власні команди, тобто перемкнути канал, збільшити гучність або просто вимкнути телевізор, коли мені заманеться.

Замисліться про це на хвильку. Це означає, що якщо ви балакаєте з кимось у кімнаті, де є телевізор із голосовим управлінням, і вмикаєте його посеред розмови, телевізор може записати всі ваші слова. Ба навіть більше: розмова про майбутній шкільний фестиваль печива може потрапити на сервер десь далеко за межами вашої вітальні. По суті, доступ до даних є не лише в Samsung, а й в іншої компанії під назвою Nuance, яка займається розпізнаванням голосу. І ці дві компанії дістануть неймовірно важливу інформацію про майбутній ярмарок.

А тепер ближче до реальності: зазвичай бесіди у вашій вітальні з телевізором далеко не про печиво. Можливо, ви говорите про щось незаконне. Про щось, що неодмінно зацікавить правоохоронні органи. Цілком ймовірно, ці компанії повідомляють правоохоронців лиш про щось небезпечне, але якщо представники закону вже зацікавлені у вашій особі, вони можуть отримати ордер на вилучення записів усіх ваших розмов. «Вибач, але на тебе доніс твій розумний телевізор...»

Samsung, зі свого боку, заявив, що про ситуацію із прослуховуванням згадується в політиці конфіденційності, на яку всі користувачі опосередковано погоджуються, коли вмикають телевізор. От скажіть мені, коли ви востаннє читали політику конфіденційності перед тим, як уперше ввімкнути девайс? Samsung запевняє, що найближчим часом усі його телевізійні комунікації будуть зашифровані[242]. Але станом на 2015 рік більшість моделей на ринку досі незахищені.

На щастя, існує спосіб вимкнути цю моторошну функцію на телевізорі від Samsung і, мабуть, від інших виробників. На Samsung PN60F8500 й аналогічних продуктах перейдіть у «Меню налаштувань», виберіть «Розумні функції», потім знайдіть рядок «Розпізнавання голосу» й натисніть «Вимк». Але якщо хочете, щоб ваш телевізор не записував конфіденційних розмов, доведеться пожертвувати комфортом. Ви більше не зможете увійти в кімнату і ввімкнути телевізор голосом. Однак усе ще можна взяти пульт дистанційного керування, натиснути кнопку мікрофона й озвучити команду. Або встати з дивана і перемкнути канал самостійно. Знаю. Життя — річ тяжка.

До речі, незашифрованими потоками даних грішить не лише Samsung. У ході тестування телевізорів LG Smart TV дослідник виявив, що дані відправляються через інтернет в LG щоразу, як глядач перемикає канал. А ще в телевізорі включений за замовчуванням параметр «Збір інформації про перегляд». Ваша «інформація про перегляд» містить усі назви файлів з USB-накопичувача, який ви під'єднуєте до телевізора LG. Скажімо, флешки з фотографіями із сімейного відпочинку. Дослідники провели ще один експеримент: створили тестовий відеофайл і завантажили його на USB-накопичувач, який потім під'єднали до телевізора. Проаналізувавши мережевий трафік, вони виявили, що назва

відеофайлу передалася в незашифрованому вигляді через HTTP-трафік і відправилася за адресою GB.smartshare.lgtvsdp.com.

Sensory — компанія, що розробляє вбудовані елементи розпізнавання мови для розумної техніки — сподівається піти ще далі. «Ми вважаємо, що магія [розумних телевізорів] у тому, щоб вони постійно працювали і постійно слухали, — переконує Тодд Мозер, генеральний директор Sensory. — Зараз ця функція споживає забагато енергії. Тож Samsung вчинив мудро, створивши режим прослуховування. Але ми хочемо вийти за рамки і позбутися режимів. Телевізори будуть працювати й слухати нон-стоп, хоч би де ви були»[243].

Тепер ви знаєте, на що здатен ваш цифровий телевізор. Виникає логічне питання: а чи може підслуховувати розмови вимкнений мобільний телефон? Тут є три думки: «так», «ні» і «залежить від ситуації».

Дехто у сфері інформаційної безпеки заприсягається, що телефон перестає підслуховувати, лише якщо витягнути з нього батарею. Однак доказів цьому замало. Є й ті, хто вважає, що вимкнути телефон цілком достатньо — тут уже аргументації побільше. Але я знаю такі випадки, коли через спеціальний вірус смартфон вимикається не до кінця і все ще може записувати розмови поблизу. Тож усе залежить від сукупності чинників.

Існують такі телефони, які «прокидаються», варто вам сказати магічну фразу — щось на зразок голосових телевізорів. А це означає, що телефони постійно слухають, чекаючи на фразу. І всі ваші слова записуються або пересилаються в компанію. Те саме і з телефонами, зараженими шкідливим ПЗ: камера та мікрофон активні весь час, коли ви нікому не телефонуєте. Але, думаю, такі випадки — рідкість.

Що ж, повернемося до теми. Дехто у сфері інформаційної безпеки впевнений, що можна активувати телефон, навіть коли він вимкнений. Так, деякі віруси таки можуть зімітувати вимкнення телефона, коли насправді він працює. Але припущення, що хтось може активувати вимкнений телефон без батареї, здається мені безглуздим. Майже будь-який девайс, що має ПЗ і живиться від акумулятора, можна зламати. Через бекдор[244] не важко змусити девайс прикидатися вимкненим, коли це не так. Однак із девайсом без живлення зробити нічого не можна. Чи можна? Дехто вважає, що АНБ умонтовує в телефони чипи, які слугують джерелом живлення й допомагають стежити за нами, навіть якщо з телефона витягнути батарею.

Навіть якщо ваш телефон підслухати вас не може, то браузер на ньому — легко. Десь 2013 року Google запустив так званий «готвордінг» — функцію, яка допомагає активувати режим прослуховування в Chrome простою командою. Подібний принцип взяли за основу Siri від Apple, Cortana від Microsoft і Alexa від Amazon. Отже, і ваш телефон, і ПК, і отой девайс на журнальному столику — усі вони містять внутрішні хмарні служби, створені реагувати на голосові команди на зразок: «Сірі, де найближча автозаправка?». Вони слухають. І якщо вас це не

лякає, то просто скажу, що запити голосового пошуку записуються і зберігаються необмежений термін[245].

Необмежений.

Як багато ці пристрої чують? Якщо чесно, ніхто досі не знає, що вони роблять, коли не відповідають на запитання або не вмикають/вимикають телевізор. Приміром, дослідники виявили, що у браузері Chrome на звичайному ПК хтось (може, Google?) вмикає мікрофон і слухає всі розмови. Ця функція перекочувала в Chrome від його близнюка з відкритим вихідним кодом — браузера Chromium. У 2015 році дослідники виявили, що у Chromium хтось (може, Google?) слухає всі розмови. Виявилося, браузер вмикає мікрофон за замовчуванням. Однак попри те, що код був частиною ПЗ з відкритим вихідним кодом, дослідити його детальніше не вдалося.

Із цими браузерами все складно. По-перше, «відкритий вихідний код» передбачає, що будь-хто має змогу зазирнути в код. Але тут код — це кіт у мішку, якого ніхто й ніколи не бачив. По-друге, код перекочував у популярну версію браузера через автоматичне оновлення від Google, від якого користувачі не мали змоги відмовитися. І станом на 2015 рік Google все ще його не прибрав. Загалом люди таки можуть відмовитися, але ця відмова вимагає таких глибоких навичок кодування, що середньостатистичний користувач сам не впорається[246].

Але є й інші, більш прості способи приглушити цю моторошну шпигунську функцію в Chrome та інших програмах. На веб-камеру просто наклейте шматок непрозорого скотчу, а в роз'єм для мікрофона на ПК вставте заглушку — такий собі фальшивий мікрофон. Для цього візьміть старі, зламані навушники і відріжте від штекера дріт, потім вставте заглушку в роз'єм для мікрофона. Тепер ваш комп'ютер вважатиме, що там є мікрофон, коли насправді його нема. Ясна річ, якщо ви захочете зателефонувати по скайпу, спершу доведеться дістати заглушку. А ще обов'язково переконайтеся, що два дроти на заглушці не контактують, інакше підсмажите вхід для мікрофона.

Ще один розумний пристрій, що мешкає в нас вдома, — динамік Amazon Echo, через який можна замовляти фільми та інші продукти від Amazon голосом. Echo завжди ввімкнений і слухає кожне наше слово в очікуванні фрази, яка його активує. Позаяк Amazon Echo має більше функцій, ніж розумний телевізор, під час активації користувач має проговорити пристрою до двадцяти п'яти унікальних фраз, перш ніж давати якісь команди. Динамік може озвучити погоду на вулиці, результати останніх спортивних змагань, а також замовити товари — варто лиш попросити. Враховуючи, скільки загальних фраз розпізнають технології Amazon (приміром, «Чи буде завтра дощ?»), логічно припустити, що Echo чує більше, ніж ваш розумний телевізор.

На щастя, Amazon дає змогу видалити голосові дані з Echo[247]. Якщо хочете видалити всі дані (наприклад, якщо хочете продати пристрій), то зробити це можна через інтернет[248].

Усі пристрої на голосовому управлінні «пробуджуються» від конкретної фрази. Але ми й гадки не маємо, що вони роблять під час простою, коли не чують жодних команд. Отож раджу вимикати функцію голосової активації в параметрах конфігурації, коли вона вам не потрібна. Не хвилюйтеся, її завжди можна знову ввімкнути.

Тож додайте Amazon Echo до вашого інтернету речей разом із телевізором, термостатом і холодильником.

Стоп.

Холодильником?

Samsung анонсував модель холодильника, який з'єднується з вашим Google-календарем і відображає майбутні події на вбудованому у двері пласкому екрані. Щось на зразок звичайної дощечки, яку ви туди чіпляли раніше. Хіба що тепер холодильник під'єднується до інтернету через ваш Google-акаунт.

Визнаю, у Samsung було кілька вдалих ідей. По-перше, вони реалізували протокол HTTPS, тому трафік між холодильником і сервером Google-календаря зашифрований. По-друге, Samsung висунув свій футуристичний холодильник як тестовий зразок на DEF CON 23 — одній з найбільших хакерських конвенцій у світі.

Але, за словами дослідників інформаційної безпеки Кена Мунро і Девіда Лоджа, які звикли ламати цифрові телевізори, Samsung не перевіряє сертифікат серверів Google, коли надсилає запит на інформацію з календаря. Сертифікат є гарантом того, що зв'язок між холодильником і серверами безпечні. А так будь-який зловмисник може підробити сертифікат і дістати доступ до з'єднання між холодильником і Google[249].

Ну і що?

Якщо зловмисник проникне у вашу домашню мережу, то зможе не лише попсувати вам молоко і яйця в холодильнику, а й дістати доступ до інформації в Google-акаунті. Вкрасти ваш логін і пароль можна через звичайну атаку посередника, яка дасть змогу хакерові прочитати вашу електронну пошту чи завдати ще більшої шкоди.

Розумні холодильники — поки що явище не повсюдне. Але само собою зрозуміло: що більше девайсів ми під'єднаємо до інтернету і власних домашніх мереж, то більше буде дір у безпеці. І це лякає. Особливо коли йдеться про щось дійсно цінне і конфіденційне, як-от власний дім.

Компанії, що створюють девайси для інтернету речей, працюють над застосунками, які перетворять будь-який пристрій на охоронну систему. Наприклад, колись у вашому телевізорі з'явиться камера відеоспостереження, а застосунок для смартфона чи планшета дасть змогу спостерігати за будь-якою кімнатою вдома чи на роботі дистанційно. А ще можна автоматично вмикати світло, коли датчики фіксують рух всередині чи біля будинку.

Лише уявіть: ви під'їжджаєте до свого дому, а застосунок на телефоні чи в машині фіксує вашу геолокацію і сповіщає систему сигналізації, що ви скоро

прибудете. За п'ятнадцять метрів від будинку застосунок каже домашній сигналізації розблокувати вхідні чи гаражні двері (мобільний застосунок уже під'єднався до будинку і пройшов автентифікацію). Сигналізація під'єднується до системи освітлення і вмикає світло на ґанку, у коридорі і, може, навіть у вітальні чи кухні. Крім того, непогано було б приходити додому під м'яку камерну музику чи новий топ-40 пісень від Spotify, які лунають зі стереосистеми. І, ясна річ, до вашого приходу температура підіймається чи падає залежно від погоди і ваших уподобань.

Домашні сигналізації стали популярними на межі XXI століття. Раніше технік встановлював у дверях та на вікнах будинку датчики, дроти від яких вели до центрального контролера, а той під'єднувався до стаціонарного телефона й обмінювався через нього повідомленнями з охоронною службою. Якщо ви ставили будинок на сигналізацію, а хтось сторонній пробирався через двері чи вікна, охоронна служба вам телефонувала.

Також установлювалася автономна батарея на випадок, якщо зникне живлення. Однак зазвичай позбавити стаціонарного телефона живлення можна, лише відрізавши телефонний дріт, що веде до будинку.

Коли більшість людей позбулася стаціонарних дротяних телефонів і перейшла виключно на мобільний зв'язок, охоронні фірми почали працювати зі стільниковими телефонами. Останнім часом вони працюють через мобільні застосунки.

Датчики на дверях і вікнах тепер бездротові. Так набагато зручніше: не треба свердлити і тягнути огидні кабелі. Але так ще й набагато більше ризику. Дослідники неодноразово зазначали, що сигнал від бездротових датчиків не шифрується. Потенційному зловмисникові достатньо лиш перехопити зв'язок між пристроями, щоб відключити сигналізацію. Наприклад, якщо я зламаю вашу локальну мережу, то зможу перехопити повідомлення між серверами охоронної компанії і вашою системою сигналізації (якщо вона під'єднана до локальної мережі і не зашифрована). А з цими повідомленнями на руках я зможу підмінити команди сигналізації й отримати контроль над вашим розумним будинком.

Зараз деякі компанії пропонують «самостійну» сигналізацію. Тобто в разі будь-яких маніпуляцій із датчиками на ваш мобільний телефон надходить текстове повідомлення з інформацією про зміну. Або застосунок виводить зображення з домашньої веб-камери. У будь-якому випадку, ви самі контролюєте ситуацію і будинок. Чудовий варіант... поки вам не відключать Wi-Fi.

Навіть якщо інтернет вдома працює, зловмисники все одно можуть вимкнути чи заглушити сигнали системи сигналізації. Наприклад, спровокувати хибну тривогу (за яку подекуди доводиться платити домовласникові), що можна зробити з вулиці на відстані до 230 метрів. Забагато хибних тривог можуть

виставити систему ненадійною (і витягнути з кишені домовласника кругленьку суму).

Або зловмисник може заглушити сигнали «самостійного» датчика, транслюючи радіошум, який перешкоджає зв'язку між датчиками й головним контролером. Це знешкоджує сигналізацію, нейтралізує захист і допомагає злочинцю проникнути в будинок.

Чимало людей установили собі домашні веб-камери: чи то для власної безпеки, чи то для контролю прибиральника або няні, чи то для спостереження за похилою, немічною людиною або близькими з особливими потребами. На жаль, більшість таких веб-камер вразливі до дистанційних атак.

Є така загальнодоступна пошукова система Shodan, яка містить інформацію про нетрадиційні пристрої, під'єднані до інтернету[250]. Shodan відображає не лише домашні пристрої, під'єднані до інтернету речей, а й внутрішні мережі муніципальних служб й автоматизовані системи керування, які неправильно приєднали до громадської мережі. А ще потоки даних із купи неправильно налаштованих веб-камер у всьому світі. За підрахунками, щодня у світі працюють до ста тисяч веб-камер із під'єднанням до інтернету, які слабко захищені або незахищені взагалі.

Серед них й інтернет-камери без автентифікації за замовчуванням від компанії D-Link, через які можна стежити за особистим життям людей (залежно від ракурсу камери). Зловмисник може просто пошукати в інтернеті, які моделі камер D-Link ідуть за замовчуванням без автентифікації, а потім зайти на, приміром, Shodan, знайти потрібні моделі й насолоджуватися відео з чужих камер на дозвіллі.

Щоб цього не трапилося, вимикайте інтернет-камери, коли вони вам не потрібні. Краще зробити це вручну, щоб точно переконатися. А коли користуєтеся камерами, перевірте, що на них стоїть автентифікація і сильний пароль — не той, який іде за замовчуванням.

Якщо думаєте, що ваш дім — кошмар для конфіденційності, то не кваптеся з висновками. У наступному розділі я розповім вам про роботу.

---

232 http://www.amazon.com/review/R3IMEYJFO6YWHD.

233 https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home.pdf.

234 http://venturebeat.com/2014/08/10/hello-dave-i-control-your-thermostat-googles-nest-gets-hacked/.

235 HAL 9000 — вигаданий комп'ютер із циклу творів «Космічна Одіссея» Артура Кларка, що мав здатність до самонавчання і є прикладом штучного інтелекту в науковій фантастиці. — *Прим. пер.*

236 http://www.forbes.com/sites/kashmirhill/2014/07/16/nest-hack-privacy-tool/.

237 http://venturebeat.com/2014/08/10/hello-dave-i-control-your-thermostat-googles-nest-gets-hacked/.

238 http://www.networkworld.com/article/2909212/security0/schneier-on-really-bad-iot-security-it-s-going-to-come-crashing-down.html.

239 http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/.

240 http://www.dhanjani.com/blog/2013/08/hacking-lightbulbs.html.

241 http://www.wired.com/2009/11/baby-monitor/.

242 http://www.bbc.com/news/technology-31523497.

243 http://mashable.com/2012/05/29/sensory-galaxy-s-iii/.

244 Бекдор (від англ. back door — «чорний хід») — ефект алгоритму, який навмисно вбудовується розробником і допомагає отримати несанкціонований доступ до даних чи дистанційного керування операційною системою і комп'ютером загалом. — *Прим. пер.*

245 http://www.forbes.com/sites/marcwebertobias/2014/01/26/heres-how-easy-it-is-for-google-chrome-to-eavesdrop-on-your-pc-microphone/.

246 http://www.theguardian.com/technology/2015/jun/23/google-eavesdropping-tool-installed-computers-without-permission.

247 Думаю, найпростіший спосіб — відкрити застосунок Amazon Echo. Перейдіть до налаштувань, а потім виберіть Історія>Індивідуальний запис>Видалити.

248 Увійдіть у свій акаунт на Amazon, потім клікніть Налаштування акаунта>Мої пристрої> ->Amazon Exo>Видалити.

249 http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/.

250 www.shodan.io.

Розділ 13

Про що не має знати ваш бос

Усе ще читаєте? Думаю, ви не на жарт стурбовані своїм приватним життям. Але більшість із нас ховає це життя не від федерального уряду — нас хвилює робота. Зокрема начальники, які стежать за тим, що ми робимо в інтернеті через корпоративну мережу (купуємо товари, граємо в ігри, просто байдикуємо). Ми просто хочемо прикрити свій зад!

І з кожним днем це дається дедалі важче, почасти завдяки мобільним телефонам. Щоразу, коли фінансовому менеджерові Чиказької ландшафтної компанії Джейн Роджерс треба знати, чи на робочих місцях її підлеглі, вона перевіряє їх точне місцеперебування на ноутбуці. Для цього Джейн, як і решта менеджерів і директорів, користується програмою стеження на корпоративних смартфонах і технічними фургонами, обладнаними GPS. Якось клієнт запитав Джейн, чи був один з їхніх ландшафтних дизайнерів на місці робіт. Кілька кліків — і Джейн підтвердила, що між 10:00 і 10:30 один з її працівників був у вказаному місці.

Телематичний сервіс, яким користується Роджерс, виходить далеко за межі геолокації. Наприклад, на дев'яти корпоративних телефонах вона може проглядати фотографії, текстові повідомлення та імейли, відправлені її садівниками. Вона також має доступ до журналу викликів й історії браузера. Але Роджерс запевняє, що користується лише функцією GPS[251].

Стеження по GPS уже давно використовують у сфері послуг. Приміром, логістичній компанії UPS — у поєднанні з власною системою алгоритмічного прокладання маршруту ORION — це дало можливість скоротити витрати на бензин шляхом моніторингу і вибору оптимальних маршрутів для своїх водіїв. А ще компанія змогла попрощатися з ледачими кур'єрами. У результаті UPS збільшила обсяг доставлень на 1,4 мільйона додаткових посилок у день, позбавившись водночас тисячі водіїв[252].

Усе це чудово... для роботодавців, які запевняють, що з більшими прибутками зможуть платити більшу зарплатню. Але як почуваються працівники? У тотального контролю є й інший бік медалі. Якось журнал Harper's Magazine опублікував історію про водія, за яким стежили по GPS під час роботи. Водій (який побажав залишитися інкогніто) розповів, що програма розраховувала час доставлення по секундах і сигналізувала, коли він не вкладався в оптимальний час. Часто наприкінці робочого дня затримок збиралося аж на чотири години.

Як так сталося? Водій каже, що інколи за один маршрут треба доставити кілька посилок, а ORION часто це не враховує. Його колеги з нью-йоркського сортувального центру потерпають від хронічних болів у спині й колінах, бо намагаються доставити якомога більше вантажу за раз, щоб виконувати норму

за програмою. Навіть попри постійні попередження від компанії про роботу з важкими посилками. Люди стають жертвами спостереження.

Ще одна сфера, де шпигування за працівниками досить популярне, — це сфера харчування. Обслуговий персонал контролюють й оцінюють різноманітними способами — від камер у стелі ресторану до планшетів на столах відвідувачів. Дослідження, проведене 2013 року вченими з Вашингтонського університету, Університету Бріґама Янґа і Массачусетського технологічного інституту, показало, що програма моніторингу крадіжок, яку встановили в 392 ресторанах, скоротила кількість внутрішніх крадіжок на 22 %[253]. Як я і казав, активне спостереження змінює поведінку людей.

Наразі в США не існує федеральних законів, які забороняють компаніям стежити за своїми працівниками. Лише штати Делавер і Коннектикут вимагають, щоб роботодавці повідомляли підлеглим про спостереження. Але в більшості штатів співробітники й гадки не мають, контролюють їх на роботі чи ні.

А як щодо офісних працівників? Американська асоціація менеджменту повідомила, що 66 % роботодавців контролюють інтернет-трафік підлеглих, 45 % фіксують натискання клавіш на комп'ютері (і вважають час простою як «перерви»), а 43 % продивляються електронну пошту співробітників[254]. Деякі компанії стежать за календарями Outlook, темами імейлів і миттєвими повідомленнями. Ці дані нібито допомагають з'ясувати, на що підлеглі витрачають робочий час: скільки продавці спілкуються з клієнтами, які підрозділи компанії контактують між собою по електронній пошті, скільки часу співробітники витрачають на наради і як довго відсутні на робочому місці.

Звичайно, є й позитивний аспект: так компанія може ефективніше планувати наради й організовувати взаємодію різних відділів. Але це не скасовує того факту, що хтось таки збирає корпоративні дані. І одного чудового дня ці дані можуть потрапити до рук правоохоронців або принаймні позначитися на оцінці продуктивності.

На роботі ви як на долоні. Усе, що проходить через корпоративну мережу, належить компанії. Це не ваше. Якщо плануєте відпустку, перевіряєте особисту пошту чи останнє замовлення на Amazon через корпоративний телефон, ноутбук або VPN, не дивуйтеся, що компанія контролює кожен ваш крок.

Є один простий спосіб обвести навколо пальця занадто допитливого менеджера чи навіть колег. Якщо вам потрібно на нараду чи в туалет і доводиться залишити робочий стіл, заблокуйте екран комп'ютера. Серйозно. Ніколи не залишайте відкритим імейл чи подробиці проекту, на який ви вбили кілька тижнів. Вони як приманка. Заблокуйте комп'ютер до повернення. Це лише кілька секунд, але зекономить вам купу нервів. Ще можна встановити таймер, який блокуватиме неактивний екран через кілька секунд. Або завантажте собі блютуз-застосунок, який автоматично заблокує екран, якщо ваш телефон не поруч з комп'ютером. Хоча не так давно з'явилися спеціальні USB-

пристрої для розблокування. Деякі компанії деактивують USB-порти на корпоративних ноутбуках і ПК. Якщо ж у вас USB-порти робочі, то ваш комп'ютер можна розблокувати і без пароля[255].

Протягом робочого дня через наші комп'ютери проходять не лише корпоративні секрети, а й особисті імейли з документами, які ми іноді друкуємо на роботі. Якщо турбуєтеся про конфіденційність, забудьте про особисті справи в офісі. Зведіть міцну стіну між життям робочим і особистим. Або беріть з дому власний ноутбук чи айпад, якщо вам кортить зайнятися особистими справами під час перерви. Якщо у вас стільниковий телефон, ніколи не користуйтеся корпоративним Wi-Fi. Якщо у вас портативний хот-спот, вимкніть трансляцію ідентифікатора SSID (див. розділ 8). В особистих справах користуйтеся на роботі лише мобільним інтернетом.

Коли приходите на роботу, залишайте все особисте вдома. Ви б не стали говорили про вкрай особисті речі з малознайомими колегами, так? Тож тримайте власні справи подалі від комп'ютерної мережі компанії (особливо, якщо шукаєте щось, пов'язане зі здоров'ям чи новою роботою).

Це складніше, ніж здається. Ми звикли до цілодобового доступу до інформації та інтернету. Але якщо хочете оволодіти мистецтвом невидимості, у жодному разі не перетворюйте справи особисті на публічні.

Припустимо, усе, що ви робите на робочому комп'ютері, є публічним. Це ще не означає, що IT-відділ активно стежить саме за вашим ПК і покарає вас за те, що ви роздрукували своїй дитині проект на дорогому кольоровому принтері на п'ятому поверсі. Але все можливо. Запис про це збережеться. І якщо в майбутньому щодо вас виникнуть підозри, компанія таки зможе проглянути записи всього, що ви колись робили на робочому комп'ютері. Це її комп'ютер, не ваш. І її мережа. А отже, вона сканує все, що надходить і виходить з компанії.

Поясню вам на прикладі Адама, який завантажив свій кредитний звіт на робочий комп'ютер. Він увійшов на сайт кредитної установи через корпоративний комп'ютер по корпоративній мережі. Припустимо, ви, як і Адам, теж завантажили кредитний звіт на роботі. Непогано його б одразу роздрукувати, еге ж? Чому б не зробити це через отой робочий принтер у кутку? Що ж, тоді на жорсткому диску принтера опиниться копія PDF-файлу з вашою кредитною історією. Цей принтер — не ваш. Ви не знаєте, що трапиться із жорстким диском, коли принтер відживе своє і його заберуть на утилізацію. Зараз деякі принтери шифрують диски, але ви впевнені, що ваш робочий принтер саме такий? Навряд чи.

І це ще не все. Кожен документ у Word чи Excel містить метадані, що описують документ. Зазвичай це ім'я автора, дата створення, кількість редакцій, розмір файлу і деякі додаткові відомості. За замовчуванням ця інформація в продуктах Microsoft прихована: вам доведеться трохи її пошукати[256]. Однак Microsoft створив функцію «Інспектор документів», через яку можна видалити ці відомості перед тим, як відсилати документ[257].

Опитування, проведене 2012 року компаніями Xerox і McAfee, виявило, що 54 % працівників незавжди дотримуються політики комп'ютерної безпеки компанії, а 51 % хоч раз копіювали, сканували чи друкували особисту конфіденційну інформацію на роботі, якщо офіс оснащений принтером, ксероксом чи багатофункціональним пристроєм. І небезпека чатує не лише на роботі: те саме і з принтерами в місцевому копіцентрі чи бібліотеці. Усі вони оснащені жорсткими дисками, які запам'ятовують усе, що колись друкували. Якщо вам потрібно роздрукувати щось особисте, краще зробити це вдома — на принтері і по мережі, над якими у *вас* є контроль.

Шпигунство зараз стає дедалі креативнішим. Навіть на роботі. Деякі компанії пускають у хід нетрадиційні офісні пристрої, які ми сприймаємо як належне і навіть уявити не можемо, що вони здатні за нами стежити.

На думку відразу спадає історія старшокурсника Колумбійського університету на ім'я Анґ Цуй. Хлопець поставив собі запитання, чи може зламати відділ компанії і вкрасти конфіденційні дані нетрадиційним способом. Почав Цуй з атаки на лазерні принтери — невід'ємний елемент сучасного офісу.

Цуй помітив, що принтери вже давно застаріли. Я й сам це зауважував, коли проводив тести на проникнення: іноді мені вдавалося дістати доступ до корпоративної мережі саме через принтери. Усе через те, що працівники рідко змінюють пароль адміністратора на принтерах внутрішнього користування.

Програмне забезпечення та прошивка в принтерах (особливо платних, для домашнього офісу) містять купу дірок у безпеці. Проблема в тому, що мало хто бачить у робочому принтері загрозу. Люди вводять себе в оману так званою «сліпою безпекою»: якщо ніхто не помічає недоліків, то ви в безпеці.

Але, як я вже говорив, ледь не всі моделі принтерів і ксероксів мають дещо спільне: жорсткий диск. І якщо цей жорсткий диск не зашифрований (а таких ще дуже багато), можна дістати доступ до всього, що колись друкував принтер. Про це вже знають роками. Але Цуя цікавило те, чи зможе він «налаштувати» принтер проти компанії й витягнути з нього всі надруковані документи. І зробити це він хотів через атаку на код прошивки — програму, вбудовану в чип принтера. На відміну від ПК і мобільних телефонів, цифрові телевізори й інша «розумна» техніка не мають ні потужностей, ні ресурсів для функціонування повноцінної операційної системи, як-от Android, Windows чи iOS. Замість цього ці пристрої працюють на так званих операційних системах реального часу (RTOS), які зберігаються на окремих чипах всередині пристрою (і які часто називають «прошивкою»).

Ці чипи містять лише команди, потрібні для роботи системи. Не більше, не менше. Й іноді навіть ці прості команди доводиться оновлювати, переналаштовуючи або замінюючи чипи. Оскільки робиться це нечасто, виробники просто не бачать сенсу в належних заходах безпеки. Оця відсутність оновлення й була прогалиною в безпеці, якою скористався Цуй.

Хлопець вирішив подивитися, що станеться, якщо він зламає формат файлу, у якому принтери HP приймають оновлення прошивки. Виявилося, HP не перевіряють справжність кожного оновлення. Тому він створив власну прошивку принтера... і принтер прийняв її. Отак просто. Принтер не вимагав підтвердження того, що оновлення дійсно надійшло від HP. Йому було потрібно лиш те, щоб код був у належному форматі.

І цим він дав хакерові зелене світло.

В одному відомому експерименті Цуй зміг увімкнути термоблок (деталь принтера, яка нагріває папір після нанесення чорнил) і залишити його ввімкненим, що рано чи пізно призвело б до займання принтера. Постачальник (не HP) негайно запевнив, що в панелі термоблока встановлено термозахист, тому принтер просто не може перегрітися. Однак у цьому й була суть експерименту: Цую вдалося відключити функцію термозахисту, тож пристрій насправді міг загорітися.

У результаті експериментів Цуй зі своїм куратором Сальваторе Стольфо дійшли висновку, що принтери — слабкі ланки в будь-якій компанії чи будинку. Приміром, відділ кадрів компанії зі списку Fortune 500 може отримати на пошту заражене резюме. Поки кадровик друкуватиме документ, на принтер може встановитися хибна версія прошивки.

Запобігти крадіжці документів можна завдяки фупкції безпечного друку, або друку за запитом, коли документи друкуються лише після перевірки автентичності користувача (зазвичай вводиться пароль). Це можна реалізувати через PIN-код, смарт-карту чи відбиток пальця. Друк за запитом також запобігає друку несанкціонованих документів. Ви ж не хочете, щоб по офісу була розкидана конфіденційна інформація?[258]

Після принтера Цуй почав шукати в типовому офісі наступну вразливу «жертву»... і натрапив на інтернет-телефони, що працюють на протоколі VoIP. Та сама історія, що і з принтерами: ніхто не звернув уваги на ледве помітну, але таки вкрай очевидну роль цих пристроїв у зборі інформації. А ще на VoIP-телефонах можна так само підробити і встановити оновлення системи. Більшість VoIP-телефонів має функцію гучного зв'язку, якою часто користуються в офісах, щоб звільнити руки. Тож на зворотній стороні слухавки є не лише динамік, а й мікрофон. А ще в такому телефоні є важільний перемикач, який сигналізує девайсові, коли хтось бере слухавку і хоче зробити або прийняти виклик, а також коли слухавку кладе і тим самим вмикає гучний зв'язок. Цуй зрозумів: якщо зламати цей перемикач, телефон буде слухати розмови поблизу через мікрофон гучного зв'язку. І навіть не беручи слухавки!

Хоча тут існує одне «але»: на відміну від принтера, який може отримати фальшивий код по інтернету, VoIP-телефони потрібно «оновлювати» вручну. А отже, код можна поширити лише через USB-накопичувач. Але для Цуя це не було проблемою. За нічну зміну прибиральник через USB міг установити код на кожен телефон, паралельно прибираючи офіс.

Цуй представив дослідження на низці конференцій — кожен раз із новою маркою VoIP-телефонів. Щоразу виробникові повідомляли про експеримент заздалегідь. І щоразу цей виробник вносив корективи до своїх пристроїв. Але Цуй попереджає: той факт, що корективи існують, не означає, що їх вносять повсюдно. Вразливі телефони все ще можуть працювати в офісах, готелях і лікарнях.

То як же Цуй отримав дані з телефона? Позаяк компанії контролюють свої комп'ютерні мережі щодо незвичайної активності й помітили б зміни, довелося шукати інший шлях. Цуй зупинився на радіохвилях.

Дослідники зі Стенфордського університету та Ізраїлю виявили, що через мобільний телефон, який лежить поруч із комп'ютером, сторонні особи можуть підслуховувати ваші розмови. Щоб провернути фокус, спершу треба завантажити вірус на телефон. Як думаєте, наскільки спростить справу фальшивий застосунок із потрібним кодом, який жертва завантажить сама?

Шкідливе ПЗ викручує чутливість гіроскопа в телефоні на максимум, і тепер він здатен вловлювати навіть слабкі вібрації. Дослідники кажуть, що сюди входять і найменші коливання повітря, які спричинює людський голос. Операційна система Android від Google уможливлює зчитування інформації з датчиків зі швидкістю 200 Гц, або 200 циклів за секунду. Людський голос зазвичай коливається в діапазоні від 80 до 250 Гц. Тобто датчик здатен вловити більшість голосів. Дослідники навіть пішли далі і створили спеціальну програму розпізнавання голосу, яка декодує сигнали в діапазоні 80–250 Гц[259].

Щось подібне Цуй знайшов у VoIP-телефонах і принтерах. Виявляється, деталі будь-якого мікрочипа в будь-якому пристрої можна змусити коливатися в унікальній послідовності і в такий спосіб передавати дані по радіочастоті. Цей феномен Цуй назвав «фантена»[260]. Фантена — це такий собі віртуальний майданчик для потенційних зловмисників. «Офіційно, — каже дослідник безпеки Майкл Оссманн, у якого Цуй позичив ідею, — фантена — це антена, яка не задумувалася розробником як антена, але зловмисник використовує її саме так»[261].

А які ще існують способи шпигувати на роботі, окрім фантени?

Ізраїльські дослідники виявили, що якщо на звичайні стільникові телефони встановити вірус, вони зможуть приймати двійкові дані з комп'ютерів. А дещо раніше стенфордські дослідники дізналися, що датчики в телефонах можуть перехоплювати звук електронних сигналів бездротової клавіатури[262]. Ці висновки ґрунтуються на аналогічних дослідженнях, проведених ученими з MTI і Технологічного інституту Джорджії[263]. Якщо коротко, то треті особи можуть на відстані стежити за всім, що ви друкуєте, проглядаєте чи вмикаєте на роботі.

Приміром, ви користуєтеся бездротовою клавіатурою. Бездротовий радіосигнал, що йде з клавіатури на ноутбук або ПК, можна перехопити. Дослідник інформаційної безпеки Семі Камкар розробив для цього так званий KeySweeper — замасковану USB-зарядку, яка працює без дротів і фоном шукає,

розшифровує, зберігає і відправляє (через GSM) усі натискання клавіш із будь-якої бездротової клавіатури Microsoft поблизу[264].

Ми вже говорили про небезпеку фальшивих хот-спотів у кафе й аеропортах. Те саме чатує і на роботі. Хтось у вашому офісі може встановити власний хот-спот, а ваш телефон до нього автоматично під'єднається. IT-відділи зазвичай сканують приміщення на предмет таких пристроїв, але не всюди і незавжди.

Сучасний аналог такого хот-споту — власна станція стільникового зв'язку. Фемтосоти — це невеличкі пристрої, які можна придбати у вашого мобільного оператора. Вони створені для того, щоб поліпшити мобільне покриття в будинку чи офісі, де сигнал занадто слабкий. І тут є свої ризики.

Позаяк фемтосоти є базовими станціями стільникового зв'язку, ваш телефон може під'єднуватися до них без вашого відома. Подумайте про це.

У США правоохоронні органи користуються StingRay — IMSI-перехоплювачем, реалізованим у формі симулятора станції стільникового зв'язку. Існують і аналоги: TriggerFish, Wolfpack, Gossamer тощо. Хоча технології різняться, усі вони загалом працюють як фемтосоти без стільникового зв'язку і призначені для перехоплення IMSI вашого мобільного телефона. У США IMSI-перехоплювачі не таке повсюдне явище, як у Європі... поки що. Ними користуються, приміром, на масштабних соціальних протестах, щоб правоохоронці могли ідентифікувати всіх присутніх. Імовірно, організатори мітингу постійно висітимуть на телефоні, щоб скоординувати захід.

Після тривалої судової тяганини Американська спілка захисту громадянських свобод (ACLU) Північної Каліфорнії таки отримала від уряду документи, у яких докладно описано їхню роботу зі StingRay. Наприклад, спершу правоохоронцям треба отримати відповідний судовий наказ. Загалом вони користуються автоматичним реєстратором телефонних розмов, що записує набрані цифри й видає номер абонента, якому телефонують, і технологією реєстрації вхідних дзвінків. Крім того, за наявності ордера правоохоронні органи можуть легально отримати запис телефонного дзвінка або текст електронного листа. Wired написали, що в отриманих документах ідеться про пристрої, які «теоретично можуть перехоплювати вміст повідомлень, а отже, на таких пристроях треба вимкнути фупкцію перехоплення, якщо таке перехоплення не було дозволено відповідним ордером», який дає право здійснювати перехоплення повідомлень у режимі реального часу[265].

Припустимо, за вами не спостерігають правоохоронні органи. Припустимо, ви працюєте в компанії з жорсткими обмеженнями (наприклад, на комунальному підприємстві). Хтось може принести на роботу фемтосоту, щоб дзвонити в особистих справах поза телефонною системою компанії. Проблема в тому, що працівник із модифікованою фемтосотою зможе здійснити атаку посередника і прослухати ваші дзвінки чи перехопити повідомлення.

Під час виступу на конференції Black Hat USA 2013 дослідники змогли перехопити дзвінки, SMS-повідомлення і навіть веб-трафік волонтерів з

аудиторії через їхні фемтосоти від Verizon. Прогалини у фемтосотах від Verizon начебто полагодили ще до презентації, але дослідники наочно продемонстрували, що ними все одно не варто користуватися.

Деякі телефони на Android попереджають вас, коли ви перемикаєтеся з однієї стільникової мережі на іншу. Айфони — ні. «Ваш телефон під'єднається до фемтосоти без вашого відома, — пояснив дослідник Даґ Деперрі. — Це вам не Wi-Fi. Тут у вас нема вибору»[266].

Компанія Pwnie Express розробила пристрій під назвою Pwn Pulse, який ідентифікує фемтосоти і навіть IMSI-перехоплювачі на зразок StingRay[267]. Так компанії можуть дізнатися про всі стільникові мережі поблизу офісу. Уряд якось масово закупив такі девайси, що виводять повний спектр потенційних стільникових загроз, але акція була одноразовою.

Хоча скайп дуже комфортний у використанні, у питаннях конфіденційності про комфорт забудьте. За словами Едварда Сноудена, чиї одкровення вперше опублікували The Guardian, Microsoft співпрацював з АНБ для перехоплення й контролю розмов у скайпі. В одному документі йдеться про те, що програма АНБ під назвою Prism проглядає відео користувачів Skype та інших подібних програм. «Вони вже давно слухають аудіозаписи розмов, але без супроводу відео. Тепер же аналітики мають повну картину», — пишуть The Guardian[268].

У березні 2013 року студент кафедри комп'ютерних наук Університету Нью-Мексико виявив, що TOM-Skype — китайська версія Skype, створена внаслідок співпраці Microsoft і китайської компанії TOM Group, — завантажує список ключових слів на комп'ютер кожного користувача програми, бо в Китаї є слова та фрази, які забороняється шукати в інтернеті (зокрема «площа Тяньаньмень»). А ще TOM-Skype повідомляє китайському урядові ім'я власника акаунта, час і дату повідомлення, а також інформацію про те, було це повідомлення відправлено чи отримано[269].

Дослідники виявили, що навіть висококласні системи відеоконференції — оті дорогі, а не безкоштовний скайп — можна також зламати через атаку посередника. Тобто сигнал спочатку потрапляє до третіх рук, а вже потім — до вас. Те саме стосується і аудіоконференцій. Якщо в модератора конференції немає списку під'єднаних номерів і якщо він раптом не вирішить перевірити якийсь сумнівний номер (скажімо, із кодом іншої країни), то помітити непроханих осіб на лінії просто неможливо. Модератор повинен зв'язатися з новоприбулими учасниками і, якщо вони не зможуть підтвердити свою особу, перервати конференц-зв'язок і скористатися для цього іншим номером.

Скажімо, ваша компанія витратила купу грошей на дуже дорогу систему відеоконференції. Логічно припустити, що вона надійніша за систему нижчого класу. Але це не так.

Дослідник Г. Д. Мур покопався у висококласних системах і виявив, що майже всі вони автоматично відповідають на вхідні відеодзвінки за замовчуванням. Це логічно. Ви просто призначаєте збори на десяту ранку і чекаєте, поки учасники

самі приєднаються. Але будь-хто, в кого є ваш номер, може набрати його в будь-який час і, в прямому сенсі, зазирнути у ваш кабінет.

«Популярність відеосистем конференц-зв'язку у сфері венчурного капіталу й фінансів породила цілу купу вкрай ласих цілей для будь-якого зловмисника, який займається промисловим шпигунством чи хоче обійти в бізнесі конкурента», — пише Мур[270].

Як відшукати ці системи конференц-зв'язку? Вони працюють на унікальному протоколі H.323. Мур опрацював лиш маленький шматочок інтернету — і знайшов 250 тисяч систем, які користуються цим протоколом. За його оцінками, майже п'ять тисяч таких систем були налаштовані на автоматичну відповідь — мізерний відсоток, але все ж вагома цифра. І це лише крихта від усього інтернету.

Яку інформацію може зібрати зловмисник, зламавши таку систему? Камера конференц-зв'язку перебуває під контролем користувача, тож зловмисник дистанційно може її нахилити вгору, вниз, вліво або вправо. Зазвичай на таких камерах нема червоного ліхтарика, що говорить про активність камери, тому якщо ви не спостерігаєте за камерою, цілком можете і не помітити, що хтось її рухає. Камера також може масштабувати зображення. Так дослідницька група Мура змогла прочитати шестизначний пароль, що висів на стіні в шести метрах від камери. А ще зазирнути у відкриту електронну пошту на екрані користувача на іншому кінці офісу.

Наступного разу, як будете на роботі, подумайте, що можна побачити з вашої камери. Можливо, десь позаду висить організаційна структура відділу. Можливо, екран вашого робочого ПК дивиться на конференц-зал. Можливо, видно фотографії вашої родини. І все це зможе побачити зловмисник, скориставшись отриманою інформацією проти вашої компанії. Чи проти вас особисто.

Деякі розробники знають про цю проблему у своїх системах. Приміром, Polycom видала товстенне керівництво з посилення захисту, навіть обмеживши переміщення камери[271]. Проте в айтішників часто немає часу на ці рекомендації. Та й за проблему це інколи не вважають. У результаті — тисячі систем конференц-зв'язку з налаштуваннями за замовчуванням, які легко знайти в інтернеті.

Дослідники також виявили, що корпоративний брандмауер неправильно працює з протоколом H.323. Вони пропонують призначити девайсові публічну інтернет-адресу і створити для нього правило в корпоративному брандмауері.

Але найбільший ризик криється в тому, що іноді консоль адміністратора в системах конференц-зв'язку практично незахищена розробником. Приміром, якось Мур з командою змогли дістати доступ до системи юридичної фірми, де зберігалися номери всіх членів ради директорів відомого інвестиційного банку. Дослідники просто придбали старий пристрій для відеоконференцій на eBay і знайшли на жорсткому диску дані фірми, зокрема й адресну книгу з десятками

приватних номерів, більшість з яких були налаштовані на автоматичну відповідь на вхідні інтернет-дзвінки[272]. Тут як зі старими принтерами та копіювальними машинами: якщо в пристрої є жорсткий диск, треба надійно стерти з нього дані перед продажем.

Іноді на роботі нам доручають працювати над проектом разом із колегою, який перебуває десь на іншому кінці світу. Зазвичай файлами можна обмінюватися по корпоративній електронній пошті, але іноді вони настільки великі, що ви просто не зможете прикріпити їх до листа. Тож люди все частіше користуються файлообмінниками для відправки великих файлів.

Чи безпечні ці хмарні сервіси? Почасти.

Усі чотири гіганти файлообміну — iCloud від Apple, Google Диск, OneDrive від Microsoft (раніше SkyDrive) і Dropbox — забезпечують двоетапну верифікацію. Тобто ви отримуєте на телефон код доступу для підтвердження особи. І хоча всі чотири сервіси шифрують дані під час передавання, вам усе одно треба шифрувати їх перед відправкою самостійно. Звісно ж, якщо ви не хочете, щоб їх прочитала компанія чи АНБ[273].

На цьому схожість сервісів закінчується.

Двофакторна автентифікація — це добре, але я все одно можу її обійти, вкравши неактивні акаунти. Приміром, нещодавно мене попрохали зробити тест на проникнення. За допомогою загальнодоступних інструментів клієнт додав 2ФА від Google до корпоративного сервісу VPN. Я зміг увійти, знайшовши у службі каталогів компанії дані входу для співробітника, який досі не користувався VPN. Позаяк я увійшов в акаунт раніше за нього, система запропонувала мені налаштувати 2ФА через Google Authenticator. Доки співробітник не скористується своїм VPN-акаунтом, зловмисник матиме доступ.

Для «даних у стані спокою» Dropbox використовує 256-бітне шифрування AES (яке є досить надійним). Однак компанія тримає в себе ключі, що може вилитися в несанкціонований доступ з боку Dropbox чи правоохоронних органів. Google Диск і iCloud мають значно слабше 128-бітне шифрування для цього типу даних. Тобто теоритично інформацію можна розшифрувати за допомогою сильних обчислювальних потужностей. Microsoft OneDrive взагалі не обтяжує себе шифруванням. Підозрюю, що зроблено це спеціально. Може, навіть за проханням уряду.

Google Диск представив нову функцію управління правами на доступ до інформації (IRM). Тепер, окрім документів, таблиць і презентацій, створених безпосередньо в Google Документах, Google Диск приймає PDF та інші формати. Серед інших корисних функцій — можливість відключити завантаження, друк і копіювання файлів для коментаторів і гостей. А також заборонити людям, з якими ви поділилися обмеженим файлом, відкривати до нього доступ іншим. Звісно ж, функції управління доступні лише власникові файлів. Тож якщо хтось ділиться з вами файлом, саме він повинен встановити обмеження конфіденційності, не ви.

Microsoft також представив унікальну функцію пофайлового шифрування. Тут усе просто: функція, яка шифрує кожен окремий файл окремим ключем. Якщо хтось зламає один ключ, то отримає доступ до одного файлу, а не всього архіву. Але функція не працює за замовчуванням, тож користувачам доведеться звикати шифрувати кожен файл вручну.

Що не так вже погано, як здається. Раджу всім працівникам і користувачам звикнути до шифрування даних перед відправкою в «хмару». Так ви збережете контроль над ключами. Якщо урядовці раптом звернуться в Apple, Google, Dropbox чи Microsoft, то залишаться ні з чим: ключі будуть лише у вас.

А можете скористатися одним хмарним сервісом, якість якого відрізняється від решти, — SpiderOak. Він пропонує всі принади хмарного сховища і синхронізації, а також стовідсоткову конфіденційність даних. SpiderOak захищає конфіденційні дані користувачів за допомогою двофакторної автентифікації і 256-бітного шифрування AES, тож усі ваші файли й паролі будуть в безпеці. Користувачі можуть спокійно зберігати і синхронізувати конфіденційну інформацію, адже компанія не має жодного доступу до ваших даних і паролів.

Але більшість користувачів таки продовжить користуватися іншими сервісами на свій страх і ризик. Ми надто звикли до зручності хмарних сховищ. Як і правоохоронні органи. Проблема в тому, що ваші дані в «хмарі» не захищенні четвертою поправкою, як, приміром, документи в шухляді і навіть на ПК. Правоохоронні органи дедалі частіше вилучають хмарні дані. І це не може не турбувати. Доступ їм дістати досить легко: усе, що ви завантажуєте в інтернет (через електронну пошту, Google Диск, Shutterfly тощо), потрапляє на сервер, який належить постачальникові хмарних послуг, а не вам. Єдиний спосіб захиститися — це усвідомити, що всі завантажені дані можна вилучити, і діяти відповідно, заздалегідь шифруючи документи.

---

251 http://www.wsj.com/articles/ SB10001424052702303672404579151440488919138.

252 http://theweek.com/articles/564263/rise-workplace-spying.

253 https://olin.wustl.edu/docs/Faculty/Pierce_Cleaning_House.pdf.

254 http://harpers.org/archive/2015/03/the-spy-who-fired-me/.

255 https://room362.com/post/2016/snagging-creds-from-locked-machines/.

256 Зазвичай метадані документа приховані. Метадані вашого документа можна переглянути, клікнувши на кнопку Microsoft Office>Підготувати>Властивості.

257 Якщо користуєтеся «Інспектором документів», спочатку зробіть копію документа, бо внесені зміни вже неможливо скасувати. У копії документа натисніть на кнопку Microsoft Office>Підготувати>Інспектор документів. У діалоговому вікні поставте прапорці для вмісту, який потрібно перевірити. Натисніть «Перевірити». Прогляньте результати перевірки в діалоговому вікні «Інспектора документів». Натисніть «Видалити все» поруч із результатами перевірки для кожного типу прихованого вмісту, який потрібно видалити з документа.

258 http://www.infosecurity-magazine.com/news/printer-related-security-breaches-affect-63-of/.

259 http://www.wired.com/2014/08/gyroscope-listening-hack/.

260 Термін поєднав англійське слово «fun» — веселощі і «antenna» — антена. — *Прим. пер.*

261 http://ossmann.blogspot.com/2013/01/funtenna.html.

262 http://cs229.stanford.edu/proj2013/Chavez-ReconstructingNonIntrusivelyCollectedKeystrokeDataUsingCellphoneSensors.pdf.

263 https://www.cise.ufl.edu/~traynor/papers/marq-ccs11.pdf.

264 http://samy.pl/keysweeper/.

265 http://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/.

266 http://phys.org/news/2013-07-femtocell-hackers-isec-smartphone-content.html.

267 http://arstechnica.com/information-technology/2015/04/this-machine-catches-stingrays-pwnie-express-demos-cellular-threat-detector/.

268 http://www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

269 http://www.computerworld.com/article/2474090/data-privacy/new-snowden-revelation-shows-skype-may-be-privacy-s-biggest-enemy.html.

270 https://community.rapid7.com/community/metasploit/blog/2012/01/23/video-conferencing-and-self-selecting-targets.

271 http://www.polycom.com/global/documents/solutions/industry_solutions/government/max_security/uc-deployment-for-maximum-security.pdf.

272 https://community.rapid7.com/community/metasploit/blog/2012/01/23/video-conferencing-and-self-selecting-targets.

273 Наприклад, https://www.boxcryptor.com/en.

Розділ 14

Боротьба за анонімність

Кілька років тому я повертався до США з колумбійської Боготи, і після прибуття в Атланту два американських прикордонники тихенько відвели мене в окрему кімнату. Позаяк мене вже заарештовували і навіть саджали у в'язницю, я нервувався менше за середньостатистичного громадянина. І все ж було якось лячно. Я нічого не зробив, а мене протримали в цій кімнаті чотири години — майже половину часу, протягом якого можна затримати людину без арешту.

Проблеми почалися, коли прикордонник відкрив мій паспорт і перевів погляд на екран. «Кевіне, — сказав правоохоронець із широкою усмішкою на обличчі. — Така справа: там унизу чекають люди, які хочуть з вами поговорити. Але не турбуйтеся. Усе буде добре».

У Боготу мене запросила виступити з промовою газета El Tiempo. А ще я навідався до дівчини, з якою на той момент зустрічався. Поки я чекав у кімнаті «там унизу», зателефонував своїй дівчині в Боготу. Вона сказала, що їй подзвонила поліція Колумбії і попросила дозволу провести обшук посилки, яку я відправив у США через FedEx. «Вони знайшли сліди кокаїну», — додала вона. Я знав, що це брехня.

У посилці був 2,5-дюймовий внутрішній жорсткий диск. Найімовірніше, колумбійська (чи, може, американська) влада хотіла перевірити вміст диска, який був зашифрований. Кокаїн був просто безглуздим приводом відкрити коробку. Жорсткий диск мені так і не повернули.

Пізніше я дізнався, що поліція таки відкрила коробку, розібрала електронне обладнання й випадково знищила жорсткий диск, коли намагалася відкрити і перевірити його на кокаїн, просвердливши дірку. Вони могли б скористатися спеціальною викруткою. Звісно, жодних наркотиків вони не знайшли.

Тим часом прикордонники в Атланті відкрили мою валізу і знайшли MacBook Pro, ноутбук Dell XPS M1210, ноутбук ASUS 900, три чи чотири жорстких диски, безліч флешок, кілька блютуз-адаптерів і чотири телефони Nokia (кожен із власною SIM-картою, щоб можна було не оплачувати роумінг за кордоном). Усе це — стандартні інструменти в моїй професії.

А ще у валізі знайшли мій набір відмичок і клонуючий пристрій, який може зчитати й відтворити будь-яку безконтактну ключ-картку. Останній допомагає витягнути облікові дані з картки доступу, якщо помістити девайс поряд із нею. Так я можу, приміром, підробити дані з ключ-картки потрібної людини й відчинити замкнені двері без необхідності підроблювати саму картку. І все це я потягнув у Боготу, бо виступав з ключовою промовою про інформаційну безпеку. Не дивно, що очі прикордонників просто загорілися, коли вони оце все побачили. Напевне, подумали, що я задумав красти кредитки (у чому ці пристрої аж ніяк не допоможуть).

Урешті-решт прибули працівники Імміграційної та митної поліції США (ІМП) і запитали, чому я приїхав в Атланту. Я відповів, що мене запросили як модератора на конференцію з інформаційної безпеки, а Американське товариство промислової безпеки було при цьому спонсором. (Пізніше агент ФБР сам приїхав на конференцію й особисто переконався в причині моєї поїздки).

Усе стало гірше, коли я відкрив ноутбук і увійшов у пошту, щоб показати їм імейл-запрошення на конференцію.

У браузері стояло автоматичне очищення історії при запуску. Тому, коли я відкрив браузер, той одразу запропонував очистити історію. Я натиснув «ОК» — і агенти занервували. А потім я просто вимкнув MacBook кнопкою живлення, тож тепер доступ можна було дістати лише з моїм PGP-паролем.

Я не був під арештом (а мене неодноразово запевняли, що так і є), тож мав повне право не розголошувати парольну фразу. Та навіть якщо і був би: відповідно до законодавства США, я можу не розголошувати свій пароль, але реалізація цього права безпосередньо залежить від того, чи протримаєтеся ви на допиті[274]. Однак у різних країнах — різні закони. Приміром, у Великобританії та Канаді влада може змусити вас розкрити пароль.

За чотири години і ІМП, і прикордонники мене відпустили. Однак якби на мене націлилося агентство рівня АНБ, то їм би, напевно, вдалося дізнатися вміст мого жорсткого диска. Урядові служби можуть зламати прошивку вашого ПК чи телефона, вклинитися у вашу інтернет-мережу і скористатися дірками в безпеці ваших пристроїв. Я був у країнах і з жорсткішими правилами, але ніколи не мав таких проблем через судимість, як у США. Тож як виїхати за кордон із конфіденційними даними? Особливо у «ворожі» країни на зразок Китаю?

Якщо не хочете, щоб із вашого жорсткого диска витягли конфіденційні дані, у вас є кілька варіантів:

1. *Очистіть усі конфіденційні дані перед поїздкою і зробіть повне резервне копіювання.*

2. *Не видаляйте даних, але зашифруйте їх надійним ключем (хоча деякі країни можуть змусити вас назвати ключ чи пароль). Не зберігайте парольну фразу в себе: можна, наприклад, залишити її половину другу за межами США, у якого уряд не має права її питати.*

3. *Помістіть зашифровані дані в «хмару» і завантажуйте їх звідти за потреби.*

4. *Скористайтеся безкоштовною програмою (як-от VeraCrypt) і створіть приховану зашифровану папку з файлами на жорсткому диску. Але знову ж таки: якщо іноземний уряд знайде цю папку, то може змусити вас розкрити пароль.*

5. *Щоразу, коли вводите пароль на своїх пристроях, прикривайте себе й екран курткою чи іншим предметом одягу, щоб сховати інформацію від камер спостереження.*

6. *Запечатайте свій ноутбук та інші пристрої в упаковку від FedEx (чи будь-яку іншу), підпишіть її і покладіть у сейф в номері готелю. Якщо упаковку розкриють і підмінять, ви це помітите. Попереджаю: сейфи в готелі не такі вже й надійні. Раджу придбати спеціальну камеру, яка робитиме фото всіх, хто зазирне в сейф, і негайно відправлятиме вам на телефон.*

7. *І найголовніше: не ризикуйте. Завжди тягайте девайси з собою і не зводьте з них очей.*

Згідно з документами, отриманими Американською спілкою захисту громадянських свобод завдяки закону «Про свободу інформації», у період з жовтня 2008 року до червня 2010 року понад 6500 осіб стали жертвами перевірок електронних пристроїв на кордоні США. А це в середньому більше ніж триста прикордонних обшуків на місяць. І майже половина мандрівників — громадяни США.

Маловідомий факт: будь-який електронний девайс можна обшукати без ордера чи законної підозри в радіусі 160 кілометрів від кордону США, куди потрапляє і Сан-Дієго. Тож якщо ви перетнули кордон, це ще не означає, що ви в безпеці!

За огляд пасажирів і предметів, що ввозяться на територію США, відповідають дві державні установи: Митно-прикордонна служба США (МПС) у складі Міністерства національної безпеки й Імміграційна та митна поліція США (ІМП). У 2008 році Міністерство національної безпеки оголосило, що має право здійснювати обшук будь-якого електронного пристрою, що ввозиться на територію Сполучених Штатів[275]. А ще представило власну Автоматизовну систему стеження (ATS), яка миттєво заводить на вас особисте досьє (і дуже докладне), щойно ви виїжджаєте за кордон. На основі цього досьє працівники МПС вирішують, чи проводити детальний (або навіть поглиблений) обшук ваших пристроїв після повернення до США.

Уряд США може вилучити електронний пристрій, проглянути всі файли й залишити в себе девайс для подальшого вивчення — цілком законно. Працівники МПС можуть обшукати ваш пристрій, скопіювати його вміст і навіть спробувати відновити видалені зображення й відео.

Ось що в цьому випадку роблю я.

Щоб захистити приватність мою і моїх клієнтів, я шифрую конфіденційні дані на своїх ноутбуках. Коли я перебуваю за кордоном, то завантажую зашифровані файли по інтернету на захищені сервери в будь-якій точці світу. А коли планую

повертатися додому, стираю їх із комп'ютера — на випадок, якщо урядовці вирішать обшукати чи вилучити моє обладнання.

Стирання даних — не синонім видалення. Після видалення зникає лише інформація про файл у головному завантажувальному записі (індекс для пошуку частин файлу на жорсткому диску). Сам файл (або його частини) залишається на жорсткому диску доти, доки на цьому секторі не запишуться нові дані. Так експерти цифрової криміналістики можуть відновити видалені файли.

А от стирання надійно замінює видалений файл довільними даними. На твердотілих накопичувачах стирання провести складно, тому я беру з собою ноутбук зі стандартним жорстким диском і щоразу стираю його не менш як у тридцять п'ять проходів. Під час кожного проходу ПЗ сотні разів перезаписує поверх видаленої інформації випадкові дані, що ускладнює її відновлення.

Раніше я зберігав повну резервну копію пристрою на зовнішній жорсткий диск, шифрував його і відсилав другу до США. Дані на пристрої я не стирав, поки друг не підтвердить, що отримав диск цілим і неушкодженим. Опісля я надійно стирав усі особисті та клієнтські файли. Сам жорсткий диск я не форматував і операційну систему теж не чіпав. Так можна було легше відновити файли і не перейматися перевстановленням усієї системи, якщо мене раптом обшукають на кордоні.

Але після Атланти я трохи змінив процедуру. Тепер я зберігаю «клони» всіх моїх ноутбуків для подорожей у колеги. Якщо мені знадобиться один із ноутбуків у США, я просто попрохаю колегу надіслати мені клоновану систему.

А от айфон — це вже інша справа. Якщо ви колись підзаряджали айфон від ноутбука і натискали кнопку «Довіряти цьому комп'ютеру», на ноутбуці зберігається сертифікат сумісності, який надає доступ до всього вмісту айфона без введення кодового пароля. Сертифікат активуватиметься під час кожного під'єднання цього айфона до комп'ютера.

Наприклад, якщо ви під'єднаєте свій айфон до чужого комп'ютера і натиснете «довіряти», то між комп'ютером і пристроєм на iOS встановиться довірчий зв'язок. Чужий пристрій дістане доступ до всіх фотографій, відео, SMS, журналів викликів, повідомлень у WhatsApp та інших даних у телефоні без пароля. Ба навіть більше: власник комп'ютера може навіть зробити резервну копію вашого телефона через iTunes, якщо ви досі не встановили пароль на створення шифрованих резервних копій (раджу це зробити). Якщо пароль не стоїть, зловмисник може самостійно його встановити і створити резервну копію вашого айфона в себе на комп'ютері без вашого відома.

Тобто якщо правоохоронні органи захочуть зазирнути у ваш запаролений айфон, вони просто під'єднають його до вашого ноутбука, позаяк на ньому, найімовірніше, є сертифікат для цього телефона. Закарбуйте собі: ніколи не «довіряйте цьому комп'ютеру», якщо «цей комп'ютер» — не ваш.

А що робити, якщо треба скасувати всі сертифікати сумісності на вашому девайсі від Apple? Радійте: сертифікат сполучення на пристроях Apple можна

скинути[276]. Але якщо у вас айфон і треба поділитися файлами, краще скористайтеся AirDrop. Якщо потрібно зарядити телефон, під'єднайте його через кабель до власного ПК чи розетки. Не користуйтеся чужим комп'ютером. Або можна придбати «USB-презерватив» від syncstop.com, тоді можна безпечно під'єднувати телефон до будь-якого комп'ютера.

А що як у поїздку ви взяли лише айфон, без ноутбука?

Я увімкнув на айфоні Touch ID, щоби той розпізнавав лише мій відбиток пальця. І коли я наближаюся до імміграційного контролю в будь-якій країні, то просто перезавантажую телефон. Коли він знову вмикається, я свідомо не вводжу кодовий пароль. Хоча й Touch ID працює, він буде вимкнений за замовчуванням, доки я не введу код. Суд США чітко постановив, що правоохоронні органи не можуть змусити вас ввести пароль. У США ви можете не давати жодних свідчень, але, приміром, фізичний ключ від сейфа дати повинні. За тією самою логікою, суд може змусити вас дати відбитки пальців для розблокування пристрою[277]. Вихід елементарний: перезавантажте телефон. Так ваш Touch ID буде вимкнений, а пароль ви давати не повинні.

А от у Канаді все по-іншому. Якщо ви громадянин Канади, то, за законом, повинні надати свій кодовий пароль. Це трапилося з Аленом Філліпоном із Сент-Анн-де-Монтс, провінція Квебек. Він повертався додому з Домініканської Республіки і відмовився надати прикордонникам у Новій Шотландії кодовий пароль до свого телефона. Його звинуватили за статтею 153.1(b) канадського закону «Про митницю» в перешкоджанні роботі прикордонної служби. Покарання в такому випадку — тисяча доларів штрафу, з максимальним штрафом у 25 тисяч доларів і можливістю отримати рік у в'язниці[278]. Я й сам не з чуток знаю про канадський закон. Якось у 2015-му я замовив таксі з Чикаго до Торонто (не хотілося летіти в сильну грозу), і коли ми перетнули канадський кордон у Мічигані, нас одразу відправили на вторинний огляд. Може, усе через хлопця з Близького Сходу за кермом, який мав лиш ґрінкарту. Ми відразу рушили в пункт вторинної перевірки... а приїхали просто в серіал «CSI: місце злочину».

Ціла купа прикордонників змусила нас вийти з автомобіля, залишивши всередині всі наші речі, зокрема й мобільні телефони. Нас із водієм розділили. Одна прикордонниця підійшла до машини з боку водія й витягнула його телефон з тримача, після чого вибила з хлопця пароль і почала копатися в мобільному.

Я вже давно пообіцяв собі ніколи не видавати свого пароля. Здавалося, зараз от-от доведеться або відступитися від принципів, або пожертвувати виступом у Канаді... Але тут на допомогу прийшла соціальна інженерія.

Я закричав прикордонниці, яка рилася в телефоні водія. «Гей! Ви ж не будете обшукувати мою валізу? Бо вона замкнена, ви її не відкриєте!». Це відразу привернуло її увагу. Вона відповіла, що має повне право обшукати мою валізу.

Але я наполягав: «Я її замкнув, тому ви її не обшукаєте».

Пам'ятаю, як два прикордонники підійшли до мене й почали вибивати ключ. Я запитав, навіщо їм обшукувати мої речі, а вони знову пояснили, що мають повне право. Тож я витягнув гаманець і передав прикордонникові ключ від валізи.

І все. Вони геть забули про мобільні телефони й зосередилися на моїй валізі. Місію виконано. Хоч і обманним шляхом. На щастя, мене відпустили, так і не запитавши пароля від мобільного.

У метушні обшуку легко відволіктися. Не дозволяйте собі стати жертвою обставин. Коли проходите контрольно-пропускний пункт, переконайтеся, що ваш ноутбук і електронні пристрої лежать на конвеєрній стрічці останніми. Навряд чи вам захочеться, щоб ноутбук чекав вас на іншому кінці, поки хтось попереду затримує чергу. Крім того, якщо вам треба вийти з черги, завжди беріть ноутбук й інші девайси з собою.

Не очікуйте на кордоні США такого самого захисту конфіденційності, як у себе вдома. Якщо ви лікар, юрист або якось пов'язані з бізнесом, поглиблений прикордонний обшук може поставити під загрозу конфіденційність фахової інформації. Сюди належать комерційна таємниця, спілкування між адвокатом і клієнтом або лікарем та пацієнтом, а також дослідницькі й бізнесові стратегії, щодо захисту конфіденційності яких мандрівник має юридичні і контрактні зобов'язання.

Решта з нас теж ризикує: обшук жорсткого диска й мобільних пристроїв може розкрити нашу електронну пошту, медичну і навіть фінансову інформацію. Якщо ви нещодавно відвідали «ворожі» для інтересів США країни, то майте на увазі, що вам світить додаткова перевірка від прикордонників.

Країни з репресивною владою — ще небезпечніші. Вони можуть наполягати на ретельнішому обшуку ваших електронних пристроїв, тобто перегляді електронної пошти й перевірці папки із завантаженими файлами. А ще існує вірогідність, що вони встановлять шпигунську програму на ваш девайс, особливо якщо забирають його для огляду.

Деякі компанії видають своїм співробітниками одноразові телефони й ноутбуки для поїздки за кордон. Після того як співробітник повертається назад у Сполучені Штати, пристрій або викидають, або чистять. Але для більшості з нас шифрування файлів перед завантаженням у «хмару» чи купівля нового пристрою для подальшої утилізації — не варіант.

Отже, не беріть з собою пристрої з конфіденційними даними без гострої потреби. Якщо ж потреба є, намагайтеся залишити щонайменше інформації. Замість звичайного телефона раджу придбати одноразовий, лише на час поїздки. Тим паче, тарифи на дзвінки та інтернет у роумінгу просто обурливі. Краще взяти з собою «розлочений» одноразовий телефон і придбати місцеву SIM-карту в країні призначення.

Якщо вам здається, що проходження кордону — найжахливіша частина поїздки, не поспішайте з висновками. Обшукати можуть і ваш номер у готелі.

Той випадок з Атлантою — не єдина моя поїздка до Колумбії 2008-го. Потім я ще кілька разів літав у Боготу... і в одній із таких поїздок у моєму готельному номері трапилося щось дивне. І це був не якийсь там сумнівний готель — ні, тут часто зупинялися колумбійські чиновники.

Але, можливо, у цьому і була проблема.

Ми з дівчиною вирішили повечеряти в ресторані, а коли повернулися і вставили у дверний замок ключ-картку, блимнув жовтий індикатор. Не зелений. Не червоний. Жовтий. Який сигналізує про те, що двері замкнені зсередини.

Я спустився до стійки реєстрації і попрохав нову ключ-картку. І знову жовтий індикатор. Я спустився за ключем ще раз: той самий результат. Після третього разу я вмовив адміністрацію готелю піднятися зі мною. Двері відчинилися.

На перший погляд, у номері все мало цілком нормальний вигляд. Тоді я списав інцидент на несправність замка. І лише повернувшись до Сполучених Штатів, я зрозумів, що насправді сталося.

Перед від'їздом до Боготи я зателефонував колишній дівчині Дарсі Вуд, яка раніше була провідним техніком у TechTV, попросивши її приїхати й замінити жорсткий диск на ноутбуці MacBook Pro. Тоді дістати жорсткий диск із MacBook було не так уже й легко. Однак Дарсі це вміла. Замість нього вона поставила новенький диск, який я відформатував і встановив на нього операційну систему OS X.

За кілька тижнів, коли я повернувся з Колумбії, я знов попросив Дарсі приїхати в Лас-Вегас і поміняти диски назад.

Дарсі відразу помітила, що щось не так. Хтось закрутив гвинти жорсткого диска набагато сильніше, ніж вона.

Імовірно, поки мене не було в номері готелю, хтось дістав із ноутбука диск і зробив копію.

Таке ж нещодавно трапилося і зі Стефаном Ессером — дослідником, який прославився джейлбрейком iOS-продуктів. У твіттер він виклав фотографію свого жахливо зібраного жорсткого диска.

Навіть диск із мінімальним обсягом даних містить якусь інформацію. На щастя, я скористався функцією PGP Whole Disk Encryption від Symantec, яка шифрує весь вміст жорсткого диска. (Також можете спробувати WinMagic для Windows або FileVault 2 для OS X; докладніше про це трохи далі). Тож клон мого диска — річ абсолютна даремна, якщо в злодія нема ключа для розблокування. Тепер, через той випадок у Боготі, у подорожах я завжди тягаю ноутбук із собою, навіть коли вечеряю в ресторані. Якщо ж узяти з собою ноутбук я не можу, то ніколи не залишаю його в режимі гібернації. Я повністю його вимикаю. Інакше зловмисник може зробити дамп пам'яті й отримати ключі PGP-шифрування для всього диска[279]. Тож доводиться вимикати ноутбук.

* * *

На початку книжки я розповідав про обачність, з якою Едвард Сноуден намагався зберегти таємницю свого листування з Лорою Пойтрас. Однак щойно

секретні дані Сноудена були готові до оприлюднення, їм із Пойтрас треба було їх десь зберегти. Усі популярні операційні системи — Windows, iOS, Android і навіть Linux — мають діри в безпеці. Як і будь-яке ПЗ. Тож їм була потрібна надійна операційна система, яка зашифрована від самого початку і розблоковується лише ключем.

Шифрування жорсткого диска працює так: щоразу, як ви вмикаєте комп'ютер, вводите надійний пароль чи навіть парольну фразу, як-от: «We don't need no education» (з відомої пісні гурту Pink Floyd). Після цього операційна система завантажується, а ви дістаєте доступ до своїх файлів і можете спокійно працювати. Затримок у роботі ви не помітите: драйвер шифрує файли прозоро й миттєво. Однак якщо ви підете і залишите свій пристрій без нагляду — хай навіть на мить — хтось може дістати доступ до ваших файлів (позаяк вони розблоковані). Завжди пам'ятайте: коли ваш зашифрований жорсткий диск розблоковано, ви повинні з обачністю ставитися до його безпеки. Щойно ви вимикаєте комп'ютер, ключ шифрування щезає з операційної системи: пристрій просто видаляє ключ із пам'яті, тож дані на диску стають недоступними[280].

Tails — це операційна система, яку можна запустити на будь-якому сучасному комп'ютері і яка не залишає на жорсткому диску (в ідеалі, із захистом від запису) жодних слідів, за якими можна відновити дані[281]. Завантажте Tails на DVD або USB-флешку і налаштуйте послідовність початкового завантаження в BIOS чи EFI (для OS X) на диск або флешку з Tails. Тепер при вмиканні комп'ютер запустить нову операційну систему, яка має кілька інструментів для захисту конфіденційності, зокрема Tor-браузер. Завдяки таким інструментам можна шифрувати імейли за допомогою PGP, шифрувати USB і жорсткі диски, а також захищати повідомлення через протокол OTR.

Якщо хочете зашифрувати не весь диск, а лиш окремі файли, у вас є кілька варіантів. Приміром, безкоштовна програма TrueCrypt, яка все ще існує, але вже не підтримується і не має функції повного шифрування диска. Позаяк розробник програмою більше не займається, вона вразлива до нових методів дешифрування. Тож якщо досі користуєтеся TrueCrypt, пам'ятайте про ризик. Зараз заміною TrueCrypt 7.1a є VeraCrypt — продовження першого проекту.

Є й кілька платних програм. Найочевидніша — Windows BitLocker, яка зазвичай не входить до домашньої Windows. Установивши BitLocker, відкрийте «Провідник», клікніть правою кнопкою миші на «Диск C» і прокрутіть до рядка «Включити BitLocker». У роботі BitLocker спирається на особливий чип TPM на материнській платі. Він відповідає за розблокування ключа шифрування лише після перевірки програми завантажувача на цілісність. Це — ідеальний захист від так званої атаки «злої покоївки» («evil maid»), про яку ми поговоримо трохи пізніше. BitLocker можна налаштувати на розблокування системи або при звичайному вмиканні комп'ютера, або лише за наявності PIN-коду чи спеціальної флешки. Останній варіант набагато безпечніший. А ще вам можуть

запропонувати зберегти ключі в акаунті Microsoft. Не робіть цього. Так ви, по суті, віддасте Microsoft свої ключі (які в них, можливо, і так уже є).

Але BitLocker має кілька недоліків. По-перше, він використовує генератор псевдовипадкових чисел (PRNG) під назвою Dual_EC_DRBG (скорочення від «генератор детермінованих випадкових чисел на основі подвійної еліптичної кривої»), який може містити бекдори від АНБ[282]. А ще програму розробила приватна компанія, а отже, вам доведеться повірити Microsoft на слово, що ПЗ працює і жодних бекдорів від АНБ не має. Із програмним забезпеченням з відкритим вихідним кодом таких проблем не виникає. І ще один недолік BitLocker: якщо не придбати програму за 250 доларів, доведеться повідомити ключ Microsoft. Тобто якщо ви не заплатите, правоохоронні органи зможуть вилучити ваш ключ у компанії.

І все ж, попри всі застереження, правозахисники з EFF рекомендують BitLocker для середньостатистичного споживача, який хоче захистити свої файли[283]. Однак майте на увазі, що BitLocker можна обійти[284]. Ще один платний варіант — повне шифрування PGP Whole Disk Encryption (WDE) від Symantec. Ним користується купа університетів і корпорацій. Я теж раніше ним користувався. Технологію WDE розробив Філ Циммерманн — людина, яка створила PGP для електронної пошти. Як і BitLocker, PGP підтримує TPM-чип і забезпечує додаткову автентифікацію при ввімкненні комп'ютера. Безстрокова ліцензія коштує приблизно 200 доларів.

А ще є WinMagic — один із небагатьох варіантів, який вимагає не лише пароль, а й двофакторну автентифікацію. Програма не спирається на єдиний майстер-пароль. Натомість зашифровані файли групуються, а вже кожній групі призначається окремий пароль. Так процес відновлення пароля значно ускладнюється, тож варіант не для всіх.

А для Apple існує FileVault 2. Щоб ввімкнути FileVault 2, відкрийте «Системні налаштування», клікніть позначку «Безпека і конфіденційність» і переключіться на вкладку FileVault. Знову ж таки, не зберігайте ключ шифрування в акаунті Apple. Так ви віддасте ключ компанії, яка, своєю чергою, може віддати його правоохоронним органам. Натомість виберіть «Створити ключ відновлення і не використовувати акаунт iCloud», а потім роздрукуйте або запишіть собі десь цей ключ із двадцяти чотирьох символів. Пильнуйте ключ, бо кожен, хто його знайде, зможе розблокувати ваш жорсткий диск.

Якщо у вас на айфоні чи айпаді стоїть iOS 8 або більш пізня версія, вміст пристрою автоматично шифрується. Крім того, Apple пішов ще далі і заявив, що ключ існує лише на девайсі користувача. А отже, уряд США не може вилучити ключ у Apple: він є унікальним для кожного пристрою. Директор ФБР Джеймс Комі стверджує, що незламне шифрування — не надто гарна ідея. У своїй промові він сказав: «Досвідчені злочинці скористаються цими методами, щоб ховатися від закону. Тож ось моє питання: навіщо все це?»[285] Дехто боїться, що шифрування захищатиме поганих людей.

Через цей страх у 1990-х моя справа відкладалася раз за разом, кілька місяців поспіль, поки я нудився у в'язниці. Мої адвокати намагалися дістати доступ до інформації, яку уряд планував використати проти мене в суді. Уряд відмовився передавати зашифровані файли, поки я не віддам ключ для розшифровки. Я відмовився передавати ключ[286]. А суд відмовився зобов'язувати уряд надати інформацію, бо я відмовився передавати ключ[287].

Пристрої на Android, починаючи з версії 3.0 (Honeycomb), теж можуть шифруватися. Але більшість із нас цим не переймається. Починаючи з Android 5.0 (Lollipop), жорсткі диски шифруються за замовчуванням у серії телефонів Nexus, але на телефонах інших виробників, як-от LG чи Samsung, функція є факультативною, Якщо ви захочете зашифрувати свій телефон на Android, готуйтеся до того, що це займе приблизно годину, а пристрій має бути під'єднаним до живлення від початку і до кінця. Кажуть, шифрування телефона не надто знижує продуктивність, але якщо ви вже зашифрували пристрій, скасувати це неможливо.

У будь-якій програмі повного шифрування диска завжди є шанс бекдору. Якось одна компанія найняла мене протестувати USB-продукт, що дає змогу користувачам зберігати файли в зашифрованому контейнері. В ході аналізу коду ми виявили, що розробник заклав у пристрій секретний бекдор: ключ для розблокування зашифрованого контейнера був захований на USB-накопичувачі у випадковому місці. А отже, кожен, хто знає розташування ключа, може розблокувати дані, зашифровані користувачем.

Ще більше засмучує те, що часто компанії навіть не знають, що робити з цією інформацією. Коли я закінчив тестування зашифрованого USB-пристрою, генеральний директор зателефонував мені і запитав, чи варто йому залишити бекдор. Його турбувало те, що правоохоронним органам чи АНБ може знадобитися доступ до даних користувача. Один той факт, що він поставив мені це питання, уже достатньо промовистий.

У звіті про прослуховування 2014 року уряд США повідомив, що зіткнувся із зашифрованими дисками лише на 25 з 3554 пристроїв, обшук яких проводили правоохоронні органи[288]. І вони все одно змогли розшифрувати 21 з 25 дисків. Так, шифрування вбереже ваші дані від пересічного злодія, а от від оснащеного до зубів уряду — навряд чи.

Якось давно дослідниця Йоанна Рутковська писала про явище, яке охрестила атакою «злої покоївки»[289]. Скажімо, хтось залишає в номері готелю вимкнений ноутбук із зашифрованим жорстким диском на TrueCrypt або PGP Whole Disk Encryption. (У Боготі я користувався другим варіантом і також вимикав ноутбук). Коли вас немає, хтось прокрадається в номер і вставляє USB-накопичувач зі шкідливим завантажувачем. Потім треба завантажити ноутбук з USB, щоб шкідливий завантажувач проникнув у систему і в перспективі вкрав парольну фразу користувача. Усе. Пастка готова.

Найкращим кандидатом для цього є покоївка чи людина, яка може часто навідуватися в номер готелю без особливих підозр, — звідси і назва атаки. Покоївка може легко потрапити в будь-який номер наступного дня і ввести секретну комбінацію, яка витягне парольну фразу, таємно збережену на диску. Тепер зловмисник може спокійно ввести пароль і дістати доступ до всіх ваших файлів.

Я не знаю, чи провернув хтось таке з моїм ноутбуком у Боготі. Сам жорсткий диск витягли, а потім повернули назад із занадто щільно закрученими гвинтами. На щастя, диск не містив жодної важливої інформації.

А як щодо готельного сейфа? Краще ж туди покласти ноутбук, ніж залишити його на виду чи у валізі? Так, але різниця мізерна. Під час нещодавньої конференції Black Hat я зупинився в готелі Four Seasons у Лас-Вегасі. У сейф я поклав 4 тисячі доларів готівкою, кілька кредиток і чеки. За кілька днів мені знадобилося відкрити сейф, але код не підходив. Я викликав охорону, і вона його відкрила. Я відразу помітив, що моя пачка стодоларових купюр дещо потоншала. Там було лише 2 тисячі доларів. Куди ж поділися ще дві? Охорона готелю й гадки не мала. Мій друг, що спеціалізується на фізичному тестуванні на проникнення, спробував зламати сейф, але не зміг. Сьогодні це все ще загадка. За іронією долі, сейф називався «Безпечне місце» (Safe Place).

Німецька антивірусна компанія G DATA виявила, що в готельних номерах, де зупинявся їхній персонал, найчастіше на сейфі стояв пароль за замовчуванням (0000). Тобто байдуже, який пароль виберете ви: кожен, хто знає пароль за замовчуванням, дістане доступ до ваших речей. Однак G DATA додає, що ця інформація перевірялася не систематично, а епізодично, протягом кількох років[290].

Якщо зловмисник не знає пароля за замовчуванням до сейфа в готелі, він може спробувати зламати його грубою силою. Хоча в менеджера готелю є аварійний електронний пристрій, що під'єднується до USB-порту і відкриває сейф, кмітливий злодій може просто відкрутити пластину на передній панелі сейфа й відкрити замок за допомогою цифрового пристрою. Або закоротити дроти і скинути пароль, а потім ввести новий код.

Якщо це вас не бентежить, то як вам таке? G DATA теж виявила, що зчитувачі кредиток на сейфах (через які ви сплачуєте користування сейфом) передають дані третій стороні, яка може витягнути дані вашої картки і скористатися ними чи продати в інтернеті.

Зараз у готелях замки в номерах закриваються за технологією NFC або ключ-картками на магнітних смугах. Великий плюс у тому, що готель може за мить змінити код доступу ключа на стійці реєстрації. Якщо ви раптом загубите картку, можете попрохати нову. Менеджер надсилає простий код на ваш замок, і коли ви дістанетеся до свого номера, нова ключ-картка вже працюватиме. Але інструмент MagSpoof від Семі Камкара може підробити правильну послідовність

і відкрити замок готельного номера, який працює на картці з магнітною смугою. Цей пристрій показали в одній із серій телесеріалу «Містер Робот».

Побутує думка, що на ключ-картці можуть зберігатися особисті дані, позаяк вона працює на магнітній смузі або чипі NFC. Це міф. Але міська легенда живе і процвітає. В окрузі Сан-Дієго навіть зародилася відома історія про заступника шерифа, який запевнив, що ім'я гостя, його домашню адресу та інформацію про кредитку можна знайти на ключ-картці готелю. Можливо, ви бачили цей імейл. Має він приблизно такий вигляд:

Співробітники правоохоронних органів Південної Каліфорнії, до функцій яких входить виявлення нових загроз особистій безпеці, нещодавно встановили, який тип інформації міститься в повсюдно поширених ключ-картках готельних номерів.

Хоча й картки від номерів різняться в кожному готелі, ключ, отриманий у мережі готелів DoubleTree, став темою регіональної презентації крадіжки особистих даних і містить таку інформацію:

- *ім'я гостя;*
- *часткову домашню адресу гостя;*
- *номер кімнати в готелі;*
- *дату заїзду і виїзду;*
- *номер і термін дії кредитної картки гостя!*

Коли ви повідомляєте ці дані на стійці реєстрації, будь-який співробітник може дістати до них доступ, просто просканувавши картку в готельному сканері. Співробітник може взяти кілька карток додому і, за допомогою спеціального сканера, дістати доступ до інформації на ноутбуці, вирушивши за покупками з вашою кредиткою.

Готель не стирає даних з картки, поки не видасть її наступному гостю. Зазвичай вона зберігається в шухляді на стійці реєстрації. Із вашою інформацією!!!

Краще забирайте картки із собою або знищуйте! Ніколи не залишайте їх у готелі й ніколи не здавайте на стійку реєстрації, коли виїжджаєте з номера. Штраф вам за це не випишуть[291].

Правдивість цього листа ну дуже сумнівна[292]. Чесно кажучи, для мене це — справжня маячня.

Теоретично, перераховану інформацію можна завантажити на ключ-картку, але це вже щось зі сфери фантастики, навіть для мене. Кожному гостю готеля призначають унікальний номер-заповнювач — щось на зразок токена. І

пов'язати його з реальними даними можна лише за наявності доступу до внутрішніх комп'ютерів, де проводять фінансові розрахунки.

Не думаю, що треба збирати і знищувати всі старі ключ-картки... але заборонити вам, звісно ж, не можу.

Ще одне популярне питання, що стосується подорожей і особистих даних: що зашифровано в штрих-коді на вашому авіаквитку? Що він може про вас розповісти? Правду кажучи, не надто багато. Якщо у вас нема номера постійного пасажира.

З 2005 року Міжнародна асоціація повітряного транспорту ухвалила рішення про посадкові талони зі штрих-кодом з однієї простої причини: магнітні обходилися набагато дорожче. За підрахунками, економія становила 1,5 мільярда доларів. Крім того, пасажири відтепер можуть самостійно завантажити авіаквитки зі штрих-кодом і роздрукувати їх вдома або ж просто показати з телефона під час посадки.

Думаю, ви розумієте, що нова процедура мала спиратися на певний стандарт. За словами дослідника Шона Юінга, зазвичай типовий штрих-код на посадковому талоні містить безневинну інформацію: ім'я пасажира, назву авіакомпанії, номер місця, аеропорт вильоту, аеропорт прибуття та номер рейсу[293]. А от із номером постійного пасажира все набагато серйозніше[294]. Усі авіакомпанії тепер захищають акаунти своїх клієнтів на сайті персональними паролями. Витік номера постійного пасажира — це не так страшно, як витік номера соціального страхування, але теж шкодить конфіденційності.

Інша справа — це картки лояльності, що продаються в супермаркетах, аптеках, на заправках тощо. На відміну від авіаквитків, які повинні бути зареєстровані на ваше реальне ім'я, картки лояльності можна оформити під фальшивим ім'ям, адресою та номером телефону (який вам варто запам'ятати), тож покупку неможливо буде пов'язати з вашою особою.

Заселившись у готель, ви неодмінно вмикаєте комп'ютер і бачите список доступних Wi-Fi мереж: «гість готелю» «tmobile123,» «айфон Кімберлі», «attwifi», «Android Стіва», «хот-спот Чака» чи щось таке. До якої варто під'єднатися? Сподіваюся, ви вже здогадалися.

Більшість готелів має незашифрований Wi-Fi, і все ж вимагає прізвище гостя й номер кімнати для автентифікації. Однак є спосіб обійти це й дістати анонімний, безкоштовний доступ.

Приміром, можна зателефонувати з власного номера на будь-який інший (можливо, той, що на іншому кінці коридору), прикинувшись обслуговуванням номерів. Якщо готель фіксує ідентифікатор абонента, скористайтеся стаціонарним телефоном. По телефону скажіть, що два бургери скоро будуть у номері. Коли гість каже, що нічого не замовляв, ввічливо попрохайте назвати прізвище, щоб виправити помилку. Тепер у вас є номер кімнати (у яку ви телефонували) і прізвище. А більше і не потрібно, щоб пройти автентифікацію повноцінного гостя готелю, хоча ви й не платили за інтернет.

Припустимо, ви зупинилися в п'ятизірковому готелі з безкоштовним або платним інтернетом. Після під'єднання до мережі вам може вискочити оповіщення про доступне оновлення Adobe (або якогось іншого виробника програмного забезпечення). Якщо ви звикли до порядку в комп'ютері, то неодмінно виникне спокуса встановити оновлення й забути про це. Але мережу в готелі варто за замовчуванням вважати небезпечною. Навіть якщо на ній стоїть пароль. Це не ваш домашній інтернет, тож оновлення може бути фальшивим. А якщо ви завантажите таке фальшиве оновлення, то ненавмисно встановите собі на комп'ютер вірусний код.

Якщо ви, як і я, часто перебуваєте в роз'їздах, то оновлення перетворюються на проблему. Перевірити справжність оновлення дуже складно. Якщо ви завантажуєте його через інтернет у готелі, вас можуть спрямувати на фальшивий сайт зі шкідливим «оновленням». Якщо є така можливість, краще скористайтеся телефоном, щоб перевірити наявність оновлення на офіційному сайті постачальника. А ще краще, зачекайте, поки повернетеся в безпечну мережу — приміром, на роботу або додому — і вже звідти завантажуйте оновлення[295].

Дослідники з «Лабораторії Касперського» — компанії, що розробляє системиу ПЗ, — виявили групу кіберзлочинців під назвою DarkHotel (або Tapaoux), які користуються цією схемою. Вони знаходять керівника компанії, який має зупинитися в конкретному елітному готелі, і заражають сервери готелю вірусом перед його приїздом. Коли керівник реєструється й під'єднується до готельного Wi-Fi, вірус потрапляє на його девайс. Після успішного зараження шкідливу програму видаляють із сервера готелю.

Дослідники кажуть, що схема працює вже майже десятиліття. Хоча зазвичай це стосується керівників, що зупиняються в розкішних готелях в Азії, трапитися таке може будь-де. Для загалу група зловмисників зазвичай використовує низькорівневу атаку цільового фішингу, а більш складну «готельну» атаку залишає для одиничних і дуже цінних жертв, як-от керівників у сфері ядерної енергетики й оборонної промисловості.

Одне з перших досліджень припустило, що DarkHotel базується в Південній Кореї, бо кілоґер (вірус, який записує кількість натискань клавіш у зараженій системі), що використовують в атаках, містить у коді корейські символи. А вразливості, на яких паразитували хакери, виявилися вкрай прихованими вадами, про які раніше не чули й самі розробники. Крім того, південнокорейську назву в кілоґері простежили до інших складних кілоґерів, якими раніше користувалися в Кореї.

Однак варто зазначити, що цього недостатньо для підтвердження теорії. Програмне забезпечення можна по шматочках зібрати з різних джерел. Чи взагалі замаскувати його так, ніби воно створене в одній країні, а по факту — в іншій.

Щоб завантажити шкідливе ПЗ на ноутбуки, DarkHotel використовує підроблені сертифікати, нібито випущені урядом Малайзії і Deutsche Telekom. У

розділі 5 я вже казав, що сертифікати потрібні для перевірки автентичності програмного забезпечення або сервера. А ще вірус активується лише через півроку після завантаження — так хакери відводять від себе підозри IT-відділів, які можуть пов'язати вірус із візитом у готель.

Дослідники з «Лабораторії Касперського» дізналися про атаку лиш після того, як їхні клієнти заразилися в кількох розкішних готелях Азії. Антивірусна компанія звернулася до інтернет-провайдера, який обслуговував обидва готелі, і той погодився на спільне розслідування атаки в його мережах. Хоча вірусні файли вже давно зникли з серверів, записи про їх видалення залишилися. І вони відповідали датам перебування постраждалих гостей.

Найпростіший спосіб захиститися від подібних атак — вмикати VPN, щойно під'єдналися до інтернету в готелі. Особисто я користуюся дешевим VPN — усього шість доларів на місяць. Однак якщо хочете стати невидимими, він не підійде, позаяк не має налаштувань анонімності.

Якщо прагнете справжньої невидимості, не довіряйте VPN-сервісу реальну інформацію. А для цього треба заздалегідь зареєструвати фальшиву імейл-адресу (див. розділ 2) і користуватися відкритою бездротовою мережею. Щойно зареєструєте фальшивий імейл, створіть біткоїн-гаманець через Tor, знайдіть біткоїн-банкомат, щоб поповнити цей гаманець, а потім «відмийте» біткоїн через міксер, щоб його не можна було простежити до вашого блокчейну. Для процесу відмивання потрібно два біткоїн-гаманці, зареєстровані через два різні сеанси Tor. З першого гаманця ви відправляєте біткоїни до міксера, а на другий отримуєте «відмиті» біткоїни.

Коли ви переконалися у своїй анонімності (тобто під'єдналися до відкритого Wi-Fi не в полі зору камер плюс увімкнули Tor), знайдіть VPN-сервіс, який приймає оплату біткоїнами. І сплачуйте відмитими біткоїнами. Деякі VPN, як от WiTopia, блокують Tor. Знайдіть такий, що не блокує і, в ідеалі, не зберігає логів підключення.

Так ми не розголошуємо VPN-провайдерові реальну IP-адресу чи ім'я. Однак будьте обережні з таким VPN: під час під'єднання не заходьте в сервіси, зареєстровані на реальне ім'я і не під'єднуйтеся з IP-адреси, яку можна пов'язати з вами. Можливо, варто навіть розглянути варіант з анонімною купівлею одноразового телефона (див. розділ 2).

Краще за все придбати портативний хот-спот, купівлю якого важко буде простежити до вас. Наприклад, попрохайте зробити це когось іншого, щоб ваше обличчя не світилося на камерах спостереження в магазині. Коли користуєтеся анонімним хот-спотом, вимкніть усі персональні пристрої, що посилають стільниковий сигнал, щоб ваші особисті девайси не фігурували в тій самій точці, що й анонімний.

Якщо підсумувати сказане вище, то ось що вам треба зробити, щоб отримати анонімний інтернет у подорожі:

1. Купуйте передплачені подарункові картки анонімно (див. розділ 6). В

ЄС можна анонімно придбати передплачені кредитки на viabuy.com.

2. Користуйтеся відкритим Wi-Fi, змінивши перед цим MAC-адресу (див. розділ 7).
3. Знайдіть імейл-провайдера, який дає змогу зареєструватися без перевірки по SMS. Або можете придбати собі номер у скайпі за допомогою Tor і передплаченої подарункової картки. Через скайп можна приймати дзвінки для підтвердження особи. Обов'язково переконайтеся, що не потрапили в поле зору камер (тобто робіть це не в Starbucks чи схожому місці, нашпигованому камерами спостереження). Коли реєструєте імейл, приховайте своє місцеперебування за допомогою Tor.
4. Укажіть нову, анонімну імейл-адресу під час реєстрації на сайті, де можна створити біткоїн-гаманець і купити валюту (приміром, paxful.com). Знову ж таки, не забудьте про Tor. А біткоїни купуйте на передплачені подарункові картки.
5. Зареєструйте ще один анонімний імейл і ще один біткоїн-гаманець. Перед цим обов'язково перепідключіться до Tor і зайдіть через нову сесію, щоб перший імейл і гаманець ніяк не можна було пов'язати з другими.
6. Пропустіть біткоїни через міксер, щоб відстежити походження валюти було важко. Надішліть «відмиті» біткоїни на другий гаманець.
7. Оформіть на відмиті біткоїни передплату на VPN-сервіс, який не зберігає логів трафіка чи IP-з'єднання. Про логи можна дізнатися з політики конфіденційності VPN-провайдера (зверніть увагу на TorGuard).
8. Придбайте портативний одноразовий хот-спот через іншу особу і лише за готівку.
9. Під'єднуйтеся через анонімний хот-спот до інтернету подалі від дому, роботи й особистих стільникових пристроїв.
10. Увімкнувши хот-спот, одразу під'єднайтеся до VPN.
11. Заходьте в інтернет лише через Tor.

---

274 Адже це — прикордонний обшук, і арешт був би неправомірним. Американські суди досі не визначилися, чи має підозрюваний розголошувати свої паролі. Поки що. Проте суд постановив, що підозрюваного можна примусити пройти автентифікацію на айфоні через Touch ID (відбиток пальця). Щоб убезпечити себе, щоразу, як проходите через митницю, перезавантажуйте айфон чи будь-який пристрій Apple з Touch ID і не вводьте кодовий пароль. Поки не введете код, Touch ID не працюватиме.

275 http://www.computerweekly.com/Articles/2008/03/13/229840/us-department-of-homeland-security-holds-biggest-ever-cybersecurity.htm.

276 На iOS 8 або пізніших версіях операційної системи можна скинути всі сертифікати сполучення, натиснувши Параметри>Загальні>Скидання>Скинути місце і приватність або Скинути налаштування мережі. Дослідник Джонатан Здзіарски писав на цю тему у своєму блозі. Я не буду поміщати його поради в книжку, але якщо ви ставитеся до питання серйозно, можете почитати. Див. http://www.zdziarski.com/blog/?p=2589.

277 http://www.engadget.com/2014/10/31/court-rules-touch-id-is-not-protected-by-the-fifth-amendment-bu/.

278 http://www.cbc.ca/news/canada/nova-scotia/quebec-resident-alain-philippon-to-fight-charge-for-not-giving-up-phone-password-at-airport-1.2982236.

279 http://www.ghacks.net/2013/02/07/forensic-tool-to-decrypt-truecrypt-bitlocker-and-pgp-contains-and-disks-released/.

280 https://www.symantec.com/content/en/us/enterprise/white_papers/b-pgp_how_wholedisk_encryption_works_WP_21158817.en-us.pdf.

281 http://www.kanguru.com/storage-accessories/kanguru-ss3.shtml.

282 https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html.

283 https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/.

284 http://www.securityweek.com/researcher-demonstrates-simple-bitlocker-bypass.

285 https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

286 http://www.nytimes.com/library/tech/00/01/cyber/cyberlaw/28law.html.

287 https://partners.nytimes.com/library/tech/00/01/cyber/cyberlaw/28law.html.

288 https://www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack-iphones/.

289 http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html.

290 https://blog.gdatasoftware.com/blog/article/hotel-safes-are-they-really-safe.html.

291 http://www.snopes.com/crime/warnings/hotelkey.asp.

292 http://www.themarysue.com/hotel-key-myth/.

293 https://shaun.net/posts/whats-contained-in-a-boarding-pass-barcode.

294 Мабуть, United Airlines — одна з небагатьох авіакомпаній, яка видає частковий номер постійного пасажира. Більшість авіакомпаній поміщають у штрих-код повний номер.

295 http://www.wired.com/2014/11/darkhotel-malware/.

Розділ 15
ФБР не спить

У жовтні 2013 року у відділі наукової фантастики філії Публічної бібліотеки Сан-Франциско в Ґлен-парк — недалеко від своєї квартири — Росс Вільям Ульбріхт відповідав клієнтам в онлайн-чаті власної компанії. Людина по той бік екрана думала, що спілкується з адміністратором сайту, який в інтернеті називав себе Жахливим Піратом Робертсом (ЖПР) — ім'я він запозичив із фільму «Принцеса-наречена». Насправді ж цей ЖПР був Россом Ульбріхтом — адміністратором і власником інтернет-магазину наркотиків Silk Road («Шовковий шлях»), а також суб'єктом федерального розшуку[296]. В роботі Ульбріхт часто користувався громадським Wi-Fi — приміром, у бібліотеці. Можливо, він думав, навіть якщо ФБР і впізнає в ньому ЖПР, то ніколи не завалиться з рейдом у громадське місце. Однак того дня «клієнт», з яким спілкувався Ульбріхт, насправді був таємним агентом ФБР.

Щоб керувати онлайн-магазином наркотиків, де клієнти могли анонімно придбати кокаїн, героїн і широкий спектр «дизайнерських наркотиків», була потрібна певна зухвалість. Сайт містився в даркнеті (див. розділ 2), тож доступний був лише через Tor. Оплачували товар лише біткоїнами. Власник Silk Road був обережний... але недостатньо.

За кілька місяців до того, як Ульбріхт листувався в Публічній бібліотеці Сан-Франциско, а ФБР кружляло навколо, на сцені з'явився несподіваний герой, пов'язаний із федеральним розшуком. Герой, який мав докази, що зв'язують Ульбріхта з ЖПР. Ним був співробітник Служби внутрішніх доходів США на ім'я Ґері Елфорд, який зацікавився історією «Шовкового шляху» і вечорами ретельно шукав у ґуґлі будь-яку інформацію. Одне з найперших згадувань про Silk Road датувалося 2011 роком. Хтось під ніком «Альтоїд» згадав про нього в чаті одного сайту. Оскільки на той час Silk Road ще не з'явився, Елфорд припустив, що Альтоїд мав внутрішню інформацію про сайт. Логічно, що Елфорд почав шукати й інші згадування.

І натрапив на скарб.

Виявилося, Альтоїд написав і в чат іншого сайту, але видалив вихідне повідомлення. Однак Елфорд знайшов відповідь на видалене запитання, яка містила текст повідомлення. Альтоїд писав, що якщо хтось може відповісти на його запитання, то може зв'язатися з ним за адресою rossulbricht@gmail.com.[297]

І це була не єдина його помилка. Згодом на поверхню виринули й повідомлення на інших сайтах. Приміром, на сайті Stack Overflow запитання було відправлено з імейлу rossulbricht@gmail.com, але потім ім'я відправника змінили на ЖПР.

Правило невидимості номер один: ніколи не пов'язуйте свою анонімну інтернет-персону зі справжньою. Ніколи.

Після цього знайшлися й інші ниточки, що вели до Ульбріхта. Він, як і ЖПР, підтримував Рона Пола, вільний ринок і лібертаріанську філософію. Якось Ульбріхт навіть замовив кілька фальшивих водійських посвідчень на різні імена з різних штатів, які й привели федералів до його дверей у Сан-Франциско в липні 2013 року... хіба що тоді вони й гадки не мали, що мають справу з ЖПР.

Докази ставали дедалі переконливішими, і, зрештою, того жовтневого ранку 2013 року, щойно Ульбріхт зайшов у чат підтримки клієнтів, федеральні агенти почали тихо просочуватися в бібліотеку в Ґлен-парк. Із хірургічною точністю вони схопили Ульбріхта, перш ніж той устиг вимкнути ноутбук. Якби ноутбук вимкнувся, деякі ключові докази були б знищені. Але за мить після арешту федерали таки сфотографували відкритий екран системного адміністратора на сайті Silk Road і тим самим довели зв'язок між Ульбріхтом, Жахливим Піратом Робертсом і Silk Road. А також поклали кінець будь-яким надіям на анонімність.

Того жовтневого ранку в Ґлен-парк Ульбріхт зайшов на сайт Silk Road від імені адміністратора. І ФБР про це знало, бо спостерігало за його під'єднанням до інтернету. А що, якби він міг підробити геолокацію? Що, якби його не було в бібліотеці, а сам він під'єднався через проксі-сервер?

Улітку 2015 року дослідник Бен Коділл із компанії Rhino Security оголосив, що не лише презентує на DEF CON 23 свій новий пристрій ProxyHam, а й продаватиме його за собівартістю (приблизно 200 доларів) у торговій кімнаті конференції. Але десь за тиждень Коділл заявив, що презентацію скасовано, а перші зразки ProxyHam будуть знищені. Давати коментарі щодо цього розробник відмовився[298].

Виступи на масштабних конференціях з інформаційної безпеки скасовують з різних причин. Зазвичай дослідників змушують мовчати або компанії, розробки яких потраплять під удар, або ж федеральний уряд. Однак Коділл мав на меті не вказати на недоліки чужих продуктів — він створив щось унікальне.

Але ось що цікаво: щойно ідея потрапляє в інтернет, вона залишається там назавжди. Тож навіть якщо федерали чи інші служби переконали Коділла в тому, що виступ суперечить інтересам національної безпеки, хтось неодмінно взявся б за розроблення аналогічного пристрою. Що і сталося.

ProxyHam — дуже віддалена точка доступу. За принципом роботи вона схожа на Wi-Fi роутер у вас вдома чи на роботі. Єдине, що людина, яка користується і контролює ProxyHam, може перебувати десь за півтора кілометра. Через сигнал на частоті 900 МГц Wi-Fi передавач може під'єднатися до антени комп'ютера на відстані аж до чотирьох кілометрів. Якби Ульбріхт скористався таким пристроєм, ФБР могло оточити бібліотеку в Ґлен-парку, поки Росс сидів би в якомусь підвалі за кілька кварталів звідти.

Користь таких пристроїв очевидна для людей, які живуть у країнах із жорстким режимом. Контакт із зовнішнім світом через Tor — це ризик, на який іде купа людей. Подібний девайс нашарував би ще один рівень безпеки, маскуючи геолокацію користувача.

Однак хтось дуже не хотів, щоб Коділл розповідав про це на DEF CON. В інтерв'ю Коділл заперечував втручання Федеральної комісії зі зв'язку. Wired припустив, що таємне встановлення ProxyHam у чужу мережу може бути розцінено як несанкціонований доступ за драконівським і розпливчастим законом «Про боротьбу з комп'ютерним шахрайством та зловживанням». Але Коділл відмовляється коментувати жодні припущення.

Однак, як я вже сказав, щойно ідея потрапить в інтернет, хтось-таки за неї візьметься. Так дослідник інформаційної безпеки Семі Камкар створив ProxyGambit, — по суті, аналог ProxyHam.[299] Єдина відмінність: замість радіосигналу він використовує зворотний стільниковий трафік, а отже, користувач може перебувати не за кілька кілометрів від пристрою, а на іншому кінці світу. Круто!

Звісно ж, ProxyGambit і подібні пристрої перетворяться на головний біль правоохоронних органів, щойно ними вирішать скористатися злочинці.

Ульбріхтівський Silk Road був інтернет-магазином наркотиків. Це не те, що ви знайдете в ґуґлі. Це не те, що можна легко індексувати в так званій поверхневій мережі. Поверхнева мережа, що містить такі знайомі нам амазон і ютуб, — це лише п'ять відсотків всього інтернету. Усі ті сайти, про які ми чули, на які ми заходимо — це мізерна цифра порівняно з фактичною кількістю сайтів в інтернеті, більшість яких прихована від пошуковиків.

Набагато більшим за поверхневу мережу є мережа глибинна — та частина інтернету, що прихована за паролями доступу: наприклад, вміст книжкового каталогу філії Публічної бібліотеки Сан-Франциско у Ґлен-парку. А ще в глибинну мережу входить більшість сайтів за передплатою і внутрішніх сайтів компаній. Netflix. Pandora. Думаю, ви мене зрозуміли.

І, нарешті, невеликий клаптик інтернету, відомий як «темна мережа», або даркнет. Зазвичай у цю частину інтернету не потрапити через звичайний браузер, і тим паче через Google, Bing та Yahoo.

Саме в даркнеті мешкав Silk Road, поряд із сайтами, де можна найняти кілера чи придбати дитячу порнографію. Такі сайти живуть у «темній мережі», бо вона майже є анонімною. Я кажу «майже», бо, по суті, нічого анонімного не існує.

Доступ до даркнету можна дістати лише через Tor-браузер, тож усі сайти в цьому кутку інтернету мають складну буквено-цифрову URL-адресу і закінчуються на «onion» («цибулина»). Як я вже згадував, цибулеву маршрутизацію розробила Дослідницька лабораторія ВМС США, щоби дати людям у країнах із жорсткою владою можливість зв'язатися один з одним й із зовнішнім світом. А ще я казав, що Tor під'єднує ваш браузер не безпосередньо до сайту, а встановлює зв'язок з іншим сервером, який під'єднується до ще одного сервера, а той уже до цільового сайту. Наявність декількох хопів ускладнює завдання тим, хто хоче вас відстежити.

Сайти на зразок Silk Road є продуктами прихованих сервісів Tor-мережі. Їхні URL-адреси генеруються за алгоритмом, а списки веб-сайтів даркнету постійно

змінюються. Через Tor можна проглядати як поверхневу мережу, так і даркнет. Ще один варіант браузера, з якого також можна дістати доступ як до мережі поверхневої, так і темної, — I2P.

Однак ще до закриття Silk Road дехто припускав, що АНБ та інші агентства таки можуть ідентифікувати користувачів в даркнеті. Один із таких способів — створення і контроль так званих вихідних вузлів — точок, через які запит передається до прихованих сайтів. Хоча так визначити початкового користувача все одно неможливо.

Для цього спостерігач має помітити, що на доступ до такого-то сайту щойно надіслали запит, а кількома секундами раніше хтось в Нью-Гемпширі запустив Tor-браузер. На цьому етапі спостерігач може лиш припустити, що дві події якось пов'язані. Але якщо згодом запит на доступ до сайту і запуск Tor-браузера за мить до цього повторяться, тут уже можна говорити про закономірність. Щоб уникнути таких закономірностей, не переривайте під'єднання Tor-браузера.
Ульбріхт поставився до безпеки недбало. Очевидно, попервах у нього не було плану, тож у перших обговореннях Silk Road він чергував справжню адресу електронної пошти з фальшивою.

Як бачите, у сучасному світі не можна й кроку ступити, не залишивши десь в інтернеті слідів реальної особи. Але, як я вже сказав на початку: трохи пильності — і ви теж зможете освоїти мистецтво невидимості. На наступних сторінках я покажу вам, як саме.

---

296 https://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/.

297 http://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html?_r=0.

298 http://www.wired.com/2015/07/online-anonymity-box-puts-mile-away-ip-address/.

299 https://samy.pl/proxygambit/.

Розділ 16

Як оволодіти мистецтвом невидимості

Якщо ви дочитали аж до цієї сторінки, то, напевно, вже задумалися про власний досвід. Чи про те, як легко (або важко) буде зникнути в інтернеті. Чи про те, як далеко хочете (або не хочете) зайти. Може, все це взагалі не для вас? У вас же немає державних секретів! Але що як ви застрягли в судовій тяганині з колишньою пасією? Або посварилися з босом? Або спілкуєтеся з другом, який усе ще потерпає від жорстокості близьких? Або хочете сховати деякі свої дії від адвоката? Існує безліч законних причин, з яких вам може знадобитися анонімно користуватися інтернетом чи іншими технологіями. То які кроки треба зробити, щоб повністю зникнути з радарів? Скільки часу знадобиться? І скільки це коштуватиме?

Якщо ви ще досі не усвідомили, що, аби стати невидимим в інтернеті, треба створити окрему особистість, абсолютно з вами не пов'язану. Це і є анонімність. А коли ви виходите з «режиму інкогніто», треба добряче пильнувати, щоб ваше реальне життя ніяк не торкалося цієї анонімної особи. Тож вам потрібно придбати кілька окремих девайсів виключно для анонімної діяльності. А це може влетіти в добру копійку.

Як варіант, можна створити віртуальну машину просто на робочому столі власного ноутбука. Віртуальна машина — це програмний комп'ютер. Вона міститься всередині спеціального застосунку, як-от VMware Fusion. Ви можете завантажити на віртуальну машину ліцензійну копію Windows 10 і вказати, скільки ОЗУ, дискового простору тощо вона може використовувати. Спостерігачеві на іншому кінці інтернету здаватиметься, що ви користуєтеся комп'ютером на Windows 10, навіть якщо насправді у вас Mac.

Професійні дослідники інформаційної безпеки постійно користуються віртуальними машинами, створюючи і знищуючи їх одним рухом. Але навіть серед професіоналів існує ризик витоку даних. Наприклад, ви можете запустити віртуальну машину на Windows 10 і необачно увійти у свій імейл. Тепер цю віртуальну машину можна пов'язати з вами.

Отже, перший крок до анонімності — придбання окремого ноутбука лише для вашої анонімної діяльності в інтернеті. Бо варто вам хоч раз оступитися і зайти на мить в особисту пошту з віртуальної машини — ви програли. Тож рекомендую придбати недорогий ноутбук на Windows (а ще краще — Linux, якщо ви знаєте, як ним користуватися). MacBook Pro не рекомендую лише тому, що він набагато дорожчий за ноутбук на Windows.

Раніше я рекомендував придбати ще один ноутбук — зокрема Chromebook — лише для фінансових операцій в інтернеті. Але є й інший варіант — айпад. Зареєструвати Apple ID можна на особисту адресу електронної пошти і кредитку

або через подарункову картку iTunes. Позаяк девайс призначений лише для безпечного діалогу з банком, невидимість тут не є метою.

Але якщо ви прагнете до анонімності, то Chromebook — не найкращий варіант. Він не дасть вам такої самої гнучкості, як ноутбук на Windows чи операційній системі на основі Linux (приміром, Ubuntu). Windows 10 — непогане рішення, якщо ви проігноруєте прохання системи зареєструвати акаунт у Microsoft. Не варто зв'язувати цей комп'ютер із Microsoft у жодному разі.

Купувати ноутбук треба в магазині готівкою, а не через інтернет, щоб покупку не змогли простежити до вас. І не забувайте, що новий ноутбук містить бездротову мережеву карту з унікальною MAC-адресою. Якщо її якось дізнаються, то зможуть відстежити власника комп'ютера. Наприклад, якщо ви сидите в Starbucks і вмикаєте ноутбук, система прозондує приміщення на наявність бездротових мереж, до яких ви під'єднувалися раніше. Якщо в кафе стоїть моніторингове обладнання, що реєструє цей запит, то воно може дізнатися вашу справжню MAC-адресу. А уряд може відстежити покупку ноутбука, якщо встановить зв'язок між MAC-адресою вашої мережевої карти і серійним номером комп'ютера. Опісля федералам потрібно буде лиш визначити, хто купив конкретний ноутбук, — і все. Вас ідентифікують. Не думаю, що це складно.

Раджу встановити Tails (див. розділ 14) і Tor (див. розділ 2) і використовувати їх замість вбудованої операційної системи й браузера.

Не входьте в жодні акаунти на сайтах і в застосунках від реальної особи. Ви вже переконалися, як легко відстежити людину й комп'ютер в інтернеті. Заходити кудись під справжнім ім'ям — геть погана ідея. Банки та інші сайти постійно запитують відбиток пальця, щоб запобігти шахрайству, а це залишає помітний слід на девайсі. Тож якщо колись зайдете на ті самі сайти анонімно, вони можуть ідентифікувати ваш комп'ютер.

А ще непогано було б відключати Wi-Fi роутер перед тим, як вмикаєте вдома анонімний ноутбук. Якщо під'єднаєтеся до домашнього маршрутизатора, провайдер зможе отримати MAC-адресу анонімного комп'ютера (якщо цей постачальник володіє і керує вашим домашнім маршрутизатором). Тож раджу завжди купувати власний роутер, над яким у вас буде повний контроль. Так провайдер не отримає MAC-адреси комп'ютерів у вашій локальній мережі й бачитиме лише MAC-адресу самого маршрутизатора, а це для вас жодного ризику не несе.

Вам потрібно мати змогу відхреститися від своїх дій. Вам потрібно провести своє з'єднання через кілька проксі, щоб слідчим було дуже важко зв'язати його не лише з вами — узагалі з єдиною людиною. Я от припустився помилки, коли був утікачем. Я неодноразово маскував свою геолокацію, під'єднуючись зі стільникового телефона до модемів Netcom — привиду інтернет-провайдерів минулого. Позаяк робив я це з однієї точки, мій ворог (Цутому Сімомура)

визначив стільникову вежу, до якої під'єднувався мій телефон, — і знайти мене через радіопеленгування стало завиграшки. Це допомогло йому визначити мою геолокацію і передати її ФБР[300]. Висновок такий: ніколи не користуйтеся анонімним ноутбуком удома чи на роботі. Ніколи. Тож якщо купуватимете окремий девайс, пообіцяйте собі ніколи не перевіряти з нього особистий імейл, фейсбук і навіть прогноз погоди[301].

Ще один перевірений спосіб відстежити вас в інтернеті — за рухом грошей. А вам, як не крути, доведеться за щось платити. Тож не поспішайте вмикати анонімний ноутбук і шукати відкриту бездротову мережу — спершу треба непомітно придбати кілька подарункових карток. Позаяк магазини, де продаються подарункові картки, переважно мають камери спостереження біля прилавка, треба діяти вкрай обережно. Не купуйте їх особисто — краще попрохайте про це випадкову людину з вулиці, а самі почекайте на безпечній відстані.

Але як це провернути? Особисто я знаходжу когось на стоянці й жаліюся, що в магазині працює моя колишня, на яку я геть не хочу натрапити. Зійде все, що звучить правдоподібно. Можете навіть додати, що в неї проти вас заборонний припис. Певен, за 100 доларів подяки перспектива допомогти матиме досить привабливий вигляд.

Що ж, лазівку для того, щоб зайти в магазин і придбати кілька передплачених карток, ми знайшли. Але які саме картки купувати? Раджу взяти кілька передплачених карток з фіксованою сумою в 100 доларів. Поповнювані кредитки не підійдуть, бо, відповідно до «Патріотичного акта», під час активації доведеться розсекретити свою особу і вказати справжнє ім'я, адресу, дату народження та номер соціального страхування, які можна буде звірити по базах кредитних установ. А називати видумане ім'я або чужий номер соціального страхування — це протизаконно і навряд чи варто ризику.

Ми ж хочемо стати невидимками, а не порушниками закону.

Раджу купувати подарункові кредитки Vanilla Visa чи Vanilla Mastercard на 100 доларів у мережевих аптеках, 7-Eleven, Walmart чи інших великих гіпермаркетах. Такі картки зазвичай купують на подарунок, а працюють вони як і звичайні кредитки. Особисту інформацію вказувати не треба, а придбати їх можна анонімно й готівкою. Якщо ви мешкаєте в ЄС, то можете анонімно замовити таку кредитну картку на viabuy.com. У Європі їх можуть відправити на поштове відділення, яке не запитує у вас посвідчення особи. Сайт надсилає вам PIN-код, яким ви можете відкрити поштову скриньку й забрати картку інкогніто (звісно ж, якщо там нема камер).

Як же ж тепер скористатися новим ноутбуком і анонімними передплаченими картками?

З появою недорогих оптичних носіїв даних громадські місця, що надають безкоштовний бездротовий доступ, тепер можуть роками зберігати записи з камер спостереження, а слідчі — відносно легко отримати їх і відшукати

потенційних підозрюваних. Засікши вас на камерах, вони можуть просто проаналізувати список MAC-адрес, що під'єдналися до бездротової мережі в цей період, і зіставити їх із вашою MAC-адресою. Ось чому важливо змінювати MAC-адресу щоразу, як під'єднуєтеся до безкоштовної Wi-Fi мережі. Знайдіть місце по сусідству з тим, де є безкоштовний Wi-Fi. Наприклад, китайський ресторан поруч із Starbucks чи іншим закладом, який транслює безкоштовну мережу. Сядьте за столик біля стіни, за якою той заклад із роутером. Можливо, швидкість з'єднання буде повільнішою, але так ви отримаєте відносну анонімність (принаймні якщо слідчі не почнуть проглядати записи з усіх камер спостереження поблизу).

Імовірно, бездротова мережа зареєструє і збереже вашу MAC-адресу відразу після автентифікації. Пам'ятаєте коханку генерала Девіда Петреуса? Пам'ятаєте, що дати її заїздів у готелі відповідали датам появи її MAC-адреси в мережах цих готелів? Не дозволяйте таким дурним помилкам скомпрометувати вашу анонімність. Змінюйте MAC-адресу щоразу, як під'єднуєтеся до громадського Wi-Fi (див. розділ 7).

Що ж, поки все досить чітко і ясно. Придбайте окремий ноутбук для анонімної діяльності. Придбайте подарункові картки інкогніто. Щоб не потрапити на камери спостереження, знайдіть Wi-Fi мережу, сигнал якої дістає до сусіднього закладу. І змінюйте MAC-адресу під час кожного під'єднання до безкоштовної бездротової мережі.

Ясна річ, це ще не все. Далеко не все. Ми лише починаємо.

Можна найняти ще одну підставну особу, на цей раз для важливої покупки — особистого хот-споту. Якщо пам'ятаєте, ФБР зловило мене, бо я під'єднувався до мереж у всьому світі через стільниковий телефон і модем. З часом моє місцеперебування розкрили, тому що телефон раз за разом під'єднувався до одної стільникової вежі. А через радіопеленгатор мій телефон знайти було дуже просто. Не повторюйте моїх помилок. Найміть незнайомця, який піде в салон Verizon (або AT&T чи T-Mobile) і придбає особистий хот-спот, через який можна під'єднуватися до інтернету за допомогою стільникових даних. А отже, у вас буде власний, локальний достун до інтернету, і вам не доведеться під'єднуватися до громадського Wi-Fi. Але, якщо хочете захистити анонімність, ніколи не користуйтеся персональним хот-спотом в одній точці кілька разів.

Коли наймаєте підставного покупця, не світіть перед ним номерним знаком автомобіля чи іншою особистою інформацією. Дайте йому 200 доларів готівкою за хот-спот і пообіцяйте 100 доларів винагороди, коли той повернеться з девайсом. У результаті оператор продасть персональний хот-спот «фальшивому покупцеві», і вас у жодному разі не викриють. А ще можна заодно придбати й кілька передплачених карток. Не гарантую, що підставний покупець не змиється з вашими грошима, але заради анонімності можна ризикнути. Опісля поповнювати одноразовий пристрій можна буде біткоїнами[302].

Якщо ви анонімно придбали портативний хот-спот, запам'ятайте: заради Бога, ніколи не вмикайте пристрій удома! Це як з анонімним ноутбуком. Щоразу, як ви вмикаєте хот-спот, його реєструє найближча вежа стільникового зв'язку. Буде сумно, якщо адреса вашого будинку, роботи або улюбленого закладу з'явиться в логах мобільного оператора.

І ніколи не вмикайте особистий телефон чи особистий ноутбук у тому самому місці, де й анонімний ноутбук, хот-спот чи одноразовий телефон. Не змішувати їх вкрай важливо. Будь-який запис, який зможе пов'язати вашу анонімну особу з реальною, зведе нанівець усю операцію.

А тепер, озброївшись передплаченими подарунковими картками й особистим хот-спотом із передплаченим тарифним планом (звісно ж, купленими анонімно двома абсолютно різними людьми, які не мають про вас жодної особистої інформації, з якою можна звернутися до поліції), ви вже майже готові. Майже. З цього часу створюйте й заходьте в усі аканути лише через Tor-браузер, бо він постійно змінює вашу IP-адресу.

Спершу відкрийте Tor і заведіть собі кілька анонімних імейлів. Не повторюйте помилок Росса Ульбріхта. Якщо пам'ятаєте, у даркнеті він неодноразово вказував особистий імейл стосовно Silk Road. Завдяки цим випадковим ниточкам, що зв'язували особу Жахливого Пірата Робертса і Росса Ульбріхта, слідчі змогли довести, що обидва імені належали одній людині.

У боротьбі із шахраями більшість мейл-сервісів, як-от Gmail, Hotmail, Outlook і Yahoo, потребують верифікації через мобільний телефон. Тобто під час реєстрації вам треба ввести номер свого мобільного телефону, на який одразу надійде текстове повідомлення для підтвердження вашої особи.

Так, ви завжди можете вказати номер одноразового телефону. Але пам'ятайте, що цей одноразовий телефон і картки поповнення треба купувати анонімно, тобто придбати через третіх осіб, яких не можна ніяк пов'язати з вами. Крім того, одноразовим телефоном не можна користуватися поблизу інших ваших стільникових пристроїв. Тож краще залиште особистий телефон удома.

Щоб купити біткоїни в інтернеті, вам знадобляться як мінімум дві анонімні адреси електронної пошти і два біткоїн-гаманці. Тож як створити анонімний імейл? Як ті, що були в Едварда Сноудена і Лори Пойтрас?

Я провів дослідження і, знайшовши кілька придатних сервісів, зміг створити один імейл на protonmail.com і ще один на tutanota.com. Усе через Tor і без жодних вимог підтвердити мою особу. Не вимагали ці сервіси верифікації і на етапі налаштування пошти. Можете провести власне дослідження: пошукайте служби електронної пошти й подивіться, чи запитують вони ваш номер мобільного в процесі реєстрації. А ще зауважте, скільки інформації вони потребують для створення акаунта. Ще один непоганий варіант — fastmail.com. Він не такий багатий на функції, як Gmail, але є платним сервісом, тож не збирає даних користувачів і не містить реклами.

Отже, тепер у вас є ноутбук зі встановленими Tor і Tails, одноразовий телефон, кілька анонімних передплачених карток і анонімний хот-спот з анонімно придбаним тарифним планом. Але ви все ще не готові. Щоб підтримувати анонімність, доведеться конвертувати наші анонімні подарункові картки в біткоїни.

У розділі 6 ми говорили про таку віртуальну валюту як біткоїн. Самі собою біткоїни не анонімні. Їх завжди можна відстежити до покупця через так званий блокчейн, а далі — й усі покупки за ці гроші. Тож сам собою біткоїн вас не сховає. Спершу нам доведеться провести кошти відповідно до схеми анонімності: спочатку перетворити передплачені подарункові картки на біткоїни, а їх уже перегнати через міксер. У результаті у вас з'являться анонімні біткоїни, якими можна спокійно користуватися для платежів. А «відмиті» біткоїни знадобляться нам для оплати VPN-сервісу і майбутніх поповнень портативного хот-споту й одноразового телефона. Біткоїн-гаманець можна створити через Tor на paxful.com чи деінде. Деякі сайти пропонують придбати біткоїни за подарункові картки, приміром, за Vanilla Visa чи Vanilla Mastercard, про які я вже згадував. Але тут існує суттєвий мінус: за послугу доведеться заплатити величезну комісію — щонайменше 50 %. Сам же paxful.com більше схожий на eBay: сайт просто пропонує список продавців біткоїнів, із якими з'єднує покупців.

Ясна річ, анонімність коштує дорого. Що менше особистої інформації прохають для транзакції, то більше ви заплатите. І це логічно: люди, які продають біткоїни, йдуть на величезний ризик, не перевіряючи вашу особу. Особисто я зміг придбати біткоїни в обмін на анонімні подарункові картки Vanilla Visa за курсом 1,70 долара до одного, що просто нечувано. Але дешевше «купити» анонімність складно.

Як я вже казав, біткоїн сам собою не є анонімним. Наприклад, десь там зберігається запис, що я обміняв передплачені подарункові картки на біткоїни. Слідчий може підняти ці записи й простежити мої біткоїни до подарункових карток.

Але біткоїни можна відмити і стерти будь-який зв'язок зі мною.

Відмиванням грошей злочинці займалися споконвіку. Зазвичай процедура популярна у сфері торгівлі наркотиками, але трапляється й у «білокомірцевій» злочинності. Відмиваючи гроші, ви приховуєте особу початкового власника. Зазвичай кошти проводять по кількох банках інших країн, які мають суворі закони щодо конфіденційності. Виявляється, щось подібне можна провернути і з віртуальною валютою. Для цього потрібні міксери. Вони беруть біткоїни з різних джерел і змішують — або міксують — їх так, що отриманий біткоїн зберігає вартість, але містить сліди кількох власників. Як результат, дуже важко сказати, котрий із цих власників зробив конкретну покупку. Але будьте обережні: в інтернеті тусується купа шахраїв.

Однак я ризикнув. Я знайшов біткоїн-міксер, який провів мені транзакцію і зняв за це додаткову плату. Так, я отримав обіцяні гроші, але подумайте ось про що: у цього міксера тепер є один із моїх анонімних імейлів і обидві біткоїн-адреси, які брали участь в транзакції. Тому я вирішив ще трохи замести сліди. Біткоїни я переслав на другий гаманець, створений у новому сеансі Tor, який згенерував кілька хопів між мною та цільовим сайтом. Тепер транзакція була достатньо заплутана. З'ясувати, що ці дві біткоїн-адреси належать тій самій людині, тепер було майже неможливо. Ясна річ, біткоїн-міксер може співпрацювати з третіми особами й передати їм обидві адреси. Ось чому так важливо купувати передплачені картки анонімно.

Використавши подарункові картки для купівлі біткоїнів, не забудьте надійно утилізувати пластикові картки (не викидайте їх у смітник біля дому). Раджу скористатися шредером, розрахованим на пластикові картки, а залишки викинути в якийсь смітник подалі від дому та роботи.

Щойно отримаєте відмиті біткоїни, можете йти на VPN-сервіс за додатковим шаром конфіденційності.

Якщо ви справді прагнете анонімності, краще не довіряйте VPN-провайдерам. Особливо тим, які заприсягаються, що не зберігають жодних логів. Думаю, вони все одно видадуть ваші дані, якщо на них натиснуть правоохоронні органи чи АНБ.

Я от, наприклад, щиро переконаний, що всі VPN-провайдери мають якось розв'язувати проблеми у власній мережі. А для розв'язання цих проблем логи таки потрібні — приміром, логи підключення, за якими можна зіставити клієнтів з вихідними IP-адресами.

Позаяк навіть найкращим провайдерам довіряти не варто, ми заплатимо за VPN-сервіс відмитими біткоїнами і зареєструємося через Tor-браузер. Раджу вам переглянути умови надання послуг і політику конфіденційності всіх VPN-провайдерів і вибрати того, що здається найбільш прийнятним. Ідеального ви все одно не знайдете — хоча б уже був непоганий. І пам'ятайте, що жодному провайдерові не можна довіряти свою анонімність. Ви повинні дбати про неї самі й усвідомлювати, що навіть найменша помилка може розкрити вашу особу.

Тепер у вас є окремий ноутбук із Tor чи Tails і VPN-провайдером, оплаченим відмитими біткоїнами, анонімно куплений хот-спот і ще відмиті біткоїни про запас. Що ж, ви впоралися з легкою частиною: підготовкою. Це коштуватиме вам кілька сотень доларів (може, навіть до п'ятисот), але всі частини системи є анонімними, тож відстежити вас за ними буде майже неможливо. А тепер найважчий етап: зберегти анонімність.

Усі плоди ретельної підготовки можна за мить звести нанівець, скориставшись анонімним хот-спотом удома. Або ввімкнувши особистий телефон, планшет чи інший стільниковий пристрій, пов'язаний із вашою реальною особою, у місці, де користуєтеся анонімними девайсами. Лише один маленький промах — і слідчий зможе пов'язати вас із цією геолокацією через аналіз логів мобільного

провайдера. Якщо ваші пристрої неодноразово реєструватимуться одночасно з анонімними девайсами на тій самій стільниковій базі, ваша конспірація опиниться під загрозою.

Я вже наводив кілька прикладів.

Якщо вас раптом розкриють, а ви знову захочете зникнути з радарів, доведеться пройти через процес підготовки ще раз, тобто стерти і перевстановити операційну систему на анонімному ноутбуці, створити нові анонімні імейли для біткоїн-гаманців, купити новий анонімний хот-спот. Згадайте, як Едвард Сноуден і Лора Пойтрас створили додаткові анонімні імейли для спілкування тет-а-тет, хоча вже мали зашифровану електронну пошту. Але все це необхідно, лише якщо ви підозрюєте, що вашу першу анонімну систему розкрили. А так можете спокійно інкогніто сидіти в інтернеті через Tor-браузер (щоразу з нової сесії), анонімний хот-спот і VPN.

Ясна річ, будете ви дотримуватися моїх рекомендацій повністю чи частково — справа ваша.

Але навіть якщо ви виконуватимете мої поради на сто відсотків, все одно є шанс, що вас впізнають. Як? За стилем вашого тексту.

Існує купа досліджень щодо особливостей підбирання слів, якими люди часто користуються в електронних листах і коментарях у соцмережах. Проаналізувавши слова, дослідники часто можуть визначити стать і етнічну належність людини. Але до конкретики тут далеко.

Чи недалеко?

Під час Другої світової війни британський уряд установив у всій країні станції прослуховування для перехоплення сигналів німецьких військ. Уже незабаром союзники досягли успіхів у дешифруванні цих сигналів — у маєтку Блечлі-Парк, де базувалася Урядова школа кодів та шифрів і був зламаний код німецької «Енігми». До того часу військові у Блечлі-Парку, перехоплюючи німецькі телеграфні повідомлення, могли ідентифікувати відправника за унікальною розстановкою інтервалів між крапками й тире. Наприклад, могли дізнатися, коли одного телеграфіста змінював інший, і навіть почали давати їм імена.

Як узагалі звичайні крапки й тире можуть указати на людину, яка їх відправила? Річ у тому, що часовий інтервал між двома натисканнями телеграфного ключа можна виміряти. Згодом цей метод охрестили «кулаком відправника», бо всіх операторів ключа Морзе можна було ідентифікувати за їхніми унікальними «кулаками». Від початку телеграф призначався не для цього (головне те, що було в повідомленні, а не хто його послав), але в цьому випадку особливості набору стали цікавим побічним продуктом.

Сьогодні ж, завдяки прогресу цифрових технологій, електронні пристрої можуть виміряти особливості натискання клавіші на клавіатурах з точністю до наносекунди: не тільки тривалість утримання однієї клавіші, а й швидкість натискання наступної. Так можна легко розрізнити, хто друкує спокійно, а хто

несамовито лупить по клавіатурі. У поєднанні з підбором слів, це може багато розповісти про аноніма.

І це перетворюється на проблему, якщо ви намагаєтеся анонімізувати IP-адресу. Цільовий сайт усе ще може впізнати вас: не за технічними характеристиками, а за людськими. Таке ще називається поведінковим аналізом.

Припустимо, у Tor ви натрапили на анонімний сайт, який хоче створити ваш профіль натискання клавіш. Можливо, за цим стоять зловмисники, які хочуть дізнатися про вас більше. А може, і правоохоронні органи.

Купа фінансових установ вже користується аналізом натискання клавіш для захисту автентифікації користувачів. Тобто якщо хтось і отримає ваш логін і пароль, він не зможе підробити ритм вашого друкування. І добре, якщо це потрібно для автентифікації в інтернеті. А якщо ні?

Позаяк такий аналіз провести завиграшки, дослідники Пер Торшейм і Пол Мур створили плагін для Chrome під назвою Keyboard Privacy. Плагін реєструє ваші натискання клавіш, а потім відтворює їх із різними інтервалами. Суть у тому, щоб додати елемент випадковості у ваш звичний ритм натискання клавіш. Тож плагін може додатково маскувати ваші анонімні дії в інтернеті[303].

Отже, розділяти в інтернеті життя реальне й анонімне цілком можливо, але це потребує постійної пильності. У попередньому розділі я розповідав про феєричні провали в мистецтві невидимості. Спроби були чудові, але дуже короткі.

Приміром, Росс Ульбріхт не надто ретельно сконструював своє альтер-его, подекуди вказуючи справжній імейл замість анонімного, особливо попервах. Трохи глибокого пошуку в ґуґлі — і слідчий зміг зіставити достатньо інформації, щоб розкрити таємничого власника Silk Road.

А як щодо Едварда Сноудена й інших людей, які перебувають під наглядом однієї або кількох урядових установ? Наприклад, Сноуден має обліковий запис у твітері. Як і більшість експертів із конфіденційності. Інакше як би мені вдалося зіштовхнути їх лобами в інтернеті? І водночас вони начебто залишаються «невидимими». Цьому в мене є кілька пояснень.

Вони не під пильним наглядом. Можливо, уряд знає про їхнє місцеперебування, але йому байдуже. Припустимо, вони не порушують законів. Тоді як дізнатися, чи втратили вони десь пильність? Вони можуть стверджувати, що користуються Tor лише для анонімних імейлів, але, знову ж таки, хто знає? Може, вони з цього акаунта купують фільми на Netflix?

Вони під наглядом, але їх не можна заарештувати. Думаю, це вже ближче до Сноудена. Можливо, у якийсь момент він проколовся, і тепер за ним активно стежать, куди б він не пішов... Але він живе в Росії. А в Росії нема жодних підстав його заарештовувати й повертати в Сполучені Штати.

Зауважте, що я сказав не «помилився», а «проколовся». Якщо у вас нема таланту неймовірної уваги до деталей, то жити двома життями вам буде важко. Я знаю, що кажу. Я сам проколовся. Я послабив оборону, коли скористався одним

і тим самим місцем, щоб дістати доступ до комп'ютерів через мережу стільникового зв'язку.

У сфері безпеки є одна непохитна істина: наполегливий зловмисник неодмінно досягне успіху, якщо в нього буде достатньо часу й ресурсів. Я завжди зламував системи моїх клієнтів, коли тестував їх на проникнення. Своєю анонімністю ви лиш ставите зловмисникові якомога більше перешкод, сподіваючись, що той здасться і перейде до іншої цілі.

Більшості з нас треба сховатися зовсім ненадовго. Ушитися від начальника, який хоче вас звільнити. Обвести навколо пальця колишню пасію, адвокати якої шукають на вас хоч щось, що можна використати в суді. Втекти від моторошного сталкера, який побачив на фейсбуці ваше фото і тепер псує вам нерви. Яка б у вас не була причина, описаних кроків цілком вистачить на той період, щоби виплутатися з халепи.

Анонімність у сучасному цифровому світі потребує тяжкої роботи й постійної пильності. Вимоги до анонімності в кожної людини різні: може, вам треба захистити паролі й особисті документи від колег? Або сховатися від набридливого шанувальника? Чи втекти від правоохоронних органів, бо ви — інформатор?

Від ваших індивідуальних потреб залежить те, які кроки вам треба зробити, щоб підтримувати бажаний рівень анонімності. Можливо, вам вистачить надійних паролів і способів боротися з офісним принтером, який за вами шпигує. А може, доведеться пройти кожен описаний тут крок, щоб слідчі не змогли розсекретити вашу справжню особу.

Але всім нам варто хоч трохи дізнатися про те, як звести до мінімуму наші сліди в цифровому світі. Усі ми здатні двічі подумати, перш ніж постити фотографію з домашньою адресою на задньому плані. Чи зазначати реальну дату народження й іншу особисту інформацію в профілях у соцмережах. Чи лазити в інтернеті без розширення HTTPS Everywhere. Чи робити конфіденційні дзвінки або надсилати конфіденційні повідомлення без інструмента наскрізного шифрування на зразок Signal. Чи писати лікарю через AOL, MSN Messenger або Google Talk без OTR. Чи надсилати конфіденційний імейл без PGP або GPG.

І ми здатні заздалегідь подбати про особисту інформацію. Усвідомити, що навіть, здавалося б, безневинні дії — запостити фотографію, забути змінити стандартний логін і пароль, скористатися робочим телефоном для особистих повідомлень чи створити обліковий запис на фейсбуці для дитини — ведуть до сумних наслідків на все життя. Тож треба діяти.

Ця книжка про те, як користуватися інтернетом, зберігаючи водночас дорогоцінну конфіденційність. Усі ми — від абсолютних «чайників» у комп'ютерах до фахівців з інформаційної безпеки — повинні приділити час і увагу мистецтву, яке стає все важливішим із кожним днем. Мистецтву невидимості.

300 Але це не кінець історії. Попри те що співробітники ФБР визначили мій житловий комплекс, вони не знали, де конкретно я мешкав. Але дізналися, коли я якось вийшов на вулицю ввечері. Про це можна прочитати в моїй книжці «Привид у дротах» (Ghost in the Wires).

301 Сайти на зразок Weather Underground фіксують довготу й широту місцезнаходження відвідувача в URL.

302 Наприклад, https://www.bitrefill.com.

303 https://nakedsecurity.sophos.com/2015/07/30/websites-can-track-us-by-the-way-we-type-heres-how-to-stop-it/.

Подяки

Цю книжку присвячую моїй люблячій матері Шеллі Джафф і бабусі Рібі Вартанян, які жертвували заради мене всім, скільки я себе пам'ятаю. Байдуже, у яку халепу я встрявав: мої матуся й бабуся завжди були поруч, тим паче в тяжкі часи. Ця книжка не з'явилася б без моєї чудової родини, яка дарувала мені тонни безумовної любові й підтримки протягом усього життя.

15 квітня 2013 року моя мати померла після тривалої боротьби з раком легенів. Після довгих років страждань і битв із наслідками хіміотерапії. І все ж страшні процедури, якими в сучасній медицині стримують рак, подарували нам кілька світлих днів. Зазвичай у таких пацієнтів украй обмаль часу. Зазвичай за кілька місяців вони здаються під тиском хвороби. Мені дуже пощастило провести з нею той час, поки вона тримала удар у своїй жахливій боротьбі. Я вдячний, що мене виростила така любляча і віддана мати, яку я вважаю своїм найкращим другом. Моя мама — просто дивовижна людина, і я невимовно за нею сумую.

7 березня 2012 року в лікарні «Санрайз» у Лас-Вегасі раптово померла моя бабуся. Усі ми були певні, що лікування пройде успішно і вона повернеться додому, але цього так і не сталося. За кілька років до смерті бабуся дуже нервувалася і сумувала через хворобу моєї мами. Нам її страшенно не вистачає. Хотів би я, щоб вона була тут, поряд зі мною, і могла радіти моїм успіхам.

Сподіваюся, що ця книжка потішить моїх маму й бабусю. Сподіваюся, вони пишатимуться тим, що я допомагаю людям захищати своє право на приватне життя.

Дуже прикро, щоб мій батько, Алан Митник, і брат, Адам Митник, не можуть відсвяткувати разом зі мною публікацію цієї важливої книжки. Книжки про те, як бути невидимим в епоху, де шпигунство і спостереження стали нормою.

Я мав щастя долучити до написання книжки фахівця з інформаційної безпеки і конфіденційності Роберта Вемосі. Безцінні знання Роба у сфері безпеки і неймовірний талант письменника допомогли йому знайти сильні історії, перевірити їх і причепурити мою писанину так, щоб її зрозуміла будь-яка пересічна людина. Знімаю капелюха перед Робом, який вклав у цей проект тонну зусиль. Чесно кажучи, без нього я не впорався б.

Також хочу подякувати тим людям, які доклали руку до моєї професійної кар'єри і повністю віддалися справі. Мій літературний агент з LaunchBooks, Девід Ф'юґейт, вів переговори щодо контракту на книжку і співробітництва з видавцем — Little, Brown and Company. Концепцію «мистецтва невидимості» видумав Джон Раф'юз зі 121 Minds, який є моїм агентом з питань публічних виступів і рекламних компаній, а також керує стратегічним розвитком бізнесу в моїй компанії. Джон за власною ініціативою запропонував мені ідею для книжки разом із макетом обкладинки. Він постійно підштовхував мене написати

книжку, яка б допомогла населенню планети захистити свої права на особисте життя від навали «Великого брата» і великих даних. Джон просто неймовірний.

І я вдячний Little, Brown and Company за шанс попрацювати над таким чудовим проектом. Дякую моєму редакторові, Джону Парслі, за його старанну роботу й відмінні поради щодо книжки. Спасибі, Джоне!

Хочу подякувати моєму другу Мікко Гюппонену — директору з досліджень у F-Secure — за те, що витратив свій дорогоцінний час на передмову до цієї книжки. Мікко — шанований експерт у галузі інформаційної безпеки та конфіденційності, який уже двадцять п'ять років працює над дослідженням вірусів.

А ще я вдячний Томі Туомінену з F-Secure за те, що знайшов час у своєму щільному графіку для технічного огляду рукопису, вказав на помилки і звернув увагу на все, що я упустив.