Розв’яжи свою проблему з усмішкою

Пан із банку знає моє ім’я і має надто багато вільного часу

Як розпізнати фальшивий дзвінок із банку та самостійно перевірити особу співрозмовника



Max Paradox

Пан із банку знає моє ім’я і має надто багато вільного часу

Як розпізнати фальшивий дзвінок із банку та самостійно перевірити особу співрозмовника

Max Paradox

Rozwiąż swój problem z przymrużeniem oka

ISBN: 9788384905722

ALL-IN Rafał Płonkowski



ЗМІСТ

INTRO 5

Розділ 1 - Добрий день, телефоную з банку. Принаймні я так стверджую 11

Розділ 2 - Звідки він усе це знає? Анатомія довіри в кредит 20

Розділ 3 - Гроші зникнуть за п’ять хвилин, або як шахрай краде твій час, перш ніж украде щось інше 29

Розділ 4 - Три чарівні слова: «Я на цьому знаюся». Чому уявні засоби захисту не працюють 38

Розділ 5 - Вибачте, що не дозволяю себе ошукати. Пастка надмірної ввічливості 48

Розділ 6 - Будь ласка, натисніть тут. Технологія, яка мала допомагати, а почала віддавати накази 58

Розділ 7 - Залишився лише один крок. Чому так важко перервати розпочату процедуру 67

Розділ 8 - Коли шахрай одягає мундир авторитету. Чому посада не замінює доказів 75

Розділ 9 - Поклади слухавку, але з розумом. Мистецтво повернути контроль над телефонною розмовою 84

Розділ 10 - Перевіряй банк, а не розповідь. Як насправді перевірити співрозмовника 93

Розділ 11 - Код надійшов, отже, усе гаразд? Як читати банківські повідомлення, поки не стало запізно 102

Розділ 12 - Я вже повідомив код. Що тепер? Перша допомога банківському рахунку без паніки й самобичування..... 112

Розділ 13 - Банківський дзвінок під лупою. Як перевірити підозрілу історію, не стаючи детективом 122

Розділ 14 - Домашній центр безпеки. Підготуйся, перш ніж зателефонує пан, який рятує заощадження.....132

Розділ 15 - Банк не відповідає, телефон божеволіє, а шахрай у чудовому настрої. Що робити, коли ідеальний план руйнується 142

Розділ 16 - Гроші пішли, а пан із банку зник. Як упорядкувати справи після шахрайства 152

Розділ 17 - Це не мій рахунок, але моя проблема. Як допомогти близькій людині, яка розмовляє з шахраєм.....162

Розділ 18 - Безпечна звичка замість щоденної підозріливості. Як залишатися пильним, не живучи в стані тривоги.....171

Розділ 19 - Знову телефонують. Як розпізнати загрозу, що повертається, перш ніж вона знову заволодіє твоєю увагою 181

Розділ 20 - Пан із банку може зачекати. Твої гроші, твої правила..... 191

INTRO

Телефон дзвонить о 14:37. Номер здається знайомим, можливо, навіть нагадує той, що вказаний на офіційному сайті банку. Ти відповідаєш, адже ти відповідальна людина. На іншому кінці лінії лунає ввічливий чоловічий голос. Чоловік представляється співробітником відділу безпеки, називає твоє ім'я та прізвище, а потім повідомляє, що щойно було виявлено підозрілу спробу переказу грошей із твого рахунку. Звучить серйозно. Дуже серйозно. Особливо з огляду на те, що пан говорить спокійно, професійно й із такою впевненістю, ніби кілька хвилин тому особисто врятував світову фінансову систему, а тепер знайшов ще п'ять хвилин, щоб урятувати твої заощадження.

Проблема в тому, що ти не маєш жодного уявлення, ким він є насправді.

Пан знає твоє ім'я. Знає, у якому банку ти маєш рахунок. Може назвати населений пункт, де ти живеш, а іноді навіть частину номера банківського рахунку. Усе збігається, тому твій мозок починає виконувати доволі ризиковану операцію: перетворює знання кількох фактів на доказ надійності співрозмовника. Тим часом ім'я, прізвище чи номер телефону - це не таємничі заклинання, доступні виключно працівникам банків. Вони могли потрапити до сторонніх осіб із різних джерел. А номер телефону, який відображається на екрані? На жаль, він теж не завжди говорить правду. Технологія підміни номера, відома як спуфінг, дозволяє зробити так, що на екрані ти побачиш зовсім не те, звідки насправді надходить дзвінок.

Саме тому й з'явилася ця книжка. Не для того, щоб від завтра ти відповідав на кожен дзвінок словами: «Назвіть, будь ласка, дівоче прізвище голови правління банку та третю цифру розміру взуття директора відділення». Хоча, мушу визнати, це був би цікавий спосіб відлякувати телемаркетологів. Ідеться про дещо значно практичніше: навчитися розпізнавати ситуації, коли хтось намагається скористатися твоєю довірою, а також перевіряти особу співрозмовника, не дотримуючись інструкцій людини, яку ти саме й намагаєшся перевірити.

Адже саме тут ховається найбільший абсурд усієї ситуації. Незнайомець телефонує, стверджує, що працює в банку, а коли ти просиш підтвердити його особу, пропонує просто повірити йому на слово. Або може переключити тебе на свого керівника. Керівник, звісно, існує, принаймні в межах цієї розмови. Можливо, він сидить на сусідньому стільці, має такий самий телефон і щойно отримав підвищення до начальника відділу безпеки завдяки видатному вмінню змінювати тембр голосу.

Телефонне шахрайство не завжди починається з незграбної брехні. Часто воно нагадує професійно підготовлену процедуру. Співрозмовник може використовувати правильні терміни, знати основні банківські правила та чудово розуміти, яких повідомлень ти очікуєш від фінансової установи. Він навіть може застерігати тебе від шахраїв, що є особливо нахабним, але, на жаль, корисним для нього прийомом. Коли хтось каже, що захищає тебе від злочинців, цілком природно сприймати його як людину, яка стоїть на правильному боці. Однак сама заява про захист ще не означає, що тебе справді захищають. Пожежник у пластиковій касці

теж може кричати «Пожежа!», але перш ніж віддати йому ключі від квартири, варто перевірити, чи справді він приїхав пожежною машиною.

Найважливішим інструментом шахрая часто стає не технологія, а тиск. Ти чуєш, що гроші ось-ось зникнуть, діяти потрібно негайно, розмову не можна переривати, а консультація з будь-ким іншим може поставити під загрозу безпеку рахунку. Кожне наступне речення залишає дедалі менше простору для спокійного мислення. Тобі зовсім не обов'язково бути наївним, щоб відчути напруження. Достатньо мати заощадження, рахунки, які потрібно оплатити, і не надто захоплюватися перспективою, що хтось купить собі телевізор за твої гроші. Шахраєві не потрібно переконувати тебе в усьому одразу. Достатньо отримати згоду на перший, на вигляд цілком невинний крок, а потім використати твою залученість у подальшу розмову.

Можливо, ти думаєш, що ніколи не потрапив би на такий гачок. Це дуже приємне переконання. На жаль, шахрай не проводить іспит на інтелект. Він шукає момент, коли ти зайнятий, втомлений, наляканий або просто впевнений, що розмовляєш із потрібною людиною. Хтось може чудово знати правила безпеки й попри це припуститися помилки, коли на іншому кінці лінії чує тривожне попередження щодо власних грошей. Тому замість того, щоб плекати відчуття власної невразливості, краще виробити простий порядок дій, який працюватиме навіть тоді, коли твоя концентрація вирішила піти на обідню перерву.

У цій книжці ти навчишся відрізняти інформацію, яка лише звучить переконливо, від тієї, яка справді щось підтверджує. Побачиш, як розпізнавати типові спроби

психологічного тиску, чому знайомий номер на екрані не гарантує безпеки та яке значення мають прохання повідомити коди, паролі, встановити застосунок або здійснити переказ. Але насамперед ти познайомишся з принципом, який дозволяє повернути собі контроль над розмовою: саме ти обираєш незалежний канал зв'язку з банком, замість того щоб залишатися в каналі, який обрав для тебе незнайомець.

Уяви, що тобі повідомляють тривожну інформацію про підозрілу транзакцію. Замість того щоб вступати в дискусію, ти завершуєш дзвінок. Потім самостійно відкриваєш офіційний банківський застосунок або користуєшся номером, знайденим на справжньому сайті банку чи на платіжній картці. Зв'язуєшся з банком незалежно від попереднього співрозмовника й запитуєш, чи справді існує проблема, яка потребує втручання. Ти не набираєш номер, продиктований людиною, яка телефонувала, не натискаєш на надіслане посилання й не вважаєш повторний дзвінок від тієї самої особи підтвердженням її повноважень. Це не якась видовищна контррозвідувальна операція. Тобі не потрібні навушник у вусі, темні окуляри чи кодова назва «Операція Депозит». Потрібен лише принцип, який можна застосувати під тиском.

Звісно, реальні ситуації бувають складнішими за такий акуратний приклад. Що робити, коли співрозмовник знає подробиці твого рахунку? Коли стверджує, що завершення дзвінка означатиме втрату грошей? Коли наказує підтвердити операцію в застосунку, хоча хвилину тому запевняв, що намагається її заблокувати? А що, коли ти вже повідомив частину інформації або виконав якусь вказівку й лише тепер починаєш відчувати, що

щось не так? У такі моменти тобі потрібні не докори сумління, а зрозуміла послідовність дій. Не кожна помилка означає втрату коштів, але деякі ситуації вимагають негайного контакту з банком і захисту доступу до рахунку. Зволікання через страх осоромитися може обійтися дорожче, ніж сама помилка.

Ми також не вдаватимемо, що кожен дзвінок із банку є шахрайством. Банки справді зв'язуються зі своїми клієнтами, зокрема з питань безпеки. Отже, мета полягає не в тому, щоб перетворити здорову обережність на підозріливість до кожної людини з телефонною слухавкою. Ідеться про розмежування двох речей: вислухати інформацію та виконати вказівку. Ти можеш серйозно поставитися до попередження, не визнаючи автоматично особу того, хто його передає. Можеш залишатися ввічливим, не розкриваючи своїх даних. Можеш завершити розмову, не запитуючи дозволу. А головне - можеш самостійно перевірити ситуацію, навіть якщо співрозмовник переконує тебе, що це абсолютно неможливо.

Останнє особливо кумедне. Установа, якій ти довірив свої гроші, нібито забороняє тобі зв'язуватися з нею через офіційні канали. Це приблизно так само логічно, якби ресторан попереджав, що перевірка його адреси на власному сайті призведе до вибуху кухні. Якщо хтось наполегливо заважає тобі провести незалежну перевірку, тобі навіть не потрібно остаточно з'ясовувати, чи є ця людина шахраєм, щоб перестати виконувати її вказівки. Достатньо того, що ти не маєш підтвердження, з ким саме розмовляєш.

Я не обіцяю, що після прочитання цієї книжки жоден злочинець ніколи не зможе застати тебе зненацька.

Методи шахрайства змінюються, а навіть розсудливі люди можуть помилятися. Проте можна навчитися реагувати так, щоб один телефонний дзвінок не позбавляв тебе можливості самостійно ухвалювати рішення. Замість того щоб намагатися запам'ятати всі можливі сценарії, ти сформуєш звичку перевіряти джерело інформації, розпізнавати маніпуляції та зупиняти дії, наслідків яких не розумієш.

І коли наступного разу зателефонує пан із банку, який знає твоє ім'я, прізвище й, очевидно, має необмежений запас часу для порятунку твого майна, тобі не доведеться вгадувати, чи він герой, чи людина з надзвичайно гнучким ставленням до чужої власності. Ти подякуєш за інформацію, завершиш розмову й сам перевіриш усе там, де потрібно.

Пан може знати твоє ім'я. Але це не означає, що останнє слово обов'язково має залишитися за ним.

Розділ 1 - Добрий день, телефоную з банку. Принаймні я так стверджую

Найбільш тривожне в телефонному шахрайстві те, що його початок може бути зовсім нецікавим. Жодного зловісного сміху, драматичної музики чи голосу людини, яка з дитинства мріяла про кар'єру злочинця. Звичайний телефонний дзвінок, ввічливе привітання й речення, вимовлене тоном людини, яка щодня розв'язує подібні проблеми. Якби співрозмовника оцінювали виключно за культурою спілкування, чимало шахраїв отримали б чудову характеристику та пропозицію провести тренінг з обслуговування клієнтів. На жаль, гарні манери не є сертифікатом чесності, а голос, що звучить професійно, не доводить, що його власник працює в банку.

Уяви Марту, яка щойно повернулася з покупками. Вона намагається розібрати пакети, знайти місце для продуктів, які точно не планувала купувати, й водночас переконати домашніх, що йогурти потрібно класти в холодильник, а не вести з ними багатогодинні переговори. Саме тоді дзвонить телефон. Чоловік представляється Адамом Ковальським із відділу безпеки банку й повідомляє про спробу несанкціонованої транзакції. Він називає банк, ім'я Марти та останні цифри її номера телефону. Потім запитує, чи намагалася вона щойно здійснити переказ. Марта відповідає, що ні. Співрозмовник одразу заявляє, що саме цього й побоювався. Його тон стає серйознішим, але залишається ввічливим. Усе звучить настільки переконливо, що Марта відкладає покупки, забуваючи

навіть про морозиво, яке починає незворотне перетворення на солодкий суп.

У цій короткій сцені сталося дещо важливіше за просту передачу інформації. Співрозмовник заволодів увагою Марти. Ще мить тому вона сама вирішувала, як провести свій день. Тепер стороння людина визначає її пріоритети, описує загрозу й натякає, що лише співпраця з ним допоможе уникнути втрат. Саме тому фальшиві дзвінки з банку іноді виявляються ефективними. Шахраєві зовсім не обов'язково одразу просити гроші. Спочатку йому потрібно зайняти місце у твоїй голові, бажано те, яке зазвичай відведене для невідкладних справ.

Коли розмова виглядає саме так, як і повинна

Багато людей уявляють шахрая як людину, яка нервово говорить, плутає назви установ і в кожному другому реченні пропонує переказати гроші на рахунок свого двоюрідного брата. Такі співрозмовники теж трапляються, але будувати власну безпеку на очікуванні очевидних помилок ризиковано. Добре підготовлений злочинець уміє наслідувати манеру спілкування справжніх банківських консультантів. Використовує офіційні формулювання, називає свою посаду, може повідомити службовий ідентифікаційний номер і розмовляти мовою процедур. Іноді на тлі чути інші розмови, що нагадують роботу великого контакт-центру. Однак саме враження організованості ще не доводить, що дзвінок справді надходить із банку.

Варто зрозуміти різницю між інформацією, яку повідомляє співрозмовник, та інформацією, підтвердженою незалежно. Коли людина каже: «Мене звати Адам Ковальський, я старший спеціаліст із питань безпеки», ти дізнаєшся лише те, як вона хоче

представитися. Коли називає службовий номер, ти все одно маєш справу з інформацією з того самого джерела. Звісно, можна записати прізвище та ідентифікатор, але не варто сприймати їх як перепустку до довіри. Інакше достатньо було б купити елегантний блокнот, вивчити кілька банківських термінів і оголосити себе директором із безпеки всієї галактики.

Справжній консультант може знати дані клієнта, оскільки користується банківськими системами. Шахрай також може володіти частиною такої інформації, отриманої різними способами. Тому самого збігу прізвища, адреси чи основних деталей недостатньо. Важливіше те, чого співрозмовник від тебе очікує та чи дозволяє без перешкод підтвердити ситуацію через незалежний офіційний канал. Особливо тривожними є вимоги повідомити пароль, код авторизації, PIN-код, встановити невідоме програмне забезпечення або підтвердити операції, яких ти сам не ініціював. Такі вказівки вимагають негайно зупинитися, незалежно від того, наскільки переконливо описана загроза.

Справжній банк може телефонувати з питань безпеки. Проте це не означає, що кожну розмову потрібно продовжувати доти, доки людина, яка телефонує, не вирішить її завершити. Ти маєш право сказати, що самостійно зв’яжешся з установою. Не потрібно переконувати співрозмовника у правильності свого рішення чи докладно пояснювати, чому ти йому не довіряєш. Телефонна розмова - не судове засідання, а ти не зобов’язаний представляти докази, перш ніж покласти слухавку.

Перша пастка: сплутати ввічливість з обов’язком

Повернімося до Марти. Фальшивий консультант ставить їй наступні запитання. Спочатку прості, на які легко відповісти. Чи має вона рахунок у цьому банку? Чи користується мобільним застосунком? Чи здійснювала останнім часом переказ невідомому отримувачу? Кожна відповідь робить розмову природнішою. Марта відчуває, що бере участь у стандартній процедурі. Поступово в неї також виникає ледь помітне відчуття обов'язку співпрацювати, адже хтось витрачає власний час, щоб допомогти їй у небезпечній ситуації.

Так працює механізм поступового залучення. Співрозмовникові не потрібно починати з прохання, яке відразу викличе спротив. Спершу він може отримати низку відповідей, а потім перейти до дедалі вимогливіших вказівок. Звісно, те, що ти відповів на кілька нейтральних запитань, зовсім не означає, що згодом не можеш відмовити. Проблема виникає тоді, коли людина починає сприймати попередню співпрацю як зобов'язання продовжувати її. Якщо вже так багато сказала, завершити розмову здається їй неввічливим або нелогічним.

Цю ілюзію варто зруйнувати заздалегідь. Ти можеш перервати розмову після першого речення, після п'ятого запитання або через десять хвилин. Не існує правила, за яким час, витрачений на незнайомця, створює обов'язок повідомляти йому нову інформацію. Якщо під час розмови ти починаєш відчувати дискомфорт, цього вже достатньо, щоб зупинитися. Не потрібно чекати вимоги настільки підозрілої, що пролунає сирена, а телефон сам покаже напис «УВАГА, ШАХРАЙ».

На практиці допомагає одне заздалегідь підготовлене спокійне речення: «Дякую за інформацію. Я завершу розмову й самостійно зв'яжуся з банком через офіційний

канал». Воно не містить звинувачень, не провокує суперечки й чітко визначає наступну дію. Якщо співрозмовник почне протестувати, можна повторити своє рішення, а потім завершити дзвінок. Ти не зобов'язаний отримувати його схвалення. Зрештою, людина, яка справді дбає про безпеку твоїх грошей, не повинна очікувати, що ти відмовишся від розумної перевірки виключно заради того, щоб не образити її почуттів.

Друга пастка: знайомий номер на екрані

Телефон Марти показує номер, схожий на номер банку. Це ще більше зміцнює її переконання, що все гаразд. Адже важко запідозрити телефон у брехні. Пристрій коштував кілька тисяч злотих, уміє розпізнавати обличчя власника й прокладати маршрут на інший кінець Європи. Здавалося б, він повинен знати, хто телефонує. На жаль, технічні можливості смартфона не означають, що кожен елемент інформації про дзвінок був надійно перевірений.

Підміна телефонного номера, тобто спуфінг, може призвести до того, що на екрані отримувача з'явиться номер, відмінний від справжнього джерела дзвінка. Існують механізми, які обмежують подібні зловживання, проте не варто вважати, що номер на дисплеї завжди гарантує особу того, хто телефонує. Навіть збереження банківського номера в контактах не розв'язує проблему. Телефон може показати знайому назву, тому що розпізнає представлений номер, а не тому, що особисто перевірив документи про працевлаштування людини на іншому кінці лінії.

Варто розрізняти вхідний дзвінок і самостійне встановлення зв'язку. Коли хтось телефонує тобі, саме ця

людина ініціює спілкування й представляється. Коли ти сам набираєш номер, отриманий із надійного незалежного джерела, то повертаєш собі контроль над вибором установи, з якою намагаєшся зв'язатися. Це не чарівна гарантія розв'язання всіх проблем, але такий крок суттєво змінює ситуацію. Ти більше не покладаєшся виключно на слова незнайомця.

При цьому не слід користуватися номером, надісланим у SMS підозрілим співрозмовником, або посиланням, яке він щойно продиктував. Це було б приблизно те саме, що перевіряти чесність продавця сумнівних годинників, зателефонувавши його приятелю, рекомендованому як незалежний експерт з автентичності. Контактні дані мають походити з джерела, якому ти довіряєш незалежно від поточної розмови, наприклад з офіційного банківського застосунку, справжнього вебсайту, який ти відкрив самостійно, або документів, раніше отриманих від банку.

Розпізнавання загрози починається з правильного запитання

Ти не завжди знатимеш, чи є співрозмовник шахраєм. І зовсім не обов'язково з'ясувати це негайно. Правильна реакція не вимагає розгадати кримінальну загадку за тридцять секунд. Достатньо усвідомити, що особа на іншому кінці лінії не пройшла незалежної перевірки й водночас намагається впливати на твої фінансові рішення. Це вже достатня причина, щоб відкласти виконання її вказівок.

Багато людей зосереджуються на запитанні: «Чи звучить ця людина переконливо?». Значно корисніше запитати: «Що я можу безпечно зробити, не припускаючи, що ця людина говорить правду?». Перше

запитання змушує оцінювати голос, поведінку та деталі, які можуть бути заздалегідь підготовленою частиною шахрайства. Друге дозволяє обрати дію, незалежну від цих вражень. Можна записати інформацію про нібито підозрілу транзакцію, завершити дзвінок і перевірити все самостійно. Тобі не потрібна ані впевненість, що співрозмовник бреше, ані доказ, що він чесний.

Саме так чинить Марта, коли їй вдається повернути собі трохи спокою. Вона каже, що сама зателефонує до банку. Чоловік відповідає, що часу немає й кожна хвилина збільшує ризик втрати коштів. Марта відчуває тривогу, але не змінює рішення. Вона завершує розмову, відкриває офіційний банківський застосунок і користується доступною там можливістю зв'язку. Описує отриманий дзвінок і просить перевірити рахунок. Лише інформація, отримана під час незалежного контакту, стає підставою для подальших рішень.

У нашому прикладі з'ясовується, що банк не підтверджує описаної спроби переказу. Марті не обов'язково знати, ким був чоловік, який телефонував, і звідки він отримав її дані. Вона зробила те, що було потрібно: не передала конфіденційної інформації, не підтвердила жодної операції й не дозволила незнайомцеві визначати спосіб перевірки.

А морозиво? На жаль, банк не займається захистом заморожених продуктів. Кожна процедура має свої межі.

Чому здорового глузду не завжди достатньо

Легко сказати, що достатньо просто зберігати здоровий глузд. Значно важче пояснити, що саме це означає в момент, коли хтось повідомляє про загрозу грошам, які ти відкладав кілька років. Здоровий глузд - не

кнопка, натисканням якої можна миттєво вимкнути страх. Це радше набір правил, визначених заздалегідь, завдяки яким не доводиться щоразу ухвалювати всі рішення з нуля.

Тому варто ще до отримання підозрілого дзвінка знати, де знайти офіційні контактні дані банку та як виглядає безпечне спілкування з його працівниками. Можна перевірити в застосунку доступні канали допомоги, ознайомитися з попередженнями, які публікує твій банк, і з'ясувати, як потрібно реагувати на несанкціоновані транзакції. Така підготовка не є перебільшенням. Так само як знання шляху евакуації не означає, що ти щодня очікуєш пожежі, знання способу зв'язку з банком не вимагає переконання, ніби весь світ намагається захопити твій рахунок.

Важливо також не оцінювати власну безпеку лише крізь призму попереднього досвіду. Той факт, що протягом десяти років жоден підозрілий дзвінок не призвів до проблем, не доводить, що наступний теж буде нешкідливим. З іншого боку, отримання фальшивого дзвінка не означає автоматично, що твій рахунок уже захоплено. Потрібно розрізняти спробу шахрайства й реальне порушення безпеки. Паніка після кожного дзвінка з невідомого номера була б такою самою непрактичною, як і безумовна довіра кожному, хто представляється консультантом.

Добре підготовлений співрозмовник може звучати переконливо, а справжній працівник банку може мати невдалий день, говорити нерозбірливо або забути про вишукане привітання. Тому не варто будувати рішення на конкурсі телефонної харизми. Безпечна поведінка повинна працювати незалежно від того, чи має людина,

яка телефонує, оксамитовий голос радіоведучого, чи звучить як хтось, хто щойно випив третю каву й досі не може змиритися з понеділком.

Зрештою, мета не в тому, щоб перемогти шахрая в суперечці. Ти не мусиш доводити йому, що розгадав його наміри, або продовжувати розмову до моменту, коли він зізнається у своїй провині. Іноді найрозумнішим завершенням є звичайне відключення дзвінка. Без драматичної фінальної репліки, без промови й без ефектної розв'язки, гідної бойовика.

Твоїм грошам не потрібен видовищний герой. Їм потрібен власник, який знає, коли перестати слухати незнайомця.

Розділ 2 - Звідки він усе це знає? Анатомія довіри в кредит

Коли незнайомець вимовляє твоє ім’я, зазвичай це не справляє великого враження. Ім’я можна знайти на посилках, у повідомленнях, документах та інтернет-профілях. Але якщо людина, яка телефонує, додає прізвище, назву банку й кілька подробиць твого життя, ситуація починає виглядати інакше. Тобі здається, що ти розмовляєш із кимось, хто має особливий доступ до інформації. У голові виникає просте рівняння: якщо він знає подробиці, отже, є тим, за кого себе видає. Проблема в тому, що це рівняння ґрунтується на хибному припущенні, а хтось саме намагається виставити тобі рахунок за його використання.

Уяви Томаша, який відповідає на дзвінок під час перерви на роботі. Співрозмовниця представляється працівницею банку, називає його повне ім’я та прізвище, а потім згадує платіжну картку й підозрілу активність на рахунку. Томаш запитує, звідки вона має цю інформацію. Жінка спокійно відповідає, що бачить усе в системі. Навіть називає кілька цифр, які асоціюються в нього з банківським рахунком. Томаш перестає ставити запитання. Якщо працівниця бачить систему, значить, усе офіційно. Йому навіть не спало на думку, що слова «я бачу це в системі» можна вимовити й тоді, коли єдиною системою є відкрита електронна таблиця з даними.

Це не означає, що кожна людина, яка телефонує, має таку базу або що кожне розкрите ім’я походить із витоку інформації. Дані можуть потрапляти до сторонніх людей різними шляхами, а частина з них перебуває у