Ви не анонімні

Довіра, яку ви не обирали

Просто кажучи: за вашою електронною поштою будь-хто за кілька секунд може дізнатися, де у вас є акаунти, а іноді й ваше обличчя та ім'я. Це не збій: це інтернет, який працює як завжди. Питання не в тому, чи можуть вас побачити — можуть — а в тому, кому ви змушені довіряти. І є лише одне місце, де немає нікого посередині: розмова напряму, з одного пристрою на інший.

Достатньо електронної пошти. Не обов'язково вашої: будь-якої. Її вводять у кілька безкоштовних інструментів — легальних, публічних, доступних для тих, хто хоче їх шукати — і за кілька секунд з'являється список: у яких сервісах зареєстрована ця пошта, іноді фотографія профілю, іноді ім'я та прізвище, які власник вважав, що нікому не давав. Не потрібно бути техніком. Не зламується жоден пароль. Не скоюється жодного злочину. Вся ця інформація вже була там — опублікована, зареєстрована або злита — чекаючи, поки хтось спроможеться її зібрати.

Спокусливо сприймати це як збій: прогалину, необережність, щось, що хтось повинен виправити. Це не так. Це нормальна робота відкритого вебу. Щоразу, коли ви реєструєтесь у сервісі, заповнюєте форму, публікуєте відгук або з'являєтеся в чиємусь витоку даних, ви залишаєте слід. Жоден з цих слідів не є серйозним сам по собі. Проблема — якщо це взагалі проблема — виникає від їх об'єднання, а об'єднати їх просто.

Тут багато хто захищається розумною фразою: «мені нічого приховувати» або «я дбаю про свої акаунти». Перша плутає приховування з вибором; ми до цього повернемося. Друга ігнорує той факт, що більшу частину цього сліду залишили не ви: його залишив торговий реєстр, вебсайт, який зазнав витоку, знайомий, який завантажив фото з вами та позначив вас. Анонімність в інтернеті майже ніколи не є властивістю, якою ви володієте; це щонайбільше незрозумілість: тимчасовий факт того, що ще ніхто не спромігся подивитися.

Досі ми говорили про те, що одна людина може зробити за кілька секунд вручну. А тепер приберіть людину. Те, що роками захищало більшість із нас, було не анонімністю, а відсутністю інтересу: щоб вас знайти, хтось повинен захотіти подивитися, а ніхто не має часу дивитися на всіх. Цей останній бар'єр — зусилля подивитися — це саме те, чого не має машина. Автоматизована система може виконувати ту саму перевірку не проти однієї цілі, а проти цілого населення; не один раз, а безупинно; не через підозру, а за замовчуванням. Те, на що раніше у слідчого йшли години на кожну людину, тепер робиться з мільйонами одночасно, не вимагаючи ні від кого часу чи уваги. Не потрібно припускати, хто б хотів це зробити — компанія, група, держава — достатньо зрозуміти, що більше не потрібно обирати, на кого дивитися. Можна дивитися на всіх.

Ось чому питання «чи можуть вони мене знайти?» неправильне. Відповідь — так, і так буде все частіше. Корисне питання інше: кому і наскільки я змушений довіряти, щоб жити в мережі? Тому що це те, що ви насправді робите щодня, найчастіше не замислюючись. Ви довіряєте, що сервіс, де ви реєструєтесь, буде добре зберігати ваші дані. Ви довіряєте, що ваш оператор не прослуховуватиме ваші дзвінки. Ви довіряєте, що програма обміну повідомленнями, якою користуються всі — скажімо, WhatsApp — робить те, що обіцяє. Ви довіряєте серверу посередині, компанії, яка ним керує, країні, де він знаходиться, безкоштовному інструменту, який хтось розмістив у мережі. Кожна з цих ланок є рішенням про довіру.

Різниця в тому, що майже жодного з них ви не приймали свідомо: вони йшли в комплекті. Ці ланки, які прослизають між вами та іншою людиною, на жаргоні називаються довіреними посередниками; назва має менше значення, ніж ідея про те, що вони там є і що їх багато.

Є чесний спосіб перевірити все це: зробити це з собою. І вам не потрібно, щоб ми вам щось давали. Відкрийте браузер, напишіть три чи чотири слова — щось на кшталт «що інтернет знає про мою пошту» — і сама мережа покладе інструменти перед вами. Ця легкість вже є половиною відповіді: якщо ви знаходите їх за десять секунд, будь-хто може знайти те, що вони кажуть про вас.

Ми не пропонуємо вам наш список, і це навмисно. Якби ми його дали, вам довелося б нам довіряти: що ми обрали правильно, що ці сторінки залишатимуться надійними через п'ять років, що за жодною з них немає — сьогодні чи завтра — когось із поганими намірами. Ми не можемо обіцяти цього щодо сторінок, які ми не контролюємо, і ми вважаємо за краще не давати обіцянок, які не можемо виконати. Саме про це і є ця стаття. Але шукати це самостійно має ціну: пошукова система не відрізняє законне від пастки. Створити сторінку, яка імітує реальний інструмент, запитує вашу електронну пошту та зберігає її, дуже просто. Тому перед тим, як писати щось де-небудь, варто знати, як читати адресу.

Примітка — прочитайте адресу, перш ніж довіряти їй. Фальшива сторінка може скопіювати до останнього пікселя справжню; що вона майже ніколи не може підробити, так це свою адресу. Перш ніж щось писати на сайті, прочитайте адресний рядок, а не сторінку. Ім'я, яке вирішує все, знаходиться зліва від останньої частини (`.com`, `.org`, `.ua`): у `bezpechnyi-bank.dyvnyi-sait.top` справжній власник — не ваш банк, це `dyvnyi-sait.top`. Не довіряйте зміненим буквам (`0` замість `o`), зайвим словам, дефісам там, де ви їх не очікуєте, і дивним закінченням. Замок і `https` кажуть лише про те, що з'єднання зашифроване — а не про те, що власник чесний: у шахрая також є замок. А перші результати, позначені як «реклама», знаходяться там, тому що хтось заплатив, а не тому, що вони надійні. Кожна з цих перевірок, по суті, є тим самим питанням: наскільки я довіряю цій адресі і чому?

Дійшовши до цього моменту, варто описати протилежність всьому цьому: канал без посередників. Двоє людей самотньо розмовляють на вершині гори. Між ними немає ні листоноші, ні комутатора, ні сервера, ні компанії, ні країни. І все ж, зверніть увагу: довіра не зникає і там. Якщо ви розповідаєте секрет іншій людині, ви їй довіряєте. Цю довіру не можна забрати — та й не потрібно — бо вона єдина, яку ви дійсно обрали: ви знаєте, кому довіряєте і чому.

Чого немає на горі, так це всього іншого. Нікого посередині. І саме це, а не що інше, є єдиною моделлю, яку можна чесно відтворити в цифровому вигляді: прямий канал від одного пристрою до іншого, без нічого і нікого на шляху. Це не усуває довіри — це було б брехнею — це усуває посередників. Це залишає вас наодинці з єдиною неминучою довірою, тією, яку ви дійсно обрали. Це, до речі, архітектура, з якої ми пишемо ці сторінки; але аргумент тримається сам по собі, незалежно від того, хто його будує.

Тож ні, ви не анонімні і, мабуть, ніколи більше ними не будете. Але це ніколи не було тією битвою, яка мала значення. Неможливо жити — чи сидіти в інтернеті — нікому не довіряючи; той, хто намагається це зробити, не стає вільнішим, він лише стає самотнішим. Зрілість — це не недовіра, яка є іншою формою наївності. Це вимогливість: знати, кому ви віддаєте свою довіру, скільки, в обмін на що і — перш за все — знати, коли ви віддаєте її комусь, не прийнявши такого рішення.

Майже нічого в житті не є чорним або білим; майже все живе в сірій зоні між ними, і навчитися орієнтуватися в цьому сірому — це велика частина того, що означає мати розсудливість. Єдиним винятком є те, що добре зроблено на заводі: те, що за своїм дизайном не просить вас довіряти нікому іншому, крім людини, з якою ви вже вирішили поговорити. Решта — все інше — це питання того, скільки і кому.

Від редакції: коли в цих Cuadernos згадуються компанії або продукти, це робиться не для того, щоб когось звинуватити. Ті, хто їх створює, роблять роботу, якою користуються і яку цінують мільйони людей. Ми вказуємо на структурну проблему — модель, а не бренд. Бренди з'являються як приклад, тому що вони впізнавані для читача.

Джерела та додаткова література

- OSINT (розвідка на основі відкритих джерел) — збір інформації з уже загальнодоступних даних; це не втручання чи шпигунство.
- Reglamento (UE) 2016/679 (RGPD) — щодо обробки персональних даних, включаючи об'єднання даних, які окремо були загальнодоступними.
- Публічні реєстри (торгові, судові, реєстри нерухомості) — легітимне і багате джерело персональної інформації майже в усій Європі.
- У цій самій колекції: зошити про наскрізне шифрування та «Те, що підпис не може виправити» розвивають, з іншого кута зору, ту саму ідею.

← ПопереднійТе, що підпис не може виправити

Останні матеріали

- Рефлексія · 27 травня 2026 р. Те, що підпис не може виправити
- Аналіз · 26 травня 2026 р. Реальна vs уявна конфіденційність: питання, які варто собі поставити
- Аналіз · 25 травня 2026 р. Self-hosting як професійна практика

Візьміть цю статтю з собою куди завгодно.

↓ Markdown ↓ Звичайний текст ↓ PDF

Файл буде завантажено на ваш пристрій. Звідти ви можете зберегти його, імпортувати в Solo2 або поділитися ним де завгодно. Cuadernos не вирішує місце призначення за вас.

Сургучна печатка · SHA-256 10ef781ec000e67a04bfd606ef7d45b813076b42eb17953c0413206d1fc770ff

Cuadernos Lacre · Видання Menzuri Gestión S.L. ·
автор R.Eugenio · під редакцією команди Solo2.