Nie jesteś anonimowy

Zaufanie, którego nie wybrałeś

Mówiąc wprost: mając twój e-mail, każdy może w kilka sekund dowiedzieć się, gdzie masz konto, a czasem poznać twoją twarz i nazwisko. To nie jest błąd: to jest normalne działanie internetu. Pytanie nie brzmi, czy mogą cię zobaczyć —mogą—, ale komu jesteś zmuszony zaufać. I jest tylko jedno miejsce, w którym nie ma nikogo pośrodku: rozmowa bezpośrednio, z jednego urządzenia na drugie.

Wystarczy adres e-mail. Niekoniecznie twój: czyjkolwiek. Wpisuje się go w garść darmowych narzędzi —legalnych, publicznych, dostępnych dla każdego, kto chce szukać— i w kilka sekund pojawia się lista: w jakich usługach zarejestrowany jest ten e-mail, czasem zdjęcie profilowe, czasem imię i nazwisko, którego właściciel sądził, że nikomu nie podał. Nie trzeba być specjalistą technicznym. Żadne hasła nie są łamane. Nie popełnia się żadnego przestępstwa. Wszystkie te informacje już tam były —opublikowane, zarejestrowane lub ujawnione w wyciekach— i czekały, aż ktoś zada sobie trud ich zebrania.

Kuszące jest odczytanie tego jako błędu: naruszenia, zaniedbania, czegoś, co ktoś powinien naprawić. Tak nie jest. To normalne funkcjonowanie otwartej sieci. Za każdym razem, gdy rejestrujesz się w usłudze, wypełniasz formularz, publikujesz recenzję lub pojawiasz się w cudzym wycieku danych, zostawiasz ślad. Żaden z tych śladów sam w sobie nie jest poważny. Problem —jeśli w ogóle jest to problem— powstaje poprzez ich zebranie, a ich zebranie jest proste.

W tym miejscu wiele osób broni się rozsądnym zdaniem: «nie mam nic do ukrycia» lub «dbam o swoje konta». Pierwsze myli ukrywanie się z wybieraniem; wrócimy do tego. Drugie ignoruje fakt, że większość z tych śladów nie została pozostawiona przez ciebie: pozostawił je rejestr handlowy, strona internetowa, która padła ofiarą wycieku, znajomy, który przesłał zdjęcie z tobą i cię oznaczył. Anonimowość w internecie prawie nigdy nie jest twoją własnością; jest co najwyżej mrokiem: tymczasowym faktem, że nikt jeszcze nie pofatygował się, by spojrzeć.

Do tej pory mówiliśmy o tym, co jedna osoba może zrobić ręcznie w kilka sekund. Teraz usuń tę osobę. To, co przez lata chroniło większość z nas, nie było anonimowością, lecz brakiem zainteresowania: aby cię znaleźć, ktoś musi pofatygować się i poszukać, a nikt nie ma czasu, by patrzeć na wszystkich. Tej ostatniej bariery —wysiłku szukania— maszyna po prostu nie ma. Zautomatyzowany system może wykonać to samo krzyżowe sprawdzenie nie przeciwko jednemu celowi, lecz przeciwko całej populacji; nie raz, lecz bez przerwy; nie z powodu podejrzeń, lecz domyślnie. To, co dawniej zajmowało śledczemu godziny na jedną osobę, teraz odbywa się u milionów naraz, nie kosztując nikogo czasu ani uwagi. Nie trzeba zakładać, kto chciałby to zrobić —firma, grupa, państwo—; wystarczy zrozumieć, że nie trzeba już wybierać, kogo obserwować. Można obserwować wszystkich.

Dlatego «czy mogą mnie znaleźć?» to złe pytanie. Odpowiedź brzmi tak, i będzie tak w coraz większym stopniu. Przydatne pytanie brzmi inaczej: komu i w jakiej mierze jestem zmuszony zaufać, aby żyć w sieci? Ponieważ to właśnie robisz każdego dnia, niemal zawsze bez zastanowienia. Ufasz, że usługa, w której się rejestrujesz, będzie dobrze strzec twoich danych. Ufasz, że twój operator telekomunikacyjny nie będzie podsłuchiwał twoich rozmów. Ufasz, że aplikacja do komunikacji, z której wszyscy korzystają —powiedzmy WhatsApp— robi to, co deklaruje. Ufasz serwerowi znajdującemu się pośrodku, firmie, która nim zarządza, państwu, w którym się on znajduje, darmowemu narzędziu, które ktoś umieścił w sieci. Każde z tych ogniw to decyzja o zaufaniu. Różnica

polega na tym, że prawie żadnej z nich nie podjąłeś świadomie: były w pakiecie. Te ogniwa, które wciskają się między ciebie a drugą osobę, nazywane są w żargonie pośrednikami zaufania; nazwa ma mniejsze znaczenie niż to, że tam są i że jest ich wielu.

Jest jeden uczciwy sposób, by to wszystko sprawdzić: zrób to sam ze sobą. I nie potrzebujesz, żebyśmy cokolwiek ci dawali. Otwórz przeglądarkę, wpisz trzy lub cztery słowa —coś w stylu «co internet wie o moim e-mailu»— a sama sieć podsunie ci narzędzia. Ta łatwość jest już w połowie odpowiedzią: jeśli ty potrafisz je znaleźć w dziesięć sekund, to każdy może znaleźć to, co o tobie mówią.

Nie oferujemy naszej własnej listy, i robimy to celowo. Gdybyśmy ci ją podali, musiałbyś nam zaufać: że dobrze wybraliśmy, że te strony będą godne zaufania za pięć lat, że za żadną z nich —dziś czy jutro— nie stoi ktoś o złych intencjach. Nie możemy tego obiecać w przypadku stron, których nie kontrolujemy, i wolelibyśmy nie składać obietnic, których nie możemy dotrzymać. Właśnie o tym mówi ten artykuł. Ale samodzielne szukanie ma swoją cenę: wyszukiwarka nie odróżnia tego, co legalne, od pułapki. Stworzenie strony, która imituje prawdziwe narzędzie, prosi cię o e-mail i go zatrzymuje, jest trywialne. Zanim więc cokolwiek gdziekolwiek wpiszesz, powinieneś wiedzieć, jak czytać adresy.

Uwaga — przeczytaj adres przed obdarzeniem go zaufaniem. Fałszywa strona może skopiować prawdziwą co do piksela; tym, czego prawie nigdy nie może sfałszować, jest jej adres. Zanim cokolwiek wpiszesz na stronie, przeczytaj pasek adresu, a nie samą stronę. Nazwą, która się liczy, jest ta znajdująca się tuż po lewej stronie ostatniej części (`.com`, `.org`, `.pl`): w przypadku `bezpieczny-bank.dziwna-strona.top` prawdziwym właścicielem nie jest twój bank, tylko `dziwna-strona.top`. Uważaj na zmienione litery (`0` zamiast `o`), dodatkowe słowa, myślniki tam, gdzie się ich nie spodziewasz, i nietypowe końcówki. Kłódka i `https` mówią tylko, że połączenie jest szyfrowane —a nie, że właściciel jest uczciwy—: oszust też ma kłódkę. A pierwsze wyniki oznaczone jako «reklama» są tam, ponieważ ktoś zapłacił, a nie dlatego, że można im zaufać. Każde z tych sprawdzeń sprowadza się w istocie do tego samego pytania: jak bardzo ufam temu adresowi i dlaczego?

Będąc tutaj, warto opisać przeciwieństwo tego wszystkiego: kanał bez pośredników. Dwie osoby rozmawiające w odosobnieniu na szczycie góry. Nie ma między nimi listonosza, centrali telefonicznej, serwera, firmy ani państwa. A jednak, zwróć uwagę: zaufanie tam nie znika. Jeśli zdradzasz drugiej osobie tajemnicę, ufasz jej. Tego zaufania nie da się usunąć —i nie ma takiej potrzeby— ponieważ jest ono jedynym, które naprawdę wybrałeś: wiesz, komu ufasz i dlaczego.

Czego nie ma na górze, to całej reszty. Nikogo pośrodku. I ten model, żaden inny, jako jedyny może zostać uczciwie odtworzony w sferze cyfrowej: bezpośredni kanał z jednego urządzenia na drugie, bez niczego i nikogo po drodze. Nie eliminuje zaufania —to by było kłamstwo—; eliminuje pośredników. Zostawia cię z jedynym nieuniknionym zaufaniem, tym, które sam wybrałeś. To swoją drogą architektura, z której piszemy te strony; ale ten argument broni się sam, niezależnie od tego, kto go konstruuje.

Więc nie, nie jesteś anonimowy i prawdopodobnie już nigdy nie będziesz. Ale to nigdy nie była najważniejsza bitwa. Nie da się żyć —ani poruszać po sieci— bez zaufania komukolwiek; ten, kto próbuje to zrobić, wcale nie jest bardziej wolny, jest po prostu bardziej samotny. Dojrzałość nie polega na nieufności, która jest tylko inną formą naiwności. Polega na byciu wymagającym: na wiedzy, komu obdarzasz swoje zaufanie, jak dalece, w zamian za co i —przede wszystkim— na świadomości, kiedy obdarzasz nim kogoś bez podejmowania decyzji.

Prawie nic w życiu nie jest białe ani czarne; prawie wszystko tkwi w szarości pośrodku, a nauka poruszania się w tej szarości to znaczna część tego, co oznacza posiadanie dobrego osądu. Jedynym wyjątkiem jest to, co jest dobrze wykonane fabrycznie: to, co z założenia nie wymaga od ciebie zaufania do nikogo poza osobą, z którą już zdecydowałeś się porozmawiać. Reszta —cała reszta— to tylko kwestia tego, jak bardzo i w stosunku do kogo.

Nota redakcyjna: gdy te Cuadernos wymieniają firmy lub produkty, nie robią tego, by oskarżać. Ci, którzy je tworzą, wykonują pracę, z której korzystają i którą doceniają miliony ludzi. To, na co wskazujemy, ma charakter strukturalny — model, a nie marka. Marki pojawiają się jako przykłady, ponieważ są rozpoznawalne dla czytelnika.

Źródła i dodatkowa lektura

- OSINT (biały wywiad) — gromadzenie informacji na podstawie już dostępnych publicznie danych; to nie jest włamanie ani szpiegostwo.
- Reglamento (UE) 2016/679 (RGPD) — o przetwarzaniu danych osobowych, w tym agregacji danych, które oddzielnie były publiczne.
- Rejestry publiczne (handlowe, sądowe, majątkowe) — legalne i obfite źródło informacji osobistych w niemal całej Europie.
- W tej samej kolekcji: notatniki o szyfrowaniu end-to-end oraz «Czego podpis nie może naprawić» rozwijają z innej perspektywy tę samą ideę.

← PoprzedniCzego podpis nie może naprawić

Ostatnie lektury

- Refleksja · 27 maja 2026 Czego podpis nie może naprawić
- Analiza · 26 maja 2026 Prywatność rzeczywista vs pozorna: pytania, które warto sobie zadać
- Analiza · 25 maja 2026 Self-hosting jako praktyka zawodowa

Zabierz ten artykuł tam, gdzie go potrzebujesz.

↓ Markdown ↓ Zwykły tekst ↓ PDF

Plik zostanie pobrany na Twoje urządzenie. Stamtąd możesz go zapisać, zaimportować do Solo2 lub udostępnić w dowolnym miejscu. Cuadernos nie decyduje o miejscu docelowym za Ciebie.

Pieczęć lakowa · SHA-256 f2150bfced3de67d68f2845f661e327b79f2fea808ae2fb9db35b2b46620d294

Cuadernos Lacre · Publikacja Menzuri Gestión S.L. ·
napisana przez R.Eugenio · redagowana przez zespół Solo2.