Размисъл · 29 юни 2026 г.

← Предишна

Не сте анонимни

Доверието, което не сте избрали

Просто казано: с вашия имейл всеки може да разбере за секунди къде имате акаунт, а понякога лицето и името ви. Това не е грешка: така работи интернет откраи време. Въпросът не е дали могат да ви видят — могат —, а на кого сте принудени да се доверите. И има само едно място без никой по средата: директният разговор, от устройство на устройство.

Достатъчен е един имейл. Не е задължително вашият: всеки. Въвежда се в шепа безплатни инструменти — легални, публични, достъпни за всеки, който иска да ги потърси — и за броени секунди се появява списък: в кои услуги е регистриран този имейл, понякога профилна снимка, понякога име и фамилия, които собственикът му е смятал, че не е давал на никого. Не е нужно да сте технически експерт. Не се разбива никаква парола. Не се извършва никакво престъпление. Цялата тази информация вече е била там — публикувана, регистрирана или изтекла — чакайки някой да си направи труда да я събере.

Изкушаващо е да приемем това за грешка: пробив, недоглеждане, нещо, което някой трябва да поправи. Не е. Това е нормалното функциониране на отворената мрежа. Всеки път, когато се регистрирате в услуга, попълвате формуляр, публикувате отзив или се появявате в нечие чуждо изтичане на данни, оставяте следа. Нито една от тези следи не е сериозна сама по себе си. Проблемът — ако изобщо е проблем — възниква от събирането им, а събирането им е просто.

Тук много хора се защитават с разумна фраза: „аз нямам какво да крия“ или „аз внимавам за акаунтите си“. Първата бърка криенето с избирането; ще се върнем на това. Втората пренебрегва факта, че по-голямата част от тази следа не сте оставили вие: оставил я е търговският регистър, сайтът, от който са изтекли данни, познатият, който е качил снимка с вас и ви е отбелязал. Анонимността в интернет почти никога не е свойство, което притежавате; тя е, в най-добрия случай, неизвестност: временното обстоятелство, че никой все още не си е направил труда да потърси.

Дотук говорихме за това какво може да направи един човек за няколко секунди, ръчно. Сега премахнете човека. Това, което години наред предпазваше почти всички ни, не беше анонимността, а липсата на интерес: за да ви намери, някой трябва да си направи труда да потърси, а никой няма време да търси всеки. Тази последна бариера — усилието да се търси — е точно това, което една машина няма. Автоматизирана система може да направи същото съпоставяне не срещу една цел, а срещу цяло население; не веднъж, а без почивка; не по подозрение, а по подразбиране. Това, което преди отнемаше часове на един изследовател за всеки човек, сега се прави върху милиони едновременно, без да струва време или внимание на когото и да било. Няма нужда да предполагаме кой би искал да го направи — компания, група, държава —; достатъчно е да разберем, че вече не е нужно да се избира кой да бъде търсен. Може да се търсят всички.

Затова „могат ли да ме намерят?“ е грешният въпрос. Отговорът е да, и ще бъде все повече така. Полезният въпрос е друг: на кого и колко съм принуден да се доверя, за да живея свързан? Защото точно това правите всеки ден, почти винаги без да се замисляте. Доверявате се, че услугата, в която се регистрирате, ще пази добре данните ви. Доверявате се, че операторът ви няма да подслушва разговорите ви. Доверявате се, че приложението за съобщения, което всички използват — да речем WhatsApp —, прави това, което казва, че прави. Доверявате се на сървъра по средата, на компанията, която го

управлява, на страната, в която се намира, на безплатния инструмент, който някой е пуснал в мрежата. Всяко от тези звена е решение за доверие. Разликата е, че почти нито едно от тях не сте взели съзнателно: те са дошли в комплект. Тези звена, които се вмъкват между вас и другия човек, на жаргон се наричат посредници на доверие; името има по-малко значение от идеята, че са там и че са много.

Има един честен начин да проверите всичко това: направете го със себе си. И нямате нужда ние да ви даваме каквото и да било. Отворете браузъра си, напишете три или четири думи — нещо като „какво знае интернет за моя имейл“ — и самата мрежа ще постави инструментите пред вас. Тази лекота сама по себе си е половината отговор: ако вие ги намерите за десет секунди, всеки може да намери какво казват за вас.

Ние не ви предлагаме наш списък и това е умишлено. Ако ви го дадем, ще трябва да ни се доверите: че сме избрали добре, че тези страници ще бъдат надеждни след пет години, че зад никоя от тях няма — днес или утре — някой с лоши намерения. Не можем да обещаем това за страници, които не контролираме, и предпочитаме да не даваме обещания, които не можем да изпълним. Точно за това става дума в тази статия. Но ако ги търсите сами, има цена: търсачката не различава легитимното от капана. Създаването на страница, която имитира реален инструмент, иска имейла ви и го задържа, е тривиално. Затова, преди да пишете каквото и да било където и да било, е добре да знаете как да четете даден адрес.

Бележка — прочетете адреса, преди да му се доверите. Една фалшива страница може да копира до последния пиксел истинската; това, което почти никога не може да фалшифицира, е нейният адрес. Преди да въведете каквото и да било в даден сайт, прочетете адресната лента, не страницата. Името, което има значение, е това, залепено вляво от последната част (`.com`, `.org`, `.bg`): в `sigurna-banka.stranen-sait.top`, истинският собственик не е вашата банка, а `stranen-sait.top`. Не се доверявайте на променени букви (`0` вместо `o`), на излишни думи, на тирета, където не ги очаквате, и на странни окончания. Катинарът и `https` само казват, че връзката е криптирана — не че собственикът е честен —: измамникът също има катинар. А първите резултати, маркирани като „реклама“, са там, защото някой е платил, а не защото са надеждни. Всяка от тези проверки в същността си е същият въпрос: доколко се доверявам на този адрес и защо?

Стигайки дотук, е добре да опишем обратното на всичко това: канал без посредници. Двама души, сами на върха на една планина, разговарят. Няма пощальон, няма централа, няма сървър, няма компания, няма държава по средата. И все пак, забележете: дори там доверието не изчезва. Ако кажете тайна на другия човек, вие му се доверявате. Това доверие не може да бъде премахнато — а и няма нужда —, защото е единственото, което наистина сте избрали: знаете на кого се доверявате и защо.

Това, което го няма в планината, е всичко останало. Никой по средата. И това, и нищо друго, е единственият модел, който може да бъде възпроизведен честно в дигиталния свят: директен канал от едно устройство към друго, без нищо и никого по пътя. Той не премахва доверието — това би било лъжа —; той премахва посредниците. Оставя ви насаме с единственото неизбежно доверие, това, което вие сте избрали. Между другото, това е архитектурата, върху която градим тези страници; но аргументът е валиден сам по себе си, независимо кой го изгражда.

Така че не, не сте анонимни и вероятно никога повече няма да бъдете. Но това никога не е била битката, която има значение. Не може да се живее — нито да се сърфира — без да се доверявате на никого; този, който се опитва, не е по-свободен, просто е по-самотен. Зрялостта не е недоверие, което е друга форма на наивност. Тя означава да сте взискателни: да знаете на кого давате доверието си, колко, в замяна на какво и — преди всичко — да знаете кога го давате на някого, без да сте го решили.

Почти нищо в живота не е черно или бяло; почти всичко живее в сивото по средата, и да се научиш да се движиш в това сиво е голяма част от това какво означава да имаш критерий. Единственото изключение е това, което идва добре направено фабрично: това, което по дизайн не изисква от вас да се доверявате на никого, освен на човека, с когото вече сте решили да разговаряте. Останалото — всичко останало — е въпрос на това колко и на кого.

Редакционна бележка: Когато тези Cuadernos споменават компании или продукти, това не е с цел обвинение. Хората, които ги създават, вършат работа, която милиони използват и ценят. Това, което посочваме, е структурно — моделът, а не марката. Марките се появяват като пример, защото са тези, които читателят разпознава.

Източници и допълнително четиво

- OSINT (разузнаване от открити източници) — събиране на информация от вече публични данни; не е проникване или шпионаж.
- Reglamento (UE) 2016/679 (RGPD) — относно обработването на лични данни, включително агрегирането на данни, които поотделно са били публични.
- Публични регистри (търговски, съдебни, имотни) — легитимен и изобилен източник на лична информация в почти цяла Европа.
- В същата поредица: тетрадките за криптиране от край до край и „Какво един подпис не може да поправи“ развиват, от друг ъгъл, същата идея.

← ПредишнаКакво един подпис не може да поправи

Скорошни четива

- Размисъл · 27 май 2026 г. Какво един подпис не може да поправи
- Анализ · 26 май 2026 г. Реална срещу привидна поверителност: въпросите, които е добре да си зададете
- Анализ · 25 май 2026 г. Self-hosting като професионална практика

Вземете тази статия със себе си навсякъде, където ви е необходима.

↓ Markdown ↓ Обикновен текст ↓ PDF

Файлът ще бъде изтеглен на вашето устройство. Оттам можете да го запазите, импортирате в Solo2 или споделите където пожелаете. Cuadernos не решава дестинацията вместо вас.

Восъчен печат · SHA-256 69d2d19211bfd0fe68a4d96bd87beb0efa2e5bf8bcfeb82ad50f448ec698b209

Cuadernos Lacre · Публикация на Menzuri Gestión S.L. ·
написана от R.Eugenio · редактирана от екипа на Solo2.