Вы не анонимны

Доверие, которое вы не выбирали

Проще говоря: зная вашу электронную почту, любой может за считанные секунды выяснить, где у вас есть аккаунты, а иногда и ваше лицо, и имя. Это не ошибка: так всегда работал интернет. Вопрос не в том, могут ли вас увидеть — могут, — а в том, кому вы вынуждены доверять. И есть только одно место без посредников: говорить напрямую, от устройства к устройству.

Достаточно одной электронной почты. Не обязательно вашей: чьей угодно. Вы вводите её в несколько бесплатных инструментов — легальных, публичных, доступных всем желающим — и через пару секунд появляется список: в каких сервисах зарегистрирована эта почта, иногда фото профиля, иногда имя и фамилия, которые владелец, как он думал, никому не давал. Для этого не нужно быть техническим специалистом. Никакие пароли не взламываются. Никаких преступлений не совершается. Вся эта информация уже была там — опубликована, зарегистрирована или слита — и просто ждала, пока кто-нибудь не возьмется её собрать.

Соблазнительно считать это ошибкой: уязвимостью, недосмотром, чем-то, что кто-то должен исправить. Это не так. Это нормальная работа открытой сети. Каждый раз, когда вы регистрируетесь в сервисе, заполняете форму, публикуете отзыв или фигурируете в чужой утечке данных, вы оставляете след. Ни один из этих следов сам по себе не опасен. Проблема — если это вообще проблема — возникает, когда их собирают вместе, а сделать это очень просто.

Многие люди здесь защищаются разумной фразой: «мне нечего скрывать» или «я слежу за своими аккаунтами». Первая путает понятие «скрываться» с понятием «выбирать»; мы к этому еще вернемся. Вторая игнорирует тот факт, что бóльшую часть этого следа оставили не вы: его оставили торговый реестр, сайт, подвергшийся утечке, знакомый, который выложил фото с вами и отметил вас. Анонимность в интернете почти никогда не является свойством, которым вы обладаете; в лучшем случае это невидимость: временный факт того, что никто просто не удосужился пока поискать.

До сих пор мы говорили о том, что может сделать один человек за пару секунд вручную. А теперь уберите человека. То, что годами защищало почти всех нас, было не анонимностью, а отсутствием интереса: чтобы найти вас, кому-то нужно было потрудиться поискать, а ни у кого нет времени искать всех подряд. И именно этого последнего барьера — усилий на поиск — у машины нет. Автоматизированная система может выполнять такую же перекрестную проверку не против одной цели, а против целой популяции; не разово, а непрерывно; не из-за подозрений, а по умолчанию. То, на что раньше у исследователя уходили часы работы на каждого человека, теперь делается над миллионами одновременно, не требуя ничьего времени или внимания. Не нужно предполагать, кто хотел бы это сделать — компания, группа лиц или государство; достаточно понять, что больше не нужно выбирать, кого искать. Можно искать всех.

Поэтому вопрос «могут ли они меня найти?» в корне неверен. Ответ — да, и так будет всё чаще. Полезный вопрос звучит иначе: кому и насколько я вынужден доверять, чтобы жить в сети? Потому что это то, что вы делаете каждый день, почти всегда не задумываясь. Вы доверяете сервису, в котором регистрируетесь, что он будет надежно хранить ваши данные. Вы доверяете оператору связи, что он не будет прослушивать ваши звонки. Вы доверяете мессенджеру, которым пользуются все — скажем,

WhatsApp, — что он делает то, что заявляет. Вы доверяете серверу посередине, компании, которая им управляет, стране, в которой он находится, бесплатному инструменту, который кто-то выложил в сеть. Каждое из этих звеньев — это решение о доверии. Разница в том, что почти ни одно из них вы не принимали осознанно: они шли в комплекте. Эти звенья, которые вклиниваются между вами и другим человеком, на профессиональном жаргоне называют доверенными посредниками; название менее важно, чем тот факт, что они есть и их много.

Есть честный способ проверить всё это: сделайте это с самим собой. И вам не нужно, чтобы мы вам что-то давали. Откройте браузер, напишите три-четыре слова — что-то вроде «что интернет знает о моей почте» — и сама сеть покажет вам эти инструменты. Эта легкость сама по себе — половина ответа: если вы находите их за десять секунд, кто угодно может найти то, что они говорят о вас.

Мы сознательно не предлагаем вам свой список. Если бы мы его дали, вам пришлось бы доверять нам: что мы выбрали правильно, что эти сайты будут по-прежнему надежными через пять лет, что ни за одним из них нет — сегодня или завтра — кого-то с плохими намерениями. Мы не можем обещать этого за сайты, которые не контролируем, и предпочитаем не давать обещаний, которые не можем выполнить. Именно об этом и написана эта статья. Но за самостоятельный поиск приходится платить: поисковик не отличает легитимное от ловушки. Создать сайт, который имитирует реальный инструмент, просит вашу почту и сохраняет её, — проще простого. Поэтому, прежде чем что-то где-то писать, стоит научиться читать адреса.

Примечание — читайте адрес, прежде чем доверять ему. Поддельный сайт может скопировать до последнего пикселя настоящий; что он почти никогда не может подделать, так это свой адрес. Прежде чем что-то писать на сайте, посмотрите в адресную строку, а не на страницу. Главное имя — это то, которое примыкает слева к последней части (`.com`, `.org`, `.ru`): в `nadezhny-bank.stranny-sayt.top` реальным владельцем является не ваш банк, а `stranny-sayt.top`. Относитесь с подозрением к замененным буквам (`0` вместо `o`), лишним словам, дефисам там, где вы их не ждете, и странным окончаниям. Замок и `https` говорят лишь о том, что соединение зашифровано, а не о честности владельца: у мошенников тоже есть замок. А первые результаты с пометкой «реклама» находятся там потому, что за них кто-то заплатил, а не потому, что они надежны. Каждая из этих проверок по сути является одним и тем же вопросом: насколько я доверяю этому адресу и почему?

Дойдя до этого момента, стоит описать противоположность всего этого: канал без посредников. Два человека, одни на вершине горы, разговаривают. Между ними нет ни почтальона, ни телефонной станции, ни сервера, ни компании, ни страны. И тем не менее, заметьте: доверие никуда не исчезает и там. Если вы рассказываете другому человеку секрет, вы доверяете ему. Это доверие невозможно убрать — да и не нужно, — потому что это единственное доверие, которое вы действительно выбрали: вы знаете, кому доверяете и почему.

Чего нет на горе, так это всего остального. Никого посередине. И именно эта, а не какая-то другая, единственная модель может быть честно воспроизведена в цифровой среде: прямой канал от одного устройства к другому, без чего-либо и кого-либо на пути. Она не устраняет доверие — это было бы ложью; она устраняет посредников. Она оставляет вас наедине с единственным неизбежным доверием — тем, которое вы сами выбрали. Кстати, именно на этой архитектуре мы и пишем эти страницы; но аргумент говорит сам за себя, кто бы его ни построил.

Так что нет, вы не анонимны, и, скорее всего, больше никогда ими не будете. Но это никогда и не было главной битвой. Невозможно жить — или пользоваться интернетом, — никому не доверяя; тот, кто пытается это делать, не становится более свободным, он лишь становится более одиноким. Зрелость — это не недоверие, которое является лишь другой формой наивности. Это быть требовательным: знать, кому вы оказываете доверие, насколько, в обмен на что и — самое главное — знать, когда вы доверяете его кому-то, не принимая решения об этом.

В жизни почти нет ничего черного или белого; почти всё обитает в серой зоне посередине, и умение ориентироваться в этой серости — это большая часть того, что означает иметь здравый смысл.

Единственным исключением является то, что изначально сделано правильно: то, что по своему устройству не требует от вас доверять никому, кроме человека, с которым вы уже решили поговорить. Всё остальное — абсолютно всё — это вопрос о том, насколько и кому.

От редакции: когда в этих Cuadernos упоминаются компании или продукты, это делается не для того, чтобы кого-то обвинить. Те, кто их создает, делают работу, которой пользуются и которую ценят миллионы людей. Мы указываем на структурную проблему — модель, а не бренд. Бренды появляются в качестве примера, потому что они узнаваемы для читателя.

Источники и дополнительная литература

- OSINT (разведка по открытым источникам) — сбор информации из уже публичных данных; это не вторжение и не шпионаж.
- Reglamento (UE) 2016/679 (RGPD) — о защите персональных данных, включая агрегацию данных, которые по отдельности являлись публичными.
- Публичные реестры (торговые, судебные, имущественные) — законный и обширный источник личной информации почти по всей Европе.
- В этой же серии: тетради о сквозном шифровании и «Чего не может исправить подпись» развивают ту же идею, но под другим углом.

← ПредыдущийТо, что подпись не может исправить

Недавние материалы

- Размышления · 27 мая 2026 г. То, что подпись не может исправить
- Анализ · 26 мая 2026 г. Реальная vs мнимая конфиденциальность: вопросы, которые стоит себе задать
- Анализ · 25 мая 2026 г. Self-hosting как профессиональная практика

Возьмите эту статью с собой туда, где она вам понадобится.

↓ Markdown ↓ Простой текст ↓ PDF

Файл будет загружен на ваше устройство. Оттуда вы можете сохранить его, импортировать в Solo2 или поделиться им где угодно. Cuadernos не решает место назначения за вас.

Сургучная печать · SHA-256 06eb0e335a67f549165598a5892771431688feeacf222c345d1b39bf239f1330

Cuadernos Lacre · Издание Menzuri Gestión S.L. ·
текст R.Eugenio · под редакцией команды Solo2.