

شما ناشناس نیستید

اعتمادی که انتخاب نکردید

به زبان ساده: با ایمیل شما، هر کسی در چند ثانیه متوجه می‌شود کجا حساب دارید، و گاهی چهره و نامتان را می‌یابد. این یک نقص نیست: این عملکرد معمول اینترنت است. سؤال این نیست که آیا می‌توانند شما را ببینند — می‌توانند —، بلکه این است که مجبورید به چه کسی اعتماد کنید. و تنها یک جا وجود دارد که هیچ‌کس در میان نیست: گفتگوی مستقیم، از یک دستگاه به دستگاه دیگر.

یک ایمیل کافی است. لزوماً ایمیل شما نه: هر ایمیلی. در مشتی از ابزارهای رایگان وارد می‌شود — قانونی، عمومی، در دسترس هر کسی که بخواهد جستجو کند — و در عرض چند ثانیه لیستی ظاهر می‌شود: آن ایمیل در چه سرویس‌هایی ثبت شده است، گاهی یک عکس پروفایل، گاهی نام و نام خانوادگی که صاحبش فکر می‌کرد به کسی نداده است. نیازی به تخصص فنی نیست. هیچ رمز عبوری شکسته نمی‌شود. هیچ جرمی رخ نمی‌دهد. تمام آن اطلاعات از قبل آنجا بود — منتشر، ثبت، یا فاش شده — و منتظر بود تا کسی زحمت کنار هم گذاشتن آن‌ها را بکشد.

وسوسه‌انگیز است که این را به عنوان یک نقص در نظر بگیریم: یک شکاف، یک بی‌دقتی، چیزی که کسی باید آن را برطرف کند. این‌طور نیست. این عملکرد عادی وب باز است. هر بار که در سرویسی ثبت‌نام می‌کنید، فرمی را پر می‌کنید، نظری منتشر می‌کنید یا در افشای اطلاعات جای دیگری ظاهر می‌شوید، ردی از خود به جا می‌گذارید. هیچ‌کدام از این ردپاها به تنهایی خطرناک نیستند. مشکل — اگر مشکلی باشد — از کنار هم قرار دادن آن‌ها ناشی می‌شود، و کنار هم قرار دادن آن‌ها ساده است.

در اینجا بسیاری از افراد با یک جمله منطقی از خود دفاع می‌کنند: «من چیزی برای پنهان کردن ندارم»، یا «من مراقب حساب‌هایم هستم». اولی پنهان شدن را با حق انتخاب اشتباه می‌گیرد؛ به آن بازخواهیم گشت. دومی نادیده می‌گیرد که بیشتر این ردپاها را شما به جا نگذاشته‌اید: اداره ثبت شرکت‌ها، سایتی که دچار نشت اطلاعات شده، آشنایی که عکسی با شما آپلود کرده و شما را تگ کرده است. ناشناس بودن در اینترنت تقریباً هرگز دارایی شما نیست؛ حداکثر، تاریکی است: این واقعیت موقت که هنوز کسی زحمت نگاه کردن را به خود نداده است.

تا اینجا درباره کاری صحبت کردیم که یک فرد می‌تواند در چند ثانیه، به صورت دستی انجام دهد. حالا آن فرد را حذف کنید. چیزی که سال‌ها بیشتر ما را محافظت کرده، ناشناس بودن نبوده، بلکه بی‌توجهی بوده است: برای پیدا کردن شما، کسی باید زحمت نگاه کردن را بکشد، و هیچ‌کس وقت ندارد به همه نگاه کند. آن آخرین سد — زحمت نگاه کردن — دقیقاً همان چیزی است که یک ماشین ندارد. یک سیستم خودکار می‌تواند همان تطبیق را نه علیه یک هدف، بلکه علیه کل یک جمعیت انجام دهد؛ نه یک بار، بلکه بی‌وقفه؛ نه به دلیل سوءظن، بلکه به صورت پیش‌فرض. کاری که پیش از این برای یک محقق روی هر شخص ساعت‌ها طول می‌کشید، حالا هم‌زمان روی میلیون‌ها نفر انجام می‌شود، بدون اینکه وقت یا توجهی از کسی بگیرد. نیازی نیست حدس بزنیم چه کسی می‌خواهد این کار را بکند — یک شرکت، یک گروه، یک دولت —؛ کافی است درک کنیم که دیگر نیازی به انتخاب این نیست که به چه کسی نگاه کنیم. می‌توان به همه نگاه کرد.

به همین دلیل، «آیا می‌توانند مرا پیدا کنند؟» سؤال اشتباهی است. پاسخ بله است، و روز به روز بیشتر بله خواهد بود. سؤال مفید چیز دیگری است: برای زندگی متصل به شبکه، مجبورم به چه کسی و چقدر اعتماد کنم؟ زیرا این کاری است که هر روز، اغلب بدون فکر کردن، انجام می‌دهید. اعتماد می‌کنید که سرویسی که در آن ثبت‌نام می‌کنید اطلاعاتتان را خوب نگه می‌دارد. اعتماد می‌کنید که اپراتور تلفن شما به تماس‌هایتان گوش نمی‌دهد. اعتماد می‌کنید که برنامه پیام‌رسانی که همه استفاده می‌کنند — مثلاً WhatsApp — همان کاری را می‌کند که می‌گوید. به

سرور واسط، شرکتی که آن را اداره می‌کند، کشوری که در آن است، ابزار رایگانی که کسی در شبکه قرار داده اعتماد می‌کنید. هر یک از این حلقه‌ها، یک تصمیم اعتماد است. تفاوت در این است که تقریباً هیچ‌کدام را آگاهانه نگرفته‌اید؛ این‌ها همراه سیستم بوده‌اند. در اصطلاح، به این حلقه‌هایی که بین شما و شخص دیگر قرار می‌گیرند، واسطه‌های اعتماد می‌گویند؛ نام آن‌ها کمتر از این واقعیت اهمیت دارد که آن‌ها آنجا هستند و تعدادشان زیاد است.

یک راه صادقانه برای بررسی همه این‌ها وجود دارد: خودتان آن را امتحان کنید. و نیازی نیست ما چیزی به شما بدهیم. مرورگر خود را باز کنید، سه یا چهار کلمه تایپ کنید — چیزی مانند «اینترنت درباره ایمیل من چه می‌داند» — و خود وب ابزارها را پیش روی شما قرار خواهد داد. همین سهولت به تنهایی نیمی از پاسخ است: اگر شما در ده ثانیه آن‌ها را پیدا می‌کنید، هر کسی می‌تواند آنچه را که درباره شما می‌گویند پیدا کند.

ما فهرستی از سوی خودمان به شما ارائه نمی‌دهیم، و این عمدی است. اگر این کار را می‌کردیم، باید به ما اعتماد می‌کردید: به اینکه خوب انتخاب کرده‌ایم، به اینکه آن سایت‌ها پنج سال دیگر هم قابل اعتماد خواهند بود، به اینکه در پشت هیچ‌کدام از آن‌ها — امروز یا فردا — فردی با نیت بد وجود ندارد. ما نمی‌توانیم چنین قولی در مورد سایت‌هایی بدهیم که کنترلی روی آن‌ها نداریم، و ترجیح می‌دهیم قولی ندهیم که نمی‌توانیم به آن عمل کنیم. این دقیقاً موضوع همین مقاله است. اما این که خودتان جستجو کنید هزینه‌ای دارد: موتور جستجو بین سایت مشروع و تله تفاوتی قائل نمی‌شود. راه‌اندازی سایتی که ابزاری واقعی را تقلید می‌کند، ایمیل شما را می‌خواهد و آن را نگه می‌دارد، بسیار آسان است. بنابراین، قبل از نوشتن هر چیزی در هر جایی، بهتر است بدانید چگونه یک آدرس را بخوانید.

نکته — قبل از اعتماد به یک آدرس، آن را بخوانید. یک صفحه جعلی می‌تواند یک صفحه واقعی را تا آخرین پیکسل کپی کند؛ آنچه تقریباً هرگز نمی‌تواند جعل کند، آدرس آن است. قبل از اینکه چیزی در یک سایت بنویسید، نوار آدرس را بخوانید، نه صفحه را. نامی که تعیین‌کننده است، همان است که در سمت چپ قسمت آخر (.org, .com, .ir) چسبیده است: در bank-amn.site-ajib.top، مالک واقعی بانک شما نیست، site-ajib.top است. به حروفی که تغییر کرده‌اند (یک 0 به جای o)، کلمات اضافی، خط تیره‌هایی در جاهای غیرمنتظره و پایان‌های عجیب بی‌اعتماد باشید. قفل و https فقط می‌گویند که اتصال رمزگذاری شده است — نه اینکه مالک صادق است —: یک کلاهبردار نیز قفل دارد. و اولین نتایجی که با علامت «آگهی» مشخص شده‌اند به این دلیل آنجا هستند که کسی پول پرداخت کرده، نه به این دلیل که قابل اعتمادند. هر یک از این بررسی‌ها، در اصل، همان سؤال است: چقدر به این آدرس اعتماد دارم و چرا؟

در این مرحله، توصیف نقطه مقابل همه این‌ها مفید است: یک کانال بدون واسطه. دو نفر، تنها در بالای یک کوه، در حال صحبت. هیچ پستی، مرکز تماس، سرور، شرکت یا کشوری در میان نیست. و با این حال، دقت کنید: اعتماد در آنجا نیز ناپدید نمی‌شود. اگر رازی را به شخص مقابل بگویید، به او اعتماد می‌کنید. این اعتماد را نمی‌توان حذف کرد — و نیازی هم نیست — زیرا این تنها اعتمادی است که واقعاً انتخاب کرده‌اید: می‌دانید به چه کسی اعتماد می‌کنید و چرا.

آنچه در کوهستان وجود ندارد، بقیه چیزهاست. هیچ‌کس در میان نیست. و این تنها مدلی است که می‌تواند به طور صادقانه در دنیای دیجیتال بازتولید شود: یک کانال مستقیم از یک دستگاه به دستگاه دیگر، بدون هیچ چیز و هیچ‌کس در طول مسیر. این مدل اعتماد را از بین نمی‌برد — گفتن این حرف دروغ است؛ واسطه‌ها را از بین می‌برد. شما را تنها با اعتمادی ناگزیر رها می‌کند، اعتمادی که خودتان انتخاب کردید. اتفاقاً، این همان معماری است که از طریق آن این صفحات را می‌نویسیم؛ اما این استدلال، فارغ از اینکه چه کسی آن را ساخته، به خودی خود پابرجاست.

بنابراین نه، شما ناشناس نیستید، و احتمالاً دیگر هم نخواهید بود. اما این هرگز نبردی نبود که اهمیت داشت. نمی‌توان زندگی کرد — یا ویرگردی کرد — بدون اینکه به کسی اعتماد کرد؛ کسی که تلاش می‌کند چنین کند آزادتر نیست، فقط نتاثر است. بلوغ، بی‌اعتمادی نیست، که آن هم شکل دیگری از ساده‌لوحی است. بلوغ یعنی سخت‌گیر بودن: دانستن اینکه به چه کسی، چقدر و در ازای چه چیزی اعتماد می‌کنید و — از همه مهم‌تر — دانستن اینکه چه زمانی بدون اینکه خودتان تصمیم گرفته باشید، به کسی اعتماد می‌کنید.

تقریباً هیچ چیز در زندگی سیاه یا سفید نیست؛ تقریباً همه چیز در ناحیه خاکستری میانه زندگی می‌کند، و یادگیری حرکت در این ناحیه خاکستری، بخش بزرگی از معنای داشتن قدرت تشخیص است. تنها استثنا، چیزی است که از کارخانه خوب ساخته شده باشد: چیزی که از روی طراحی، از شما نمی‌خواهد به هیچ‌کس جز شخصی که تصمیم گرفته‌اید با او صحبت کنید، اعتماد کنید. بقیه چیزها — تمام بقیه چیزها — مسئله «چقدر» و «به چه کسی» است.

یادداشت تحریریه: وقتی این Cuadernos نام شرکت‌ها یا محصولات را می‌برد، برای متهم کردن نیست. کسانی که آن‌ها را می‌سازند کارهایی انجام می‌دهند که میلیون‌ها نفر از آن استفاده کرده و قدردانی می‌کنند. آنچه ما به آن اشاره می‌کنیم ساختاری است — مدل، نه نام تجاری. نام‌های تجاری به عنوان مثال ذکر می‌شوند چون همان‌هایی هستند که خواننده می‌شناسد.

منابع و مطالعه بیشتر

- OSINT (هوش منابع باز) — جمع‌آوری اطلاعات از داده‌هایی که از قبل عمومی هستند؛ این نفوذ یا جاسوسی نیست.
- Reglamento (UE) 2016/679 (RGPD) — درباره پردازش داده‌های شخصی، از جمله جمع‌آوری داده‌هایی که به صورت جداگانه عمومی بوده‌اند.
- ثبت‌های عمومی (شرکت‌ها، قضایی، املاک) — منبع مشروع و فراوان اطلاعات شخصی در تقریباً سراسر اروپا.
- در همین مجموعه: دفترچه‌های مربوط به رمزگذاری سرتاسری و «آنچه یک امضا نمی‌تواند حل کند»، همین ایده را از زاویه‌ای دیگر بسط می‌دهند.

← [السابق آنچه یک امضا نمی‌تواند اصلاح کند](#)

قراءات حدیثه

- [تامل ۲۷۰ مة ۲۰۲۶ آنچه یک امضا نمی‌تواند اصلاح کند](#)
- [تحلیل ۲۶۰ مة ۲۰۲۶ حریم خصوصی واقعی در مقابل ظاهری: سؤالاتی که باید از خود پرسید](#)
- [تحلیل ۲۵۰ مة ۲۰۲۶ Self-hosting به عنوان یک فعالیت حرفه‌ای](#)

این مقاله را هر کجا که نیاز دارید همراه خود ببرید.

↓ [مارک‌داون](#) ↓ [متن ساده](#) ↓ [PDF](#)

فایل در دستگاه شما دانلود خواهد شد. از آنجا می‌توانید آن را ذخیره کنید، به Solo2 وارد کنید یا در هر کجا که می‌خواهید به اشتراک بگذارید. Cuadernos مقصد را برای شما تعیین نمی‌کند.

ختم شمعی · SHA-256 bfcca32be8ef645bde492290223175afe2c6979fa11a17efdb9099519db5a9dd

[قابلیت‌ها](#) [تازه‌ها](#) [بلاگ](#) [راهنما](#) [درباره](#) [تماس](#)
[شفافیت](#) [تأیید](#) [حریم خصوصی](#) [شرایط](#) [کوکی‌ها](#)

• Cuadernos Lacre · نشریه من [Menzuri Gestión S.L.](#) · کتبها R.Eugenio · حررها فریق [Solo2](#).

این وب‌سایت از کوکی استفاده نمی‌کند. هر چیزی که مرورگر شما بارگذاری می‌کند توسط ما نوشته یا نظارت شده و روی سرورهای اروپایی ما میزبانی می‌شود: شمارنده بازدید ناشناس (Umami، میزبانی شده به صورت خودکار) و حداقل جاوا اسکریپت لازم برای انتخابگر زبان و ترجیح تم روشن/تیره شما، که روی دستگاه خودتان ذخیره می‌شود. بدون منابع شرکت‌های خارجی، بدون ردیاب، بدون پروفایل، بدون اشتراک‌گذاری داده. اگر می‌خواهید ما را دنبال کنید: [RSS](#).