

VPN thực sự là gì

Nó thay đổi ai có thể nhìn thấy bạn, chứ không phải có ai nhìn thấy được hay không.

Nói một cách dễ hiểu: VPN khiến nhà mạng internet hoặc Wi-Fi sân bay không còn thấy bạn kết nối đến đâu. Thông tin đó không biến mất mà được chuyển sang công ty VPN, nơi giờ đây nhìn thấy nó. Những gì vốn đã được mã hóa, như email hay ngân hàng, thì trước đó cũng đã được mã hóa rồi. Nó phục vụ cho một vài mục đích cụ thể và thường được quảng cáo như thể làm được nhiều hơn thế rất nhiều.

Trong nhiều năm, tôi nghe nói về VPN và không mấy bận tâm, cũng giống như với phần mềm diệt virus: tôi không dùng phần mềm diệt virus, hoặc hầu như không bao giờ. Tôi có bản sao lưu mọi thứ ở ba nơi, theo thời gian thực, và rất cẩn thận với những gì mình tải xuống, các liên kết mình nhấp vào và các trang web mình truy cập. Đó không phải là sự an toàn tuyệt đối một trăm phần trăm, nhưng là cách hiệu quả với tôi. Một ngày nọ, tôi thấy ưu đãi VPN chỉ hơn hai euro một tháng và đã mua vì tò mò. Nó hoạt động tốt, nhưng chẳng giúp ích được gì nhiều cho tôi: chẳng hạn như thử một dịch vụ mà khi đó chỉ mở ở Hoa Kỳ. Tôi có cảm thấy an toàn hơn không? Không. Nếu họ lại đưa ra mức giá đó, có thể tôi sẽ gia hạn; nếu không thì thôi. Đó chỉ là trải nghiệm cá nhân của tôi, chẳng chứng minh được điều gì. Vì vậy, tôi tự hỏi chính xác thì VPN làm được những gì. Và đây là cách tôi hiểu về nó.

Hãy tưởng tượng bạn bỏ một lá thư vào thùng thư với địa chỉ người nhận hiển thị rõ ràng. Người đưa thư biết bạn gửi thư cho ai, dù không thể đọc được nội dung nếu thư được niêm phong. Người đưa thư đó chính là nhà mạng internet của bạn. VPN đặt lá thư của bạn vào trong một chiếc phong bì khác, gửi đến một bên trung gian mở phong bì ra và chuyển tiếp đi. Người đưa thư thông thường không còn thấy địa chỉ thực tế nữa. Họ chỉ thấy bạn đang gửi thư cho bên trung gian đó.

Bất kỳ ai kiểm soát mạng mà bạn kết nối, chẳng hạn như Wi-Fi ở sân bay, sẽ không còn thấy bạn truy cập vào đâu. Nhưng bên trung gian giờ đây lại thấy những gì nhà mạng từng thấy, và đôi khi còn nhiều hơn thế, vì toàn bộ lưu lượng của bạn đều đi qua họ. Sự giám sát không hề biến mất: nó chỉ đổi chủ. Tên gọi của nó cũng xuất phát từ đó.

Hơn nữa, hầu hết mọi việc bạn làm ngày nay, như mở email hay đăng nhập ngân hàng, vốn đã được mã hóa trên đường đến máy chủ đích nhờ vào biểu tượng ổ khóa của trình duyệt. Điều đó diễn ra dù có hay không có VPN. VPN chỉ bổ sung thêm sự bảo vệ ở chặng đầu tiên, cho đến máy chủ của chính nó. Từ đó trở đi, lộ trình vẫn như thường lệ.

Đó là lý do tại sao có những điều nó không thể hứa hẹn với bạn, mặc dù đôi khi người ta bán nó theo cách đó. Nếu bạn đã đăng nhập vào email hoặc tài khoản ngân hàng, dịch vụ đó biết bạn là ai, có VPN hay không. Nó cũng không đảm bảo rằng không ai nhìn vào lưu lượng truy cập của bạn: nó chỉ thay đổi ai là người nhìn. Việc công ty tuyên bố «không lưu nhật ký» chỉ là một lời hứa, cũng giống như khi một nền tảng lớn nói «tin nhắn của bạn được mã hóa, chúng tôi không đọc». Một cuộc kiểm toán có thể chứng thực điều đó tại một thời điểm nhất định, nhưng đó vẫn là điều bạn phải đặt niềm tin vào, chứ không phải một thiết kế không thể vi phạm về mặt bản chất.

Và nội dung của một cuộc trò chuyện vẫn giữ nguyên. Nếu ứng dụng nhắn tin của bạn đã mã hóa đầu cuối, VPN chẳng đóng góp thêm gì. Nếu không, VPN cũng không thể khắc phục được: nó chỉ bảo vệ đường đi của tin nhắn, chứ không bảo vệ những gì ứng dụng hoặc máy chủ của nó làm với tin nhắn khi tới nơi.

Không điều gì trong số này khiến nó trở nên vô dụng. Việc che giấu điểm đến kết nối trước Wi-Fi công cộng, trước một nhà mạng muốn bán lịch sử duyệt web hoặc một quốc gia chặn dịch vụ nào đó là một nhiệm vụ thực tế và nó làm rất tốt. Chỉ có điều, hoạt động tiếp thị thường hứa hẹn nhiều hơn những gì lớp bảo vệ này có thể mang lại.

Câu hỏi cần đặt ra, với VPN hay bất kỳ dịch vụ nào hứa hẹn bảo vệ bạn, không phải là «nó có được mã hóa không?». Có lẽ là có, ít nhất là một chặng. Câu hỏi thực sự là: tôi đang đặt niềm tin mà mình vừa tước bỏ từ kẻ khác vào tay ai? Và tôi còn lại gì nếu niềm tin đó hóa ra không có cơ sở?

VPN, khi làm tốt nhiệm vụ của mình, chỉ thay đổi bên trung gian trong kết nối của bạn. Một ứng dụng như Solo2, nơi tin nhắn không đi qua bất kỳ máy chủ nào, sẽ loại bỏ hoàn toàn bên trung gian khỏi cuộc trò chuyện. Chúng không cạnh tranh nhau: chúng giải quyết những vấn đề khác nhau.

Nhầm lẫn giữa hai điều này là một cách rất phổ biến khiến người ta tin rằng mình được bảo vệ nhiều hơn thực tế.

Ghi chú của biên tập viên: khi các Cuadernos này nêu tên các công ty hoặc sản phẩm, đó không phải là để cáo buộc. Những người tạo ra chúng làm những công việc mà hàng triệu người sử dụng và trân trọng. Những gì chúng tôi chỉ ra mang tính cấu trúc — về mô hình, không phải thương hiệu. Các thương hiệu xuất hiện như một ví dụ vì đó là những gì người đọc nhận ra.

Nguồn tham khảo và đọc thêm

- Giao thức HTTPS và mã hóa truyền tải là các tiêu chuẩn mở, được IETF tài liệu hóa công khai.
- Trong cùng bộ sưu tập này: «Khi không có ai ở giữa» và «Bạn không ẩn danh» phân tích, từ những góc nhìn khác, chính ranh giới giữa cấu trúc kỹ thuật và lời hứa.

[← Trước Bạn không ẩn danh](#)

Các bài đọc gần đây

- [Suy ngẫm · 29 tháng 6, 2026 Bạn không ẩn danh](#)
- [Suy ngẫm · 27 tháng 5, 2026 Lo que una firma no puede arreglar](#)
- [Phân tích · 26 tháng 5, 2026 Quyền riêng tư thực sự vs biểu hiện: những câu hỏi bạn nên tự đặt ra](#)

Tài bài viết này để sử dụng ở bất cứ đâu bạn cần.

[↓ Markdown](#) [↓ Văn bản thuần túy](#) [↓ PDF](#)

Tệp sẽ được tải xuống thiết bị của bạn. Từ đó, bạn có thể lưu trữ, nhập vào Solo2 hoặc chia sẻ ở bất cứ đâu. Cuadernos không quyết định điểm đến thay cho bạn.

Dấu sập · SHA-256 d5496b4982a825b0776e4208aadc0f7ed2d1372ad0fefc5d96fe8dfd5b1c4547

[Tính năng](#) [Giá cả](#) [Cài đặt](#) [Tin tức mới](#) [Blog](#) [Pro](#) [Trợ giúp](#) [Giới thiệu](#) [Liên hệ](#)
[Minh bạch](#) [Xác minh](#) [Quyền riêng tư](#) [Điều khoản](#) [Cookie](#)

Cuadernos Lacre · Một ấn phẩm của [Menzuri Gestión S.L.](#) ·
viết bởi R.Eugenio · được biên tập bởi đội ngũ [Solo2](#).

Trang web này không sử dụng cookie. Mọi thứ trình duyệt của bạn tải đều do chúng tôi viết hoặc giám sát và được lưu trữ trên máy chủ Châu Âu của chúng tôi: trình đếm lượt truy cập ẩn danh (Umami, tự lưu trữ) và lượng JavaScript tối thiểu cần thiết cho trình chọn ngôn ngữ và tùy chọn chế độ sáng/tối của bạn, được lưu trên chính thiết bị của bạn. Không tài nguyên từ các công ty bên ngoài, không trình theo dõi, không lập hồ sơ, không chia sẻ dữ liệu. Nếu bạn muốn theo dõi chúng tôi: [RSS](#).