

VPN คืออะไรกันแน่

เปลี่ยนว่าใครมองเห็นคุณได้ ไม่ใช่มีใครมองเห็นได้หรือไม่

เพื่อให้เข้าใจตรงกัน: VPN ทำให้ผู้ให้บริการอินเทอร์เน็ตของคุณ หรือ Wi-Fi ของสนามบิน ไม่เห็นว่าคุณเชื่อมต่อ กับที่ใด ข้อมูลนั้นไม่ได้หายไปไหน แต่ถูกส่งไปยังบริษัท VPN ซึ่งตอนนี้เป็นผู้มองเห็นแทน สิ่งที่เข้ารหัสอยู่ แล้ว เช่น อีเมลหรือธนาคาร ก็เข้ารหัสอยู่ก่อนแล้ว มันมีประโยชน์สำหรับเรื่องเฉพาะเจาะจงไม่กี่อย่าง และ มักถูกทำการตลาดราวกับว่าทำได้มากกว่านั้นมาก

เป็นเวลาหลายปีที่ได้ยินเรื่อง VPN แต่ไม่ได้สนใจ เหมือนกับโปรแกรมป้องกันไวรัส: ผมไม่ใช่โปรแกรม ป้องกันไวรัส หรือแทบจะไม่เคยใช้เลย ผมสำรองข้อมูลทุกอย่างไว้สามแห่งแบบเรียลไทม์ และระมัดระวัง อย่างมากกับสิ่งที่ดาวน์โหลด ลิงก์ที่คลิก และเว็บไซต์ที่เข้าชม มันไม่ใช่ความปลอดภัยแบบร้อยเปอร์เซ็นต์ แต่มันคือสิ่งที่ได้ผลสำหรับผม วันหนึ่งผมเห็นข้อเสนอ VPN ราคาเพียงสองยูโรกว่าต่อเดือน จึงสมัครเพราะ ความอยากรู้ มันทำงานได้ดี แต่แทบไม่มีประโยชน์อะไรกับผมเลย: เช่น การลองใช้บริการที่ตอนนั้นเปิดให้ บริการเฉพาะในสหรัฐอเมริกาเท่านั้น ผมรู้สึกปลอดภัยขึ้นไหม? ไม่เลย ถ้ามีข้อเสนอราคานี้อีก ผมอาจจะต่อ อายุ ถ้าไม่มี ก็ไม่ต่อ นี่เป็นเพียงประสบการณ์ของผม มันไม่ได้พิสูจน์อะไร ผมจึงถามตัวเองว่า VPN ทำงาน อย่างไรกันแน่ และนี่คือสิ่งที่ผมเข้าใจ

ลองนึกภาพว่าคุณหย่อนจดหมายลงในตู้ไปรษณีย์โดยระบุที่อยู่ของผู้รับไว้อย่างชัดเจน บุรุษไปรษณีย์จะเห็น ว่าคุณส่งให้ใคร แม้จะไม่สามารถอ่านได้หากจดหมายปิดผนึกอยู่ บุรุษไปรษณีย์คนนั้นคือผู้ให้บริการ อินเทอร์เน็ตของคุณ VPN จะนำจดหมายของคุณใส่ไว้ในซองอีกชั้นหนึ่ง จำหน้าถึงตัวกลางที่จะเป็นคนเปิด และส่งต่อให้ บุรุษไปรษณีย์ตามปกติของคุณจะไม่เห็นที่อยู่ที่แท้จริงอีกต่อไป เขาเห็นเพียงว่าคุณเขียนถึง ตัวกลางคนนั้น

ใครก็ตามที่ควบคุมเครือข่ายที่คุณเชื่อมต่อ เช่น Wi-Fi ของสนามบิน จะไม่เห็นอีกต่อไปว่าคุณกำลังไปที่ไหน แต่ตอนนี้ตัวกลางจะเห็นสิ่งที่ผู้ให้บริการของคุณเคยเห็น และบางครั้งอาจเห็นมากกว่านั้น เพราะทราฟฟิก ทั้งหมดของคุณไหลผ่านเขา การสอดส่องไม่ได้หายไป: แค่เปลี่ยนมือ นั่นจึงเป็นที่มาของชื่อ

นอกจากนี้ เกือบทุกสิ่งที่คุณทำในปัจจุบัน เช่น การเปิดอีเมลหรือเข้าสู่ระบบธนาคาร ก็เดินทางแบบเข้ารหัส ไปยังเซิร์ฟเวอร์ปลายทางอยู่แล้วด้วยแม่กุญแจของเบราว์เซอร์ สิ่งนี้เกิดขึ้นทั้งที่มี VPN และไม่มี VPN โดย

VPN เพิ่มการปกป้องเฉพาะในช่วงแรกเท่านั้น คือจนถึงเซิร์ฟเวอร์ของตัวเอง จากตรงนั้น เส้นทางก็เหมือนเดิมตามปกติ

นั่นคือเหตุผลที่มีบางสิ่งที่มีมันไม่สามารถสัญญาให้คุณได้ แม้ว่าบางครั้งจะถูกโฆษณาเช่นนั้นก็ตาม หากคุณลงชื่อเข้าใช้อีเมลหรือธนาคาร บริการนั้นก็รู้ว่าเป็นคุณ ไม่ว่าจะ VPN หรือไม่ก็ตาม มันไม่ได้รับประกันว่าไม่มีใครดูทราฟฟิกของคุณ: มันแค่เปลี่ยนว่าใครเป็นคนดู การที่บริษัทบอกว่า «ไม่เก็บบันทึก» เป็นเพียงคำสัญญา เหมือนกับเวลาที่แพลตฟอร์มขนาดใหญ่บอกว่า «ข้อความของคุณได้รับการเข้ารหัส เราไม่ได้อ่าน» การตรวจสอบภายนอกอาจสนับสนุนคำกล่าวอ้างนั้นได้ ณ เวลาใดเวลาหนึ่ง แต่มันก็ยังคงเป็นสิ่งที่คุณต้องไว้วางใจว่าจะปฏิบัติตาม ไม่ใช่สิ่งที่ไม่สามารถละเมิดได้โดยการออกแบบเชิงโครงสร้าง

และเนื้อหาของสนทนาก็ยังคงเหมือนเดิม หากแอปส่งข้อความของคุณเข้ารหัสแบบต้นทางถึงปลายทางอยู่แล้ว VPN ก็ไม่ได้ช่วยอะไรเพิ่ม หากแอปไม่ได้ทำเช่นนั้น VPN ก็แก้ไขไม่ได้เช่นกัน: มันปกป้องเส้นทางของข้อความ ไม่ใช่สิ่งที่แอปหรือเซิร์ฟเวอร์จะทำกับข้อความเมื่อไปถึง

ไม่มีอะไรในนี้ที่ทำให้มันไร้ประโยชน์ การซ่อนตำแหน่งที่คุณเชื่อมต่อจาก Wi-Fi สาธารณะ จากผู้ให้บริการที่ต้องการขายประวัติการท่องเว็บ หรือจากประเทศที่บล็อกบริการบางอย่าง ถือเป็นงานที่ทำได้จริง และมันทำได้ดี สิ่งที่เกิดขึ้นคือการตลาดมักจะสัญญาเกินกว่าที่ชั้นการปกป้องกันจะให้

คำถามที่ควรถาม ไม่ว่าจะกับ VPN หรือบริการใดก็ตามที่สัญญาว่าจะปกป้องคุณ ไม่ใช่ «มันเข้ารหัสหรือไม่?» ซึ่งอาจจะเข้ารหัส อย่างน้อยก็ในช่วงหนึ่ง คำถามที่แท้จริงคือ: เรากำลังมอบความไว้วางใจที่เราเพิ่งดึงออกมาจากผู้อื่นไว้กับใคร? และจะเหลืออะไรหากความไว้วางใจนั้นพิสูจน์แล้วว่าไร้เหตุผล?

VPN เมื่อทำหน้าที่ได้ดี จะทำเพียงเปลี่ยนตัวกลางในการเชื่อมต่อของคุณ ส่วนแอปอย่าง Solo2 ซึ่งข้อความไม่ผ่านเซิร์ฟเวอร์ใดๆ เลย จะตัดตัวกลางออกจากการสนทนาโดยสิ้นเชิง ทั้งสองไม่ได้แข่งขันกัน: พวกมันแก้ปัญหาคนละอย่าง

การสับสนระหว่างสองสิ่งนี้เป็นวิธีทั่วไปที่ทำให้ผู้คนเชื่อว่าตนเองได้รับการปกป้องมากกว่าความเป็นจริง

หมายเหตุจากบรรณาธิการ: เมื่อ Cuadernos เหล่านี้เอ่ยชื่อบริษัทหรือผลิตภัณฑ์ ไม่ใช่เพื่อการกล่าวหา ผู้ที่สร้างสรรค์สิ่งเหล่านั้นได้ทำงานที่คนนับล้านได้ใช้และชื่นชอบ สิ่งที่เรากำลังชี้ให้เห็นคือเรื่องเชิงโครงสร้าง — รูปแบบธุรกิจ ไม่ใช่แบรนด์ แบรนด์ต่างๆ ถูกยกมาเป็นตัวอย่างเพราะเป็นสิ่งที่ผู้อ่านรู้จัก

แหล่งข้อมูลและการอ่านเพิ่มเติม

- โพรโตคอล HTTPS และการเข้ารหัสการส่งข้อมูลเป็นมาตรฐานเปิด ซึ่งได้รับการบันทึกไว้อย่างเปิดเผยโดย IETF
- ในชุดบทความเดียวกันนี้: «เมื่อไม่มีใครอยู่ตรงกลาง» และ «คุณไม่ได้เป็นนิรนาม» ได้สำรวจความแตกต่างระหว่างโครงสร้างและคำสัญญาจากมุมมองอื่นๆ

[← ก่อนหน้าคุณไม่ได้เป็นนิรนาม](#)

บทความล่าสุด

- [บทสะท้อนความคิด · 29 มิถุนายน 2026 คุณไม่ได้เป็นนิรนาม](#)
- [บทสะท้อน · 27 พฤษภาคม 2026 สิ่งที่ลายเซ็นไม่สามารถแก้ไขได้](#)
- [การวิเคราะห์ · 26 พฤษภาคม 2026 ความเป็นส่วนตัวที่แท้จริง vs ความเป็นส่วนตัวที่ฉาบฉวย: คำถามที่คุณควรตั้งกับตัวเอง](#)

ดาวน์โหลดบทความนี้เก็บไว้เพื่อใช้งานได้ทุกที่ที่คุณต้องการ

[↓ Markdown](#) [↓ ข้อความธรรมดา](#) [↓ PDF](#)

ไฟล์จะถูกดาวน์โหลดลงในอุปกรณ์ของคุณ คุณสามารถบันทึก นำเข้าสู่ Solo2 หรือแชร์ได้ทุกที่ตามต้องการ
Cuadernos จะไม่กำหนดปลายทางแทนคุณ

ตราประทับครั้ง · SHA-256 f7a116cbe4eb640a7ef8340add2427f153cdecf423870ebe19ab05a85cc85727

[คุณสมบัติ](#) [ราคา](#) [ติดตั้ง](#) [มีอะไรใหม่](#) [บล็อก](#) [Pro](#) [ช่วยเหลือ](#) [เกี่ยวกับ](#) [ติดต่อ](#)
[ความโปร่งใส](#) [การตรวจสอบ](#) [ความเป็นส่วนตัว](#) [เงื่อนไข](#) [คุกกี้](#)

Cuadernos Lacre · สิ่งพิมพ์ของ [Menzuri Gestión S.L.](#) ·

เขียนโดย R.Eugenio · เรียบเรียงโดยทีมงาน [Solo2](#)

เว็บไซต์ของเราไม่ใช้คุกกี้ ทุกสิ่งที่เบราว์เซอร์ของคุณโหลดนั้นเราเป็นผู้เขียนหรือกำกับดูแล และโฮสต์อยู่บนเซิร์ฟเวอร์ยุโรปของเรา ได้แก่ ตัวนับการเข้าชมแบบไม่ระบุตัวตน (Umami โฮสต์เอง) และ JavaScript ขั้นต่ำที่จำเป็นสำหรับตัวเลือกภาษาและการตั้งค่าธีมสว่าง/มืดของคุณ ซึ่งจะถูกบันทึกไว้บนอุปกรณ์ของคุณเอง ไม่มีทรัพยากรจากบริษัทภายนอก ไม่มีเครื่องมือติดตาม ไม่มีการสร้างโปรไฟล์ ไม่มีการแชร์ข้อมูล หากคุณต้องการติดตามเรา: [RSS](#)