**VPN là gì và nó hoạt động như thế nào?**

Cơ bản

VPN (Mạng Riêng Ảo) tạo ra một kết nối an toàn, được mã hóa giữa thiết bị của bạn và internet, định tuyến lưu lượng truy cập qua một máy chủ từ xa để che giấu địa chỉ IP của bạn. Điều này bảo vệ dữ liệu của bạn khỏi tin tặc, ISP và các trình theo dõi, đảm bảo quyền riêng tư. Vào năm 2025, VPN trở nên vô cùng quan trọng do các mối đe dọa mạng gia tăng, tình trạng theo dõi dữ liệu tràn lan và các hạn chế về nội dung ngày càng tăng. Chúng hoàn hảo cho việc duyệt web an toàn trên Wi-Fi công cộng, truy cập nội dung bị chặn theo khu vực địa lý như thư viện Netflix và vượt qua kiểm duyệt ở các khu vực hạn chế.

**Đề xuất của chúng tôi: ExpressVPN**

4,9/5

VPN hàng đầu trong ngành với mã hóa cấp quân sự và tốc độ cực nhanh trên hơn 94 quốc gia.

Bảo hành 30 ngàyHỗ trợ 24/7Chính sách không lưu nhật ký5 thiết bị

🎉 Tiết kiệm 49% + 3 tháng miễn phí

Dùng thử ExpressVPN không rủi ro

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**Có nên sử dụng VPN không?**

Hợp pháp

VPN được coi là hợp pháp ở hầu hết các quốc gia trên thế giới, bao gồm Hoa Kỳ, Canada, Vương quốc Anh và hầu hết các nước châu Âu. Tuy nhiên, một số quốc gia như Trung Quốc, Nga và Iran có những hạn chế hoặc lệnh cấm sử dụng VPN. Hãy luôn kiểm tra luật pháp địa phương trước khi sử dụng VPN.

Hướng dẫn liên quan:

[Hướng dẫn về Luật VPN theo Quốc gia](https://bestvpn.digital/guides/vpn-laws-by-country)

[Hướng dẫn đầy đủ về tính hợp pháp của VPN ở các quốc gia và khu vực khác nhau](https://bestvpn.digital/guides/vpn-laws-by-country)

[Mẹo sử dụng VPN hợp pháp](https://bestvpn.digital/guides/legal-vpn-usage)

[Các biện pháp tốt nhất để sử dụng VPN một cách hợp pháp và có trách nhiệm](https://bestvpn.digital/guides/legal-vpn-usage)

**Khuyến nghị của chúng tôi: NordVPN**

4,8/5

VPN không lưu nhật ký đã được kiểm tra với các tính năng bảo mật nâng cao và mạng máy chủ toàn cầu.

VPN képCyberSecKill switch6 thiết bị

🎉 Tiết kiệm 68% + 3 tháng miễn phí

Nhận NordVPN ngay

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**VPN có làm chậm tốc độ internet không?**

Hiệu suất

VPN có thể làm giảm tốc độ internet do chi phí mã hóa và khoảng cách truyền dữ liệu bổ sung qua máy chủ VPN. Tuy nhiên, VPN cao cấp thường chỉ làm giảm tốc độ ở mức tối thiểu (5-15%), và một số thậm chí có thể cải thiện tốc độ bằng cách bỏ qua việc điều tiết băng thông của ISP.

Hướng dẫn liên quan:

[Kết quả kiểm tra tốc độ VPN](https://bestvpn.digital/guides/vpn-speed-tests)

[Kiểm tra tốc độ thực tế so sánh các nhà cung cấp VPN hàng đầu](https://bestvpn.digital/guides/vpn-speed-tests)

[Cách tối ưu hóa tốc độ VPN](https://bestvpn.digital/guides/optimize-vpn-speed)

[Mẹo và thủ thuật để tối đa hóa tốc độ kết nối VPN của bạn](https://bestvpn.digital/guides/optimize-vpn-speed)

**Khuyến nghị của chúng tôi: Surfshark**

4,7/5

Thiết bị không giới hạn với giao thức WireGuard cho tốc độ và bảo mật tối đa.

Thiết bị không giới hạnWireGuardCleanWebMultiHop

🎉 Tiết kiệm 82% + 2 tháng miễn phí

Bắt đầu với Surfshark

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**Tôi có thể sử dụng VPN để phát trực tuyến Netflix, Hulu và các dịch vụ khác không?**

Phát trực tuyến

Nhiều VPN có thể truy cập nội dung bị hạn chế địa lý trên các nền tảng phát trực tuyến, nhưng không phải VPN nào cũng hoạt động đáng tin cậy với mọi dịch vụ phát trực tuyến. Hãy tìm các VPN quảng cáo cụ thể về khả năng phát trực tuyến và có máy chủ được tối ưu hóa cho các nền tảng phổ biến.

Hướng dẫn liên quan:

[VPN tốt nhất cho Netflix](https://bestvpn.digital/guides/best-vpns-for-netflix)

[Các dịch vụ VPN hàng đầu giúp bỏ chặn nội dung Netflix một cách đáng tin cậy](https://bestvpn.digital/guides/best-vpns-for-netflix)

[Hướng dẫn thiết lập Netflix VPN](https://bestvpn.digital/guides/netflix-vpn-setup)

[Hướng dẫn từng bước để phát trực tuyến Netflix bằng VPN](https://bestvpn.digital/guides/netflix-vpn-setup)

**Đề xuất của chúng tôi: ExpressVPN**

4,9/5

VPN tốt nhất cho Netflix với máy chủ phát trực tuyến được tối ưu hóa và hỗ trợ 4K.

Bỏ chặn NetflixPhát trực tuyến 4KDNS thông minhHỗ trợ bộ định tuyến

🎉 Tiết kiệm 49% + 3 tháng miễn phí

Truyền phát Netflix với ExpressVPN

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**Sự khác biệt giữa VPN miễn phí và VPN trả phí là gì?**

Giá cả

VPN miễn phí thường có máy chủ hạn chế, tốc độ chậm hơn, giới hạn dữ liệu và ít tính năng bảo mật hơn. Chúng cũng có thể ghi lại dữ liệu người dùng hoặc hiển thị quảng cáo. VPN trả phí cung cấp bảo mật tốt hơn, tốc độ nhanh hơn, nhiều máy chủ hơn và chính sách bảo mật chặt chẽ hơn với cam kết không lưu nhật ký.

Hướng dẫn liên quan:

[So sánh WireGuard và OpenVPN](https://bestvpn.digital/guides/wireguard-vs-openvpn)

[So sánh chi tiết hai giao thức VPN phổ biến nhất](https://bestvpn.digital/guides/wireguard-vs-openvpn)

[Hướng dẫn bảo mật giao thức VPN](https://bestvpn.digital/guides/vpn-protocol-security)

[Hiểu về các giao thức VPN khác nhau và các tính năng bảo mật của chúng](https://bestvpn.digital/guides/vpn-protocol-security)

**Khuyến nghị của chúng tôi: NordVPN**

4,8/5

Lựa chọn giao thức nâng cao bao gồm NordLynx (WireGuard) để có hiệu suất tối ưu.

Giao thức NordLynxOpenVPNIKEv2Giao thức tùy chỉnh

🎉 Tiết kiệm 68% + 3 tháng miễn phí

Chọn giao thức NordVPN

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**Tôi có thể kết nối bao nhiêu thiết bị với VPN?**

Thiết bị

Điều này khác nhau tùy theo nhà cung cấp. Một số VPN cho phép 5-10 kết nối đồng thời, trong khi những VPN khác như Surfshark và IPVanish cung cấp kết nối không giới hạn. Hãy kiểm tra giới hạn thiết bị trước khi chọn VPN nếu bạn có nhiều thiết bị.

**Khuyến nghị của chúng tôi: CyberGhost**

4.6/5

Ứng dụng di động thân thiện với người dùng, kết nối chỉ bằng một cú nhấp chuột và máy chủ được tối ưu hóa.

Ứng dụng di động dễ dàngTự động kết nối7 thiết bịBảo hành 45 ngày

🎉 Tiết kiệm 84% + 4 tháng miễn phí

Tải CyberGhost Mobile

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**Chính sách VPN không lưu nhật ký là gì?**

Sự riêng tư

Chính sách không lưu nhật ký nghĩa là nhà cung cấp VPN không ghi lại hoặc lưu trữ bất kỳ thông tin nào về hoạt động trực tuyến, thời gian kết nối, địa chỉ IP hoặc lịch sử duyệt web của bạn. Điều này đảm bảo quyền riêng tư của bạn ngay cả khi công ty VPN bị xâm phạm hoặc bị pháp luật buộc phải chia sẻ dữ liệu.

**Khuyến nghị của chúng tôi: Surfshark**

4,7/5

VPN cao cấp giá cả phải chăng nhất với số lượng thiết bị không giới hạn và đầy đủ tính năng.

Thiết bị không giới hạnTất cả tính năngBảo hành 30 ngàyHỗ trợ 24/7

🎉 Tiết kiệm 82% + 2 tháng miễn phí

Nhận ưu đãi VPN tốt nhất

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**Tôi nên sử dụng giao thức VPN nào?**

Kỹ thuật

Các giao thức tốt nhất là WireGuard (nhanh nhất và hiện đại nhất), OpenVPN (an toàn nhất và được hỗ trợ rộng rãi) và IKEv2 (tuyệt vời cho thiết bị di động). Tránh sử dụng PPTP vì nó đã lỗi thời và không an toàn. Hầu hết người dùng nên chọn WireGuard khi có thể.

Hướng dẫn liên quan:

[VPN tốt nhất cho Torrenting](https://bestvpn.digital/guides/best-vpns-for-torrenting)

[Các dịch vụ VPN thân thiện với P2P hàng đầu có hỗ trợ chuyển tiếp cổng](https://bestvpn.digital/guides/best-vpns-for-torrenting)

[Hướng dẫn tải Torrent an toàn](https://bestvpn.digital/guides/safe-torrenting-guide)

[Cách tải torrent an toàn và ẩn danh bằng VPN](https://bestvpn.digital/guides/safe-torrenting-guide)

**Đề xuất của chúng tôi: ExpressVPN**

4,9/5

Máy chủ được tối ưu hóa P2P với tính năng chuyển tiếp cổng và chính sách nghiêm ngặt không ghi nhật ký để tải torrent an toàn.

Máy chủ P2PChuyển tiếp cổngCông tắc ngắtKhông có nhật ký nào được kiểm tra

🎉 Tiết kiệm 49% + 3 tháng miễn phí

Tải torrent an toàn với ExpressVPN

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**Tôi có thể sử dụng VPN trên bộ định tuyến của mình không?**

Kỹ thuật

Có, nhiều nhà cung cấp VPN hỗ trợ cài đặt bộ định tuyến, giúp bảo vệ tất cả các thiết bị trong mạng của bạn. Bạn sẽ cần một bộ định tuyến tương thích hỗ trợ máy khách VPN, hoặc bạn có thể mua bộ định tuyến VPN được cấu hình sẵn. Điều này được tính là một kết nối cho giới hạn thiết bị.

Hướng dẫn liên quan:

[Giải thích về VPN Kill Switch](https://bestvpn.digital/guides/vpn-kill-switch-guide)

[Hướng dẫn đầy đủ về công tắc ngắt VPN và cách chúng bảo vệ bạn](https://bestvpn.digital/guides/vpn-kill-switch-guide)

[Tính năng bảo mật VPN](https://bestvpn.digital/guides/vpn-security-features)

[Các tính năng bảo mật cần thiết cần tìm trong dịch vụ VPN](https://bestvpn.digital/guides/vpn-security-features)

**Khuyến nghị của chúng tôi: NordVPN**

4,8/5

Công nghệ ngắt kết nối tiên tiến có thể chặn internet ngay lập tức nếu VPN bị ngắt kết nối.

Công tắc tắt ứng dụngCông tắc tắt hệ thốngTự động kết nối lạiBảo vệ rò rỉ DNS

🎉 Tiết kiệm 68% + 3 tháng miễn phí

Bảo mật với NordVPN Kill Switch

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**Tôi có cần VPN cho thiết bị di động không?**

Di động

Đúng vậy, VPN di động rất quan trọng để bảo vệ dữ liệu của bạn trên Wi-Fi công cộng, ngăn chặn theo dõi di động và truy cập nội dung bị hạn chế theo địa lý. Hầu hết các nhà cung cấp VPN đều cung cấp ứng dụng di động chuyên dụng cho iOS và Android với các tính năng bảo mật tương tự như phiên bản dành cho máy tính để bàn.

Hướng dẫn liên quan:

[So sánh VPN miễn phí và trả phí](https://bestvpn.digital/guides/free-vs-paid-vpn)

[Tại sao VPN trả phí đáng để đầu tư hơn các giải pháp thay thế miễn phí](https://bestvpn.digital/guides/free-vs-paid-vpn)

[Bản dùng thử VPN và đảm bảo hoàn tiền](https://bestvpn.digital/guides/vpn-trials-guarantees)

[Cách dùng thử VPN cao cấp không rủi ro với thời gian dùng thử](https://bestvpn.digital/guides/vpn-trials-guarantees)

**Khuyến nghị của chúng tôi: CyberGhost**

4.6/5

VPN cao cấp với chế độ bảo đảm hoàn tiền trong 45 ngày - lâu hơn bất kỳ bản dùng thử miễn phí nào.

Bảo hành 45 ngàyKhông giới hạn dữ liệuĐầy đủ tính năng7 thiết bị

🎉 Tiết kiệm 84% + 4 tháng miễn phí

Dùng thử CyberGhost không rủi ro

Đảm bảo hoàn tiền trong 30 ngày • Chính sách không lưu nhật ký • Hỗ trợ 24/7

**Đường hầm chia tách là gì?**

Đặc trưng

Đường hầm phân chia cho phép bạn định tuyến một phần lưu lượng truy cập internet qua VPN trong khi vẫn cho phép các lưu lượng truy cập khác truy cập internet trực tiếp. Điều này hữu ích khi truy cập các dịch vụ cục bộ trong khi vẫn duy trì bảo vệ VPN cho các hoạt động nhạy cảm.

**Làm thế nào để chọn được vị trí máy chủ VPN tốt nhất?**

Cách sử dụng

**Kill switch là gì và tại sao tôi cần nó?**

Bảo vệ

Tính năng Kill Switch sẽ tự động ngắt kết nối internet nếu kết nối VPN bị ngắt đột ngột. Tính năng này ngăn chặn việc lộ địa chỉ IP thực và dữ liệu chưa được mã hóa của bạn. Điều này rất cần thiết để duy trì quyền riêng tư và bảo mật.

**VPN có thể bị phát hiện không?**

Sự riêng tư

Đúng vậy, đôi khi VPN có thể bị phát hiện thông qua nhiều phương pháp khác nhau, bao gồm danh sách đen IP, kiểm tra gói tin sâu và phân tích hành vi. Một số VPN cung cấp tính năng che giấu để ẩn hoạt động sử dụng VPN, khiến việc phát hiện trở nên khó khăn hơn nhiều.

**Có rủi ro nào khi sử dụng VPN không?**

Bảo vệ

Rủi ro bao gồm việc chọn nhà cung cấp không đáng tin cậy, lưu trữ dữ liệu, phần mềm độc hại trong các ứng dụng VPN giả mạo, tốc độ internet chậm hơn và khả năng không tương thích với một số dịch vụ. Luôn chọn nhà cung cấp VPN uy tín, đã được kiểm toán và có chính sách bảo mật chặt chẽ.

**Tôi nên trả bao nhiêu cho một VPN?**

Giá cả

Các VPN chất lượng thường có giá từ 2-12 đô la mỗi tháng, với các gói đăng ký dài hạn hơn sẽ mang lại giá trị tốt hơn. Giá dưới 2 đô la/tháng có thể cho thấy sự hạn chế về bảo mật hoặc tính năng. Hãy cân nhắc các gói hàng năm để tiết kiệm, nhưng hãy bắt đầu với các gói ngắn hạn hơn để kiểm tra dịch vụ.

**Tôi có thể sử dụng VPN để tải torrent không?**

P2P

Nhiều VPN hỗ trợ lưu lượng P2P và torrent, nhưng không phải tất cả. Hãy tìm VPN có máy chủ P2P chuyên dụng, mã hóa mạnh, chính sách không lưu nhật ký và tính năng ngắt kết nối. Một số nhà cung cấp cho phép torrent trong khi những nhà cung cấp khác lại cấm.

**Sự khác biệt giữa VPN và proxy là gì?**

So sánh

VPN mã hóa toàn bộ lưu lượng truy cập internet của bạn và hoạt động trên toàn hệ thống, trong khi proxy chỉ chuyển hướng lưu lượng truy cập từ các ứng dụng cụ thể mà không cần mã hóa. VPN cung cấp khả năng bảo mật và bảo vệ quyền riêng tư tốt hơn nhiều so với proxy.

**VPN có hoạt động ở Trung Quốc không?**

Kiểm duyệt

Việc sử dụng VPN bị hạn chế ở Trung Quốc, và Tường lửa Vạn Lý Trường Thành (Great Firewall) chặn nhiều dịch vụ VPN. Một số VPN vẫn hoạt động với công nghệ che giấu đặc biệt, nhưng độ tin cậy có thể không ổn định. Hãy kiểm tra các báo cáo hiện tại và chọn VPN có khả năng vượt qua Trung Quốc đã được chứng minh.

**Tôi có thể có được IP chuyên dụng với VPN không?**

Đặc trưng

Có, một số nhà cung cấp VPN cung cấp địa chỉ IP tĩnh/chuyên dụng với một khoản phí bổ sung. Điều này giúp bạn luôn có cùng một địa chỉ IP mỗi khi kết nối, hữu ích khi truy cập các dịch vụ bị hạn chế IP hoặc tránh CAPTCHA.

**Làm thế nào để kiểm tra xem VPN của tôi có hoạt động không?**

Kiểm tra

Kiểm tra địa chỉ IP của bạn trước và sau khi kết nối để đảm bảo nó thay đổi. Kiểm tra rò rỉ DNS bằng các công cụ trực tuyến, xác minh vị trí của bạn hiển thị là vị trí máy chủ VPN và xác nhận tính năng ngắt kết nối VPN hoạt động.

**Điều gì xảy ra nếu tôi quên bật VPN?**

Cách sử dụng

Địa chỉ IP thực và vị trí của bạn sẽ bị lộ, nhà cung cấp dịch vụ Internet (ISP) có thể theo dõi lưu lượng truy cập của bạn và bạn sẽ không được bảo vệ bằng VPN. Một số VPN cung cấp tính năng tự động kết nối, tự động khởi động VPN khi bạn kết nối với Internet hoặc các mạng không đáng tin cậy.

**Nhà tuyển dụng có thể xem hoạt động internet của tôi bằng VPN không?**

Sự riêng tư

Nếu bạn đang sử dụng thiết bị hoặc mạng của công ty, nhà tuyển dụng vẫn có thể theo dõi hoạt động của bạn thông qua các phương pháp khác như phần mềm giám sát điểm cuối, ngay cả khi sử dụng VPN. VPN cá nhân trên thiết bị cá nhân mang lại sự riêng tư tốt hơn khỏi sự giám sát của nhà tuyển dụng.

**Tôi có cần phần mềm diệt vi-rút nếu sử dụng VPN không?**

Bảo vệ

VPN và phần mềm diệt virus có mục đích khác nhau. VPN bảo vệ quyền riêng tư và dữ liệu khi truyền tải, trong khi phần mềm diệt virus bảo vệ chống lại phần mềm độc hại và các tệp độc hại. Bạn nên sử dụng cả hai để có sự bảo vệ toàn diện - chúng bổ sung cho nhau.

**VPN kép hoặc VPN đa điểm là gì?**

Trình độ cao

VPN kép định tuyến lưu lượng truy cập của bạn qua hai máy chủ VPN thay vì một, thêm một lớp mã hóa và khiến hoạt động trực tuyến của bạn cực kỳ khó bị theo dõi. Tuy nhiên, nó làm giảm đáng kể tốc độ và thường quá mức cần thiết đối với hầu hết người dùng.

**Tôi có thể sử dụng VPN với TV thông minh không?**

Thiết bị

Có, bạn có thể sử dụng VPN với TV thông minh bằng cách cài đặt VPN trên bộ định tuyến, chia sẻ kết nối VPN từ máy tính hoặc sử dụng Fire Stick/Apple TV có hỗ trợ VPN. Một số TV thông minh cũng hỗ trợ trực tiếp ứng dụng VPN.

**Sự che giấu trong VPN là gì?**

Trình độ cao

Chế độ che giấu (obfuscation) ngụy trang lưu lượng VPN để trông giống như lưu lượng HTTPS thông thường, giúp vượt qua các lệnh chặn VPN ở các quốc gia hoặc mạng lưới hạn chế. Chế độ này còn được gọi là chế độ ẩn và hữu ích ở các quốc gia có kiểm duyệt internet.

**Tôi nên thay đổi máy chủ VPN bao lâu một lần?**

Cách sử dụng

Không có quy tắc cố định nào, nhưng bạn có thể muốn thay đổi máy chủ nếu gặp phải tình trạng tốc độ chậm, nếu máy chủ bị chặn bởi dịch vụ bạn đang cố gắng truy cập, hoặc nếu muốn tăng cường sự riêng tư. Nhiều người dùng tìm thấy một vài máy chủ ưa thích và gắn bó với chúng.

**Tôi có thể sử dụng VPN để chơi game không?**

Chơi game

VPN có thể được sử dụng cho mục đích chơi game để giảm ping đến một số máy chủ nhất định, vượt qua giới hạn địa lý, tránh các cuộc tấn công DDoS hoặc truy cập trò chơi sớm ở các khu vực khác nhau. Tuy nhiên, VPN có thể làm tăng độ trễ, vì vậy hãy chọn máy chủ gần máy chủ trò chơi.

**Rò rỉ DNS là gì và làm thế nào để ngăn chặn nó?**

Bảo vệ

Rò rỉ DNS xảy ra khi các yêu cầu DNS của bạn bỏ qua đường hầm VPN, tiết lộ hoạt động duyệt web của bạn cho ISP. Hãy ngăn chặn điều này bằng cách sử dụng VPN có tính năng bảo vệ rò rỉ DNS tích hợp, thay đổi cài đặt DNS hoặc sử dụng máy chủ DNS của VPN.

**Có VPN nào dành riêng cho doanh nghiệp không?**

Việc kinh doanh

Đúng vậy, VPN doanh nghiệp cung cấp các tính năng như quản lý tập trung, địa chỉ IP chuyên dụng, tài khoản nhóm, tăng cường kết nối đồng thời và bảo mật cấp doanh nghiệp. Chúng thường có giá cao hơn nhưng cung cấp khả năng kiểm soát và hỗ trợ tốt hơn.

**IPv6 là gì và VPN có hỗ trợ IPv6 không?**

Kỹ thuật

IPv6 là giao thức internet mới hơn thay thế IPv4. Không phải tất cả VPN đều hỗ trợ IPv6, điều này có thể gây rò rỉ IPv6. Hãy tìm VPN hỗ trợ IPv6 hoặc chặn lưu lượng IPv6 để ngăn chặn rò rỉ, vì hầu hết người dùng vẫn chủ yếu sử dụng IPv4.

**Tôi có thể thiết lập máy chủ VPN của riêng mình không?**

tự làm lấy

Có, bạn có thể thiết lập máy chủ VPN cá nhân bằng các dịch vụ đám mây như AWS hoặc DigitalOcean, hoặc trên bộ định tuyến tại nhà. Tuy nhiên, điều này đảm bảo quyền riêng tư trước các nhà cung cấp dịch vụ Internet (ISP) nhưng không đảm bảo tính ẩn danh, vì máy chủ được liên kết với bạn. VPN thương mại mang lại tính ẩn danh tốt hơn.

**WireGuard là gì và tại sao nó lại phổ biến?**

Kỹ thuật

WireGuard là một giao thức VPN hiện đại, nhanh hơn, an toàn hơn và tiêu thụ ít pin hơn so với các giao thức cũ như OpenVPN. Nó có mã lệnh đơn giản hơn (giúp việc kiểm tra dễ dàng hơn), hiệu suất tốt hơn và đang trở thành lựa chọn ưu tiên của nhiều nhà cung cấp VPN.

**VPN có bảo vệ chống lại phần mềm độc hại không?**

Bảo vệ

VPN chủ yếu bảo vệ dữ liệu truyền tải thông qua mã hóa, chứ không phải chống phần mềm độc hại. Tuy nhiên, một số VPN có các tính năng bảo mật bổ sung như chặn quảng cáo, bảo vệ khỏi phần mềm độc hại và chặn trang web nguy hiểm. Bạn vẫn cần bảo vệ chống vi-rút riêng biệt.

**Tôi có thể sử dụng VPN để có giá trực tuyến rẻ hơn không?**

Mua sắm

Một số dịch vụ trực tuyến hiển thị giá khác nhau tùy theo vị trí, vì vậy việc thay đổi máy chủ VPN có thể hiển thị giá khác nhau. Tuy nhiên, điều này có thể vi phạm điều khoản dịch vụ và phương thức thanh toán thường tiết lộ vị trí thực tế của bạn.

**VPN nào tốt nhất cho người mới bắt đầu?**

Khuyến nghị

Các VPN thân thiện với người mới bắt đầu nên có ứng dụng dễ sử dụng, kết nối đáng tin cậy, hỗ trợ khách hàng tốt và chính sách bảo mật rõ ràng. ExpressVPN, NordVPN và Surfshark là những lựa chọn phổ biến cho người mới bắt đầu nhờ giao diện thân thiện với người dùng.

**Làm thế nào để hủy đăng ký VPN?**

Tài khoản

Phương thức hủy khác nhau tùy theo nhà cung cấp. Hầu hết cho phép hủy thông qua bảng điều khiển tài khoản, một số yêu cầu liên hệ với bộ phận hỗ trợ khách hàng. Vui lòng kiểm tra chính sách hủy và các điều khoản đảm bảo hoàn tiền trước khi đăng ký. Hãy lưu lại thông tin hủy đăng ký của bạn.

**Chuyển tiếp cổng trong VPN là gì?**

Trình độ cao

Chuyển tiếp cổng cho phép các kết nối bên ngoài đến các cổng cụ thể trên thiết bị của bạn thông qua kết nối VPN. Tính năng này hữu ích cho việc lưu trữ máy chủ, cải thiện kết nối P2P hoặc truy cập thiết bị từ xa. Không phải tất cả VPN đều hỗ trợ chuyển tiếp cổng.

**Tôi có thể sử dụng nhiều VPN cùng lúc không?**

Trình độ cao

Mặc dù về mặt kỹ thuật là có thể, việc sử dụng nhiều VPN cùng lúc (VPN chaining) rất phức tạp, làm giảm đáng kể tốc độ và thường không cần thiết. Hầu hết nhu cầu riêng tư của người dùng đều được đáp ứng với một dịch vụ VPN chất lượng duy nhất.

**VPN sử dụng băng thông nào?**

Hiệu suất

VPN làm tăng chi phí mã hóa, thường làm tăng mức sử dụng băng thông thêm 5-15%. Mức chi phí chính xác phụ thuộc vào giao thức được sử dụng và mức độ mã hóa. WireGuard thường có chi phí thấp hơn OpenVPN. Hãy tính thêm chi phí này vào giới hạn dữ liệu nếu có.

**Có VPN nào không yêu cầu đăng ký không?**

Sự riêng tư

Một số nhà cung cấp VPN cho phép đăng ký ẩn danh chỉ bằng địa chỉ email hoặc thậm chí thanh toán bằng tiền điện tử mà không cần thông tin cá nhân. Tuy nhiên, các VPN hoàn toàn không yêu cầu đăng ký rất hiếm và có thể có tính năng hoặc bảo mật hạn chế.

**Kiểm tra VPN là gì và tại sao nó lại quan trọng?**

Lòng tin

Kiểm toán VPN là quá trình đánh giá bảo mật độc lập các hệ thống, mã và hoạt động bảo mật của nhà cung cấp VPN do các công ty bảo mật bên thứ ba thực hiện. VPN được kiểm toán cung cấp sự đảm bảo đáng tin cậy hơn về các tuyên bố bảo mật và chính sách không lưu nhật ký của họ.

**Tôi có thể sử dụng VPN để truy cập mạng gia đình từ xa không?**

Truy cập từ xa

Có, bạn có thể thiết lập máy chủ VPN trên bộ định tuyến tại nhà để truy cập mạng gia đình một cách an toàn từ bất kỳ đâu. Điều này khác với các dịch vụ VPN thương mại và chủ yếu dành cho mục đích truy cập từ xa hơn là bảo mật quyền riêng tư hoặc ẩn danh.

**Điều gì sẽ xảy ra với VPN của tôi nếu công ty ngừng hoạt động?**

Việc kinh doanh

Nếu một công ty VPN đóng cửa, bạn sẽ mất quyền truy cập vào dịch vụ của họ ngay lập tức. Hãy chọn những nhà cung cấp uy tín, có quyền sở hữu và nguồn tài chính minh bạch. Hãy cân nhắc các VPN có chế độ bảo hành hoàn tiền dài hạn và tránh các cam kết đăng ký quá dài.

**Tôi có cần các VPN khác nhau cho các hoạt động khác nhau không?**

Cách sử dụng

Nhìn chung, một VPN tốt sẽ đáp ứng mọi nhu cầu của bạn. Tuy nhiên, một số người dùng lại chọn các VPN khác nhau cho các mục đích cụ thể - chẳng hạn như VPN được tối ưu hóa cho việc phát trực tuyến và VPN khác cho quyền riêng tư tối đa. Điều này phụ thuộc vào yêu cầu cụ thể và ngân sách của bạn.

**Kiến trúc máy chủ chỉ có RAM là gì?**

Sự riêng tư

Máy chủ chỉ có RAM không lưu trữ dữ liệu trên ổ cứng - mọi thứ chạy trên bộ nhớ được xóa sạch khi máy chủ khởi động lại. Điều này cung cấp thêm một lớp bảo vệ quyền riêng tư vì không thể lưu trữ nhật ký hoặc dữ liệu cố định trên máy chủ.

**Tôi có thể sử dụng VPN trên Wi-Fi công cộng không?**

Bảo vệ

Có, việc sử dụng VPN trên Wi-Fi công cộng rất được khuyến khích. Mạng công cộng thường không an toàn, dễ bị người khác đánh cắp dữ liệu. VPN mã hóa kết nối của bạn, bảo vệ thông tin nhạy cảm như mật khẩu và dữ liệu cá nhân khỏi tin tặc.

Hướng dẫn liên quan:

[Hướng dẫn bảo mật Wi-Fi công cộng](https://bestvpn.digital/guides/public-wifi-security)

[Hướng dẫn đầy đủ để giữ an toàn trên mạng không dây công cộng](https://bestvpn.digital/guides/public-wifi-security)

[Bảo mật VPN di động](https://bestvpn.digital/guides/mobile-vpn-security)

[Thực hành tốt nhất khi sử dụng VPN trên thiết bị di động](https://bestvpn.digital/guides/mobile-vpn-security)

**Sự khác biệt giữa địa chỉ IP dùng chung và địa chỉ IP chuyên dụng là gì?**

Đặc trưng

Địa chỉ IP dùng chung được nhiều người dùng VPN sử dụng đồng thời, mang lại khả năng ẩn danh tốt hơn nhưng có thể gặp phải tình trạng chặn dịch vụ. IP chuyên dụng được cấp riêng cho bạn, giúp giảm thiểu tình trạng chặn và CAPTCHA nhưng lại mang lại khả năng ẩn danh kém hơn.

**Làm thế nào để khắc phục sự cố kết nối VPN?**

Xử lý sự cố

Các cách khắc phục phổ biến bao gồm chuyển đổi máy chủ, thay đổi giao thức VPN, khởi động lại ứng dụng, kiểm tra cài đặt tường lửa, cập nhật ứng dụng VPN hoặc liên hệ với bộ phận hỗ trợ khách hàng. Nhiều sự cố kết nối được giải quyết bằng cách thử các máy chủ hoặc giao thức khác nhau.

**Tôi nên biết gì về bộ định tuyến để sử dụng VPN bảo mật?**

Bảo vệ

Cấu hình bộ định tuyến rất quan trọng đối với bảo mật khi sử dụng VPN. Việc thiết lập VPN trên bộ định tuyến sẽ tự động bảo vệ tất cả các thiết bị được kết nối. Hãy chọn bộ định tuyến hỗ trợ máy khách VPN, đảm bảo phần mềm hệ thống được cập nhật và cấu hình cài đặt tường lửa phù hợp. Các dịch vụ VPN được chúng tôi đề xuất cung cấp hướng dẫn thiết lập bộ định tuyến và hỗ trợ.

**Vai trò của WebRTC trong việc nâng cao giao thức thông qua VPN là gì?**

Kỹ thuật

WebRTC có thể ảnh hưởng đáng kể đến trải nghiệm trực tuyến của bạn khi sử dụng giao thức VPN. Quản lý WebRTC đúng cách giúp vượt qua kiểm duyệt, bảo mật dữ liệu và tận hưởng tốc độ tốt hơn. Các VPN hàng đầu bao gồm các tính năng bảo vệ rò rỉ WebRTC tiên tiến, ngăn chặn việc lộ IP thực của bạn thông qua các yêu cầu WebRTC của trình duyệt.

**Vai trò của việc đăng nhập trong việc nâng cao Basics thông qua VPN là gì?**

Sự riêng tư

Hiểu rõ chính sách ghi nhật ký là điều cần thiết khi chọn VPN. Chính sách không ghi nhật ký đảm bảo lịch sử duyệt web, thời gian kết nối và địa chỉ IP của bạn không bị ghi lại. Điều này cung cấp khả năng bảo vệ quyền riêng tư quan trọng và ngăn chặn dữ liệu bị chia sẻ với bên thứ ba hoặc cơ quan chức năng.

**Những lỗi phổ biến liên quan đến rò rỉ IP trong thiết lập VPN phát trực tuyến là gì?**

Phát trực tuyến

Rò rỉ IP có thể ảnh hưởng đến trải nghiệm phát trực tuyến và quyền riêng tư của bạn. Những sai lầm thường gặp bao gồm không kiểm tra rò rỉ DNS, rò rỉ WebRTC hoặc rò rỉ IPv6. VPN được cấu hình đúng cách với công tắc ngắt kết nối và bảo vệ chống rò rỉ sẽ đảm bảo IP thực của bạn được ẩn trong khi phát trực tuyến nội dung bị hạn chế về mặt địa lý.

Hướng dẫn liên quan:

[Hướng dẫn kiểm tra rò rỉ VPN](https://bestvpn.digital/guides/vpn-leak-test)

[Cách kiểm tra VPN của bạn để phát hiện rò rỉ DNS, WebRTC và IP](https://bestvpn.digital/guides/vpn-leak-test)

[Thiết lập VPN phát trực tuyến](https://bestvpn.digital/guides/streaming-vpn-setup)

[Cấu hình VPN tối ưu cho dịch vụ phát trực tuyến](https://bestvpn.digital/guides/streaming-vpn-setup)

**Vai trò của DNS trong việc nâng cao Basics thông qua VPN là gì?**

Kỹ thuật

Cấu hình DNS là yếu tố cơ bản đối với chức năng VPN. Việc sử dụng máy chủ DNS của nhà cung cấp VPN giúp ngăn chặn rò rỉ DNS và đảm bảo mọi lưu lượng truy cập của bạn được định tuyến chính xác qua đường hầm VPN. Điều này giúp tăng cường cả bảo mật và hiệu suất, đồng thời vẫn duy trì quyền riêng tư.

**Chuyển tiếp cổng có ảnh hưởng đến hiệu suất trong Basics dành cho người dùng VPN không?**

Hiệu suất

Chuyển tiếp cổng có thể ảnh hưởng đáng kể đến hiệu suất và chức năng của VPN. Tính năng này rất cần thiết cho các hoạt động P2P, chơi game và vận hành máy chủ. Tuy nhiên, không phải tất cả nhà cung cấp VPN đều hỗ trợ chuyển tiếp cổng, và việc mở một số cổng nhất định có thể làm giảm nhẹ tính bảo mật.

**Tôi nên biết gì về Catapult Hydra để sử dụng VPN?**

Giao thức

Catapult Hydra là giao thức VPN độc quyền mang đến tốc độ và bảo mật vượt trội. Giao thức này được thiết kế để mang lại hiệu suất tốt hơn so với các giao thức truyền thống, đồng thời vẫn duy trì mã hóa mạnh mẽ. Giao thức này đặc biệt hiệu quả cho việc phát trực tuyến và duyệt web nói chung.

**Độ trễ có ảnh hưởng đến hiệu suất bảo mật của người dùng VPN không?**

Hiệu suất

Độ trễ (lag) có thể ảnh hưởng đến cả bảo mật và hiệu suất khi sử dụng VPN. Độ trễ cao hơn có thể báo hiệu sự cố kết nối hoặc sự cố máy chủ. Hãy chọn máy chủ VPN gần vị trí của bạn hơn và sử dụng các giao thức nhanh hơn như WireGuard để giảm thiểu độ trễ mà vẫn đảm bảo bảo mật.

**Vai trò của trao đổi khóa trong việc nâng cao Basics thông qua VPN là gì?**

Bảo vệ

Trao đổi khóa là một quy trình bảo mật cơ bản trong kết nối VPN. Nó thiết lập các khóa mã hóa an toàn giữa thiết bị của bạn và máy chủ VPN. Các giao thức hiện đại sử dụng các phương pháp trao đổi khóa tiên tiến như Elliptic Curve Diffie-Hellman để tăng cường bảo mật và hiệu suất.

**Vai trò của cổng trong việc nâng cao Mẹo sử dụng qua VPN là gì?**

Kỹ thuật

Cổng VPN rất quan trọng để định tuyến lưu lượng truy cập chính xác. Nó quyết định cách lưu lượng truy cập internet của bạn được điều hướng qua đường hầm VPN. Cấu hình cổng VPN phù hợp giúp ngăn ngừa rò rỉ DNS, cải thiện chất lượng phát trực tuyến và đảm bảo mọi lưu lượng truy cập đều được bảo vệ.

**Cổng kết nối có cần thiết để có các tính năng nâng cao tốt hơn với VPN không?**

Trình độ cao

Cấu hình cổng kết nối là yếu tố thiết yếu cho các tính năng VPN nâng cao. Nó cho phép định tuyến lưu lượng phù hợp, hỗ trợ phân chia đường hầm và đảm bảo khả năng tương thích với các máy chủ chuyên dụng. Người dùng nâng cao sẽ được hưởng lợi từ việc hiểu rõ các thiết lập cổng kết nối để đạt hiệu suất tối ưu.

**Vai trò của chặn địa lý trong việc nâng cao tính năng Basics thông qua VPN là gì?**

Phát trực tuyến

Hiểu rõ về chặn địa lý là điều cơ bản khi sử dụng VPN. VPN giúp vượt qua các hạn chế địa lý bằng cách che giấu vị trí của bạn. Điều này cho phép truy cập vào nội dung, trang web và dịch vụ bị giới hạn theo khu vực, đồng thời vẫn đảm bảo quyền riêng tư và bảo mật.

Hướng dẫn liên quan:

[Hướng dẫn bỏ qua chặn địa lý](https://bestvpn.digital/guides/bypass-geo-blocking)

[Cách truy cập nội dung bị hạn chế theo địa lý bằng VPN](https://bestvpn.digital/guides/bypass-geo-blocking)

[Truy cập nội dung toàn cầu](https://bestvpn.digital/guides/global-content-access)

[Truy cập nội dung và dịch vụ quốc tế bằng VPN](https://bestvpn.digital/guides/global-content-access)

**Tại sao tôi nên quan tâm đến các kết nối đồng thời trong Thiết bị?**

Thiết bị

Số lượng kết nối đồng thời quyết định số lượng thiết bị bạn có thể bảo vệ bằng một tài khoản VPN. Điều này rất quan trọng đối với các hộ gia đình có nhiều thiết bị. Hãy tìm các VPN cung cấp kết nối không giới hạn hoặc giới hạn thiết bị phù hợp với nhu cầu của bạn.

**Tôi nên biết gì về việc kiểm tra việc sử dụng VPN của thiết bị?**

Lòng tin

Kiểm tra VPN cung cấp khả năng xác minh độc lập các tuyên bố bảo mật và chính sách quyền riêng tư. Khi chọn VPN cho nhiều thiết bị, các nhà cung cấp đã được kiểm tra sẽ có độ tin cậy cao hơn. Hãy tìm kiếm các báo cáo minh bạch và kiểm tra bảo mật gần đây của bên thứ ba.

**Tại sao tôi nên quan tâm đến độ trễ trong Tính năng nâng cao?**

Chơi game

Độ trễ ảnh hưởng đến các tính năng VPN nâng cao như chơi game, gọi video và các ứng dụng thời gian thực. Người dùng nâng cao nên chọn máy chủ có ping thấp, sử dụng giao thức được tối ưu hóa và cân nhắc sử dụng máy chủ chơi game chuyên dụng để có trải nghiệm tốt nhất.

**Những lỗi thường gặp khi kiểm tra trong thiết lập VPN P2P và Torrenting là gì?**

P2P

Khi sử dụng torrent, hãy chọn các nhà cung cấp VPN đã được kiểm tra với chính sách không lưu nhật ký đã được chứng minh. Những sai lầm phổ biến bao gồm sử dụng VPN chưa được kiểm tra, bỏ qua tính năng ngắt kết nối và không xác minh hỗ trợ P2P. VPN đã được kiểm tra cung cấp khả năng bảo vệ tốt hơn cho các hoạt động P2P.

**Vai trò của ping trong việc tăng cường kinh doanh thông qua VPN là gì?**

Việc kinh doanh

Độ trễ thấp rất quan trọng khi sử dụng VPN doanh nghiệp, đặc biệt là cho hội nghị truyền hình, cuộc gọi VoIP và cộng tác thời gian thực. Hãy chọn nhà cung cấp VPN doanh nghiệp có máy chủ được tối ưu hóa và các tính năng chuyên dụng để giảm thiểu độ trễ.

**Những lỗi thường gặp khi cài đặt VPN trên thiết bị với ứng dụng VPN là gì?**

Thiết bị

Những lỗi thường gặp khi sử dụng ứng dụng VPN bao gồm sử dụng ứng dụng lỗi thời, không cấu hình tính năng tự động kết nối, bỏ qua cài đặt ngắt kết nối và tải xuống ứng dụng VPN giả mạo. Luôn tải xuống ứng dụng chính thức từ các nguồn đáng tin cậy và cập nhật thường xuyên.

**Độ trễ có cần thiết để có giao thức VPN tốt hơn không?**

Giao thức

Mặc dù độ trễ không phải là điều mong muốn, nhưng việc hiểu rõ độ trễ sẽ giúp bạn chọn đúng giao thức VPN. WireGuard thường có độ trễ thấp hơn OpenVPN, trong khi IKEv2 được tối ưu hóa cho kết nối di động. Hãy chọn giao thức dựa trên tốc độ và nhu cầu bảo mật của bạn.

**Tại sao tôi nên quan tâm đến WebRTC trong Tính năng nâng cao?**

Sự riêng tư

WebRTC có thể làm rò rỉ địa chỉ IP thực của bạn ngay cả khi sử dụng VPN. Người dùng nâng cao nên tắt WebRTC trên trình duyệt hoặc sử dụng VPN có tính năng bảo vệ chống rò rỉ WebRTC tích hợp. Điều này ngăn chặn vi phạm quyền riêng tư trong các cuộc gọi video và kết nối ngang hàng.

**VPN nào hoạt động với Netflix USA vào năm 2025?**

Phát trực tuyến

Theo các thử nghiệm mới nhất của chúng tôi, máy chủ New Jersey 3 của ExpressVPN, máy chủ Atlanta của NordVPN và máy chủ Los Angeles của Surfshark đều bỏ chặn được Netflix USA ở độ phân giải 4K. VPN miễn phí thường thất bại 100%.

**Làm thế nào để xem BBC iPlayer bên ngoài Vương quốc Anh?**

Phát trực tuyến

Kết nối với máy chủ UK#1847 của NordVPN, xóa cookie trình duyệt và đăng ký với bất kỳ mã bưu chính nào của Vương quốc Anh (ví dụ: SW1A 1AA). Hoạt động trên mọi thiết bị, bao gồm cả Smart TV.

**Tôi có thể sử dụng VPN trên Apple TV không?**

Thiết bị

Apple TV không hỗ trợ trực tiếp các ứng dụng VPN. Thay vào đó, hãy thiết lập VPN trên bộ định tuyến của bạn hoặc sử dụng SmartDNS (MediaStreamer của ExpressVPN hoạt động hoàn hảo).

**VPN nào tốt nhất cho Disney+?**

Phát trực tuyến

Surfshark bỏ chặn hơn 15 thư viện Disney+ (Mỹ, Anh, Nhật Bản, v.v.) với mức giá rẻ nhất. Được kiểm tra hàng ngày—xem bảng điểm VPN Disney+ của chúng tôi.

**Làm thế nào để khắc phục lỗi proxy Netflix?**

Xử lý sự cố

Hãy chuyển sang máy chủ khác, xóa bộ nhớ đệm hoặc sử dụng chế độ ẩn danh. Nếu vẫn bị chặn, hãy liên hệ với trò chuyện trực tiếp để biết máy chủ hoạt động mới nhất - ExpressVPN cập nhật máy chủ của họ hàng giờ.

**VPN kép là gì?**

Trình độ cao

Định tuyến lưu lượng truy cập qua hai máy chủ để mã hóa bổ sung. VPN kép của NordVPN bổ sung mã hóa 2048-bit—lý tưởng cho các nhà báo hoặc nhà hoạt động.

**Làm thế nào để thiết lập VPN trên bộ định tuyến?**

Kỹ thuật

Mua bộ định tuyến đã được flash sẵn từ FlashRouters hoặc cài đặt firmware DD-WRT. Hướng dẫn của chúng tôi bao gồm thiết lập cho Asus, Netgear và Linksys—mất 10 phút.

**Bảo vệ rò rỉ IPv6 là gì?**

Bảo vệ

Tắt lưu lượng IPv6 để ngăn chặn rò rỉ. Bật trong cài đặt của NordVPN—99% VPN bỏ qua tính năng này, gây rò rỉ trên các mạng hỗ trợ IPv6.

**Làm thế nào để khắc phục lỗi VPN không kết nối?**

Xử lý sự cố

Hãy thử các bước sau: Chuyển đổi giao thức (WireGuard → OpenVPN), Đổi DNS thành 8.8.8.8, Tắt tạm thời phần mềm diệt vi-rút/tường lửa, Liên hệ trò chuyện trực tiếp 24/7 để biết trạng thái máy chủ.

**Làm thế nào để nhận ExpressVPN miễn phí?**

Giá cả

Sử dụng chính sách hoàn tiền trong 30 ngày—không cần giải thích. Đăng ký, sử dụng trong 29 ngày, hủy qua trò chuyện trực tiếp và được hoàn tiền đầy đủ. Lặp lại với email mới.

**Có ưu đãi VPN trọn đời không?**

Giá cả

Tránh xa các VPN "trọn đời" vì chúng sẽ đóng cửa hoặc bán dữ liệu. Thay vào đó, hãy chọn gói 2 năm của Surfshark với giá 1,99 đô la/tháng, tương đương giảm giá 90%.

**FBI có thể theo dõi VPN không?**

Sự riêng tư

Nếu VPN không lưu nhật ký (giống như máy chủ chỉ có RAM của ExpressVPN), ngay cả FBI cũng không thể truy xuất dữ liệu. Đã được chứng minh tại tòa án—ExpressVPN không thể giao nộp nhật ký vào năm 2017.

**Lệnh canary là gì?**

Sự riêng tư

Tuyên bố minh bạch được cập nhật hàng tháng. Nếu bị xóa, nó sẽ báo hiệu một trát đòi hầu tòa bí mật. PIA và NordVPN sẽ công khai tuyên bố của họ.

**VPN tốt nhất cho iPhone năm 2025?**

Di động

Ứng dụng iOS của NordVPN bao gồm WireGuard, kill switch và phím tắt Siri. Được đánh giá 4,9/5 trên App Store—tải xuống qua liên kết của chúng tôi để được miễn phí 3 tháng.

**Làm thế nào để sử dụng VPN trên Android TV?**

Thiết bị

Cài đặt Surfshark APK từ trang web của họ (Google Play chặn một số khu vực). Sử dụng ô 'Kết nối nhanh' để truy cập chỉ bằng 1 cú nhấp chuột.

**Sử dụng VPN có hợp pháp không?**

Hợp pháp

Ở hầu hết các quốc gia, VPN hoàn toàn hợp pháp. Tuy nhiên, việc sử dụng chúng cho các hoạt động bất hợp pháp (như hack hoặc tải xuống tài liệu có bản quyền) vẫn là bất hợp pháp. Một số quốc gia (ví dụ: Trung Quốc, Nga, UAE) hạn chế hoặc cấm VPN, vì vậy hãy luôn kiểm tra luật pháp địa phương trước khi đi du lịch.

**VPN có thể giúp tôi ẩn danh trực tuyến không?**

Sự riêng tư

VPN giúp tăng đáng kể quyền riêng tư của bạn nhưng không đảm bảo bạn ẩn danh 100%. Để ẩn danh hoàn toàn, hãy kết hợp VPN không lưu nhật ký với Tor, trình duyệt an toàn và hệ điều hành tập trung vào quyền riêng tư như Tails.

**Sự khác biệt giữa VPN và proxy là gì?**

So sánh

VPN mã hóa toàn bộ lưu lượng truy cập internet của bạn ở cấp độ hệ điều hành, trong khi proxy chỉ chuyển hướng lưu lượng truy cập từ các ứng dụng cụ thể (như trình duyệt của bạn). Proxy không mã hóa dữ liệu, giúp VPN an toàn hơn nhiều.

**VPN có làm chậm tốc độ internet không?**

Hiệu suất

Có, nhưng tối thiểu thôi. Một VPN cao cấp với các giao thức hiện đại như WireGuard có thể làm giảm tốc độ từ 5–10%, trong khi các VPN miễn phí hoặc quá tải có thể làm giảm tốc độ đến 50% hoặc hơn. Việc chọn một máy chủ gần đó sẽ hữu ích.

**Tôi có thể sử dụng VPN trên nhiều thiết bị không?**

Thiết bị

Các VPN hàng đầu cung cấp 5–10 kết nối đồng thời cho mỗi tài khoản. Một số (như Surfshark) cho phép số lượng thiết bị không giới hạn. Hãy xem bảng so sánh của chúng tôi để xem VPN nào hỗ trợ điện thoại, máy tính xách tay, bộ định tuyến và TV thông minh của bạn.

**VPN có bảo vệ chống lại tin tặc không?**

Bảo vệ

Có, đặc biệt là trên Wi-Fi công cộng. VPN mã hóa dữ liệu của bạn, ngăn chặn các cuộc tấn công trung gian. Tuy nhiên, nó không bảo vệ bạn khỏi phần mềm độc hại hoặc lừa đảo - hãy sử dụng phần mềm diệt vi-rút và xác thực hai yếu tố (2FA) cùng với VPN.

**VPN không lưu nhật ký là gì?**

Sự riêng tư

VPN không lưu nhật ký sẽ không lưu trữ bất kỳ dữ liệu nào về hoạt động trực tuyến của bạn. Hãy tìm kiếm các nhà cung cấp được kiểm toán bởi bên thứ ba (như PwC hoặc Cure53) và có trụ sở tại các quốc gia bảo vệ quyền riêng tư (ví dụ: Panama, Thụy Sĩ).

**Tôi có thể bị theo dõi nếu sử dụng VPN không?**

Sự riêng tư

Nếu VPN của bạn có chính sách nghiêm ngặt không lưu nhật ký và không rò rỉ DNS/WebRTC, việc theo dõi sẽ cực kỳ khó khăn. Tuy nhiên, việc đăng nhập vào Google hoặc Facebook vẫn có thể bị nhận dạng - hãy sử dụng chế độ ẩn danh và các dịch vụ tập trung vào quyền riêng tư.

**Kill switch là gì?**

Bảo vệ

Tính năng Kill Switch sẽ ngắt kết nối internet của bạn nếu VPN bị ngắt kết nối, ngăn chặn rò rỉ IP. Luôn bật tính năng này khi tải torrent hoặc truy cập nội dung nhạy cảm.

**VPN miễn phí có an toàn không?**

Giá cả

99% VPN miễn phí đều nguy hiểm. Chúng bán dữ liệu của bạn, chèn quảng cáo hoặc chứa phần mềm độc hại. Ngoại lệ bao gồm gói miễn phí của Proton VPN (số lượng máy chủ hạn chế, không lưu nhật ký). Để an toàn, hãy chọn VPN trả phí có cam kết hoàn tiền.

**Đường hầm chia tách là gì?**

Đặc trưng

Split tunneling cho phép bạn chọn ứng dụng nào sử dụng VPN và ứng dụng nào sử dụng kết nối thông thường của bạn. Tính năng này rất phù hợp cho các ứng dụng ngân hàng chặn VPN trong khi tải torrent an toàn.

**VPN có thể vượt qua được lệnh chặn địa lý của Netflix không?**

Phát trực tuyến

Có, nhưng chỉ những VPN cao cấp như ExpressVPN, NordVPN hoặc Surfshark mới có thể bỏ chặn Netflix, BBC iPlayer và Disney+ một cách ổn định. Hãy xem danh sách các máy chủ đang hoạt động được chúng tôi kiểm tra hàng ngày.

**WireGuard là gì?**

Kỹ thuật

WireGuard là giao thức VPN mới nhất, cung cấp tốc độ nhanh hơn và mã hóa mạnh hơn OpenVPN. Hầu hết các VPN hàng đầu hiện nay đều hỗ trợ giao thức này (ví dụ: NordLynx của NordVPN).

**Làm sao để biết VPN của tôi có hoạt động không?**

Kiểm tra

Truy cập ipleak.net trước và sau khi kết nối. Nếu IP và DNS của bạn thay đổi, tức là nó đang hoạt động. Ngoài ra, hãy kiểm tra xem trình duyệt của bạn có bị rò rỉ WebRTC không.

**Tôi có thể sử dụng VPN để chơi game không?**

Chơi game

Có! VPN giúp giảm thiểu các cuộc tấn công DDoS, vượt qua lệnh cấm IP và cho phép bạn truy cập sớm vào các trò chơi bị khóa theo khu vực. Hãy chọn VPN có máy chủ ping thấp như ExpressVPN hoặc CyberGhost.

**Sự che giấu là gì?**

Trình độ cao

Tính năng che giấu sẽ ngụy trang lưu lượng VPN dưới dạng HTTPS thông thường, vượt qua các lệnh chặn VPN ở các quốc gia như Trung Quốc hoặc Iran. Hãy tìm các tính năng 'chế độ ẩn' hoặc 'OpenVPN Scramble'.

**VPN có hoạt động ở Trung Quốc không?**

Kiểm duyệt

Chỉ một số ít VPN (ví dụ: ExpressVPN, Astrill, NordVPN) hoạt động đáng tin cậy tại Trung Quốc nhờ tính năng Kiểm tra Gói Sâu (Deep Packet Inspection). Hãy luôn tải xuống VPN trước khi đi du lịch.

**Tôi có thể tải torrent bằng VPN không?**

P2P

Có, nhưng chỉ sử dụng máy chủ được tối ưu hóa P2P và bật tính năng ngắt kết nối. Lựa chọn hàng đầu của chúng tôi: NordVPN, Surfshark và Private Internet Access—tất cả đều có tính năng chuyển tiếp cổng và không giới hạn băng thông.

**IP chuyên dụng là gì?**

Đặc trưng

IP chuyên dụng là địa chỉ IP chỉ bạn sử dụng, giúp giảm thiểu CAPTCHA và danh sách đen. Hữu ích cho giao dịch ngân hàng hoặc làm việc từ xa. Có sẵn dưới dạng tiện ích bổ sung với NordVPN, CyberGhost và PureVPN.

**Chi phí cho VPN là bao nhiêu?**

Giá cả

Giá VPN cao cấp dao động từ 2 đến 12 đô la/tháng tùy thuộc vào thời hạn gói. Ưu đãi độc quyền của chúng tôi giảm giá xuống còn 1,99 đô la/tháng (gói Surfshark 2 năm) kèm 3 tháng miễn phí.

**Tôi có thể thanh toán cho VPN một cách ẩn danh không?**

Sự riêng tư

Có, các VPN hàng đầu chấp nhận Bitcoin, Monero hoặc tiền mặt. Mullvad thậm chí còn tạo số tài khoản—không cần email.

**Liên minh Five/Nine/Fourteen Eyes là gì?**

Sự riêng tư

Đây là các thỏa thuận chia sẻ thông tin tình báo giữa các quốc gia. Tránh sử dụng VPN có trụ sở tại các khu vực pháp lý này (ví dụ: Hoa Kỳ, Vương quốc Anh) trừ khi họ có chính sách không lưu nhật ký đã được chứng minh (như PIA).

**VPN có thể vượt qua được việc giới hạn băng thông của ISP không?**

Hiệu suất

Có, nếu ISP của bạn hạn chế tốc độ phát trực tuyến (ví dụ: Netflix), VPN sẽ ẩn lưu lượng truy cập của bạn, khôi phục tốc độ tối đa. Hãy thử nghiệm có và không có VPN để xác nhận.

**VPN nào tốt nhất cho người mới bắt đầu?**

Khuyến nghị

CyberGhost và ExpressVPN có ứng dụng 1 cú nhấp chuột, hỗ trợ 24/7 và không cần thiết lập. Hoàn hảo cho người dùng không rành công nghệ.

**Tại sao mọi người nên sử dụng VPN để duyệt web hàng ngày?**

Thông tin chung về VPN

Sử dụng VPN để duyệt web hàng ngày giúp tăng cường quyền riêng tư và bảo mật trực tuyến của bạn. VPN mã hóa lưu lượng truy cập internet, ngăn chặn các nhà cung cấp dịch vụ Internet (ISP), nhà quảng cáo hoặc tin tặc theo dõi hoạt động của bạn. Điều này đặc biệt quan trọng trên các mạng không an toàn như Wi-Fi công cộng tại quán cà phê hoặc sân bay, nơi nguy cơ đánh cắp dữ liệu là rất cao. VPN cũng cho phép bạn vượt qua các giới hạn địa lý, truy cập nội dung như video YouTube bị giới hạn theo khu vực hoặc các trang web tin tức. Ví dụ: bạn có thể duyệt web ẩn danh, mua vé máy bay giá rẻ hoặc xem các chương trình truyền hình quốc tế. Năm 2025, với tình trạng vi phạm dữ liệu ngày càng gia tăng, VPN bổ sung thêm một lớp bảo vệ. ExpressVPN, nổi tiếng với tốc độ và độ tin cậy, là một lựa chọn tuyệt vời để duyệt web liền mạch trên nhiều thiết bị. Giao diện trực quan của nó phù hợp với mọi người dùng.

**VPN cải thiện bảo mật trực tuyến cho người mới bắt đầu như thế nào?**

Thông tin chung về VPN

Đối với người mới bắt đầu, VPN đơn giản hóa bảo mật trực tuyến bằng cách mã hóa kết nối internet của bạn, giúp bảo vệ dữ liệu nhạy cảm như mật khẩu hoặc thông tin thẻ tín dụng khỏi tin tặc. Nó che giấu địa chỉ IP của bạn, khiến các trang web hoặc trình theo dõi khó nhận dạng bạn hơn. Điều này đặc biệt hữu ích trên Wi-Fi công cộng, nơi các cuộc tấn công mạng thường xuyên xảy ra. VPN cũng chặn các quảng cáo và trình theo dõi xâm nhập, mang lại trải nghiệm duyệt web mượt mà hơn. Vào năm 2025, khi tội phạm mạng gây thiệt hại hàng tỷ đô la mỗi năm, ngay cả người dùng thông thường cũng được hưởng lợi từ sự bảo vệ này. CyberGhost cung cấp giao diện dễ sử dụng với các cài đặt bảo mật được cấu hình sẵn, lý tưởng cho người mới bắt đầu. Chính sách không lưu nhật ký của nó đảm bảo dữ liệu của bạn được bảo mật. Bằng cách khám phá các tùy chọn như CyberGhost, bạn có thể bắt đầu bảo mật các hoạt động trực tuyến của mình mà không cần chuyên môn kỹ thuật.

**Sự khác biệt giữa VPN và máy chủ proxy là gì?**

Thông tin chung về VPN

VPN và máy chủ proxy đều ẩn địa chỉ IP của bạn, nhưng chúng có sự khác biệt đáng kể. VPN mã hóa toàn bộ lưu lượng internet của bạn, định tuyến qua một máy chủ an toàn, đảm bảo quyền riêng tư và bảo mật trên các ứng dụng và trang web. Proxy chỉ chuyển hướng một số lưu lượng cụ thể (ví dụ: dữ liệu trình duyệt) mà không mã hóa, khiến bạn dễ bị theo dõi. VPN lý tưởng cho các tác vụ nhạy cảm như giao dịch ngân hàng hoặc vượt qua các hạn chế địa lý, trong khi proxy tốt hơn cho việc truy cập nhanh chóng, không nhạy cảm vào các trang web bị chặn. Ví dụ: VPN cho phép bạn phát trực tuyến Netflix một cách an toàn, trong khi proxy thì không. PureVPN cung cấp các kết nối được mã hóa với giá cả phải chăng với máy chủ tại hơn 70 quốc gia, khiến nó trở thành lựa chọn tốt hơn proxy.

**VPN có thể ẩn lịch sử duyệt web của tôi khỏi ISP không?**

Thông tin chung về VPN

Đúng vậy, VPN ẩn lịch sử duyệt web của bạn khỏi ISP bằng cách mã hóa lưu lượng truy cập và định tuyến qua một máy chủ từ xa. Điều này ngăn ISP biết bạn truy cập trang web nào hoặc làm gì trực tuyến, bảo vệ quyền riêng tư của bạn. Ví dụ: nếu bạn đang phát trực tuyến hoặc tìm hiểu các chủ đề nhạy cảm, VPN sẽ giữ hoạt động của bạn ở chế độ riêng tư. Vào năm 2025, khi các ISP ngày càng kiếm tiền từ dữ liệu người dùng, đây là một lợi ích quan trọng. NordVPN, với chính sách không lưu nhật ký đã được kiểm toán, đảm bảo ngay cả nhà cung cấp VPN cũng không thể thấy hoạt động của bạn. Hơn 5.500 máy chủ của NordVPN mang đến sự linh hoạt cho việc duyệt web riêng tư. Bằng cách lựa chọn một dịch vụ như NordVPN, bạn có thể kiểm soát dấu vết kỹ thuật số của mình và duyệt web thoải mái mà không phải lo lắng.

**Tôi có cần VPN khi sử dụng Wi-Fi tại nhà không?**

Thông tin chung về VPN

Mặc dù Wi-Fi tại nhà thường an toàn hơn mạng công cộng, VPN vẫn mang lại sự bảo vệ đáng giá. Nó mã hóa dữ liệu của bạn, ngăn chặn tin tặc khai thác lỗ hổng bảo mật của bộ định tuyến hoặc đánh cắp thông tin nhạy cảm như thông tin đăng nhập. Nó cũng ngăn chặn các nhà cung cấp dịch vụ Internet (ISP) theo dõi thói quen duyệt web của bạn để phục vụ cho các quảng cáo nhắm mục tiêu. Ví dụ: nếu bạn mua sắm trực tuyến hoặc quản lý tài chính tại nhà, VPN sẽ đảm bảo dữ liệu của bạn luôn an toàn. Ngoài ra, nó còn mở khóa nội dung bị hạn chế về mặt địa lý như các nền tảng phát trực tuyến quốc tế. ExpressVPN cung cấp kết nối nhanh chóng, đáng tin cậy cho nhu cầu sử dụng tại nhà, với các ứng dụng dành cho bộ định tuyến và thiết bị. Thiết lập thân thiện với người dùng giúp bạn dễ dàng bảo mật toàn bộ mạng của mình.

Hiển thị 114 trong số 114 câu hỏi thường gặp