**VPN چیست و چگونه کار می‌کند؟**

مبانی

یک VPN (شبکه خصوصی مجازی) یک اتصال امن و رمزگذاری شده بین دستگاه شما و اینترنت ایجاد می‌کند و ترافیک را از طریق یک سرور از راه دور مسیریابی می‌کند تا آدرس IP شما را پنهان کند. این امر داده‌های شما را از هکرها، ISPها و ردیاب‌ها محافظت می‌کند و حریم خصوصی را تضمین می‌کند. در سال 2025، VPNها به دلیل افزایش تهدیدات سایبری، ردیابی گسترده داده‌ها و افزایش محدودیت‌های محتوا حیاتی هستند. آنها برای مرور ایمن در Wi-Fi عمومی، دسترسی به محتوای مسدود شده جغرافیایی مانند کتابخانه‌های Netflix و دور زدن سانسور در مناطق محدودکننده عالی هستند.

**توصیه ما: ExpressVPN**

۴.۹/۵

VPN پیشرو در صنعت با رمزگذاری درجه نظامی و سرعت فوق العاده بالا در بیش از ۹۴ کشور.

ضمانت 30 روزهپشتیبانی 24/7سیاست عدم ثبت وقایع5 دستگاه

🎉 ۴۹٪ تخفیف + ۳ ماه اشتراک رایگان

ExpressVPN بدون ریسک را امتحان کنید

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**آیا استفاده از VPN قانونی است؟**

قانونی

VPN ها در اکثر کشورهای جهان، از جمله ایالات متحده، کانادا، انگلستان و اکثر کشورهای اروپایی قانونی هستند. با این حال، برخی از کشورها مانند چین، روسیه و ایران محدودیت‌ها یا ممنوعیت‌هایی برای استفاده از VPN دارند. همیشه قبل از استفاده از VPN، قوانین محلی را بررسی کنید.

راهنماهای مرتبط:

[راهنمای قوانین VPN بر اساس کشور](https://bestvpn.digital/guides/vpn-laws-by-country)

[راهنمای کامل قانونی بودن VPN در کشورها و مناطق مختلف](https://bestvpn.digital/guides/vpn-laws-by-country)

[نکات قانونی استفاده از VPN](https://bestvpn.digital/guides/legal-vpn-usage)

[بهترین شیوه‌ها برای استفاده قانونی و مسئولانه از VPNها](https://bestvpn.digital/guides/legal-vpn-usage)

**پیشنهاد ما: NordVPN**

۴.۸/۵

VPN بدون گزارش حسابرسی شده با ویژگی‌های امنیتی پیشرفته و شبکه سرور جهانی.

دو دستگاه سوئیچ VPNCyberSecKill

🎉 ۶۸٪ تخفیف + ۳ ماه اشتراک رایگان

همین حالا NordVPN را دریافت کنید

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**آیا VPN ها سرعت اینترنت را کاهش می دهند؟**

عملکرد

VPN ها می‌توانند به دلیل سربار رمزگذاری و مسافت اضافی که داده‌ها از طریق سرورهای VPN طی می‌کنند، سرعت اینترنت را کاهش دهند. با این حال، VPN های پریمیوم معمولاً باعث کاهش حداقل سرعت (5-15٪) می‌شوند و برخی حتی ممکن است با دور زدن محدودیت ISP سرعت را بهبود بخشند.

راهنماهای مرتبط:

[نتایج تست سرعت VPN](https://bestvpn.digital/guides/vpn-speed-tests)

[تست‌های سرعت در دنیای واقعی برای مقایسه ارائه دهندگان برتر VPN](https://bestvpn.digital/guides/vpn-speed-tests)

[چگونه سرعت VPN را بهینه کنیم](https://bestvpn.digital/guides/optimize-vpn-speed)

[نکات و ترفندهایی برای به حداکثر رساندن سرعت اتصال VPN شما](https://bestvpn.digital/guides/optimize-vpn-speed)

**توصیه ما: Surfshark**

۴.۷/۵

دستگاه‌های نامحدود با پروتکل WireGuard برای حداکثر سرعت و امنیت.

دستگاه‌های نامحدود، WireGuardCleanWebMultiHop

🎉 ۸۲٪ تخفیف + ۲ ماه اشتراک رایگان

با Surfshark شروع کنید

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**آیا می‌توانم از VPN برای پخش Netflix، Hulu و سایر سرویس‌ها استفاده کنم؟**

پخش جریانی

بسیاری از VPN ها می‌توانند به محتوای محدود جغرافیایی در پلتفرم‌های استریم دسترسی پیدا کنند، اما همه VPN ها با هر سرویس استریمی به طور قابل اعتمادی کار نمی‌کنند. به دنبال VPN هایی باشید که به طور خاص قابلیت‌های استریم را تبلیغ می‌کنند و سرورهایی دارند که برای پلتفرم‌های محبوب بهینه شده‌اند.

راهنماهای مرتبط:

[بهترین VPN ها برای Netflix](https://bestvpn.digital/guides/best-vpns-for-netflix)

[سرویس‌های برتر VPN که محتوای Netflix را به طور قابل اعتمادی از حالت انسداد خارج می‌کنند](https://bestvpn.digital/guides/best-vpns-for-netflix)

[راهنمای راه اندازی نتفلیکس وی پی ان](https://bestvpn.digital/guides/netflix-vpn-setup)

[راهنمای گام به گام برای پخش Netflix با VPN](https://bestvpn.digital/guides/netflix-vpn-setup)

**توصیه ما: ExpressVPN**

۴.۹/۵

بهترین VPN برای Netflix با سرورهای جریان بهینه شده و پشتیبانی از 4K.

رفع انسداد Netflix، پخش 4K، DNS هوشمند، پشتیبانی از روتر

🎉 ۴۹٪ تخفیف + ۳ ماه اشتراک رایگان

پخش Netflix با ExpressVPN

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**تفاوت بین VPN های رایگان و پولی چیست؟**

قیمت‌گذاری

VPN های رایگان معمولاً سرورهای محدود، سرعت پایین‌تر، محدودیت حجم داده و ویژگی‌های امنیتی کمتری دارند. آنها همچنین ممکن است داده‌های کاربر را ثبت کنند یا تبلیغات نشان دهند. VPN های پولی امنیت بهتر، سرعت بالاتر، سرورهای بیشتر و سیاست‌های حفظ حریم خصوصی قوی‌تری را با تضمین عدم ثبت اطلاعات ارائه می‌دهند.

راهنماهای مرتبط:

[مقایسه WireGuard در مقابل OpenVPN](https://bestvpn.digital/guides/wireguard-vs-openvpn)

[مقایسه دقیق دو پروتکل محبوب VPN](https://bestvpn.digital/guides/wireguard-vs-openvpn)

[راهنمای امنیت پروتکل VPN](https://bestvpn.digital/guides/vpn-protocol-security)

[درک پروتکل‌های مختلف VPN و ویژگی‌های امنیتی آنها](https://bestvpn.digital/guides/vpn-protocol-security)

**پیشنهاد ما: NordVPN**

۴.۸/۵

انتخاب پروتکل پیشرفته از جمله NordLynx (WireGuard) برای عملکرد بهینه.

پروتکل NordLynx پروتکل‌های سفارشی OpenVPNIKEv2

🎉 ۶۸٪ تخفیف + ۳ ماه اشتراک رایگان

پروتکل‌های NordVPN را انتخاب کنید

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**چند دستگاه را می‌توانم به یک VPN وصل کنم؟**

دستگاه‌ها

این بسته به ارائه دهنده متفاوت است. برخی از VPN ها امکان اتصال همزمان 5 تا 10 را فراهم می کنند، در حالی که برخی دیگر مانند Surfshark و IPVanish اتصالات نامحدود ارائه می دهند. اگر دستگاه های زیادی دارید، قبل از انتخاب VPN، محدودیت دستگاه را بررسی کنید.

**پیشنهاد ما: CyberGhost**

۴.۶/۵

برنامه‌های تلفن همراه کاربرپسند با اتصال با یک کلیک و سرورهای بهینه‌شده.

برنامه‌های موبایل آساناتصال خودکار7 دستگاهضمانت 45 روزه

🎉 ۸۴٪ تخفیف + ۴ ماه اشتراک رایگان

دریافت CyberGhost موبایل

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**سیاست VPN بدون گزارش چیست؟**

حریم خصوصی

سیاست عدم ثبت اطلاعات به این معنی است که ارائه دهنده VPN هیچ اطلاعاتی در مورد فعالیت‌های آنلاین، زمان اتصال، آدرس‌های IP یا سابقه مرور شما ثبت یا ذخیره نمی‌کند. این امر حریم خصوصی شما را تضمین می‌کند، حتی اگر شرکت VPN به خطر بیفتد یا از نظر قانونی مجبور به اشتراک‌گذاری داده‌ها شود.

**توصیه ما: Surfshark**

۴.۷/۵

مقرون به صرفه ترین VPN پریمیوم با تعداد نامحدود دستگاه و تمام ویژگی های موجود.

تعداد نامحدود دستگاه، تمام ویژگی‌ها، ضمانت 30 روزه، پشتیبانی 24 ساعته

🎉 ۸۲٪ تخفیف + ۲ ماه اشتراک رایگان

بهترین پیشنهاد VPN را دریافت کنید

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**از کدام پروتکل VPN باید استفاده کنم؟**

فنی

بهترین پروتکل‌ها WireGuard (سریع‌ترین و مدرن‌ترین)، OpenVPN (امن‌ترین و گسترده‌ترین پشتیبانی) و IKEv2 (عالی برای موبایل) هستند. از PPTP اجتناب کنید زیرا قدیمی و ناامن است. اکثر کاربران باید WireGuard را در صورت موجود بودن انتخاب کنند.

راهنماهای مرتبط:

[بهترین VPN ها برای تورنت](https://bestvpn.digital/guides/best-vpns-for-torrenting)

[سرویس‌های برتر VPN سازگار با P2P با پشتیبانی از ارسال پورت](https://bestvpn.digital/guides/best-vpns-for-torrenting)

[راهنمای تورنت ایمن](https://bestvpn.digital/guides/safe-torrenting-guide)

[چگونه با VPN به صورت ایمن و ناشناس تورنت کنیم](https://bestvpn.digital/guides/safe-torrenting-guide)

**توصیه ما: ExpressVPN**

۴.۹/۵

سرورهای بهینه شده P2P با قابلیت ارسال پورت و سیاست سختگیرانه عدم ثبت گزارش برای تورنت ایمن.

سرورهای P2P، ارسال پورت، سوئیچ Kill، هیچ گزارشی حسابرسی نشده است

🎉 ۴۹٪ تخفیف + ۳ ماه اشتراک رایگان

تورنت ایمن با ExpressVPN

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**آیا می‌توانم از VPN روی روتر خود استفاده کنم؟**

فنی

بله، بسیاری از ارائه دهندگان VPN از نصب روتر پشتیبانی می‌کنند که از تمام دستگاه‌های موجود در شبکه شما محافظت می‌کند. شما به یک روتر سازگار نیاز دارید که از کلاینت‌های VPN پشتیبانی کند، یا می‌توانید یک روتر VPN از پیش پیکربندی شده خریداری کنید. این به عنوان یک اتصال برای محدودیت‌های دستگاه محسوب می‌شود.

راهنماهای مرتبط:

[سوئیچ kill VPN توضیح داده شده است](https://bestvpn.digital/guides/vpn-kill-switch-guide)

[راهنمای کامل سوئیچ‌های kill VPN و نحوه محافظت آنها از شما](https://bestvpn.digital/guides/vpn-kill-switch-guide)

[ویژگی‌های امنیتی VPN](https://bestvpn.digital/guides/vpn-security-features)

[ویژگی‌های امنیتی ضروری که باید در یک سرویس VPN جستجو کنید](https://bestvpn.digital/guides/vpn-security-features)

**پیشنهاد ما: NordVPN**

۴.۸/۵

فناوری پیشرفته kill switch که در صورت قطع VPN، فوراً اینترنت را مسدود می‌کند.

سوئیچ kill برنامه، سوئیچ kill سیستم، اتصال مجدد خودکار، محافظت در برابر نشت DNS

🎉 ۶۸٪ تخفیف + ۳ ماه اشتراک رایگان

با NordVPN Kill Switch ایمن شوید

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**آیا برای دستگاه‌های تلفن همراه به VPN نیاز دارم؟**

موبایل

بله، VPN های موبایل برای محافظت از اطلاعات شما در Wi-Fi عمومی، جلوگیری از ردیابی موبایل و دسترسی به محتوای محدود شده جغرافیایی مهم هستند. اکثر ارائه دهندگان VPN، برنامه های موبایل اختصاصی برای iOS و اندروید با همان ویژگی های امنیتی نسخه های دسکتاپ ارائه می دهند.

راهنماهای مرتبط:

[مقایسه VPN رایگان در مقابل پولی](https://bestvpn.digital/guides/free-vs-paid-vpn)

[چرا VPN های پولی ارزش سرمایه‌گذاری نسبت به گزینه‌های رایگان را دارند؟](https://bestvpn.digital/guides/free-vs-paid-vpn)

[ضمانت‌های آزمایشی VPN و بازگشت وجه](https://bestvpn.digital/guides/vpn-trials-guarantees)

[چگونه VPN های پریمیوم بدون ریسک را با دوره های آزمایشی امتحان کنیم](https://bestvpn.digital/guides/vpn-trials-guarantees)

**پیشنهاد ما: CyberGhost**

۴.۶/۵

VPN پریمیوم با ضمانت بازگشت وجه ۴۵ روزه - طولانی‌تر از هر دوره آزمایشی رایگان.

ضمانت ۴۵ روزه بدون محدودیت داده، امکانات کامل، ۷ دستگاه

🎉 ۸۴٪ تخفیف + ۴ ماه اشتراک رایگان

CyberGhost را بدون ریسک امتحان کنید

ضمانت بازگشت وجه ۳۰ روزه • سیاست عدم ثبت گزارش • پشتیبانی ۲۴ ساعته

**تونل سازی اسپلیت چیست؟**

ویژگی‌ها

تونل‌سازی اسپلیت به شما این امکان را می‌دهد که بخشی از ترافیک اینترنت خود را از طریق VPN هدایت کنید و در عین حال به سایر ترافیک اجازه دهید مستقیماً به اینترنت دسترسی داشته باشند. این برای دسترسی به سرویس‌های محلی و در عین حال حفظ محافظت VPN برای فعالیت‌های حساس مفید است.

**چگونه بهترین مکان سرور VPN را انتخاب کنم؟**

کاربرد

**سوئیچ kill چیست و چرا به آن نیاز دارم؟**

امنیت

اگر اتصال VPN به طور غیرمنتظره‌ای قطع شود، یک سوئیچ kill به طور خودکار اتصال اینترنت شما را قطع می‌کند. این کار از افشای آدرس IP واقعی و داده‌های رمزگذاری نشده شما جلوگیری می‌کند. این برای حفظ حریم خصوصی و امنیت ضروری است.

**آیا VPN ها قابل شناسایی هستند؟**

حریم خصوصی

بله، VPN ها گاهی اوقات از طریق روش‌های مختلفی از جمله لیست‌های سیاه IP، بازرسی عمیق بسته‌ها و تجزیه و تحلیل رفتاری قابل شناسایی هستند. برخی از VPN ها ویژگی‌های مبهم‌سازی را برای پنهان کردن استفاده از VPN ارائه می‌دهند که تشخیص را بسیار سخت‌تر می‌کند.

**آیا استفاده از VPN خطراتی دارد؟**

امنیت

خطرات شامل انتخاب یک ارائه‌دهنده غیرقابل اعتماد که داده‌ها را ثبت می‌کند، بدافزار در برنامه‌های VPN جعلی، سرعت اینترنت پایین‌تر و ناسازگاری احتمالی با برخی سرویس‌ها می‌شود. همیشه ارائه‌دهندگان VPN معتبر و حسابرسی‌شده با سیاست‌های حفظ حریم خصوصی قوی را انتخاب کنید.

**چقدر باید برای VPN هزینه کنم؟**

قیمت‌گذاری

VPN های با کیفیت معمولاً 2 تا 12 دلار در ماه هزینه دارند و اشتراک های طولانی تر ارزش بهتری ارائه می دهند. قیمت های کمتر از 2 دلار در ماه ممکن است نشان دهنده عدم امنیت یا ویژگی های مناسب باشد. برای صرفه جویی، طرح های سالانه را در نظر بگیرید، اما برای آزمایش سرویس، با دوره های کوتاه تر شروع کنید.

**آیا می‌توانم از VPN برای تورنت استفاده کنم؟**

همتا به همتا

بسیاری از VPN ها از ترافیک P2P و تورنت پشتیبانی می‌کنند، اما نه همه آنها. به دنبال VPN هایی با سرورهای اختصاصی P2P، رمزگذاری قوی، سیاست‌های عدم ثبت گزارش و سوئیچ‌های kill باشید. برخی از ارائه دهندگان به طور خاص تورنت را مجاز می‌دانند در حالی که برخی دیگر آن را ممنوع می‌کنند.

**تفاوت VPN و پروکسی چیست؟**

مقایسه

VPN ها تمام ترافیک اینترنت شما را رمزگذاری می‌کنند و در کل سیستم کار می‌کنند، در حالی که پروکسی‌ها فقط ترافیک را از برنامه‌های خاص و بدون رمزگذاری هدایت می‌کنند. VPN ها امنیت و محافظت از حریم خصوصی بسیار بهتری نسبت به پروکسی‌ها ارائه می‌دهند.

**آیا VPN ها در چین کار می کنند؟**

سانسور

استفاده از VPN در چین محدود شده است و فایروال بزرگ چین بسیاری از سرویس‌های VPN را مسدود می‌کند. برخی از VPN ها هنوز با فناوری‌های خاص مبهم‌سازی کار می‌کنند، اما قابلیت اطمینان آنها می‌تواند ناپایدار باشد. گزارش‌های فعلی را بررسی کنید و VPN هایی را انتخاب کنید که قابلیت‌های اثبات شده‌ای برای دور زدن چین دارند.

**آیا می‌توانم با VPN یک IP اختصاصی دریافت کنم؟**

ویژگی‌ها

بله، برخی از ارائه دهندگان VPN آدرس‌های IP اختصاصی/استاتیک را با هزینه اضافی ارائه می‌دهند. این به شما هر بار که متصل می‌شوید، آدرس IP یکسانی می‌دهد که می‌تواند برای دسترسی به سرویس‌های دارای محدودیت IP یا اجتناب از CAPTCHA مفید باشد.

**چگونه می‌توانم آزمایش کنم که آیا VPN من کار می‌کند؟**

آزمایش

قبل و بعد از اتصال، آدرس IP خود را بررسی کنید تا مطمئن شوید که تغییر می‌کند. با استفاده از ابزارهای آنلاین، نشت DNS را آزمایش کنید، تأیید کنید که مکان شما به عنوان مکان سرور VPN ظاهر می‌شود و با قطع اتصال VPN، از عملکرد سوئیچ kill اطمینان حاصل کنید.

**اگر فراموش کنم VPN خود را روشن کنم چه اتفاقی می‌افتد؟**

کاربرد

آدرس IP واقعی و موقعیت مکانی شما قابل مشاهده خواهد بود، ISP شما می‌تواند ترافیک شما را ببیند و شما محافظت VPN نخواهید داشت. برخی از VPN ها ویژگی‌های اتصال خودکار را ارائه می‌دهند که هنگام اتصال به اینترنت یا شبکه‌های غیر قابل اعتماد، VPN را به طور خودکار شروع می‌کنند.

**آیا کارفرمایان می‌توانند فعالیت اینترنتی من را با VPN ببینند؟**

حریم خصوصی

اگر از تجهیزات یا شبکه‌های شرکت استفاده می‌کنید، کارفرمایان ممکن است همچنان فعالیت شما را از طریق روش‌های دیگری مانند نرم‌افزار نظارت بر نقاط پایانی، حتی با VPN، رصد کنند. VPN های شخصی روی دستگاه‌های شخصی، حریم خصوصی بهتری را در برابر رصد کارفرما فراهم می‌کنند.

**آیا در صورت داشتن VPN به آنتی ویروس نیاز دارم؟**

امنیت

VPN و آنتی ویروس اهداف متفاوتی دارند. VPN از حریم خصوصی و داده‌های در حال انتقال محافظت می‌کند، در حالی که آنتی ویروس در برابر بدافزارها و فایل‌های مخرب محافظت می‌کند. شما باید از هر دو برای محافظت جامع استفاده کنید - آنها مکمل یکدیگر هستند.

**دابل VPN یا چند هاپ چیست؟**

پیشرفته

VPN دوگانه ترافیک شما را از طریق دو سرور VPN به جای یک سرور هدایت می‌کند، یک لایه رمزگذاری اضافی اضافه می‌کند و ردیابی فعالیت آنلاین شما را بسیار دشوار می‌کند. با این حال، سرعت را به میزان قابل توجهی کاهش می‌دهد و معمولاً برای اکثر کاربران بیش از حد است.

**آیا می‌توانم از VPN با تلویزیون‌های هوشمند استفاده کنم؟**

دستگاه‌ها

بله، شما می‌توانید با نصب VPN روی روتر خود، اشتراک‌گذاری اتصال VPN از رایانه خود یا استفاده از دستگاه‌های پخش موسیقی/تلویزیون‌های اپل مجهز به VPN، از VPN در تلویزیون‌های هوشمند استفاده کنید. برخی از تلویزیون‌های هوشمند نیز مستقیماً از برنامه‌های VPN پشتیبانی می‌کنند.

**مبهم‌سازی در VPN چیست؟**

پیشرفته

مبهم‌سازی، ترافیک VPN را طوری پنهان می‌کند که شبیه ترافیک HTTPS معمولی به نظر برسد و به دور زدن بلوک‌های VPN در کشورها یا شبکه‌های محدودکننده کمک کند. به این حالت، حالت مخفی نیز گفته می‌شود و در کشورهایی با سانسور اینترنت مفید است.

**هر چند وقت یکبار باید سرورهای VPN را تغییر دهم؟**

کاربرد

هیچ قانون مشخصی وجود ندارد، اما اگر سرعت اینترنت شما پایین است، اگر سرور توسط سرویسی که می‌خواهید به آن دسترسی داشته باشید مسدود شده است، یا به صورت دوره‌ای برای حفظ حریم خصوصی بیشتر، ممکن است بخواهید سرورها را تغییر دهید. بسیاری از کاربران چند سرور ترجیحی پیدا می‌کنند و به آنها پایبند می‌مانند.

**آیا می‌توانم از VPN برای بازی استفاده کنم؟**

بازی

می‌توان از VPNها برای بازی استفاده کرد تا پینگ به سرورهای خاص را کاهش دهند، محدودیت‌های جغرافیایی را دور بزنند، از حملات DDoS جلوگیری کنند یا زودتر به بازی‌ها در مناطق مختلف دسترسی پیدا کنند. با این حال، VPNها ممکن است تأخیر را افزایش دهند، بنابراین سرورهایی را انتخاب کنید که به سرورهای بازی نزدیک باشند.

**نشت DNS چیست و چگونه می‌توانم از آن جلوگیری کنم؟**

امنیت

نشت DNS زمانی رخ می‌دهد که درخواست‌های DNS شما از تونل VPN عبور می‌کنند و فعالیت مرور شما را برای ISP شما آشکار می‌کنند. با استفاده از VPNهایی که دارای محافظت داخلی در برابر نشت DNS هستند، تغییر تنظیمات DNS یا استفاده از سرورهای DNS VPN از آن جلوگیری کنید.

**آیا VPN ها مخصوص کسب و کارها وجود دارند؟**

کسب و کار

بله، VPN های تجاری امکاناتی مانند مدیریت متمرکز، آدرس‌های IP اختصاصی، حساب‌های تیمی، افزایش اتصالات همزمان و امنیت در سطح سازمانی را ارائه می‌دهند. آنها معمولاً هزینه بیشتری دارند اما کنترل و پشتیبانی بهتری ارائه می‌دهند.

**IPv6 چیست و آیا VPN ها از آن پشتیبانی می کنند؟**

فنی

IPv6 پروتکل اینترنتی جدیدتری است که جایگزین IPv4 شده است. همه VPN ها از IPv6 پشتیبانی نمی‌کنند، که می‌تواند باعث نشت IPv6 شود. به دنبال VPN هایی باشید که یا از IPv6 پشتیبانی می‌کنند یا ترافیک IPv6 را برای جلوگیری از نشت مسدود می‌کنند، زیرا اکثر کاربران هنوز در درجه اول از IPv4 استفاده می‌کنند.

**آیا می‌توانم سرور VPN خودم را راه‌اندازی کنم؟**

خودتان انجام دهید

بله، شما می‌توانید با استفاده از سرویس‌های ابری مانند AWS یا DigitalOcean یا روی روتر خانگی خود، یک سرور VPN شخصی راه‌اندازی کنید. با این حال، این کار حریم خصوصی را از ISPها فراهم می‌کند اما ناشناس بودن را تضمین نمی‌کند، زیرا سرور به شما متصل است. VPNهای تجاری ناشناس بودن بهتری ارائه می‌دهند.

**WireGuard چیست و چرا محبوب است؟**

فنی

WireGuard یک پروتکل VPN مدرن است که سریع‌تر، امن‌تر و از باتری کمتری نسبت به پروتکل‌های قدیمی‌تر مانند OpenVPN استفاده می‌کند. این پروتکل کد ساده‌تری دارد (که ممیزی آن را آسان‌تر می‌کند)، عملکرد بهتری دارد و در حال تبدیل شدن به انتخاب ارجح بسیاری از ارائه‌دهندگان VPN است.

**آیا VPN ها در برابر بدافزار محافظت می کنند؟**

امنیت

VPN ها در درجه اول از طریق رمزگذاری از داده‌های در حال انتقال محافظت می‌کنند، نه در برابر بدافزار. با این حال، برخی از VPN ها شامل ویژگی‌های امنیتی اضافی مانند مسدودکننده‌های تبلیغات، محافظت در برابر بدافزار و مسدود کردن وب‌سایت‌های خطرناک هستند. شما هنوز به محافظت جداگانه از آنتی ویروس نیاز دارید.

**آیا می‌توانم از VPN برای دریافت قیمت‌های آنلاین ارزان‌تر استفاده کنم؟**

خرید

برخی از سرویس‌های آنلاین قیمت‌های متفاوتی را بر اساس موقعیت مکانی نشان می‌دهند، بنابراین تغییر سرور VPN شما ممکن است قیمت‌های متفاوتی را نشان دهد. با این حال، این ممکن است شرایط خدمات را نقض کند و روش‌های پرداخت اغلب به هر حال موقعیت واقعی شما را فاش می‌کنند.

**بهترین VPN برای مبتدیان چیست؟**

توصیه‌ها

VPN های مناسب برای مبتدیان باید دارای برنامه های کاربردی آسان، اتصالات قابل اعتماد، پشتیبانی خوب از مشتری و سیاست های حفظ حریم خصوصی واضح باشند. ExpressVPN، NordVPN و Surfshark به دلیل رابط های کاربرپسند خود، انتخاب های محبوبی برای مبتدیان هستند.

**چگونه اشتراک VPN خود را لغو کنم؟**

حساب کاربری

روش‌های لغو اشتراک بسته به ارائه‌دهنده متفاوت است. اکثر آنها امکان لغو اشتراک را از طریق داشبورد حساب کاربری شما فراهم می‌کنند، برخی نیاز به تماس با پشتیبانی مشتری دارند. قبل از اشتراک، سیاست لغو اشتراک و شرایط ضمانت بازگشت وجه را بررسی کنید. سوابق لغو اشتراک خود را نگه دارید.

**پورت فورواردینگ در VPN چیست؟**

پیشرفته

فوروارد کردن پورت به اتصالات خارجی اجازه می‌دهد تا از طریق اتصال VPN به پورت‌های خاصی در دستگاه شما دسترسی پیدا کنند. این قابلیت برای میزبانی سرورها، بهبود اتصالات P2P یا دسترسی از راه دور به دستگاه‌ها مفید است. همه VPNها از فوروارد کردن پورت پشتیبانی نمی‌کنند.

**آیا می‌توانم همزمان از چندین VPN استفاده کنم؟**

پیشرفته

اگرچه از نظر فنی امکان‌پذیر است، اما استفاده همزمان از چندین VPN (زنجیره‌ای کردن VPN) پیچیده است، سرعت را به میزان قابل توجهی کاهش می‌دهد و معمولاً غیرضروری است. اکثر نیازهای حریم خصوصی کاربران با یک سرویس VPN با کیفیت واحد برآورده می‌شود.

**VPN ها از چه پهنای باندی استفاده می کنند؟**

عملکرد

VPN ها سربار رمزگذاری را اضافه می‌کنند، که معمولاً استفاده از پهنای باند را 5 تا 15 درصد افزایش می‌دهد. مقدار دقیق آن به پروتکل مورد استفاده و سطح رمزگذاری بستگی دارد. WireGuard معمولاً سربار کمتری نسبت به OpenVPN دارد. در صورت لزوم، این مورد را در هزینه‌های داده لحاظ کنید.

**آیا VPN هایی وجود دارند که نیازی به ثبت نام نداشته باشند؟**

حریم خصوصی

برخی از ارائه دهندگان VPN امکان ثبت نام ناشناس فقط با استفاده از آدرس های ایمیل یا حتی پرداخت های ارز دیجیتال بدون اطلاعات شخصی را فراهم می کنند. با این حال، VPN های کاملاً بدون ثبت نام نادر هستند و ممکن است ویژگی ها یا امنیت محدودی داشته باشند.

**ممیزی VPN چیست و چرا اهمیت دارد؟**

اعتماد

ممیزی VPN یک بررسی امنیتی مستقل از سیستم‌ها، کدها و رویه‌های حفظ حریم خصوصی ارائه‌دهنده VPN توسط شرکت‌های امنیتی شخص ثالث است. VPNهای ممیزی‌شده، اطمینان قابل اعتمادتری از ادعاهای امنیتی و سیاست‌های عدم ثبت اطلاعات ارائه می‌دهند.

**آیا می‌توانم از VPN برای دسترسی از راه دور به شبکه خانگی‌ام استفاده کنم؟**

دسترسی از راه دور

بله، شما می‌توانید یک سرور VPN روی روتر خانگی خود راه‌اندازی کنید تا از هر مکانی به طور ایمن به شبکه خانگی خود دسترسی داشته باشید. این با سرویس‌های VPN تجاری متفاوت است و در درجه اول برای دسترسی از راه دور است تا حفظ حریم خصوصی یا ناشناس بودن.

**اگر شرکت از کار بیفتد، چه اتفاقی برای VPN من می‌افتد؟**

کسب و کار

اگر یک شرکت VPN تعطیل شود، شما بلافاصله دسترسی به خدمات آنها را از دست می‌دهید. ارائه دهندگان معتبر با مالکیت و بودجه شفاف را انتخاب کنید. VPN هایی را در نظر بگیرید که ضمانت بازگشت وجه طولانی تری ارائه می‌دهند و از تعهدات اشتراک بسیار طولانی مدت خودداری می‌کنند.

**آیا برای فعالیت‌های مختلف به VPN های مختلف نیاز دارم؟**

کاربرد

به طور کلی، یک VPN خوب باید تمام نیازهای شما را برطرف کند. با این حال، برخی از کاربران VPN های مختلفی را برای اهداف خاص انتخاب می کنند - مانند یکی بهینه شده برای پخش جریانی و دیگری برای حداکثر حریم خصوصی. این بستگی به نیازها و بودجه خاص شما دارد.

**معماری سرور فقط مبتنی بر رم چیست؟**

حریم خصوصی

سرورهایی که فقط از RAM استفاده می‌کنند، هیچ داده‌ای را روی هارد دیسک ذخیره نمی‌کنند - همه چیز از حافظه‌ای اجرا می‌شود که هنگام راه‌اندازی مجدد سرورها پاک می‌شود. این یک لایه اضافی از محافظت از حریم خصوصی فراهم می‌کند زیرا هیچ گزارش یا داده ماندگاری نمی‌تواند روی سرورها ذخیره شود.

**آیا می‌توانم از VPN در وای‌فای عمومی استفاده کنم؟**

امنیت

بله، استفاده از VPN در وای‌فای عمومی اکیداً توصیه می‌شود. شبکه‌های عمومی اغلب ناامن هستند و به دیگران اجازه می‌دهند داده‌های شما را رهگیری کنند. VPN اتصال شما را رمزگذاری می‌کند و از اطلاعات حساس مانند رمزهای عبور و داده‌های شخصی در برابر هکرها محافظت می‌کند.

راهنماهای مرتبط:

[راهنمای امنیت وای‌فای عمومی](https://bestvpn.digital/guides/public-wifi-security)

[راهنمای جامع برای حفظ امنیت در شبکه‌های بی‌سیم عمومی](https://bestvpn.digital/guides/public-wifi-security)

[امنیت VPN موبایل](https://bestvpn.digital/guides/mobile-vpn-security)

[بهترین شیوه‌ها برای استفاده از VPN در دستگاه‌های تلفن همراه](https://bestvpn.digital/guides/mobile-vpn-security)

**تفاوت بین آدرس‌های IP اشتراکی و اختصاصی چیست؟**

ویژگی‌ها

آدرس‌های IP اشتراکی به طور همزمان توسط چندین کاربر VPN استفاده می‌شوند و ناشناس بودن بهتری را ارائه می‌دهند، اما ممکن است با مسدود شدن سرویس مواجه شوند. IPهای اختصاصی فقط به شما اختصاص داده می‌شوند و مسدود شدن و CAPTCHA را کاهش می‌دهند، اما ناشناس بودن کمتری را ارائه می‌دهند.

**چگونه مشکلات اتصال VPN را عیب یابی کنم؟**

عیب‌یابی

راه حل‌های رایج شامل تعویض سرور، تغییر پروتکل‌های VPN، راه‌اندازی مجدد برنامه، بررسی تنظیمات فایروال، به‌روزرسانی برنامه VPN یا تماس با پشتیبانی مشتری است. بسیاری از مشکلات اتصال با امتحان کردن سرورها یا پروتکل‌های مختلف حل می‌شوند.

**برای استفاده از VPN امنیتی چه چیزهایی را باید در مورد روتر بدانم؟**

امنیت

پیکربندی روتر برای امنیت هنگام استفاده از VPN بسیار مهم است. راه‌اندازی VPN روی روتر شما به طور خودکار از تمام دستگاه‌های متصل محافظت می‌کند. روترهایی را انتخاب کنید که از کلاینت‌های VPN پشتیبانی می‌کنند، مطمئن شوید که سیستم عامل به‌روزرسانی شده است و تنظیمات فایروال مناسب را پیکربندی کنید. سرویس‌های VPN پیشنهادی ما راهنماها و پشتیبانی راه‌اندازی روتر را ارائه می‌دهند.

**نقش WebRTC در بهبود پروتکل‌ها از طریق VPN چیست؟**

فنی

WebRTC می‌تواند هنگام استفاده از پروتکل‌های VPN به طور قابل توجهی بر تجربه آنلاین شما تأثیر بگذارد. مدیریت صحیح WebRTC به دور زدن سانسور، ایمن‌سازی داده‌های شما و لذت بردن از سرعت‌های بهتر کمک می‌کند. VPN های برتر شامل ویژگی‌های پیشرفته محافظت در برابر نشت WebRTC هستند که از افشای IP واقعی شما از طریق درخواست‌های WebRTC مرورگر جلوگیری می‌کنند.

**نقش ورود به سیستم در بهبود Basics از طریق VPN چیست؟**

حریم خصوصی

درک سیاست‌های ثبت وقایع هنگام انتخاب VPN ضروری است. سیاست‌های عدم ثبت وقایع تضمین می‌کنند که تاریخچه مرور، زمان اتصال و آدرس‌های IP شما ثبت نمی‌شوند. این امر محافظت حیاتی از حریم خصوصی را فراهم می‌کند و از به اشتراک گذاشتن داده‌ها با اشخاص ثالث یا مقامات جلوگیری می‌کند.

**اشتباهات رایج در نشت IP در تنظیمات VPN استریمینگ چیست؟**

پخش جریانی

نشت IP می‌تواند تجربه پخش و حریم خصوصی شما را به خطر بیندازد. اشتباهات رایج شامل عدم بررسی نشت DNS، نشت WebRTC یا نشت IPv6 است. VPN های پیکربندی شده صحیح با کلیدهای kill و محافظت در برابر نشت، تضمین می‌کنند که IP واقعی شما هنگام پخش محتوای محدود جغرافیایی پنهان می‌ماند.

راهنماهای مرتبط:

[راهنمای تست نشت VPN](https://bestvpn.digital/guides/vpn-leak-test)

[چگونه VPN خود را برای نشت DNS، WebRTC و IP آزمایش کنیم؟](https://bestvpn.digital/guides/vpn-leak-test)

[راه‌اندازی VPN استریمینگ](https://bestvpn.digital/guides/streaming-vpn-setup)

[پیکربندی بهینه VPN برای سرویس‌های استریم](https://bestvpn.digital/guides/streaming-vpn-setup)

**نقش DNS در بهبود Basics از طریق VPN چیست؟**

فنی

پیکربندی DNS برای عملکرد VPN اساسی است. استفاده از سرورهای DNS ارائه دهنده VPN شما از نشت DNS جلوگیری می‌کند و تضمین می‌کند که تمام ترافیک شما به درستی از طریق تونل VPN هدایت می‌شود. این امر ضمن حفظ حریم خصوصی، امنیت و عملکرد را افزایش می‌دهد.

**آیا پورت فورواردینگ روی عملکرد در Basics برای کاربران VPN تأثیر می‌گذارد؟**

عملکرد

فوروارد کردن پورت می‌تواند به طور قابل توجهی بر عملکرد و کارایی VPN تأثیر بگذارد. این امر برای فعالیت‌های P2P، بازی و اجرای سرورها ضروری است. با این حال، همه ارائه دهندگان VPN از فوروارد کردن پورت پشتیبانی نمی‌کنند و ممکن است با باز کردن پورت‌های خاص، امنیت را کمی کاهش دهد.

**نکات استفاده از VPN در مورد catapult hydra چیست؟**

پروتکل‌ها

Catapult Hydra یک پروتکل اختصاصی VPN است که سرعت و امنیت بیشتری را ارائه می‌دهد. این پروتکل به گونه‌ای طراحی شده است که ضمن حفظ رمزگذاری قوی، عملکرد بهتری نسبت به پروتکل‌های سنتی ارائه دهد. این پروتکل به ویژه برای پخش آنلاین و مرور عمومی مؤثر است.

**آیا تاخیر در عملکرد بخش امنیت برای کاربران VPN تأثیر می‌گذارد؟**

عملکرد

تأخیر (لگ) می‌تواند هنگام استفاده از VPN هم بر امنیت و هم بر عملکرد تأثیر بگذارد. تأخیر بالاتر ممکن است نشان‌دهنده مشکلات اتصال یا مشکلات سرور باشد. سرورهای VPN را نزدیک‌تر به موقعیت مکانی خود انتخاب کنید و از پروتکل‌های سریع‌تری مانند WireGuard استفاده کنید تا ضمن حفظ امنیت، تأخیر را به حداقل برسانید.

**نقش تبادل کلید در ارتقای Basics از طریق VPN چیست؟**

امنیت

تبادل کلید یک فرآیند امنیتی اساسی در اتصالات VPN است. این فرآیند کلیدهای رمزگذاری امنی را بین دستگاه شما و سرور VPN برقرار می‌کند. پروتکل‌های مدرن از روش‌های پیشرفته تبادل کلید مانند Elliptic Curve Diffie-Hellman برای امنیت و عملکرد بهتر استفاده می‌کنند.

**نقش درگاه (gateway) در بهبود نکات استفاده از طریق VPN چیست؟**

فنی

دروازه VPN برای مسیریابی صحیح ترافیک بسیار مهم است. این دروازه تعیین می‌کند که چگونه ترافیک اینترنت شما از طریق تونل VPN هدایت شود. پیکربندی صحیح دروازه از نشت DNS جلوگیری می‌کند، کیفیت پخش را بهبود می‌بخشد و محافظت از تمام ترافیک را تضمین می‌کند.

**آیا درگاه (gateway) برای ویژگی‌های پیشرفته بهتر با VPN ضروری است؟**

پیشرفته

پیکربندی دروازه برای ویژگی‌های پیشرفته VPN ضروری است. این پیکربندی امکان مسیریابی صحیح ترافیک را فراهم می‌کند، از تونل‌سازی تقسیم‌شده پشتیبانی می‌کند و سازگاری با سرورهای تخصصی را تضمین می‌کند. کاربران حرفه‌ای برای عملکرد بهینه از درک تنظیمات دروازه بهره‌مند می‌شوند.

**نقش مسدودسازی جغرافیایی در بهبود Basics از طریق VPN چیست؟**

پخش جریانی

درک مسدودسازی جغرافیایی برای استفاده از VPN اساسی است. VPN ها با پنهان کردن موقعیت مکانی شما، به دور زدن محدودیت‌های جغرافیایی کمک می‌کنند. این امر امکان دسترسی به محتوا، وب‌سایت‌ها و سرویس‌های دارای قفل منطقه‌ای را در عین حفظ حریم خصوصی و امنیت فراهم می‌کند.

راهنماهای مرتبط:

[راهنمای دور زدن مسدود کردن جغرافیایی](https://bestvpn.digital/guides/bypass-geo-blocking)

[نحوه دسترسی به محتوای محدود جغرافیایی با VPN](https://bestvpn.digital/guides/bypass-geo-blocking)

[دسترسی به محتوای جهانی](https://bestvpn.digital/guides/global-content-access)

[دسترسی به محتوا و خدمات بین‌المللی با VPN](https://bestvpn.digital/guides/global-content-access)

**چرا باید به اتصالات همزمان در بخش Devices اهمیت بدهم؟**

دستگاه‌ها

اتصالات همزمان تعیین می‌کند که با یک حساب VPN می‌توانید از چند دستگاه محافظت کنید. این برای خانواده‌هایی که چندین دستگاه دارند بسیار مهم است. به دنبال VPNهایی باشید که اتصالات نامحدود یا محدودیت‌های دستگاه کافی برای نیازهای شما ارائه می‌دهند.

**در مورد ممیزی استفاده از VPN در دستگاه‌ها چه چیزهایی را باید بدانم؟**

اعتماد

ممیزی‌های VPN، تأیید مستقل ادعاهای امنیتی و سیاست‌های حفظ حریم خصوصی را ارائه می‌دهند. هنگام انتخاب VPN برای چندین دستگاه، ارائه دهندگان ممیزی شده، قابلیت اعتماد بیشتری را ارائه می‌دهند. به دنبال ممیزی‌های امنیتی اخیر شخص ثالث و گزارش‌های شفافیت باشید.

**چرا باید به تأخیر در ویژگی‌های پیشرفته اهمیت بدهم؟**

بازی

تأخیر بر ویژگی‌های پیشرفته VPN مانند بازی، تماس‌های ویدیویی و برنامه‌های بلادرنگ تأثیر می‌گذارد. کاربران پیشرفته باید سرورهایی با پینگ پایین انتخاب کنند، از پروتکل‌های بهینه استفاده کنند و برای بهترین تجربه، سرورهای اختصاصی بازی را در نظر بگیرند.

**اشتباهات رایج در ممیزی در تنظیمات VPN P2P و Torrenting چیست؟**

همتا به همتا

هنگام تورنت، ارائه دهندگان VPN ممیزی شده با سیاست های عدم ثبت گزارش اثبات شده را انتخاب کنید. اشتباهات رایج شامل استفاده از VPN های ممیزی نشده، نادیده گرفتن ویژگی های kill switch و عدم تأیید پشتیبانی P2P است. VPN های ممیزی شده محافظت بهتری برای فعالیت های P2P ارائه می دهند.

**نقش پینگ در بهبود کسب و کار از طریق VPN چیست؟**

کسب و کار

پینگ پایین برای استفاده از VPN تجاری، به ویژه برای کنفرانس ویدیویی، تماس‌های VoIP و همکاری در لحظه، بسیار مهم است. ارائه دهندگان VPN تجاری را با سرورهای بهینه شده و ویژگی‌های تجاری اختصاصی برای حداقل تأخیر انتخاب کنید.

**اشتباهات رایج در تنظیمات VPN دستگاه‌ها با برنامه‌های VPN چیست؟**

دستگاه‌ها

اشتباهات رایج در برنامه‌های VPN شامل استفاده از برنامه‌های قدیمی، پیکربندی نکردن ویژگی‌های اتصال خودکار، نادیده گرفتن تنظیمات kill switch و دانلود برنامه‌های VPN جعلی است. همیشه برنامه‌های رسمی را از منابع معتبر دانلود کنید و آنها را به‌روز نگه دارید.

**آیا تاخیر برای پروتکل‌های بهتر با VPN ضروری است؟**

پروتکل‌ها

اگرچه تأخیر مطلوب نیست، اما درک تأخیر به انتخاب پروتکل VPN مناسب کمک می‌کند. WireGuard معمولاً تأخیر کمتری نسبت به OpenVPN ارائه می‌دهد، در حالی که IKEv2 برای اتصالات موبایل بهینه شده است. پروتکل‌ها را بر اساس نیازهای سرعت و امنیت خود انتخاب کنید.

**چرا باید به WebRTC در ویژگی‌های پیشرفته اهمیت بدهم؟**

حریم خصوصی

WebRTC حتی هنگام استفاده از VPN می‌تواند آدرس IP واقعی شما را فاش کند. کاربران حرفه‌ای باید WebRTC را در مرورگرهای خود غیرفعال کنند یا از VPNهایی با محافظت داخلی در برابر نشت WebRTC استفاده کنند. این امر از نقض حریم خصوصی در طول تماس‌های ویدیویی و اتصالات نظیر به نظیر جلوگیری می‌کند.

**کدام VPN در سال 2025 با Netflix USA کار می کند؟**

پخش جریانی

طبق آخرین آزمایش‌های ما، سرور ExpressVPN در نیوجرسی ۳، سرور NordVPN در آتلانتا و سرور Surfshark در لس‌آنجلس، Netflix USA را با کیفیت 4K از حالت مسدود خارج می‌کنند. VPN های رایگان در ۱۰۰٪ مواقع با شکست مواجه می‌شوند.

**چگونه iPlayer بی‌بی‌سی را در خارج از بریتانیا تماشا کنیم؟**

پخش جریانی

به سرور NordVPN در بریتانیا با کد پستی #1847 متصل شوید، کوکی‌های مرورگر را پاک کنید و با هر کد پستی در بریتانیا (مثلاً SW1A 1AA) ثبت‌نام کنید. روی همه دستگاه‌ها از جمله تلویزیون‌های هوشمند کار می‌کند.

**آیا می‌توانم از VPN در اپل تی‌وی استفاده کنم؟**

دستگاه‌ها

اپل تی‌وی مستقیماً از برنامه‌های VPN پشتیبانی نمی‌کند. در عوض، VPN را روی روتر خود تنظیم کنید یا از SmartDNS استفاده کنید (MediaStreamer اکسپرس وی‌پی‌ان بی‌نقص کار می‌کند).

**کدام VPN برای دیزنی پلاس بهترین است؟**

پخش جریانی

سورفشارک بیش از ۱۵ کتابخانه دیزنی پلاس (ایالات متحده، انگلستان، ژاپن و غیره) را با ارزان‌ترین قیمت از حالت مسدود خارج می‌کند. روزانه آزمایش می‌شود - به کارت امتیازی دیزنی پلاس VPN ما مراجعه کنید.

**چگونه خطای پروکسی Netflix را برطرف کنیم؟**

عیب‌یابی

به یک سرور دیگر بروید، حافظه پنهان را پاک کنید یا از حالت ناشناس استفاده کنید. اگر هنوز مسدود هستید، برای اطلاع از آخرین سرور فعال با چت زنده تماس بگیرید - ExpressVPN سرور خود را هر ساعت به‌روزرسانی می‌کند.

**وی پی ان دابل چیست؟**

پیشرفته

برای رمزگذاری بیشتر، ترافیک را از طریق دو سرور هدایت می‌کند. دابل وی‌پی‌ان شرکت NordVPN رمزگذاری ۲۰۴۸ بیتی را اضافه می‌کند - ایده‌آل برای روزنامه‌نگاران یا فعالان.

**چگونه VPN را روی روتر تنظیم کنیم؟**

فنی

یک روتر از پیش فلش شده از FlashRouters بخرید یا فریمور DD-WRT را نصب کنید. راهنمای ما تنظیمات Asus، Netgear و Linksys را پوشش می‌دهد - 10 دقیقه طول می‌کشد.

**محافظت در برابر نشت IPv6 چیست؟**

امنیت

ترافیک IPv6 را برای جلوگیری از نشت غیرفعال می‌کند. در تنظیمات NordVPN فعال کنید - 99٪ از VPN ها این را نادیده می‌گیرند و باعث نشت در شبکه‌های دارای IPv6 می‌شوند.

**چگونه مشکل وصل نشدن VPN را حل کنیم؟**

عیب‌یابی

این مراحل را امتحان کنید: پروتکل‌ها را تغییر دهید (WireGuard → OpenVPN)، DNS را به ۸.۸.۸.۸ تغییر دهید، آنتی‌ویروس/فایروال را به‌طور موقت غیرفعال کنید، برای اطلاع از وضعیت سرور با چت زنده ۲۴ ساعته تماس بگیرید.

**چگونه ExpressVPN را به صورت رایگان دریافت کنیم؟**

قیمت‌گذاری

از ضمانت بازگشت وجه ۳۰ روزه بدون هیچ سوالی استفاده کنید. ثبت نام کنید، به مدت ۲۹ روز استفاده کنید، از طریق چت زنده لغو کنید و کل مبلغ را پس بگیرید. با یک ایمیل جدید این کار را تکرار کنید.

**آیا معاملات مادام العمر VPN وجود دارد؟**

قیمت‌گذاری

از VPN های «طول عمر» اجتناب کنید - آنها داده ها را خاموش یا می فروشند. در عوض، طرح ۲ ساله Surfshark را با قیمت ۱.۹۹ دلار در ماه تهیه کنید - معادل ۹۰٪ تخفیف.

**آیا FBI می‌تواند VPN را ردیابی کند؟**

حریم خصوصی

اگر VPN هیچ لاگی (مانند سرورهای فقط RAM در ExpressVPN) ثبت نکند، حتی FBI هم نمی‌تواند داده‌ها را بازیابی کند. در دادگاه ثابت شد - ExpressVPN در سال ۲۰۱۷ نتوانست لاگ‌ها را تحویل دهد.

**قناری گارانتی چیست؟**

حریم خصوصی

بیانیه شفافیت ماهانه به‌روزرسانی می‌شود. اگر حذف شود، نشان‌دهنده احضاریه محرمانه است. PIA و NordVPN بیانیه خود را به صورت عمومی منتشر می‌کنند.

**بهترین VPN برای آیفون در سال 2025؟**

موبایل

اپلیکیشن iOS NordVPN شامل WireGuard، kill switch و میانبرهای Siri است. امتیاز ۴.۹ از ۵ در اپ استور - از طریق لینک ما به مدت ۳ ماه رایگان دانلود کنید.

**چگونه از VPN در اندروید تی‌وی استفاده کنیم؟**

دستگاه‌ها

Surfshark APK را از وب‌سایت آنها نصب کنید (گوگل پلی برخی مناطق را مسدود می‌کند). برای دسترسی با یک کلیک از کاشی «اتصال سریع» استفاده کنید.

**آیا استفاده از VPN قانونی است؟**

قانونی

در بیشتر کشورها، VPN ها کاملاً قانونی هستند. با این حال، استفاده از آنها برای فعالیت‌های غیرقانونی (مانند هک یا تورنت کردن مطالب دارای حق چاپ) همچنان غیرقانونی است. برخی کشورها (به عنوان مثال، چین، روسیه، امارات متحده عربی) VPN ها را محدود یا ممنوع کرده‌اند، بنابراین همیشه قبل از سفر قوانین محلی را بررسی کنید.

**آیا VPN می‌تواند من را به صورت آنلاین ناشناس کند؟**

حریم خصوصی

VPN به طور قابل توجهی حریم خصوصی شما را افزایش می‌دهد اما شما را ۱۰۰٪ ناشناس نمی‌کند. برای ناشناس ماندن کامل، یک VPN بدون گزارش را با Tor، مرورگرهای امن و سیستم عامل‌های متمرکز بر حریم خصوصی مانند Tails ترکیب کنید.

**تفاوت بین VPN و پروکسی چیست؟**

مقایسه

یک VPN تمام ترافیک اینترنت شما را در سطح سیستم عامل رمزگذاری می‌کند، در حالی که یک پروکسی فقط ترافیک را از برنامه‌های خاص (مانند مرورگر شما) تغییر مسیر می‌دهد. پروکسی‌ها داده‌ها را رمزگذاری نمی‌کنند و همین امر VPNها را بسیار امن‌تر می‌کند.

**آیا VPN ها سرعت اینترنت را کاهش می دهند؟**

عملکرد

بله، اما حداقل. یک VPN پریمیوم با پروتکل‌های مدرن مانند WireGuard می‌تواند سرعت را ۵ تا ۱۰ درصد کاهش دهد، در حالی که VPN های رایگان یا پر ازدحام می‌توانند سرعت را ۵۰ درصد یا بیشتر کاهش دهند. انتخاب یک سرور نزدیک کمک می‌کند.

**آیا می‌توانم از VPN روی چندین دستگاه استفاده کنم؟**

دستگاه‌ها

VPN های برتر 5 تا 10 اتصال همزمان برای هر حساب ارائه می دهند. برخی (مانند Surfshark) به تعداد نامحدود دستگاه اجازه اتصال می دهند. نمودار مقایسه ما را بررسی کنید تا ببینید کدام VPN ها از تلفن، لپ تاپ، روتر و تلویزیون هوشمند شما پشتیبانی می کنند.

**آیا VPN از هکرها محافظت می‌کند؟**

امنیت

بله، مخصوصاً در وای‌فای عمومی. VPN داده‌های شما را رمزگذاری می‌کند و از حملات مرد میانی جلوگیری می‌کند. با این حال، از شما در برابر بدافزار یا فیشینگ محافظت نمی‌کند - از آنتی‌ویروس و احراز هویت دو مرحله‌ای در کنار VPN خود استفاده کنید.

**VPN بدون گزارش چیست؟**

حریم خصوصی

یک VPN بدون گزارش هیچ داده‌ای در مورد فعالیت آنلاین شما ذخیره نمی‌کند. به دنبال ارائه‌دهندگانی باشید که توسط اشخاص ثالث (مانند PwC یا Cure53) حسابرسی شده‌اند و در حوزه‌های قضایی دوستدار حریم خصوصی (مثلاً پاناما، سوئیس) مستقر هستند.

**آیا در صورت استفاده از VPN، ردیابی می‌شوم؟**

حریم خصوصی

اگر VPN شما سیاست سختگیرانه‌ای برای عدم ثبت وقایع دارد و DNS/WebRTC را نشت نمی‌دهد، ردیابی بسیار دشوار است. با این حال، ورود به گوگل یا فیس‌بوک هنوز شما را شناسایی می‌کند - از حالت ناشناس و سرویس‌های متمرکز بر حریم خصوصی استفاده کنید.

**سوئیچ مرگ چیست؟**

امنیت

در صورت قطع شدن VPN، یک kill switch اینترنت شما را قطع می‌کند و از نشت IP جلوگیری می‌کند. همیشه هنگام تورنت یا دسترسی به محتوای حساس، این ویژگی را فعال کنید.

**آیا VPN های رایگان ایمن هستند؟**

قیمت‌گذاری

۹۹٪ از VPN های رایگان خطرناک هستند. آنها اطلاعات شما را می‌فروشند، تبلیغات تزریق می‌کنند یا حاوی بدافزار هستند. موارد استثنا شامل نسخه رایگان Proton VPN (سرورهای محدود، بدون لاگ) می‌شود. برای ایمنی، به VPN های پولی با ضمانت بازگشت وجه پایبند باشید.

**تونل سازی اسپلیت چیست؟**

ویژگی‌ها

تونل‌سازی اسپلیت به شما امکان می‌دهد انتخاب کنید کدام برنامه‌ها از VPN و کدام‌ها از اتصال معمولی شما استفاده کنند. این ویژگی برای برنامه‌های بانکی که VPNها را مسدود می‌کنند و در عین حال تورنت ایمن انجام می‌دهند، عالی است.

**آیا VPN می‌تواند از بلوک‌های جغرافیایی Netflix عبور کند؟**

پخش جریانی

بله، اما فقط VPN های پریمیوم مانند ExpressVPN، NordVPN یا Surfshark به طور مداوم Netflix، BBC iPlayer و Disney+ را از حالت مسدود خارج می‌کنند. لیست سرورهای فعال ما را که روزانه آزمایش شده‌اند، بررسی کنید.

**وایرگارد چیست؟**

فنی

WireGuard جدیدترین پروتکل VPN است که سرعت بالاتر و رمزگذاری قوی‌تری نسبت به OpenVPN ارائه می‌دهد. اکثر VPN های برتر اکنون از آن پشتیبانی می‌کنند (به عنوان مثال، NordLynx از NordVPN).

**چگونه بفهمم VPN من کار می‌کند؟**

آزمایش

قبل و بعد از اتصال به ipleak.net مراجعه کنید. اگر IP و DNS شما تغییر کرد، یعنی درست کار می‌کند. همچنین نشت WebRTC را در مرورگر خود بررسی کنید.

**آیا می‌توانم از VPN برای بازی استفاده کنم؟**

بازی

بله! VPN حملات DDoS را کاهش می‌دهد، ممنوعیت‌های IP را دور می‌زند و به شما امکان می‌دهد زودتر به بازی‌های دارای محدودیت جغرافیایی دسترسی پیدا کنید. VPN با سرورهای پینگ پایین مانند ExpressVPN یا CyberGhost را انتخاب کنید.

**مبهم‌سازی چیست؟**

پیشرفته

مبهم‌سازی، ترافیک VPN را به عنوان HTTPS معمولی پنهان می‌کند و از انسداد VPN در کشورهایی مانند چین یا ایران عبور می‌کند. به دنبال ویژگی‌های «حالت مخفی» یا «OpenVPN Scramble» باشید.

**آیا VPN ها در چین کار می کنند؟**

سانسور

فقط تعداد کمی از VPN ها (مثلاً ExpressVPN، Astrill، NordVPN) به دلیل بازرسی عمیق بسته‌ها (Deep Packet Inspection) در چین به طور قابل اعتمادی کار می‌کنند. همیشه قبل از سفر VPN را دانلود کنید.

**آیا می‌توانم با VPN تورنت کنم؟**

همتا به همتا

بله، اما فقط از سرورهای بهینه شده P2P با قابلیت kill switch فعال استفاده کنید. انتخاب‌های برتر ما: NordVPN، Surfshark و Private Internet Access - همه با قابلیت پورت فورواردینگ و بدون محدودیت پهنای باند.

**آی پی اختصاصی چیست؟**

ویژگی‌ها

یک IP اختصاصی، آدرس IP است که فقط شما از آن استفاده می‌کنید و باعث کاهش کپچا و قرار گرفتن در لیست سیاه می‌شود. برای امور بانکی یا کار از راه دور مفید است. به عنوان یک افزونه با NordVPN، CyberGhost و PureVPN در دسترس است.

**هزینه VPN چقدر است؟**

قیمت‌گذاری

VPN های پریمیوم بسته به مدت زمان پلن، از ۲ تا ۱۲ دلار در ماه متغیر هستند. پیشنهادهای ویژه ما قیمت‌ها را به ۱.۹۹ دلار در ماه (پلن ۲ ساله Surfshark) با ۳ ماه رایگان کاهش می‌دهد.

**آیا می‌توانم هزینه VPN را به صورت ناشناس پرداخت کنم؟**

حریم خصوصی

بله، VPN های برتر بیت کوین، مونرو یا پول نقد را می پذیرند. مولود حتی یک شماره حساب ایجاد می کند - نیازی به ایمیل نیست.

**اتحاد پنج/نه/چهارده چشم چیست؟**

حریم خصوصی

اینها توافق‌نامه‌های اشتراک‌گذاری اطلاعات بین کشورها هستند. از VPN های مستقر در این حوزه‌های قضایی (مثلاً ایالات متحده، انگلستان) خودداری کنید، مگر اینکه سیاست عدم گزارش‌گیری اثبات‌شده‌ای (مانند PIA) داشته باشند.

**آیا VPN می‌تواند از محدودیت ISP عبور کند؟**

عملکرد

بله، اگر ارائه‌دهنده‌ی خدمات اینترنتی شما (مثلاً نتفلیکس) پخش آنلاین را محدود می‌کند، VPN ترافیک شما را پنهان می‌کند و سرعت کامل را بازیابی می‌کند. برای تأیید، با VPN و بدون VPN امتحان کنید.

**بهترین VPN برای مبتدیان چیست؟**

توصیه‌ها

CyberGhost و ExpressVPN برنامه‌هایی با یک کلیک، پشتیبانی ۲۴ ساعته و بدون نیاز به تنظیمات دارند. ایده‌آل برای کاربران غیرفنی.

**چرا باید کسی برای وبگردی روزمره از VPN استفاده کند؟**

اطلاعات عمومی VPN

استفاده از VPN برای مرور روزانه، حریم خصوصی و امنیت آنلاین شما را افزایش می‌دهد. این سرویس، ترافیک اینترنت شما را رمزگذاری می‌کند و از نظارت ISPها، تبلیغ‌کنندگان یا هکرها بر فعالیت‌های شما جلوگیری می‌کند. این امر به ویژه در شبکه‌های ناامن مانند Wi-Fi عمومی در کافه‌ها یا فرودگاه‌ها، که سرقت داده‌ها در آنها خطر دارد، بسیار مهم است. VPN همچنین به شما امکان می‌دهد محدودیت‌های جغرافیایی را دور بزنید و به محتوایی مانند ویدیوهای YouTube یا سایت‌های خبری با قفل منطقه‌ای دسترسی پیدا کنید. به عنوان مثال، می‌توانید به صورت ناشناس مرور کنید، پروازهای ارزان‌تر بخرید یا برنامه‌های تلویزیونی بین‌المللی را پخش کنید. در سال 2025، با افزایش نقض داده‌ها، VPN یک لایه محافظتی اضافه می‌کند. ExpressVPN که به دلیل سرعت و قابلیت اطمینان خود شناخته شده است، گزینه بسیار خوبی برای مرور یکپارچه در بین دستگاه‌ها است. رابط کاربری بصری آن برای همه کاربران مناسب است.

**چگونه یک VPN امنیت آنلاین را برای مبتدیان بهبود می‌بخشد؟**

اطلاعات عمومی VPN

برای مبتدیان، یک VPN با رمزگذاری اتصال اینترنت شما، امنیت آنلاین را ساده می‌کند، که از داده‌های حساس مانند رمزهای عبور یا جزئیات کارت اعتباری در برابر هکرها محافظت می‌کند. این VPN آدرس IP شما را می‌پوشاند و شناسایی شما را برای وب‌سایت‌ها یا ردیاب‌ها دشوارتر می‌کند. این امر به ویژه در Wi-Fi عمومی، جایی که حملات سایبری رایج است، مفید است. VPN همچنین تبلیغات و ردیاب‌های مزاحم را مسدود می‌کند و یک تجربه مرور روان‌تر را ایجاد می‌کند. در سال 2025، با هزینه‌های میلیاردی جرایم سایبری سالانه، حتی کاربران معمولی نیز از این محافظت بهره‌مند می‌شوند. CyberGhost یک رابط کاربری آسان با تنظیمات امنیتی از پیش پیکربندی شده ارائه می‌دهد که برای تازه واردان ایده‌آل است. سیاست عدم ثبت اطلاعات آن تضمین می‌کند که داده‌های شما خصوصی باقی بمانند. با بررسی گزینه‌هایی مانند CyberGhost، می‌توانید بدون تخصص فنی، فعالیت‌های آنلاین خود را ایمن کنید.

**تفاوت بین VPN و سرور پروکسی چیست؟**

اطلاعات عمومی VPN

VPN و پروکسی سرور هر دو آدرس IP شما را می‌پوشانند، اما تفاوت‌های قابل توجهی با هم دارند. VPN تمام ترافیک اینترنت شما را رمزگذاری می‌کند، آن را از طریق یک سرور امن مسیریابی می‌کند و از حریم خصوصی و امنیت در برنامه‌ها و وب‌سایت‌ها اطمینان حاصل می‌کند. پروکسی‌ها فقط ترافیک خاصی (مثلاً داده‌های مرورگر) را بدون رمزگذاری هدایت می‌کنند و شما را در برابر جاسوسی آسیب‌پذیر می‌کنند. VPNها برای کارهای حساس مانند بانکداری یا دور زدن محدودیت‌های جغرافیایی ایده‌آل هستند، در حالی که پروکسی‌ها برای دسترسی سریع و غیر حساس به سایت‌های مسدود شده بهتر هستند. به عنوان مثال، VPN به شما امکان می‌دهد Netflix را به صورت ایمن پخش کنید، در حالی که پروکسی ممکن است این کار را نکند. PureVPN اتصالات رمزگذاری شده و مقرون به صرفه‌ای را با سرورها در بیش از 70 کشور ارائه می‌دهد و آن را به انتخابی قوی‌تر از پروکسی‌ها تبدیل می‌کند.

**آیا VPN می‌تواند سابقه مرور من را از ISP من پنهان کند؟**

اطلاعات عمومی VPN

بله، یک VPN با رمزگذاری ترافیک شما و مسیریابی آن از طریق یک سرور از راه دور، تاریخچه مرور شما را از ISP شما پنهان می‌کند. این امر مانع از آن می‌شود که ISP شما ببیند از کدام وب‌سایت‌ها بازدید می‌کنید یا چه کاری را به صورت آنلاین انجام می‌دهید و از حریم خصوصی شما محافظت می‌کند. به عنوان مثال، اگر در حال پخش یا تحقیق در مورد موضوعات حساس هستید، یک VPN فعالیت شما را خصوصی نگه می‌دارد. در سال 2025، با افزایش درآمدزایی ISPها از داده‌های کاربر، این یک مزیت کلیدی است. NordVPN، با سیاست عدم گزارش حسابرسی شده خود، تضمین می‌کند که حتی ارائه دهنده VPN نیز نمی‌تواند فعالیت شما را ببیند. بیش از 5500 سرور آن، انعطاف‌پذیری را برای مرور خصوصی ارائه می‌دهند. با انتخاب سرویسی مانند NordVPN، می‌توانید کنترل ردپای دیجیتالی خود را حفظ کرده و بدون نگرانی مرور کنید.

**آیا هنگام استفاده از وای‌فای خانگی به VPN نیاز دارم؟**

اطلاعات عمومی VPN

اگرچه وای‌فای خانگی عموماً امن‌تر از شبکه‌های عمومی است، اما VPN همچنان محافظت ارزشمندی را ارائه می‌دهد. این شبکه، داده‌های شما را رمزگذاری می‌کند و مانع از سوءاستفاده هکرها از امنیت ضعیف روتر یا رهگیری اطلاعات حساس مانند اطلاعات ورود به سیستم می‌شود. همچنین مانع از ردیابی عادات مرور شما توسط ISPها برای تبلیغات هدفمند می‌شود. به عنوان مثال، اگر در خانه خرید آنلاین انجام می‌دهید یا امور مالی خود را مدیریت می‌کنید، VPN تضمین می‌کند که داده‌های شما ایمن باقی می‌مانند. علاوه بر این، محتوای محدود شده جغرافیایی مانند پلتفرم‌های پخش بین‌المللی را باز می‌کند. ExpressVPN اتصالات سریع و قابل اعتمادی را برای استفاده خانگی، با برنامه‌هایی برای روترها و دستگاه‌ها ارائه می‌دهد. راه‌اندازی کاربرپسند آن، ایمن‌سازی کل شبکه شما را آسان می‌کند.

نمایش ۱۱۴ از ۱۱۴ سوال متداول