نام: _____ تاریخ: _____ نمره: _____

ایستگاه بررسی 10

پرسش‌های متداول VPN

کاربرگ تعاملی و راهنمای مطالعه

بر اساس: باز کردن راهنمای VPN در VPN.com: **https://www.vpn.com/vpn/**

کاربرگ VPN چیست

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش A)

رایج‌ترین پرسش‌ها و پاسخ‌هایی را که مشتریان بالقوه دربارهٔ استفاده از شبکه‌های خصوصی مجازی دارند مرور کنید.

Q1: VPN چیست و چگونه کار می‌کند؟

شبکهٔ خصوصی مجازی (VPN) اتصال اینترنت شما را رمزگذاری می‌کند و ترافیک شما را از طریق یک سرور راه‌دور امن عبور می‌دهد. این کار IP عمومی شما را پنهان می‌کند و آنچه ناظران شبکهٔ محلی و ISP شما دربارهٔ ترافیک عبوری از تونل VPN می‌بینند را محدود می‌کند.

Q2: چرا باید از VPN استفاده کنم؟

VPN از حریم خصوصی دیجیتال شما محافظت می‌کند، اتصال شما را در شبکه‌های Wi-Fi عمومی (مانند کافه‌ها یا فرودگاه‌ها) ایمن می‌کند، ممکن است وقتی ISP نوع ترافیک رمزگذاری‌شده را شناسایی نکند، کاهش سرعت مبتنی بر فعالیت را کم کند، محدودیت‌های جغرافیایی را دور می‌زند تا به محتوای جهانی دسترسی پیدا کنید، و به ایمن‌سازی منابع کار از راه دور کمک می‌کند.

Q3: آیا VPN مرا در فضای آنلاین کاملاً ناشناس می‌کند؟

خیر. هرچند VPN نشانی IP شما را پنهان و ترافیک را رمزگذاری می‌کند، همچنان می‌توانید از طریق کوکی‌های مرورگر، حساب‌های فعال (مانند Google یا Facebook)، انگشت‌نگاری مرورگر، یا اگر ارائه‌دهندهٔ VPN شما داده‌هایتان را ثبت کند، ردیابی شوید.

Q4: آیا VPN سرعت اینترنت من را کاهش می‌دهد؟

بله، اندکی. فرایند رمزگذاری و فاصلهٔ فیزیکی تا سرور VPN تأخیر و سربار اضافه می‌کنند. این تأثیر بسته به ارائه‌دهنده، پروتکل، فاصلهٔ سرور، دستگاه و شرایط شبکه متفاوت است.

Q5: آیا استفاده از VPN قانونی است؟

استفاده از VPN در بسیاری از کشورها قانونی است، اما برخی حوزه‌های قضایی خدمات VPN را محدود، تنظیم یا مسدود می‌کنند. کاربران باید پیش از استفاده قوانین محلی فعلی را بررسی کنند. برای جزئیات بیشتر، راهنماهای قانونی‌بودن را در VPN.com مطالعه کنید.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش B)

رایج‌ترین پرسش‌ها و پاسخ‌هایی را که مشتریان بالقوه دربارهٔ استفاده از شبکه‌های خصوصی مجازی دارند مرور کنید.

Q6: آیا می‌توانم از VPN رایگان استفاده کنم؟

VPNهای رایگان ممکن است به تبلیغات، ویژگی‌های محدود، تحلیل‌های استفاده، سقف داده یا مدل‌های درآمدزایی دیگر متکی باشند. کاربران باید پیش از استفاده سیاست حریم خصوصی، مالکیت، ممیزی‌ها و مدل کسب‌وکار ارائه‌دهنده را بررسی کنند.

Q7: سیاست «بدون‌لاگ» چیست؟

سیاست بدون ثبت گزارش مشخص می‌کند ارائه‌دهنده می‌گوید کدام داده‌های فعالیت و اتصال را نگه نمی‌دارد. دامنهٔ دقیق آن متفاوت است، بنابراین خوانندگان باید سیاست و یافته‌های ممیزی مستقل را بررسی کنند.

Q8: چگونه بهترین VPN را انتخاب کنم؟

به دنبال سیاست‌های عدم ثبت لاگِ ممیزی‌شده، پروتکل‌های قوی (WireGuard، OpenVPN)، مکان‌های امن سرور، سرعت بالا، سرورهای فقطRAM، قابلیت kill switch و صلاحیت قضایی خارج از اتحادهای تبادل اطلاعات اطلاعاتی (مانند 5/9/14 چشم) باشید.

Q9: آیا می‌توانم VPN را روی گوشی و تلویزیون هوشمند خود استفاده کنم؟

بله. ارائه‌دهندگان مدرن VPN برنامه‌های اختصاصی برای Linux، Windows، macOS، Android، iOS و تلویزیون‌های هوشمند و همچنین راه‌اندازی روی روتر برای محافظت از همهٔ دستگاه‌های شبکهٔ خانگی شما ارائه می‌دهند.

Q10: کلید قطع (Kill Switch) چیست؟

Kill Switch قابلیتی امنیتی است که اگر اتصال VPN قطع شود، دستگاه شما را به‌طور خودکار از اینترنت جدا می‌کند. این کار از نشت داده‌های رمزگذاری‌نشده یا IP واقعی شما جلوگیری می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش C)

جنبه‌های فنی و ساختاری شبکه‌های خصوصی مجازی و پروتکل‌های تونل‌سازی امن را بررسی کنید.

Q1: تفاوت OpenVPN، WireGuard و IKEv2 چیست؟

WireGuard یک پروتکل مدرن و سبک است (فقط حدود 4,000 خط کد) که سرعت بالا و زمان اتصال کوتاه ارائه می‌دهد. OpenVPN یک پروتکل متن‌باز بسیار امن و محک‌خورده است. IKEv2 به‌دلیل توانایی اتصال مجدد سریع هنگام تغییر شبکه برای دستگاه‌های موبایل عالی است. [4]

Q2: مسیریابی دو VPN یا Multi-Hop چیست؟

روش چندجهشی ترافیک شما را به‌صورت متوالی از دو یا چند سرور VPN عبور می‌دهد. این کار لایهٔ رمزگذاری دوم اضافه می‌کند و اگر یک سرور آسیب ببیند، کمک می‌کند نشانی IP واقعی شما از جهش دوم پنهان بماند.

Q3: نشت WebRTC چیست و VPN چگونه از آن جلوگیری می‌کند؟

WebRTC یک پروتکل مرورگر است که حتی هنگام فعال بودن VPN می‌تواند نشانی‌های IP محلی و عمومی واقعی شما را فاش کند. VPNهای ممتاز درخواست‌های WebRTC را در برنامه‌های دسکتاپ/موبایل و افزونه‌های مرورگر خود مسدود یا جعل می‌کنند.

Q4: سرورهای فقطRAM چیستند و چرا اهمیت دارند؟

سرورهای سنتی داده را روی هارددیسک می‌نویسند که می‌تواند توقیف یا آسیب‌دیده شود. سرورهای فقط-RAM (بدون دیسک) کاملاً در حافظهٔ فرار (RAM) اجرا می‌شوند. وقتی سرور مجدداً راه‌اندازی یا خاموش شود، داده‌های موجود در حافظه پاک می‌شوند.

Q5: مبهم‌سازی چگونه مسدودسازی VPN را دور می‌زند؟

مبهم‌سازی (یا «Stealth VPN») ترافیک VPN را طوری پنهان می‌کند که شبیه ترافیک HTTPS معمولی (پورت 443) به نظر برسد. این کار می‌تواند به عبور از بازرسی عمیق بسته (DPI) کمک کند که دولت‌ها یا شبکه‌های مدرسه و دفتر برای مسدود کردن VPN به کار می‌برند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش D)

جنبه‌های فنی و ساختاری شبکه‌های خصوصی مجازی و پروتکل‌های تونل‌سازی امن را بررسی کنید.

Q6: Split Tunneling چیست و چه زمانی باید از آن استفاده کنم؟

Split Tunneling به شما اجازه می‌دهد انتخاب کنید کدام برنامه‌ها از تونل رمزگذاری‌شدهٔ VPN عبور کنند و کدام مستقیماً به اینترنت وصل شوند. از آن استفاده کنید تا برنامه‌های بانکی حساس از VPN عبور کنند و بازی‌های محلی مستقیماً وصل شوند و تأخیر ناشی از VPN را نداشته باشند.

Q7: رازداری پیشرو (Perfect Forward Secrecy) چگونه کار می‌کند؟

PFS تضمین می‌کند که برای هر نشست یک کلید رمزگذاری منحصربه‌فرد و موقت تولید شود. حتی اگر کلید خصوصی در آینده فاش شود، نمی‌توان از آن برای رمزگشایی نشست‌های گذشته یا آینده استفاده کرد، زیرا آن‌ها از کلیدهای مستقل استفاده کرده‌اند.

Q8: ائتلاف‌های 5/9/14 Eyes چیستند و چرا باید برایم مهم باشند؟

صلاحیت قضایی می‌تواند بر فرایند حقوقی‌ای که یک ارائه‌دهنده ممکن است با آن روبه‌رو شود اثر بگذارد، اما خطر عملی برای حریم خصوصی به این هم بستگی دارد که ارائه‌دهنده چه داده‌هایی را نگه می‌دارد، معماری فنی، مالکیت، گزارش‌دهی شفافیت و سابقهٔ ممیزی آن چیست.

Q9: محافظت در برابر نشت DNS چیست؟

محافظت در برابر نشت DNS دستگاه شما را وادار می‌کند پرس‌وجوهای جست‌وجوی وب‌سایت (پرس‌وجوهای DNS) را به‌جای سرورهای ISP شما، از طریق سرورهای DNS خصوصی و رمزگذاری‌شدهٔ VPN ارسال کند. این کار مانع می‌شود ISP شما بتواند ردیابی کند از چه سایت‌هایی بازدید می‌کنید.

Q10: آیا VPN می‌تواند محدودسازی اینترنت توسط ISP را دور بزند؟

گاهی. وقتی ISP به‌طور انتخابی فعالیت‌های قابل‌شناسایی را کند می‌کند، VPN ممکن است کمک کند، اما بر ازدحام، سقف داده، محدودیت‌های سرعت در سطح حساب یا کیفیت ضعیف شبکه غلبه نمی‌کند.

منابع و مراجع فنی

نشریات ارجاع‌شده، مشخصات رمزنگاری و استانداردهای رسمی اسنادی که در سراسر این کاربرگ استفاده شده‌اند.

منابع علمی و صنعتی

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637