Nome: _____ Data: _____ Pontuação: _____

PONTO DE CONTROLO 10

Perguntas frequentes sobre VPN

Ficha de trabalho interativa e guia de estudo

Com base em Abrir o Guia de VPN da VPN.com: **https://www.vpn.com/pt/vpn/**

Ficha de trabalho: o que é uma VPN

Ponto de controlo 10: Perguntas frequentes básicas sobre VPN (Parte A)

Revê as perguntas e respostas mais comuns que os potenciais clientes colocam sobre a utilização de redes privadas virtuais.

Q1: O que é uma VPN e como funciona?

Uma Rede Privada Virtual (VPN) encripta a tua ligação à Internet e encaminha o teu tráfego através de um servidor remoto seguro. Isto oculta o teu endereço IP público e limita o que os observadores da rede local e o teu ISP podem ver sobre o tráfego encaminhado pelo túnel VPN.

Q2: Porque devo utilizar uma VPN?

Uma VPN protege a tua privacidade digital, protege a tua ligação em redes Wi-Fi públicas (como cafés ou aeroportos), pode reduzir a limitação baseada na atividade quando o ISP não consegue identificar o tipo de tráfego encriptado, contorna restrições geográficas para aceder a conteúdos globais e ajuda a proteger recursos de trabalho remoto.

Q3: Uma VPN torna-me completamente anónimo online?

Não. Embora uma VPN oculte o teu endereço IP e encripte o tráfego, podes continuar a ser rastreado através de cookies do navegador, contas ativas (como Google ou Facebook), identificação por impressão digital do navegador ou se o teu fornecedor de VPN registar os teus dados.

Q4: Uma VPN vai tornar a minha ligação à Internet mais lenta?

Sim, ligeiramente. O processo de encriptação e a distância física ao servidor VPN acrescentam latência e sobrecarga. O impacto varia consoante o fornecedor, o protocolo, a distância ao servidor, o dispositivo e as condições da rede.

Q5: É legal usar uma VPN?

A utilização de VPN é legal em muitos países, mas algumas jurisdições restringem, regulam ou bloqueiam os serviços de VPN. Os utilizadores devem verificar a legislação local em vigor antes de usar. Para mais detalhes, consulta os guias de legalidade na VPN.com.

Ponto de controlo 10: Perguntas frequentes básicas sobre VPN (Parte B)

Revê as perguntas e respostas mais comuns que os potenciais clientes colocam sobre a utilização de redes privadas virtuais.

Q6: Posso usar uma VPN gratuita?

As VPN gratuitas podem depender de publicidade, de funcionalidades limitadas, de análises de utilização, de limites de dados ou de outros modelos de rentabilização. Os utilizadores devem consultar a política de privacidade, a propriedade, as auditorias e o modelo de negócio do fornecedor antes de as utilizar.

Q7: O que é uma política de «não guardar registos» (no-logs)?

Uma política de não registos descreve que dados de atividade e de ligação um fornecedor afirma não reter. O âmbito exato varia, pelo que os leitores devem consultar a política e as conclusões de auditorias independentes.

Q8: Como escolho a melhor VPN?

Procura políticas de não registo auditadas, protocolos robustos (WireGuard, OpenVPN), localizações de servidores seguras, velocidades rápidas, servidores apenas com RAM, uma funcionalidade de kill switch e uma jurisdição fora de alianças de partilha de informações (como as 5/9/14 Eyes).

Q9: Posso usar uma VPN no meu telemóvel e na smart TV?

Sim. Os fornecedores de VPN modernos oferecem aplicações dedicadas para iOS, Android, macOS, Windows, Linux e smart TV, bem como configurações em routers para proteger todos os dispositivos da tua rede doméstica.

Q10: O que é um Kill Switch?

Um Kill Switch é uma funcionalidade de segurança que desliga automaticamente o teu dispositivo da Internet se a ligação VPN cair. Isto evita a fuga dos teus dados não encriptados ou do teu IP real.

Ponto de controlo 10: Perguntas frequentes avançadas sobre VPN (Parte C)

Explora aspetos técnicos e estruturais das redes privadas virtuais e dos protocolos de tunneling seguro.

Q1: Qual é a diferença entre WireGuard, OpenVPN e IKEv2?

O WireGuard é um protocolo moderno e leve (apenas cerca de 4000 linhas de código) que oferece velocidades elevadas e tempos de ligação rápidos. O OpenVPN é um protocolo de código aberto muito seguro e testado em batalha. O IKEv2 é excelente para dispositivos móveis graças à capacidade de voltar a ligar-se rapidamente ao mudar de rede. [4]

Q2: O que é o encaminhamento de VPN dupla ou Multi-Hop?

O Multi-Hop encaminha o teu tráfego através de dois ou mais servidores VPN em sequência. Isto acrescenta uma segunda camada de encriptação e ajuda a manter o teu endereço IP real oculto do segundo salto se um servidor for comprometido.

Q3: O que é a fuga de WebRTC e como a evita uma VPN?

O WebRTC é um protocolo de navegador que pode revelar os teus endereços IP local e público reais, mesmo quando uma VPN está ativa. As VPN premium bloqueiam ou falsificam os pedidos WebRTC nas suas aplicações para computador/telemóvel e nas extensões de navegador.

Q4: O que são servidores só com RAM e porque são importantes?

Os servidores tradicionais gravam dados em discos rígidos, que podem ser apreendidos ou comprometidos. Os servidores só com RAM (sem disco) funcionam inteiramente em memória volátil (RAM). Quando o servidor é reiniciado ou desligado, os dados guardados na memória são apagados.

Q5: Como contorna a ofuscação os bloqueios de VPN?

A ofuscação (ou "Stealth VPN") disfarça o tráfego VPN para parecer tráfego HTTPS normal (porta 443). Isto pode ajudar a contornar a inspeção profunda de pacotes (DPI) usada por governos ou redes escolares/de escritório para bloquear VPN.

Ponto de controlo 10: Perguntas frequentes avançadas sobre VPN (Parte D)

Explora aspetos técnicos e estruturais das redes privadas virtuais e dos protocolos de tunneling seguro.

Q6: O que é o split tunneling e quando devo usá-lo?

O split tunneling permite escolher quais as aplicações que passam pelo túnel VPN encriptado e quais as que se ligam diretamente à internet. Usa-o para encaminhar aplicações bancárias sensíveis pela VPN enquanto os jogos locais se ligam diretamente, evitando a latência acrescentada pela VPN.

Q7: Como funciona a confidencialidade de encaminhamento (Perfect Forward Secrecy)?

O PFS garante que é gerada uma chave de encriptação única e temporária para cada sessão. Mesmo que uma chave privada seja comprometida no futuro, não pode ser usada para decifrar sessões passadas ou futuras, porque estas usaram chaves independentes.

Q8: O que são as alianças 5/9/14 Eyes e porque me devem interessar?

A jurisdição pode afetar o processo legal que um fornecedor pode enfrentar, mas o risco prático para a privacidade depende também dos dados que o fornecedor conserva, da sua arquitetura técnica, da propriedade, dos relatórios de transparência e do historial de auditorias.

Q9: O que é a proteção contra fugas de DNS?

A proteção contra fugas de DNS força o teu dispositivo a enviar as consultas de pesquisa de sites (consultas DNS) através dos servidores DNS privados e encriptados da VPN, em vez dos servidores do teu ISP. Isto impede o teu ISP de rastrear os sites que visitas.

Q10: Uma VPN pode contornar a limitação de velocidade da Internet imposta pelo ISP?

Por vezes. Uma VPN pode ajudar quando um ISP abranda seletivamente atividades identificáveis, mas não supera a congestão, os limites de dados, os limites de velocidade ao nível da conta nem uma rede de fraca qualidade.

Referências técnicas e fontes

Publicações citadas, especificações criptográficas e normas oficiais de documentos utilizadas ao longo desta ficha de trabalho.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[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