Nome: _____ **Data:** _____ **Punteggio:** _____

Come nascondere il tuo indirizzo IP Scheda di lavoro

Nascondere gli indirizzi IP, mascherare la posizione, proxy, Tor e prevenire le perdite di DNS/WebRTC

PANORAMICA DI APPRENDIMENTO SULLE VPN

STUDENTE
STATO DI STUDENTE
Percorso Network Defender

SICURO
STATO DELLA CONNESSIONE
Protezione dei pacchetti di dati

ATTIVO
PROTEZIONE DALLE FUGHE
Protezione dalle fughe di DNS e IPv6

Benvenuto! Questo pacchetto di attività ti guida attraverso i principi fondamentali delle reti private virtuali (VPN). Esplorerai come i tunnel cifrati proteggono i tuoi dati, come funzionano i protocolli di rete e come individuare e ridurre le perdite di privacy.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia i concetti e i protocolli delle VPN.**
- [ ] **Parti 5-7: Risolvi cruciverba e parole nascoste.**
- [ ] **Parti 8-9: Risolvi casi di studio e la sfida del codice.**
- [ ] **Parte 10: Consulta le pagine delle domande frequenti di base e avanzate.**
- [ ] **Parte 11: Esplora 10 fatti interessanti dal mondo reale.**
- [ ] **Bonus: sfida Pensa veloce.**

Apri la guida alle VPN di VPN.com

URL: https://www.vpn.com/it/vpn/

Il tuo percorso di apprendimento sulle VPN

- Spiega come funzionano gli indirizzi IP e come rivelano le posizioni.
- Confronta proxy, Tor e VPN per il mascheramento degli indirizzi di rete.
- Individua i metodi per rilevare e prevenire le perdite di DNS e WebRTC.
- Comprendi come i siti web tracciano gli utenti tramite il loro IP pubblico.
- Valuta l'instradamento multi-hop e i tunnel cifrati per la protezione dell'IP.

ISTRUZIONI DELLA SCHEDA DI LAVORO SULLA PROTEZIONE DELL'IP

Rispondi alle domande a scelta multipla e vero/falso, completa le frasi con gli spazi vuoti usando l'elenco di parole, abbina le definizioni e risolvi il cruciverba e la ricerca di parole. Applica le tue conoscenze al nascondere il tuo indirizzo IP e al prevenire le perdite. Concludi con l'attività bonus Pensa veloce.

NASCONDERE IL TUO IP (INTRODUZIONE)

Il tuo indirizzo IP è un indirizzo postale digitale che espone la tua posizione fisica e le tue abitudini in rete. Nascondere il tuo IP è la prima linea di difesa contro il tracciamento online, la profilazione mirata e il blocco geografico. Capire come mascherare in sicurezza il tuo indirizzo aiuta a proteggere la tua privacy online.

LEGGI CON ATTENZIONE OGNI PUNTO DI CONTROLLO E SELEZIONA O SCRIVI LA RISPOSTA CORRETTA.

Punto di controllo 1: Sfida a scelta multipla

1. Che cosa rivela ai siti web che visiti l'indirizzo IP pubblico di un dispositivo?

- A. Il numero di carta di credito dell'utente
- B. La tua posizione approssimativa e il nome del tuo provider
- C. L'intera directory dei file locali
- D. Le impostazioni della lingua della tastiera

2. Quale metodo nasconde il tuo IP e cifra tutto il traffico a livello di sistema?

- A. Un normale proxy web
- B. Eliminare i cookie del browser
- C. Una rete privata virtuale (VPN)
- D. Disabilitare il firewall nativo

3. Qual è un importante limite di privacy nell'uso di un proxy web gratuito?

- A. Non cifra il traffico dati sulle reti pubbliche
- B. Richiede l'installazione di un sistema operativo esterno
- C. È totalmente illegale negli Stati Uniti
- D. Richiede il collegamento a una linea telefonica dedicata

4. In che modo la rete Tor offre un elevato anonimato agli utenti?

- A. Accelerando le velocità di connessione
- B. Instradando il traffico attraverso tre relay gestiti da volontari
- C. Registrando il tuo nome in un database globale
- D. Limitando l'accesso alle sole agenzie governative

5. Che cos'è una perdita DNS (DNS leak)?

- A. Un errore nell'invio di un'email all'indirizzo sbagliato
- B. Quando le query DNS aggirano il tunnel VPN e vanno all'ISP
- C. Un guasto hardware all'alimentatore del router locale
- D. Un aggiornamento del driver dell'adattatore di rete locale

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Un server proxy cifra il traffico in background del sistema operativo proprio come una VPN.

○ Vero ○ Falso

7 Domanda 7

7. L'instradamento di Tor è molto sicuro ma riduce la velocità di navigazione in rete.

○ Vero ○ Falso

8 Domanda 8

8. Le perdite WebRTC possono esporre il tuo vero IP durante una sessione VPN attiva.

○ Vero ○ Falso

9 Domanda 9

9. Con una VPN attiva e senza fughe, il tuo provider non può vedere quali siti web visiti.

○ Vero ○ Falso

10 Domanda 10

10. Nascondere il tuo indirizzo IP blocca il tracciamento tramite fingerprinting del browser.

○ Vero ○ Falso

Punto di controllo 3: Inserimento dei termini chiave

Leggi ogni frase qui sotto e completa lo spazio vuoto con il termine corretto dell'elenco di parole.

1. Un bypass del tunnel sicuro che espone le tue query di dominio si chiama _____ .

2. Le API di comunicazione _____ basate sul browser possono far trapelare accidentalmente il tuo indirizzo IP nativo.

3. Un _____ web reindirizza il traffico del browser ma non cifra il contenuto dei pacchetti.

4. La cifratura a più livelli della rete _____ offre alti livelli di anonimato.

5. Il tuo _____ pubblico è assegnato dal tuo operatore e rivela la tua zona.

6. Aggirare i blocchi regionali dei contenuti multimediali si ottiene tramite il _____ della posizione.

BANCA DELLE PAROLE DEL VOCABOLARIO

INDIRIZZO IP MASCHERAMENTO PERDITA DNS PROXY TOR TRACKING ISP TUNNEL VPN WEBRTC

Scrivi qui le tue risposte:

1. _____ **2.** _____

3. _____ **4.** _____

5. _____ **6.** _____

Punto di controllo 4: Abbinamento di concetti di rete

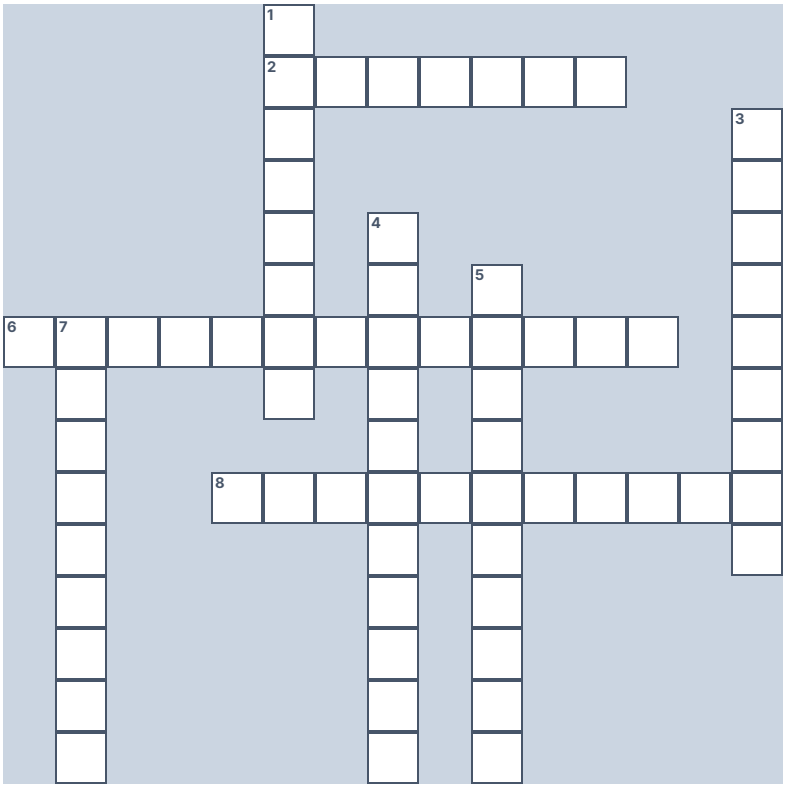
ABBINAMENTO DELLE DEFINIZIONI

Abbina ogni termine del vocabolario a sinistra alla sua definizione corretta a destra scrivendo la lettera corrispondente (A-H) nella casella compilabile.

☐	1. Indirizzo IP	A	Cifra tutto il traffico di un dispositivo e lo instrada attraverso un server VPN.
☐	2. Tunnel VPN	B	Instrada i dati attraverso tre server volontari, crittografando livelli a ogni passaggio.
☐	3. Rete Tor	C	Instradamento della connessione attraverso il server di un altro paese per aggirare i blocchi geografici.
☐	4. Proxy web	D	Etichetta numerica univoca che identifica l'interfaccia di un dispositivo su internet.
☐	5. Perdita DNS	E	Reindirizza il traffico del browser a livello di applicazione senza crittografia di sistema.
☐	6. API WebRTC	F	La registrazione, da parte del tuo operatore di telecomunicazioni, delle destinazioni del traffico internet non cifrato.
☐	7. Mascheramento della posizione	G	Query che vengono risolte al di fuori del tunnel VPN, esponendo all'ISP i domini visitati.
☐	8. Tracciamento da parte dell'ISP	H	Funzione del browser per voce/video che può aggirare i tunnel ed esporre i veri indirizzi IP.

Punto di controllo 5: Cruciverba

Risolvi il cruciverba digitando le lettere nelle caselle bianche attive. I numeri corrispondono alle definizioni qui sotto.



ORIZZONTALI

2. Instrada i dati attraverso tre server di volontari, cifrando i livelli a ogni passaggio (7)

6. Instradamento della connessione tramite un server di un altro paese per aggirare i blocchi geografici (13)

8. Etichetta numerica univoca che identifica l'interfaccia di un dispositivo su internet (11)

VERTICALI

1. Reindirizza il traffico del browser a livello di applicazione, senza cifratura del sistema (8)

3. Cifra tutto il traffico di un dispositivo e lo instrada attraverso un server VPN (9)

4. La registrazione delle destinazioni del traffico internet non cifrato da parte del tuo operatore telefonico (11)

5. Query risolte al di fuori del tunnel VPN, che espongono i domini visitati all'ISP (10)

7. Funzione del browser per voce e video che può aggirare i tunnel ed esporre gli indirizzi IP reali (9)

Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

Gli utenti di screen reader e di tastiera possono digitare le risposte del cruciverba direttamente nei campi di testo qui sotto.

ORIZZONTALI

2 orizzontale: Instrada i dati attraverso tre server di volontari, cifrando i livelli a ogni passaggio (7 lettere):

6 orizzontale: Instradamento della connessione tramite un server di un altro paese per aggirare i blocchi geografici (13 lettere):

8 orizzontale: Etichetta numerica univoca che identifica l'interfaccia di un dispositivo su internet (11 lettere):

VERTICALI

1 verticale: Reindirizza il traffico del browser a livello di applicazione, senza cifratura del sistema (8 lettere):

3 verticale: Cifra tutto il traffico di un dispositivo e lo instrada attraverso un server VPN (9 lettere):

4 verticale: La registrazione delle destinazioni del traffico internet non cifrato da parte del tuo operatore telefonico (11 lettere):

5 verticale: Query risolte al di fuori del tunnel VPN, che espongono i domini visitati all'ISP (10 lettere):

7 verticale: Funzione del browser per voce e video che può aggirare i tunnel ed esporre gli indirizzi IP reali (9 lettere):

Punto di controllo 6: Cerca la parola nascosta

Trova gli 8 termini chiave del vocabolario nascosti nella griglia qui sotto. Le parole possono essere orizzontali, verticali o diagonali.

T R A C K I N G I S P R Y B H

P L Z C T R B E W I P A G J R

I O P N W C M Z Y G Y O W E U

O K V P B N V T M G V D T Y U

Z S N D A T I D R E P E K R B

Z X Z Y M R Q X I P T D A D J

I Q V W W L J H T O H G B E I

R K T S V R Z E R H E S C A L

I Q C Z M K V R U A S W J M M

D H H N B E W Y X O R P H R F

N M A S C H E R A M E N T O K

I T L R W H B U F Y O Y W S H

T X T U N N E L V P N A P U N

N Z O I Q T I P V U O U U K A

E P M K A N V G G P Q X Y J K

ELENCO DELLE PAROLE DEL VOCABOLARIO

INDIRIZZOIP TUNNELVPN RETETOR PROXYWEB PERDITADNS APIWEBRTC MASCHERAMENTO TRACKINGISP

Punto di controllo 6, alternativa: Abbinamento accessibile del vocabolario

Abbina ciascuno degli 8 termini del vocabolario della Ricerca di parole alla sua definizione corretta scrivendo la lettera (A-H) nello spazio vuoto.

TERMINI DEL VOCABOLARIO

- **A. INDIRIZZOIP**
- **B. TUNNELVPN**
- **C. RETETOR**
- **D. PROXYWEB**
- **E. PERDITADNS**
- **F. APIWEBRTC**
- **G. MASCHERAMENTO**
- **H. TRACKINGISP**

DEFINIZIONI E CAMPI DI ABBINAMENTO

_____ 1. Reindirizza il traffico del browser a livello di applicazione, senza cifratura del sistema.

_____ 2. Instradamento della connessione tramite un server di un altro paese per aggirare i blocchi geografici.

_____ 3. Funzione del browser per voce e video che può aggirare i tunnel ed esporre gli indirizzi IP reali.

_____ 4. Etichetta numerica univoca che identifica l'interfaccia di un dispositivo su internet.

_____ 5. Instrada i dati attraverso tre server di volontari, cifrando i livelli a ogni passaggio.

_____ 6. La registrazione delle destinazioni del traffico internet non cifrato da parte del tuo operatore telefonico.

_____ 7. Query risolte al di fuori del tunnel VPN, che espongono i domini visitati all'ISP.

_____ 8. Cifra tutto il traffico di un dispositivo e lo instrada attraverso un server VPN.

Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave delle VPN. Scrivi le tue risposte nelle caselle compilabili.

1. **RZINIZIODPI** _____
2. **RTROTEE** _____
3. **PTNAEISDDR** _____
4. **ETMSAHORNE MAC** _____
5. **VEUNLNTPN** _____
6. **EBXWPYRO** _____
7. **BATCRWPEI** _____
8. **INPIATKRSGC** _____

Attività bonus: Pensa veloce

3 RISPOSTE PER CATEGORIA. VINCE CHI COMPLETA PER PRIMO LA LISTA.

1	Motivi per usare una VPN quando viaggi			
2	Browser che conosci			
3	Cose che una VPN può nascondere			
4	Parole legate alla privacy			
5	Parole di questa scheda che vuoi ricordare			
6	Cose che un sito web può dedurre dal tuo IP			
7	Numeri o simboli in un indirizzo IP			
8	Falsi miti sulle VPN			
9	Servizi VPN che conosci			
10	Cose che il tuo provider internet può vedere			
11	Promesse che fa un buon provider VPN			
12	Cose che possono far trapelare il tuo vero IP			
13	Motivi per nascondere la tua posizione			
14	Modi per nascondere il tuo indirizzo IP			
15	Dispositivi che possono usare una VPN			

Punto di controllo 8: Casi di studio sulle VPN

Applica i concetti che hai imparato per risolvere gli scenari reali qui sotto.

SARAH (STUDENTESSA AL BAR)

👩‍💻 "Ehi! Sono seduta al Coffee & Bytes. C'è una rete pubblica non protetta chiamata 'Free_Wi-Fi_No_Password'. Voglio accedere alla mia email della scuola e caricare il mio compito, ma ho paura degli hacker. Quali sono i rischi di usare questa rete senza una VPN e come fa una VPN a proteggere i miei dati?"

ALEX (STUDENTE VIAGGIATORE)

👩‍💻 "Oh no! Sono all'estero per un progetto e sto cercando di guardare un documentario di biologia ospitato su un server nel mio paese d'origine. Ma il sito dice 'Questo video non è disponibile nella tua posizione attuale.' Perché sono bloccato e come può aiutarmi una VPN a guardarlo?"

Punto di controllo 9: Decifrare il codice

Per completare la tua formazione sul mascheramento dell'IP, decifra questo messaggio segreto su come nascondere le tue tracce digitali.

CHIAVE DI CIFRATURA LETTERA-NUMERO

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

14 1 19 3 15 14 4 9 9 12 20 21 15

9 14 4 9 18 9 26 26 15 3 15 14 21 14

19 9 19 20 5 13 1 15 3 3 21 12 20 15

Messaggio decifrato:

SUGGERIMENTO: OGNI NUMERO RAPPRESENTA LA POSIZIONE DI QUELLA LETTERA NELL'ALFABETO (AD ES. 1 = A, 2 = B, 26 = Z).

Punto di controllo 10: Domande frequenti di base sulle VPN (Parte A)

Rivedi le domande e le risposte più comuni che i potenziali clienti pongono sull'uso delle reti private virtuali.

Q1: Che cos'è una VPN e come funziona?

Una Virtual Private Network (VPN) cifra la tua connessione Internet e instrada il tuo traffico attraverso un server remoto sicuro. In questo modo maschera il tuo indirizzo IP pubblico e limita ciò che gli osservatori della rete locale e il tuo ISP possono vedere del traffico instradato attraverso il tunnel VPN.

Q2: Perché dovrei usare una VPN?

Una VPN protegge la tua privacy digitale, mette al sicuro la connessione sulle reti Wi-Fi pubbliche (come bar o aeroporti), può ridurre il throttling basato sull'attività quando l'ISP non riesce a identificare il tipo di traffico cifrato, aggira le restrizioni geografiche per accedere a contenuti globali e aiuta a proteggere le risorse di lavoro da remoto.

Q3: Una VPN mi rende completamente anonimo online?

No. Anche se una VPN nasconde il tuo indirizzo IP e crittografa il traffico, puoi comunque essere tracciato tramite i cookie del browser, gli account attivi (come Google o Facebook), il fingerprinting del browser o se il tuo provider VPN registra i tuoi dati.

Q4: Un proxy web nasconde il mio indirizzo IP?

Sì, ma solo per il traffico inviato attraverso di esso, di solito il tuo browser. La maggior parte dei proxy web non cifra i tuoi dati, quindi il tuo ISP o il gestore della rete può comunque vedere ciò che invii e ricevi.

Q5: Nascondere il mio IP è legale?

In molti paesi sì, ma alcuni limitano o vietano le VPN e altri strumenti usati per nascondere un indirizzo IP. Nascondere il tuo IP non rende mai legale un atto illegale, quindi controlla le leggi locali prima di usarne uno.

Punto di controllo 10: Domande frequenti di base sulle VPN (Parte B)

Rivedi le domande e le risposte più comuni che i potenziali clienti pongono sull'uso delle reti private virtuali.

Q6: Tor nasconde il mio IP?

Sì. Tor invia il tuo traffico attraverso tre relay di volontari (guard, middle ed exit), quindi i siti web vedono l'indirizzo del relay di uscita, e nessun relay singolo conosce sia chi sei sia dove vai. [1]

Q7: Cosa rivela il mio IP?

Il tuo IP pubblico di solito rivela il tuo ISP e una posizione approssimativa, come il tuo paese o la tua città. I siti possono anche usarlo per collegare tra loro le tue visite e per applicare blocchi geografici.

Q8: Come verifico che sia nascosto?

Connettiti alla tua VPN, poi visita un sito di controllo dell'IP ed esegui i test di fuga DNS e WebRTC. L'IP e i server DNS mostrati dovrebbero appartenere alla VPN, non al tuo provider. Se compare il tuo IP reale, attiva la protezione dalle fughe.

Q9: Posso usare una VPN sul telefono e sulla smart TV?

Sì. I provider VPN moderni offrono app dedicate per iOS, Android, macOS, Windows, Linux e smart TV, oltre a configurazioni per router che proteggono tutti i dispositivi della tua rete domestica.

Q10: Che cos'è un Kill Switch?

Il Kill Switch è una funzione di sicurezza che scollega automaticamente il dispositivo da Internet se la connessione VPN cade. In questo modo i tuoi dati non cifrati o il tuo vero indirizzo IP non vengono esposti.

Punto di controllo 10: Domande frequenti avanzate sulle VPN (Parte C)

Esplora gli aspetti tecnici e strutturali delle reti private virtuali e dei protocolli di tunneling sicuro.

Q1: Perché i siti web possono ancora tracciarmi dopo che ho nascosto il mio indirizzo IP?

Nascondere il tuo IP non impedisce il fingerprinting del browser. I tracker possono combinare dettagli come la risoluzione dello schermo, i font installati e le impostazioni del browser in un identificatore, e anche i cookie o gli account con accesso effettuato possono identificarti, quindi usa anche un browser attento alla privacy. [3]

Q2: Che cos'è il routing a doppia VPN o Multi-Hop?

Il multi-hop instrada il tuo traffico attraverso due o più server VPN in sequenza. Questo aggiunge un secondo livello di crittografia e aiuta a mantenere nascosto il tuo vero indirizzo IP al secondo hop se un server viene compromesso.

Q3: Cos'è la fuga WebRTC e come la previene una VPN?

WebRTC è un protocollo del browser che può rivelare i tuoi veri indirizzi IP locale e pubblico anche quando una VPN è attiva. Le VPN premium bloccano o falsificano le richieste WebRTC nelle loro app desktop/mobili e nelle estensioni del browser.

Q4: Il traffico IPv6 può far trapelare il mio vero indirizzo IP?

Sì, se la tua VPN instrada nel tunnel solo l'IPv4. Il tuo dispositivo potrebbe allora inviare traffico IPv6 fuori dal tunnel, esponendo un indirizzo assegnato dal tuo ISP. Usa una VPN che instradi nel tunnel o blocchi l'IPv6 e verificalo con un test di perdite IPv6.

Q5: Come aggira i blocchi VPN l'offuscamento?

L'offuscamento (o "Stealth VPN") fa apparire i pacchetti del traffico VPN come normale traffico web HTTPS (porta 443). Questo aiuta a superare la Deep Packet Inspection (DPI) usata da governi o reti scolastiche e aziendali per bloccare le VPN.

Punto di controllo 10: Domande frequenti avanzate sulle VPN (Parte D)

Esplora gli aspetti tecnici e strutturali delle reti private virtuali e dei protocolli di tunneling sicuro.

Q6: Lo split tunneling espone il mio vero indirizzo IP?

Sì, per le app che escludi. Il traffico inviato fuori dal tunnel usa il tuo IP reale, e la RFC 8828 osserva che WebRTC può rivelare l'indirizzo dell'ISP sotto una VPN con split tunneling, a meno che il browser non lo limiti. [2]

Q7: Cos'è un indirizzo IP condiviso e come aiuta la privacy?

Con un IP condiviso, molti utenti VPN appaiono online con lo stesso indirizzo nello stesso momento. Questo rende molto più difficile per un sito web associare una singola visita a te rispetto a un IP dedicato usato solo da te.

Q8: Il mio ISP può vedere che sto usando una VPN per nascondere il mio IP?

Di solito sì. Il tuo ISP può vedere che ti connetti all'indirizzo IP di un server VPN, quando ti connetti e quanti dati invii, ma non i siti web che visiti né il contenuto all'interno del tunnel cifrato.

Q9: Cos'è la protezione dalle fughe DNS?

La protezione dalle fughe di DNS costringe il tuo dispositivo a inviare le richieste di ricerca dei siti web (richieste DNS) attraverso i server DNS privati e cifrati della VPN anziché quelli del tuo ISP. Questo impedisce al tuo ISP di tracciare quali siti visiti.

Q10: Per nascondere il mio IP è meglio un proxy o una VPN?

Di solito una VPN è meglio. Nasconde il tuo IP per ogni app del dispositivo e cifra il traffico, mentre un proxy web in genere copre solo il browser e spesso non aggiunge alcuna cifratura.

Parte 11: 10 fatti interessanti sulle VPN e spunti dal mondo reale

Rivedi questi fatti e approfondimenti reali, molto utili, sulla storia, sul mercato e sulla tecnologia delle VPN.

1. PRIMO PROTOCOLLO VPN

PPTP (Point-to-Point Tunneling Protocol), un primo protocollo VPN nato negli anni '90 da un gruppo guidato da Microsoft, oggi è considerato non sicuro, quindi le VPN moderne usano WireGuard o OpenVPN.

2. FINGERPRINTING

Nascondere il tuo IP non impedisce il fingerprinting del browser, che può identificarti a partire da dettagli come la risoluzione dello schermo e i font installati. [3]

3. LA RIVOLUZIONE WIREGUARD

WireGuard ha un codice molto snello, progettato per l'efficienza, che lo rende più facile da controllare per individuare vulnerabilità di sicurezza rispetto ai protocolli tradizionali.

4. ESPOSIZIONE DELL'INDIRIZZO WEBRTC

La RFC 8828 avverte che WebRTC può scoprire sia l'indirizzo pubblico di una VPN sia l'indirizzo dell'ISP su cui la VPN funziona, a meno che il browser non lo limiti. [2]

5. ORIGINI DELL'ALLEANZA 5-EYES

La partnership di intelligence Five Eyes tra Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda è nata dalla cooperazione tra gli Alleati nell'intelligence dei segnali durante la seconda guerra mondiale.

6. ISPEZIONE APPROFONDITA DEI PACCHETTI

I firewall avanzati usano la Deep Packet Inspection (DPI) per analizzare i metadati dei pacchetti di rete e bloccare le caratteristiche standard delle connessioni VPN.

7. RIUTILIZZO DEL CIRCUITO TOR

Tor riutilizza lo stesso circuito per circa dieci minuti e poi ne crea uno nuovo, il che rende più difficile collegare tra loro le tue attività di navigazione. [1]

8. VPN DECENTRALIZZATE

Le VPN decentralizzate (dVPN) distribuiscono il traffico su una rete di nodi gestiti da peer, riducendo la dipendenza da un singolo provider centralizzato.

9. ANONIMATO: TOR CONTRO VPN

Una VPN fa passare il traffico attraverso un solo provider, mentre Tor (The Onion Router) lo invia attraverso tre relay volontari (guard, middle, exit) per massimizzare la privacy. [1]

10. PROXY CONTRO TUNNEL VPN

Un proxy web cambia l'indirizzo IP che un sito vede per il traffico del tuo browser, ma a differenza di una VPN di solito non cifra quel traffico né copre le altre app del dispositivo. [5]

Riferimenti tecnici e fonti

Pubblicazioni citate, specifiche crittografiche e standard di documentazione ufficiali utilizzati in questa scheda di lavoro.

RIFERIMENTI ACCADEMICI E DI SETTORE

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

Soluzioni: nascondere gli indirizzi IP, mascherare la posizione, proxy, Tor e prevenire le perdite di DNS/WebRTC

1 Domanda 1

Risposta corretta: B

NOTA DIDATTICA

Che cosa rivela ai siti web che visiti l'indirizzo IP pubblico di un dispositivo? → La tua posizione approssimativa e il nome del tuo provider

2 Crittografia di sistema della VPN

LATENZA

Risposta corretta: C

NOTA DIDATTICA

A differenza dei proxy, che reindirizzano solo il traffico del browser, una VPN crea un tunnel cifrato a livello di sistema, proteggendo applicazioni in background, giochi e query del sistema operativo. Citazione: Tor Project Relays, W3C WebRTC API.

3 Assenza di crittografia nei proxy

SICUREZZA WI-FI

Risposta corretta: A

NOTA DIDATTICA

I proxy web inoltrano solo il traffico del browser senza crittografare il contenuto dei pacchetti, quindi il gestore della rete o il provider (ISP) può comunque tracciare il tuo traffico di contenuti. Citazione: IETF Proxy Vulnerabilities.

4 Domanda 4

Risposta corretta: B

NOTA DIDATTICA

In che modo la rete Tor offre un elevato anonimato agli utenti? → Instradando il traffico attraverso tre relay gestiti da volontari

5 Fughe di DNS dal tunnel

PRIVACY

Risposta corretta: B

NOTA DIDATTICA

Una fuga DNS si verifica quando le richieste di risoluzione dei nomi di dominio aggirano il tunnel VPN e vanno direttamente ai resolver del tuo ISP, esponendo i registri dei domini visitati. Fonti: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Dettagli sui limiti dei proxy** MASCHERAMENTO DELL'IP — **Risposta corretta: Falso**

NOTA DIDATTICA

I proxy funzionano a livello di applicazione e non hanno l'integrazione con il driver di rete a livello di sistema di un tunnel VPN. Fonte: IETF Proxy Vulnerabilities.

7 **Domanda 7** — **Risposta corretta: Vero**

NOTA DIDATTICA

Instradare il traffico attraverso tre relay di volontari con cifratura a strati aggiunge latenza, quindi Tor di solito è più lento di una connessione diretta.

8 **Domanda 8** — **Risposta corretta: Vero**

NOTA DIDATTICA

WebRTC può rivelare gli indirizzi locali e, con alcune configurazioni VPN, l'IP pubblico assegnato dal provider sotto il tunnel (RFC 8828).

9 **Domanda 9** — **Risposta corretta: Vero**

NOTA DIDATTICA

Senza fughe di DNS o WebRTC, il provider vede solo il traffico cifrato verso il server VPN, non i siti che visiti.

10 **Limiti del fingerprinting** NO-LOG — **Risposta corretta: Falso**

NOTA DIDATTICA

Il fingerprinting prende di mira le metriche di configurazione del dispositivo (risoluzione dello schermo, font, plugin) che restano visibili anche quando l'IP è nascosto. Citazione: EFF Tracking Evasion.

Chiavi del vocabolario e griglia di valutazione

Griglia di valutazione per l'insegnante: assegna 1 punto per ogni abbinamento corretto (8 punti in totale) e per ogni termine di contesto (6 punti in totale).

PUNTO DI CONTROLLO 4: SOLUZIONI ABBINAMENTO DI CONCETTI

D 1. Indirizzo IP	A 2. Tunnel VPN	B 3. Rete Tor	E 4. Proxy web
G 5. Perdita DNS	H 6. API WebRTC	C 7. Mascheramento della posizione	F 8. Tracciamento da parte dell'ISP

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 PERDITA DNS	2 WEBRTC	3 PROXY	4 TOR
5 INDIRIZZO IP	6 MASCHERAMENTO		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 D – PROXYWEB	2 G – MASCHERAMENTO	3 F – APIWEBRTC	4 A – INDIRIZZOIP
5 C – RETETOR	6 H – TRACKINGISP	7 E – PERDITADNS	8 B – TUNNELVPN

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare Indirizzo IP, Tunnel VPN e Rete Tor con parole proprie e fare un esempio per ciascuno.

Casi di studio:
Chiedi agli studenti di motivare le loro raccomandazioni con fatti tratti dalla scheda anziché con supposizioni.

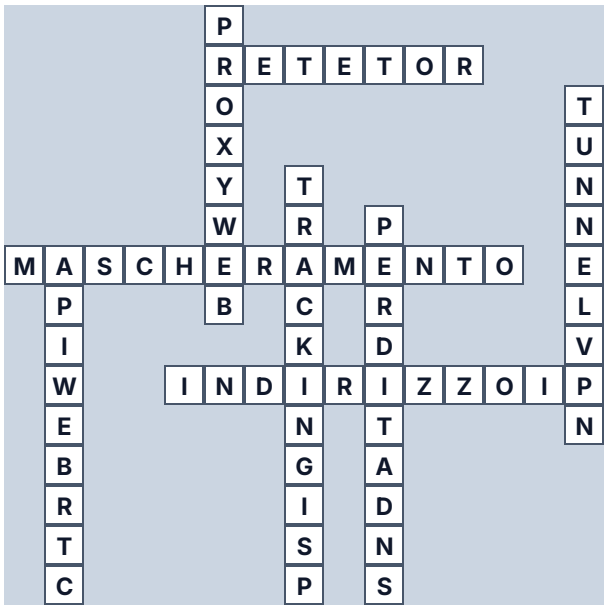
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

T	R	A	C	K	I	N	G	I	S	P	R	Y	B	H
P	L	Z	C	T	R	B	E	W	I	P	A	G	J	R
I	O	P	N	W	C	M	Z	Y	G	Y	O	W	E	U
O	K	V	P	B	N	V	T	M	G	V	D	T	Y	U
Z	S	N	D	A	T	I	D	R	E	P	E	K	R	B
Z	X	Z	Y	M	R	Q	X	I	P	T	D	A	D	J
I	Q	V	W	W	L	J	H	T	O	H	G	B	E	I
R	K	T	S	V	R	Z	E	R	H	E	S	C	A	L
I	Q	C	Z	M	K	V	R	U	A	S	W	J	M	M
D	H	H	N	B	E	W	Y	X	O	R	P	H	R	F
N	M	A	S	C	H	E	R	A	M	E	N	T	O	K
I	T	L	R	W	H	B	U	F	Y	O	Y	W	S	H
T	X	T	U	N	N	E	L	V	P	N	A	P	U	N
N	Z	O	I	Q	T	I	P	V	U	O	U	U	K	A
E	P	M	K	A	N	V	G	G	P	Q	X	Y	J	K

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

2 orizzontale: RETETOR Instrada i dati attraverso tre server di volontari, cifrando i livelli a ogni passaggio (7 lettere)

6 orizzontale: MASCHERAMENTO Instradamento della connessione tramite un server di un altro paese per aggirare i blocchi geografici (13 lettere)

8 orizzontale: INDIRIZZOIP Etichetta numerica univoca che identifica l'interfaccia di un dispositivo su internet (11 lettere)

VERTICALI

1 verticale: PROXYWEB Reindirizza il traffico del browser a livello di applicazione, senza cifratura del sistema (8 lettere)

3 verticale: TUNNELVPN Cifra tutto il traffico di un dispositivo e lo instrada attraverso un server VPN (9 lettere)

4 verticale: TRACKINGISP La registrazione delle destinazioni del traffico internet non cifrato da parte del tuo operatore telefonico (11 lettere)

5 verticale: PERDITADNS Query risolte al di fuori del tunnel VPN, che espongono i domini visitati all'ISP (10 lettere)

7 verticale: APIWEBRTC Funzione del browser per voce e video che può aggirare i tunnel ed esporre gli indirizzi IP reali (9 lettere)

Soluzioni delle parole mescolate e del codice cifrato

Chiave di valutazione per l'attività di riordino delle parole del vocabolario e per la sfida del codice segreto.

CHIAVE DELLE PAROLE DA RIORDINARE

1. RZINIZIODPI — **INDIRIZZOIP**
2. RTROTEE — **RETETOR**
3. PTNAEISDDR — **PERDITADNS**
4. ETMSAHORNEMAC — **MASCHERAMENTO**
5. VEUNLNTPN — **TUNNELVPN**
6. EBXWPYRO — **PROXYWEB**
7. BATCRWPEI — **APIWEBRTC**
8. INPIATKRSGC — **TRACKINGISP**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"NASCONDI IL TUO INDIRIZZO CON UN SISTEMA OCCULTO"

Soluzioni dei casi di studio

A Scenario A: sicurezza della rete pubblica

SNIFFING E CRITTOGRAFIA | Il dilemma di Sarah

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Rischi: sniffing dei pacchetti, intercettazione dei dati e attacchi man-in-the-middle. Qualcuno sulla stessa rete del bar potrebbe catturare i suoi dati di accesso o il file dei compiti.
- Protezione VPN: cifra i dati utili dei pacchetti di rete, rendendo illeggibile il traffico del tunnel intercettato per chi origlia passivamente sulla rete locale, quando la VPN è configurata correttamente.

B Scenario B: Accesso a risorse bloccate

GEO-BLOCCO E IP | Il dilemma di Alex

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Perché è bloccato: l'host di streaming usa il blocco geografico, che associa l'indirizzo IP locale del viaggiatore al suo paese fisico e lo blocca in base alle licenze territoriali.
- Come aiuta la VPN: mascherando la sua posizione reale instradando il traffico attraverso un server nel suo paese d'origine. Il sito vede l'IP del paese d'origine e consente l'accesso.