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

Sicurezza e crittografia del Wi-Fi pubblico

Attacchi man-in-the-middle, access point non autorizzati, sniffing dei pacchetti, tunnel VPN e crittografia HTTPS.

PANORAMICA DI APPRENDIMENTO SULLA SICUREZZA DEL WI-FI PUBBLICO

PROTETTO
CRITTOGRAFIA DEI DATI
Standard AES a 256 bit

CONFORME
STANDARD GLOBALI
Framework GDPR e CCPA

ZERO-TRUST
POLITICA DI ACCESSO
Autenticazione a più fattori

Benvenuto! Questo pacchetto di attività ti guida attraverso la sicurezza del Wi-Fi pubblico. Esplorerai le reti non cifrate, gli attacchi man-in-the-middle (MitM), i punti di accesso non autorizzati, il packet sniffing, i tunnel VPN e la sicurezza del transito HTTPS.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia la sicurezza informatica e la prevenzione delle minacce.**
- [ ] **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 alla sicurezza informatica di VPN.com

URL: https://www.vpn.com/it/sicurezza-informatica/sicurezza-wifi-pubblico/

Il tuo percorso di apprendimento sulla sicurezza del Wi-Fi pubblico

- Individua i rischi comuni del Wi-Fi pubblico, tra cui il packet sniffing e i punti di accesso non autorizzati.
- Implementa tunnel di crittografia VPN per proteggere i dati in transito.
- Imponi HTTPS e impostazioni sicure del browser web per i lavoratori da remoto.

ISTRUZIONI DELLA GUIDA SULLA SICUREZZA DEL WI-FI PUBBLICO

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 alla sicurezza dell'accesso remoto. Concludi con l'attività bonus Pensa veloce.

SICUREZZA DEL WI-FI PUBBLICO E PROTEZIONE DEL TRANSITO (INTRODUZIONE)

Gli hotspot Wi-Fi pubblici non cifrati lasciano il traffico di rete esposto allo sniffing dei pacchetti e allo spoofing Evil Twin. Forzare il traffico attraverso tunnel di crittografia VPN sicuri e applicare le regole HSTS solo HTTPS protegge le sessioni dall'intercettazione sulla rete locale.

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

Punto di controllo 1: Sfida a scelta multipla

1. Che cos'è un attacco Man-in-the-Middle (MitM)?

- A. Intercettare e alterare le comunicazioni tra due parti su una rete condivisa
- B. Una tecnica di estrazione di database che prende di mira i record degli utenti
- C. Sovraccaricare i server web con richieste di traffico di rete
- D. Cancellare i volumi di archiviazione dell'unità disco locale

2. Che cos'è un access point non autorizzato (Evil Twin)?

- A. Un hotspot Wi-Fi dannoso configurato con lo stesso SSID di una rete legittima
- B. Uno strumento amministrativo usato per monitorare i backup dei database
- C. Una configurazione sicura del gateway VPN
- D. Un record DNS che associa i server di posta autorizzati

3. Come protegge una VPN il traffico del Wi-Fi pubblico?

- A. Racchiude tutti i pacchetti di rete in un tunnel cifrato, rendendoli illeggibili agli sniffer
- B. Blocca automaticamente tutte le richieste di connessione in ingresso
- C. Modifica l'indirizzo MAC della scheda di rete fisica
- D. Elimina i cookie memorizzati nella cache del browser web

4. Che cos'è il packet sniffing?

- A. Usare strumenti hardware o software per catturare e registrare i pacchetti di rete
- B. Cercare file duplicati nelle directory locali
- C. Limitare i privilegi di lettura del database in base ai ruoli degli utenti
- D. Cifrare le unità di archiviazione usando chiavi AES-256

5. Qual è il ruolo di HTTPS?

- A. Cifrare il traffico della sessione tra il browser e il server web
- B. Filtrare i messaggi email in ingresso al gateway
- C. Comprimere le immagini per caricare le pagine più velocemente
- D. Gestire le strutture dei file nello storage collegato alla rete

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Gli utenti connessi possono catturare facilmente dati in chiaro sulle reti Wi-Fi pubbliche aperte.

- ◯ Vero
- ◯ Falso

7 Domanda 7

7. I punti di accesso non autorizzati (Evil Twin) sono sempre autorizzati dagli amministratori di rete.

- ◯ Vero
- ◯ Falso

8 Domanda 8

8. Una VPN è inefficace nel proteggere il traffico dal packet sniffing sulle reti pubbliche.

- ◯ Vero
- ◯ Falso

9 Domanda 9

9. HTTPS cifra solo il percorso dell'URL, lasciando il payload dei pacchetti in chiaro.

- ◯ Vero
- ◯ Falso

10 Domanda 10

10. Gli hotspot Wi-Fi che usano la sicurezza WPA3 offrono una protezione più forte rispetto alle reti aperte e senza password.

- ◯ 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. Catturare le password private su un Wi-Fi pubblico è l' _____ delle comunicazioni.
2. Analizzare i pacchetti grezzi su una rete locale si chiama packet _____ .
3. Un hotspot illegittimo che imita il Wi-Fi di un hotel è un _____ .
4. Proteggere il transito del traffico web richiede la cifratura con _____ .
5. Cifrare tutto il traffico di rete in uscita richiede un _____ .
6. Un percorso di comunicazione cifrato attraverso le reti pubbliche è un _____ .

BANCA DELLE PAROLE DEL VOCABOLARIO

CIFRATURA WPA | CLIENT VPN | EVIL TWIN | FIREWALL | HTTPS | INTERCETTAZIONE | SNIFFING | TUNNEL

Scrivi qui le tue risposte:

1.
2.
3.
4.
5.
6.

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

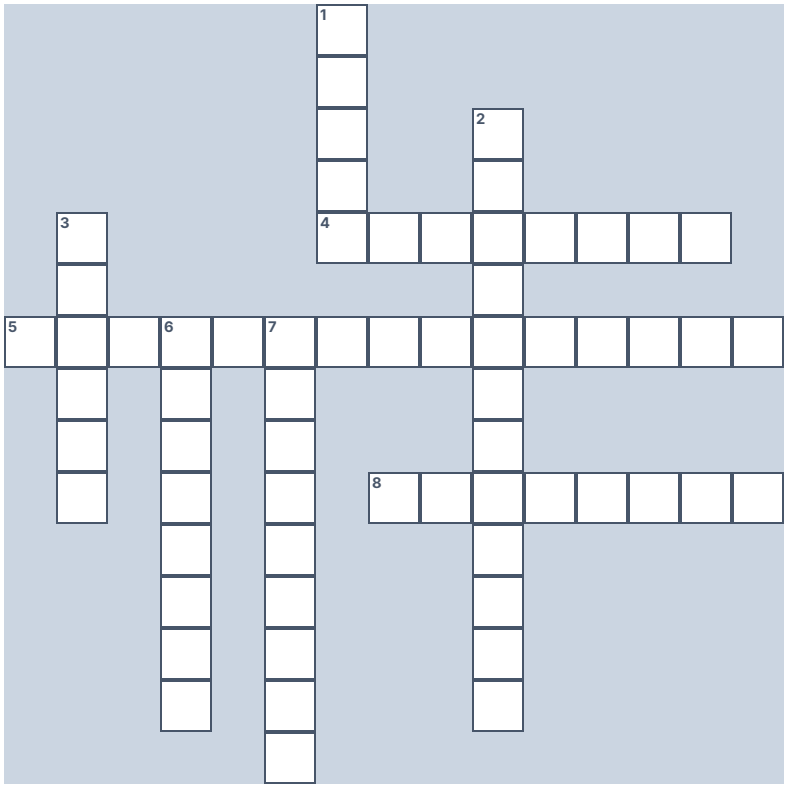
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. INTERCETTAZIONE	A	Standard moderno di sicurezza Wi-Fi.
☐	2. SNIFFING	B	Percorso dati sicuro in transito.
☐	3. EVIL TWIN	C	Filtrare il traffico in entrata.
☐	4. HTTPS	D	Hotspot non autorizzato che imita il Wi-Fi.
☐	5. VPN	E	Lettura del traffico in transito.
☐	6. TUNNEL	F	Acquisire i pacchetti di dati di rete.
☐	7. WPA3	G	Rete privata virtuale cifrata.
☐	8. FIREWALL	H	Trasmissione web sicura.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

4. Cattura dei pacchetti di dati di rete. (8)

5. Lettura del traffico in transito. (15)

8. Filtraggio del traffico in entrata. (8)

VERTICALI

1. Trasmissione web sicura. (5)

2. Moderno standard WPA3 (WPA tre) di sicurezza Wi-Fi. (12)

3. Percorso dati sicuro in transito. (6)

6. Hotspot illegittimo che imita un Wi-Fi. (8)

7. Rete privata virtuale cifrata. (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

4 orizzontale: Cattura dei pacchetti di dati di rete. (8 lettere):

5 orizzontale: Lettura del traffico in transito. (15 lettere):

8 orizzontale: Filtraggio del traffico in entrata. (8 lettere):

VERTICALI

1 verticale: Trasmissione web sicura. (5 lettere):

2 verticale: Moderno standard WPA3 (WPA tre) di sicurezza Wi-Fi. (12 lettere):

3 verticale: Percorso dati sicuro in transito. (6 lettere):

6 verticale: Hotspot illegittimo che imita un Wi-Fi. (8 lettere):

7 verticale: Rete privata virtuale cifrata. (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 U N N E L I I N N K Q P G M
M N Q R S T S N T G C C S Q O
H I S B W P D T S Z I V C Z W
F W K H T Z D E N D F Q X P C
N T U T B A Z R N D R K A D O
P L H D F H I C D R A Q M E I
V I R Z S F F E Q V T F A A Q
T V O N P I T T X S U Q K R U
N E S D N R Y T B N R F S X W
E J A R Z E Y A Y I A L G I M
I R J M L W T Z O F W H Q Q H
L Z A O V A G I U F P B Y R Y
C B H L Z L G O J I A O P N W
C M Z Y G L Y N O N W U K V P
B N V T M G V E D G Y U K R B

ELENCO DELLE PAROLE DEL VOCABOLARIO

INTERCETTAZIONE SNIFFING EVILTWIN HTTPS CLIENTVPN TUNNEL CIFRATURAWPA FIREWALL

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	DEFINIZIONI E CAMPI DI ABBINAMENTO
A. INTERCETTAZIONE	_____ 1. Moderno standard WPA3 (WPA tre) di sicurezza Wi-Fi.
B. SNIFFING	_____ 2. Hotspot illegittimo che imita un Wi-Fi.
C. EVILTWIN	_____ 3. Cattura dei pacchetti di dati di rete.
D. HTTPS	_____ 4. Percorso dati sicuro in transito.
E. CLIENTVPN	_____ 5. Filtraggio del traffico in entrata.
F. TUNNEL	_____ 6. Lettura del traffico in transito.
G. CIFRATURAWPA	_____ 7. Rete privata virtuale cifrata.
H. FIREWALL	_____ 8. Trasmissione web sicura.

Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave della sicurezza informatica. Scrivi le tue risposte nelle caselle fornite.

1. CEATZNTTIOI NEER
2. LENVIWTI
3. CTNLVNEPI
4. PRAFUATWAC IR
5. FINGFSNI
6. PHTST
7. ETNLNU
8. EIWLFLAR

Attività bonus: Pensa veloce

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

1	Motivi per aggiornare il software			
2	Dispositivi che si collegano automaticamente al Wi-Fi			
3	Informazioni che non dovresti mai condividere			
4	Buone abitudini sicure che puoi iniziare oggi			
5	Modi per restare al sicuro in un bar			
6	Dispositivi che possono essere hackerati			
7	Cose che un hacker può vedere su un Wi-Fi aperto			
8	Segnali di una rete Wi-Fi falsa			
9	Alternative al Wi-Fi pubblico			
10	Segnali di allarme in un'email			
11	Cose che non fai sul Wi-Fi pubblico			
12	Luoghi con Wi-Fi gratuito			
13	Modi per proteggere i tuoi account			
14	Segnali che indicano che un computer è infetto			
15	Nomi di Wi-Fi che sembrano sospetti			

Punto di controllo 8: Casi di studio sulla sicurezza informatica

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

CASO DI STUDIO 1: CONTENIMENTO DELL'INTERCETTAZIONE DEI PACCHETTI SU WI-FI PUBBLICO



Scenario: Un dirigente commerciale da remoto, collegato alla rete Wi-Fi pubblica di un aeroporto, nota che diverse email aziendali sensibili vengono diffuse poco dopo essere state inviate in chiaro.

Domanda di discussione: Analizza i rischi delle reti pubbliche e illustra una soluzione di cifratura del traffico.

CASO DI STUDIO 2: DIFESA DA HOTSPOT FALSI EVIL TWIN



Scenario: Degli aggressori installano un punto di accesso wireless non autorizzato chiamato 'CoffeeShop_Guest' che imita un hotspot legittimo di un bar, catturando il traffico di rete degli ospiti ignari.

Domanda di discussione: Descrivi nel dettaglio i passaggi di verifica per rilevare e bloccare i punti di accesso non autorizzati.

Punto di controllo 9: Decifrare il codice

Un professionista della sicurezza informatica protegge le risorse di rete dagli attori delle minacce online. Usa la chiave lettera-numero qui sotto per decifrare il messaggio scrivendo le lettere corrispondenti negli spazi vuoti.

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

3	9	6	18	1		9	12		20	18	1	6	6	9	3	15	
4	5	12															

23	9	6	9		16	21	2	2	12	9	3	15		3	15	14	
21	14	1															

22	16	14

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 sulla sicurezza informatica (Parte A)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q1: Perché il Wi-Fi pubblico non è sicuro?

Il Wi-Fi pubblico aperto non cifra il traffico via etere, quindi chi si trova nelle vicinanze può intercettare qualsiasi dato non protetto. [2]

Q2: Che cos'è il packet sniffing?

Un packet sniffer cattura i dati grezzi che transitano su un'interfaccia di rete, esponendo password in chiaro e dettagli del traffico.

Q3: Cos'è un Evil Twin?

Un access point non autorizzato creato da hacker che imita il nome e le impostazioni di un hotspot Wi-Fi locale affidabile.

Q4: Come mi protegge una VPN?

Instrada il tuo traffico attraverso un tunnel cifrato, nascondendo la tua attività di navigazione agli sniffer della rete locale.

Q5: HTTPS mi protegge sul Wi-Fi pubblico?

Sì, cifra i dati scambiati tra il tuo browser e il sito web, e una VPN aggiunge un ulteriore livello di protezione.

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte B)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q6: Cos'è WPA3?

Lo standard moderno Wi-Fi Protected Access, che offre una crittografia più forte e protezione contro gli attacchi a dizionario offline. [1]

Q7: Il Wi-Fi pubblico può diffondere malware?

Sì, gli aggressori possono intercettare il traffico e inserire richieste di download dannose (drive-by download) nella tua sessione del browser.

Q8: Qual è il rischio della condivisione di file?

Se la condivisione dei file è attiva, altri utenti della rete pubblica possono leggere o modificare l'elenco delle cartelle locali.

Q9: Cos'è un captive portal?

La pagina di accesso che le reti di hotel o caffè usano per concedere l'accesso a internet, che a volte può essere falsificata dagli aggressori.

Q10: Devo disattivare il Wi-Fi quando non lo uso?

Sì, disattivare il Wi-Fi impedisce al tuo dispositivo di connettersi automaticamente a reti non attendibili.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte C)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q1: Come sfrutta il DNS un attacco Man-in-the-Middle?

Usando il DNS spoofing su un router fraudolento per indirizzare i browser bersaglio verso pagine di destinazione di phishing simili invece dei domini originali.

Q2: Che cos'è il session hijacking?

Un aggressore che intercetta un cookie di sessione non cifrato sul Wi-Fi pubblico e lo importa per aggirare l'accesso con credenziali.

Q3: Cos'è lo SSL stripping?

Un attacco MitM in cui un aggressore declassa la richiesta HTTPS sicura di un utente a HTTP non cifrato, catturando i dati di accesso in chiaro.

Q4: Come protegge HSTS dallo SSL stripping?

HTTP Strict Transport Security obbliga i browser a connettersi solo tramite HTTPS, rifiutando il ripiego su HTTP non cifrato. [3]

Q5: Cos'è una VPN con split tunneling?

Una configurazione che instrada attraverso la VPN solo il traffico aziendale mentre invia direttamente i dati Internet pubblici, il che può comportare il rischio di esposizione tramite percorsi di fuga.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte D)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q6: Perché WPA2 è vulnerabile a KRACK?

Il Key Reinstallation Attack sfrutta l'handshake a quattro vie del WPA2 per decifrare i pacchetti senza la password del Wi-Fi.

Q7: Cos'è l'isolamento dei client?

Un'impostazione di sicurezza del router che impedisce ai dispositivi Wi-Fi collegati di comunicare direttamente tra loro, bloccando lo sniffing locale.

Q8: Come usano gli aggressori i server DNS falsi?

Configurano router non autorizzati per assegnare ai client server DNS falsi, consentendo loro di intercettare e riscrivere tutte le ricerche web.

Q9: Una VPN può nascondere il mio indirizzo MAC locale?

No. Gli indirizzi MAC sono identificatori locali di livello 2; usa invece l'impostazione di randomizzazione MAC integrata nel tuo dispositivo (indirizzo privato).

Q10: Che cos'è un attacco di spoofing del captive portal?

Un aggressore che ospita un falso portale di autenticazione su un hotspot non autorizzato per rubare credenziali spacciandosi per un accesso Wi-Fi gratuito.

Parte 11: 10 fatti e spunti reali sulla sicurezza informatica

Rivedi fatti reali su violazioni della sicurezza, meccanismi di difesa e standard di conformità.

1. APPROFONDIMENTO SULLA SICUREZZA

I lavoratori da remoto usano spesso il Wi-Fi di bar, hotel e aeroporti, dove non possono controllare la sicurezza della rete.

2. APPROFONDIMENTO SULLA SICUREZZA

Un hotspot non autorizzato Evil Twin può copiare il nome esatto e l'indirizzo MAC di una rete affidabile, confondendo i dispositivi.

3. APPROFONDIMENTO SULLA SICUREZZA

Il software di packet sniffing come Wireshark è gratuito e può mostrare in chiaro le password HTTP non cifrate.

4. APPROFONDIMENTO SULLA SICUREZZA

La sicurezza WPA3 utilizza la Simultaneous Authentication of Equals (SAE) per proteggere dagli attacchi di forza bruta locali.

5. APPROFONDIMENTO SULLA SICUREZZA

Gli attacchi di SSL stripping aggirano le protezioni HTTPS di base intercettando sul gateway i reindirizzamenti HTTP iniziali.

6. APPROFONDIMENTO SULLA SICUREZZA

Le intestazioni di risposta HTTP Strict Transport Security (HSTS) impediscono ai browser di tornare a connessioni HTTP non cifrate. [3]

7. APPROFONDIMENTO SULLA SICUREZZA

Disattivare la 'Connessione automatica' impedisce agli smartphone di connettersi a reti non autorizzate che imitano quelle reali negli spazi pubblici.

8. APPROFONDIMENTO SULLA SICUREZZA

Le configurazioni VPN aziendali «always-on» costringono tutto il traffico di rete dei lavoratori da remoto a passare attraverso i firewall aziendali.

9. APPROFONDIMENTO SULLA SICUREZZA

I punti di accesso non autorizzati possono fornire risposte DNS falsificate, reindirizzando i domini presi di mira verso server di phishing.

10. APPROFONDIMENTO SULLA SICUREZZA

Senza una VPN, gli altri utenti di un hotspot aperto possono vedere quali siti e server contatta il tuo dispositivo.

Riferimenti tecnici e fonti

La guida di studio e i puzzle interattivi sono compilati a partire dagli standard globali NIST, OWASP e di conformità alla privacy dei dati.

RIFERIMENTI ACCADEMICI E DI SETTORE

[1] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Soluzioni: Punto di controllo 1 – Scelta multipla

1 Domanda 1

Risposta corretta: A

NOTA DIDATTICA

Che cos'è un attacco Man-in-the-Middle (MitM)? → Intercettare e alterare le comunicazioni tra due parti su una rete condivisa

2 Domanda 2

Risposta corretta: A

NOTA DIDATTICA

Che cos'è un access point non autorizzato (Evil Twin)? → Un hotspot Wi-Fi dannoso configurato con lo stesso SSID di una rete legittima

3 Domanda 3

Risposta corretta: A

NOTA DIDATTICA

Come protegge una VPN il traffico del Wi-Fi pubblico? → Racchiude tutti i pacchetti di rete in un tunnel cifrato, rendendoli illeggibili agli sniffer

4 Domanda 4

Risposta corretta: A

NOTA DIDATTICA

Che cos'è il packet sniffing? → Usare strumenti hardware o software per catturare e registrare i pacchetti di rete

5 Domanda 5

Risposta corretta: A

NOTA DIDATTICA

Qual è il ruolo di HTTPS? → Cifrare il traffico della sessione tra il browser e il server web

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Domanda 6** — **Risposta corretta: Vero**

NOTA DIDATTICA

Gli utenti connessi possono catturare facilmente dati in chiaro sulle reti Wi-Fi pubbliche aperte.

7 **Domanda 7** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: un Evil Twin è un hotspot non autorizzato creato da un aggressore per imitarne uno reale.

8 **Domanda 8** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: una VPN cifra il traffico in un tunnel, quindi gli sniffer locali non possono leggerlo.

9 **Domanda 9** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: HTTPS cifra l'intero scambio HTTP, compreso il percorso dell'URL e il contenuto della pagina.

10 **Domanda 10** — **Risposta corretta: Vero**

NOTA DIDATTICA

Gli hotspot Wi-Fi che usano la sicurezza WPA3 offrono una protezione più forte rispetto alle reti aperte e senza password.

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

E 1. INTERCETTAZIONE	F 2. SNIFFING	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. TUNNEL	A 7. WPA3	C 8. FIREWALL

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 INTERCETTAZIONE	2 SNIFFING	3 EVIL TWIN	4 HTTPS
5 CLIENT VPN	6 TUNNEL		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 G – CIFRATURAWPA	2 C – EVILTWIN	3 B – SNIFFING	4 F – TUNNEL
5 H – FIREWALL	6 A – INTERCETTAZIONE	7 E – CLIENTVPN	8 D – HTTPS

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare INTERCETTAZIONE, SNIFFING e EVIL TWIN 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.

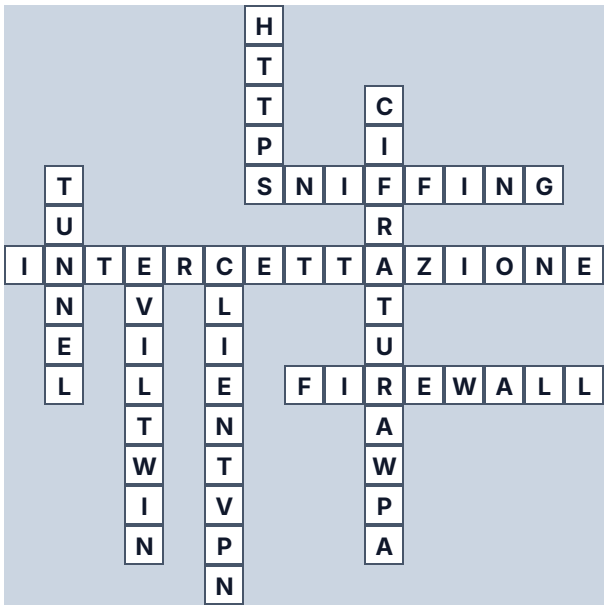
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

4 orizzontale: SNIFFING Cattura dei pacchetti di dati di rete. (8 lettere)

5 orizzontale: INTERCETTAZIONE Lettura del traffico in transito. (15 lettere)

8 orizzontale: FIREWALL Filtraggio del traffico in entrata. (8 lettere)

VERTICALI

1 verticale: HTTPS Trasmissione web sicura. (5 lettere)

2 verticale: CIFRATURAWPA Moderno standard WPA3 (WPA tre) di sicurezza Wi-Fi. (12 lettere)

3 verticale: TUNNEL Percorso dati sicuro in transito. (6 lettere)

6 verticale: EVILTWIN Hotspot illegittimo che imita un Wi-Fi. (8 lettere)

7 verticale: CLIENTVPN Rete privata virtuale cifrata. (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. CEATZNTTIOINEER — **INTERCETTAZIONE**
2. LENVIWTI — **EVILTWIN**
3. CTNLVNEPI — **CLIENTVPN**
4. PRAFUATWACIR — **CIFRATURAWPA**
5. FINGFSNI — **SNIFFING**
6. PHTST — **HTTPS**
7. ETNLNU — **TUNNEL**
8. EIWLFLAR — **FIREWALL**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"CIFRA IL TRAFFICO DEL WIFI PUBBLICO CON UNA VPN"

Soluzioni dei casi di studio

A Caso di studio 1: contenimento dell'intercettazione dei pacchetti su Wi-Fi pubblico

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un dirigente commerciale da remoto connesso a una rete Wi-Fi pubblica di un aeroporto nota che diverse email aziendali sensibili vengono divulgate poco dopo essere state inviate in chiaro.
- Strategia e soluzione consigliate: Rendi obbligatorio l'uso di un client VPN aziendale su tutte le postazioni remote. Applica estensioni del browser solo HTTPS e blocca i protocolli non crittografati (come HTTP e FTP) sul firewall del client.

B Caso di studio 2: Difesa da hotspot falsi evil twin

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: Alcuni aggressori installano un access point wireless non autorizzato chiamato «CoffeeShop_Guest» che imita l'hotspot legittimo di un bar e intercettano il traffico di rete degli ospiti ignari.
- Strategia e soluzione consigliate: verificare i BSSID (indirizzi MAC dei punti di accesso) per accertare l'autenticità della rete. Applicare la convalida della postura del client per bloccare la connessione alle reti aperte e imporre l'uso di hotspot cellulari per il lavoro sensibile.