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

Attacchi di phishing e ingegneria sociale

Spear phishing, truffe di whaling, protocolli SPF/DKIM/DMARC, spoofing del mittente e formazione sulla sicurezza per i dipendenti.

PANORAMICA DI APPRENDIMENTO SUGLI ATTACCHI DI PHISHING

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 gli attacchi di phishing e l'ingegneria sociale. Esplorerai lo spear phishing, il whaling, lo spoofing dei domini, i protocolli SPF/DKIM/DMARC, la sicurezza dei link e la formazione di sensibilizzazione dei dipendenti.

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/attacchi-phishing/

Il tuo percorso di apprendimento sulla mitigazione del phishing

- Individua le comuni truffe di phishing, vishing e pop-up di assistenza.
- Implementa procedure di verifica delle transazioni fuori banda.
- Configura le regole SPF, DKIM e DMARC per bloccare i domini contraffatti.

ISTRUZIONI DELLA GUIDA SUGLI ATTACCHI DI PHISHING

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 all'autenticazione delle email. Concludi con l'attività bonus Pensa veloce.

ATTACCHI DI PHISHING E INGEGNERIA SOCIALE (INTRODUZIONE)

Gli attacchi di phishing sfruttano messaggi mirati, truffe di whaling e spoofing di dominio per raccogliere le credenziali di accesso degli utenti. Proteggere i sistemi aziendali richiede di implementare regole SPF, DKIM e DMARC al gateway insieme a passaggi di approvazione fuori banda.

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 lo spear phishing?

- A. Un'email di phishing mirata, adattata a una specifica persona o organizzazione
- B. Un'email di massa inviata a milioni di indirizzi casuali
- C. Un attacco di rete che inonda di traffico i server web
- D. Una tecnica di estrazione da database che prende di mira i record degli utenti

2. Quale protocollo permette a un dominio di elencare nel DNS i propri indirizzi IP di invio autorizzati per contrastare lo spoofing?

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3. Che cos'è un attacco di whaling?

- A. Una campagna di phishing rivolta specificamente a dirigenti aziendali di alto profilo
- B. Un attacco SQL injection rivolto ai backup dei database
- C. Il furto fisico di apparecchiature router di una rete locale
- D. Una scansione automatizzata di credential stuffing con attacco a forza bruta

4. Che cosa fa DKIM?

- A. Aggiunge una firma crittografica alle email per verificare l'autenticità del mittente
- B. Blocca il traffico di pacchetti di rete in ingresso al firewall
- C. Crittografa i volumi di archiviazione dei database a riposo
- D. Analizza gli allegati email alla ricerca di malware basato su firme

5. Qual è il ruolo di DMARC?

- A. Indicare ai server di posta riceventi come gestire i controlli SPF/DKIM falliti
- B. Decifrare le password di sistema usando rainbow table precalcolate
- C. Comprimere gli allegati email prima della consegna
- D. Configurare i privilegi di accesso all'instradamento di rete

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Lo spear phishing si basa su email generiche di massa inviate a milioni di indirizzi casuali.

Vero Falso

7 Domanda 7

7. Le policy DMARC possono istruire i server di posta a rifiutare i messaggi falsificati non autorizzati.

Vero Falso

8 Domanda 8

8. La verifica SPF funziona convalidando la firma crittografica del corpo dell'email.

Vero Falso

9 Domanda 9

9. Gli attacchi di whaling prendono di mira gli amministratori aziendali di basso livello per accedere ai file dei database.

Vero Falso

10 Domanda 10

10. La verifica fuori banda delle richieste di pagamento aiuta a fermare le truffe con bonifici.

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. Prendere di mira un dipendente specifico con informazioni personalizzate è lo _____ phishing.
2. Falsificare l'intestazione di un'email per far sembrare legittimi i messaggi è lo _____ del mittente.
3. L'elenco, nei record DNS, degli IP dei server di posta autorizzati è il _____ .
4. Lo standard di firma delle email che verifica il mittente è _____ .
5. Stabilire criteri per rifiutare i controlli SPF/DKIM falliti si basa su _____ .
6. Una campagna di phishing rivolta ai dirigenti di alto livello si chiama _____ .

BANCA DELLE PAROLE DEL VOCABOLARIO

DKIM DMARC PHISHING RECORD SPF SPEAR SPOOFING VISHING WHALING

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

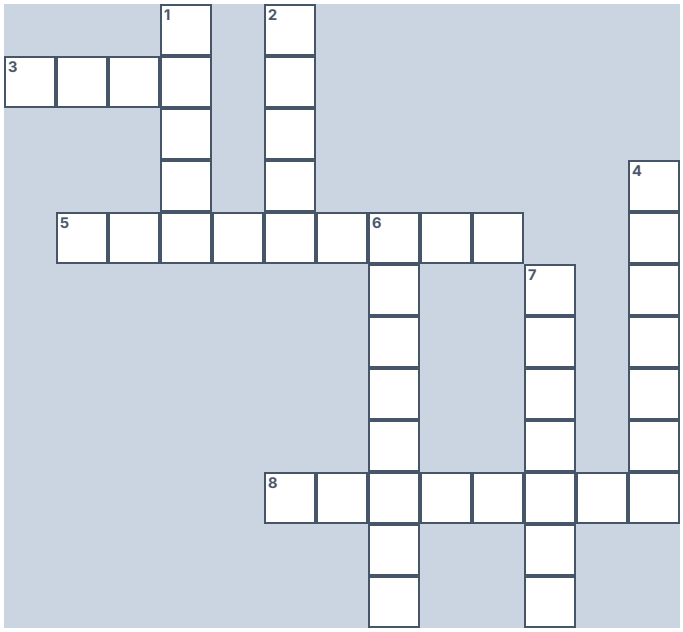
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. SPEAR	A	Telefonate truffa basate sulla voce.
☐	2. SPOOFING	B	Prendono di mira i dirigenti di livello C.
☐	3. SPF	C	Istruzioni di rifiuto delle policy.
☐	4. DKIM	D	IP dei mittenti autorizzati dal DNS.
☐	5. DMARC	E	Email di ingegneria sociale.
☐	6. WHALING	F	Email mirata e personalizzata.
☐	7. PHISHING	G	Falsificazione dell'indirizzo email del mittente.
☐	8. VISHING	H	Firma crittografica nelle email.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

3. Firma crittografica nelle email. (4)

5. IP dei mittenti autorizzati nel DNS. (9)

8. Email di ingegneria sociale. (8)

VERTICALI

1. Istruzioni di policy per il rifiuto. (5)

2. Email mirata e personalizzata. (5)

4. Chiamate truffa vocali. (7)

6. Falsificazione dell'indirizzo email del mittente. (8)

7. Bersaglio: dirigenti di alto livello. (7)

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

3 orizzontale: Firma crittografica nelle email. (4 lettere):

5 orizzontale: IP dei mittenti autorizzati nel DNS. (9 lettere):

8 orizzontale: Email di ingegneria sociale. (8 lettere):

VERTICALI

1 verticale: Istruzioni di policy per il rifiuto. (5 lettere):

2 verticale: Email mirata e personalizzata. (5 lettere):

4 verticale: Chiamate truffa vocali. (7 lettere):

6 verticale: Falsificazione dell'indirizzo email del mittente. (8 lettere):

7 verticale: Bersaglio: dirigenti di alto livello. (7 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.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

SPEAR SPOOFING RECORDSPF DKIM DMARC WHALING PHISHING VISHING

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. SPEAR	1. Falsificazione dell'indirizzo email del mittente.
B. SPOOFING	2. Email mirata e personalizzata.
C. RECORDSPF	3. Chiamate truffa vocali.
D. DKIM	4. IP dei mittenti autorizzati nel DNS.
E. DMARC	5. Email di ingegneria sociale.
F. WHALING	6. Istruzioni di policy per il rifiuto.
G. PHISHING	7. Firma crittografica nelle email.
H. VISHING	8. Bersaglio: dirigenti di alto livello.

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. **AESRP** _____
2. **FRPOEDSRC** _____
3. **ADCRM** _____
4. **SNGIHPHI** _____
5. **FIPGOSNO** _____
6. **IMDK** _____
7. **WNIGHLA** _____
8. **IHGVNIS** _____

Attività bonus: Pensa veloce

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

1	Dispositivi che possono essere hackerati			
2	Segnali di un'email di phishing			
3	Segnali che indicano che un computer è infetto			
4	Parole che creano una falsa urgenza			
5	Modi per verificare un mittente			
6	Persone a cui puoi chiedere aiuto per l'IT			
7	Cose di cui fai il backup			
8	Pesci o creature marine che conosci			
9	Aziende di cui i truffatori fingono di essere			
10	Buone abitudini sicure che puoi iniziare oggi			
11	Cose da fare dopo aver cliccato su un link falso			
12	Cose da fare dopo una fuga di dati			
13	Canali in cui avviene il phishing			
14	Cose che non invii mai per email			
15	Modi per proteggere i tuoi account			

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: RISOLUZIONE DI UN ATTACCO DI WHALING AI VERTICI AZIENDALI

👨‍💻

Scenario: Un direttore finanziario (CFO) riceve un'email altamente personalizzata che sostiene di provenire dall'amministratore delegato e che chiede un bonifico urgente di 50.000 $ per concludere l'acquisto riservato di un dominio.

Domanda di discussione: Analizza i rischi di spoofing del marchio e descrivi nel dettaglio SPF/DKIM/DMARC e i controlli di autenticazione.

CASO DI STUDIO 2: IMPLEMENTARE LE POLICY DI GATEWAY SPF/DKIM/DMARC

👨‍💻

Scenario: Un'azienda non supera gli audit di sicurezza perché le email di marketing in uscita vengono spesso segnalate come spam e gli hacker stanno falsificando attivamente il dominio del marchio aziendale.

Domanda di discussione: Definisci controlli tecnici e amministrativi per verificare l'autenticità delle email.

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

19	3	15	16	18	9		9	14	7	5	7	14	5	18	9	1
19	15	3	9	1	12	5		3	15	14		1	21	4	9	20
			4	5	12	12	5		5	13	1	9	12			

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: Che cos'è il phishing?

Il phishing è un attacco di ingegneria sociale in cui i criminali inviano messaggi fraudolenti per indurre gli utenti a condividere dati sensibili.

Q2: Qual è la differenza tra phishing e spear phishing?

Il phishing prende di mira grandi gruppi con contenuti generici, mentre lo spear phishing prende di mira vittime specifiche usando dettagli personalizzati.

Q3: Cos'è il whaling?

Il whaling è un attacco di phishing altamente mirato rivolto a dirigenti di alto profilo che detengono potere amministrativo.

Q4: Cos'è lo spoofing delle email?

Lo spoofing delle email consiste nel creare messaggi email con un indirizzo del mittente falsificato per indurre il destinatario a fidarsi della fonte.

Q5: Come previene lo spoofing l'SPF?

Pubblica nel DNS un elenco di indirizzi IP mittenti autorizzati, consentendo ai server riceventi di verificare l'origine della posta. [1]

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 DKIM?

DomainKeys Identified Mail aggiunge una firma crittografica alle intestazioni delle email, dimostrando che un dominio se ne è assunto la responsabilità e che il messaggio non è stato alterato.

Q7: Che cosa significa DMARC?

Domain-based Message Authentication, Reporting, and Conformance. [2]

Q8: Cos'è una policy DMARC?

Una policy che indica ai server di posta come trattare i messaggi che non superano SPF/DKIM (none, quarantine o reject). [2]

Q9: Cos'è il vishing?

Phishing vocale (vishing), in cui gli aggressori usano telefonate fraudolente per ottenere dati amministrativi o finanziari.

Q10: Come aiutano gli strumenti di scansione dei link?

Analizzano e riscrivono i link delle email in arrivo per verificare la sicurezza delle pagine web di destinazione nel momento del clic.

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 funziona un attacco omografico?

Gli aggressori registrano nomi di dominio usando caratteri Unicode non ASCII simili a quelli originali per imitare visivamente un nome di dominio legittimo.

Q2: Che cos'è una rappresentazione punycode?

Una codifica che converte i nomi di dominio Unicode in stringhe compatibili con ASCII che iniziano con 'xn--' in modo che il DNS possa gestirli.

Q3: Perché 'p=reject' è lo stato DMARC più sicuro?

Chiede ai server riceventi di rifiutare la posta che non supera DMARC (SPF/DKIM allineati) durante la sessione SMTP, bloccando lo spoofing diretto. [2]

Q4: Come aggirano gli aggressori le regole SPF?

Sfruttando domini simili (typosquatting) o usando account compromessi su servizi di posta di terze parti legittimi.

Q5: Cos'è la compromissione delle email aziendali (BEC)?

Una truffa aziendale in cui gli aggressori violano o impersonano account email aziendali per autorizzare pagamenti fraudolenti.

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: Come blocca il phishing l'autenticazione a più fattori?

Richiede token secondari (come le chiavi hardware) che non possono essere rubati solo tramite pagine di destinazione fasulle.

Q7: Cos'è una pagina di destinazione per la raccolta di credenziali?

Un portale di accesso contraffatto progettato per catturare in tempo reale nomi utente, password e token MFA inseriti.

Q8: Cos'è il subdomain hijacking?

Un aggressore che prende il controllo di un puntatore di sottodominio DNS inutilizzato per ospitare pagine di destinazione di phishing dannose sotto un dominio principale affidabile.

Q9: Come funziona il controllo dell'allineamento DKIM?

Verifica che il dominio nell'intestazione 'From' corrisponda al dominio che ha firmato crittograficamente il messaggio nell'intestazione DKIM.

Q10: Qual è il ruolo di un gateway email?

Filtrare le email in arrivo, controllare i link, eseguire gli allegati in sandbox e convalidare la conformità a SPF/DKIM/DMARC.

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

Phishing e spoofing sono stati il tipo di reato più segnalato all'IC3 dell'FBI nel 2025, con 191.561 denunce. [4]

2. APPROFONDIMENTO SULLA SICUREZZA

La business email compromise (BEC) ha causato nel 2025 oltre 3 miliardi di dollari di perdite segnalate all'IC3 dell'FBI. [4]

3. APPROFONDIMENTO SULLA SICUREZZA

Gli attacchi omografici usano lettere cirilliche simili per duplicare visivamente nei browser i domini di marchio a corrispondenza esatta.

4. APPROFONDIMENTO SULLA SICUREZZA

Con «p=reject», un dominio chiede ai destinatari di rifiutare le email che non superano i controlli durante la consegna, anziché archiviarle come spam. [2]

5. APPROFONDIMENTO SULLA SICUREZZA

Gli attacchi di whaling rivolti ai CEO richiedono comunemente pagamenti urgenti per fusioni riservate o acquisti di domini.

6. APPROFONDIMENTO SULLA SICUREZZA

I portali di credential harvesting copiano le vere pagine di accesso, così le vittime digitano le password direttamente nel modulo dell'attaccante.

7. APPROFONDIMENTO SULLA SICUREZZA

Le linee guida congiunte della CISA sul phishing raccomandano la formazione degli utenti insieme a DMARC, SPF, DKIM e MFA resistente al phishing. [3]

8. APPROFONDIMENTO SULLA SICUREZZA

La valutazione SPF è limitata a 10 termini che richiedono query DNS; superare il limite restituisce un risultato 'permerror'. [1]

9. APPROFONDIMENTO SULLA SICUREZZA

Le chiavi di sicurezza hardware FIDO2 offrono una protezione supportata dalla crittografia contro la raccolta remota delle credenziali.

10. APPROFONDIMENTO SULLA SICUREZZA

Il phishing è uno dei modi più comuni con cui gli aggressori ottengono il primo accesso a un'organizzazione, ed è per questo che una formazione regolare di sensibilizzazione è una difesa efficace.

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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

[2] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

[3] 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

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[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 lo spear phishing? → Un'email di phishing mirata, adattata a una specifica persona o organizzazione

2 Domanda 2 — **Risposta corretta: A**

NOTA DIDATTICA

SPF pubblica nel DNS gli host di invio autorizzati di un dominio, così i destinatari possono controllare il mittente della busta.

3 Domanda 3 — **Risposta corretta: A**

NOTA DIDATTICA

Che cos'è un attacco di whaling? → Una campagna di phishing rivolta specificamente a dirigenti aziendali di alto profilo

4 Domanda 4 — **Risposta corretta: A**

NOTA DIDATTICA

Che cosa fa DKIM? → Aggiunge una firma crittografica alle email per verificare l'autenticità del mittente

5 Domanda 5 — **Risposta corretta: A**

NOTA DIDATTICA

Qual è il ruolo di DMARC? → Indicare ai server di posta riceventi come gestire i controlli SPF/DKIM falliti

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Domanda 6** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: lo spear phishing è mirato a persone specifiche, a differenza del phishing generico di massa.

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

NOTA DIDATTICA

Le policy DMARC possono istruire i server di posta a rifiutare i messaggi falsificati non autorizzati.

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

NOTA DIDATTICA

Falso: SPF controlla l'IP di invio rispetto al DNS; è DKIM a verificare una firma crittografica.

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

NOTA DIDATTICA

Falso: il whaling prende di mira i dirigenti di alto livello, che possono approvare pagamenti e accedere a dati sensibili.

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

NOTA DIDATTICA

Vero: confermare le richieste di pagamento tramite un canale separato e noto aiuta a fermare le frodi con bonifici.

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

F 1. SPEAR	G 2. SPOOFING	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING	E 7. PHISHING	A 8. VISHING

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 SPEAR	2 SPOOFING	3 RECORD SPF	4 DKIM
5 DMARC	6 WHALING		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 B – SPOOFING	2 A – SPEAR	3 H – VISHING	4 C – RECORDSPF
5 G – PHISHING	6 E – DMARC	7 D – DKIM	8 F – WHALING

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare SPEAR, SPOOFING e SPF 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.

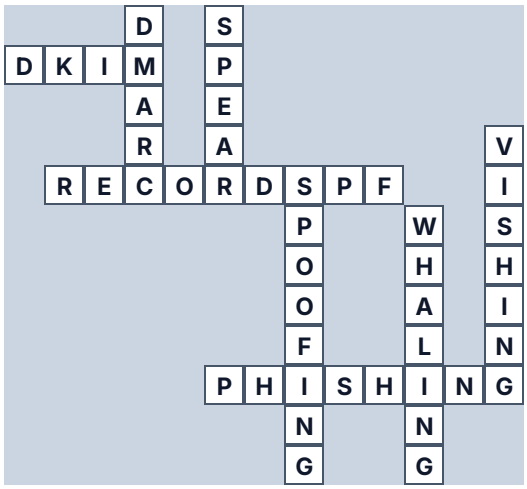
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

3 orizzontale: DKIM Firma crittografica nelle email. (4 lettere)

5 orizzontale: RECORDSPF IP dei mittenti autorizzati nel DNS. (9 lettere)

8 orizzontale: PHISHING Email di ingegneria sociale. (8 lettere)

VERTICALI

1 verticale: DMARC Istruzioni di policy per il rifiuto. (5 lettere)

2 verticale: SPEAR Email mirata e personalizzata. (5 lettere)

4 verticale: VISHING Chiamate truffa vocali. (7 lettere)

6 verticale: SPOOFING Falsificazione dell'indirizzo email del mittente. (8 lettere)

7 verticale: WHALING Bersaglio: dirigenti di alto livello. (7 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. AESRP — SPEAR
2. FRPOEDSRC — RECORDSPF
3. ADCRM — DMARC
4. SNGIHPHI — PHISHING
5. FIPGOSNO — SPOOFING
6. IMDK — DKIM
7. WNIGHLA — WHALING
8. IHGVNIS — VISHING

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"SCOPRI INGEGNERIA SOCIALE CON AUDIT DELLE EMAIL"

Soluzioni dei casi di studio

A Caso di studio 1: risoluzione di un attacco di whaling ai vertici aziendali

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un Chief Financial Officer riceve un'email molto personalizzata che sostiene di provenire dal CEO e chiede un bonifico rapido di 50.000 $ per concludere l'acquisto riservato di un dominio.
- Strategia e soluzione consigliate: configurare DMARC con una policy 'p=reject' per bloccare i domini mittente falsificati. Aggiungere banner di avviso per i mittenti esterni sul gateway e richiedere una conferma verbale, out-of-band, per tutte le transazioni finanziarie.

B Caso di studio 2: Implementare le policy di gateway SPF/DKIM/DMARC

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: Un'azienda non supera gli audit di sicurezza perché le sue email di marketing in uscita vengono spesso segnalate come spam e gli hacker falsificano attivamente il dominio del suo marchio.
- Strategia e soluzione consigliate: Pubblica un record TXT per SPF che indichi gli IP dei mittenti autorizzati. Configura le chiavi di firma DKIM sui server di posta in uscita e analizza i report di feedback DMARC in formato XML in arrivo per individuare gli abusi.