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

Truffe online e ingegneria sociale Guida alla protezione

Phishing via email, domini falsificati, vishing, truffe di supporto, verifica fuori banda, BEC

PANORAMICA DI APPRENDIMENTO SULLE TRUFFE ONLINE

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 difesa dalle truffe online. Esplorerai i siti web di phishing falsi, le tattiche di ingegneria sociale, le truffe di assistenza, i vettori di frode tramite bonifico e i metodi di verifica dei pagamenti.

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/truffe-online/

Il tuo percorso di apprendimento sulla protezione dalle truffe online

- Individua gli indicatori comuni delle truffe di assistenza e dei domini di typosquatting.
- Implementa protocolli di verifica delle email (SPF, DKIM, DMARC) contro lo spoofing.
- Stabilisci la verifica delle transazioni fuori banda per prevenire le frodi con bonifici aziendali.

ISTRUZIONI DELLA GUIDA SULLE TRUFFE ONLINE

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 protezione dalle truffe online. Concludi con l'attività bonus Pensa veloce.

TRUFFE ONLINE E PROTEZIONE DALL'INGEGNERIA SOCIALE (INTRODUZIONE)

Le truffe online sfruttano il comportamento umano tramite phishing, pop-up di assistenza, vishing e frodi tramite bonifico. Imporre la verifica delle transazioni fuori banda e le regole di dominio SPF/DKIM/DMARC aiuta a bloccare i vettori di ingegneria sociale al gateway.

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

Punto di controllo 1: Sfida a scelta multipla

1. Qual è il principale indicatore di una truffa del falso supporto tecnico?

- A. Un pop-up che afferma che il tuo sistema è infetto e ti chiede di chiamare un numero di telefono
- B. Un aggiornamento di sicurezza automatico scaricato da un registro ufficiale
- C. Un gestore di password che si rifiuta di compilare le credenziali su un dominio aziendale
- D. Un backup di file in background eseguito su una configurazione con unità esterna

2. Quale tecnica usa domini mittente falsificati per rubare i dati bancari?

- A. Phishing via email
- B. Scansione delle porte
- C. Iniezione in memoria
- D. Distruzione crittografica

3. Che cosa rappresenta la frode del bonifico bancario?

- A. Indurre le vittime con l'ingegneria sociale a inviare denaro a falsi conti aziendali
- B. Crittografare i database di sistema usando payload ransomware
- C. Interrogare i database tramite comandi di SQL injection
- D. Eseguire il backup dei file di sistema su dischi di archiviazione offline

4. Perché i truffatori creano falsi siti di shopping?

- A. Rubare agli acquirenti i dati delle carte di credito e le credenziali di pagamento
- B. Ospitare tabelle di database per l'analisi del malware in sandbox
- C. Per velocizzare la consegna degli ordini online
- D. Per testare gratuitamente nuovi design di siti web

5. Che cosa significa vishing?

- A. Truffe di phishing vocale tramite reti telefoniche per rubare credenziali
- B. Scansionare le reti locali alla ricerca di dispositivi di sistema non protetti
- C. Ripristinare i database di sistema dopo una violazione non autorizzata
- D. Eseguire codice non attendibile all'interno di container virtuali sicuri

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Le truffe di phishing prendono di mira solo gli utenti finali, mai i dirigenti bersaglio del whaling.

- ◯ Vero
- ◯ Falso

7 Domanda 7

7. I domini falsificati usano spesso piccoli errori di battitura (come amaz0n.com) per imitare marchi affidabili.

- ◯ Vero
- ◯ Falso

8 Domanda 8

8. Le truffe di assistenza tecnica si risolvono concedendo a chi chiama l'accesso remoto.

- ◯ Vero
- ◯ Falso

9 Domanda 9

9. L'ingegneria sociale sfrutta la psicologia umana, come la paura e l'urgenza, per aggirare le regole di sicurezza.

- ◯ Vero
- ◯ Falso

10 Domanda 10

10. Le richieste di bonifico dovrebbero sempre essere verificate tramite canali di comunicazione fuori banda.

- ◯ 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. Le email fraudolente che ingannano gli utenti si chiamano _____ .
2. Gli indirizzi web che imitano marchi affidabili sono indirizzi _____ .
3. Le truffe vocali che prendono di mira i dati bancari si chiamano _____ .
4. Un pop-up che chiede denaro per rimuovere un virus è una _____ di assistenza tecnica.
5. Confermare una richiesta di pagamento richiede una _____ fuori banda.
6. Reindirizzare le transazioni aziendali verso i conti dei ladri è la cosiddetta _____ .

BANCA DELLE PAROLE DEL VOCABOLARIO

CONTRAFFATTI FRODE BONIFICO PHISHING SMISHING TRUFFA VERIFICA VISHING WHALING

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

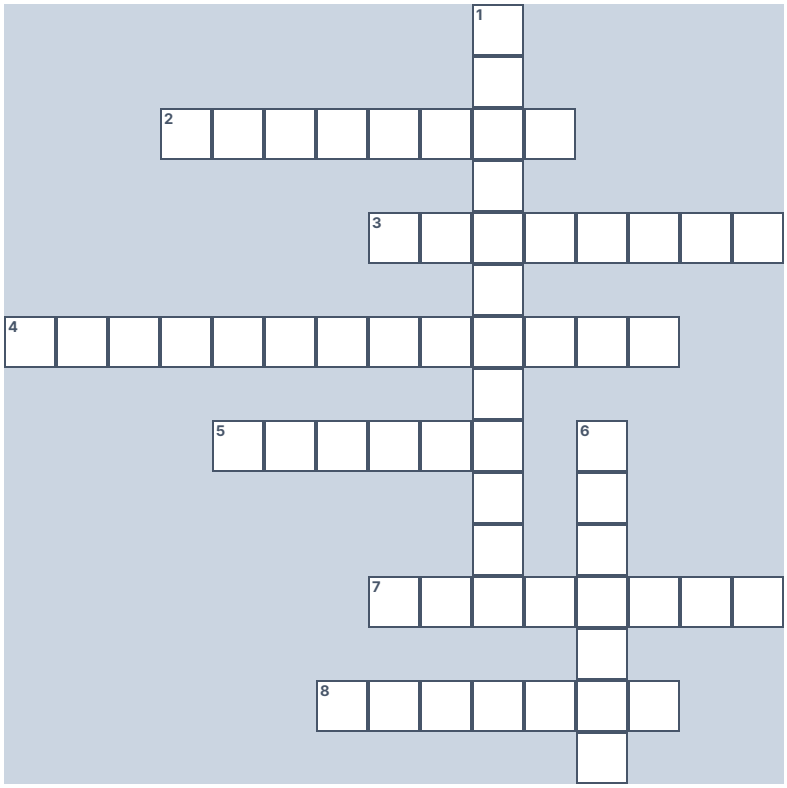
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. PHISHING	A	Reindirizzamento fraudolento di transazioni bancarie verso conti criminali.
☐	2. FALSIFICATO	B	Schema fraudolento progettato per rubare denaro o credenziali di accesso alle vittime.
☐	3. VISHING	C	Invio di SMS truffa per rubare le credenziali degli account mobili.
☐	4. TRUFFA	D	Chiamate vocali fraudolente progettate per rubare credenziali e dati degli account.
☐	5. VERIFICA	E	Attacchi di phishing mirato volti a rubare le credenziali ai dirigenti di livello C.
☐	6. WIRE	F	Mittente di email o indirizzo di sito web imitato, progettato per sembrare legittimo.
☐	7. WHALING	G	Campagne email fraudolente progettate per rubare credenziali di accesso e password.
☐	8. SMISHING	H	Confermare i dettagli di pagamento usando un metodo di contatto secondario affidabile.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

2. Invio di SMS truffa per rubare le credenziali degli account mobili. (8)

3. Conferma dei dati di pagamento tramite un metodo di contatto secondario affidabile. (8)

4. Reindirizzamento fraudolento di transazioni bancarie verso conti di criminali. (13)

5. Schema fraudolento progettato per sottrarre denaro o credenziali di accesso alle vittime. (6)

7. Campagne email fraudolente progettate per rubare credenziali di accesso e password. (8)

8. Attacchi di phishing mirati che puntano a rubare le credenziali ai dirigenti di alto livello. (7)

VERTICALI

1. Indirizzi email di mittenti o siti web imitati, progettati per sembrare legittimi. (12)

6. Chiamate vocali fraudolente progettate per rubare credenziali e dati degli account. (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

2 orizzontale: Invio di SMS truffa per rubare le credenziali degli account mobili. (8 lettere):

3 orizzontale: Conferma dei dati di pagamento tramite un metodo di contatto secondario affidabile. (8 lettere):

4 orizzontale: Reindirizzamento fraudolento di transazioni bancarie verso conti di criminali. (13 lettere):

5 orizzontale: Schema fraudolento progettato per sottrarre denaro o credenziali di accesso alle vittime. (6 lettere):

7 orizzontale: Campagne email fraudolente progettate per rubare credenziali di accesso e password. (8 lettere):

8 orizzontale: Attacchi di phishing mirati che puntano a rubare le credenziali ai dirigenti di alto livello. (7 lettere):

VERTICALI

1 verticale: Indirizzi email di mittenti o siti web imitati, progettati per sembrare legittimi. (12 lettere):

6 verticale: Chiamate vocali fraudolente progettate per rubare credenziali e dati degli account. (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.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

PHISHING CONTRAFFATTI VISHING TRUFFA VERIFICA FRODEBONIFICO WHALING SMISHING

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. PHISHING
B. CONTRAFFATTI
C. VISHING
D. TRUFFA
E. VERIFICA
F. FRODEBONIFICO
G. WHALING
H. SMISHING

	DEFINIZIONI E CAMPI DI ABBINAMENTO
	1. Indirizzi email di mittenti o siti web imitati, progettati per sembrare legittimi.
	2. Conferma dei dati di pagamento tramite un metodo di contatto secondario affidabile.
	3. Reindirizzamento fraudolento di transazioni bancarie verso conti di criminali.
	4. Invio di SMS truffa per rubare le credenziali degli account mobili.
	5. Attacchi di phishing mirati che puntano a rubare le credenziali ai dirigenti di alto livello.
	6. Chiamate vocali fraudolente progettate per rubare credenziali e dati degli account.
	7. Campagne email fraudolente progettate per rubare credenziali di accesso e password.
	8. Schema fraudolento progettato per sottrarre denaro o credenziali di accesso alle vittime.

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. NSHPIHGI
2. VSGNIHI
3. IEVFIACR
4. GHILNWA
5. OTFFINRAACTT
6. FFTUAR
7. FINBFRIEOCOOD
8. SMHGSNII

Attività bonus: Pensa veloce

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

1	Dispositivi che possono essere hackerati			
2	Frasi che i truffatori usano spesso			
3	Metodi di pagamento che chiedono i truffatori			
4	Tipi di truffe online			
5	Offerte troppo belle per essere vere			
6	Luoghi in cui segnalare una truffa			
7	Parole legate alla sicurezza informatica			
8	Persone che puoi mettere in guardia sulle truffe			
9	Cose di cui fai il backup			
10	Segnali di allarme in un'email			
11	Segnali che indicano che un computer è infetto			
12	Modi per verificare un negozio online			
13	Modi per proteggere i tuoi account			
14	Cose da fare se vieni truffato			
15	Cose da fare dopo una fuga di dati			

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: PREVENZIONE DI TRUFFE CON BONIFICI AZIENDALI

👷

Scenario: Il reparto finanziario riceve un'email urgente da un indirizzo di fornitore falsificato, che chiede di indirizzare i futuri bonifici delle fatture verso un nuovo codice di instradamento.

Domanda di discussione: Descrivi la politica di verifica contro le frodi con bonifici e indica i controlli di autenticazione delle email.

CASO DI STUDIO 2: INCIDENTE DI PHISHING DI TIPO WHALING AI DANNI DI UN DIRIGENTE

👷

Scenario: Un dirigente ha cliccato su un link di phishing che affermava di contenere un documento sicuro per una riunione del consiglio di amministrazione, inserendo le proprie credenziali aziendali principali su un portale falsificato.

Domanda di discussione: Descrivi nel dettaglio i passaggi di risposta all'incidente e spiega come verificare gli accessi del dirigente.

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

18	9	12	5	22	1		9	12		16	8	9	19	8	9	14	7		
3	15	14		22	5	18	9	6	9	3	1		19	3	1	14	14	5	18

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 una truffa online?

Uno schema fraudolento che usa i canali digitali per indurre le vittime a inviare denaro o a cedere credenziali personali.

Q2: Qual è il principale indicatore del phishing via email?

Un messaggio che dichiara un'urgenza (come la sospensione dell'account) e ti indirizza a un link che non corrisponde al dominio ufficiale.

Q3: Cos'è il typosquatting?

Registrare domini con errori di battitura comuni di marchi popolari (come amaz0n.com) per ospitare falsi siti di phishing.

Q4: Cos'è una truffa del supporto tecnico?

Un pop-up che afferma che il tuo PC è infetto e ti induce a chiamare un numero e a pagare per un falso software di pulizia o per servizi di accesso remoto. [1]

Q5: Cos'è il vishing?

Attacchi di phishing che usano telefonate vocali per indurre le vittime a fornire i dati del conto bancario o di accesso.

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

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q6: Cosa significa frode telematica (wire fraud)?

Reindirizzamento delle transazioni di pagamento verso conti truffaldini fingendosi fornitori o dirigenti.

Q7: Cos'è il whaling?

Una forma di spear phishing altamente mirata, rivolta direttamente a obiettivi di alto valore come i dirigenti aziendali di livello C.

Q8: Cos'è lo smishing?

Messaggi di testo truffaldini inviati a dispositivi mobili, contenenti link che portano a portali falsi o ad aggiornamenti di tracciamento.

Q9: Perché la verifica out-of-band è fondamentale?

Conferma i dettagli della transazione tramite un canale di comunicazione separato (come una telefonata), evitando le conversazioni email compromesse.

Q10: Come funziona una falsa truffa di deposito a garanzia (escrow)?

I truffatori creano un sito di deposito a garanzia (escrow) falso, sostenendo che i fondi siano custoditi in modo sicuro, poi rubano il bonifico dell'acquirente.

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 usano i truffatori la BEC (Business Email Compromise) per eseguire frodi tramite bonifico?

Dirottano l'account email di un dipendente legittimo, monitorano le conversazioni sulle fatture e inviano dati di fatturazione aggiornati con conti bancari fraudolenti.

Q2: Qual è il rischio degli attacchi omografici IDN nelle truffe online?

Usare caratteri non ASCII che sembrano identici alle lettere normali (ad es. la 'a' cirillica) per registrare domini contraffatti che imitano marchi reali.

Q3: Perché l'ispezione delle intestazioni delle email è importante per individuare le truffe?

Rivela l'IP effettivo del server di origine e lo stato di validazione SPF/DKIM, mostrando se il dominio del mittente è falsificato.

Q4: Come sfruttano i truffatori del supporto tecnico i software di desktop remoto?

Usano utilità come AnyDesk o TeamViewer per connettersi al dispositivo della vittima, installare malware e rubare le password salvate.

Q5: Qual è l'obiettivo delle truffe con anticipo di denaro (advance-fee)?

Indurre le vittime a pagare in anticipo commissioni di elaborazione in cambio di un'enorme ricompensa finanziaria che non esiste.

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 usano i truffatori la profilazione sui social media per il phishing mirato?

Compilano le strutture organizzative aziendali e i nomi dei dipendenti per redigere email di spear phishing convincenti.

Q7: Perché i negozi online falsi offrono sconti molto alti?

Per indurre gli acquirenti a inserire i dati della propria carta di credito, catturando le credenziali per riutilizzarle o rivenderle sui forum di carding.

Q8: Come bloccano le truffe di phishing i record DMARC?

DMARC permette ai proprietari di domini di chiedere ai destinatari di mettere in quarantena o rifiutare la posta che non supera i controlli SPF e DKIM allineati, bloccando lo spoofing diretto. [5]

Q9: Qual è la minaccia dei portali di raccolta delle credenziali?

Pagine di destinazione falsificate progettate per sembrare identiche a Microsoft 365 o agli spazi di lavoro Google, che rubano le credenziali di accesso man mano che vengono inserite.

Q10: Come segnalano e disattivano i domini truffa i team di sicurezza?

Inviando le prove della frode all'email per gli abusi del registrar, al fornitore di hosting e al registro Google Safe Browsing.

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. [2]

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. [2]

3. APPROFONDIMENTO SULLA SICUREZZA

I domini typosquatting differiscono dai veri nomi di marca per uno o due caratteri, quindi un'occhiata veloce può non notarli.

4. APPROFONDIMENTO SULLA SICUREZZA

Le truffe di assistenza tecnica hanno causato oltre $2.1 miliardi di perdite segnalate all'IC3 dell'FBI nel 2025. [2]

5. APPROFONDIMENTO SULLA SICUREZZA

Gli attacchi omografici appaiono identici nella barra degli indirizzi del browser, a meno che il browser non mostri le configurazioni punycode.

6. APPROFONDIMENTO SULLA SICUREZZA

Le truffe tramite SMS (smishing) usano messaggi brevi e urgenti con link, lasciando alle vittime poco contesto per riconoscere la frode.

7. APPROFONDIMENTO SULLA SICUREZZA

Gli attacchi di whaling prendono di mira le email dei dirigenti perché controllano l'accesso a bonifici di pagamento di importo elevato.

8. APPROFONDIMENTO SULLA SICUREZZA

Verificare le modifiche di pagamento chiamando un numero di telefono noto e salvato è una difesa fondamentale contro le frodi BEC con bonifico.

9. APPROFONDIMENTO SULLA SICUREZZA

I siti web di deposito a garanzia (escrow) falsi sono una truffa comune nei marketplace online: sembrano un servizio di pagamento sicuro, ma rubano il bonifico dell'acquirente.

10. APPROFONDIMENTO SULLA SICUREZZA

Google Safe Browsing avvisa gli utenti prima che aprano siti che ha segnalato per phishing o malware.

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] Federal Trade Commission. (n.d.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

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

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

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

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

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

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

Soluzioni: Punto di controllo 1 – Scelta multipla

1 Domanda 1

Risposta corretta: A

NOTA DIDATTICA

Qual è il principale indicatore di una truffa del falso supporto tecnico? → Un pop-up che afferma che il tuo sistema è infetto e ti chiede di chiamare un numero di telefono

2 Domanda 2

Risposta corretta: A

NOTA DIDATTICA

Quale tecnica usa domini mittente falsificati per rubare i dati bancari? → Phishing via email

3 Domanda 3

Risposta corretta: A

NOTA DIDATTICA

Che cosa rappresenta la frode del bonifico bancario? → Indurre le vittime con l'ingegneria sociale a inviare denaro a falsi conti aziendali

4 Domanda 4

Risposta corretta: A

NOTA DIDATTICA

Perché i truffatori creano falsi siti di shopping? → Rubare agli acquirenti i dati delle carte di credito e le credenziali di pagamento

5 Domanda 5

Risposta corretta: A

NOTA DIDATTICA

Che cosa significa vishing? → Truffe di phishing vocale tramite reti telefoniche per rubare credenziali

Soluzioni: Punto di controllo 2 – Vero o falso

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

NOTA DIDATTICA

Falso: il phishing prende di mira anche i dirigenti; il whaling è phishing diretto ai vertici aziendali.

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

NOTA DIDATTICA

I domini falsificati usano spesso piccoli errori di battitura (come amaz0n.com) per imitare marchi affidabili.

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

NOTA DIDATTICA

Falso: dare a un truffatore del finto supporto l'accesso remoto gli permette di installare malware e rubare dati.

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

NOTA DIDATTICA

L'ingegneria sociale sfrutta la psicologia umana, come la paura e l'urgenza, per aggirare le regole di sicurezza.

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

NOTA DIDATTICA

Le richieste di bonifico dovrebbero sempre essere verificate tramite canali di comunicazione fuori banda.

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

G 1. PHISHING	F 2. FALSIFICATO	D 3. VISHING	B 4. TRUFFA
H 5. VERIFICA	A 6. WIRE	E 7. WHALING	C 8. SMISHING

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 PHISHING	2 CONTRAFFATTI	3 VISHING	4 TRUFFA
5 VERIFICA	6 FRODE BONIFICO		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 B – CONTRAFFATTI	2 E – VERIFICA	3 F – FRODEBONIFICO	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – TRUFFA

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare PHISHING, FALSIFICATO e VISHING 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.

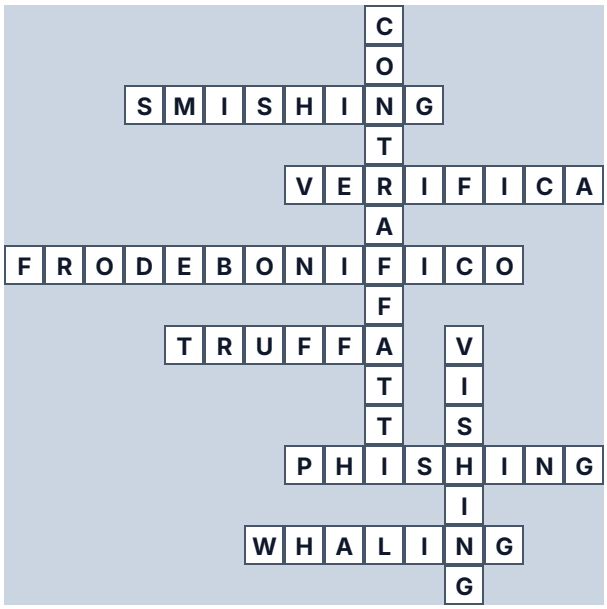
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

2 orizzontale: SMISHING Invio di SMS truffa per rubare le credenziali degli account mobili. (8 lettere)

3 orizzontale: VERIFICA Conferma dei dati di pagamento tramite un metodo di contatto secondario affidabile. (8 lettere)

4 orizzontale: FRODEBONIFICO Reindirizzamento fraudolento di transazioni bancarie verso conti di criminali. (13 lettere)

5 orizzontale: TRUFFA Schema fraudolento progettato per sottrarre denaro o credenziali di accesso alle vittime. (6 lettere)

7 orizzontale: PHISHING Campagne email fraudolente progettate per rubare credenziali di accesso e password. (8 lettere)

8 orizzontale: WHALING Attacchi di phishing mirati che puntano a rubare le credenziali ai dirigenti di alto livello. (7 lettere)

VERTICALI

1 verticale: CONTRAFFATTI Indirizzi email di mittenti o siti web imitati, progettati per sembrare legittimi. (12 lettere)

6 verticale: VISHING Chiamate vocali fraudolente progettate per rubare credenziali e dati degli account. (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. NSHPIHGI — **PHISHING**
2. VSGNIHI — **VISHING**
3. IEVFIACR — **VERIFICA**
4. GHILNWA — **WHALING**
5. OTFFINRAACTT — **CONTRAFFATTI**
6. FFTUAR — **TRUFFA**
7. FINBFRIEOCOOD — **FRODEBONIFICO**
8. SMHGSNII — **SMISHING**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"RILEVA IL PHISHING CON VERIFICA SCANNER"

Soluzioni dei casi di studio

A Caso di studio 1: prevenzione di truffe con bonifici aziendali

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un reparto finanziario riceve un'email urgente da un indirizzo di fornitore falsificato, che chiede di indirizzare i futuri bonifici delle fatture verso un nuovo codice di instradamento.
- Strategia e soluzione consigliate: Applica una politica di doppia autorizzazione per tutti i pagamenti. Implementa una verifica fuori banda tramite un numero di telefono salvato in precedenza e blocca sul gateway le email provenienti da domini falsificati.

B Caso di studio 2: Incidente di phishing di tipo whaling ai danni di un dirigente

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: Un dirigente ha cliccato su un link di phishing che affermava di contenere un documento riservato per una riunione del consiglio di amministrazione e ha inserito le proprie credenziali aziendali principali su un portale falsificato.
- Strategia e soluzione consigliate: Isola il dispositivo del dirigente. Reimposta tutti i token di sessione e le credenziali aziendali. Esamina i log di accesso per verificare l'esfiltrazione di dati e implementa l'MFA hardware su tutti gli accessi.