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

Prevenzione del furto di identità e dei beni
Guida alla sicurezza

Fughe di credenziali, MFA, monitoraggio del dark web, avvisi di blocco del credito, ingegneria sociale

PANORAMICA DI APPRENDIMENTO SULLA PREVENZIONE DEL FURTO DI IDENTITÀ

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 prevenzione e la mitigazione del furto d'identità. Esplorerai le fughe di credenziali, l'autenticazione a più fattori, il monitoraggio del dark web, gli avvisi di blocco del credito e la difesa dall'ingegneria sociale.

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/furto-identita/

Il tuo percorso di apprendimento sulla protezione dell'identità

- Comprendi i rischi di esposizione delle credenziali sui forum del dark web.
- Implementa l'autenticazione a più fattori (MFA) e gli avvisi di blocco del credito.
- Progetta difese di sicurezza aziendali contro le truffe mirate di ingegneria sociale.

ISTRUZIONI DELLA GUIDA SUL FURTO DI IDENTITÀ

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 dell'identità. Concludi con l'attività bonus Pensa veloce.

PREVENZIONE DEL FURTO DI IDENTITÀ E SICUREZZA DEI BENI (INTRODUZIONE)

Il furto di identità sfrutta credenziali trapelate e accessi deboli per prendere il controllo di account personali e aziendali. Adottare MFA, blocchi del credito, scanner del dark web e framework SPF/DKIM/DMARC costituisce una difesa fondamentale contro la sostituzione di persona digitale.

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 metodo principale usato dai ladri di identità per rubare le credenziali di accesso?

- A. Inviare falsi avvisi via email per indurre gli utenti a inserire le password su portali contraffatti
- B. Ascoltare trasmissioni radio vicino all'ufficio aziendale di un utente
- C. Deframmentare l'unità di archiviazione del server locale di un utente
- D. Scollegare le configurazioni di backup di rete esterne

2. Quale controllo di sicurezza offre la difesa più forte contro le fughe di credenziali?

- A. Autenticazione multifattore con chiavi hardware
- B. Creare password lunghe usando i formati predefiniti del browser
- C. Cambiare i nomi utente delle email ogni sei mesi
- D. Eliminare le cronologie del browser con i cookie di tracciamento memorizzati

3. Che cosa rappresenta il blocco del credito (credit freeze)?

- A. Bloccare i rapporti di credito per impedire ai truffatori di aprire prestiti non autorizzati
- B. Eliminare dai database la cronologia delle transazioni dei conti bancari
- C. Disattivare i lettori a banda magnetica delle carte di credito sugli scanner
- D. Cifrare a riposo i dischi rigidi dei database locali

4. Perché il monitoraggio del dark web è utile?

- A. Avvisa gli utenti se le loro credenziali trapelate compaiono in database illeciti
- B. Impedisce l'esecuzione del malware attivo nelle sandbox virtuali
- C. Accelera la velocità di instradamento del browser sulle reti virtuali
- D. Blocca i tentativi di accesso tramite SQL injection al database di back-end

5. Che cosa significa ingegneria sociale?

- A. Manipolare le persone affinché rivelino volontariamente credenziali riservate
- B. Scansionare le porte dei server aziendali alla ricerca di exploit di sicurezza attivi
- C. Eseguire il backup dei file del database di sistema su dischi rigidi offline
- D. Instradare i pacchetti di rete attraverso tre nodi onion cifrati

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Il furto di identità riguarda solo gli account digitali online, non la posta cartacea.

- ○ Vero
- ○ Falso

7 Domanda 7

7. Imporre l'MFA su tutti gli account personali blocca la maggior parte degli attacchi bot di credential stuffing.

- ○ Vero
- ○ Falso

8 Domanda 8

8. Un blocco del credito impedisce i controlli del credito ma ti impedisce di accedere al tuo conto bancario.

- ○ Vero
- ○ Falso

9 Domanda 9

9. I gestori di password proteggono gli utenti dal phishing rifiutandosi di compilare automaticamente le password su domini falsificati.

- ○ Vero
- ○ Falso

10 Domanda 10

10. Le email di phishing usano spesso un linguaggio urgente per provocare risposte emotive e rapide.

- ○ 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. I ladri di identità prendono di mira le password personali e le _____ degli utenti.

2. Gli avvisi agli utenti sulle violazioni dei database individuano le _____ degli account privati.

3. Richiedere un codice temporaneo per accedere si chiama autenticazione _____ (MFA).

4. Cercare dati rubati nei forum degli hacker è il _____ del dark web.

5. Bloccare le verifiche di credito non autorizzate richiede un _____ del credito.

6. Formare i dipendenti sulla consapevolezza del phishing costruisce una _____ attiva della sicurezza.

BANCA DELLE PAROLE DEL VOCABOLARIO

BLOCCO CREDENZIALI DIFESA FUGHE DI DATI MONITORAGGIO MULTIFATTORE PHISHING SPOOFING

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

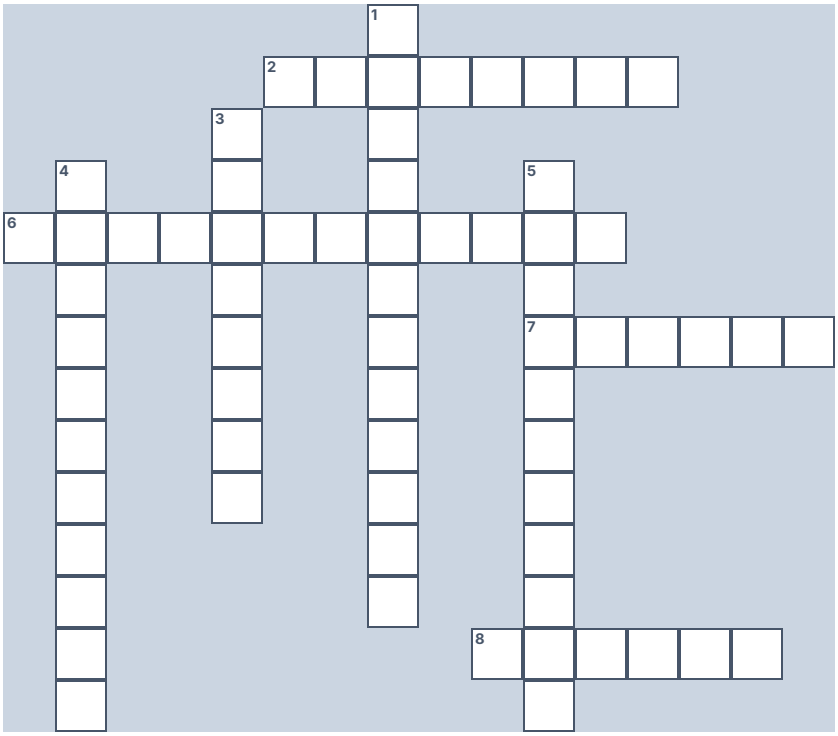
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. CREDENZIALI	A	Passaggio di verifica aggiuntivo (come le chiavi hardware) che protegge gli accessi agli account.
☐	2. PERDITE	B	Creare un sito web o un'email falsi per imitare un'organizzazione legittima.
☐	3. MFA	C	Limitazione dell'accesso ai fascicoli di credito per prevenire richieste di prestito fraudolente.
☐	4. MONITORAGGIO	D	Esposizione non autorizzata di database privati contenenti record personali degli utenti.
☐	5. BLOCCO	E	Formazione e controlli tecnici usati per proteggersi dal furto di identità.
☐	6. DIFESA	F	Invio di messaggi fraudolenti per indurre gli utenti a cedere le credenziali.
☐	7. SPOOFING	G	Scansione di forum online e canali di hacker alla ricerca di dati aziendali rubati.
☐	8. PHISHING	H	Nomi utente, password e token privati usati per autenticare le identità digitali.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

2. Creazione di un sito web o di un'email falsi per imitare un'organizzazione legittima. (8)

6. Passaggio di verifica secondario (come le chiavi hardware) che protegge gli accessi agli account. (12)

7. Formazione e controlli tecnici usati per proteggersi dal furto di identità. (6)

8. Limitazione dell'accesso ai dati di credito per impedire richieste di prestito fraudolente. (6)

VERTICALI

1. Scansione di forum online e canali di hacker alla ricerca di dati aziendali rubati. (12)

3. Invio di messaggi fraudolenti per indurre gli utenti a rivelare le credenziali. (8)

4. Esposizione non autorizzata di database privati che contengono dati personali degli utenti. (11)

5. Nomi utente, password e token privati usati per autenticare le identità digitali. (11)

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: Creazione di un sito web o di un'email falsi per imitare un'organizzazione legittima. (8 lettere):

6 orizzontale: Passaggio di verifica secondario (come le chiavi hardware) che protegge gli accessi agli account. (12 lettere):

7 orizzontale: Formazione e controlli tecnici usati per proteggersi dal furto di identità. (6 lettere):

8 orizzontale: Limitazione dell'accesso ai dati di credito per impedire richieste di prestito fraudolente. (6 lettere):

VERTICALI

1 verticale: Scansione di forum online e canali di hacker alla ricerca di dati aziendali rubati. (12 lettere):

3 verticale: Invio di messaggi fraudolenti per indurre gli utenti a rivelare le credenziali. (8 lettere):

4 verticale: Esposizione non autorizzata di database privati che contengono dati personali degli utenti. (11 lettere):

5 verticale: Nomi utente, password e token privati usati per autenticare le identità digitali. (11 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.

O R G Y B H L Z G J O P N W C

I M N Z G N I F O O P S Y G D

G Y I O W U K V P B N V T I M

G G H V D Y U K R B X Z F Y M

A R S Q X I P D A D J E Q C V

R W I W L J H T H G S B E R I

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

T A P L Q C Z M K V R U A D S

I W J M M H H N H R F K T E L

N R W H B U O C C O L B F N Y

O M U L T I F A T T O R E Z O

M Y W S H T X A P U N N Z I O

I Q F U G H E D I D A T I A T

I P V U O U U K A E P M K L A

N V G G P Q X Y J K V J Y I W

ELENCO DELLE PAROLE DEL VOCABOLARIO

CREDENZIALI FUGHEDIDATI MULTIFATTORE MONITORAGGIO BLOCCO DIFESA SPOOFING PHISHING

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. CREDENZIALI
B. FUGHEDIDATI
C. MULTIFATTORE
D. MONITORAGGIO
E. BLOCCO
F. DIFESA
G. SPOOFING
H. PHISHING

DEFINIZIONI E CAMPI DI ABBINAMENTO
_____ 1. Invio di messaggi fraudolenti per indurre gli utenti a rivelare le credenziali.
_____ 2. Nomi utente, password e token privati usati per autenticare le identità digitali.
_____ 3. Creazione di un sito web o di un'email falsi per imitare un'organizzazione legittima.
_____ 4. Formazione e controlli tecnici usati per proteggersi dal furto di identità.
_____ 5. Scansione di forum online e canali di hacker alla ricerca di dati aziendali rubati.
_____ 6. Limitazione dell'accesso ai dati di credito per impedire richieste di prestito fraudolente.
_____ 7. Esposizione non autorizzata di database privati che contengono dati personali degli utenti.
_____ 8. Passaggio di verifica secondario (come le chiavi hardware) che protegge gli accessi agli account.

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. EZLRNICAEID
2. EUIFMORLTTAT
3. BOCOCL
4. ONGIFSPO
5. AUDIGIEDFTH
6. OTGGOIAMORNI
7. SDEAFI
8. SHHGPNII

Attività bonus: Pensa veloce

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

1	Cose da fare se ti rubano l'identità			
2	Cose da non condividere sui social media			
3	Cose di cui fai il backup			
4	Tessere o documenti nel tuo portafoglio			
5	Documenti che dovresti proteggere			
6	Cose da fare dopo una fuga di dati			
7	Motivi per aggiornare il software			
8	Informazioni che vuole un ladro d'identità			
9	Dispositivi che possono essere hackerati			
10	Luoghi da cui possono trapelare i tuoi dati			
11	Buone abitudini sicure che puoi iniziare oggi			
12	Segnali che indicano che un computer è infetto			
13	Modi per dimostrare chi sei			
14	Segnali di un furto d'identità			
15	Segnali di allarme in un'email			

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: PROTEZIONE DALL'IMPERSONIFICAZIONE DELL'IDENTITÀ DEI DIRIGENTI



Scenario: Un dirigente di alto profilo del livello C-suite è stato preso di mira da nomi di dominio con errori di battitura (typosquatting) che imitano la sua email personale per truffare i clienti. Progetta un piano di protezione del marchio.

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: ESPOSIZIONE DELLE CREDENZIALI AZIENDALI NEL DARK WEB



Scenario: Un dump di un database del dark web contiene diverse centinaia di credenziali aziendali appartenenti ad amministratori di sistema di un'azienda. Progetta una strategia di mitigazione.

Domanda di discussione: Descrivi il processo di pulizia delle credenziali e pianifica l'introduzione di un gestore di password.

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

16	18	15	20	5	7	7	9		9	4	5	14	20	9	20	1

4	9	7	9	20	1	12	5		3	15	14		12	1		13	6	1

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 furto d'identità?

Un reato in cui un aggressore ruba dati personali (come password o numeri di previdenza sociale) per impersonare un'altra persona a scopo di lucro.

Q2: Qual è la causa più comune del furto d'identità?

Il phishing è uno dei principali modi in cui i criminali ottengono le password, attirando gli utenti su siti web falsi e contraffatti.

Q3: Come protegge le identità l'autenticazione a più fattori (MFA)?

L'MFA richiede una seconda prova (come una chiave hardware) per accedere, bloccando gli attaccanti anche se rubano la tua password.

Q4: Cos'è un blocco del credito (credit freeze)?

Un servizio gratuito che impedisce alle agenzie di credito di condividere il tuo fascicolo di credito, evitando che i truffatori aprano nuovi prestiti a tuo nome. [2]

Q5: Cos'è il monitoraggio del dark web?

Software che controlla i forum degli hacker per individuare email, password e record personali trapelati e ti avvisa se i tuoi dati sono esposti.

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 credential stuffing?

Bot automatizzati che provano elenchi di password trapelate su centinaia di siti web per prendere il controllo di account attivi.

Q7: Perché lo spoofing delle email è pericoloso?

Consente agli aggressori di falsificare il nome del mittente nelle email, facendo sembrare i messaggi di phishing provenienti da colleghi fidati.

Q8: Come impediscono il furto di identità i gestori di password?

Memorizzano password complesse e uniche per ogni account e rifiutano di compilare automaticamente le credenziali su domini di phishing falsi.

Q9: Cos'è lo spear phishing?

Un attacco di phishing altamente mirato, personalizzato con il nome e i dettagli della vittima per aumentare le probabilità di inganno.

Q10: In che cosa un avviso di credito differisce da un blocco?

Un avviso indica ai finanziatori di verificare la tua identità prima di aprire account, mentre un blocco impedisce del tutto l'accesso al tuo fascicolo di credito. [2]

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 porta il SIM swapping al furto d'identità?

Gli aggressori convincono il personale dell'operatore a trasferire il numero di telefono della vittima su una nuova SIM, dirottando i codici 2FA inviati via SMS.

Q2: Qual è il ruolo di DMARC nel prevenire il furto d'identità?

DMARC consente ai proprietari di domini di bloccare le email falsificate prima che raggiungano le caselle di posta, impedendo che email false imitino i domini aziendali.

Q3: Perché il furto di identità sintetica è difficile da individuare?

I truffatori combinano numeri di previdenza sociale (SSN) reali con nomi e date di nascita falsi per costruire profili di credito del tutto nuovi, aggirando gli avvisi di frode di base.

Q4: Come sfruttano le identità personali i data broker?

I data broker raccolgono registri pubblici, comportamento sul web e cronologie degli acquisti per compilare dossier di profilo, che possono essere divulgati o venduti.

Q5: Perché l'MFA basata su SMS è considerata vulnerabile?

Il traffico SMS è vulnerabile a intercettazione, phishing e exploit di SIM swapping a livello di operatore.

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: Cos'è un blocco del fascicolo di credito?

Un servizio commerciale simile a un blocco, che consente agli utenti di sbloccare o bloccare all'istante il proprio fascicolo di credito tramite un'app mobile.

Q7: Come alimentano il furto di identità le violazioni dei dati aziendali?

I database trapelati espongono milioni di credenziali in chiaro, fornendo ai ladri i dati grezzi necessari per eseguire frodi di identità mirate.

Q8: Qual è il rischio di condividere troppo sui social media?

Condividere pubblicamente i nomi degli animali domestici, i luoghi di nascita e i cognomi da nubile delle madri fornisce ai ladri le risposte alle comuni domande di recupero dell'account.

Q9: Come proteggono i profili di identità gli accessi biometrici?

La biometria lega gli accessi a tratti come le impronte digitali o il volto; se restano sul dispositivo sono difficili da rubare, ma i dati biometrici archiviati possono subire perdite.

Q10: Come contrasta il furto d'identità la Red Flags Rule?

Una normativa federale che impone alle istituzioni finanziarie di sviluppare programmi scritti per rilevare e rispondere ai segnali di allarme del furto di identità.

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

IdentityTheft.gov, gestito dalla FTC, consente alle vittime negli Stati Uniti di segnalare il furto di identità e di ottenere un piano di recupero personalizzato. [1]

2. APPROFONDIMENTO SULLA SICUREZZA

Le chiavi di sicurezza hardware sono un'autenticazione a più fattori (MFA) resistente al phishing, il tipo di MFA più forte che la CISA raccomanda. [4]

3. APPROFONDIMENTO SULLA SICUREZZA

Le password compromesse sono un punto di ingresso comune nelle violazioni dei dati e alimentano le successive frodi di identità.

4. APPROFONDIMENTO SULLA SICUREZZA

Un blocco del credito è gratuito per legge federale e impedisce ai finanziatori di consultare i fascicoli di credito finché non viene sbloccato. [2]

5. APPROFONDIMENTO SULLA SICUREZZA

DMARC permette ai proprietari di domini di indicare ai server di posta di rifiutare o mettere in quarantena le email falsificate che non superano i controlli. [7]

6. APPROFONDIMENTO SULLA SICUREZZA

Lo SIM swapping consente agli hacker di aggirare l'autenticazione a due fattori basata su SMS sui portali bancari.

7. APPROFONDIMENTO SULLA SICUREZZA

La frode di identità sintetica mescola dati reali e falsi, rendendo difficile per i finanziatori individuarla.

8. APPROFONDIMENTO SULLA SICUREZZA

Molte persone riutilizzano la stessa password su più account online, quindi una sola violazione può esporne diversi.

9. APPROFONDIMENTO SULLA SICUREZZA

I data broker compilano dossier dettagliati su un gran numero di consumatori, creando un rischio concentrato per la privacy.

10. APPROFONDIMENTO SULLA SICUREZZA

Riprendersi da un furto di identità può richiedere mesi di lavoro, ad esempio per contestare gli addebiti e correggere i rapporti di credito.

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.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[5] 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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[7] 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 metodo principale usato dai ladri di identità per rubare le credenziali di accesso? → Inviare falsi avvisi via email per indurre gli utenti a inserire le password su portali contraffatti

2 Domanda 2

Risposta corretta: A

NOTA DIDATTICA

Quale controllo di sicurezza offre la difesa più forte contro le fughe di credenziali? → Autenticazione multifattore con chiavi hardware

3 Domanda 3

Risposta corretta: A

NOTA DIDATTICA

Che cosa rappresenta il blocco del credito (credit freeze)? → Bloccare i rapporti di credito per impedire ai truffatori di aprire prestiti non autorizzati

4 Domanda 4

Risposta corretta: A

NOTA DIDATTICA

Perché il monitoraggio del dark web è utile? → Avvisa gli utenti se le loro credenziali trapelate compaiono in database illeciti

5 Domanda 5

Risposta corretta: A

NOTA DIDATTICA

Che cosa significa ingegneria sociale? → Manipolare le persone affinché rivelino volontariamente credenziali riservate

Soluzioni: Punto di controllo 2 – Vero o falso

6 Domanda 6

Risposta corretta: Falso

NOTA DIDATTICA

Il furto d'identità può iniziare anche offline, ad esempio con posta o documenti rubati.

7 Domanda 7

Risposta corretta: Vero

NOTA DIDATTICA

Imporre l'MFA su tutti gli account personali blocca la maggior parte degli attacchi bot di credential stuffing.

8 Domanda 8

Risposta corretta: Falso

NOTA DIDATTICA

Un blocco del credito impedisce nuove verifiche di credito ma non incide sui tuoi conti esistenti.

9 Domanda 9

Risposta corretta: Vero

NOTA DIDATTICA

I gestori di password proteggono gli utenti dal phishing rifiutandosi di compilare automaticamente le password su domini falsificati.

10 Domanda 10

Risposta corretta: Vero

NOTA DIDATTICA

Le email di phishing usano spesso un linguaggio urgente per provocare risposte emotive e rapide.

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

H 1. CREDENZIALI	D 2. PERDITE	A 3. MFA	G 4. MONITORAGGIO
C 5. BLOCCO	E 6. DIFESA	B 7. SPOOFING	F 8. PHISHING

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 CREDENZIALI	2 FUGHE DI DATI	3 MULTIFATTORE	4 MONITORAGGIO
5 BLOCCO	6 DIFESA		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 H – PHISHING	2 A – CREDENZIALI	3 G – SPOOFING	4 F – DIFESA
5 D – MONITORAGGIO	6 E – BLOCCO	7 B – FUGHEDIDATI	8 C – MULTIFATTORE

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare CREDENZIALI, PERDITE e MFA 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.

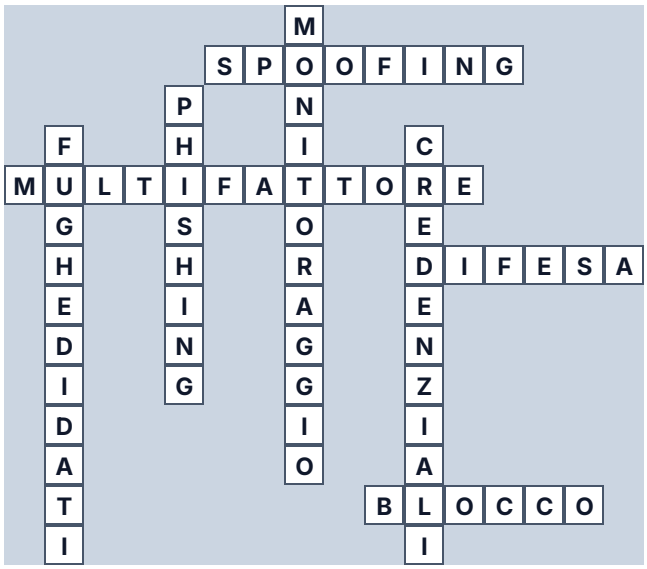
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

2 orizzontale: SPOOFING Creazione di un sito web o di un'email falsi per imitare un'organizzazione legittima. (8 lettere)

6 orizzontale: MULTIFATTORE Passaggio di verifica secondario (come le chiavi hardware) che protegge gli accessi agli account. (12 lettere)

7 orizzontale: DIFESA Formazione e controlli tecnici usati per proteggersi dal furto di identità. (6 lettere)

8 orizzontale: BLOCCO Limitazione dell'accesso ai dati di credito per impedire richieste di prestito fraudolente. (6 lettere)

VERTICALI

1 verticale: MONITORAGGIO Scansione di forum online e canali di hacker alla ricerca di dati aziendali rubati. (12 lettere)

3 verticale: PHISHING Invio di messaggi fraudolenti per indurre gli utenti a rivelare le credenziali. (8 lettere)

4 verticale: FUGHEDIDATI Esposizione non autorizzata di database privati che contengono dati personali degli utenti. (11 lettere)

5 verticale: CREDENZIALI Nomi utente, password e token privati usati per autenticare le identità digitali. (11 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. EZLRNICAEID — **CREDENZIALI**
2. EUIFMORLTTAT — **MULTIFATTORE**
3. BOCOCL — **BLOCCO**
4. ONGIFSPO — **SPOOFING**
5. AUDIGIEDFTH — **FUGHEDIDATI**
6. OTGGOIAMORNI — **MONITORAGGIO**
7. SDEAFI — **DIFESA**
8. SHHGPNII — **PHISHING**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"PROTEGGI IDENTITA DIGITALE CON LA MFA"

Soluzioni dei casi di studio

A Caso di studio 1: protezione dall'impersonificazione dell'identità dei dirigenti

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un dirigente di alto livello (C-suite) di alto profilo è stato preso di mira da nomi di dominio typosquatted che imitano la sua email personale per truffare i clienti. Progetta un piano di protezione del marchio.
- Strategia e soluzione consigliate: Registra tutte le varianti ortografiche comuni del nome del dirigente. Implementa protocolli di autenticazione email (DMARC, DKIM, SPF) per prevenire la falsificazione del dominio. Applica l'MFA hardware su tutti gli accessi aziendali dei dirigenti di alto livello (C-suite).

B Caso di studio 2: Esposizione delle credenziali aziendali nel dark web

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un dump di database del dark web contiene diverse centinaia di credenziali aziendali appartenenti ad amministratori di sistema di un'azienda. Progetta una strategia di mitigazione.
- Strategia e soluzione consigliate: eseguire un reset delle password a livello aziendale. Imporre l'uso di un gestore di password aziendale. Applicare l'MFA su tutti i portali di sistema e impostare avvisi automatici continui di monitoraggio del dark web.