Nume: _____ Data: _____ Punctaj: _____

Prevenirea furtului de identitate și securitatea activelor Ghid de securitate

Scurgeri de credențiale, MFA, monitorizare dark web, alerte de înghețat al creditului, inginerie socială

PREZENTARE GENERALĂ A ÎNVĂȚĂRII: PREVENIREA FURTULUI DE IDENTITATE

SECURIZAT
CRIPTAREA DATELOR
Standardul AES pe 256 de biți

CONFORM
STANDARDE GLOBALE
Cadrele GDPR și CCPA

ZERO-TRUST
POLITICĂ DE ACCES
Autentificare multifactor

Bun venit! Acest pachet de activități te ghidează prin prevenirea și atenuarea furtului de identitate. Vei explora scurgerile de acreditări, autentificarea multifactor, monitorizarea dark web, alertele de înghețare a creditului și apărarea împotriva ingineriei sociale.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește securitatea cibernetică și prevenirea amenințărilor.**
- [ ] **Partea 5-7: Rezolvă puzzle-uri de tip cuvinte încrucișate și căutare de cuvinte.**
- [ ] **Partea 8-9: Rezolvă studii de caz și provocarea cu codul cifrat.**
- [ ] **Partea 10: Parcurge paginile de întrebări frecvente de bază și avansate.**
- [ ] **Partea 11: Explorează 10 fapte interesante din lumea reală.**
- [ ] **Bonus: provocarea Gândește repede.**

Deschide Ghidul VPN.com de securitate cibernetică

URL: https://www.vpn.com/ro/securitate-cibernetica/furt-de-identitate/

Harta ta de învățare despre protecția identității

- Înțelege riscurile expunerii credențialelor pe forumurile din dark web.
- Implementează autentificarea multifactor (MFA) și alertele de înghețare a creditului.
- Proiectează apărări de securitate corporative împotriva escrocheriilor de inginerie socială țintite.

INSTRUCȚIUNI PENTRU GHIDUL DESPRE FURTUL DE IDENTITATE

Răspunde la întrebările cu alegere multiplă și adevărat/fals, completează propozițiile cu spații libere folosind banca de cuvinte, asociază definițiile și rezolvă cuvintele încrucișate și puzzle-ul de căutare a cuvintelor. Aplică ce ai învățat despre protecția identității. Încheie cu activitatea bonus Gândește repede.

PREVENIREA FURTULUI DE IDENTITATE ȘI SECURITATEA ACTIVELOR (INTRODUCERE)

Furtul de identitate exploatează datele de autentificare scurse și autentificările slabe pentru a prelua conturi personale și corporative. Implementarea MFA, a înghețării creditului, a scanerelor pentru dark web și a cadrelor SPF/DKIM/DMARC formează o apărare esențială împotriva uzurpării identității digitale.

CITEȘTE ATENT FIECARE PUNCT DE CONTROL ȘI ALEGE SAU SCRIE RĂSPUNSUL CORECT.

Punct de control 1: Provocare cu alegere multiplă

1. Care este metoda principală prin care hoții de identitate fură datele de conectare?

- A. Trimiterea de alerte false prin e-mail care păcălesc utilizatorii să introducă parole pe portaluri falsificate
- B. Ascultarea emisiunilor radio din apropierea biroului corporativ al unui utilizator
- C. Defragmentarea unității de stocare locale a serverului unui utilizator
- D. Deconectarea configurațiilor externe de backup al rețelei

2. Ce control de securitate oferă cea mai puternică apărare împotriva scurgerilor de credențiale?

- A. Autentificare multi-factor cu chei hardware
- B. Crearea de parole lungi folosind formatele implicite ale browserului
- C. Schimbarea numelor de utilizator de e-mail la fiecare șase luni
- D. Ștergerea istoricelor de urmărire din cookie-urile stocate în browser

3. Ce reprezintă înghețarea creditului?

- A. Blocarea rapoartelor de credit pentru a împiedica hoții să deschidă împrumuturi neautorizate
- B. Ștergerea istoricelor tranzacțiilor din conturile bancare din baze de date
- C. Dezactivarea cititoarelor magnetice de carduri de credit de pe scannere
- D. Criptarea la repaus a hard disk-urilor bazei de date locale

4. De ce este utilă monitorizarea dark web-ului?

- A. Alertează utilizatorii dacă datele lor de autentificare scurse apar în baze de date ilicite
- B. Împiedică rularea software-ului rău intenționat activ în sandbox-uri virtuale
- C. Accelerează viteza de rutare a browserului în rețelele virtuale
- D. Blochează încercările de acces SQL injection la baza de date din backend

5. Ce înseamnă inginerie socială?

- A. Manipularea oamenilor pentru a-i determina să dezvăluie de bunăvoie date confidențiale de autentificare
- B. Scanarea porturilor serverelor corporative în căutarea exploatărilor de securitate active
- C. Copierea de rezervă a fișierelor bazei de date a sistemului pe hard disk-uri offline
- D. Rutarea pachetelor de rețea prin trei noduri onion criptate

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Furtul de identitate afectează doar conturile digitale online, nu și corespondența poștală fizică.

- ○ Adevărat
- ○ Fals

7 Întrebare 7

7. Impunerea MFA pe toate conturile personale blochează majoritatea atacurilor botnet de tip credential stuffing.

- ○ Adevărat
- ○ Fals

8 Întrebare 8

8. O înghețare a creditului blochează verificările de credit, dar te împiedică să accesezi propriul cont bancar.

- ○ Adevărat
- ○ Fals

9 Întrebare 9

9. Managerii de parole îi protejează pe utilizatori de phishing prin refuzul de a completa automat parole pe domenii falsificate.

- ○ Adevărat
- ○ Fals

10 Întrebare 10

10. E-mailurile de phishing folosesc adesea un limbaj urgent pentru a declanșa reacții emoționale și rapide.

- ○ Adevărat
- ○ Fals

Punct de control 3: Inserarea termenilor-cheie

Citește fiecare propoziție de mai jos și completează spațiul liber cu termenul corect din Banca de cuvinte.

1. Hoții de identitate vizează parolele personale și alte _____ ale utilizatorilor.

2. Alertarea utilizatorilor despre breșele din bazele de date identifică _____ de conturi private.

3. Solicitarea unui cod temporar pentru autentificare se numește autentificare _____ .

4. Scanarea forumurilor hackerilor pentru date furate se numește _____ pe dark web.

5. Blocarea verificărilor de credit neautorizate necesită o _____ a creditului.

6. Instruirea angajaților privind phishing-ul construiește o _____ activă de securitate.

BANCĂ DE CUVINTE DIN VOCABULAR

APĂRARE CREDENȚIALE ÎNGHEȚARE MONITORIZARE MULTIFACTOR PHISHING SCURGERI SPOOFING

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor despre securitate

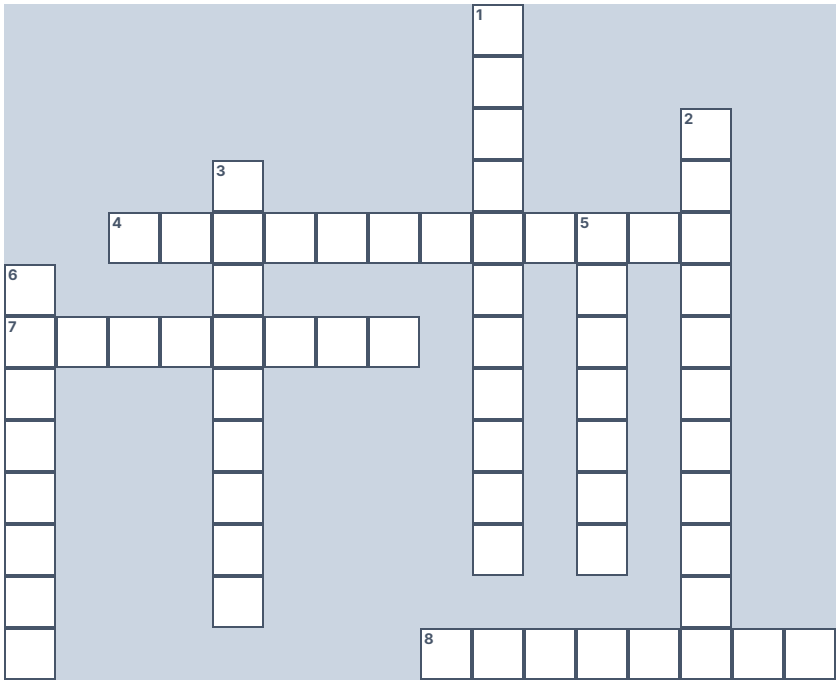
ASOCIEREA DEFINIȚIILOR

Asociază fiecare termen de vocabular din stânga cu definiția corectă din dreapta, scriind litera corespunzătoare (A-H) în câmpul de completare.

☐	1. CREDENȚIALE	A	Pas suplimentar de verificare (precum cheile hardware) care protejează autentificarea în cont.
☐	2. SCURGERI	B	Crearea unui site web sau a unui e-mail fals pentru a imita o organizație legitimă.
☐	3. MFA	C	Restricționarea accesului la dosarele de credit pentru a preveni cererile frauduloase de împrumut.
☐	4. MONITORIZARE	D	Expunerea neautorizată a unor baze de date private care conțin înregistrări personale ale utilizatorilor.
☐	5. ÎNGHEȚARE	E	Instruire și controale tehnice folosite pentru a proteja împotriva furtului de identitate.
☐	6. APĂRARE	F	Trimiterea de mesaje frauduloase pentru a păcăli utilizatorii să-și dezvăluie datele de autentificare.
☐	7. FALSIFICARE (SPOOFING)	G	Scanarea forumurilor online și a canalelor hackerilor în căutarea datelor corporative furate.
☐	8. PHISHING	H	Nume de utilizator, parole și token-uri private folosite pentru a autentifica identități digitale.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

4. Scanarea forumurilor online și a canalelor hackerilor pentru date corporative furate. (12)

7. Trimiterea de mesaje frauduloase pentru a păcăli utilizatorii să renunțe la credențiale. (8)

8. Expunerea neautorizată a bazelor de date private care conțin înregistrări personale ale utilizatorilor. (8)

VERTICAL

1. Pas secundar de verificare (precum cheile hardware) care protejează autentificările în conturi. (11)

2. Nume de utilizator, parole și token-uri private folosite pentru autentificarea identităților digitale. (11)

3. Restricționarea accesului la dosarele de credit pentru a preveni cererile frauduloase de împrumut. (9)

5. Instruire și controale tehnice folosite pentru a proteja împotriva furtului de identitate. (7)

6. Crearea unui site web sau a unui e-mail fals care imită o organizație legitimă. (8)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos.

ORIZONTAL

4 orizontal: Scanarea forumurilor online și a canalelor hackerilor pentru date corporative furate. (12 litere):

7 orizontal: Trimiterea de mesaje frauduloase pentru a păcăli utilizatorii să renunțe la credențiale. (8 litere):

8 orizontal: Expunerea neautorizată a bazelor de date private care conțin înregistrări personale ale utilizatorilor. (8 litere):

VERTICAL

1 vertical: Pas secundar de verificare (precum cheile hardware) care protejează autentificările în conturi. (11 litere):

2 vertical: Nume de utilizator, parole și token-uri private folosite pentru autentificarea identităților digitale. (11 litere):

3 vertical: Restricționarea accesului la dosarele de credit pentru a preveni cererile frauduloase de împrumut. (9 litere):

5 vertical: Instruire și controale tehnice folosite pentru a proteja împotriva furtului de identitate. (7 litere):

6 vertical: Crearea unui site web sau a unui e-mail fals care imită o organizație legitimă. (8 litere):

Punct de control 6: Căutarea cuvintelor ascunse

Găsește în grila de mai jos cei 8 termeni cheie de vocabular ascunși. Cuvintele pot fi orizontale, verticale sau diagonale.

I C R Q L D I Î S Z Ș E R U D

E G A A R O M N P T S X Q Î S

L N T S B M Y G Ă F C S W W Î

A I A R A Z Y H Y K U F I M R

I F Î L P L T E O G R Q Q M G

Ț O Z A Ă O U Ț F Ț G Â Y U S

N O Y Ă R G L A Z F E Î N L P

E P N W A Â L R Z Y R F X T O

D S V Ț R J U E P Ă I N U I T

E L G U E B X Ț J R Ă W Z F X

R M O N I T O R I Z A R E A L

C S Q W H O C A B Î Q V W C W

K I P H I S H I N G H T H T F

Ă D I J Ș S V R Z D H D S O Â

A K Q Â Z L J U S Ț A S W R Î

LISTĂ DE CUVINTE DIN VOCABULAR

CREDENȚIALE SCURGERI MULTIFACTOR MONITORIZARE ÎNGHEȚARE APĂRARE SPOOFING PHISHING

Punct de control 6, variantă alternativă: Asocierea accesibilă a vocabularului

Asociază fiecare dintre cei 8 termeni de vocabular din Căutarea de cuvinte cu definiția corectă, scriind litera (A-H) în spațiul liber.

TERMENI DE VOCABULAR

- **A. CREDENȚIALE**
- **B. SCURGERI**
- **C. MULTIFACTOR**
- **D. MONITORIZARE**
- **E. ÎNGHEȚARE**
- **F. APĂRARE**
- **G. SPOOFING**
- **H. PHISHING**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Trimiterea de mesaje frauduloase pentru a păcăli utilizatorii să renunțe la credențiale.
2. Nume de utilizator, parole și token-uri private folosite pentru autentificarea identităților digitale.
3. Crearea unui site web sau a unui e-mail fals care imită o organizație legitimă.
4. Instruire și controale tehnice folosite pentru a proteja împotriva furtului de identitate.
5. Scanarea forumurilor online și a canalelor hackerilor pentru date corporative furate.
6. Restricționarea accesului la dosarele de credit pentru a preveni cererile frauduloase de împrumut.
7. Expunerea neautorizată a bazelor de date private care conțin înregistrări personale ale utilizatorilor.
8. Pas secundar de verificare (precum cheile hardware) care protejează autentificările în conturi.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie de securitate cibernetică. Scrie răspunsurile în casetele de introducere furnizate.

1. EȚLRNICAEED
2. IRUMOFLTCAT
3. ÎȚENAEHRG
4. ONGIFSPO
5. GECIRSRU
6. ETZAORIMORNI
7. ARAEPRĂ
8. SHHGPNII

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Lucruri de făcut dacă ți se fură identitatea			
2	Lucruri pe care să nu le distribui pe rețelele sociale			
3	Lucruri pe care le salvezi într-o copie de rezervă			
4	Carduri sau acte de identitate din portofelul tău			
5	Documente pe care ar trebui să le protejezi			
6	Lucruri de făcut după o scurgere de date			
7	Motive pentru care ar trebui să actualizezi software-ul			
8	Informații pe care le vrea un hoț de identitate			
9	Dispozitive care pot fi sparte			
10	Locuri de unde pot ieși datele tale			
11	Obiceiuri sigure pe care le poți începe de azi			
12	Semne că un calculator este infectat			
13	Moduri de a dovedi cine ești			
14	Semne ale furtului de identitate			
15	Semnale de avertizare într-un e-mail			

Punct de control 8: Studii de caz despre securitatea cibernetică

Aplică conceptele pe care le-ai învățat pentru a rezolva scenariile reale de mai jos.

STUDIU DE CAZ 1: PROTEJAREA ÎMPOTRIVA FALSIFICĂRII IDENTITĂȚII UNUI DIRECTOR



Scenariu: Un director de rang înalt (C-suite) a fost vizat de nume de domenii cu greșeli de scriere intenționate (typo-squatting), care imită adresa lui personală de e-mail pentru a înșela clienții. Proiectează un plan de protecție a brandului.

Întrebare de discuție: Analizează riscurile de falsificare a brandului și detaliază SPF/DKIM/DMARC și controalele de autentificare.

STUDIU DE CAZ 2: EXPUNEREA CREDENȚIALELOR CORPORATIVE PE DARK WEB



Scenariu: Un dump de bază de date de pe dark web conține câteva sute de credențiale corporative aparținând administratorilor de sistem ai unei companii. Proiectează o strategie de reducere a riscului.

Întrebare de discuție: Descrie pe scurt procesul de curățare a credențialelor și planifică implementarea unui manager de parole.

Punct de control 9: Descifrează codul

Un profesionist în securitate cibernetică protejează activele rețelei de actorii amenințărilor online. Folosește cheia literă–număr de mai jos pentru a descifra mesajul, scriind literele corespunzătoare în spațiile libere.

CHEIE DE CRIPTARE LITERĂ-NUMĂR

A=1 Ă=2 Â=3 B=4 C=5 D=6 E=7 F=8 G=9 H=10 I=11

Î=12 J=13 K=14 L=15 M=16 N=17 O=18 P=19 Q=20 R=21 S=22

Ș=23 T=24 Ț=25 U=26 V=27 W=28 X=29 Y=30 Z=31

19	21	18	24	7	13	7	1	31	2

11	6	7	17	24	11	24	1	24	7	1	5	26

16	26	15	24	11	8	1	5	24	18	21

Mesaj descifrat:

SFAT: FIECARE NUMĂR REPREZINTĂ POZIȚIA ACELEI LITERE ÎN ALFABET (DE EX. 1 = A, 2 = B, 31 = Z).

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea A)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q1: Ce este furtul de identitate?

O infracțiune în care un atacator fură date personale (precum parole sau numere SSN) pentru a se da drept altcineva în scop de câștig financiar.

Q2: Care este cea mai frecventă cauză a furtului de identitate?

Phishing-ul este una dintre principalele modalități prin care hoții obțin parole, atrăgându-i pe utilizatori pe site-uri false, falsificate.

Q3: Cum protejează autentificarea multifactor (MFA) identitățile?

MFA necesită o a doua dovadă (precum o cheie hardware) pentru autentificare, blocând atacatorii chiar dacă îți fură parola.

Q4: Ce este înghețarea creditului (credit freeze)?

Un serviciu gratuit care împiedică birourile de credit să partajeze dosarul tău de credit, oprind hoții să deschidă împrumuturi noi pe numele tău. [2]

Q5: Ce este monitorizarea dark web?

Software care verifică forumurile hackerilor pentru e-mailuri, parole și înregistrări personale scurse și te alertează dacă datele tale sunt expuse.

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea B)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Ce înseamnă credential stuffing?

Boți automatizați care testează liste de parole scurse pe sute de site-uri web pentru a prelua conturi active.

Q7: De ce este periculoasă falsificarea e-mailului (email spoofing)?

Le permite atacatorilor să falsifice numele expeditorului în e-mailuri, făcând ca mesajele de phishing să pară că provin de la colegi de încredere.

Q8: Cum opresc managerii de parole furtul de identitate?

Stochează parole complexe și unice pentru fiecare cont și refuză să completeze automat datele de autentificare pe domenii de phishing false.

Q9: Ce este spear phishing-ul?

Un atac de phishing extrem de țintit, personalizat cu numele și detaliile victimei pentru a crește șansa de înșelare.

Q10: Prin ce se deosebește o alertă de credit de o înghețare a creditului?

O alertă le spune creditorilor să-ți verifice identitatea înainte de a deschide conturi, în timp ce o înghețare blochează complet accesul la dosarul tău de credit. [2]

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea C)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q1: Cum duce SIM swapping la furtul de identitate?

Atacatorii conving personalul operatorului de telefonie să transfere numărul de telefon al victimei pe un nou card SIM, deturnând codurile 2FA trimise prin SMS.

Q2: Care este rolul DMARC în prevenirea furtului de identitate?

DMARC permite proprietarilor de domenii să blocheze ajungerea e-mailurilor falsificate în căsuțele de intrare, oprind e-mailurile false care imită domeniile corporative.

Q3: De ce este dificil de detectat furtul de identitate sintetică?

Hoții combină SSN-uri reale cu nume și date de naștere false pentru a construi profiluri de credit complet noi, ocolind alertele de bază de fraudă.

Q4: Cum exploatează brokerii de date identitățile personale?

Brokerii de date colectează înregistrări publice, comportament web și istoricul achizițiilor pentru a compila dosare de profil, care pot fi scurse sau vândute.

Q5: De ce este considerată vulnerabilă MFA prin SMS?

Traficul SMS este vulnerabil la interceptare, phishing și exploatări de tip SIM-swapping la nivel de operator.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea D)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q6: Ce este blocarea dosarului de credit?

Un serviciu comercial similar unei înghețări, care le permite utilizatorilor să deblocheze sau să blocheze instantaneu dosarul de credit printr-o aplicație mobilă.

Q7: Cum alimentează brețele de date corporative furtul de identitate?

Bazele de date scurse expun milioane de credențiale în text simplu, oferind hoților datele brute necesare pentru a comite fraude de identitate țintite.

Q8: Care este riscul partajării excesive pe rețelele sociale?

Partajarea publică a numelor animalelor de companie, a locurilor de naștere și a numelui de fată al mamei le oferă hoților răspunsurile la întrebările obișnuite de recuperare a contului.

Q9: Cum protejează autentificările biometrice profilurile de identitate?

Biometria leagă autentificările de trăsături precum amprentele sau fețele; păstrate pe dispozitiv, sunt greu de furat, dar datele biometrice stocate pot fi scurse.

Q10: Cum combate regula Red Flags furtul de identitate?

O reglementare federală care impune instituțiilor financiare să elaboreze programe scrise pentru a detecta semnele de avertizare ale furtului de identitate și a răspunde la ele.

Partea 11: 10 fapte și perspective din lumea reală despre securitatea cibernetică

Parcurge fapte din lumea reală despre breșele de securitate, mecanismele de apărare și standardele de conformitate.

1. INFORMAȚII DESPRE SECURITATE

IdentityTheft.gov, administrat de FTC, le permite victimelor din SUA să raporteze furtul de identitate și să primească un plan personal de recuperare. [1]

2. INFORMAȚII DESPRE SECURITATE

Cheile de securitate hardware reprezintă MFA rezistent la phishing, cel mai puternic tip de MFA pe care îl recomandă CISA. [4]

3. INFORMAȚII DESPRE SECURITATE

Parolele compromise sunt un punct de intrare frecvent în breșele de date și alimentează fraudele de identitate ulterioare.

4. INFORMAȚII DESPRE SECURITATE

O înghețare a creditului este gratuită conform legii federale și împiedică creditorii să verifice dosarele de credit până la deblocare. [2]

5. INFORMAȚII DESPRE SECURITATE

DMARC permite proprietarilor de domenii să spună serverelor de e-mail să respingă sau să pună în carantină e-mailurile falsificate care nu trec verificările. [7]

6. INFORMAȚII DESPRE SECURITATE

Schimbul de SIM (SIM swapping) permite hackerilor să ocolească autentificarea în doi pași prin SMS pe portalurile bancare.

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Frauda cu identități sintetice combină detalii reale și false, ceea ce o face greu de detectat de către creditori.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

Multe persoane refolosesc aceeași parolă pentru conturile online, așa că o singură breșă poate expune mai multe dintre ele.

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Brokerii de date compilează dosare detaliate despre un număr mare de consumatori, ceea ce creează un risc concentrat pentru confidențialitate.

10. INFORMAȚII DESPRE SECURITATE

Recuperarea în urma furtului de identitate poate dura luni de muncă, cum ar fi contestarea taxelor și corectarea rapoartelor de credit.

Referințe tehnice și surse

Ghidul de studiu și puzzle-urile interactive sunt alcătuite pe baza standardelor globale NIST, OWASP și de conformitate privind confidențialitatea datelor.

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[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

Barem: Punct de control 1 – Alegere multiplă

1 Întrebarea 1 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Care este metoda principală prin care hoții de identitate fură datele de conectare? → Trimiterea de alerte false prin e-mail care păcălesc utilizatorii să introducă parole pe portaluri falsificate

2 Întrebarea 2 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce control de securitate oferă cea mai puternică apărare împotriva scurgerilor de credențiale? → Autentificare multi-factor cu chei hardware

3 Întrebarea 3 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce reprezintă înghețarea creditului? → Blocarea rapoartelor de credit pentru a împiedica hoții să deschidă împrumuturi neautorizate

4 Întrebarea 4 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

De ce este utilă monitorizarea dark web-ului? → Alertează utilizatorii dacă datele lor de autentificare scurse apar în baze de date ilicite

5 Întrebarea 5 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce înseamnă inginerie socială? → Manipularea oamenilor pentru a-i determina să dezvăluie de bunăvoie date confidențiale de autentificare

Barem: Punct de control 2 – Adevărat sau fals

6 Întrebarea 6

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Furtul de identitate poate începe și offline, de exemplu prin corespondență sau documente furate.

7 Întrebarea 7

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Impunerea MFA pe toate conturile personale blochează majoritatea atacurilor botnet de tip credential stuffing.

8 Întrebarea 8

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Înghețarea creditului oprește noile verificări de credit, dar nu afectează conturile tale existente.

9 Întrebarea 9

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Managerii de parole îi protejează pe utilizatori de phishing prin refuzul de a completa automat parole pe domenii falsificate.

10 Întrebarea 10

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

E-mailurile de phishing folosesc adesea un limbaj urgent pentru a declanșa reacții emoționale și rapide.

Chei de vocabular și grilă de notare

Barem de notare pentru profesor: Acordă 1 punct pentru fiecare asociere corectă (8 puncte în total) și pentru fiecare termen din context (6 puncte în total).

PUNCT DE CONTROL 4: BAREM – ASOCIEREA CONCEPTELOR

H 1. CREDENȚIALE	D 2. SCURGERI	A 3. MFA	G 4. MONITORIZARE
C 5. ÎNGHEȚARE	E 6. APĂRARE	B 7. FALSIFICARE (SPOOFING)	F 8. PHISHING

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 CREDENȚIALE	2 SCURGERI	3 MULTIFACTOR	4 MONITORIZARE
5 ÎNGHEȚARE	6 APĂRARE		

PUNCT DE CONTROL 6, VARIANTĂ ALTERNATIVĂ: BAREM – ASOCIEREA CUVINTELOR

1 H – PHISHING	2 A – CREDENȚIALE	3 G – SPOOFING	4 F – APĂRARE
5 D – MONITORIZARE	6 E – ÎNGHEȚARE	7 B – SCURGERI	8 C – MULTIFACTOR

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica CREDENȚIALE, SCURGERI și MFA cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

Studii de caz:
Cere elevilor să își susțină recomandările cu fapte din fișă, nu cu presupuneri.

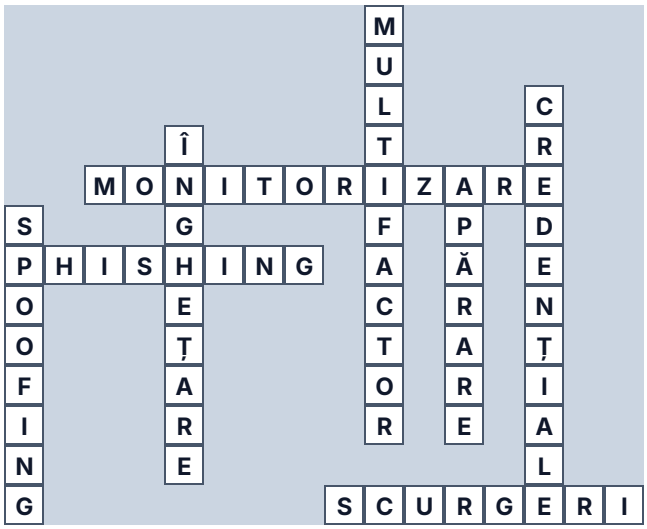
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

4 orizontal: MONITORIZARE Scanarea forumurilor online și a canalelor hackerilor pentru date corporative furate. (12 litere)

7 orizontal: PHISHING Trimiterea de mesaje frauduloase pentru a păcăli utilizatorii să renunțe la credențiale. (8 litere)

8 orizontal: SCURGERI Expunerea neautorizată a bazelor de date private care conțin înregistrări personale ale utilizatorilor. (8 litere)

VERTICAL

1 vertical: MULTIFACTOR Pas secundar de verificare (precum cheile hardware) care protejează autentificările în conturi. (11 litere)

2 vertical: CREDENȚIALE Nume de utilizator, parole și token-uri private folosite pentru autentificarea identităților digitale. (11 litere)

3 vertical: ÎNGHEȚARE Restricționarea accesului la dosarele de credit pentru a preveni cererile frauduloase de împrumut. (9 litere)

5 vertical: APĂRARE Instruire și controale tehnice folosite pentru a proteja împotriva furtului de identitate. (7 litere)

6 vertical: SPOOFING Crearea unui site web sau a unui e-mail fals care imită o organizație legitimă. (8 litere)

Cuvinte amestecate și barem pentru codul cifrat

Barem pentru activitatea de descifrare a cuvintelor de vocabular și pentru provocarea Codul secret.

BAREMUL PENTRU DESCIFRAREA CUVINTELOR

1. E Ț L R N I C A E E D — **CREDENȚIALE**
2. I R U M O F L T C A T — **MULTIFACTOR**
3. Î Ț E N A E H R G — **ÎNGHEȚARE**
4. O N G I F S P O — **SPOOFING**
5. G E C I R S R U — **SCURGERI**
6. E T Z A O R I M O R N I — **MONITORIZARE**
7. A R A E P R Ă — **APĂRARE**
8. S H H G P N I I — **PHISHING**

BAREMUL PROVOCĂRII CU CODUL SECRET

"PROTEJEAZĂ IDENTITATEA CU MULTIFACTOR"

Barem pentru studiile de caz

A Studiu de caz 1: Protejarea împotriva falsificării identității unui director

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un executiv de rang înalt (C-suite) a fost vizat de nume de domenii cu greșeli de scriere (typo-squatting) care imită e-mailul său personal pentru a frauda clienți. Proiectează un plan de protecție a mărcii.
- Strategie și soluție recomandată: Înregistrează toate variantele ortografice uzuale ale numelui directorului. Implementează protocoale de autentificare a e-mailului (DMARC, DKIM, SPF) pentru a preveni falsificarea domeniului. Impune MFA hardware pentru toate autentificările corporative ale conducerii executive (C-suite).

B Studiu de caz 2: Expunerea credențialelor corporative pe dark web

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un dump de bază de date de pe dark web conține câteva sute de credențiale corporative aparținând administratorilor de sistem ai unei întreprinderi. Proiectează o strategie de atenuare.
- Strategie și soluție recomandate: Efectuează o resetare a parolelor la nivelul întregii companii. Impune folosirea unui manager de parole enterprise. Aplică MFA pe toate portalurile sistemului și configurează alerte automate continue de monitorizare a dark web.