Nume: _____ **Data:** _____ **Punctaj:** _____

Escrocherii online și inginerie socială Ghid de protecție

Phishing prin e-mail, domenii falsificate, vishing, escrocherii de asistență, verificare în afara canalului (out-of-band), BEC

PREZENTARE GENERALĂ DESPRE ESCROCHERIILE ONLINE

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 apărarea împotriva fraudelor online. Vei explora site-urile false de phishing, tacticile de inginerie socială, fraudele de asistență, vectorii fraudelor prin transfer bancar și metodele de verificare a plăților.

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/escrocherii-online/

Harta ta de învățare despre protecția împotriva fraudelor online

- Identifică indicatorii frecvenți ai înșelătoriilor de tip suport tehnic și ai domeniilor typosquatting.
- Implementează protocoale de verificare a e-mailului (SPF, DKIM, DMARC) împotriva falsificării.
- Stabilește verificarea tranzacțiilor în afara canalului (out-of-band) pentru a preveni frauda cu transferuri bancare în afaceri.

INSTRUCȚIUNI DESPRE ESCROCHERIILE ONLINE

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 împotriva fraudelor online. Încheie cu activitatea bonus Gândește repede.

PROTECȚIA ÎMPOTRIVA ESCROCHERIILOR ONLINE ȘI A INGINERIEI SOCIALE (INTRODUCERE)

Escrocheriile online exploatează comportamentul uman prin phishing, ferestre pop-up de asistență, vishing și fraudă prin transfer bancar. Verificarea tranzacțiilor prin canale separate și regulile de domeniu SPF/DKIM/DMARC ajută la blocarea vectorilor de inginerie socială la nivelul gateway-ului.

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

Punct de control 1: Provocare cu alegere multiplă

1. Care este indicatorul principal al unei înșelăciuni de tip suport tehnic?

- A. O fereastră pop-up care pretinde că sistemul tău este infectat și cere să suni la un număr de telefon
- B. O actualizare de securitate automată descărcată dintr-un registru oficial
- C. Un manager de parole care refuză să completeze datele de autentificare pe un domeniu corporativ
- D. O copie de rezervă a fișierelor în fundal, care rulează pe o configurație cu unitate externă

2. Ce tehnică folosește domenii de expeditor falsificate pentru a fura datele bancare?

- A. Phishing prin e-mail
- B. Scanarea porturilor
- C. Injectare în memorie
- D. Distrugerea criptografică

3. Ce reprezintă frauda prin transfer bancar?

- A. Păcălirea victimelor să trimită bani în conturi corporative false prin inginerie socială
- B. Criptarea bazelor de date de sistem folosind sarcini utile de tip ransomware
- C. Interogarea bazelor de date prin comenzi de tip SQL injection
- D. Copierea de rezervă a fișierelor de sistem pe discuri de stocare offline

4. De ce creează escrocii site-uri false de cumpărături?

- A. Pentru a fura detaliile cardurilor de credit și datele de plată ale cumpărătorilor
- B. Pentru a găzdui tabele de baze de date pentru analiza software-ului rău intenționat în sandbox
- C. Pentru a accelera livrarea comenzilor online
- D. Pentru a testa gratuit noi designuri de site-uri web

5. Ce înseamnă vishing?

- A. Înșelăciuni de tip voice phishing prin rețelele telefonice pentru a fura datele de autentificare
- B. Scanarea rețelelor locale pentru dispozitive de sistem nesecurizate
- C. Restaurarea bazelor de date ale sistemului după o breșă neautorizată
- D. Rularea codului nesigur în interiorul unor containere virtuale securizate

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Escrocheriile de phishing vizează doar utilizatorii finali, niciodată țintele de nivel executiv de tip whaling.

- ◯ Adevărat
- ◯ Fals

7 Întrebare 7

7. Domeniile falsificate folosesc adesea mici greșeli de tastare (precum amaz0n.com) pentru a imita branduri de încredere.

- ◯ Adevărat
- ◯ Fals

8 Întrebare 8

8. Escrocheriile de tip suport tehnic pot fi rezolvate acordând acces la distanță persoanei care sună.

- ◯ Adevărat
- ◯ Fals

9 Întrebare 9

9. Ingineria socială exploatează psihologia umană, cum ar fi frica și urgența, pentru a ocoli regulile de securitate.

- ◯ Adevărat
- ◯ Fals

10 Întrebare 10

10. Cererile de transfer bancar ar trebui verificate întotdeauna prin canale de comunicare separate (out-of-band).

- ◯ 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. E-mailurile frauduloase care păcălesc utilizatorii se numesc _____ .

2. Adresele web care imită mărci de încredere sunt _____ .

3. Escrocheriile vocale care vizează datele bancare se numesc _____ .

4. Un pop-up care cere bani pentru eliminarea unui virus este o _____ de asistență tehnică.

5. Confirmarea unei cereri de plată necesită _____ printr-un alt canal.

6. Trimiterea tranzacțiilor comerciale către conturile hoților prin înșelăciune este o _____ de fonduri.

BANCĂ DE CUVINTE DIN VOCABULAR

DETURNARE FALSIFICATE ÎNȘELĂCIUNE PHISHING SMISHING VERIFICARE VISHING WHALING

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor despre securitate

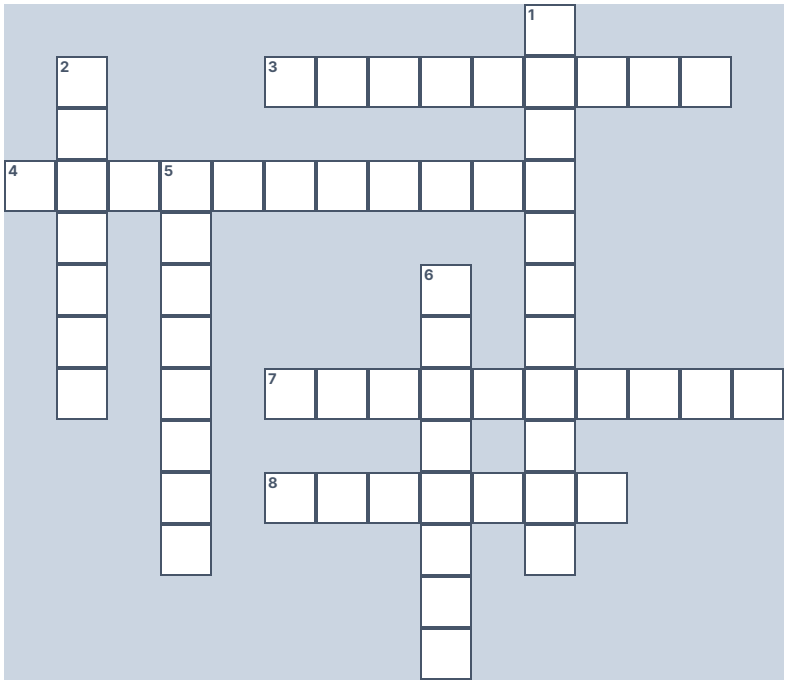
ASOCIEREA DEFINIȚIILOR

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

☐	1. PHISHING	A	Redirecționarea frauduloasă a tranzacțiilor bancare către conturi infracționale.
☐	2. FALSIFICAT	B	Schemă frauduloasă concepută pentru a fura bani sau date de acces de la victime.
☐	3. VISHING	C	Trimiterea de mesaje text de tip fraudă pentru a fura datele de autentificare ale conturilor mobile.
☐	4. ESCROCHERIE	D	Apeluri vocale frauduloase concepute pentru a fura datele de autentificare și detaliile contului.
☐	5. VERIFICARE	E	Atacuri de phishing țintite care urmăresc furtul datelor de autentificare de la directori de rang înalt (C-level).
☐	6. CABLU	F	Adresă de expeditor de e-mail sau de site imitată, concepută să pară legitimă.
☐	7. WHALING	G	Campanii de e-mail frauduloase concepute pentru a fura datele de autentificare și parolele.
☐	8. SMISHING	H	Confirmarea detaliilor de plată printr-o metodă de contact secundară de încredere.

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

3. Redirecționarea frauduloasă a tranzacțiilor bancare către conturi infracționale. (9)

4. Adresă de expeditor sau de site imitată, creată să pară legitimă. (11)

7. Confirmarea detaliilor de plată printr-o metodă de contact secundară, de încredere. (10)

8. Apeluri vocale frauduloase menite să fure credențiale și detalii de cont. (7)

VERTICAL

1. Schemă frauduloasă menită să fure bani sau accesul la credențialele victimelor. (11)

2. Atacuri de phishing țintite, care vizează furtul credențialelor directorilor de nivel C. (7)

5. Trimiterea de mesaje text de tip escrocherie pentru a fura credențialele conturilor mobile. (8)

6. Campanii frauduloase de e-mail menite să fure datele de autentificare și parolele. (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

3 orizontal: Redirecționarea frauduloasă a tranzacțiilor bancare către conturi infracționale. (9 litere):

4 orizontal: Adresă de expeditor sau de site imitată, creată să pară legitimă. (11 litere):

7 orizontal: Confirmarea detaliilor de plată printr-o metodă de contact secundară, de încredere. (10 litere):

8 orizontal: Apeluri vocale frauduloase menite să fure credențiale și detalii de cont. (7 litere):

VERTICAL

1 vertical: Schemă frauduloasă menită să fure bani sau accesul la credențialele victimelor. (11 litere):

2 vertical: Atacuri de phishing țintite, care vizează furtul credențialelor directorilor de nivel C. (7 litere):

5 vertical: Trimiterea de mesaje text de tip escrocherie pentru a fura credențialele conturilor mobile. (8 litere):

6 vertical: Campanii frauduloase de e-mail menite să fure datele de autentificare și parolele. (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.

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

LISTĂ DE CUVINTE DIN VOCABULAR

PHISHING FALSIFICATE VISHING ÎNȘELĂCIUNE VERIFICARE DETURNARE WHALING SMISHING

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. PHISHING
B. FALSIFICATE
C. VISHING
D. ÎNȘELĂCIUNE
E. VERIFICARE
F. DETURNARE
G. WHALING
H. SMISHING

	DEFINIȚII ȘI CÂMPURI DE ASOCIERE
	1. Adresă de expeditor sau de site imitată, creată să pară legitimă.
	2. Confirmarea detaliilor de plată printr-o metodă de contact secundară, de încredere.
	3. Redirecționarea frauduloasă a tranzacțiilor bancare către conturi infracționale.
	4. Trimiterea de mesaje text de tip escrocherie pentru a fura credențialele conturilor mobile.
	5. Atacuri de phishing țintite, care vizează furtul credențialelor directorilor de nivel C.
	6. Apeluri vocale frauduloase menite să fure credențiale și detalii de cont.
	7. Campanii frauduloase de e-mail menite să fure datele de autentificare și parolele.
	8. Schemă frauduloasă menită să fure bani sau accesul la credențialele victimelor.

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. **NSHPIHGI** _____
2. **VSGNIHI** _____
3. **VIRCEFEIAR** _____
4. **GHILNWA** _____
5. **AACILEIFFTS** _____
6. **LEĂINUÎNCȘE** _____
7. **NDREAUERT** _____
8. **SMHGSNII** _____

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Dispozitive care pot fi sparte			
2	Expresii pe care le folosesc adesea escrocii			
3	Metode de plată pe care le cer escrocii			
4	Tipuri de escrocherii online			
5	Oferte prea bune ca să fie adevărate			
6	Locuri în care poți raporta o escrocherie			
7	Cuvinte legate de securitatea cibernetică			
8	Persoane pe care le poți avertiza despre escrocherii			
9	Lucruri pe care le salvezi într-o copie de rezervă			
10	Semnale de avertizare într-un e-mail			
11	Semne că un calculator este infectat			
12	Moduri de a verifica un magazin online			
13	Moduri de a-ți proteja conturile			
14	Lucruri de făcut dacă ești înșelat			
15	Lucruri de făcut după o scurgere de date			

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: PREVENIREA ESCROCHERIILOR CU TRANSFERURI BANCARE CORPORATIVE

👷

Scenariu: Un departament financiar primește un e-mail urgent de la o adresă falsificată a unui furnizor, în care i se cere ca viitoarele transferuri pentru facturi să fie direcționate către un nou număr de rutare.

Întrebare de discuție: Descrie pe scurt politica de verificare a fraudei prin transfer bancar și specifică blocurile de autentificare a e-mailurilor.

STUDIU DE CAZ 2: INCIDENT DE PHISHING DE TIP WHALING ÎMPOTRIVA CONDUCERII

👷

Scenariu: Un director a dat clic pe un link de phishing care pretindea că deține un document securizat pentru ședința consiliului, introducând credențialele sale corporative principale pe un portal falsificat.

Întrebare de discuție: Detaliază pașii de răspuns la incident și explică cum se auditează autentificările directorului.

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

6 7 24 7 5 24 7 1 31 2

19 10 11 22 10 11 17 9 26 15 5 26 22 5 1 17 7 21

23 11 27 7 21 11 8 11 5 1 21 7

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 o escrocherie online?

O schemă frauduloasă care folosește canale digitale pentru a păcăli victimele să trimită bani sau să dezvăluie datele personale de autentificare.

Q2: Care este principalul indicator al unui e-mail de phishing?

Un mesaj care pretinde urgență (precum suspendarea contului) și te direcționează către un link care nu corespunde domeniului oficial.

Q3: Ce este typosquatting?

Înregistrarea domeniilor cu greșeli de scriere frecvente ale unor mărci populare (precum amaz0n.com) pentru a găzdui site-uri false de phishing.

Q4: Ce este o escrocherie de suport tehnic?

O fereastră pop-up care pretinde că PC-ul tău este infectat, îndemnându-te să suni la un număr și să plătești pentru software fals de curățare sau pentru servicii de acces la distanță. [1]

Q5: Ce este vishing-ul?

Atacuri de phishing prin apeluri telefonice vocale, pentru a păcăli victimele să dezvăluie datele contului bancar sau de autentificare.

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 fraudă electronică (wire fraud)?

Redirecționarea tranzacțiilor de plată către conturi de escrocherie prin uzurparea identității unor furnizori sau directori.

Q7: Ce este whaling-ul?

O formă extrem de țintită de spear phishing, care vizează direct ținte de mare valoare, precum directorii de nivel executiv ai companiilor.

Q8: Ce este smishing-ul?

Mesaje text de escrocherie trimise pe dispozitive mobile, care conțin link-uri către portaluri false sau actualizări de urmărire.

Q9: De ce este esențială verificarea out-of-band?

Confirmă detaliile tranzacției printr-un canal de comunicare separat (cum ar fi un apel telefonic), evitând conversațiile de e-mail compromise.

Q10: Cum funcționează o escrocherie cu cont escrow fals?

Escrocii creează un site escrow falsificat, pretinzând că fondurile sunt păstrate în siguranță, apoi fură transferul bancar al cumpărătorului.

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 folosesc escrocii BEC (Business Email Compromise) pentru a comite fraude prin transfer bancar?

Preiau contul de e-mail al unui angajat legitim, monitorizează conversațiile despre facturi și trimit detalii de facturare actualizate cu conturi bancare frauduloase.

Q2: Care este riscul atacurilor homograf IDN în escrocheriile online?

Folosirea caracterelor non-ASCII care arată identic cu literele obișnuite (de ex., „a” chirilic) pentru a înregistra domenii falsificate care imită branduri reale.

Q3: De ce este importantă inspectarea antetelor e-mailului în detectarea escrocheriilor?

Dezvăluie adresa IP reală a serverului de origine și starea validării SPF/DKIM, arătând dacă domeniul expeditorului este falsificat.

Q4: Cum exploatează escrocii de suport tehnic software-ul de desktop la distanță?

Folosesc utilitare precum AnyDesk sau TeamViewer pentru a se conecta la dispozitivul victimei, a planta malware și a fura parolele salvate.

Q5: Care este scopul escrocheriilor cu taxă în avans?

Păcălirea victimelor să plătească în avans taxe de procesare în schimbul unei recompense financiare mari care nu există.

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: Cum folosesc escrocii profilarea pe rețelele sociale pentru phishing țintit?

Compilează structurile organizaționale ale companiei și numele angajaților pentru a redacta e-mailuri convingătoare de spear-phishing.

Q7: De ce oferă magazinele web false reduceri mari?

Pentru a-i momi pe cumpărători să introducă datele cardului de credit, captând credențiale pentru reutilizare sau revânzare pe forumuri de carding.

Q8: Cum blochează înregistrările DMARC escrocheriile de phishing?

DMARC permite proprietarilor de domenii să ceară destinatarilor să pună în carantină sau să respingă mesajele care nu trec verificările SPF și DKIM aliniate, blocând falsificarea directă. [5]

Q9: Care este amenințarea portalurilor de colectare a acreditărilor?

Pagini de destinație falsificate, concepute să arate exact ca spațiile de lucru Microsoft 365 sau Google, care fură datele de autentificare pe măsură ce sunt introduse.

Q10: Cum raportează și dezactivează echipele de securitate domeniile de escrocherie?

Prin trimiterea dovezilor de fraudă către e-mailul de abuz al registrarului, furnizorul de găzduire și registrul Google Safe Browsing.

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

Phishing-ul și falsificarea identității (spoofing) au fost cel mai frecvent raportat tip de infracțiune către IC3 al FBI în 2025, cu 191.561 de plângeri. [2]

2. INFORMAȚII DESPRE SECURITATE

Compromiterea e-mailului de afaceri (BEC) a cauzat în 2025 pierderi de peste 3 miliarde $, raportate către IC3 al FBI. [2]

3. INFORMAȚII DESPRE SECURITATE

Domeniile cu greșeli de scriere intenționate (typosquatting) diferă de numele reale ale brandurilor printr-un caracter sau două, așa că o privire rapidă le poate omite.

4. INFORMAȚII DESPRE SECURITATE

Escrocheriile de tip suport tehnic au cauzat în 2025 pierderi de peste 2,1 miliarde USD raportate către IC3 al FBI. [2]

5. INFORMAȚII DESPRE SECURITATE

Atacurile homograf arată identic în barele de adrese ale browserelor, cu excepția cazului în care browserul afișează configurațiile punycode.

6. INFORMAȚII DESPRE SECURITATE

Escrocheriile prin mesaje SMS (smishing) folosesc mesaje scurte și urgente cu link-uri, lăsând victimelor puțin context pentru a recunoaște frauda.

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Atacurile de tip whaling vizează e-mailurile executivilor, deoarece aceștia controlează accesul la transferuri bancare mari.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

Verificarea modificărilor de plată printr-un apel la un număr de telefon cunoscut, salvat, este o apărare esențială împotriva fraudei BEC cu transferuri bancare.

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Site-urile false de cont escrow (de garanție) sunt o escrocherie frecventă pe piețele online: arată ca un serviciu de plată sigur, dar fură transferul bancar al cumpărătorului.

10. INFORMAȚII DESPRE SECURITATE

Google Safe Browsing avertizează utilizatorii înainte să deschidă site-uri semnalate pentru phishing sau malware.

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.). 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

Barem: Punct de control 1 – Alegere multiplă

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

NOTĂ PENTRU PROFESOR

Care este indicatorul principal al unei înșelăciuni de tip suport tehnic? → O fereastră pop-up care pretinde că sistemul tău este infectat și cere să suni la un număr de telefon

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

NOTĂ PENTRU PROFESOR

Ce tehnică folosește domenii de expeditor falsificate pentru a fura datele bancare? → Phishing prin e-mail

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

NOTĂ PENTRU PROFESOR

Ce reprezintă frauda prin transfer bancar? → Păcălirea victimelor să trimită bani în conturi corporative false prin inginerie socială

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

NOTĂ PENTRU PROFESOR

De ce creează escrocii site-uri false de cumpărături? → Pentru a fura detaliile cardurilor de credit și datele de plată ale cumpărătorilor

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

NOTĂ PENTRU PROFESOR

Ce înseamnă vishing? → Înșelăciuni de tip voice phishing prin rețelele telefonice pentru a fura datele de autentificare

Barem: Punct de control 2 – Adevărat sau fals

6 Întrebarea 6

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fals: phishing-ul vizează și directorii; whaling este phishing îndreptat către liderii de rang înalt.

7 Întrebarea 7

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Domeniile falsificate folosesc adesea mici greșeli de tastare (precum amaz0n.com) pentru a imita branduri de încredere.

8 Întrebarea 8

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fals: oferirea accesului la distanță unui escroc de tip asistență tehnică îi permite acestuia să planteze malware și să fure date.

9 Întrebarea 9

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Ingineria socială exploatează psihologia umană, cum ar fi frica și urgența, pentru a ocoli regulile de securitate.

10 Întrebarea 10

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Cererile de transfer bancar ar trebui verificate întotdeauna prin canale de comunicare separate (out-of-band).

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

G 1. PHISHING	F 2. FALSIFICAT	D 3. VISHING	B 4. ESCROCHERIE
H 5. VERIFICARE	A 6. CABLU	E 7. WHALING	C 8. SMISHING

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 PHISHING	2 FALSIFICATE	3 VISHING	4 ÎNȘELĂCIUNE
5 VERIFICARE	6 DETURNARE		

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

1 B – FALSIFICATE	2 E – VERIFICARE	3 F – DETURNARE	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – ÎNȘELĂCIUNE

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica PHISHING, FALSIFICAT și VISHING 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.

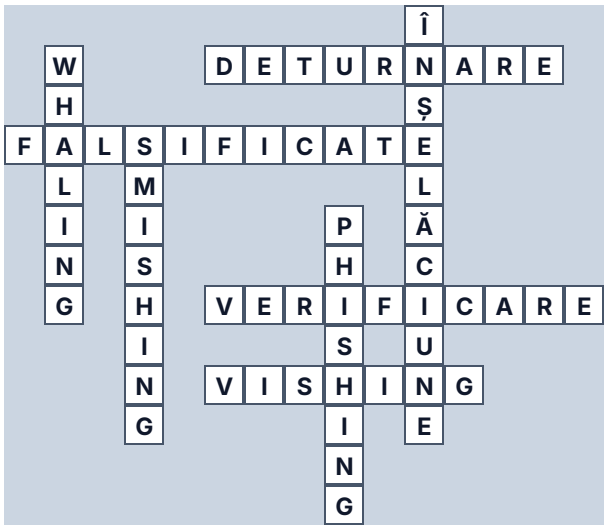
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

3 orizontal: DETURNARE Redirecționarea frauduloasă a tranzacțiilor bancare către conturi infracționale. (9 litere)

4 orizontal: FALSIFICATE Adresă de expeditor sau de site imitată, creată să pară legitimă. (11 litere)

7 orizontal: VERIFICARE Confirmarea detaliilor de plată printr-o metodă de contact secundară, de încredere. (10 litere)

8 orizontal: VISHING Apeluri vocale frauduloase menite să fure credențiale și detalii de cont. (7 litere)

VERTICAL

1 vertical: ÎNȘELĂCIUNE Schemă frauduloasă menită să fure bani sau accesul la credențialele victimelor. (11 litere)

2 vertical: WHALING Atacuri de phishing țintite, care vizează furtul credențialelor directorilor de nivel C. (7 litere)

5 vertical: SMISHING Trimiterea de mesaje text de tip escrocherie pentru a fura credențialele conturilor mobile. (8 litere)

6 vertical: PHISHING Campanii frauduloase de e-mail menite să fure datele de autentificare și parolele. (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. N S H P I H G I — **PHISHING**
2. V S G N I H I — **VISHING**
3. V I R C E F E I A R — **VERIFICARE**
4. G H I L N W A — **WHALING**
5. A A C I L E I F F T S — **FALSIFICATE**
6. L E Ă I N U Î N C Ș E — **ÎNȘELĂCIUNE**
7. N D R E A U E R T — **DETURNARE**
8. S M H G S N I I — **SMISHING**

BAREMUL PROVOCĂRII CU CODUL SECRET

"DETECTEAZĂ PHISHINGUL CU SCANER ȘI VERIFICARE"

Barem pentru studiile de caz

A Studiu de caz 1: Prevenirea escrocheriilor cu transferuri bancare corporative

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un departament financiar primește un e-mail urgent de la o adresă falsificată a unui furnizor, care cere ca viitoarele transferuri pentru facturi să fie direcționate către un nou cod de rutare.
- Strategie și soluție recomandată: Impune o politică de dublă autorizare pentru toate plățile. Implementează verificarea prin alt canal, folosind un număr de telefon salvat în prealabil, și blochează la nivel de gateway e-mailurile cu domenii falsificate.

B Studiu de caz 2: Incident de phishing de tip whaling împotriva conducerii

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un director a făcut clic pe un link de phishing care pretindea că conține un document securizat pentru ședința consiliului și și-a introdus datele de autentificare corporative principale pe un portal fals.
- Strategie și soluție recomandată: Izolează dispozitivul directorului. Resetează toate token-urile de sesiune și credențialele corporative. Examinează jurnalele de acces pentru ieșiri de date și implementează MFA hardware pentru toate autentificările.