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

# Atacuri de phishing și inginerie socială

Spear phishing, escrocherii de tip whaling, protocoalele SPF/DKIM/DMARC, falsificarea expeditorului și instruirea angajaților în materie de securitate.

## PREZENTARE GENERALĂ DESPRE ATACURILE DE PHISHING

**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 atacurile de phishing și ingineria socială. Vei explora spear phishing-ul, whaling-ul, falsificarea domeniilor, protocoalele SPF/DKIM/DMARC, siguranța link-urilor și instruirea de sensibilizare a angajaților.

### 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/atacuri-de-tip-phishing/

# Harta ta de învățare despre reducerea riscurilor de phishing

- Identifică înșelătoriile frecvente de tip phishing, vishing și ferestre pop-up de suport.
- Implementează proceduri de verificare a tranzacțiilor prin canal separat (out-of-band).
- Configurează regulile SPF, DKIM și DMARC pentru a bloca domeniile falsificate.

## INSTRUCȚIUNI DESPRE ATACURILE DE PHISHING

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 autentificarea e-mailului. Încheie cu activitatea bonus Gândește repede.

## ATACURI DE PHISHING ȘI INGINERIE SOCIALĂ (INTRODUCERE)

Atacurile de phishing folosesc mesaje țintite, escrocherii de tip whaling și falsificarea domeniilor pentru a colecta credențialele de autentificare ale utilizatorilor. Securizarea sistemelor corporative necesită implementarea regulilor SPF, DKIM și DMARC la nivelul gateway-ului, alături de pași de aprobare prin canale separate.

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

## Punct de control 1: Provocare cu alegere multiplă

**1. Ce este spear phishing?**

- A. Un e-mail de phishing țintit, adaptat unei anumite persoane sau organizații
- B. Un e-mail în masă trimis către milioane de adrese aleatorii
- C. Un atac de rețea care inundă serverele web cu trafic
- D. O tehnică de extragere din baza de date care vizează înregistrările utilizatorilor

**2. Ce protocol permite unui domeniu să listeze în DNS adresele IP de trimitere autorizate, pentru a combate falsificarea?**

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

**3. Ce este un atac de tip whaling?**

- A. O campanie de phishing țintită special spre directori de companii cu profil înalt
- B. Un atac de tip SQL injection care vizează copiile de rezervă ale bazelor de date
- C. Furtul fizic al echipamentelor router dintr-o rețea locală
- D. O scanare automată de tip brute-force cu credential stuffing

**4. Ce face DKIM?**

- A. Adaugă o semnătură criptografică la e-mailuri pentru a verifica autenticitatea expeditorului
- B. Blochează la nivelul firewall-ului traficul de pachete de rețea de intrare
- C. Criptează volumele de stocare ale bazelor de date în repaus
- D. Scanează atașamentele e-mailurilor în căutarea malware-ului bazat pe semnături

**5. Care este rolul DMARC?**

- A. Indicarea serverelor de e-mail destinatare cum să trateze verificările SPF/DKIM eșuate
- B. Decriptarea parolelor de sistem folosind tabele rainbow precalculate
- C. Comprimarea atașamentelor de e-mail înainte de livrare
- D. Configurarea privilegiilor de acces la rutarea rețelei

## Punct de control 2: Provocare Adevărat sau Fals

### 6 Întrebare 6

6. Spear phishing se bazează pe e-mailuri generice în masă trimise către milioane de adrese aleatorii.

- ○ Adevărat
- ○ Fals

### 7 Întrebare 7

7. Politicile DMARC pot instrui serverele de e-mail să respingă mesajele falsificate neautorizate.

- ○ Adevărat
- ○ Fals

### 8 Întrebare 8

8. Verificarea SPF funcționează prin validarea semnăturii criptografice a corpului e-mailului.

- ○ Adevărat
- ○ Fals

### 9 Întrebare 9

9. Atacurile de tip whaling vizează administratorii corporativi de nivel scăzut pentru a accesa fișiere din baze de date.

- ○ Adevărat
- ○ Fals

### 10 Întrebare 10

10. Verificarea în afara canalului (out-of-band) a cererilor de plată ajută la oprirea fraudelor prin transfer bancar.

- ○ 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. Țintirea unui anumit angajat cu informații personalizate este phishing de tip _____ .

2. Falsificarea antetului unui e-mail pentru ca mesajele să pară legitime se numește _____ al expeditorului.

3. Lista de IP-uri autorizate ale serverelor de e-mail, publicată în DNS, este înregistrarea _____ .

4. Standardul de semnătură criptografică din e-mail care oferă verificarea expeditorului este _____ .

5. Stabilirea unor politici de respingere a verificărilor SPF/DKIM eșuate folosește _____ .

6. O campanie de phishing care vizează directori de nivel C se numește _____ .

**BANCĂ DE CUVINTE DIN VOCABULAR**

DKIM DMARC PHISHING SPEAR SPF SPOOFING VISHING WHALING

**Scrie răspunsurile aici:**

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

# Punct de control 4: Asocierea conceptelor despre securitate

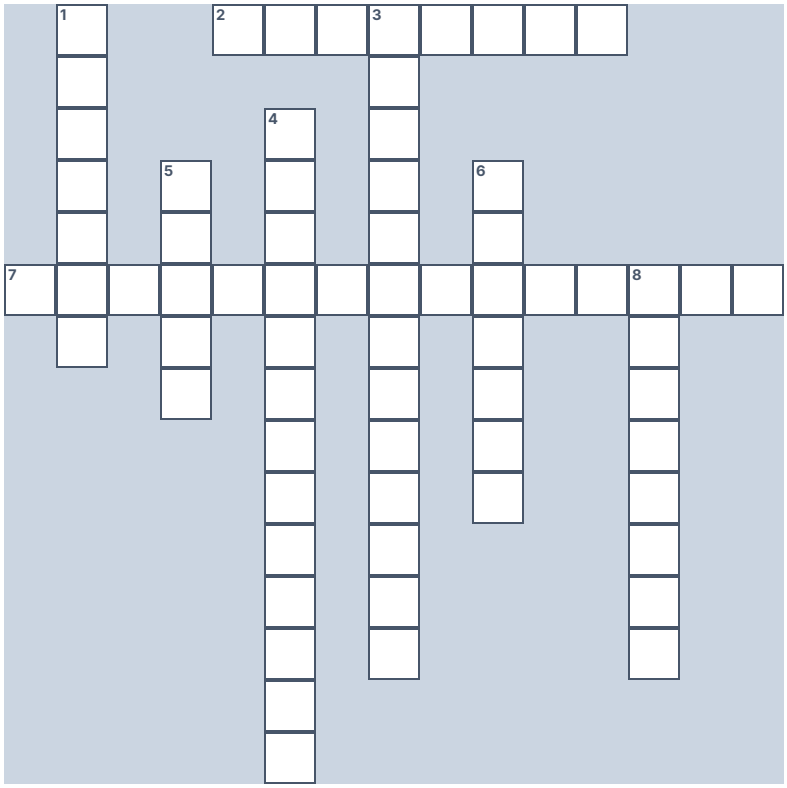
## ASOCIEREA DEFINIȚIILOR

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

| | | | |
|---|---|---|---|
| ☐ | 1. SPEAR | A | Apeluri de înșelăciune prin voce. |
| ☐ | 2. FALSIFICARE (SPOOFING) | B | Vizează directori de rang înalt (C-level). |
| ☐ | 3. SPF | C | Instrucțiuni de respingere a politicii. |
| ☐ | 4. DKIM | D | Adrese IP autorizate să trimită pentru DNS. |
| ☐ | 5. DMARC | E | E-mail de inginerie socială. |
| ☐ | 6. WHALING | F | E-mail personalizat și țintit. |
| ☐ | 7. PHISHING | G | Falsificarea adresei de e-mail a expeditorului. |
| ☐ | 8. VISHING | H | Semnătură criptografică în e-mail. |

## 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

**2. E-mail de inginerie socială. (8)**

**7. Adrese IP autorizate pentru expediere, publicate în DNS. (15)**

### VERTICAL

**1. Apeluri vocale de tip escrocherie. (7)**

**3. Semnătură criptografică în e-mail. (13)**

**4. Instrucțiuni de politică pentru respingere. (13)**

**5. E-mail personalizat și țintit. (5)**

**6. Vizarea directorilor de nivel C. (7)**

**8. Falsificarea adresei de e-mail a expeditorului. (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

**2 orizontal: E-mail de inginerie socială. (8 litere):**

**7 orizontal: Adrese IP autorizate pentru expediere, publicate în DNS. (15 litere):**

## VERTICAL

**1 vertical: Apeluri vocale de tip escrocherie. (7 litere):**

**3 vertical: Semnătură criptografică în e-mail. (13 litere):**

**4 vertical: Instrucțiuni de politică pentru respingere. (13 litere):**

**5 vertical: E-mail personalizat și țintit. (5 litere):**

**6 vertical: Vizarea directorilor de nivel C. (7 litere):**

**8 vertical: Falsificarea adresei de e-mail a expeditorului. (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.

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

### LISTĂ DE CUVINTE DIN VOCABULAR

SPEAR SPOOFING ÎNREGISTRARESPF SEMNĂTURĂDKIM POLITICĂDMARC
WHALING PHISHING VISHING

# 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. SPEAR |
| B. SPOOFING |
| C. ÎNREGISTRARESPF |
| D. SEMNĂTURĂDKIM |
| E. POLITICĂDMARC |
| F. WHALING |
| G. PHISHING |
| H. VISHING |

| DEFINIȚII ȘI CÂMPURI DE ASOCIERE |
| --- |
| 1. Falsificarea adresei de e-mail a expeditorului. |
| 2. E-mail personalizat și țintit. |
| 3. Apeluri vocale de tip escrocherie. |
| 4. Adrese IP autorizate pentru expediere, publicate în DNS. |
| 5. E-mail de inginerie socială. |
| 6. Instrucțiuni de politică pentru respingere. |
| 7. Semnătură criptografică în e-mail. |
| 8. Vizarea directorilor de nivel C. |

## 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. **AESRP** _____

2. **NIASRTSÎFPE RERG** _____

3. **OPĂMDRCLCT IAI** _____

4. **SNGIHPHI** _____

5. **FIPGOSNO** _____

6. **ĂDUTKMIĂSE RMN** _____

7. **WNIGHLA** _____

8. **IHGVNIS** _____

# Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

| | | | | |
|---|---|---|---|---|
| 1 | Dispozitive care pot fi sparte | | | |
| 2 | Semne ale unui e-mail de phishing | | | |
| 3 | Semne că un calculator este infectat | | | |
| 4 | Cuvinte care creează o falsă urgență | | | |
| 5 | Moduri de a verifica un expeditor | | | |
| 6 | Persoane pe care le poți întreba pentru ajutor IT | | | |
| 7 | Lucruri pe care le salvezi într-o copie de rezervă | | | |
| 8 | Pești sau creaturi marine pe care le cunoști | | | |
| 9 | Companii pe care escrocii se prefac că le reprezintă | | | |
| 10 | Obiceiuri sigure pe care le poți începe de azi | | | |
| 11 | Lucruri de făcut după ce ai dat clic pe un link fals | | | |
| 12 | Lucruri de făcut după o scurgere de date | | | |
| 13 | Canale prin care are loc phishing-ul | | | |
| 14 | Lucruri pe care nu le trimiți niciodată prin e-mail | | | |
| 15 | Moduri de a-ți proteja conturile | | | |

# 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: REMEDIEREA UNUI ATAC DE TIP WHALING ÎMPOTRIVA CONDUCERII DE TOP

👨‍💻

**Scenariu:** Un director financiar (CFO) primește un e-mail extrem de personalizat, care pretinde că vine de la CEO și cere un transfer rapid de 50.000 USD pentru a finaliza o achiziție confidențială de domeniu.

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

## STUDIU DE CAZ 2: IMPLEMENTAREA POLITICILOR GATEWAY SPF/DKIM/DMARC

👨‍💻

**Scenariu:** O companie eșuează la auditurile de securitate deoarece e-mailurile de marketing trimise sunt marcate frecvent ca spam, iar hackerii falsifică activ domeniul brandului companiei.

**Întrebare de discuție:** Stabilește controale tehnice și administrative pentru a verifica autenticitatea e-mailurilor.

## 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 | | 11 | 17 | 9 | 11 | 17 | 7 | 21 | 11 | 1 |
| | | | | | | | | | | | | | | | | | | | |
| 22 | 18 | 5 | 11 | 1 | 15 | 2 | | 19 | 21 | 11 | 17 | | 1 | 26 | 6 | 11 | 24 | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | 7 | 16 | 1 | 11 | 15 | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |

**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 phishing-ul?

Phishing-ul este un atac de inginerie socială în care infractorii trimit mesaje frauduloase pentru a păcăli utilizatorii să partajeze date sensibile.

### Q2: Care este diferența dintre phishing și spear phishing?

Phishing-ul vizează grupuri largi cu conținut generic, în timp ce spear phishing-ul vizează victime specifice folosind detalii personalizate.

### Q3: Ce este whaling?

Whaling este un atac de phishing extrem de țintit, îndreptat împotriva executivilor de rang înalt care dețin putere administrativă.

### Q4: Ce este falsificarea e-mailului (email spoofing)?

Falsificarea e-mailului (email spoofing) este crearea unor mesaje de e-mail cu o adresă de expeditor falsificată, pentru a-l păcăli pe destinatar să aibă încredere în sursă.

### Q5: Cum previne SPF falsificarea?

Publică în DNS o listă de adrese IP autorizate să trimită e-mailuri, permițând serverelor receptoare să verifice sursa e-mailului. [1]

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

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

### Q6: Ce este DKIM?

DomainKeys Identified Mail adaugă o semnătură criptografică în antetele e-mailurilor, dovedind că un domeniu și-a asumat responsabilitatea și că mesajul nu a fost modificat.

### Q7: Ce înseamnă DMARC?

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

### Q8: Ce este o politică DMARC?

O politică ce le spune serverelor de e-mail cum să trateze mesajele care nu trec de SPF/DKIM (none, quarantine sau reject). [2]

### Q9: Ce este vishing-ul?

Phishing vocal, în care atacatorii folosesc apeluri telefonice frauduloase pentru a obține date administrative sau financiare.

### Q10: Cum ajută scanerele de link-uri?

Scanează și rescriu linkurile din e-mailurile primite pentru a verifica siguranța paginilor web de destinație în momentul clicului.

# 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 funcționează un atac homograf?

Atacatorii înregistrează nume de domenii folosind caractere Unicode non-ASCII asemănătoare, pentru a imita vizual un nume de domeniu legitim.

### Q2: Ce este o reprezentare punycode?

O codificare care convertește numele de domenii Unicode în șiruri compatibile ASCII care încep cu „xn--", astfel încât DNS să le poată gestiona.

### Q3: De ce este „p=reject" cea mai sigură stare DMARC?

Cere serverelor receptoare să respingă e-mailurile care nu trec de DMARC (SPF/DKIM aliniate) în timpul sesiunii SMTP, blocând falsificarea directă. [2]

### Q4: Cum ocolesc atacatorii regulile SPF?

Prin exploatarea domeniilor asemănătoare (typosquatting) sau prin folosirea conturilor compromise de pe servicii de e-mail terțe legitime.

### Q5: Ce este compromiterea e-mailului de business (BEC)?

O fraudă corporativă în care atacatorii preiau sau uzurpă conturi de e-mail ale companiilor pentru a autoriza plăți frauduloase.

# 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 oprește autentificarea multifactor phishing-ul?

Necesită token-uri secundare (precum chei hardware) care nu pot fi furate doar prin pagini de destinație asemănătoare.

### Q7: Ce este o pagină de destinație pentru colectarea acreditărilor?

Un portal de autentificare imitație, conceput să captureze în timp real numele de utilizator, parolele și token-urile MFA introduse.

### Q8: Ce este deturnarea subdomeniilor?

Un atacator care preia controlul unui pointer DNS de subdomeniu nefolosit pentru a găzdui pagini de destinație de phishing rău intenționate sub un domeniu părinte de încredere.

### Q9: Cum funcționează verificarea alinierii DKIM?

Verifică dacă domeniul din antetul „From” se potrivește cu domeniul care a semnat criptografic mesajul în antetul DKIM.

### Q10: Care este rolul unui gateway de e-mail?

Filtrarea e-mailurilor primite, auditarea linkurilor, rularea atașamentelor în sandbox și validarea conformității SPF/DKIM/DMARC.

# 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. [4]

**2. INFORMAȚII DESPRE SECURITATE**

Compromiterea e-mailului de afaceri (BEC) a cauzat în 2025 pierderi de peste 3 miliarde $, raportate către IC3 al FBI. [4]

**3. INFORMAȚII DESPRE SECURITATE**

Atacurile homograf folosesc litere chirilice asemănătoare vizual pentru a duplica domeniile de marcă cu potrivire exactă în browsere.

**4. INFORMAȚII DESPRE SECURITATE**

Cu p=reject, un domeniu cere destinatarilor să refuze e-mailurile care nu trec verificarea în timpul livrării, nu să le trimită în spam. [2]

**5. INFORMAȚII DESPRE SECURITATE**

Atacurile de tip whaling care vizează CEO-ii cer de obicei plăți urgente pentru fuziuni confidențiale sau achiziții de domenii.

**6. INFORMAȚII DESPRE SECURITATE**

Portalurile de colectare a credențialelor copiază pagini reale de autentificare, astfel încât victimele își introduc parolele direct în formularul atacatorului.

**7. PERSPECTIVĂ ASUPRA SECURITĂȚII**

Ghidul comun al CISA privind phishing-ul recomandă instruirea utilizatorilor, alături de DMARC, SPF, DKIM și MFA rezistent la phishing. [3]

**8. PERSPECTIVĂ ASUPRA SECURITĂȚII**

Evaluarea SPF este limitată la 10 termeni care interoghează DNS; depășirea limitei returnează rezultatul 'permerror'. [1]

**9. PERSPECTIVĂ ASUPRA SECURITĂȚII**

Cheile hardware de securitate FIDO2 oferă o protecție susținută criptografic împotriva colectării de la distanță a datelor de autentificare.

**10. INFORMAȚII DESPRE SECURITATE**

Phishing-ul este una dintre cele mai frecvente căi prin care atacatorii pătrund prima dată într-o organizație, motiv pentru care instruirea periodică de conștientizare este o apărare eficientă.

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

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

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

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

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

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

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

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

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

## Barem: Punct de control 1 – Alegere multiplă

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

**NOTĂ PENTRU PROFESOR**

Ce este spear phishing? → Un e-mail de phishing țintit, adaptat unei anumite persoane sau organizații

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

**NOTĂ PENTRU PROFESOR**

SPF publică în DNS gazdele de trimitere autorizate ale unui domeniu, astfel încât destinatarii să poată verifica expeditorul din plic.

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

**NOTĂ PENTRU PROFESOR**

Ce este un atac de tip whaling? → O campanie de phishing țintită special spre directori de companii cu profil înalt

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

**NOTĂ PENTRU PROFESOR**

Ce face DKIM? → Adaugă o semnătură criptografică la e-mailuri pentru a verifica autenticitatea expeditorului

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

**NOTĂ PENTRU PROFESOR**

Care este rolul DMARC? → Indicarea serverelor de e-mail destinatare cum să trateze verificările SPF/DKIM eșuate

## Barem: Punct de control 2 – Adevărat sau fals

### 6 Întrebarea 6

**Răspuns corect: Fals**

**NOTĂ PENTRU PROFESOR**

Fals: spear phishing-ul este adaptat unor persoane specifice, spre deosebire de phishing-ul generic în masă.

### 7 Întrebarea 7

**Răspuns corect: Adevărat**

**NOTĂ PENTRU PROFESOR**

Politicile DMARC pot instrui serverele de e-mail să respingă mesajele falsificate neautorizate.

### 8 Întrebarea 8

**Răspuns corect: Fals**

**NOTĂ PENTRU PROFESOR**

Fals: SPF verifică IP-ul de trimitere în raport cu DNS; DKIM este cel care verifică o semnătură criptografică.

### 9 Întrebarea 9

**Răspuns corect: Fals**

**NOTĂ PENTRU PROFESOR**

Fals: whaling vizează directori de rang înalt, care pot aproba plăți și pot accesa date sensibile.

### 10 Întrebarea 10

**Răspuns corect: Adevărat**

**NOTĂ PENTRU PROFESOR**

Adevărat: confirmarea cererilor de plată printr-un canal separat, cunoscut, ajută la oprirea fraudei prin transfer bancar.

# 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

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

## PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

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

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

| | | | |
|---|---|---|---|
| 1 B – SPOOFING | 2 A – SPEAR | 3 H – VISHING | 4 C – ÎNREGISTRARESPF |
| 5 G – PHISHING | 6 E – POLITICĂDMARC | 7 D – SEMNĂTURĂDKIM | 8 F – WHALING |

## NOTE DE DISCUȚIE PENTRU PROFESORI

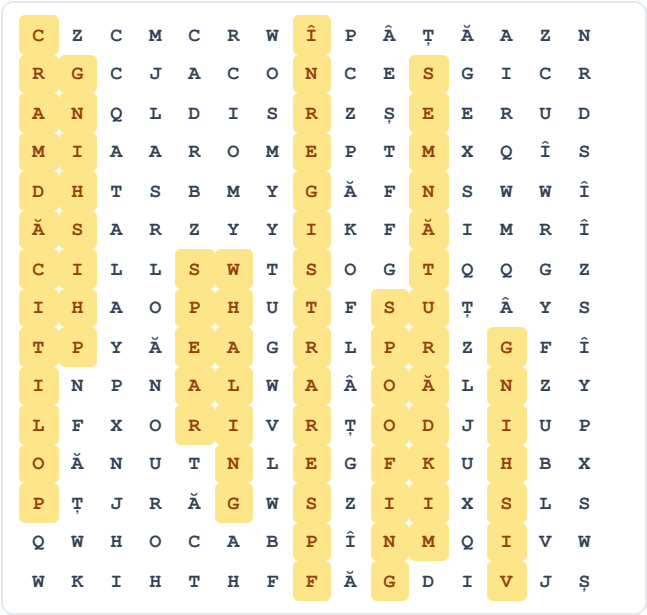
**Termeni-cheie:**
Verifică dacă elevii pot explica SPEAR, FALSIFICARE (SPOOFING) și SPF cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

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

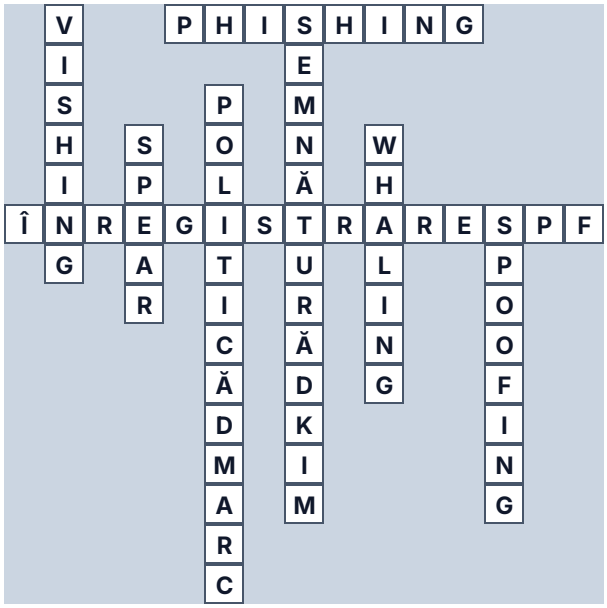
**Evaluarea surselor:**
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

# Chei de rezolvare ale puzzle-urilor și note pentru profesor

## SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE




## SOLUȚIA CUVINTELOR ÎNCRUCIȘATE




## GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

### ORIZONTAL

**2 orizontal: PHISHING** E-mail de inginerie socială. (8 litere)

**7 orizontal: ÎNREGISTRARESPF** Adrese IP autorizate pentru expediere, publicate în DNS. (15 litere)

### VERTICAL

**1 vertical: VISHING** Apeluri vocale de tip escrocherie. (7 litere)

**3 vertical: SEMNĂTURĂDKIM** Semnătură criptografică în e-mail. (13 litere)

**4 vertical: POLITICĂDMARC** Instrucțiuni de politică pentru respingere. (13 litere)

**5 vertical: SPEAR** E-mail personalizat și țintit. (5 litere)

**6 vertical: WHALING** Vizarea directorilor de nivel C. (7 litere)

**8 vertical: SPOOFING** Falsificarea adresei de e-mail a expeditorului. (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. AESRP — SPEAR
2. NIASRTSÎFPERERG — ÎNREGISTRARESPF
3. OPĂMDRCLCTIAI — POLITICĂDMARC
4. SNGIHPHI — PHISHING
5. FIPGOSNO — SPOOFING
6. ĂDUTKMIĂSERMN — SEMNĂTURĂDKIM
7. WNIGHLA — WHALING
8. IHGVNIS — VISHING

## BAREMUL PROVOCĂRII CU CODUL SECRET

**"DETECTEAZĂ INGINERIA SOCIALĂ PRIN AUDIT EMAIL"**

# Barem pentru studiile de caz

## A Studiu de caz 1: Remedierea unui atac de tip whaling împotriva conducerii de top

Soluția profesorului

### GHID DE NOTARE

**Răspunsurile elevilor ar trebui să acopere următoarele puncte:**

- Analiza scenariului: Directorul financiar (CFO) primește un e-mail foarte personalizat, care pretinde că provine de la CEO și cere un transfer rapid de 50.000 de dolari pentru a încheia o achiziție confidențială de domeniu.
- Strategie și soluție recomandate: Configurează DMARC cu politica 'p=reject' pentru a bloca domeniile expeditorilor falsificate. Adaugă bannere de avertizare pentru expeditori externi la gateway și cere confirmare verbală, out-of-band, pentru toate tranzacțiile financiare.

## B Studiu de caz 2: Implementarea politicilor gateway SPF/DKIM/DMARC

Soluția profesorului

### GHID DE NOTARE

**Răspunsurile elevilor ar trebui să acopere următoarele puncte:**

- Analiza scenariului: O companie nu trece auditurile de securitate deoarece e-mailurile de marketing trimise sunt marcate frecvent ca spam, iar hackerii falsifică activ domeniul de brand al companiei.
- Strategie și soluție recomandată: Publică o înregistrare TXT pentru SPF care enumeră IP-urile expeditorilor autorizați. Configurează cheile de semnare DKIM pe serverele de e-mail de ieșire și analizează rapoartele XML de feedback DMARC primite pentru a identifica abuzurile.