Emri: _____ Data: _____ Pikët: _____

Sulmet phishing dhe inxhinieria sociale

Spear phishing, mashtrimet whaling, protokollet SPF/DKIM/DMARC, falsifikimi i dërguesit dhe trajnimi i sigurisë për punonjësit.

PËRMBLEDHJE MËSIMORE PËR SULMET PHISHING

I SIGURUAR
ENKRIPTIMI I TË DHËNAVE
Standardi AES 256-bit

I PËRPUTHSHËM
STANDARDET GLOBALE
Kornizat GDPR dhe CCPA

ZERO-TRUST
POLITIKA E QASJES
Autentikim me shumë faktorë

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes sulmeve phishing dhe inxhinierisë sociale. Do të eksplorosh spear phishing-un, whaling-un, falsifikimin e domeneve, protokollet SPF/DKIM/DMARC, sigurinë e lidhjeve dhe trajnimin për ndërgjegjësim të punonjësve.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro sigurinë kibernetike dhe parandalimin e kërcënimeve.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për sigurinë kibernetike

URL: https://www.vpn.com/sq/siguria-kibernetike/sulmet-e-phishing/

Udhërrëfyesi yt mësimor për zbutjen e phishing-ut

- Identifiko mashtrimet e zakonshme phishing, vishing dhe pop-up-et e mbështetjes teknike.
- Zbato procedura verifikimi të transaksioneve jashtë kanalit (out-of-band).
- Konfiguro rregullat SPF, DKIM dhe DMARC për të bllokuar domenet e falsifikuara.

UDHËZIME PËR UDHËZUESIN E SULMEVE PHISHING

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për vërtetimin e emailit. Përfundo me aktivitetin bonus Mendo shpejt.

SULMET PHISHING DHE INXHINIERIA SOCIALE (HYRJE)

Sulmet phishing përdorin mesazhe të synuara, mashtrime whaling dhe falsifikim domenesh për të mbledhur kredencialet e hyrjes së përdoruesve. Sigurimi i sistemeve korporative kërkon vendosjen e rregullave SPF, DKIM dhe DMARC në portë, së bashku me hapa miratimi nëpërmjet një kanali të veçantë.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E SAKTË.

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1 **1. Çfarë është spear phishing?**

- A. Një email phishing i synuar, i përshtatur për një individ ose organizatë të caktuar
- B. Një email masiv i gjerë i dërguar te miliona adresa të rastësishme
- C. Një sulm rrjeti që vërshon serverët e uebit me trafik
- D. Një teknikë nxjerrjeje nga baza e të dhënave që synon regjistrimet e përdoruesve

2 **2. Cili protokoll i lejon një domeni të listojë në DNS adresat IP të autorizuara për dërgim, për të luftuar falsifikimin?**

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

3 **3. Çfarë është një sulm whaling?**

- A. Një fushatë phishing e synuar posaçërisht ndaj drejtuesve korporativë të profilit të lartë
- B. Një sulm SQL injection që synon kopjet rezervë të bazës së të dhënave
- C. Një vjedhje fizike e pajisjeve të router-ave të rrjetit lokal
- D. Një skanim i automatizuar brute-force me credential stuffing

4 **4. Çfarë bën DKIM?**

- A. Shton një nënshkrim kriptografik në emailet për të verifikuar autenticitetin e dërguesit
- B. Bllokon në firewall trafikun hyrës të paketave të rrjetit
- C. Enkripton vëllimet e ruajtjes së bazës së të dhënave në pushim
- D. Skanon bashkëngjitjet e email-it për malware të bazuar në nënshkrime

5 **5. Cili është roli i DMARC?**

- A. Udhëzimi i serverëve marrës të emailit se si t'i trajtojnë kontrollet e dështuara SPF/DKIM
- B. Deshifrimi i fjalëkalimeve të sistemit duke përdorur rainbow tables të llogaritura paraprakisht
- C. Kompresimi i bashkëngjitjeve të emailit përpara dorëzimit
- D. Konfigurimi i privilegjeve të qasjes në rutim të rrjetit

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetja 6

6. Spear phishing mbështetet te email-e masive gjenerike të dërguara miliona adresave të rastësishme.

- ○ E vërtetë
- ○ E gabuar

7 Pyetja 7

7. Politikat e DMARC mund t'u japin serverëve të postës udhëzim të refuzojnë mesazhet e falsifikuara të paautorizuara.

- ○ E vërtetë
- ○ E gabuar

8 Pyetja 8

8. Verifikimi SPF funksionon duke validuar nënshkrimin kriptografik të trupit të email-it.

- ○ E vërtetë
- ○ E gabuar

9 Pyetja 9

9. Sulmet whaling synojnë administratorët e nivelit të ulët në kompani për të aksesuar skedarët e bazave të të dhënave.

- ○ E vërtetë
- ○ E gabuar

10 Pyetja 10

10. Verifikimi jashtë kanalit (out-of-band) i kërkesave për pagesë ndihmon të ndalohen mashtrimet me transferta financiare.

- ○ E vërtetë
- ○ E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. **Synimi i një punonjësi të caktuar me informacion të personalizuar është phishing** _____ .

2. **Ndryshimi i kokës së emailit që mesazhet të duken legjitime quhet** _____ **i dërguesit.**

3. **Lista e regjistrimeve DNS të IP-ve të autorizuara të serverëve të postës është** _____ .

4. **Standardi i nënshkrimit të emailit që ofron verifikim të dërguesit është** _____ .

5. **Vendosja e politikave për refuzimin e kontrolleve të dështuara SPF/DKIM përdor** _____ .

6. **Një fushatë phishing që synon drejtuesit e nivelit C quhet** _____ .

BANKA E FJALËVE TË LEKSIKUT

DMARC FALSIFIKIM FIREWALL NËNSHKRIM DKIM RANSOMWARE REKORD SPF SPEAR WHALING

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

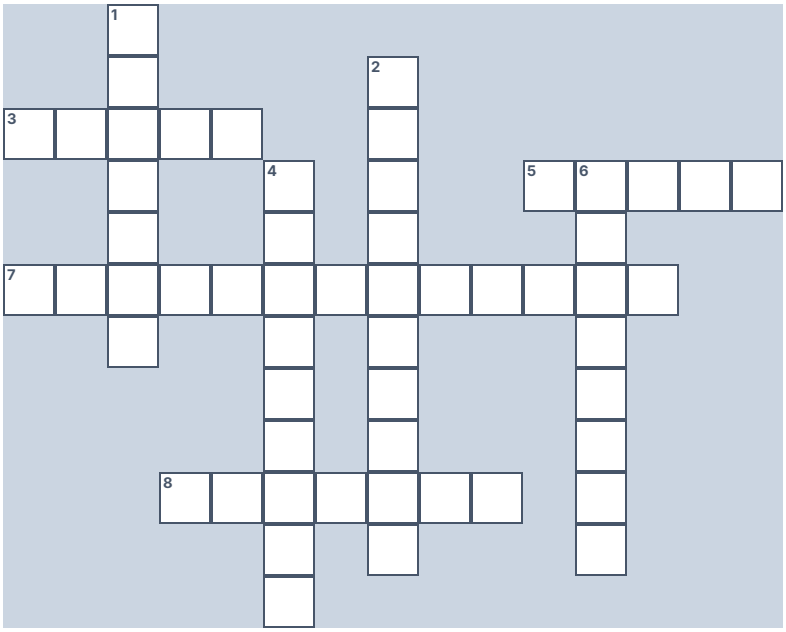
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. SPEAR	A	Telefonata mashtruese me zë.
☐	2. FALSIFIKIM	B	Shënjestro drejtuesit e nivelit C.
☐	3. SPF	C	Udhëzime refuzimi të politikës.
☐	4. DKIM	D	IP-të e dërguesve të autorizuar nga DNS.
☐	5. DMARC	E	Email i inxhinierisë sociale.
☐	6. WHALING	F	Email i synuar i personalizuar.
☐	7. PHISHING	G	Falsifikimi i adresës së email-it të dërguesit.
☐	8. VISHING	H	Nënshkrim kriptografik në email.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

3. Udhëzime politike për refuzim. (5)

5. Email i synuar i personalizuar. (5)

7. Nënshkrim kriptografik në email. (13)

8. Telefonata mashtruese me zë. (7)

VERTIKALISHT

1. Synimi i drejtuesve të nivelit C. (7)

2. Falsifikimi i adresës së emailit të dërguesit. (10)

4. IP-të e autorizuara të dërguesve në DNS. (9)

6. Email i inxhinierisë sociale. (8)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë.

HORIZONTALISHT

3 horizontalisht: Udhëzime politike për refuzim. (5 shkronja):

5 horizontalisht: Email i synuar i personalizuar. (5 shkronja):

7 horizontalisht: Nënshkrim kriptografik në email. (13 shkronja):

8 horizontalisht: Telefonata mashtruese me zë. (7 shkronja):

VERTIKALISHT

1 vertikalisht: Synimi i drejtuesve të nivelit C. (7 shkronja):

2 vertikalisht: Falsifikimi i adresës së emailit të dërguesit. (10 shkronja):

4 vertikalisht: IP-të e autorizuara të dërguesve në DNS. (9 shkronja):

6 vertikalisht: Email i inxhinierisë sociale. (8 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

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

LISTA E FJALËVE TË LEKSIKUT

SPEAR FALSIFIKIM REKORDSPF NËNSHKRIMDKIM DMARC WHALING PHISHING VISHING

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

- **A. SPEAR**
- **B. FALSIFIKIM**
- **C. REKORDSPF**
- **D. NËNSHKRIMDKIM**
- **E. DMARC**
- **F. WHALING**
- **G. PHISHING**
- **H. VISHING**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Falsifikimi i adresës së emailit të dërguesit.
2. Email i synuar i personalizuar.
3. Telefonata mashtruese me zë.
4. IP-të e autorizuara të dërguesve në DNS.
5. Email i inxhinierisë sociale.
6. Udhëzime politike për refuzim.
7. Nënshkrim kriptografik në email.
8. Synimi i drejtuesve të nivelit C.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të sigurisë kibernetike. Shkruaji përgjigjet në kutitë e dhëna.

1. **AESRP** _____
2. **FRPOEDSRK** _____
3. **ADCRM** _____
4. **SNGIHPHI** _____
5. **KFMASIIFIL** _____
6. **HDRKKNIMNË IMS** _____
7. **WNIGHLA** _____
8. **IHGVNIS** _____

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Pajisje që mund të hakohen			
2	Shenja të një emaili phishing			
3	Shenja që një kompjuter është i infektuar			
4	Fjalë që krijojnë urgjencë të rreme			
5	Mënyra për të verifikuar një dërgues			
6	Njerëz që mund t'i pyesësh për ndihmë me IT-në			
7	Gjëra që ruan si kopje rezervë			
8	Peshq ose krijesa deti që njeh			
9	Kompani që hiqen si mashtruesit			
10	Zakone të sigurta që mund t'i fillosh sot			
11	Gjëra që bëhen pasi ke klikuar një lidhje të rreme			
12	Gjëra që bëhen pas një rrjedhjeje të dhënash			
13	Kanale ku ndodh phishing-u			
14	Gjëra që nuk i dërgon kurrë me email			
15	Mënyra për të mbrojtur llogaritë e tua			

Pika e kontrollit 8: Studime rasti për sigurinë kibernetike

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

STUDIMI I RASTIT 1: RIPARIMI I SULMIT WHALING NDAJ DREJTUESVE C-SUITE

👷

Skenari: Një Drejtor Financiar merr një email shumë të personalizuar që pretendon se vjen nga CEO-ja, duke kërkuar një transfertë të shpejtë prej 50,000 dollarësh për të mbyllur një blerje konfidenciale domeni.

Pyetje për diskutim: Analizo rreziqet e falsifikimit të markës dhe përshkruaj në detaje SPF/DKIM/DMARC dhe kontrollet e autentikimit.

STUDIMI I RASTIT 2: VENDOSJA E POLITIKAVE GATEWAY SPF/DKIM/DMARC

👷

Skenari: Një ndërmarrje po dështon në auditimet e sigurisë sepse emailet dalëse të marketingut shënohen shpesh si spam dhe hakerët po falsifikojnë në mënyrë aktive domenin e markës së kompanisë.

Pyetje për diskutim: Krijo kontrolle teknike dhe administrative për të verifikuar autenticitetin e emailit.

Pika e kontrollit 9: Deshifrimi i kodit

Një profesionist i sigurisë kibernetike mbron asetet e rrjetit nga aktorët e kërcënimeve online. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

27	2	23	14	17		15	1	16	11	18	23	14	11	15	11	16

21	17	3	11	1	14	15	6	1	23	5	11	22	11	15

6	15	1	11	14	11

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa A)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q1: Çfarë është phishing-u?

Phishing-u është një sulm i inxhinierisë sociale ku kriminelët dërgojnë mesazhe mashtruese për t'i mashtruar përdoruesit që të ndajnë të dhëna të ndjeshme.

Q2: Cili është ndryshimi midis phishing-ut dhe spear phishing?

Phishing-u synon grupe të gjera me përmbajtje të përgjithshme, ndërsa spear phishing synon viktima specifike duke përdorur detaje të personalizuara.

Q3: Çfarë është whaling?

Whaling është një sulm phishing shumë i synuar ndaj drejtuesve me profil të lartë që kanë pushtet administrativ.

Q4: Çfarë është email spoofing?

Falsifikimi i email-it është krijimi i mesazheve email me adresë dërguesi të falsifikuar për ta mashtruar marrësin që t'i besojë burimit.

Q5: Si e parandalon SPF falsifikimin (spoofing)?

Publikon në DNS një listë të adresave IP të autorizuara për dërgim, duke u lejuar serverëve marrës të verifikojnë burimin e postës. [1]

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa B)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q6: Çfarë është DKIM?

DomainKeys Identified Mail shton një nënshkrim kriptografik në kokat e email-it, duke provuar që një domen mori përgjegjësinë dhe që mesazhi nuk u ndryshua.

Q7: Çfarë do të thotë DMARC?

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

Q8: Çfarë është një politikë DMARC?

Një politikë që u tregon serverëve të postës si t'i trajtojnë mesazhet që dështojnë në SPF/DKIM (asnjë, karantinë ose refuzim). [2]

Q9: Çfarë është vishing?

Phishing me zë, ku sulmuesit përdorin telefonata mashtruese për të nxjerrë të dhëna administrative ose financiare.

Q10: Si ndihmojnë skanerët e lidhjeve?

Skanojnë dhe ripërshkruajnë lidhjet e emaileve hyrës për të verifikuar sigurinë e faqeve të uebit të destinacionit në çastin e klikimit.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa C)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q1: Si funksionon një sulm homograf?

Sulmuesit regjistrojnë emra domenesh me karaktere Unicode jo-ASCII që duken njësoj, për të imituar vizualisht një emër domeni të ligjshëm.

Q2: Çfarë është një paraqitje punycode?

Një kodim që i shndërron emrat e domeneve Unicode në vargje të përputhshme me ASCII që fillojnë me 'xn--' që DNS t'i trajtojë.

Q3: Pse është 'p=reject' gjendja DMARC më e sigurt?

U kërkon serverëve marrës të refuzojnë postën që dështon në DMARC (SPF/DKIM të përafruar) gjatë seancës SMTP, duke bllokuar falsifikimin e drejtpërdrejtë. [2]

Q4: Si i anashkalojnë sulmuesit rregullat SPF?

Duke shfrytëzuar domene të ngjashme (typosquatting) ose duke përdorur llogari të kompromentuara në shërbime emaili të ligjshme të palëve të treta.

Q5: Çfarë është kompromentimi i email-it të biznesit (BEC)?

Një mashtrim korporativ ku sulmuesit rrëmbejnë ose imitojnë llogaritë e emailit të biznesit për të autorizuar pagesa mashtruese.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa D)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q6: Si e ndalon vërtetimi shumëfaktorësh phishing-un?

Kërkon token dytësorë (si çelësa hardueri) që nuk mund të vidhen vetëm përmes faqeve të rreme të uljes.

Q7: Çfarë është një faqe zbarkimi për mbledhjen e kredencialeve?

Një portal hyrjeje i ngjashëm me origjinalin, i dizajnuar për të kapur emrat e përdoruesve, fjalëkalimet dhe token-ët MFA të futur në kohë reale.

Q8: Çfarë është rrëmbimi i nëndomenit?

Një sulmues që merr kontrollin e një treguesi të papërdorur të nëndomenit DNS për të strehuar faqe hyrëse phishing keqdashëse nën një domen prind të besuar.

Q9: Si funksionon kontrolli i përafrimit DKIM?

Verifikon që domeni në titullin 'From' përputhet me domenin që e ka nënshkruar kriptografikisht mesazhin në titullin DKIM.

Q10: Cili është roli i një gateway-i të email-it?

Filtrimi i email-eve hyrëse, auditimi i lidhjeve, vendosja e bashkëngjitjeve në sandbox dhe validimi i pajtueshmërisë me SPF/DKIM/DMARC.

Pjesa 11: 10 fakte dhe njohuri nga bota reale për sigurinë kibernetike

Rishiko fakte reale për shkeljet e sigurisë, mekanizmat e mbrojtjes dhe standardet e pajtueshmërisë.

1. PERSPEKTIVË PËR SIGURINË

Phishing-u dhe falsifikimi (spoofing) ishin lloji i krimit më i raportuar te IC3 i FBI-së në vitin 2025, me 191,561 ankesa. [4]

2. PERSPEKTIVË PËR SIGURINË

Kompromentimi i emailit të biznesit (BEC) shkaktoi mbi $3 miliardë humbje të raportuara te IC3 i FBI-së në 2025. [4]

3. PERSPEKTIVË PËR SIGURINË

Sulmet homografike përdorin shkronja cirilike të ngjashme për të dyfishuar vizualisht domenet e markave me përputhje të saktë në shfletues.

4. PERSPEKTIVË PËR SIGURINË

Me 'p=reject', një domen u kërkon marrësve të refuzojnë postën që dështon gjatë dorëzimit, jo ta arkivojnë si spam. [2]

5. PERSPEKTIVË PËR SIGURINË

Sulmet whaling që synojnë CEO-të zakonisht kërkojnë pagesa urgjente për bashkime konfidenciale ose blerje domenesh.

6. PERSPEKTIVË PËR SIGURINË

Portalet e mbledhjes së kredencialeve kopjojnë faqet reale të hyrjes, që viktimat t'i shkruajnë fjalëkalimet drejtpërdrejt në formularin e sulmuesit.

7. NJOHURI PËR SIGURINË

Udhëzimet e përbashkëta të CISA-s për phishing-un rekomandojnë trajnimin e përdoruesve krahas DMARC, SPF, DKIM dhe MFA-së rezistente ndaj phishing-ut. [3]

8. NJOHURI PËR SIGURINË

Vlerësimi i SPF kufizohet në 10 terma që bëjnë pyetje DNS; tejkalimi i kufirit kthen rezultatin 'permerror'. [1]

9. NJOHURI PËR SIGURINË

Çelësat harduerikë të sigurisë FIDO2 ofrojnë mbrojtje të mbështetur kriptografikisht ndaj mbledhjes në distancë të kredencialeve.

10. PERSPEKTIVË PËR SIGURINË

Phishing-u është një nga mënyrat më të zakonshme se si sulmuesit hyjnë fillimisht në një organizatë, prandaj trajnimi i rregullt i ndërgjegjësimit është një mbrojtje efektive.

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet globale të NIST, OWASP dhe të pajtueshmërisë me privatësinë e të dhënave.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[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

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Pyetja 1** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë është spear phishing? → Një email phishing i synuar, i përshtatur për një individ ose organizatë të caktuar

2 **Pyetja 2** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

SPF publikon në DNS hostet e autorizuara të dërgimit të një domeni, që marrësit të mund ta kontrollojnë dërguesin e zarfit.

3 **Pyetja 3** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë është një sulm whaling? → Një fushatë phishing e synuar posaçërisht ndaj drejtuesve korporativë të profilit të lartë

4 **Pyetja 4** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë bën DKIM? → Shton një nënshkrim kriptografik në emailet për të verifikuar autenticitetin e dërguesit

5 **Pyetja 5** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cili është roli i DMARC? → Udhëzimi i serverëve marrës të emailit se si t'i trajtojnë kontrollet e dështuara SPF/DKIM

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Pyetja 6** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: spear phishing është i përshtatur për persona specifikë, ndryshe nga phishing-u i përgjithshëm masiv.

7 **Pyetja 7** **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Politikat e DMARC mund t'u japin serverëve të postës udhëzim të refuzojnë mesazhet e falsifikuara të paautorizuara.

8 **Pyetja 8** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: SPF e kontrollon IP-në dërguese me DNS; DKIM është ai që verifikon një nënshkrim kriptografik.

9 **Pyetja 9** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: whaling synon ekzekutivët e lartë, të cilët mund të miratojnë pagesa dhe të hyjnë te të dhëna të ndjeshme.

10 **Pyetja 10** **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

E vërtetë: konfirmimi i kërkesave për pagesë përmes një kanali të veçantë e të njohur ndihmon të ndalohet mashtrimi me transferta.

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

F 1. SPEAR	G 2. FALSIFIKIM	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING	E 7. PHISHING	A 8. VISHING

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 SPEAR	2 FALSIFIKIM	3 REKORD SPF	4 NËNSHKRIM DKIM
5 DMARC	6 WHALING		

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

1 B – FALSIFIKIM	2 A – SPEAR	3 H – VISHING	4 C – REKORDSPF
5 G – PHISHING	6 E – DMARC	7 D – NËNSHKRIMDKIM	8 F – WHALING

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë SPEAR, FALSIFIKIM dhe SPF me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

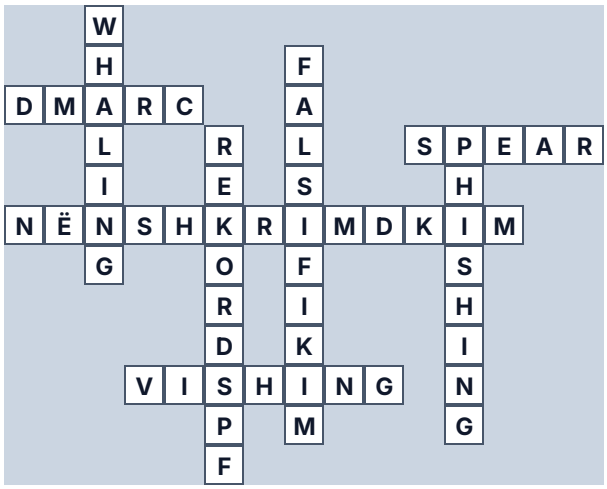
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

3 horizontalisht: DMARC Udhëzime politike për refuzim. (5 shkronja)

5 horizontalisht: SPEAR Email i synuar i personalizuar. (5 shkronja)

7 horizontalisht: NËNSHKRIMDKIM Nënshkrim kriptografik në email. (13 shkronja)

8 horizontalisht: VISHING Telefonata mashtruese me zë. (7 shkronja)

VERTIKALISHT

1 vertikalisht: WHALING Synimi i drejtuesve të nivelit C. (7 shkronja)

2 vertikalisht: FALSIFIKIM Falsifikimi i adresës së emailit të dërguesit. (10 shkronja)

4 vertikalisht: REKORDSPF IP-të e autorizuara të dërguesve në DNS. (9 shkronja)

6 vertikalisht: PHISHING Email i inxhinierisë sociale. (8 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1. AESRP — **SPEAR**
2. FRPOEDSRK — **REKORDSPF**
3. ADCRM — **DMARC**
4. SNGIHPHI — **PHISHING**
5. KFMASIIFIL — **FALSIFIKIM**
6. HDRKKNIMNËIMS — **NËNSHKRIMDKIM**
7. WNIGHLA — **WHALING**
8. IHGVNIS — **VISHING**

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"ZBULO MANIPULIMIN SOCIAL ME AUDITIM EMAILI"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Riparimi i sulmit whaling ndaj drejtuesve C-suite

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një Drejtor Financiar merr një email shumë të personalizuar që pretendon të jetë nga CEO-ja, duke kërkuar një transfertë të shpejtë prej $50,000 për të mbyllur një blerje konfidenciale domeni.
- Strategjia dhe zgjidhja e rekomanduar: Konfiguro DMARC me politikën 'p=reject' për të bllokuar domenet e falsifikuara të dërguesit. Shto banera paralajmërues për dërgues të jashtëm në portë (gateway) dhe kërko konfirmim verbal, jashtë kanalit, për të gjitha transaksionet financiare.

B Studimi i rastit 2: Vendosja e politikave gateway SPF/DKIM/DMARC

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një ndërmarrje po dështon në auditimet e sigurisë sepse email-et dalëse të marketingut shënohen shpesh si spam dhe hakerët po falsifikojnë në mënyrë aktive domenin e markës së kompanisë.
- Strategjia dhe zgjidhja e rekomanduar: Publiko një rekord TXT për SPF që tregon IP-të e autorizuara të dërguesve. Konfiguro çelësat e nënshkrimit DKIM në serverët e postës dalëse dhe analizo raportet XML të reagimit DMARC që vijnë, për të identifikuar abuzimin.