Emri: _____ Data: _____ Pikët: _____

Mashtrimet në internet dhe inxhinieria sociale
Udhëzues mbrojtjeje

Phishing me email, domene të falsifikuara, vishing, mashtrime të mbështetjes, verifikim jashtë kanalit, BEC

PËRMBLEDHJE MËSIMORE PËR MASHTRIMET NË INTERNET

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 mbrojtjes nga mashtrimet në internet. Do të eksplorosh faqet e rreme të phishing-ut, taktikat e inxhinierisë sociale, mashtrimet e mbështetjes, vektorët e mashtrimit me transfertë bankare dhe metodat e verifikimit të pagesës.

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/mashtrime-online/

Udhërrëfyesi yt mësimor për mbrojtjen nga mashtrimet në internet

- Identifiko treguesit e zakonshëm të mashtrimeve të mbështetjes teknike dhe të domeneve typosquatting.
- Zbato protokolle verifikimi të email-it (SPF, DKIM, DMARC) kundër falsifikimit.
- Vendos verifikimin e transaksioneve jashtë kanalit për të parandaluar mashtrimin biznesor me transfertat bankare.

UDHËZIME PËR UDHËZUESIN E MASHTRIMEVE NË INTERNET

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 mbrojtjen nga mashtrimet në internet. Përfundo me aktivitetin bonus Mendo shpejt.

MBROJTJA NGA MASHTRIMET NË INTERNET DHE INXHINIERIA SOCIALE (HYRJE)

Mashtrimet në internet shfrytëzojnë sjelljen njerëzore përmes phishing-ut, dritareve kërcyese të mbështetjes, vishing-ut dhe mashtrimit me transfertë bankare. Verifikimi i transaksioneve nëpërmjet një kanali të veçantë dhe rregullat e domenit SPF/DKIM/DMARC ndihmojnë të bllokohen vektorët e inxhinierisë sociale në portë.

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Cili është treguesi kryesor i një mashtrimi me mbështetje teknike?

- A. Një dritare pop-up që pretendon se sistemi yt është i infektuar dhe të kërkon të thërrasësh një numër telefoni
- B. Një përditësim automatik sigurie i shkarkuar nga një regjistër zyrtar
- C. Një menaxher fjalëkalimesh që refuzon të plotësojë kredencialet në një domen korporativ
- D. Një kopje rezervë skedarësh në sfond që ekzekutohet në një konfigurim disku të jashtëm

2. Cila teknikë përdor domene dërguesish të falsifikuar për të vjedhur të dhëna bankare?

- A. Phishing me email
- B. Skanimi i porteve
- C. Injektimi në memorie
- D. Shkatërrimi kriptografik

3. Çfarë përfaqëson mashtrimi me transfertë bankare?

- A. Mashtrimi i viktimave që të dërgojnë para në llogari të rreme korporative duke përdorur inxhinierinë sociale
- B. Enkriptimi i bazave të të dhënave të sistemit duke përdorur ngarkesa ransomware
- C. Kërkimi i bazave të të dhënave përmes komandave SQL injection
- D. Kopjimi rezervë i skedarëve të sistemit në disqe ruajtjeje jashtë linje

4. Pse krijojnë mashtruesit faqe web të rreme blerjesh?

- A. Për të vjedhur të dhënat e kartës së kreditit dhe kredencialet e pagesës nga blerësit
- B. Për të mbajtur tabela të bazës së të dhënave të analizës së malware-it në sandbox
- C. Për të përshpejtuar dorëzimin e porosive online
- D. Për të testuar falas dizajne të reja faqesh

5. Çfarë do të thotë vishing?

- A. Mashtrime phishing me zë përmes rrjeteve telefonike për të vjedhur kredencialet
- B. Skanimi i rrjeteve lokale për pajisje sistemi të pasigurta
- C. Rikthimi i bazave të të dhënave të sistemit pas një shkeljeje të paautorizuar
- D. Ekzekutimi i kodit të pabesueshëm brenda kontejnerëve virtualë të sigurt

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

6 Pyetja 6

6. Mashtrimet phishing synojnë vetëm përdoruesit fundorë, kurrë objektivat ekzekutivë të whaling.

○ E vërtetë ○ E gabuar

7 Pyetja 7

7. Domenet e falsifikuara shpesh përdorin gabime të vogla shkrimi (si amaz0n.com) për të imituar marka të besuara.

○ E vërtetë ○ E gabuar

8 Pyetja 8

8. Mashtrimet e mbështetjes mund të zgjidhen duke i dhënë telefonuesit qasje në distancë.

○ E vërtetë ○ E gabuar

9 Pyetja 9

9. Inxhinieria sociale shfrytëzon psikologjinë njerëzore si frika dhe urgjenca për të anashkaluar rregullat e sigurisë.

○ E vërtetë ○ E gabuar

10 Pyetja 10

10. Kërkesat për transferta bankare duhet të verifikohen gjithmonë përmes kanaleve komunikimi jashtë brezit (out-of-band).

○ 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. Emailet mashtruese që mashtrojnë përdoruesit quhen _____ .
2. Adresat e uebit që imitojnë marka të besuara janë të tipit _____ .
3. Mashtrimet me zë që synojnë të dhënat bankare quhen _____ .
4. Një dritare pop-up që kërkon para për heqjen e virusit është një _____ mbështetjeje.
5. Konfirmimi i një kërkese për pagesë kërkon _____ jashtë kanalit.
6. Ridrejtimi i transaksioneve të biznesit te llogaritë e hajdutëve është mashtrim me _____ bankar.

BANKA E FJALËVE TË LEKSIKUT

FIREWALL IMITUAR MASHTRIM PHISHING RANSOMWARE TRANSFERIM VERIFIKIM VISHING

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

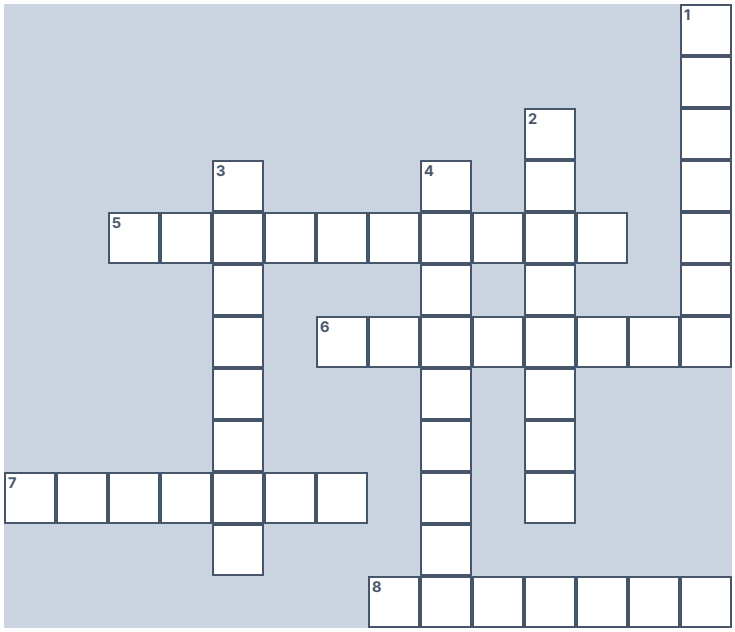
PËRPUTHJA E PËRKUFIZIMEVE

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. PHISHING	A	Ridrejtimi mashtrues i transaksioneve bankare drejt llogarive kriminale.
☐	2. I FALSIFIKUAR	B	Skemë mashtruese e krijuar për të vjedhur para ose kredenciale qasjeje nga viktimat.
☐	3. VISHING	C	Dërgimi i mesazheve tekst mashtruese për të vjedhur kredencialet e llogarisë celulare.
☐	4. MASHTRIM	D	Telefonata mashtruese me zë të krijuara për të vjedhur kredencialet dhe të dhënat e llogarisë.
☐	5. VERIFIKIM	E	Sulme phishing të synuara që synojnë të vjedhin kredenciale nga drejtuesit e nivelit C.
☐	6. TRANSFERTË BANKARE	F	Adresë e imituar e dërguesit të email-it ose e faqes së internetit, e projektuar të duket legjitime.
☐	7. WHALING	G	Fushata mashtruese me email të krijuara për të vjedhur kredencialet e hyrjes dhe fjalëkalimet.
☐	8. SMISHING	H	Konfirmimi i detajeve të pagesës përmes një metode kontakti dytësore të besuar.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

5. Ridrejtim mashtrues i transaksioneve bankare drejt llogarive kriminale. (10)

6. Fushata mashtruese me email të projektuara për të vjedhur kredencialet e hyrjes dhe fjalëkalimet. (8)

7. Sulme phishing të synuara që kërkojnë të vjedhin kredenciale nga drejtuesit e nivelit C. (7)

8. Adresë e imituar e dërguesit të emailit ose e faqes së uebit, e projektuar të duket legjitime. (7)

VERTIKALISHT

1. Telefonata mashtruese me zë të projektuara për të vjedhur kredencialet dhe detajet e llogarisë. (7)

2. Dërgimi i mesazheve tekst mashtruese për të vjedhur kredencialet e llogarisë celulare. (8)

3. Skemë mashtruese e projektuar për të vjedhur para ose qasje në kredenciale nga viktimat. (8)

4. Konfirmimi i detajeve të pagesës përmes një metode kontakti dytësore të besueshme. (9)

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

5 horizontalisht: Ridrejtim mashtrues i transaksioneve bankare drejt llogarive kriminale. (10 shkronja):

6 horizontalisht: Fushata mashtruese me email të projektuara për të vjedhur kredencialet e hyrjes dhe fjalëkalimet. (8 shkronja):

7 horizontalisht: Sulme phishing të synuara që kërkojnë të vjedhin kredenciale nga drejtuesit e nivelit C. (7 shkronja):

8 horizontalisht: Adresë e imituar e dërguesit të emailit ose e faqes së uebit, e projektuar të duket legjitime. (7 shkronja):

VERTIKALISHT

1 vertikalisht: Telefonata mashtruese me zë të projektuara për të vjedhur kredencialet dhe detajet e llogarisë. (7 shkronja):

2 vertikalisht: Dërgimi i mesazheve tekst mashtruese për të vjedhur kredencialet e llogarisë celulare. (8 shkronja):

3 vertikalisht: Skemë mashtruese e projektuar për të vjedhur para ose qasje në kredenciale nga viktimat. (8 shkronja):

4 vertikalisht: Konfirmimi i detajeve të pagesës përmes një metode kontakti dytësore të besueshme. (9 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.

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

LISTA E FJALËVE TË LEKSIKUT

PHISHING IMITUAR VISHING MASHTRIM VERIFIKIM TRANSFERIM
WHALING SMISHING

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. PHISHING

B. IMITUAR

C. VISHING

D. MASHTRIM

E. VERIFIKIM

F. TRANSFERIM

G. WHALING

H. SMISHING

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Adresë e imituar e dërguesit të emailit ose e faqes së uebit, e projektuar të duket legjitime.

2. Konfirmimi i detajeve të pagesës përmes një metode kontakti dytësore të besueshme.

3. Ridrejtim mashtrues i transaksioneve bankare drejt llogarive kriminale.

4. Dërgimi i mesazheve tekst mashtruese për të vjedhur kredencialet e llogarisë celulare.

5. Sulme phishing të synuara që kërkojnë të vjedhin kredenciale nga drejtuesit e nivelit C.

6. Telefonata mashtruese me zë të projektuara për të vjedhur kredencialet dhe detajet e llogarisë.

7. Fushata mashtruese me email të projektuara për të vjedhur kredencialet e hyrjes dhe fjalëkalimet.

8. Skemë mashtruese e projektuar për të vjedhur para ose qasje në kredenciale nga viktimat.

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. **NSHPIHGI** _____
2. **VSGNIHI** _____
3. **VIFEKMIIR** _____
4. **GHILNWA** _____
5. **URTIIAM** _____
6. **IMHRMTAS** _____
7. **RNTEFRIMSA** _____
8. **SMHGSNII** _____

Aktivitet bonus: Mendo shpejt

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

1	Pajisje që mund të hakohen			
2	Fraza që përdorin shpesh mashtruesit			
3	Mënyra pagese që kërkojnë mashtruesit			
4	Lloje mashtrimesh online			
5	Oferta që janë shumë të mira për të qenë të vërteta			
6	Vende ku mund të raportosh një mashtrim			
7	Fjalë që lidhen me sigurinë kibernetike			
8	Njerëz që mund t'i paralajmërosh për mashtrimet			
9	Gjëra që ruan si kopje rezervë			
10	Shenja paralajmëruese në një email			
11	Shenja që një kompjuter është i infektuar			
12	Mënyra për të verifikuar një dyqan online			
13	Mënyra për të mbrojtur llogaritë e tua			
14	Gjëra që bëhen nëse të mashtrojnë			
15	Gjëra që bëhen pas një rrjedhjeje të dhënash			

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: PARANDALIMI I MASHTRIMIT ME TRANSFERTË BANKARE TË KORPORATËS

👷

Skenari: Një departament financiar merr një email urgjent nga një adresë e falsifikuar furnitori, që kërkon që transferimet e ardhshme të faturave të drejtohen në një numër të ri drejtimi.

Pyetje për diskutim: Përshkruaj politikën e verifikimit të mashtrimit me transferta dhe specifiko bllokimet e autentikimit të emailit.

STUDIMI I RASTIT 2: INCIDENTI I PHISHING-UT WHALING NDAJ DREJTUESVE

👷

Skenari: Një ekzekutiv klikoi një lidhje phishing që pretendonte se përmbante një dokument të sigurt për takimin e bordit dhe futi kredencialet e tij kryesore korporative në një portal të falsifikuar.

Pyetje për diskutim: Përshkruaj në detaje hapat e reagimit ndaj incidentit dhe shpjego si auditohen identifikimet e ekzekutivit.

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		18	10	11	21	10	11	16	9		15	6

24	6	20	11	8	11	13	11	15		21	13	1	16	6	20	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 një mashtrim në internet?

Një skemë mashtruese që përdor kanale dixhitale për t'i nxitur viktimat të dërgojnë para ose të japin kredenciale personale.

Q2: Cili është treguesi kryesor i phishing-ut me email?

Një mesazh që pretendon urgjencë (si pezullimi i llogarisë) dhe të drejton te një lidhje që nuk përputhet me domenin zyrtar.

Q3: Çfarë është typosquatting?

Regjistrimi i domeneve me gabime të zakonshme shkrimi të markave të njohura (si amaz0n.com) për të hostuar faqe të rreme phishing.

Q4: Çfarë është një mashtrim i mbështetjes teknike?

Një dritare pop-up që pretendon se PC-ja jote është e infektuar, duke të drejtuar të thërrasësh një numër dhe të paguash për softuer të rremë pastrimi ose shërbime qasjeje në distancë. [1]

Q5: Çfarë është vishing?

Sulme phishing që përdorin telefonata zanore për t'i mashtruar viktimat që të japin të dhëna të llogarisë bankare ose të hyrjes.

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 do të thotë mashtrim me transferta (wire fraud)?

Ridrejtimi i transaksioneve të pagesave te llogari mashtruese duke imituar shitës ose drejtues.

Q7: Çfarë është whaling?

Një formë shumë e synuar e spear phishing që synon drejtpërdrejt objektiva me vlerë të lartë, si drejtuesit korporativë të nivelit C.

Q8: Çfarë është smishing?

Mesazhe tekst mashtruese të dërguara në pajisje mobile, me lidhje që çojnë në portale të rreme ose përditësime të rreme ndjekjeje.

Q9: Pse është kritike verifikimi jashtë kanalit (out-of-band)?

Konfirmon detajet e transaksionit përmes një kanali të veçantë komunikimi (si një telefonatë), duke shmangur ndërlidhjet e kompromentuara të email-it.

Q10: Si funksionon një mashtrim i rremë me escrow?

Mashtruesit krijojnë një faqe të falsifikuar escrow, duke pretenduar se fondet mbahen të sigurta, pastaj vjedhin depozitën e blerësit me transfertë.

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 e përdorin mashtruesit BEC (Business Email Compromise) për të kryer mashtrim me transfertë bankare?

Rrëmbejnë llogarinë e emailit të një punonjësi të ligjshëm, monitorojnë bisedat për faturat dhe dërgojnë detaje të përditësuara faturimi me llogari bankare mashtruese.

Q2: Cili është rreziku i sulmeve homografe IDN në mashtrimet në internet?

Përdorimi i karaktereve jo-ASCII që duken identike me shkronjat normale (p.sh., 'a' cirilike) për të regjistruar domene të falsifikuara që imitojnë marka të vërteta.

Q3: Pse është e rëndësishme inspektimi i header-ave të email-it në zbulimin e mashtrimeve?

Zbulon IP-në e vërtetë të serverit burimor dhe statusin e validimit SPF/DKIM, duke treguar nëse domeni i dërguesit është i falsifikuar.

Q4: Si e shfrytëzojnë mashtruesit e mbështetjes teknike softuerin e desktopit në distancë?

Përdorin mjete si AnyDesk ose TeamViewer për t'u lidhur me pajisjen e viktimës, për të vendosur malware dhe për të vjedhur fjalëkalimet e ruajtura.

Q5: Cili është qëllimi i mashtrimeve me tarifë paraprake?

Mashtrimi i viktimave që të paguajnë paraprakisht tarifa përpunimi në këmbim të një shpërblimi të madh financiar që nuk ekziston.

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 përdorin mashtruesit profilizimin në rrjetet sociale për phishing të synuar?

Përpilojnë strukturat organizative të korporatave dhe emrat e punonjësve për të hartuar emaile bindëse spear-phishing.

Q7: Pse ofrojnë dyqanet e rreme online zbritje të mëdha?

Për t'i joshur blerësit të fusin të dhënat e kartës së kreditit, duke kapur kredenciale për ripërdorim ose rishitje në forumet e carding-ut.

Q8: Si i bllokojnë regjistrimet DMARC mashtrimet phishing?

DMARC u lejon pronarëve të domeneve t'u kërkojnë marrësve të vendosin në karantinë ose të refuzojnë postën që dështon në kontrollet e përafruara SPF dhe DKIM, duke bllokuar falsifikimin e drejtpërdrejtë. [5]

Q9: Cili është kërcënimi i portaleve të mbledhjes së kredencialeve?

Faqe uebi të falsifikuara të krijuara të duken saktësisht si hapësira pune të Microsoft 365 ose Google, që vjedhin kredencialet e hyrjes ndërsa futen.

Q10: Si i raportojnë dhe i çaktivizojnë ekipet e sigurisë domenet e mashtrimit?

Duke dorëzuar prova mashtrimi te emaili i abuzimit i regjistruesit, ofruesi i hostimit dhe regjistri Google Safe Browsing.

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. [2]

2. PERSPEKTIVË PËR SIGURINË

Kompromentimi i emailit të biznesit (BEC) shkaktoi mbi $3 miliardë humbje të raportuara te IC3 i FBI-së në 2025. [2]

3. PERSPEKTIVË PËR SIGURINË

Domenet e typo-squatting-ut ndryshojnë nga emrat e vërtetë të markave me një a dy karaktere, ndaj një vështrim i shpejtë mund t'i humbasë.

4. PERSPEKTIVË PËR SIGURINË

Mashtrimet e mbështetjes teknike shkaktuan humbje mbi 2.1 miliardë $ të raportuara te IC3 i FBI-së në vitin 2025. [2]

5. PERSPEKTIVË PËR SIGURINË

Sulmet homografike duken identike në shiritat e adresave të shfletuesit, përveç nëse shfletuesi shfaq konfigurimet punycode.

6. PERSPEKTIVË PËR SIGURINË

Mashtrimet me mesazhe SMS (smishing) përdorin mesazhe të shkurtra e urgjente me lidhje, duke u lënë viktimave pak kontekst për të dalluar mashtrimin.

7. NJOHURI PËR SIGURINË

Sulmet whaling synojnë email-et e drejtuesve sepse ata kontrollojnë aksesin te transfertat e mëdha bankare të pagesave.

8. NJOHURI PËR SIGURINË

Verifikimi i ndryshimeve të pagesës duke telefonuar një numër të njohur e të ruajtur është mbrojtje kryesore ndaj mashtrimit BEC me transferta.

9. NJOHURI PËR SIGURINË

Faqet e rreme escrow janë një mashtrim i zakonshëm në tregjet në internet: duken si shërbim i sigurt pagese, por vjedhin transfertën bankare të blerësit.

10. PERSPEKTIVË PËR SIGURINË

Google Safe Browsing i paralajmëron përdoruesit para se të hapin faqe që ka shënuar për phishing ose malware.

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] 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

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

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

SHËNIM PËR MËSUESIN

Cili është treguesi kryesor i një mashtrimi me mbështetje teknike? → Një dritare pop-up që pretendon se sistemi yt është i infektuar dhe të kërkon të thërrasësh një numër telefoni

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

SHËNIM PËR MËSUESIN

Cila teknikë përdor domene dërguesish të falsifikuar për të vjedhur të dhëna bankare? → Phishing me email

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

SHËNIM PËR MËSUESIN

Çfarë përfaqëson mashtrimi me transfertë bankare? → Mashtrimi i viktimave që të dërgojnë para në llogari të rreme korporative duke përdorur inxhinierinë sociale

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

SHËNIM PËR MËSUESIN

Pse krijojnë mashtruesit faqe web të rreme blerjesh? → Për të vjedhur të dhënat e kartës së kreditit dhe kredencialet e pagesës nga blerësit

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

SHËNIM PËR MËSUESIN

Çfarë do të thotë vishing? → Mashtrime phishing me zë përmes rrjeteve telefonike për të vjedhur kredencialet

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: phishing-u synon edhe ekzekutivët; whaling është phishing i drejtuar ndaj drejtuesve të lartë.

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

SHËNIM PËR MËSUESIN

Domenet e falsifikuara shpesh përdorin gabime të vogla shkrimi (si amaz0n.com) për të imituar marka të besuara.

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

SHËNIM PËR MËSUESIN

E gabuar: dhënia e qasjes në distancë një mashtruesi të mbështetjes i lejon të implantojë malware dhe të vjedhë të dhëna.

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

SHËNIM PËR MËSUESIN

Inxhinieria sociale shfrytëzon psikologjinë njerëzore si frika dhe urgjenca për të anashkaluar rregullat e sigurisë.

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

SHËNIM PËR MËSUESIN

Kërkesat për transferta bankare duhet të verifikohen gjithmonë përmes kanaleve komunikimi jashtë brezit (out-of-band).

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

G 1. PHISHING	F 2. I FALSIFIKUAR	D 3. VISHING	B 4. MASHTRIM
H 5. VERIFIKIM	A 6. TRANSFERTË BANKARE	E 7. WHALING	C 8. SMISHING

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 PHISHING	2 IMITUAR	3 VISHING	4 MASHTRIM
5 VERIFIKIM	6 TRANSFERIM		

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

1 B – IMITUAR	2 E – VERIFIKIM	3 F – TRANSFERIM	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – MASHTRIM

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë PHISHING, I FALSIFIKUAR dhe VISHING 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.

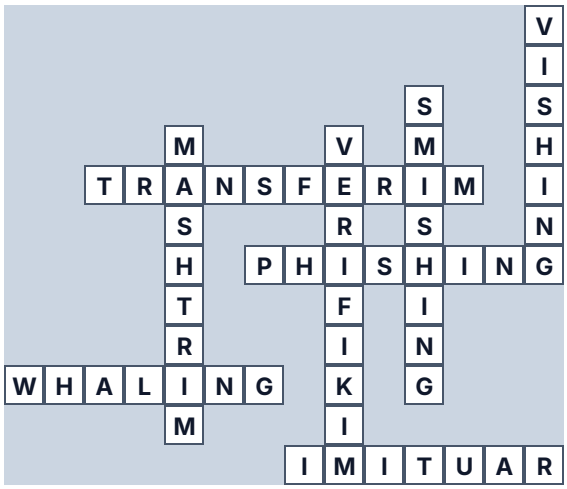
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

5 horizontalisht: TRANSFERIM Ridrejtim mashtrues i transaksioneve bankare drejt llogarive kriminale. (10 shkronja)

6 horizontalisht: PHISHING Fushata mashtruese me email të projektuara për të vjedhur kredencialet e hyrjes dhe fjalëkalimet. (8 shkronja)

7 horizontalisht: WHALING Sulme phishing të synuara që kërkojnë të vjedhin kredenciale nga drejtuesit e nivelit C. (7 shkronja)

8 horizontalisht: IMITUAR Adresë e imituar e dërguesit të emailit ose e faqes së uebit, e projektuar të duket legjitime. (7 shkronja)

VERTIKALISHT

1 vertikalisht: VISHING Telefonata mashtruese me zë të projektuara për të vjedhur kredencialet dhe detajet e llogarisë. (7 shkronja)

2 vertikalisht: SMISHING Dërgimi i mesazheve tekst mashtruese për të vjedhur kredencialet e llogarisë celulare. (8 shkronja)

3 vertikalisht: MASHTRIM Skemë mashtruese e projektuar për të vjedhur para ose qasje në kredenciale nga viktimat. (8 shkronja)

4 vertikalisht: VERIFIKIM Konfirmimi i detajeve të pagesës përmes një metode kontakti dytësore të besueshme. (9 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. NSHPIHGI — **PHISHING**
2. VSGNIHI — **VISHING**
3. VIFEKMIIR — **VERIFIKIM**
4. GHILNWA — **WHALING**
5. URTIIAM — **IMITUAR**
6. IMHRMTAS — **MASHTRIM**
7. RNTEFRIMSA — **TRANSFERIM**
8. SMHGSNII — **SMISHING**

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"ZBULO PHISHING ME VERIFIKIM SKANERI"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Parandalimi i mashtrimit me transfertë bankare të korporatës

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një departament financash merr një email urgjent nga një adresë e falsifikuar shitësi, që kërkon që transfertat e faturave të ardhshme të drejtohen te një numër i ri rrugëzimi.
- Strategjia dhe zgjidhja e rekomanduar: Zbato një politikë autorizimi të dyfishtë për të gjitha pagesat. Zbato verifikim jashtë kanalit me një numër telefoni të ruajtur më parë dhe blloko në gateway email-et me domene të falsifikuara.

B Studimi i rastit 2: Incidenti i phishing-ut whaling ndaj drejtuesve

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një drejtues klikoi një lidhje phishing që pretendonte të përmbante një dokument të sigurt për mbledhjen e bordit dhe futi kredencialet kryesore të korporatës në një portal të falsifikuar.
- Strategjia dhe zgjidhja e rekomanduar: Izolo pajisjen e drejtuesit. Rivendos të gjitha tokenët e seancave dhe kredencialet e korporatës. Rishiko regjistrat e qasjes për dalje të të dhënave dhe zbato MFA me harduer në të gjitha hyrjet.