Emri: _____ Data: _____ Pikët: _____

Parandalimi i vjedhjes së identitetit dhe pasuritë
Udhëzues sigurie

Rrjedhjet e kredencialeve, MFA, monitorimi i dark web-it, alarmet e ngrirjes së kreditit, inxhinieria sociale

PËRMBLEDHJE E MËSIMIT PËR PARANDALIMIN E VJEDHJES SË IDENTITETIT

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 parandalimit dhe zbutjes së vjedhjes së identitetit. Do të eksplorosh rrjedhjet e kredencialeve, autentikimin me shumë faktorë, monitorimin e internetit të errët, sinjalizimet e ngrirjes së kreditit dhe mbrojtjen nga inxhinieria sociale.

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/vjedhja-e-identitetit/

Udhërrëfyesi yt mësimor për mbrojtjen e identitetit

- Kupto rreziqet e ekspozimit të kredencialeve në forumet e uebit të errët.
- Zbato autentikimin me shumë faktorë (MFA) dhe njoftimet për ngrirjen e kredisë.
- Harto mbrojtje sigurie për korporatat kundër mashtrimeve të synuara të inxhinierisë sociale.

UDHËZIME PËR UDHËZUESIN E VJEDHJES SË IDENTITETIT

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 e identitetit. Përfundo me aktivitetin bonus Mendo shpejt.

PARANDALIMI I VJEDHJES SË IDENTITETIT DHE SIGURIA E PASURIVE (HYRJE)

Vjedhja e identitetit shfrytëzon kredencialet e rrjedhura dhe hyrjet e dobëta për të marrë nën kontroll llogaritë personale dhe të korporatave. Vendosja e MFA, ngrirja e kredisë, skanerët e dark web-it dhe kornizat SPF/DKIM/DMARC përbëjnë një mbrojtje kritike kundër imitimit dixhital.

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Cila është metoda kryesore që përdorin vjedhësit e identitetit për të vjedhur kredencialet e hyrjes?

- A. Dërgimi i alarmeve të rreme me email që i mashtrojnë përdoruesit të fusin fjalëkalime në portale të falsifikuara
- B. Dëgjimi i transmetimeve radiofonike pranë zyrës së korporatës së një përdoruesi
- C. Defragmentimi i diskut lokal të ruajtjes së serverit të një përdoruesi
- D. Shkëputja e konfigurimeve të jashtme të kopjeve rezervë të rrjetit

2. Cili kontroll sigurie ofron mbrojtjen më të fortë ndaj rrjedhjeve të kredencialeve?

- A. Autentikim shumëfaktorësh me çelësa harduerikë
- B. Krijimi i fjalëkalimeve të gjata duke përdorur formatet e parazgjedhura të shfletuesit
- C. Ndryshimi i emrave të përdoruesve të emailit çdo gjashtë muaj
- D. Fshirja e historive të gjurmimit të cookie-ve të ruajtura në shfletues

3. Çfarë përfaqëson ngrirja e kreditit?

- A. Kyçja e raporteve të kredisë për të parandaluar që hajdutët të hapin hua të paautorizuara
- B. Fshirja e historikut të transaksioneve të llogarive bankare nga bazat e të dhënave
- C. Çaktivizimi i lexuesve magnetikë të kartave të kreditit në skanerë
- D. Enkriptimi i diskeve të ngurtë të bazës së të dhënave në pushim

4. Pse është i dobishëm monitorimi i dark web-it?

- A. Njofton përdoruesit nëse kredencialet e tyre të rrjedhura shfaqen në baza të dhënash të paligjshme
- B. Parandalon ekzekutimin e malware-it aktiv në sandbox-e virtualë
- C. Përshpejton shpejtësinë e rutimit të shfletuesit në rrjetet virtuale
- D. Bllokon përpjekjet e qasjes SQL injection në bazën e të dhënave backend

5. Çfarë do të thotë inxhinieri sociale?

- A. Manipulimi i njerëzve që t'i zbulojnë vullnetarisht kredencialet konfidenciale
- B. Skanimi i porteve të serverëve të korporatës për shfrytëzime aktive të sigurisë
- C. Kopjimi rezervë i skedarëve të bazës së të dhënave të sistemit në hard disqe offline
- D. Rutimi i paketave të rrjetit përmes tre nyjeve onion të enkriptuara

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

6 Pyetja 6

6. Vjedhja e identitetit prek vetëm llogaritë dixhitale në internet, jo postën fizike.

- ○ E vërtetë
- ○ E gabuar

7 Pyetja 7

7. Zbatimi i MFA në të gjitha llogaritë personale bllokon shumicën e sulmeve me boto të credential stuffing.

- ○ E vërtetë
- ○ E gabuar

8 Pyetja 8

8. Një bllokim krediti (credit freeze) bllokon kontrollet e kredisë, por të pengon të qasesh në llogarinë tënde bankare.

- ○ E vërtetë
- ○ E gabuar

9 Pyetja 9

9. Menaxherët e fjalëkalimeve i mbrojnë përdoruesit nga phishing-u duke refuzuar plotësimin automatik të fjalëkalimeve në domene të falsifikuara.

- ○ E vërtetë
- ○ E gabuar

10 Pyetja 10

10. Email-et phishing shpesh përdorin gjuhë urgjente për të nxitur reagime emocionale dhe të nxituara.

- ○ 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. Vjedhësit e identitetit synojnë fjalëkalimet personale dhe _____ të përdoruesve.

2. Njoftimi i përdoruesve për shkelje të bazave të të dhënave identifikon _____ të llogarive private.

3. Kërkimi i një kodi të përkohshëm për të hyrë në llogari quhet _____ .

4. Skanimi i forumeve të hakerëve për të dhëna të vjedhura është _____ i dark web-it.

5. Bllokimi i kontrolleve të paautorizuara të kredisë kërkon një _____ të kredisë.

6. Trajnimi i punonjësve për ndërgjegjësimin ndaj phishing-ut ndërton një _____ aktive të sigurisë.

BANKA E FJALËVE TË LEKSIKUT

AUTENTIKIM MFA FALSIFIKIM KREDENCIALE MBROJTJE MONITORIM NGRIRJE PHISHING RRJEDHJE

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

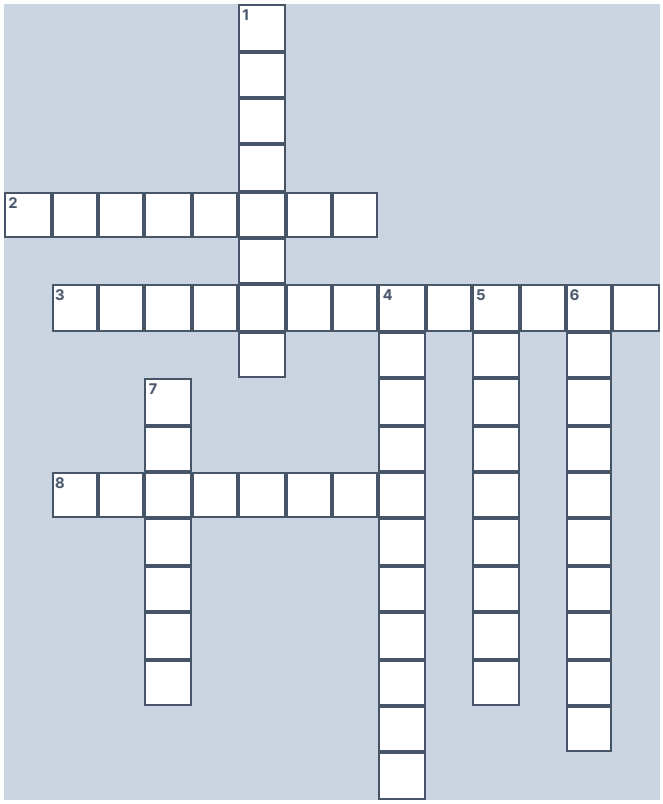
PËRPUTHJA E PËRKUFIZIMEVE

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. KREDENCIALE	A	Hap dytësor verifikimi (si çelësat hardware) që mbron hyrjet në llogari.
☐	2. RRJEDHJET	B	Krijimi i një faqeje interneti ose emaili të rremë për të imituar një organizatë legjitime.
☐	3. MFA	C	Kufizimi i qasjes në dosjet e kredisë për të parandaluar kërkesat mashtruese për hua.
☐	4. MONITORIM	D	Ekspozimi i paautorizuar i bazave të të dhënave private që përmbajnë regjistrime personale të përdoruesve.
☐	5. NGRIRJE	E	Trajnimi dhe kontrollet teknike të përdorura për t'u mbrojtur nga vjedhja e identitetit.
☐	6. MBROJTJE	F	Dërgimi i mesazheve mashtruese për t'i nxitur përdoruesit të dorëzojnë kredencialet.
☐	7. FALSIFIKIM	G	Skanimi i forumeve online dhe i kanaleve të hakerëve për të dhëna të vjedhura të korporatës.
☐	8. PHISHING	H	Emrat e përdoruesve, fjalëkalimet dhe tokenat privatë që përdoren për të vërtetuar identitetet digjitale.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

2. Ekspozim i paautorizuar i bazave të të dhënave private që përmbajnë regjistrime personale të përdoruesve. (8)

3. Hap dytësor verifikimi (si çelësat harduerikë) që mbron hyrjet në llogari. (13)

8. Trajnime dhe kontrolle teknike të përdorura për të mbrojtur nga vjedhja e identitetit. (8)

VERTIKALISHT

1. Dërgimi i mesazheve mashtruese për të nxitur përdoruesit të japin kredencialet. (8)

4. Emra përdoruesish, fjalëkalime dhe tokena privatë që përdoren për të autentikuar identitetet dixhitale. (11)

5. Skanimi i forumeve online dhe i kanaleve të hakerëve për të dhëna korporative të vjedhura. (9)

6. Krijimi i një faqeje ose emaili të rremë për të imituar një organizatë legjitime. (10)

7. Kufizimi i qasjes në dosjet e kredisë për të parandaluar aplikimet mashtruese për hua. (7)

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

2 horizontalisht: Ekspozim i paautorizuar i bazave të të dhënave private që përmbajnë regjistrime personale të përdoruesve. (8 shkronja):

3 horizontalisht: Hap dytësor verifikimi (si çelësat harduerikë) që mbron hyrjet në llogari. (13 shkronja):

8 horizontalisht: Trajnime dhe kontrolle teknike të përdorura për të mbrojtur nga vjedhja e identitetit. (8 shkronja):

VERTIKALISHT

1 vertikalisht: Dërgimi i mesazheve mashtruese për të nxitur përdoruesit të japin kredencialet. (8 shkronja):

4 vertikalisht: Emra përdoruesish, fjalëkalime dhe tokena privatë që përdoren për të autentikuar identitetet dixhitale. (11 shkronja):

5 vertikalisht: Skanimi i forumeve online dhe i kanaleve të hakerëve për të dhëna korporative të vjedhura. (9 shkronja):

6 vertikalisht: Krijimi i një faqeje ose emaili të rremë për të imituar një organizatë legjitime. (10 shkronja):

7 vertikalisht: Kufizimi i qasjes në dosjet e kredisë për të parandaluar aplikimet mashtruese për hua. (7 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.

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

LISTA E FJALËVE TË LEKSIKUT

KREDENCIALE, RRJEDHJE, AUTENTIKIMMFA, MONITORIM, NGRIRJE, MBROJTJE, FALSIFIKIM, PHISHING

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. KREDENCIALE

B. RRJEDHJE

C. AUTENTIKIMMFA

D. MONITORIM

E. NGRIRJE

F. MBROJTJE

G. FALSIFIKIM

H. PHISHING

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Dërgimi i mesazheve mashtruese për të nxitur përdoruesit të japin kredencialet.

2. Emra përdoruesish, fjalëkalime dhe tokena privatë që përdoren për të autentikuar identitetet dixhitale.

3. Krijimi i një faqeje ose emaili të rremë për të imituar një organizatë legjitime.

4. Trajnime dhe kontrolle teknike të përdorura për të mbrojtur nga vjedhja e identitetit.

5. Skanimi i forumeve online dhe i kanaleve të hakerëve për të dhëna korporative të vjedhura.

6. Kufizimi i qasjes në dosjet e kredisë për të parandaluar aplikimet mashtruese për hua.

7. Ekspozim i paautorizuar i bazave të të dhënave private që përmbajnë regjistrime personale të përdoruesve.

8. Hap dytësor verifikimi (si çelësat harduerikë) që mbron hyrjet në llogari.

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. **ECLRNIKAEED** _____
2. **FNUTTAMIAI MKE** _____
3. **INRERJG** _____
4. **FIIMSKIFAL** _____
5. **DHREERJJ** _____
6. **IIOROMTMN** _____
7. **MEJTJBOR** _____
8. **SHHGPNII** _____

Aktivitet bonus: Mendo shpejt

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

1	Gjëra që bëhen nëse të vjedhin identitetin			
2	Gjëra që nuk duhen ndarë në rrjetet sociale			
3	Gjëra që ruan si kopje rezervë			
4	Karta ose dokumente identiteti në portofolin tënd			
5	Dokumente që duhet t'i mbrosh			
6	Gjëra që bëhen pas një rrjedhjeje të dhënash			
7	Arsye për të përditësuar softuerin			
8	Informacione që dëshiron një vjedhës identiteti			
9	Pajisje që mund të hakohen			
10	Vende nga mund të rrjedhin të dhënat e tua			
11	Zakone të sigurta që mund t'i fillosh sot			
12	Shenja që një kompjuter është i infektuar			
13	Mënyra për të provuar kush je			
14	Shenja të vjedhjes së identitetit			
15	Shenja paralajmëruese në një email			

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: MBROJTJA NGA IMITIMI I IDENTITETIT TË DREJTUESVE

👷

Skenari: Një drejtues i nivelit C me profil të lartë është bërë objektiv i emrave të domeneve me gabime shtypi (typosquatting) që imitojnë emailin e tij personal për të mashtruar klientët. Harto një plan mbrojtjeje të markës.

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

STUDIMI I RASTIT 2: EKSPOZIMI I KREDENCIALEVE TË KORPORATËS NË DARK WEB

👷

Skenari: Një dump i bazës së të dhënave nga dark web përmban disa qindra kredenciale korporative që u përkasin administratorëve të sistemit të një ndërmarrjeje. Harto një strategji zbutjeje.

Pyetje për diskutim: Përshkruaj procesin e pastrimit të kredencialeve dhe planifiko një zbatim të një menaxheri fjalëkalimesh.

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

15	2	20	17	12	6		11	5	6	16	22	11	22	6	22	11	16
						5	11	25	10	11	22	1	14		15	6	
					1	23	22	6	16	22	11	13	11	15		15	8	1

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 vjedhja e identitetit?

Një krim ku sulmuesi vjedh të dhëna personale (si fjalëkalime ose SSN) për të imituar dikë tjetër për përfitim financiar.

Q2: Cili është shkaku më i zakonshëm i vjedhjes së identitetit?

Phishing-u është një nga mënyrat kryesore se si hajdutët marrin fjalëkalimet, duke i joshur përdoruesit në sajte të rreme e të falsifikuara.

Q3: Si i mbron identitetet vërtetimi shumëfaktorësh (MFA)?

MFA kërkon një provë dytësore (si një çelës hardueri) për t'u identifikuar, duke i bllokuar sulmuesit edhe nëse ta vjedhin fjalëkalimin.

Q4: Çfarë është ngrirja e kreditit (credit freeze)?

Një shërbim falas që i pengon byrotë e kredisë të ndajnë dosjen tënde të kredisë, duke ndaluar hajdutët të hapin hua të reja në emrin tënd. [2]

Q5: Çfarë është monitorimi i dark web?

Softuer që kontrollon forumet e hakerëve për email-e, fjalëkalime dhe regjistrime personale të rrjedhura dhe të njofton nëse të dhënat e tua janë ekspozuar.

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 credential stuffing?

Bot-e të automatizuar që testojnë lista fjalëkalimesh të rrjedhura në qindra faqe interneti për të marrë nën kontroll llogari aktive.

Q7: Pse është i rrezikshëm email spoofing?

U lejon sulmuesve të falsifikojnë emrin e dërguesit në email-e, duke bërë që mesazhet phishing të duken sikur vijnë nga kolegë të besuar.

Q8: Si e ndalojnë menaxherët e fjalëkalimeve vjedhjen e identitetit?

Ruajnë fjalëkalime komplekse e unike për çdo llogari dhe refuzojnë të plotësojnë automatikisht kredencialet në domene të rreme phishing.

Q9: Çfarë është spear phishing?

Një sulm phishing shumë i synuar, i personalizuar me emrin dhe detajet e viktimës për të rritur mundësinë e mashtrimit.

Q10: Si ndryshon një alarm krediti nga një ngrirje?

Një alarm u thotë huadhënësve të verifikojnë identitetin tënd para hapjes së llogarive, ndërsa një bllokim (freeze) e bllokon plotësisht qasjen në dosjen tënde të kredisë. [2]

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 çon SIM swapping te vjedhja e identitetit?

Sulmuesit bindin stafin e operatorit ta transferojë numrin e telefonit të viktimës në një SIM të re, duke rrëmbyer kodet 2FA me SMS.

Q2: Cili është roli i DMARC në parandalimin e vjedhjes së identitetit?

DMARC u lejon pronarëve të domeneve të bllokojnë email-et e falsifikuara që të mos arrijnë në kutitë postare, duke ndaluar email-et e rreme që imitojnë domenet e korporatave.

Q3: Pse është e vështirë të zbulohet vjedhja e identitetit sintetik?

Hajdutët kombinojnë SSN të vërteta me emra dhe data lindjeje të rreme për të ndërtuar profile krediti krejt të reja, duke anashkaluar alarmet bazë të mashtrimit.

Q4: Si i shfrytëzojnë ndërmjetësit e të dhënave identitetet personale?

Ndërmjetësit e të dhënave mbledhin regjistra publikë, sjelljen në internet dhe historikun e blerjeve për të përpiluar dosje profilesh, të cilat mund të rrjedhin ose të shiten.

Q5: Pse konsiderohet MFA me SMS i cenueshëm?

Trafiku SMS është i cenueshëm ndaj përgjimit, phishing-ut dhe shfrytëzimeve të ndërrimit të SIM-it në nivel operatori.

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: Çfarë është bllokimi i skedarit të kreditit?

Një shërbim komercial i ngjashëm me bllokimin (freeze), që u lejon përdoruesve ta kyçin ose zhbllokojnë menjëherë dosjen e tyre të kredisë përmes një aplikacioni celular.

Q7: Si e ushqejnë vjedhjen e identitetit shkeljet e të dhënave të korporatave?

Bazat e të dhënave të rrjedhura ekspozojnë miliona kredenciale në tekst të thjeshtë, duke u dhënë hajdutëve të dhënat e papërpunuara që u duhen për të kryer mashtrim të synuar identiteti.

Q8: Cili është rreziku i ndarjes së tepërt në rrjetet sociale?

Ndarja publike e emrave të kafshëve shtëpiake, vendlindjeve dhe mbiemrit të nënës para martesës u jep hajdutëve përgjigjet e pyetjeve të zakonshme për rikuperimin e llogarisë.

Q9: Si i mbrojnë identitetet hyrjet biometrike?

Biometria i lidh hyrjet me tipare si gjurmët e gishtërinjve ose fytyra; kur mbahen në pajisje janë të vështira për t'u vjedhur, por të dhënat biometrike të ruajtura mund të rrjedhin.

Q10: Si e luftojnë vjedhjen e identitetit Rregullat e Flamujve të Kuq (Red Flags Rule)?

Një rregullore federale që kërkon që institucionet financiare të zhvillojnë programe të shkruara për zbulimin dhe reagimin ndaj shenjave paralajmëruese të vjedhjes së identitetit.

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

IdentityTheft.gov, i drejtuar nga FTC, u lejon viktimave në SHBA të raportojnë vjedhjen e identitetit dhe të marrin një plan personal rimëkëmbjeje. [1]

2. PERSPEKTIVË PËR SIGURINË

Çelësat e sigurisë hardueri janë MFA rezistente ndaj phishing-ut, lloji më i fortë i MFA që CISA nxit. [4]

3. PERSPEKTIVË PËR SIGURINË

Fjalëkalimet e kompromentuara janë një pikë e zakonshme hyrjeje në shkeljet e të dhënave, duke ushqyer mashtrimin e mëvonshëm me identitetin.

4. PERSPEKTIVË PËR SIGURINË

Një bllokim krediti (credit freeze) është falas sipas ligjit federal dhe i pengon huadhënësit të kontrollojnë dosjet e kredisë derisa të zhbllokohet. [2]

5. PERSPEKTIVË PËR SIGURINË

DMARC u lejon pronarëve të domeneve t'u thonë serverëve të postës të refuzojnë ose të vendosin në karantinë email-et e falsifikuara që dështojnë në kontrolle. [7]

6. PERSPEKTIVË PËR SIGURINË

Ndërrimi i SIM-it u lejon hakerave të anashkalojnë vërtetimin dyfaktorësh të bazuar në SMS në portalet bankare.

7. NJOHURI PËR SIGURINË

Mashtrimi me identitet sintetik përzien detaje të vërteta dhe të rreme, duke e bërë të vështirë zbulimin nga huadhënësit.

8. NJOHURI PËR SIGURINË

Shumë njerëz e ripërdorin të njëjtin fjalëkalim në llogari të ndryshme online, ndaj një shkelje mund të ekspozojë disa prej tyre.

9. NJOHURI PËR SIGURINË

Ndërmjetësit e të dhënave hartojnë dosje të hollësishme për një numër të madh konsumatorësh, duke krijuar një rrezik të përqendruar për privatësinë.

10. PERSPEKTIVË PËR SIGURINË

Rimëkëmbja nga vjedhja e identitetit mund të kërkojë muaj punë, si kontestimi i tarifave dhe korrigjimi i raporteve të kredisë.

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.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

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

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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

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

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

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

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

SHËNIM PËR MËSUESIN

Cila është metoda kryesore që përdorin vjedhësit e identitetit për të vjedhur kredencialet e hyrjes? → Dërgimi i alarmeve të rreme me email që i mashtrojnë përdoruesit të fusin fjalëkalime në portale të falsifikuara

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

SHËNIM PËR MËSUESIN

Cili kontroll sigurie ofron mbrojtjen më të fortë ndaj rrjedhjeve të kredencialeve? → Autentikim shumëfaktorësh me çelësa harduerikë

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

SHËNIM PËR MËSUESIN

Çfarë përfaqëson ngrirja e kreditit? → Kyçja e raporteve të kredisë për të parandaluar që hajdutët të hapin hua të paautorizuara

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

SHËNIM PËR MËSUESIN

Pse është i dobishëm monitorimi i dark web-it? → Njofton përdoruesit nëse kredencialet e tyre të rrjedhura shfaqen në baza të dhënash të paligjshme

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

SHËNIM PËR MËSUESIN

Çfarë do të thotë inxhinieri sociale? → Manipulimi i njerëzve që t'i zbulojnë vullnetarisht kredencialet konfidenciale

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

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

SHËNIM PËR MËSUESIN

Vjedhja e identitetit mund të fillojë edhe jashtë linje, si me postë ose dokumente të vjedhura.

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

SHËNIM PËR MËSUESIN

Zbatimi i MFA në të gjitha llogaritë personale bllokon shumicën e sulmeve me boto të credential stuffing.

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

SHËNIM PËR MËSUESIN

Një ngrirje krediti ndalon kontrollet e reja të kredisë, por nuk ndikon në llogaritë e tua ekzistuese.

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

SHËNIM PËR MËSUESIN

Menaxherët e fjalëkalimeve i mbrojnë përdoruesit nga phishing-u duke refuzuar plotësimin automatik të fjalëkalimeve në domene të falsifikuara.

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

SHËNIM PËR MËSUESIN

Email-et phishing shpesh përdorin gjuhë urgjente për të nxitur reagime emocionale dhe të nxituara.

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

H 1. KREDENCIALE	D 2. RRJEDHJET	A 3. MFA	G 4. MONITORIM
C 5. NGRIRJE	E 6. MBROJTJE	B 7. FALSIFIKIM	F 8. PHISHING

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 KREDENCIALE	2 RRJEDHJE	3 AUTENTIKIM MFA	4 MONITORIM
5 NGRIRJE	6 MBROJTJE		

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

1 H – PHISHING	2 A – KREDENCIALE	3 G – FALSIFIKIM	4 F – MBROJTJE
5 D – MONITORIM	6 E – NGRIRJE	7 B – RRJEDHJE	8 C – AUTENTIKIMMFA

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë KREDENCIALE, RRJEDHJET dhe MFA 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.

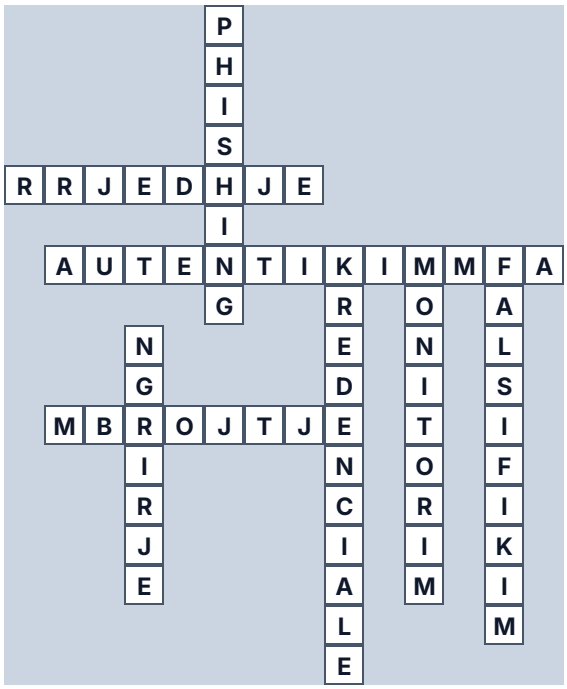
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

2 horizontalisht: RRJEDHJE Ekspozim i paautorizuar i bazave të të dhënave private që përmbajnë regjistrime personale të përdoruesve. (8 shkronja)

3 horizontalisht: AUTENTIKIMMFA Hap dytësor verifikimi (si çelësat harduerikë) që mbron hyrjet në llogari. (13 shkronja)

8 horizontalisht: MBROJTJE Trajnime dhe kontrolle teknike të përdorura për të mbrojtur nga vjedhja e identitetit. (8 shkronja)

VERTIKALISHT

1 vertikalisht: PHISHING Dërgimi i mesazheve mashtruese për të nxitur përdoruesit të japin kredencialet. (8 shkronja)

4 vertikalisht: KREDENCIALE Emra përdoruesish, fjalëkalime dhe tokena privatë që përdoren për të autentikuar identitetet dixhitale. (11 shkronja)

5 vertikalisht: MONITORIM Skanimi i forumeve online dhe i kanaleve të hakerëve për të dhëna korporative të vjedhura. (9 shkronja)

6 vertikalisht: FALSIFIKIM Krijimi i një faqeje ose emaili të rremë për të imituar një organizatë legjitime. (10 shkronja)

7 vertikalisht: NGRIRJE Kufizimi i qasjes në dosjet e kredisë për të parandaluar aplikimet mashtruese për hua. (7 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. ECLRNIKAEED — **KREDENCIALE**
2. FNUTTAMIAIMKE — **AUTENTIKIMMFA**
3. INRERJG — **NGRIRJE**
4. FIIMSKIFAL — **FALSIFIKIM**
5. DHREERJJ — **RRJEDHJE**
6. IIOROMTMN — **MONITORIM**
7. MEJTJBOR — **MBROJTJE**
8. SHHGPNII — **PHISHING**

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"MBROJE IDENTITETIN DIXHITAL ME AUTENTIKIM MFA"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Mbrojtja nga imitimi i identitetit të drejtuesve

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një drejtues i profilit të lartë i nivelit C është shënjestruar nga emra domenesh typo-squatted që imitojnë email-in e tij personal për të mashtruar klientët. Hartoni një plan mbrojtjeje të markës.
- Strategjia dhe zgjidhja e rekomanduar: Regjistro të gjitha variantet e zakonshme të shkrimit të emrit të drejtuesit. Zbato protokolle të vërtetimit të email-it (DMARC, DKIM, SPF) për të parandaluar falsifikimin e domenit. Zbato MFA me harduer në të gjitha hyrjet e korporatës së drejtuesve të nivelit C.

B Studimi i rastit 2: Ekspozimi i kredencialeve të korporatës në dark web

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një depozitim i bazës së të dhënave të dark web përmban disa qindra kredenciale korporative që u përkasin administratorëve të sistemit të një ndërmarrjeje. Hartoni një strategji zbutjeje.
- Strategjia dhe zgjidhja e rekomanduar: Kryej një rivendosje fjalëkalimesh në të gjithë kompaninë. Detyro përdorimin e një menaxheri fjalëkalimesh për ndërmarrje. Zbato MFA në të gjitha portalet e sistemit dhe vendos sinjalizime të vazhdueshme të automatizuara për monitorimin e dark web.