Nafn: _____ Dagsetning: _____ Stig: _____

Vörn gegn auðkennisþjófnaði og eignir Öryggisleiðbeiningar

Leki innskráningarupplýsinga, MFA, vöktun myrkavefs, viðvaranir um lánshæfisfrystingu, blekkingar á fólki (social engineering)

YFIRLIT NÁMS UM VÖRN GEGN AUÐKENNISÞJÓFNAÐI

VARIÐ
GAGNADULKÓÐUN
256-bita AES staðall

UPPFYLLIR KRÖFUR
ALÞJÓÐLEGIR STAÐLAR
Rammar GDPR og CCPA

ZERO-TRUST
AÐGANGSSTEFNA
Fjölþátta auðkenning

Velkomin! Þetta verkefnahefti leiðir þig í gegnum forvarnir og mótvægisaðgerðir gegn persónuþjófnaði. Þú munt kynnast leka á skilríkjum, fjölþátta auðkenningu, vöktun á dökkvefnum, viðvörunum um frystingu lánshæfis og vörnum gegn félagsverkfræði (social engineering).

ÁFANGAR VERKEFNABLAÐSINS

- [ ] **Hluti 1-4: Náðu tökum á netöryggi og varnir gegn ógnum.**
- [ ] **Hluti 5-7: Leystu krossgátur og orðaleitarþrautir.**
- [ ] **Hluti 8-9: Leystu dæmisögur og dulmálsáskorun.**
- [ ] **Hluti 10: Farðu yfir síður með algengum spurningum, grunnstig og framhaldsstig.**
- [ ] **Hluti 11: Kannaðu 10 áhugaverðar staðreyndir úr raunheimum.**
- [ ] **Auka: áskorunin Hugsaðu hratt.**

Opnaðu netöryggisleiðarvísi VPN.com

URL: https://www.vpn.com/is/cybersecurity/identity-theft/

Námsvegvísir þinn: vernd gegn persónuþjófnaði

- Skildu hættuna á að auðkenni afhjúpist á spjallborðum dökka vefsins.
- Innleiddu fjölþátta auðkenningu (MFA) og viðvaranir um lánafrystingu.
- Hannaðu varnir fyrirtækis gegn markvissum svikum með mannlegri blekkingu.

LEIÐBEININGAR UM VÖRN GEGN AUÐKENNISÞJÓFNAÐI

Svaraðu fjölvalsspurningunum og satt/ósatt-spurningunum, kláraðu eyðufyllingarsetningarnar með orðabankanum, paraðu saman skilgreiningar og leystu krossgátuna og orðaleitina. Nýttu þekkingu þína á vernd auðkennis. Ljúktu með aukaverkefninu Hugsaðu hratt.

VÖRN GEGN AUÐKENNISÞJÓFNAÐI OG ÖRYGGI EIGNA (INNGANGUR)

Auðkennisþjófnaður nýtir leka innskráningarupplýsingar og veik innskráningarkerfi til að taka yfir persónulega og fyrirtækjareikninga. Notkun MFA, lánafrystinga, leitartóla fyrir myrkvefinn og ramma SPF/DKIM/DMARC myndar mikilvæga vörn gegn stafrænni persónufölsun.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hver er helsta leið sem auðkennisþjófar nota til að stela innskráningargögnum?**

- A. Að senda fölsk viðvörunarskilaboð í tölvupósti sem blekkja notendur til að slá inn lykilorð á falsaðri gátt
- B. Að hlusta á útvarpssendingar nálægt skrifstofu fyrirtækis notanda
- C. Að affragmenta staðbundinn geymsludisk notanda á netþjóni
- D. Að aftengja ytri afritunarstillingar netsins

2 **2. Hvaða öryggisstýring veitir öflugustu vörnina gegn leka innskráningargagna?**

- A. Fjölþátta auðkenning með vélbúnaðarlyklum
- B. Að búa til löng lykilorð með sjálfgefnum sniðum vafra
- C. Að skipta um netfangsnotendanöfn á sex mánaða fresti
- D. Að eyða geymdum rakningarsögum vefkaka í vafra

3 **3. Hvað táknar frysting lánshæfis?**

- A. Að læsa lánshæfisskýrslum til að koma í veg fyrir að þjófar stofni óheimil lán
- B. Að eyða færslusögu bankareikninga úr gagnagrunnum
- C. Að slökkva á segulrandalesurum greiðslukorta í skönnum
- D. Að dulkóða staðbundna gagnagrunnsdiska í hvíld

4 **4. Hvers vegna er vöktun á dökkvefnum gagnleg?**

- A. Það lætur notendur vita ef lekin auðkenni þeirra birtast í ólöglegum gagnagrunnum
- B. Það kemur í veg fyrir að virk spilliforrit keyri í sýndarsandkössum
- C. Það flýtir fyrir leiðarvali vafra á sýndarnetum
- D. Hún lokar á tilraunir til SQL-innsprautunar í bakenda gagnagrunns

5 **5. Hvað merkir félagsleg misnotkun (social engineering)?**

- A. Að hagræða fólki til að gefa sjálfviljugt upp trúnaðarauðkenni
- B. Að skanna gáttir fyrirtækjanetþjóna eftir virkum öryggisveikleikum
- C. Að taka afrit af kerfisgagnagrunnsskrám á harða diska án nettengingar
- D. Að beina netpökkum um þrjá dulkóðaða onion-hnúta

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. Auðkennisþjófnaður hefur aðeins áhrif á stafræna netreikninga, ekki á bréfpóst.

- ◯ Satt
- ◯ Ósatt

7 Spurning 7

7. Að framfylgja MFA á öllum persónulegum reikningum hindrar flestar þjótaárásir sem prófa stolin lykilorð (credential stuffing).

- ◯ Satt
- ◯ Ósatt

8 Spurning 8

8. Lánshæfisfrysting lokar á athuganir á lánshæfi en kemur í veg fyrir að þú komist í þinn eigin bankareikning.

- ◯ Satt
- ◯ Ósatt

9 Spurning 9

9. Lykilorðastjórar vernda notendur gegn vefveiðum með því að neita að fylla sjálfkrafa út lykilorð á fölsuðum lénum.

- ◯ Satt
- ◯ Ósatt

10 Spurning 10

10. Vefveiðapóstar nota oft áríðandi orðalag til að kalla fram tilfinningaleg og fljótfærnisleg viðbrögð.

- ◯ Satt
- ◯ Ósatt

Áfangi 3: Lykilhugtök fyllt inn

Lestu hverja setningu hér að neðan og fylltu í eyðuna með réttu hugtaki úr orðabankanum.

1. Auðkennisþjófar eltast við persónuleg lykilorð og önnur _____ notenda.

2. Viðvaranir til notenda um innbrot í gagnagrunna greina þá á einkareikningum, þ.e. _____ .

3. Að krefjast tímabundins kóða við innskráningu kallast fjölþátta _____ .

4. Leit á spjallborðum tölvuþrjóta að stolnum gögnum er _____ á myrkravefnum.

5. Til að loka fyrir óheimilar lánshæfisathuganir þarf _____ á lánshæfisskrá.

6. Þjálfun starfsmanna í vitund um vefveiðar byggir upp virka _____ í öryggismálum.

ORÐABANKI

FRYSTING FÖLSUN GAGNALEKAR SKILRÍKI STAÐFESTING VEFVEIÐAR VÖKTUN VÖRN

Skrifaðu svörin þín hér:

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

Áfangi 4: Pörun hugtaka um öryggi

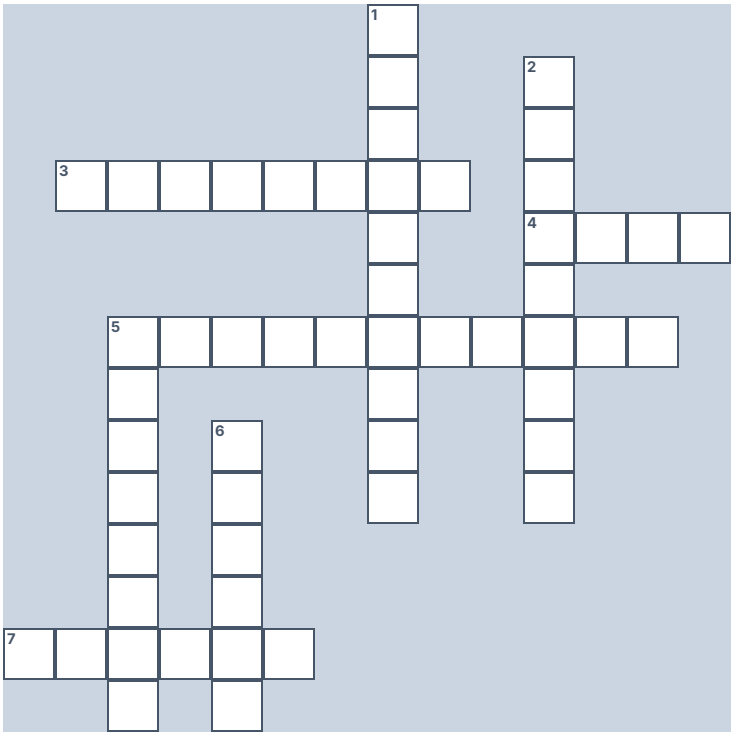
PÖRUN SKILGREININGA

Paraðu hvert hugtak til vinstri við rétta skilgreiningu til hægri með því að skrifa samsvarandi bókstaf (A-H) í útfyllanlega reitinn.

☐	1. INNSKRÁNINGARUPPLÝSINGAR	A	Aukastaðfestingarskref (til dæmis vélbúnaðarlyklar) sem ver innskráningu á reikninga.
☐	2. LEKAR	B	Að búa til falska vefsíðu eða tölvupóst sem líkir eftir lögmætri stofnun.
☐	3. MFA	C	Að takmarka aðgang að lánshæfisgögnum til að koma í veg fyrir sviksamlegar lánsumsóknir.
☐	4. VÖKTUN	D	Óheimil afhjúpun einkagagnagrunna sem innihalda persónuskrár notenda.
☐	5. FRYSTING	E	Þjálfun og tæknilegar varnir sem notaðar eru til að verjast auðkennisþjófnaði.
☐	6. VÖRN	F	Að senda sviksamleg skilaboð til að blekkja notendur til að gefa upp innskráningarupplýsingar.
☐	7. FÖLSUN	G	Að skanna spjallborð á netinu og rásir tölvuþrjóta eftir stolnum fyrirtækjagögnum.
☐	8. VEFVEIÐAR	H	Notandanöfn, lykilorð og einkatákn sem notuð eru til að auðkenna stafræn auðkenni.

Áfangi 5: Krossgáta

Leystu krossgátuna með því að slá stafi inn í virku hvítu reitina. Tölurnar vísa til vísbendinganna hér að neðan.



LÁRÉTT

3. Takmörkun á aðgangi að lánshæfisskrám til að koma í veg fyrir sviksamlegar lánsumsóknir (8)

4. Þjálfun og tæknilegar varnir sem notaðar eru til að verjast auðkennisþjófnaði (4)

5. Viðbótarstaðfestingarskref (t.d. vélbúnaðarlyklar) sem ver innskráningu á reikninga (11)

7. Leit á spjallborðum og rásum tölvuþrjóta að stolnum fyrirtækjagögnum (6)

LÓÐRÉTT

1. Óheimil birting einkagagnagrunna með persónuupplýsingum notenda (10)

2. Sending sviksamlegra skilaboða til að blekkja notendur til að gefa upp skilríki (9)

5. Notandanöfn, lykilorð og einkalyklar sem notuð eru til að auðkenna stafræn auðkenni (8)

6. Gerð falskrar vefsíðu eða tölvupósts sem líkir eftir lögmætri stofnun (6)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

Notendur skjálesara og lyklaborðs geta slegið svör krossgátunnar beint inn í textareitina hér að neðan.

LÁRÉTT

3 lárétt: Takmörkun á aðgangi að lánshæfisskrám til að koma í veg fyrir sviksamlegar lánsumsóknir (8 stafir):

4 lárétt: Þjálfun og tæknilegar varnir sem notaðar eru til að verjast auðkennisþjófnaði (4 stafir):

5 lárétt: Viðbótarstaðfestingarskref (t.d. vélbúnaðarlyklar) sem ver innskráningu á reikninga (11 stafir):

7 lárétt: Leit á spjallborðum og rásum tölvuþrjóta að stolnum fyrirtækjagögnum (6 stafir):

LÓÐRÉTT

1 lóðrétt: Óheimil birting einkagagnagrunna með persónuupplýsingum notenda (10 stafir):

2 lóðrétt: Sending sviksamlegra skilaboða til að blekkja notendur til að gefa upp skilríki (9 stafir):

5 lóðrétt: Notandanöfn, lykilorð og einkalyklar sem notuð eru til að auðkenna stafræn auðkenni (8 stafir):

6 lóðrétt: Gerð falskrar vefsíðu eða tölvupósts sem líkir eftir lögmætri stofnun (6 stafir):

Áfangi 6: Falið orð í orðaleit

Finndu 8 lykilhugtök sem eru falin í reitnum hér að neðan. Orð geta verið lárétt, lóðrétt eða á ská.

D S N I F N S F M P Ý R O D Ú
T U U E K Í B R A Á V B Ó Þ K
R J S Þ K Ý Ú Y J Đ Ö R M Í Đ
A I L N N K R S P G K M M R S
K T Ö Ú Ú S G T B T T P O V H
E T F B Y T Đ I U Æ U V D E Ö
L Y F J G A Ö N S Đ N N Đ F R
A Ý P B V Đ Á G K A Ö O Đ V K
N A Đ O Đ F É G I I Đ S R E M
G E I T Ö E V U L É R X É I A
A A R Ó N S Ö P R Ú Þ R J Đ S
G Ú T D N T R Æ Í B F T Ý A Y
Í A S Ö Æ I N Æ K K F I M R S
J L L U Ó N G P I R G Ö A O X
F V B Æ T G Æ Á G L Ö G J O P

ORÐALISTI

SKILRÍKI GAGNALEKAR STAÐFESTING VÖKTUN FRYSTING VÖRN FÖLSUN VEFVEIÐAR

Áfangi 6, valkostur: Aðgengileg orðaforðapörun

Paraðu hvert af hugtökunum 8 úr orðaleitinni við rétta skilgreiningu með því að skrifa bókstafinn (A-H) í eyðuna.

HUGTÖK
A. SKILRÍKI
B. GAGNALEKAR
C. STAÐFESTING
D. VÖKTUN
E. FRYSTING
F. VÖRN
G. FÖLSUN
H. VEFVEIÐAR

SKILGREININGAR OG PÖRUNARREITIR

1. Sending sviksamlegra skilaboða til að blekkja notendur til að gefa upp skilríki.
2. Notandanöfn, lykilorð og einkalyklar sem notuð eru til að auðkenna stafræn auðkenni.
3. Gerð falskrar vefsíðu eða tölvupósts sem líkir eftir lögmætri stofnun.
4. Þjálfun og tæknilegar varnir sem notaðar eru til að verjast auðkennisþjófnaði.
5. Leit á spjallborðum og rásum tölvuþrjóta að stolnum fyrirtækjagögnum.
6. Takmörkun á aðgangi að lánshæfisskrám til að koma í veg fyrir sviksamlegar lánsumsóknir.
7. Óheimil birting einkagagnagrunna með persónuupplýsingum notenda.
8. Viðbótarstaðfestingarskref (t.d. vélbúnaðarlyklar) sem ver innskráningu á reikninga.

Áfangi 7: Áskorun með ruglaðum orðum

Raðaðu stöfunum hér að neðan í rétta röð til að afhjúpa lykilhugtök um netöryggi. Skrifaðu svörin þín í reitina sem fylgja.

1. **KLRSÍKII** _____
2. **FGTSNEAITSÐ** _____
3. **SRFTIGNY** _____
4. **NSLUFÖ** _____
5. **KLRANEAGAG** _____
6. **UTVKNÖ** _____
7. **RVNÖ** _____
8. **REAVVEIÐF** _____

Aukaverkefni: Hugsaðu hratt

3 SVÖR Í HVERJUM FLOKKI. SÁ VINNUR SEM FYLLIR FYRST ÚT LISTANN.

1	Hlutir til að gera ef auðkenni þínu er stolið			
2	Hlutir sem ekki á að deila á samfélagsmiðlum			
3	Hlutir sem þú afritar			
4	Kort eða skilríki í veskinu þínu			
5	Skjöl sem þú ættir að vernda			
6	Hlutir til að gera eftir gagnaleka			
7	Ástæður fyrir því að uppfæra hugbúnað			
8	Upplýsingar sem persónuþjófur vill			
9	Tæki sem hægt er að brjótast inn í			
10	Staðir sem gögnin þín geta lekið frá			
11	Öruggar venjur sem þú getur byrjað á í dag			
12	Merki þess að tölva sé sýkt			
13	Leiðir til að sanna hver þú ert			
14	Merki um persónuþjófnað			
15	Viðvörunarmerki í tölvupósti			

Áfangi 8: Dæmisögur um netöryggi

Nýttu hugtökin sem þú hefur lært til að leysa raunveruleg dæmi hér að neðan.

DÆMISAGA 1: VERND GEGN ÞVÍ AÐ ÞYKJAST VERA YFIRSTJÓRNANDI



Aðstæður: Háttsettur stjórnandi hefur orðið fyrir árás með lénum með innsláttarvillum (typosquatting) sem herma eftir einkanetfangi hans til að svíkja viðskiptavini. Hannaðu vörumerkjaverndaráætlun.

Umræðuspurning: Greindu áhættu af vörumerkjahermun og lýstu SPF/DKIM/DMARC og auðkenningarstýringum í smáatriðum.

DÆMISAGA 2: INNSKRÁNINGARUPPLÝSINGAR FYRIRTÆKIS Á DJÚPVEFNUM



Aðstæður: Gagnagrunnsdump af myrkvefnum inniheldur nokkur hundruð fyrirtækjaauðkenni kerfisstjóra stórfyrirtækis. Hannaðu mótvægisáætlun.

Umræðuspurning: Lýstu hreinsunarferli auðkenna og skipuleggðu útbreiðslu lykilorðastjóra.

Áfangi 9: Leystu dulmálið

Netöryggissérfræðingur ver netkerfiseignir gegn ógnaraðilum á netinu. Notaðu lykilinn „bókstafur í tölu“ hér að neðan til að afkóða skilaboðin með því að skrifa samsvarandi bókstafi í auðu reitina.

DULMÁLSLYKILL: STAFIR Í TÖLUR

A=1 Á=2 B=3 C=4 D=5 Đ=6 E=7 É=8 F=9 G=10 H=11 I=12

Í=13 J=14 K=15 L=16 M=17 N=18 O=19 Ó=20 P=21 Q=22 R=23 S=24

T=25 U=26 Ú=27 V=28 W=29 X=30 Y=31 Ý=32 Z=33 Þ=34 Æ=35 Ö=36

28	7	23	18	5	1	6	26		1	26	6	15	7	18	18	12		17	7	6

9	14	36	16	34	2	25	25	1

24	25	1	6	9	7	24	25	12	18	10	26

Afkóðuð skilaboð:

ÁBENDING: HVER TALA STENDUR FYRIR STÖÐU STAFSINS Í STAFRÓFINU (T.D. 1 = A, 2 = B, 36 = Ö).

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti A)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q1: Hvað er persónuþjófnaður?

Glæpur þar sem árásaraðili stelur persónuupplýsingum (eins og lykilorðum eða kennitölum) til að þykjast vera einhver annar í fjárhagslegum ávinningi.

Q2: Hver er algengasta orsök persónuþjófnaðar?

Vefveiðar eru ein helsta leið þjófa til að komast yfir lykilorð, með því að lokka notendur á falskar, blekktar vefsíður.

Q3: Hvernig verndar fjölþátta auðkenning (MFA) auðkenni?

MFA krefst annarrar sönnunar (eins og vélbúnaðarlykils) til að skrá sig inn og stöðvar árásaraðila jafnvel þótt þeir steli lykilorðinu þínu.

Q4: Hvað er lánsfrysting (credit freeze)?

Ókeypis þjónusta sem hindrar lánshæfisfyrirtæki í að deila lánshæfisskrá þinni og stöðvar þjófa í að stofna ný lán í þínu nafni. [2]

Q5: Hvað er vöktun á hulduvefnum?

Hugbúnaður sem skoðar tölvuþrjótaspjallborð að lekum netföngum, lykilorðum og persónuskrám og lætur þig vita ef gögnin þín eru berskjölduð.

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti B)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q6: Hvað þýðir credential stuffing (innskráningarfylling)?

Sjálfvirk vélmenni sem prófa lekna lykilorðalista á hundruðum vefsvæða til að taka yfir virka reikninga.

Q7: Hvers vegna er fölsun tölvupóstfangs hættuleg?

Það gerir árásaraðilum kleift að falsa nafn sendanda í tölvupósti þannig að vefveiðaskilaboð virðast koma frá traustum samstarfsmönnum.

Q8: Hvernig koma lykilorðastjórar í veg fyrir auðkennisþjófnað?

Þeir geyma flókin, einkvæm lykilorð fyrir hvern aðgang og neita að fylla sjálfkrafa inn auðkenni á fölskum vefveiðilénum.

Q9: Hvað eru markvissar vefveiðar (spear phishing)?

Mjög markviss vefveiðaárás sem er sniðin að nafni og upplýsingum fórnarlambsins til að auka líkur á blekkingu.

Q10: Hvernig er lánshæfisviðvörun frábrugðin lánshæfisfrystingu?

Viðvörun lætur lánveitendur staðfesta auðkenni þitt áður en reikningar eru stofnaðir, en frysting lokar alfarið á aðgang að lánshæfisskrá þinni. [2]

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti C)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q1: Hvernig leiðir SIM-skipti til persónuþjófnaðar?

Árásarmenn sannfæra starfsfólk símafyrirtækis um að færa símanúmer fórnarlambsins yfir á nýtt SIM-kort og ræna þannig SMS-kóðum fyrir 2FA.

Q2: Hvert er hlutverk DMARC í að koma í veg fyrir persónuþjófnað?

DMARC gerir lénseigendum kleift að hindra að falsaður tölvupóstur berist í pósthólf og kemur þannig í veg fyrir að falspóstur líki eftir fyrirtækjalénum.

Q3: Hvers vegna er erfitt að greina auðkennisþjófnað með tilbúnum auðkennum?

Þjófar sameina raunveruleg kennitölunúmer (SSN) við fölsk nöfn og fæðingardaga til að byggja upp glænýja lánshæfissnið og komast framhjá grunnviðvörunum um svik.

Q4: Hvernig misnota gagnamiðlarar persónuauðkenni?

Miðlarar safna opinberum skrám, vefhegðun og kaupsögu til að setja saman persónusnið, sem getur lekið eða verið seld.

Q5: Hvers vegna telst SMS-byggð MFA viðkvæm?

SMS-umferð er berskjölduð fyrir hlerun, vefveiðum og SIM-skiptaárásum á stigi símafyrirtækja.

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti D)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q6: Hvað er lánaskrárlæsing (credit file lock)?

Viðskiptaleg þjónusta svipuð frystingu sem gerir notendum kleift að opna eða læsa lánshæfisskrá sína samstundis í gegnum snjallforrit.

Q7: Hvernig ýta gagnaleki hjá fyrirtækjum undir auðkennisþjófnað?

Lekinn gagnagrunnur afhjúpar milljónir ódulkóðaðra innskráningarupplýsinga og gefur þjófum hráu gögnin sem þarf til að fremja markvisst persónuþjófnaðarsvik.

Q8: Hver er áhættan af því að deila of miklu á samfélagsmiðlum?

Að deila opinberlega nöfnum gæludýra, fæðingarstöðum og stúlknanafni móður veitir þjófum svörin við algengum spurningum til endurheimtar reikninga.

Q9: Hvernig vernda lífkennainnskráningar auðkenni?

Lífkenni tengja innskráningar við eiginleika eins og fingraför eða andlit; séu þau geymd á tækinu er erfitt að stela þeim, en geymd lífkennigögn geta lekið.

Q10: Hvernig vinnur Red Flags Rule gegn persónuþjófnaði?

Alríkisreglugerð sem krefst þess að fjármálastofnanir þrói skrifleg áætlun um að greina og bregðast við viðvörunarmerkjum um persónuþjófnað.

Hluti 11: 10 staðreyndir um netöryggi og innsýn úr raunheimum

Farðu yfir raunverulegar staðreyndir um öryggisbrot, varnarkerfi og reglufylgnistaðla.

1. INNSÝN Í ÖRYGGI

IdentityTheft.gov, rekið af FTC, gerir fórnarlömbum í Bandaríkjunum kleift að tilkynna auðkennisþjófnað og fá persónulega endurheimtaráætlun. [1]

2. INNSÝN Í ÖRYGGI

Öryggislyklar úr vélbúnaði eru fjölþátta auðkenning (MFA) sem stenst vefveiðar, sterkasta tegund MFA sem CISA hvetur til. [4]

3. INNSÝN Í ÖRYGGI

Lykilorð í hættu eru algeng inngönguleið við gagnaleka og ýta undir síðari persónuþjófnað.

4. INNSÝN Í ÖRYGGI

Lánshæfisfrysting er ókeypis samkvæmt alríkislögum og kemur í veg fyrir að lánveitendur skoði lánshæfisskrár þar til hún er opnuð. [2]

5. INNSÝN Í ÖRYGGI

DMARC gerir lénseigendum kleift að segja póstþjónum að hafna eða setja í sóttkví fölsuðum tölvupósti sem stenst ekki athuganir. [7]

6. INNSÝN Í ÖRYGGI

SIM-skipti gera tölvuþrjótum kleift að sniðganga SMS-byggða tvíþátta auðkenningu á bankagáttum.

7. ÖRYGGISINNSÝN

Svik með tilbúin auðkenni blanda saman raunverulegum og fölskum upplýsingum, sem gerir lánveitendum erfitt að greina þau.

8. ÖRYGGISINNSÝN

Margir nota sama lykilorðið á mörgum netreikningum, svo að einn öryggisbrestur getur afhjúpað nokkra þeirra.

9. ÖRYGGISINNSÝN

Gagnamiðlarar safna ítarlegum upplýsingum um mikinn fjölda neytenda, sem skapar samþjappaða hættu fyrir persónuvernd.

10. INNSÝN Í ÖRYGGI

Það getur tekið marga mánuði að jafna sig eftir persónuþjófnað, svo sem að mótmæla gjöldum og laga lánshæfisskýrslur.

Tæknilegar heimildir og tilvísanir

Námsleiðbeiningarnar og gagnvirku þrautirnar eru unnar úr alþjóðlegum stöðlum NIST og OWASP og kröfum um persónuverndarsamræmi.

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[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

Lausnir: Áfangi 1 – Fjölval

1 **Spurning 1** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hver er helsta leið sem auðkennisþjófar nota til að stela innskráningargögnum? → Að senda fölsk viðvörunarskilaboð í tölvupósti sem blekkja notendur til að slá inn lykilorð á falsaðri gátt

2 **Spurning 2** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvaða öryggisstýring veitir öflugustu vörnina gegn leka innskráningargagna? → Fjölþátta auðkenning með vélbúnaðarlyklum

3 **Spurning 3** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað táknar frysting lánshæfis? → Að læsa lánshæfisskýrslum til að koma í veg fyrir að þjófar stofni óheimil lán

4 **Spurning 4** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvers vegna er vöktun á dökkvefnum gagnleg? → Það lætur notendur vita ef lekin auðkenni þeirra birtast í ólöglegum gagnagrunnum

5 **Spurning 5** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað merkir félagsleg misnotkun (social engineering)? → Að hagræða fólki til að gefa sjálfviljugt upp trúnaðarauðkenni

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Spurning 6** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Persónuþjófnaður getur einnig byrjað utan nets, til dæmis með stolnum pósti eða skjölum.

7 **Spurning 7** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Að framfylgja MFA á öllum persónulegum reikningum hindrar flestar þrjótaárásir sem prófa stolin lykilorð (credential stuffing).

8 **Spurning 8** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Lánshæfisfrysting stöðvar nýjar lánshæfisfyrirspurnir en hefur ekki áhrif á núverandi reikninga þína.

9 **Spurning 9** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Lykilorðastjórar vernda notendur gegn vefveiðum með því að neita að fylla sjálfkrafa út lykilorð á fölsuðum lénum.

10 **Spurning 10** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Vefveiðapóstar nota oft áríðandi orðalag til að kalla fram tilfinningaleg og fljótfærnisleg viðbrögð.

Orðalyklar og matskvarði

Einkunnaviðmið kennara: Gefðu 1 stig fyrir hverja rétta pörun (alls 8 stig) og hvert samhengishugtak (alls 6 stig).

ÁFANGI 4: LAUSNIR – PÖRUN HUGTAKA

H 1. INNSKRÁNINGARUPPLÝSINGAR	D 2. LEKAR	A 3. MFA	G 4. VÖKTUN
C 5. FRYSTING	E 6. VÖRN	B 7. FÖLSUN	F 8. VEFVEIÐAR

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 SKILRÍKI	2 GAGNALEKAR	3 STAÐFESTING	4 VÖKTUN
5 FRYSTING	6 VÖRN		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 H – VEFVEIÐAR	2 A – SKILRÍKI	3 G – FÖLSUN	4 F – VÖRN
5 D – VÖKTUN	6 E – FRYSTING	7 B – GAGNALEKAR	8 C – STAÐFESTING

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt INNSKRÁNINGARUPPLÝSINGAR, LEKAR og MFA með eigin orðum og gefið dæmi um hvert hugtak.

Dæmisögur:
Biddu nemendur að styðja tillögur sínar með staðreyndum úr verkefnablaðinu en ekki ágiskunum.

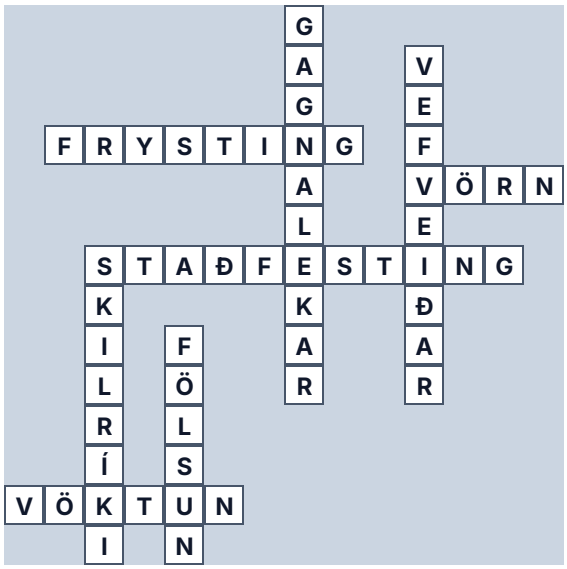
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

D	S	N	I	F	N	S	F	M	P	Ý	R	O	D	Ú
T	U	U	E	K	Í	B	R	A	Á	V	B	Ó	Þ	K
R	J	S	Þ	K	Ý	Ú	Y	J	Đ	Ö	R	M	Í	Đ
A	I	L	N	N	K	R	S	P	G	K	M	M	R	S
K	T	Ö	Ú	Ú	S	G	T	B	T	T	P	O	V	H
E	T	F	B	Y	T	Đ	I	U	Æ	U	V	D	E	Ö
L	Y	F	J	G	A	Ö	N	S	Đ	N	N	Đ	F	R
A	Ý	P	B	V	Đ	Á	G	K	A	Ö	O	Đ	V	K
N	A	Đ	O	Đ	F	É	G	I	I	Đ	S	R	E	M
G	E	I	T	Ö	E	V	U	L	É	R	X	É	I	A
A	A	R	Ó	N	S	Ö	P	R	Ú	Þ	R	J	Đ	S
G	Ú	T	D	N	T	R	Æ	Í	B	F	T	Ý	A	Y
Í	A	S	Ö	Æ	I	N	Æ	K	K	F	I	M	R	S
J	L	L	U	Ó	N	G	P	I	R	G	Ö	A	O	X
F	V	B	Æ	T	G	Æ	Á	G	L	Ö	G	J	O	P

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

3 lárétt: FRYSTING Takmörkun á aðgangi að lánshæfisskrám til að koma í veg fyrir sviksamlegar lánsumsóknir (8 stafir)

4 lárétt: VÖRN Þjálfun og tæknilegar varnir sem notaðar eru til að verjast auðkennisþjófnaði (4 stafir)

5 lárétt: STAÐFESTING Viðbótarstaðfestingarskref (t.d. vélbúnaðarlyklar) sem ver innskráningu á reikninga (11 stafir)

7 lárétt: VÖKTUN Leit á spjallborðum og rásum tölvuþrjóta að stolnum fyrirtækjagögnum (6 stafir)

LÓÐRÉTT

1 lóðrétt: GAGNALEKAR Óheimil birting einkagagnagrunna með persónuupplýsingum notenda (10 stafir)

2 lóðrétt: VEFVEIÐAR Sending sviksamlegra skilaboða til að blekkja notendur til að gefa upp skilríki (9 stafir)

5 lóðrétt: SKILRÍKI Notandanöfn, lykilorð og einkalyklar sem notuð eru til að auðkenna stafræn auðkenni (8 stafir)

6 lóðrétt: FÖLSUN Gerð falskrar vefsíðu eða tölvupósts sem líkir eftir lögmætri stofnun (6 stafir)

Lausnir: Stafaruglingur og dulmál

Lausnalykill fyrir virkni um að raða orðaforða og Secret Cipher Challenge.

LYKILL ORÐARAÐAR

1. KLRSÍKII	SKILRÍKI	5. KLRANEAGAG	GAGNALEKAR
2. FGTSNEAITSÐ	STAÐFESTING	6. UTVKNÖ	VÖKTUN
3. SRFTIGNY	FRYSTING	7. RVNÖ	VÖRN
4. NSLUFÖ	FÖLSUN	8. REAVVEIÐF	VEFVEIÐAR

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"VERNDAÐU AUÐKENNI MEÐ FJÖLÞÁTTA STAÐFESTINGU"

Lausnir dæmisagna

A Dæmisaga 1: Vernd gegn því að þykjast vera yfirstjórnandi

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Háttsettur æðsti stjórnandi hefur orðið skotmark léna með innsláttarvillum sem líkja eftir persónulegu netfangi hans til að svíkja viðskiptavini. Hannaðu vörumerkjaverndaráætlun.
- Ráðlögð aðferð og lausn: Skráðu öll algeng stafsetningarafbrigði af nafni stjórnandans. Innleiddu auðkenningarreglur fyrir tölvupóst (DMARC, DKIM, SPF) til að koma í veg fyrir fölsun léns. Framfylgdu vélbúnaðar-MFA á allar innskráningar æðstu stjórnenda fyrirtækisins.

B Dæmisaga 2: Innskráningarupplýsingar fyrirtækis á djúpvefnum

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Gagnahrúga af myrkravefnum inniheldur nokkur hundruð fyrirtækjaauðkenni sem tilheyra kerfisstjórum stórfyrirtækis. Hannaðu aðgerðaáætlun til úrbóta.
- Ráðlögð aðferð og lausn: Framkvæmdu endurstillingu lykilorða um allt fyrirtækið. Gerðu notkun lykilorðastjóra fyrir fyrirtæki skyldubundna. Framfylgdu MFA á öllum kerfisgáttum og settu upp stöðugar sjálfvirkar viðvaranir um vöktun á hulduvefnum.