Nafn: _____ Dagsetning: _____ Stig: _____

Vefveiðaárásir og félagsleg hjálparbrögð

Spear phishing, whaling-svik, SPF/DKIM/DMARC-samskiptareglur, fölsun sendanda og öryggisþjálfun starfsmanna.

YFIRLIT UM NÁMSEFNI UM VEFVEIÐAR

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 vefveiðar og félagsverkfræði (social engineering). Þú munt kynnast spjótvefveiðum (spear phishing), hvalveiðum (whaling), lénafölsun, SPF/DKIM/DMARC-samskiptareglum, öryggi tengla og þjálfun starfsfólks í árvekni.

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/netoryggd/vefveiararasir/

Námsvegvísir þinn: varnir gegn vefveiðum

- Greindu algeng svik með vefveiðum, raddveiðum og sprettiglugga um tækniaðstoð.
- Innleiddu verklag til að staðfesta færslur eftir óháðri leið (out-of-band).
- Stilltu SPF-, DKIM- og DMARC-reglur til að loka á fölsuð lén.

LEIÐBEININGAR UM VEFVEIÐAR

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

VEFVEIÐAR OG FÉLAGSLEG HJÁLPARBRÖGÐ (INNGANGUR)

Vefveiðaárásir nota markvissar skilaboð, hvalveiðasvik (whaling) og lénablekkingar til að safna innskráningarupplýsingum notenda. Til að tryggja fyrirtækjakerfi þarf að setja upp SPF-, DKIM- og DMARC-reglur við hlið netsins ásamt samþykktarskrefum eftir óháðri leið.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hvað eru markvissar vefveiðar (spear phishing)?**

- A. Markviss vefveiðapóstur sniðinn að tilteknum einstaklingi eða stofnun
- B. Víðtækur fjöldapóstur sendur á milljónir tilviljanakenndra netfanga
- C. Netárás sem flæðir yfir vefþjóna með umferð
- D. Gagnaúrdráttartækni sem beinist að notendafærslum

2 **2. Hvaða samskiptaregla gerir léni kleift að skrá leyfð sendandi IP-vistföng í DNS til að berjast gegn skopstælingu?**

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

3 **3. Hvað er hvalveiðiárás (whaling)?**

- A. Vefveiðaherferð sem beinist sérstaklega að áberandi æðstu stjórnendum fyrirtækja
- B. SQL-innspýtingarárás sem beinist að gagnagrunnsafritum
- C. Líkamlegur þjófnaður á beinabúnaði staðarnets
- D. Sjálfvirk brute-force-skönnun með innskráningarfyllingu

4 **4. Hvað gerir DKIM?**

- A. Bætir dulritunarundirskrift við tölvupóst til að staðfesta áreiðanleika sendanda
- B. Lokar fyrir komandi netpakkaumferð í eldveggnum
- C. Dulkóðar gagnagrunnsgeymslur í hvíld
- D. Skannar viðhengi í tölvupósti eftir spilliforriti með undirskriftum

5 **5. Hvert er hlutverk DMARC?**

- A. Að leiðbeina móttökupóstþjónum um hvernig á að meðhöndla misheppnaðar SPF/DKIM-athuganir
- B. Að afkóða kerfislykilorð með fyrirframreiknuðum regnbogatöflum
- C. Að þjappa tölvupóstviðhengjum fyrir afhendingu
- D. Að stilla aðgangsréttindi að netleiðum

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. Spear phishing byggir á almennum fjölpósti sem sendur er til milljóna tilviljanakenndra netfanga.

Satt Ósatt

7 Spurning 7

7. DMARC-stefnur geta lagt fyrir póstþjóna að hafna óheimiluðum fölsuðum skilaboðum.

Satt Ósatt

8 Spurning 8

8. SPF-staðfesting virkar með því að sannreyna dulritunarundirskrift meginmáls tölvupóstsins.

Satt Ósatt

9 Spurning 9

9. Hvalveiðiárásir beinast að lægra settum kerfisstjórum fyrirtækja til að komast í gagnagrunnsskrár.

Satt Ósatt

10 Spurning 10

10. Staðfesting greiðslubeiðna utan upphaflegu rásarinnar hjálpar til við að stöðva svik með millifærslum.

Satt Ósatt

Áfangi 3: Lykilhugtök fyllt inn

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

1. Að beina spjótum að tilteknum starfsmanni með persónulegum upplýsingum kallast _____ .

2. Að falsa haus tölvupósts svo skilaboðin virðist lögmæt kallast _____ á sendanda.

3. DNS-færslan sem skráir IP-tölur heimilaðra póstþjóna er _____ .

4. Undirskriftarstaðall tölvupósts sem staðfestir sendanda er _____ .

5. Að setja stefnur sem hafna pósti sem fellur á SPF/DKIM athugunum byggir á _____ .

6. Vefveiðaherferð sem beinist að framkvæmdastjórum í æðstu stöðum kallast _____ .

ORÐABANKI

DKIM DMARC FÖLSUN HVALAVEIÐAR RADDVEIÐAR SMS-SVIK SPF-FÆRSLA SPJÓTVEIÐAR

Skrifaðu svörin þín hér:

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

Áfangi 4: Pörun hugtaka um öryggi

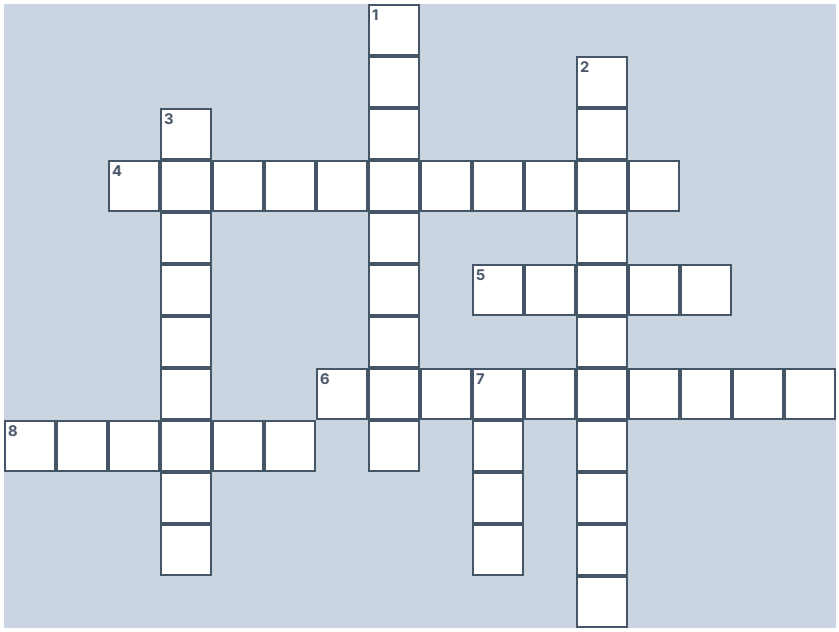
PÖRUN SKILGREININGA

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

☐	1. SPJÓT	A	Svikasímtöl í gegnum síma.
☐	2. FÖLSUN	B	Beinist að æðstu stjórnendum (C-level).
☐	3. SPF	C	Leiðbeiningar um höfnun samkvæmt stefnu.
☐	4. DKIM	D	IP-tölur sendenda sem DNS heimilar.
☐	5. DMARC	E	Tölvupóstur með félagslegri hagræðingu (social engineering).
☐	6. HVALVEIÐAR	F	Sérsniðinn markpóstur.
☐	7. VEFVEIÐAR	G	Fölsun netfangs sendanda.
☐	8. RADDVEIÐAR	H	Dulritunarundirskrift í tölvupósti.

Áfangi 5: Krossgáta

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



LÁRÉTT

4. Sérsniðinn, markvissur tölvupóstur (11)

5. Stefna um fyrirmæli um höfnun (5)

6. Svikasímtöl byggð á rödd (10)

8. Fölsun á netfangi sendanda (6)

LÓÐRÉTT

1. Félagsleg verkfræði með tölvupósti (9)

2. Markvissar veiðar á framkvæmdastjórum í æðstu stöðum (11)

3. DNS-færsla með leyfðum IP-tölum sendenda (9)

7. Dulmálsundirskrift í tölvupósti (4)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

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

LÁRÉTT

4 lárétt: Sérsniðinn, markvissur tölvupóstur (11 stafir):

5 lárétt: Stefna um fyrirmæli um höfnun (5 stafir):

6 lárétt: Svikasímtöl byggð á rödd (10 stafir):

8 lárétt: Fölsun á netfangi sendanda (6 stafir):

LÓÐRÉTT

1 lóðrétt: Félagsleg verkfræði með tölvupósti (9 stafir):

2 lóðrétt: Markvissar veiðar á framkvæmdastjórum í æðstu stöðum (11 stafir):

3 lóðrétt: DNS-færsla með leyfðum IP-tölum sendenda (9 stafir):

7 lóðrétt: Dulmálsundirskrift í tölvupósti (4 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 I F N S M V P Ý R O D Ú T

R U C E K Í B E A Á F B Ó Þ K

A J R Þ K Ý Ú F J Ð Ö R M Í Ð

Ð I A N N K R V P G L M M R S

I T M Ú Ú S G E B T S P O R H

E T D B Y P Ð I U Æ U V D A Ö

V Y F J G J Ö Ð S Ð N N Ð D R

A Ý P B V Ó Á A P A Ö O Ð D K

L A Ð O Ð T É R F G I Ð S V R

A M E I T V D Ö F U É R X E É

V A A R Ó E K N Æ P Ú Þ R I J

H S Ú T D I I N R Æ B F T Ð Ý

Y Í A S Ö Ð M Æ S Æ K F I A M

S J L L U A Ó G L P R G Ö R A

O X F V B R Æ T A Æ Á G L Ö G

ORÐALISTI

SPJÓTVEIÐAR FÖLSUN SPFFÆRSLA DKIM DMARC HVALAVEIÐAR VEFVEIÐAR RADDVEIÐAR

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	SKILGREININGAR OG PÖRUNARREITIR
A. SPJÓTVEIÐAR	_____ 1. Fölsun á netfangi sendanda.
B. FÖLSUN	_____ 2. Sérsniðinn, markvissur tölvupóstur.
C. SPFFÆRSLA	_____ 3. Svikasímtöl byggð á rödd.
D. DKIM	_____ 4. DNS-færsla með leyfðum IP-tölum sendenda.
E. DMARC	_____ 5. Félagsleg verkfræði með tölvupósti.
F. HVALAVEIÐAR	_____ 6. Stefna um fyrirmæli um höfnun.
G. VEFVEIÐAR	_____ 7. Dulmálsundirskrift í tölvupósti.
H. RADDVEIÐAR	_____ 8. Markvissar veiðar á framkvæmdastjórum í æðstu stöðum.

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. TEAPVISÐJRÓ

2. ASLFPRSÆF

3. ADCRM

4. ERAVÐIVEF

5. SLNFUÖ

6. IMDK

7. IAHVERÐAAVL

8. ADERRVAIÐD

Aukaverkefni: Hugsaðu hratt

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

1	Tæki sem hægt er að brjótast inn í			
2	Merki um vefveiðapóst			
3	Merki þess að tölva sé sýkt			
4	Orð sem skapa falskan flýti			
5	Leiðir til að kanna sendanda			
6	Fólk sem þú getur leitað til varðandi upplýsingatæknihjálp			
7	Hlutir sem þú afritar			
8	Fiskar eða sjávardýr sem þú þekkir			
9	Fyrirtæki sem svikarar þykjast vera			
10	Öruggar venjur sem þú getur byrjað á í dag			
11	Hlutir til að gera eftir að hafa smellt á falskan tengil			
12	Hlutir til að gera eftir gagnaleka			
13	Rásir þar sem vefveiðar eiga sér stað			
14	Hlutir sem þú sendir aldrei í tölvupósti			
15	Leiðir til að vernda reikningana þína			

Áfangi 8: Dæmisögur um netöryggi

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

DÆMISAGA 1: VIÐBRÖGÐ VIÐ HVALVEIÐAÁRÁS Á YFIRSTJÓRNENDUR



Aðstæður: Fjármálastjóri fær mjög persónulegan tölvupóst sem segist vera frá forstjóranum og óskar eftir skjótri $50,000 millifærslu til að ljúka trúnaðarlénakaupum.

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

DÆMISAGA 2: INNLEIÐING SPF/DKIM/DMARC-STEFNA Á GÁTT



Aðstæður: Stórfyrirtæki fellur á öryggisúttektum vegna þess að útsendir markaðspóstar eru oft merktir sem ruslpóstur og tölvuþrjótar skopstæla virkt vörumerkjalén fyrirtækisins.

Umræðuspurning: Mótaðu tæknilegar og stjórnunarlegar stýringar til að sannreyna áreiðanleika tölvupósts.

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

10	23	7	12	18	5	26

9	8	16	1	10	24	28	7	23	15	9	23	35	6	12	17	7	6

27	25	25	7	15	25	21	20	24	25	10	2	25	25	1

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 eru vefveiðar?

Vefveiðar eru árás með félagslegum hjálparbrögðum þar sem glæpamenn senda svikin skilaboð til að blekkja notendur til að gefa upp viðkvæm gögn.

Q2: Hver er munurinn á vefveiðum og markvissum vefveiðum?

Vefveiðar beinast að breiðum hópum með almennu efni, en markvissar vefveiðar beinast að tilteknum fórnarlömbum með sérsniðnum upplýsingum.

Q3: Hvað er whaling?

Hvalveiðar (whaling) eru mjög markviss vefveiðaárás gegn áberandi stjórnendum sem hafa stjórnunarvald.

Q4: Hvað er fölsun tölvupóstfangs (email spoofing)?

Fölsun tölvupósts er það þegar tölvupóstskeyti eru búin til með falsað sendanetfang til að fá viðtakandann til að treysta upprunanum.

Q5: Hvernig kemur SPF í veg fyrir fölsun?

Það birtir lista yfir heimilar sendi-IP-tölur í DNS, sem gerir móttökunetþjónum kleift að staðfesta uppruna póstsins. [1]

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

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q6: Hvað er DKIM?

DomainKeys Identified Mail bætir dulritunarundirskrift við tölvupósthausa, sem sannar að lén tók ábyrgð og að skilaboðunum var ekki breytt.

Q7: Fyrir hvað stendur DMARC?

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

Q8: Hvað er DMARC-stefna?

Stefna sem segir póstþjónum hvernig meðhöndla á skilaboð sem falla á SPF/DKIM (none, quarantine eða reject). [2]

Q9: Hvað er vishing (símasvik)?

Símavefveiðar (vishing), þar sem árásaraðilar nota svikasímtöl til að fá stjórnunar- eða fjárhagsupplýsingar.

Q10: Hvernig hjálpa tengilsskannar?

Þeir skanna og endurskrifa tengla í innkomnum tölvupósti til að sannreyna öryggi áfangastaðarvefsíðna þegar smellt er.

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

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q1: Hvernig virkar samlíkingaárás (homograph attack)?

Árásarmenn skrá lén með líkum Unicode-stöfum utan ASCII til að líkja sjónrænt eftir lögmætu léni.

Q2: Hvað er punycode-framsetning?

Kóðun sem breytir Unicode-lénsheitum í ASCII-samhæfðar strengi sem byrja á „xn--“ svo DNS ráði við þau.

Q3: Hvers vegna er „p=reject“ öruggasta DMARC-stillingin?

Það biður móttökunetþjóna að hafna pósti sem stenst ekki DMARC (samræmt SPF/DKIM) meðan á SMTP-lotunni stendur, sem kemur í veg fyrir beina fölsun. [2]

Q4: Hvernig komast árásaraðilar framhjá SPF-reglum?

Með því að nýta lík lén (typosquatting) eða nota yfirtekna reikninga hjá lögmætum tölvupóstþjónustum þriðja aðila.

Q5: Hvað er viðskiptapóstsvik (BEC)?

Svik gegn fyrirtækjum þar sem árásaraðilar yfirtaka eða herma eftir tölvupóstreikningum fyrirtækja til að heimila sviksamlegar greiðslur.

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

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q6: Hvernig stöðvar fjölþátta auðkenning vefveiðar?

Það krefst auka lykla (eins og vélbúnaðarlykla) sem ekki er hægt að stela eingöngu með eftirlíkingarvefsíðum.

Q7: Hvað er lendingarsíða sem safnar innskráningarupplýsingum?

Eftirlíkt innskráningarsvæði sem er hannað til að ná notendanöfnum, lykilorðum og MFA-táknum í rauntíma.

Q8: Hvað er rán undirléna (subdomain hijacking)?

Árásaraðili tekur yfir ónotaðan DNS-undirlénsvísi til að hýsa skaðlegar vefveiðalendingarsíður undir traustu yfirléni.

Q9: Hvernig virkar athugun á DKIM-samræmingu (alignment)?

Það staðfestir að lénið í 'From' hausnum passi við lénið sem undirritaði skilaboðin dulritunarlega í DKIM-hausnum.

Q10: Hvert er hlutverk tölvupóstgáttar?

Síun á innkomnum tölvupósti, úttekt á tenglum, einangrun viðhengja í sandbox og sannprófun á SPF/DKIM/DMARC-reglufylgni.

Hluti 11: 10 staðreyndir um netöryggi og innsýn úr raunheimum

Farðu yfir raunverulegar staðreyndir um öryggisbrot, varnarkerfi og reglufylgnistaðla.

1. INNSÝN Í ÖRYGGI

Vefveiðar og blekkingar voru algengasta glæpategundin sem tilkynnt var til IC3 hjá FBI árið 2025, með 191.561 kvörtun. [4]

2. INNSÝN Í ÖRYGGI

Viðskiptapóstsvik (BEC) ollu yfir 3 milljarða dollara tjóni sem tilkynnt var til IC3 hjá FBI árið 2025. [4]

3. INNSÝN Í ÖRYGGI

Samlíkingarárásir nota kyrillíska stafi sem líkjast latneskum til að líkja sjónrænt eftir lénum sem passa nákvæmlega við vörumerki í vöfrum.

4. INNSÝN Í ÖRYGGI

Með „p=reject“ biður lén móttakendur um að hafna pósti sem stenst ekki prófun við afhendingu, ekki að skrá hann sem ruslpóst. [2]

5. INNSÝN Í ÖRYGGI

Hvalveiðiárásir sem beinast að forstjórum biðja oft um áríðandi greiðslur vegna trúnaðarmála í samrunum eða lénakaupum.

6. INNSÝN Í ÖRYGGI

Vefveiðagáttir til innskráningarupplýsingasöfnunar afrita raunverulegar innskráningarsíður þannig að fórnarlömb slá lykilorð beint inn í eyðublað árásaraðilans.

7. ÖRYGGISINNSÝN

Sameiginlegar leiðbeiningar CISA um vefveiðar mæla með þjálfun notenda ásamt DMARC, SPF, DKIM og vefveiðaþolinni MFA. [3]

8. ÖRYGGISINNSÝN

SPF-mat er takmarkað við 10 liði sem senda DNS-fyrirspurnir; ef farið er yfir mörkin skilar það niðurstöðunni 'permerror'. [1]

9. ÖRYGGISINNSÝN

FIDO2 vélbúnaðaröryggislyklar veita dulritunarlega studda vernd gegn fjarsöfnun innskráningarupplýsinga.

10. INNSÝN Í ÖRYGGI

Vefveiðar eru ein algengasta leið árásaraðila til að komast fyrst inn í stofnun, og þess vegna er regluleg fræðsla til vitundar áhrifarík vörn.

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] 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

Lausnir: Áfangi 1 – Fjölval

1 **Spurning 1** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað eru markvissar vefveiðar (spear phishing)? → Markviss vefveiðapóstur sniðinn að tilteknum einstaklingi eða stofnun

2 **Spurning 2** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

SPF birtir leyfða sendandi hýsla léns í DNS svo viðtakendur geti athugað sendanda umslagsins.

3 **Spurning 3** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað er hvalveiðiárás (whaling)? → Vefveiðaherferð sem beinist sérstaklega að áberandi æðstu stjórnendum fyrirtækja

4 **Spurning 4** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað gerir DKIM? → Bætir dulritunarundirskrift við tölvupóst til að staðfesta áreiðanleika sendanda

5 **Spurning 5** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvert er hlutverk DMARC? → Að leiðbeina móttökupóstþjónum um hvernig á að meðhöndla misheppnaðar SPF/DKIM-athuganir

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Spurning 6** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: spjótvefveiðar eru sniðnar að tilteknu fólki, ólíkt almennum fjölpóstsvefveiðum.

7 **Spurning 7** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

DMARC-stefnur geta lagt fyrir póstþjóna að hafna óheimiluðum fölsuðum skilaboðum.

8 **Spurning 8** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: SPF ber sendandi IP-tölu saman við DNS; DKIM er það sem staðfestir dulritaða undirskrift.

9 **Spurning 9** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: „whaling“ beinist að æðstu stjórnendum, sem geta samþykkt greiðslur og fengið aðgang að viðkvæmum gögnum.

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

ATHUGASEMD FYRIR KENNARA

Satt: að staðfesta greiðslubeiðnir í gegnum sérstaka, þekkta rás hjálpar til við að stöðva svik með millifærslum.

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

F 1. SPJÓT	G 2. FÖLSUN	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. HVALVEIÐAR	E 7. VEFVEIÐAR	A 8. RADDVEIÐAR

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 SPJÓTVEIÐAR	2 FÖLSUN	3 SPF-FÆRSLA	4 DKIM
5 DMARC	6 HVALAVEIÐAR		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 B – FÖLSUN	2 A – SPJÓTVEIÐAR	3 H – RADDVEIÐAR	4 C – SPFFÆRSLA
5 G – VEFVEIÐAR	6 E – DMARC	7 D – DKIM	8 F – HVALAVEIÐAR

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt SPJÓT, FÖLSUN og SPF með eigin orðum og gefið dæmi um hvert hugtak.

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

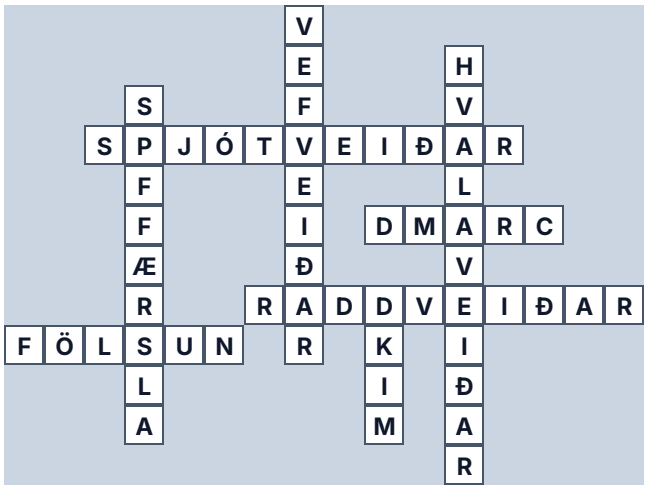
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

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

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

4 lárétt: SPJÓTVEIÐAR Sérsniðinn, markvissur tölvupóstur (11 stafir)

5 lárétt: DMARC Stefna um fyrirmæli um höfnun (5 stafir)

6 lárétt: RADDVEIÐAR Svikasímtöl byggð á rödd (10 stafir)

8 lárétt: FÖLSUN Fölsun á netfangi sendanda (6 stafir)

LÓÐRÉTT

1 lóðrétt: VEFVEIÐAR Félagsleg verkfræði með tölvupósti (9 stafir)

2 lóðrétt: HVALAVEIÐAR Markvissar veiðar á framkvæmdastjórum í æðstu stöðum (11 stafir)

3 lóðrétt: SPFFÆRSLA DNS-færsla með leyfðum IP-tölum sendenda (9 stafir)

7 lóðrétt: DKIM Dulmálsundirskrift í tölvupósti (4 stafir)

Lausnir: Stafaruglingur og dulmál

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

LYKILL ORÐARAÐAR

1. T E A P V I S Ð J R Ó — **SPJÓTVEIÐAR**
2. A S L F P R S Æ F — **SPFFÆRSLA**
3. A D C R M — **DMARC**
4. E R A V Ð I V E F — **VEFVEIÐAR**
5. S L N F U Ö — **FÖLSUN**
6. I M D K — **DKIM**
7. I A H V E R Ð A A V L — **HVALAVEIÐAR**
8. A D E R R V A I Ð D — **RADDVEIÐAR**

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"GREINDU FÉLAGSVERKFRÆÐI MEÐ ÚTTEKT PÓSTGÁTTA"

Lausnir dæmisagna

A Dæmisaga 1: Viðbrögð við hvalveiðaárás á yfirstjórnendur

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Fjármálastjóri fær mjög persónulegan tölvupóst sem segist vera frá forstjóranum og biður um hraða millifærslu upp á $50,000 til að ganga frá trúnaðarlénakaupum.
- Ráðlögð aðferð og lausn: Stilltu DMARC með „p=reject“-stefnu til að loka á falsaða sendendur. Bættu við viðvörunarborðum um utanaðkomandi sendendur á gáttinni og krefstu munnlegrar staðfestingar á annarri rás fyrir allar fjárhagsfærslur.

B Dæmisaga 2: Innleiðing SPF/DKIM/DMARC-stefna á gátt

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Aðstæður til greiningar: Fyrirtæki fellur á öryggisúttektum vegna þess að útsendur markaðspóstur er oft merktur sem ruslpóstur og tölvuþrjótar eru í virkri fölsun á léni vörumerkis fyrirtækisins.
- Ráðlögð aðferð og lausn: Birtu TXT-færslu fyrir SPF sem tilgreinir heimilar IP-tölur sendenda. Stilltu DKIM-undirskriftarlykla á útleiðandi póstþjónum og greindu innkomandi DMARC XML-skýrslur til að finna misnotkun.