Navn: _____ Dato: _____ Point: _____

Phishingangreb og social manipulation

Spear phishing, whaling-svindel, SPF/DKIM/DMARC-protokoller, spoofing af afsender og sikkerhedstræning af medarbejdere.

OVERBLIK OVER PHISHINGANGREB

SIKRET
DATAKRYPTERING
256-bit AES-standard

OVERHOLDER KRAV
GLOBALE STANDARDER
GDPR- og CCPA-rammer

ZERO-TRUST
ADGANGSPOLITIK
Multifaktorgodkendelse

Velkommen! Denne opgavepakke fører dig gennem phishing og social manipulation. Du vil udforske spear phishing, whaling, forfalskede domæner, SPF/DKIM/DMARC, sikre links og træning af medarbejdere.

OPGAVEARKETS KONTROLPUNKTER

- [ ] **Del 1-4: Lær cybersikkerhed og trusselsforebyggelse.**
- [ ] **Del 5-7: Løs kryds og tværs samt ordjagt.**
- [ ] **Del 8-9: Løs casestudier og chifferudfordring.**
- [ ] **Del 10: Gennemgå grundlæggende og avanceret FAQ.**
- [ ] **Del 11: Udforsk 10 interessante fakta fra virkeligheden.**
- [ ] **Bonus: Tænk hurtigt-udfordring.**

Åbn VPN.com's guide til cybersikkerhed

URL: https://www.vpn.com/da/cybersikkerhed/phishing-angreb/

Din læringsplan for afværgning af phishing

- Genkend almindelig phishing, vishing og falske support-pop-ups.
- Indfør bekræftelse af betalinger ad en anden kanal.
- Opsæt SPF, DKIM og DMARC mod forfalskede domæner.

VEJLEDNING TIL GUIDEN OM PHISHINGANGREB

Besvar flervalgs- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden om godkendelse af e-mail. Slut af med bonusaktiviteten Tænk hurtigt.

PHISHINGANGREB OG SOCIAL MANIPULATION (INTRODUKTION)

Phishing bruger målrettede beskeder, whaling og forfalskede domæner til at høste loginoplysninger. Beskyttelse af firmaets systemer kræver SPF, DKIM og DMARC ved porten samt godkendelse ad en anden kanal.

LÆS HVERT KONTROLPUNKT GRUNDIGT, OG VÆLG ELLER SKRIV DET RIGTIGE SVAR.

Kontrolpunkt 1: Flervalgsopgave

1. Hvad er spear phishing?

- A. En målrettet phishingmail tilpasset en bestemt person eller organisation
- B. En massemail til millioner af tilfældige adresser
- C. Et angreb, der oversvømmer servere med trafik
- D. En teknik til at trække brugerdata ud af databaser

2. Hvilken protokol lader et domæne angive sine autoriserede afsender-IP-adresser i DNS for at bekæmpe spoofing?

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

3. Hvad er et whalingangreb?

- A. Phishing rettet specifikt mod kendte topledere
- B. SQL-injektion mod databasebackups
- C. Tyveri af routere fra det lokale netværk
- D. Automatisk afprøvning af lækkede logins

4. Hvad gør DKIM?

- A. Tilføjer en kryptografisk signatur, der bekræfter afsenderen
- B. Blokerer indgående pakker i firewallen
- C. Krypterer databasediske i hvile
- D. Scanner vedhæftede filer for malware

5. Hvad er DMARC's rolle?

- A. At fortælle modtagende servere, hvad de skal gøre ved fejlet SPF/DKIM
- B. At knække adgangskoder med regnbuetabeller
- C. Komprimering af vedhæftede filer før levering
- D. At opsætte rettigheder til routing

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Spear phishing bygger på massemails til millioner af tilfældige adresser.

Sandt Falsk

7 Spørgsmål 7

7. DMARC kan bede mailservere afvise forfalskede beskeder.

Sandt Falsk

8 Spørgsmål 8

8. SPF virker ved at kontrollere den kryptografiske signatur i e-mailens tekst.

Sandt Falsk

9 Spørgsmål 9

9. Whaling rammer lavt placerede administratorer for at få adgang til databaser.

Sandt Falsk

10 Spørgsmål 10

10. Verifikation af betalingsanmodninger via en separat kanal hjælper med at stoppe svindel med bankoverførsler.

Sandt Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

Læs hver sætning nedenfor, og udfyld det tomme felt med det rigtige ord fra ordbanken.

1. At ramme en bestemt medarbejder med personlige oplysninger er _____ phishing.
2. At forfalske afsenderen, så en e-mail ser ægte ud, kaldes _____ .
3. DNS-posten med godkendte mailservere hedder _____ .
4. Signaturstandarden, der bekræfter afsenderen, hedder _____ .
5. Regler, der afviser e-mails med fejlet SPF/DKIM, bruger _____ .
6. Phishing rettet mod topledere kaldes _____ .

ORDBANK MED FAGUDTRYK

DKIM DMARC PHISHING SPEAR SPF SPOOFING VISHING WHALING

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

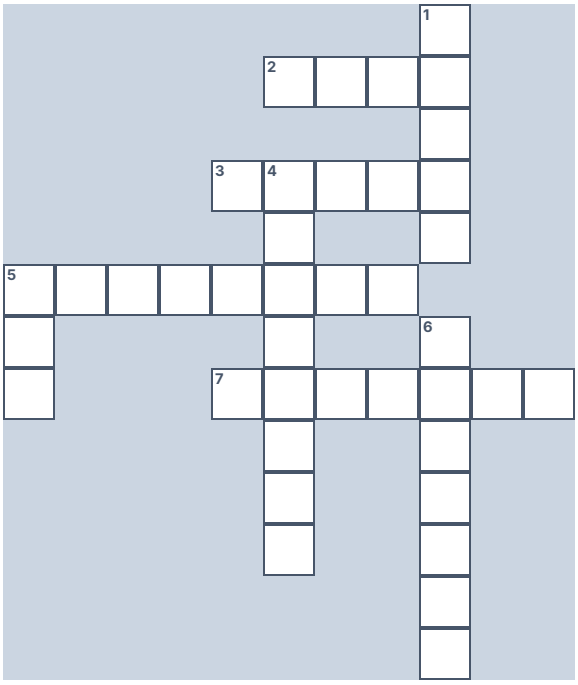
MATCH BEGREBER OG DEFINITIONER

Match hvert fagudtryk til venstre med den rigtige definition til højre ved at skrive det tilhørende bogstav (A-H) i indtastningsfeltet.

☐	1. SPEAR	A	Svindel via telefonopkald.
☐	2. SPOOFING	B	Rettet mod topledere.
☐	3. SPF	C	Regler for afvisning.
☐	4. DKIM	D	Godkendte afsender-IP'er i DNS.
☐	5. DMARC	E	E-mail med social manipulation.
☐	6. WHALING	F	Personlig, målrettet e-mail.
☐	7. PHISHING	G	Forfalskning af afsenderadressen.
☐	8. VISHING	H	Kryptografisk signatur i e-mail.

Kontrolpunkt 5: Kryds og tværs

Løs kryds og tværs ved at skrive bogstaver i de aktive hvide felter. Tallene svarer til nøglerne nedenfor.



VANDRETTE NØGLER

2. Standard, der tilføjer en kryptografisk signatur til e-mails (4)

3. ... phishing: en målrettet e-mail til en bestemt person (5)

5. Forfalskning af afsenderen, så en e-mail ser ægte ud (8)

7. Phishing rettet mod topledere (7)

LODRETTE NØGLER

1. Regler, der fortæller servere, hvad de skal gøre ved fejlet SPF eller DKIM (5)

4. Svigagtige beskeder, der skal narre brugere til at dele data (8)

5. DNS-posten med listen over godkendte mailservere (3)

6. Svindel via telefonopkald (7)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

Brugere af skærmlæser og tastatur kan skrive krydsordssvarene direkte i tekstfelterne nedenfor.

VANDRETTE NØGLER

2 vandret: Standard, der tilføjer en kryptografisk signatur til e-mails (4 bogstaver):

3 vandret: ... phishing: en målrettet e-mail til en bestemt person (5 bogstaver):

5 vandret: Forfalskning af afsenderen, så en e-mail ser ægte ud (8 bogstaver):

7 vandret: Phishing rettet mod topledere (7 bogstaver):

LODRETTE NØGLER

1 lodret: Regler, der fortæller servere, hvad de skal gøre ved fejlet SPF eller DKIM (5 bogstaver):

4 lodret: Svigagtige beskeder, der skal narre brugere til at dele data (8 bogstaver):

5 lodret: DNS-posten med listen over godkendte mailservere (3 bogstaver):

6 lodret: Svindel via telefonopkald (7 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

Find de 8 vigtige fagudtryk, der er skjult i gitteret nedenfor. Ordene kan stå vandret, lodret eller diagonalt.

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

ORDLISTE MED FAGUDTRYK

SPEAR SPOOFING SPF DKIM DMARC WHALING PHISHING VISHING

Kontrolpunkt 6, alternativ: Tilgængelig ordmatchning

Match hvert af de 8 fagudtryk fra ordjagten med den rigtige definition ved at skrive bogstavet (A-H) i det tomme felt.

FAGUDTRYK
A. SPEAR
B. SPOOFING
C. SPF
D. DKIM
E. DMARC
F. WHALING
G. PHISHING
H. VISHING

DEFINITIONER OG MATCHFELTER

1. Forfalskning af afsenderen, så en e-mail ser ægte ud.
2. ... phishing: en målrettet e-mail til en bestemt person.
3. Svindel via telefonopkald.
4. DNS-posten med listen over godkendte mailservere.
5. Svigagtige beskeder, der skal narre brugere til at dele data.
6. Regler, der fortæller servere, hvad de skal gøre ved fejlet SPF eller DKIM.
7. Standard, der tilføjer en kryptografisk signatur til e-mails.
8. Phishing rettet mod topledere.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige cybersikkerhedsbegreber. Skriv dine svar i indtastningsfelterne.

1. **AESRP**
2. **FPS**
3. **ADCRM**
4. **SNGIHPHI**
5. **FIPGOSNO**
6. **IMDK**
7. **WNIGHLA**
8. **IHGVNIS**

Bonusaktivitet: Tænk hurtigt

3 SVAR I HVER KATEGORI. DEN FØRSTE, DER UDFYLDER HELE LISTEN, VINDER.

1	Enheder, der kan blive hacket			
2	Tegn på en phishing-mail			
3	Tegn på, at en computer er inficeret			
4	Ord, der skaber falsk hast			
5	Måder at tjekke en afsender			
6	Personer, du kan spørge om it-hjælp			
7	Ting, du tager backup af			
8	Fisk eller havdyr, du kender			
9	Firmaer, svindlere udgiver sig for			
10	Sikkerhedsvaner, du kan starte i dag			
11	Ting at gøre efter et klik på et falsk link			
12	Ting at gøre efter et datalæk			
13	Kanaler, hvor phishing sker			
14	Ting, du aldrig sender på mail			
15	Måder at beskytte dine konti			

Kontrolpunkt 8: Casestudier om cybersikkerhed

Anvend de begreber, du har lært, til at løse de virkelige scenarier nedenfor.

CASESTUDIE 1: HÅNDTERING AF WHALING MOD LEDELSEN

👨‍💻

Scenarie: En økonomidirektør får en meget personlig e-mail, der foregiver at komme fra den administrerende direktør og beder om 50.000 dollar hurtigt til et fortroligt domænekøb.

Diskussion: Analysér risikoen for forfalskning af brandet, og beskriv SPF, DKIM, DMARC og kontroller for godkendelse.

CASESTUDIE 2: INDFØRELSE AF SPF, DKIM OG DMARC

👨‍💻

Scenarie: En virksomhed dumper sikkerhedsrevisioner, fordi dens marketingmails ofte havner som spam, og hackere aktivt forfalsker firmaets domæne.

Diskussion: Fastlæg tekniske og administrative kontroller, der bekræfter, at e-mails er ægte.

Kontrolpunkt 9: Afkod chifferet

En cybersikkerhedsekspert beskytter netværkets aktiver mod trusselsaktører online. Brug bogstav-til-tal-nøglen nedenfor til at afkode beskeden ved at skrive de tilsvarende bogstaver i de tomme felter.

BOGSTAV-TIL-TAL-KRYPTERINGSNØGLE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Æ=27 Ø=28 Å=29

11	15	14	20	18	15	12	12	5	18

1	6	19	5	14	4	5	18	5	14		6	28	18		4	21

11	12	9	11	11	5	18

Afkodet besked:

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z, 27 = Æ, 28 = Ø, 29 = Å).

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del A)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q1: Hvad er phishing?

Social manipulation, hvor kriminelle sender svigagtige beskeder for at narre brugere til at dele følsomme data.

Q2: Hvad er forskellen på phishing og spear phishing?

Phishing rammer brede grupper med generelt indhold, mens spear phishing rammer bestemte ofre med tilpassede detaljer.

Q3: Hvad er whaling?

Meget målrettet phishing mod kendte ledere med stor beslutningsmagt.

Q4: Hvad er forfalskning af e-mail?

E-mails med forfalsket afsender, der skal få modtageren til at stole på kilden.

Q5: Hvordan forhindrer SPF forfalskning?

Den offentliggør godkendte afsender-IP'er i DNS, så modtagende servere kan kontrollere kilden. [1]

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvad er DKIM?

DomainKeys Identified Mail tilføjer en kryptografisk signatur til e-mailens headere, som beviser, at et domæne har taget ansvar, og at beskeden ikke er ændret.

Q7: Hvad står DMARC for?

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

Q8: Hvad er en DMARC-politik?

Regler for, hvordan mailservere behandler beskeder, der fejler SPF/DKIM (none, quarantine eller reject). [2]

Q9: Hvad er vishing?

Phishing via telefon, hvor angribere bruger falske opkald til at få administrative eller økonomiske oplysninger.

Q10: Hvordan hjælper linkscannere?

De scanner og omskriver links i e-mails og tjekker destinationen, når der klikkes.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q1: Hvordan virker et homografangreb?

Angribere registrerer domæner med Unicode-tegn, der ligner almindelige bogstaver, og efterligner et ægte domæne.

Q2: Hvad er punycode?

En kodning, der omdanner Unicode-domænenavne til ASCII-kompatible strenge, der starter med 'xn--', så DNS kan håndtere dem.

Q3: Hvorfor er 'p=reject' den sikreste DMARC-indstilling?

Den beder modtagende servere om at afvise mail, der ikke består DMARC (tilpasset SPF/DKIM), under SMTP-sessionen og blokerer dermed direkte forfalskning. [2]

Q4: Hvordan omgår angribere SPF?

Med domæner, der ligner (typosquatting), eller kaprede konti hos lovlige mail-tjenester.

Q5: Hvad er kompromitteret firmamail (BEC)?

Svindel, hvor angribere kaprer eller efterligner firmamailkonti for at godkende falske betalinger.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q6: Hvordan stopper flerfaktorgodkendelse phishing?

Den kræver en ekstra nøgle (som en hardwarenøgle), der ikke kan stjæles via en falsk side alene.

Q7: Hvad er en side, der høster logins?

En falsk loginportal, der opsnapper brugernavne, adgangskoder og MFA-koder i realtid.

Q8: Hvad er kapring af underdomæner?

En angriber overtager et ubrugt underdomæne og hoster phishingsider under et betroet domæne.

Q9: Hvordan virker kontrol af DKIM-overensstemmelse?

Den kontrollerer, at domænet i 'From' er det samme, som har signeret beskeden i DKIM-headeren.

Q10: Hvad gør en e-mailgateway?

Den filtrerer e-mail, tjekker links, kører vedhæftede filer i sandkasse og kontrollerer SPF/DKIM/DMARC.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

Phishing og spoofing var den hyppigst anmeldte kriminalitetstype til FBI's IC3 i 2025 med 191,561 klager. [4]

2. SIKKERHEDSINDSIGT

Business email compromise (BEC) forårsagede over $3 milliarder i tab, der blev anmeldt til FBI's IC3 i 2025. [4]

3. SIKKERHEDSINDSIGT

Homografangreb bruger kyrilliske bogstaver, der ligner, til at kopiere brands domæner.

4. SIKKERHEDSINDSIGT

Med 'p=reject' beder et domæne modtagerne om at afvise mail, der fejler, under leveringen i stedet for at lægge den i spam. [2]

5. SIKKERHEDSINDSIGT

Whaling mod direktører beder ofte om hastebetalinger til fortrolige fusioner eller domænekøb.

6. SIKKERHEDSINDSIGT

Portaler til indsamling af loginoplysninger kopierer ægte loginsider, så ofrene taster deres adgangskoder direkte ind i angriberens formular.

7. SIKKERHEDSINDSIGT

CISA's fælles vejledning om phishing anbefaler brugertræning sammen med DMARC, SPF, DKIM og phishing-resistent MFA. [3]

8. SIKKERHEDSINDSIGT

SPF-evaluering er begrænset til 10 termer, der laver DNS-opslag; overskrides grænsen, returneres resultatet 'permerror'. [1]

9. SIKKERHEDSINDSIGT

FIDO2-hardwarenøgler giver kryptografisk beskyttelse mod høst af logins.

10. SIKKERHEDSINDSIGT

Phishing er en af de mest almindelige måder, angribere først kommer ind i en organisation på, og derfor er løbende træning i at genkende phishing et effektivt forsvar.

Tekniske referencer og kilder

Studieguiden og de interaktive opgaver er sammensat ud fra globale standarder fra NIST, OWASP og regler om databeskyttelse.

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[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

Facitliste: Kontrolpunkt 1 – Flervalg

1 Spørgsmål 1 — Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er spear phishing? → En målrettet phishingmail tilpasset en bestemt person eller organisation

2 Spørgsmål 2 — Rigtigt svar: A

UNDERVISNINGSNOTE

SPF offentliggør et domænes autoriserede afsenderværter i DNS, så modtagere kan kontrollere konvolutafsenderen.

3 Spørgsmål 3 — Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er et whalingangreb? → Phishing rettet specifikt mod kendte topledere

4 Spørgsmål 4 — Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad gør DKIM? → Tilføjer en kryptografisk signatur, der bekræfter afsenderen

5 Spørgsmål 5 — Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er DMARC's rolle? → At fortælle modtagende servere, hvad de skal gøre ved fejlet SPF/DKIM

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Spørgsmål 6** — **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Falsk: spear phishing er skræddersyet til bestemte personer, i modsætning til generisk massephishing.

7 **Spørgsmål 7** — **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

DMARC kan bede mailservere afvise forfalskede beskeder.

8 **Spørgsmål 8** — **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Falsk: SPF tjekker afsender-IP'en mod DNS; det er DKIM, der verificerer en kryptografisk signatur.

9 **Spørgsmål 9** — **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Falsk: whaling rammer topledere, som kan godkende betalinger og har adgang til følsomme data.

10 **Spørgsmål 10** — **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Sandt: at bekræfte betalingsanmodninger via en separat, kendt kanal hjælper med at stoppe overførselssvindel.

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt matchning (8 point i alt) og hvert korrekt kontekstord (6 point i alt).

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

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

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 SPEAR	2 SPOOFING	3 SPF	4 DKIM
5 DMARC	6 WHALING		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

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

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare SPEAR, SPOOFING og SPF med egne ord og give et eksempel på hvert begreb.

Casestudier:
Bed eleverne begrunde deres anbefalinger med fakta fra opgavearket frem for antagelser.

Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

2 vandret: DKIM Standard, der tilføjer en kryptografisk signatur til e-mails (4 bogstaver)

3 vandret: SPEAR ... phishing: en målrettet e-mail til en bestemt person (5 bogstaver)

5 vandret: SPOOFING Forfalskning af afsenderen, så en e-mail ser ægte ud (8 bogstaver)

7 vandret: WHALING Phishing rettet mod topledere (7 bogstaver)

LODRETTE NØGLER

1 lodret: DMARC Regler, der fortæller servere, hvad de skal gøre ved fejlet SPF eller DKIM (5 bogstaver)

4 lodret: PHISHING Svigagtige beskeder, der skal narre brugere til at dele data (8 bogstaver)

5 lodret: SPF DNS-posten med listen over godkendte mailservere (3 bogstaver)

6 lodret: VISHING Svindel via telefonopkald (7 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. AESRP — SPEAR
2. FPS — SPF
3. ADCRM — DMARC
4. SNGIHPHI — PHISHING
5. FIPGOSNO — SPOOFING
6. IMDK — DKIM
7. WNIGHLA — WHALING
8. IHGVNIS — VISHING

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"KONTROLLER AFSENDEREN FØR DU KLIKKER"

Facit til casestudier

A Casestudie 1: Håndtering af whaling mod ledelsen

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: Økonomidirektøren får en personlig e-mail, der foregiver at komme fra direktøren, og som beder om 50.000 dollar til et fortroligt domænekøb.
- Anbefalet strategi og løsning: Sæt DMARC til 'p=reject', vis advarsler om eksterne afsendere, og kræv mundtlig bekræftelse ad en anden kanal for alle betalinger.

B Casestudie 2: Indførelse af SPF, DKIM og DMARC

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: Virksomhedens marketingmails ender som spam, og hackere forfalsker aktivt firmaets domæne.
- Anbefalet strategi og løsning: Udgiv en SPF-post med godkendte afsender-IP'er, opsæt DKIM-nøgler på de udgående servere, og gennemgå DMARC-rapporterne for misbrug.