Navn: _____ Dato: _____ Poeng: _____

Nettfiskingsangrep og sosial manipulering

Spydnettfisking, hvalfangst-svindel (whaling), protokollene SPF/DKIM/DMARC, avsenderforfalskning og sikkerhetsopplæring for ansatte.

LÆRINGSOVERSIKT: NETTFISKINGSANGREP

SIKRET
DATAKRYPTERING
256-bits AES-standard

I SAMSVAR
GLOBALE STANDARDER
Rammeverk for GDPR og CCPA

ZERO TRUST
TILGANGSPOLICY
Flerfaktorautentisering

Velkommen! Dette aktivitetsheftet veileder deg gjennom phishing-angrep og sosial manipulering. Du utforsker spear phishing, whaling, domeneforfalskning, protokollene SPF/DKIM/DMARC, sikkerhet ved lenker og opplæring for å skape bevissthet blant ansatte.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk cybersikkerhet og forebygging av trusler.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms veiledning om cybersikkerhet

URL: https://www.vpn.com/no/cybersikkerhet/phishing-angrep/

Din læringsveiledning for håndtering av nettfisking

- Identifiser vanlig nettfisking, vishing og svindel med støtte-popup-vinduer.
- Innfør rutiner for verifisering av transaksjoner utenfor båndet (out-of-band).
- Konfigurer SPF-, DKIM- og DMARC-regler for å blokkere forfalskede domener.

INSTRUKSJONER FOR VEILEDNINGEN OM NETTFISKINGSANGREP

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på e-postautentisering. Avslutt med bonusaktiviteten Tenk raskt.

NETTFISKINGSANGREP OG SOSIAL MANIPULERING (INNLEDNING)

Nettfiskingsangrep bruker målrettede meldinger, hvalfangst-svindel (whaling) og domeneforfalskning for å høste brukernes påloggingsopplysninger. Sikring av bedriftssystemer krever at SPF-, DKIM- og DMARC-regler settes opp i gatewayen, sammen med godkjenningstrinn utenfor kanalen.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er spear phishing?

- A. En målrettet nettfiske-e-post skreddersydd for en bestemt person eller organisasjon
- B. En bred masse-e-post sendt til millioner av tilfeldige adresser
- C. Et nettverksangrep som oversvømmer webservere med trafikk
- D. En teknikk for å hente ut databaser som er rettet mot brukeroppføringer

2. Hvilken protokoll lar et domene oppgi sine autoriserte avsender-IP-adresser i DNS for å bekjempe forfalskning?

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

3. Hva er et whaling-angrep?

- A. En nettfiskekampanje rettet spesifikt mot profilerte toppledere i selskaper
- B. Et SQL-injeksjonsangrep rettet mot databasesikkerhetskopier
- C. Fysisk tyveri av ruterutstyr i lokalnettet
- D. En automatisert brute force-skanning med credential stuffing

4. Hva gjør DKIM?

- A. Legger til en kryptografisk signatur i e-poster for å verifisere avsenderens ekthet
- B. Blokkerer innkommende nettverkspakketrafikk i brannmuren
- C. Krypterer databaselagringsvolumer i hvile
- D. Skanner e-postvedlegg etter signaturbasert skadevare

5. Hva er rollen til DMARC?

- A. Å instruere mottakende e-postservere om hvordan de skal behandle mislykkede SPF/DKIM-kontroller
- B. Å dekryptere systempassord ved hjelp av forhåndsberegnede regnbuetabeller
- C. Å komprimere e-postvedlegg før levering
- D. Å konfigurere tilgangsprivilegier for nettverksruting

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Spydnettfisking bygger på generiske masse-e-poster sendt til millioner av tilfeldige adresser.

○ Sant ○ Usant

7 Spørsmål 7

7. DMARC-policyer kan instruere e-postservere om å avvise uautoriserte, forfalskede meldinger.

○ Sant ○ Usant

8 Spørsmål 8

8. SPF-verifisering fungerer ved å validere den kryptografiske signaturen til e-postteksten.

○ Sant ○ Usant

9 Spørsmål 9

9. Whaling-angrep rettes mot lavtstående administratorer i bedrifter for å få tilgang til databasefiler.

○ Sant ○ Usant

10 Spørsmål 10

10. Verifisering utenfor båndet (out-of-band) av betalingsforespørsler bidrar til å stoppe svindel med bankoverføringer.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. Å rette seg mot en bestemt ansatt med personlig tilpasset informasjon kalles _____ .
2. Å forfalske en e-posttopptekst for at meldinger skal se legitime ut, kalles avsender-_____ .
3. Den DNS-oppføringen som lister opp autoriserte IP-er for e-postservere, er _____ .
4. E-postsignaturstandarden som gir verifisering av avsenderen, er _____ .
5. Å etablere policyer for å avvise mislykkede SPF/DKIM-kontroller bruker _____ .
6. En nettfiskingskampanje rettet mot toppledere (C-nivå) kalles _____ .

ORDBANK

DKIM | DMARC | SMISHING | SPEAR PHISHING | SPF | SPOOFING | VISHING | WHALING

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble sikkerhetsbegreper

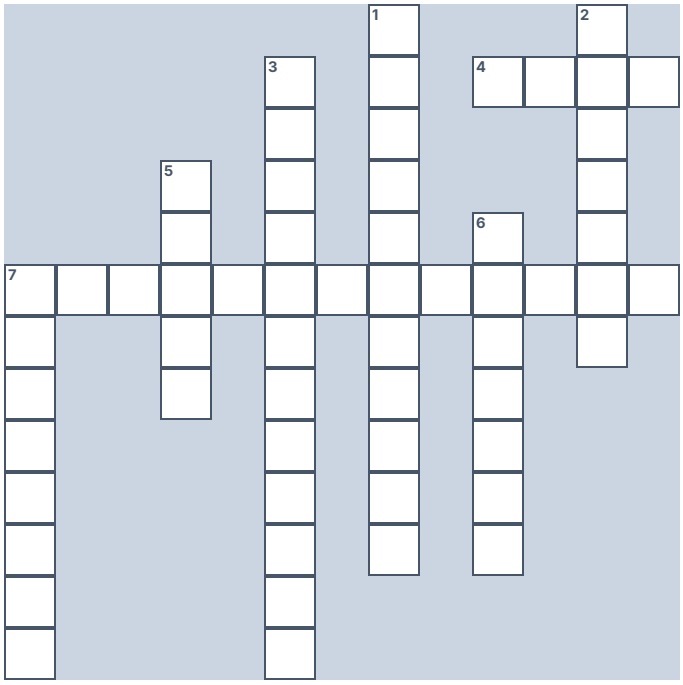
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. SPEAR PHISHING	A	Svindelsamtaler over telefon.
☐	2. FORFALSKNING (SPOOFING)	B	Retter seg mot toppledere (C-level).
☐	3. SPF	C	Instruksjoner om policyavvisning.
☐	4. DKIM	D	IP-adresser som er autorisert til å sende for DNS.
☐	5. DMARC	E	Sosial manipulering via e-post.
☐	6. WHALING	F	Målrettet personlig e-post.
☐	7. NETTFISKING	G	Forfalskning av avsenderens e-postadresse.
☐	8. VISHING	H	Kryptografisk signatur i e-post.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

4. Kryptografisk signatur i e-post. (4)

7. Personlig tilpasset, målrettet e-post. (13)

LODDRETT

1. Sosial manipulering via e-post. (11)

2. Stemmebaserte svindelsamtaler. (7)

3. DNS-autoriserte avsender-IP-er. (12)

5. Policy som gir instruksjoner om avvisning. (5)

6. Målretting mot toppledere (C-nivå). (7)

7. Forfalskning av avsenderens e-postadresse. (8)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

VANNRETT

4 vannrett: Kryptografisk signatur i e-post. (4 bokstaver):

7 vannrett: Personlig tilpasset, målrettet e-post. (13 bokstaver):

LODDRETT

1 loddrett: Sosial manipulering via e-post. (11 bokstaver):

2 loddrett: Stemmebaserte svindelsamtaler. (7 bokstaver):

3 loddrett: DNS-autoriserte avsender-IP-er. (12 bokstaver):

5 loddrett: Policy som gir instruksjoner om avvisning. (5 bokstaver):

6 loddrett: Målretting mot toppledere (C-nivå). (7 bokstaver):

7 loddrett: Forfalskning av avsenderens e-postadresse. (8 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

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

ORDLISTE

SPEARPHISHING SPOOFING SPFOPPFØRING DKIM DMARC WHALING NETTFISKING VISHING

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER
A. SPEARPHISHING
B. SPOOFING
C. SPFOPPFØRING
D. DKIM
E. DMARC
F. WHALING
G. NETTFISKING
H. VISHING

DEFINISJONER OG TILHØRENDE FELT	
	1. Forfalskning av avsenderens e-postadresse.
	2. Personlig tilpasset, målrettet e-post.
	3. Stemmebaserte svindelsamtaler.
	4. DNS-autoriserte avsender-IP-er.
	5. Sosial manipulering via e-post.
	6. Policy som gir instruksjoner om avvisning.
	7. Kryptografisk signatur i e-post.
	8. Målretting mot toppledere (C-nivå).

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper innen cybersikkerhet. Skriv svarene dine i svarboksene.

1. HESNPPIHSIG RA
2. GPPPSINFØRF O
3. ADCRM
4. SNGITFIKNET
5. FIPGOSNO
6. IMDK
7. WNIGHLA
8. IHGVNIS

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Enheter som kan hackes			
2	Tegn på en nettfiske-e-post			
3	Tegn på at en datamaskin er infisert			
4	Ord som skaper falsk hast			
5	Måter å sjekke en avsender på			
6	Personer du kan spørre om IT-hjelp			
7	Ting du tar sikkerhetskopi av			
8	Fisk eller havdyr du kjenner til			
9	Selskaper svindlere utgir seg for å være			
10	Trygge vaner du kan begynne med i dag			
11	Ting å gjøre etter å ha klikket på en falsk lenke			
12	Ting å gjøre etter en datalekkasje			
13	Kanaler der nettfiske forekommer			
14	Ting du aldri sender på e-post			
15	Måter å beskytte kontoene dine på			

Kontrollpunkt 8: Casestudier om cybersikkerhet

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

CASESTUDIE 1: UTBEDRING ETTER ET HVALFANGSTANGREP MOT TOPPLEDELSEN



Scenario: En finansdirektør (CFO) mottar en svært personlig tilpasset e-post som utgir seg for å være fra administrerende direktør og ber om en rask bankoverføring på $50,000 for å fullføre et konfidensielt domenekjøp.

Diskusjonsspørsmål: Analyser risikoene ved merkevareforfalskning, og beskriv SPF/DKIM/DMARC og autentiseringskontroller i detalj.

CASESTUDIE 2: INNFØRE GATEWAY-POLICYER FOR SPF/DKIM/DMARC



Scenario: Et selskap faller gjennom sikkerhetsrevisjoner fordi utgående markedsføringse-poster ofte markeres som søppelpost, og hackere aktivt forfalsker selskapets merkevaredomene.

Diskusjonsspørsmål: Etabler tekniske og administrative kontroller for å verifisere e-postenes ekthet.

Kontrollpunkt 9: Knekk chifferet

En cybersikkerhetsekspert beskytter nettverksressurser mot trusselaktører på nettet. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen ved å skrive de tilhørende bokstavene i de tomme feltene.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

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

15	16	16	4	1	7		19	15	19	9	1	12			
13	1	14	9	16	21	12	5	18	9	14	7		13	5	4
5	16	15	19	20	18	5	22	9	19	10	15	14			

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del A)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q1: Hva er nettfisking?

Nettfisking er et angrep med sosial manipulering der kriminelle sender uekte meldinger for å lure brukere til å dele sensitive data.

Q2: Hva er forskjellen mellom nettfisking og målrettet nettfisking (spear phishing)?

Nettfisking retter seg mot brede grupper med generisk innhold, mens målrettet nettfisking (spear phishing) retter seg mot bestemte ofre ved hjelp av tilpassede opplysninger.

Q3: Hva er whaling?

Whaling er et svært målrettet phishing-angrep rettet mot profilerte ledere som har administrativ myndighet.

Q4: Hva er e-postforfalskning (spoofing)?

E-postforfalskning er å lage e-postmeldinger med forfalsket avsenderadresse for å lure mottakeren til å stole på kilden.

Q5: Hvordan forhindrer SPF forfalskning (spoofing)?

Den publiserer en liste over autoriserte avsender-IP-adresser i DNS, slik at mottakende servere kan verifisere e-postens opprinnelse. [1]

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del B)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q6: Hva er DKIM?

DomainKeys Identified Mail legger til en kryptografisk signatur i e-postoverskrifter og beviser at et domene har tatt ansvar og at meldingen ikke er endret.

Q7: Hva står DMARC for?

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

Q8: Hva er en DMARC-policy?

En policy som forteller e-postservere hvordan de skal behandle meldinger som feiler SPF/DKIM (ingen, karantene eller avvis). [2]

Q9: Hva er vishing?

Stemmebasert phishing, der angripere bruker svindelsamtaler på telefon for å lure ut administrative eller økonomiske data.

Q10: Hvordan hjelper lenkeskannere?

De skanner og skriver om lenker i innkommende e-post for å verifisere at målsidene er trygge i øyeblikket du klikker.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del C)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q1: Hvordan fungerer et homografangrep?

Angripere registrerer domenenavn med lignende ikke-ASCII Unicode-tegn for å etterligne et legitimt domenenavn visuelt.

Q2: Hva er en punycode-representasjon?

En koding som konverterer Unicode-domenenavn til ASCII-kompatible strenger som starter med «xn--», slik at DNS kan håndtere dem.

Q3: Hvorfor er «p=reject» den tryggeste DMARC-tilstanden?

Den ber mottakende servere om å avvise e-post som ikke består DMARC (justert SPF/DKIM) under SMTP-økten, og blokkerer dermed direkte spoofing. [2]

Q4: Hvordan omgår angripere SPF-regler?

Ved å utnytte domener som ligner (typosquatting) eller bruke kompromitterte kontoer hos legitime e-posttjenester fra tredjeparter.

Q5: Hva er kompromittering av forretnings-e-post (BEC)?

En svindel rettet mot bedrifter der angripere kaprer eller utgir seg for å være forretnings-e-postkontoer for å godkjenne uredelige betalinger.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del D)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q6: Hvordan stopper flerfaktorautentisering nettfisking (phishing)?

Den krever sekundære tokener (som maskinvarenøkler) som ikke kan stjeles bare gjennom falske landingssider.

Q7: Hva er en landingsside for høsting av legitimasjon (credential harvesting)?

Et innloggingsportal-etterlignende nettsted utformet for å fange opp inntastede brukernavn, passord og MFA-koder i sanntid.

Q8: Hva er kapring av underdomener?

En angriper som tar kontroll over en ubrukt DNS-underdomenepeker for å være vert for ondsinnede nettfiske-landingssider under et pålitelig overordnet domene.

Q9: Hvordan fungerer DKIM-justeringskontrollen (alignment)?

Den verifiserer at domenet i «From»-headeren samsvarer med domenet som kryptografisk signerte meldingen i DKIM-headeren.

Q10: Hva er rollen til en e-postgateway?

Filtrering av innkommende e-post, revisjon av lenker, kjøring av vedlegg i sandkasse og validering av samsvar med SPF/DKIM/DMARC.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

Nettfisking og forfalskning var den mest rapporterte kriminalitetstypen til FBIs IC3 i 2025, med 191 561 klager. [4]

2. SIKKERHETSINNSIKT

Business email compromise (BEC) forårsaket tap på over 3 milliarder dollar rapportert til FBIs IC3 i 2025. [4]

3. SIKKERHETSINNSIKT

Homografangrep bruker kyrilliske bokstaver som ligner på latinske, for å visuelt duplisere merkevaredomener med eksakt treff i nettlesere.

4. SIKKERHETSINNSIKT

Med «p=reject» ber et domene mottakere om å avvise e-post som ikke består kontrollen under levering, i stedet for å legge den i søppelpost. [2]

5. SIKKERHETSINNSIKT

Whaling-angrep mot toppsjefer ber ofte om hasteutbetalinger i forbindelse med konfidensielle fusjoner eller domenekjøp.

6. SIKKERHETSINNSIKT

Portaler for høsting av legitimasjon kopierer ekte påloggingssider slik at ofre skriver passordene sine rett inn i angriperens skjema.

7. SIKKERHETSINNSIKT

CISAs felles veiledning om nettfisking anbefaler opplæring av brukere sammen med DMARC, SPF, DKIM og phishing-resistent MFA. [3]

8. SIKKERHETSINNSIKT

SPF-evalueringen er begrenset til 10 ledd som utløser DNS-oppslag; hvis grensen overskrides, gir det resultatet «permerror». [1]

9. SIKKERHETSINNSIKT

Maskinvarebaserte sikkerhetsnøkler med FIDO2 gir kryptografisk støttet beskyttelse mot ekstern innhøsting av påloggingsopplysninger.

10. SIKKERHETSINNSIKT

Nettfisking er en av de vanligste måtene angripere først kommer seg inn i en organisasjon på, og derfor er jevnlig opplæring i bevissthet et effektivt forsvar.

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale standarder fra NIST og OWASP og standarder for etterlevelse av personvern.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[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

Fasit: Kontrollpunkt 1 – flervalg

1 Spørsmål 1

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er spear phishing? → En målrettet nettfiske-e-post skreddersydd for en bestemt person eller organisasjon

2 Spørsmål 2

Riktig svar: A

MERKNAD TIL LÆREREN

SPF publiserer et domenes autoriserte avsendervertser i DNS slik at mottakere kan kontrollere konvoluttavsenderen.

3 Spørsmål 3

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er et whaling-angrep? → En nettfiskekampanje rettet spesifikt mot profilerte toppledere i selskaper

4 Spørsmål 4

Riktig svar: A

MERKNAD TIL LÆREREN

Hva gjør DKIM? → Legger til en kryptografisk signatur i e-poster for å verifisere avsenderens ekthet

5 Spørsmål 5

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er rollen til DMARC? → Å instruere mottakende e-postservere om hvordan de skal behandle mislykkede SPF/DKIM-kontroller

Fasit: Kontrollpunkt 2 – sant eller usant

6 Spørsmål 6

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: spydnettfiske (spear phishing) er skreddersydd for bestemte personer, i motsetning til generelt masseutsendt nettfiske.

7 Spørsmål 7

Riktig svar: Sant

MERKNAD TIL LÆREREN

DMARC-policyer kan instruere e-postservere om å avvise uautoriserte, forfalskede meldinger.

8 Spørsmål 8

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: SPF kontrollerer avsender-IP-adressen mot DNS; DKIM er den som verifiserer en kryptografisk signatur.

9 Spørsmål 9

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: «whaling» rettes mot toppledere, som kan godkjenne betalinger og ha tilgang til sensitive data.

10 Spørsmål 10

Riktig svar: Sant

MERKNAD TIL LÆREREN

Sant: å bekrefte betalingsforespørsler via en egen, kjent kanal bidrar til å stoppe svindel med bankoverføringer.

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

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

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

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

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 B – SPOOFING	2 A – SPEARPHISHING	3 H – VISHING	4 C – SPFOPPFØRING
5 G – NETTFISKING	6 E – DMARC	7 D – DKIM	8 F – WHALING

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare SPEAR PHISHING, FORFALSKNING (SPOOFING) og SPF med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

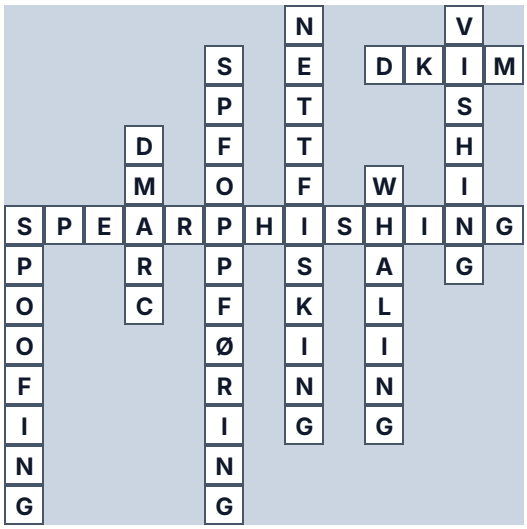
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

4 vannrett: DKIM Kryptografisk signatur i e-post. (4 bokstaver)

7 vannrett: SPEARPHISHING Personlig tilpasset, målrettet e-post. (13 bokstaver)

LODDRETT

1 loddrett: NETTFISKING Sosial manipulering via e-post. (11 bokstaver)

2 loddrett: VISHING Stemmebaserte svindelsamtaler. (7 bokstaver)

3 loddrett: SPFOPPFØRING DNS-autoriserte avsender-IP-er. (12 bokstaver)

5 loddrett: DMARC Policy som gir instruksjoner om avvisning. (5 bokstaver)

6 loddrett: WHALING Målretting mot toppledere (C-nivå). (7 bokstaver)

7 loddrett: SPOOFING Forfalskning av avsenderens e-postadresse. (8 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. HESNPPIHSIGRA — **SPEARPHISHING**
2. GPPPSINFØRFO — **SPFOPPFØRING**
3. ADCRM — **DMARC**
4. SNGITFIKNET — **NETTFISKING**
5. FIPGOSNO — **SPOOFING**
6. IMDK — **DKIM**
7. WNIGHLA — **WHALING**
8. IHGVNIS — **VISHING**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"OPPDAG SOSIAL MANIPULERING MED EPOSTREVISJON"

Fasit til casestudiene

A Casestudie 1: Utbedring etter et hvalfangstangrep mot toppledelsen

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En økonomidirektør (CFO) mottar en svært personlig tilpasset e-post som utgir seg for å være fra administrerende direktør og ber om en rask overføring på 50 000 dollar for å avslutte et konfidensielt domenekjøp.
- Anbefalt strategi og løsning: Konfigurer DMARC med policyen «p=reject» for å blokkere forfalskede avsenderdomener. Legg til advarselsbannere for eksterne avsendere i gatewayen, og krev muntlig bekreftelse utenfor båndet (out-of-band) for alle finansielle transaksjoner.

B Casestudie 2: Innføre gateway-policyer for SPF/DKIM/DMARC

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En bedrift består ikke sikkerhetsrevisjoner fordi utgående markedsførings-e-poster ofte blir merket som søppelpost, og hackere aktivt forfalsker selskapets merkedomene.
- Anbefalt strategi og løsning: Publiser en TXT-post for SPF som angir autoriserte avsender-IP-adresser. Konfigurer DKIM-signeringsnøkler på utgående e-postservere, og analyser innkommende DMARC XML-tilbakemeldingsrapporter for å identifisere misbruk.