Navn: _____ Dato: _____ Poeng: _____

Nettsvindel og sosial manipulering Veiledning om beskyttelse

Nettfisking via e-post, forfalskede domener, vishing, svindel mot kundestøtte, verifisering utenfor båndet, BEC

LÆRINGSOVERSIKT: NETTSVINDEL

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 nettbasert forsvar mot svindel. Du utforsker falske nettfiskingssider, taktikker for sosial manipulering, svindel via kundestøtte, vektorer for bankoverføringssvindel og metoder for betalingsverifisering.

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/nettsvindel/

Din læringsveiledning for beskyttelse mot svindel på nett

- Identifiser vanlige kjennetegn på supportsvindel og typosquatting-domener.
- Innfør protokoller for e-postverifisering (SPF, DKIM, DMARC) mot spoofing.
- Innfør verifisering av transaksjoner utenfor båndet for å hindre svindel med bankoverføringer i virksomheter.

INSTRUKSJONER FOR VEILEDNINGEN OM NETTSVINDEL

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

NETTSVINDEL OG BESKYTTELSE MOT SOSIAL MANIPULERING (INNLEDNING)

Nettsvindel utnytter menneskelig atferd gjennom nettfisking, støtte-popup-vinduer, vishing og svindel med bankoverføringer. Å kreve verifisering av transaksjoner utenfor kanalen og domeneregler for SPF/DKIM/DMARC bidrar til å blokkere vektorer for sosial manipulering i gatewayen.

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

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er det viktigste tegnet på en supportsvindel?

- A. Et popup-vindu som hevder at systemet ditt er infisert og krever at du ringer et telefonnummer
- B. En automatisk sikkerhetsoppdatering lastet ned fra et offisielt register
- C. En passordbehandler som nekter å fylle ut legitimasjon på et bedriftsdomene
- D. En sikkerhetskopiering av filer i bakgrunnen som kjører på en ekstern stasjon

2. Hvilken teknikk bruker forfalskede avsenderdomener for å stjele bankopplysninger?

- A. E-postnettfisking
- B. Portskanning
- C. Minneinjeksjon
- D. Kryptografisk makulering

3. Hva representerer svindel med bankoverføringer?

- A. Å lure ofre til å sende penger til falske bedriftskontoer ved hjelp av social engineering
- B. Å kryptere systemdatabaser med nyttelaster fra løsepengevirus
- C. Å spørre databaser via SQL-injeksjonskommandoer
- D. Å sikkerhetskopiere systemfiler til offline lagringsdisker

4. Hvorfor lager svindlere falske nettbutikker?

- A. Å stjele kredittkortopplysninger og betalingslegitimasjon fra kjøpere
- B. Å være vert for databasetabeller for analyse av skadevare i sandkasse
- C. For å øke leveringshastigheten på nettbestillinger
- D. For å teste nye nettstedsdesign gratis

5. Hva betyr vishing?

- A. Svindel med stemmebasert nettfiske over telefonnettverk for å stjele legitimasjon
- B. Å skanne lokale nettverk etter usikrede systemenheter
- C. Å gjenopprette systemdatabaser etter et uautorisert sikkerhetsbrudd
- D. Å kjøre ikke-klarert kode i sikre virtuelle containere

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Nettfiskingssvindel retter seg bare mot sluttbrukere, aldri mot ledere som er mål for hvalfangst (whaling).

○ Sant ○ Usant

7 Spørsmål 7

7. Forfalskede domener bruker ofte små skrivefeil (som amaz0n.com) for å etterligne pålitelige merkevarer.

○ Sant ○ Usant

8 Spørsmål 8

8. Støttesvindel kan løses ved å gi innringeren ekstern tilgang.

○ Sant ○ Usant

9 Spørsmål 9

9. Sosial manipulering utnytter menneskelig psykologi som frykt og hastverk for å omgå sikkerhetsregler.

○ Sant ○ Usant

10 Spørsmål 10

10. Forespørsler om bankoverføring bør alltid verifiseres via kommunikasjonskanaler utenfor båndet.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. Uredelige e-poster som lurer brukere kalles _____ .

2. Nettadresser som etterligner pålitelige merkevarer er _____ .

3. Stemmesvindel rettet mot bankopplysninger kalles _____ .

4. Et popup-vindu som krever penger for å fjerne virus, er en _____ med falsk teknisk støtte.

5. Å bekrefte en betalingsforespørsel krever _____ via en separat kanal.

6. Omdirigering av forretningstransaksjoner til tyvers kontoer er _____ .

ORDBANK

BANKOVERFØRING FALSIFISERTE NETTFISKING SMISHING SVINDEL VERIFISERING VISHING WHALING

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble sikkerhetsbegreper

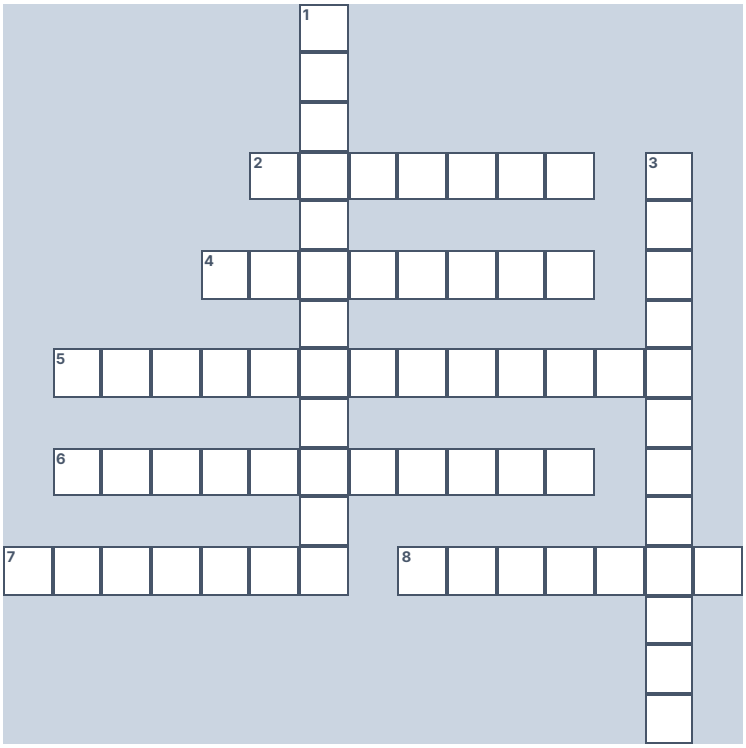
KOBLE DEFINISJONER

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

☐	1. NETTFISKING	A	Svindelaktig omdirigering av banktransaksjoner til kriminelle kontoer.
☐	2. FORFALSKET	B	Svindelopplegg som er utformet for å stjele penger eller tilgangsdata fra ofre.
☐	3. VISHING	C	Å sende svindel-tekstmeldinger for å stjele påloggingsopplysninger til mobilkontoer.
☐	4. SVINDEL	D	Svindelaktige taleanrop som er utformet for å stjele påloggingsinformasjon og kontodetaljer.
☐	5. VERIFISERING	E	Målrettede nettfiskingsangrep som har som mål å stjele påloggingsopplysninger fra toppledere (C-level).
☐	6. BANKOVERFØRING	F	Forfalsket e-postavsender eller nettstedsadresse som er laget for å se legitim ut.
☐	7. WHALING	G	Svindelaktige e-postkampanjer som er utformet for å stjele påloggingsinformasjon og passord.
☐	8. SMISHING	H	Å bekrefte betalingsopplysninger via en pålitelig sekundær kontaktmetode.

Kontrollpunkt 5: Kryssord

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



VANNRETT

2. Uredelige telefonsamtaler utformet for å stjele påloggingsopplysninger og kontodetaljer. (7)

4. Utsending av svindel-SMS for å stjele påloggingsopplysninger til mobilkontoer. (8)

5. Uredelig omdirigering av banktransaksjoner til kriminelle kontoer. (13)

6. Uredelige e-postkampanjer utformet for å stjele påloggingsopplysninger og passord. (11)

7. Målrettede nettfiskingsangrep som har som mål å stjele påloggingsopplysninger fra toppledere (C-nivå). (7)

8. Uredelig opplegg utformet for å stjele penger eller tilgang til påloggingsopplysninger fra ofre. (7)

LODDRETT

1. Bekreftelse av betalingsopplysninger via en pålitelig sekundær kontaktmetode. (12)

3. Etterlignet e-postavsender eller nettadresse utformet for å se legitim ut. (12)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

2 vannrett: Uredelige telefonsamtaler utformet for å stjele påloggingsopplysninger og kontodetaljer. (7 bokstaver):

4 vannrett: Utsending av svindel-SMS for å stjele påloggingsopplysninger til mobilkontoer. (8 bokstaver):

5 vannrett: Uredelig omdirigering av banktransaksjoner til kriminelle kontoer. (13 bokstaver):

6 vannrett: Uredelige e-postkampanjer utformet for å stjele påloggingsopplysninger og passord. (11 bokstaver):

7 vannrett: Målrettede nettfiskingsangrep som har som mål å stjele påloggingsopplysninger fra toppledere (C-nivå). (7 bokstaver):

8 vannrett: Uredelig opplegg utformet for å stjele penger eller tilgang til påloggingsopplysninger fra ofre. (7 bokstaver):

LODDRETT

1 loddrett: Bekreftelse av betalingsopplysninger via en pålitelig sekundær kontaktmetode. (12 bokstaver):

3 loddrett: Etterlignet e-postavsender eller nettadresse utformet for å se legitim ut. (12 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

NETTFISKING FALSIFISERTE BANKBEDRAGERI VISHING WHALING SVINDEL SMISHING VERIFISERING

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. NETTFISKING
B. FALSIFISERTE
C. VISHING
D. SVINDEL
E. VERIFISERING
F. BANKBEDRAGERI
G. WHALING
H. SMISHING

DEFINISJONER OG TILHØRENDE FELT	
	1. Etterlignet e-postavsender eller nettadresse utformet for å se legitim ut.
	2. Bekreftelse av betalingsopplysninger via en pålitelig sekundær kontaktmetode.
	3. Uredelig omdirigering av banktransaksjoner til kriminelle kontoer.
	4. Utsending av svindel-SMS for å stjele påloggingsopplysninger til mobilkontoer.
	5. Målrettede nettfiskingsangrep som har som mål å stjele påloggingsopplysninger fra toppledere (C-nivå).
	6. Uredelige telefonsamtaler utformet for å stjele påloggingsopplysninger og kontodetaljer.
	7. Uredelige e-postkampanjer utformet for å stjele påloggingsopplysninger og passord.
	8. Uredelig opplegg utformet for å stjele penger eller tilgang til påloggingsopplysninger fra ofre.

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. **FSNEIKNITGT** _____
2. **VSGNIHI** _____
3. **VEESNRRIGFII** _____
4. **GHILNWA** _____
5. **ARSIELIEFFTS** _____
6. **EIDSNLV** _____
7. **GEREBAABIRN DK** _____
8. **SMHGSNII** _____

Bonusaktivitet: Tenk raskt

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

1	Enheter som kan hackes			
2	Uttrykk svindlere ofte bruker			
3	Betalingsmåter svindlere ber om			
4	Typer svindel på nettet			
5	Tilbud som er for gode til å være sanne			
6	Steder å anmelde svindel			
7	Ord knyttet til cybersikkerhet			
8	Personer du kan advare mot svindel			
9	Ting du tar sikkerhetskopi av			
10	Advarselstegn i en e-post			
11	Tegn på at en datamaskin er infisert			
12	Måter å sjekke en nettbutikk på			
13	Måter å beskytte kontoene dine på			
14	Ting å gjøre hvis du blir svindlet			
15	Ting å gjøre etter en datalekkasje			

Kontrollpunkt 8: Casestudier om cybersikkerhet

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

CASESTUDIE 1: FOREBYGGING AV BEDRAGERI MED BEDRIFTSOVERFØRINGER

👷

Scenario: En økonomiavdeling mottar en hastende e-post fra en forfalsket leverandøradresse, som ber om at fremtidige fakturabetalinger sendes til et nytt rutingnummer.

Diskusjonsspørsmål: Skisser en policy for verifisering av svindel med bankoverføringer, og angi blokkeringer for e-postautentisering.

CASESTUDIE 2: NETTFISKINGSHENDELSE MED HVALFANGST MOT LEDER

👷

Scenario: En leder klikket på en nettfiskingslenke som hevdet å inneholde et sikkert dokument til et styremøte, og skrev inn de viktigste påloggingsopplysningene sine i selskapet på en forfalsket portal.

Diskusjonsspørsmål: Beskriv i detalj trinnene for hendelseshåndtering, og forklar hvordan man reviderer lederes innlogginger.

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		14	5	20	20	6	9	19	11	9	14	7

13	5	4		19	11	1	14	14	5	18		15	7	

22	5	18	9	6	9	19	5	18	9	14	7	

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 nettsvindel?

En svindelordning som bruker digitale kanaler til å lure ofre til å sende penger eller gi fra seg personlig legitimasjon.

Q2: Hva er den viktigste indikatoren på nettfisking via e-post?

En melding som hevder at det haster (som kontosuspensjon) og leder deg til en lenke som ikke samsvarer med det offisielle domenet.

Q3: Hva er typosquatting?

Registrering av domener med vanlige skrivefeil av kjente merkevarer (som amaz0n.com) for å drive falske phishing-nettsteder.

Q4: Hva er svindel med falsk kundestøtte?

Et popup-vindu som hevder at PC-en din er infisert og leder deg til å ringe et nummer og betale for falsk opprydningsprogramvare eller fjerntilgangstjenester. [1]

Q5: Hva er vishing?

Nettfiskingsangrep der telefonsamtaler brukes til å lure ofre til å oppgi bankkontoopplysninger eller påloggingsdetaljer.

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

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

Q6: Hva betyr bankoverføringssvindel (wire fraud)?

Omdirigering av betalingstransaksjoner til svindelkontoer ved å utgi seg for å være leverandører eller ledere.

Q7: Hva er whaling?

En svært målrettet form for spear phishing som retter seg direkte mot høyverdimål som toppledere i selskaper.

Q8: Hva er smishing?

Svindel-tekstmeldinger som sendes til mobile enheter og inneholder lenker til falske portaler eller sporingsoppdateringer.

Q9: Hvorfor er verifisering utenfor båndet (out-of-band) kritisk?

Den bekrefter transaksjonsdetaljer via en separat kommunikasjonskanal (som en telefonsamtale) og unngår kompromitterte e-posttråder.

Q10: Hvordan fungerer en falsk deponeringssvindel (escrow)?

Svindlere oppretter et forfalsket deponeringsnettsted (escrow), hevder at midlene holdes trygt, og stjeler deretter kjøperens bankoverføring.

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

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

Q1: Hvordan bruker svindlere BEC (Business Email Compromise, kompromittering av forretnings-e-post) til å utføre overføringssvindel?

De kaprer en legitim ansatts e-postkonto, overvåker fakturatråder og sender oppdaterte faktureringsopplysninger med falske bankkontoer.

Q2: Hva er risikoen ved IDN-homografangrep i nettsvindel?

Å bruke tegn utenfor ASCII som ser identiske ut med vanlige bokstaver (f.eks. kyrillisk 'a') til å registrere forfalskede domener som etterligner ekte merker.

Q3: Hvorfor er inspeksjon av e-postoverskrifter viktig for å oppdage svindel?

Den avslører IP-adressen til den faktiske opprinnelsesserveren og SPF/DKIM-valideringsstatusen, og viser om avsenderdomenet er forfalsket.

Q4: Hvordan utnytter svindlere som utgir seg for å være kundestøtte programvare for fjernskrivebord?

De bruker verktøy som AnyDesk eller TeamViewer til å koble til offerets enhet, plante skadevare og stjele lagrede passord.

Q5: Hva er målet med forskuddssvindel (advance-fee scams)?

Å lure ofre til å betale behandlingsgebyrer på forhånd mot en stor økonomisk belønning som ikke finnes.

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

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

Q6: Hvordan bruker svindlere profilering i sosiale medier til målrettet nettfisking (phishing)?

De samler organisasjonsstrukturer og ansattnavn i bedrifter for å skrive overbevisende spydfiske-e-poster (spear phishing).

Q7: Hvorfor tilbyr falske nettbutikker store rabatter?

For å lokke kjøpere til å oppgi kredittkortopplysninger og fange opp påloggingsinformasjon som kan gjenbrukes eller selges videre på carding-fora.

Q8: Hvordan blokkerer DMARC-poster nettfiskingssvindel (phishing)?

DMARC lar domeneeiere be mottakere om å sette i karantene eller avvise e-post som feiler justerte SPF- og DKIM-kontroller, slik at direkte forfalskning blokkeres. [5]

Q9: Hva er trusselen fra portaler som høster legitimasjon?

Forfalskede landingssider utformet for å se akkurat ut som Microsoft 365 eller Google Workspace, og som stjeler påloggingsopplysninger mens de skrives inn.

Q10: Hvordan rapporterer og deaktiverer sikkerhetsteam svindeldomener?

Ved å sende inn bevis på svindel til registrarens e-postadresse for misbruk, leverandøren av hosting og Google Safe Browsing-registeret.

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. [2]

2. SIKKERHETSINNSIKT

Business Email Compromise (BEC) forårsaket tap på over 3 milliarder dollar rapportert til FBIs IC3 i 2025. [2]

3. SIKKERHETSINNSIKT

Domener med skrivefeil (typo-squatting) avviker fra de ekte merkenavnene med ett eller to tegn, så et raskt blikk kan overse dem.

4. SIKKERHETSINNSIKT

Svindel med teknisk support forårsaket tap på over 2,1 milliarder dollar meldt til FBIs IC3 i 2025. [2]

5. SIKKERHETSINNSIKT

Homografangrep ser identiske ut i nettleserens adressefelt med mindre nettleseren viser punycode-konfigurasjoner.

6. SIKKERHETSINNSIKT

SMS-svindel (smishing) bruker korte, hastepregede meldinger med lenker, slik at ofrene får lite kontekst til å oppdage svindelen.

7. SIKKERHETSINNSIKT

Whaling-angrep rettes mot e-post til ledere fordi de kontrollerer tilgangen til store betalinger via bankoverføring.

8. SIKKERHETSINNSIKT

Å verifisere endringer i betaling ved å ringe et kjent, lagret telefonnummer er et viktig forsvar mot BEC-svindel med overføringer.

9. SIKKERHETSINNSIKT

Falske nettsteder for deponering (escrow) er en vanlig svindel på nettbaserte markedsplasser: de ser ut som en sikker betalingstjeneste, men stjeler kjøperens bankoverføring.

10. SIKKERHETSINNSIKT

Google Safe Browsing advarer brukere før de åpner nettsteder som er flagget for nettfisking eller skadevare.

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] Federal Trade Commission. (n.d.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[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] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

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

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

Fasit: Kontrollpunkt 1 – flervalg

1 Spørsmål 1

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er det viktigste tegnet på en supportsvindel? → Et popup-vindu som hevder at systemet ditt er infisert og krever at du ringer et telefonnummer

2 Spørsmål 2

Riktig svar: A

MERKNAD TIL LÆREREN

Hvilken teknikk bruker forfalskede avsenderdomener for å stjele bankopplysninger? → E-postnettfisking

3 Spørsmål 3

Riktig svar: A

MERKNAD TIL LÆREREN

Hva representerer svindel med bankoverføringer? → Å lure ofre til å sende penger til falske bedriftskontoer ved hjelp av social engineering

4 Spørsmål 4

Riktig svar: A

MERKNAD TIL LÆREREN

Hvorfor lager svindlere falske nettbutikker? → Å stjele kredittkortopplysninger og betalingslegitimasjon fra kjøpere

5 Spørsmål 5

Riktig svar: A

MERKNAD TIL LÆREREN

Hva betyr vishing? → Svindel med stemmebasert nettfiske over telefonnettverk for å stjele legitimasjon

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Spørsmål 6** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Usant: nettfiske rammer også ledere; «whaling» er nettfiske rettet mot toppledere.

7 **Spørsmål 7** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Forfalskede domener bruker ofte små skrivefeil (som amaz0n.com) for å etterligne pålitelige merkevarer.

8 **Spørsmål 8** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Usant: å gi en svindler som utgir seg for å være kundestøtte ekstern tilgang lar vedkommende plante skadevare og stjele data.

9 **Spørsmål 9** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Sosial manipulering utnytter menneskelig psykologi som frykt og hastverk for å omgå sikkerhetsregler.

10 **Spørsmål 10** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Forespørsler om bankoverføring bør alltid verifiseres via kommunikasjonskanaler utenfor båndet.

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

G 1. NETTFISKING	F 2. FORFALSKET	D 3. VISHING	B 4. SVINDEL
H 5. VERIFISERING	A 6. BANKOVERFØRING	E 7. WHALING	C 8. SMISHING

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 NETTFISKING	2 FALSIFISERTE	3 VISHING	4 SVINDEL
5 VERIFISERING	6 BANKOVERFØRING		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 B – FALSIFISERTE	2 E – VERIFISERING	3 F – BANKBEDRAGERI	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – NETTFISKING	8 D – SVINDEL

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare NETTFISKING, FORFALSKET og VISHING med egne ord og gi et eksempel på hvert.

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

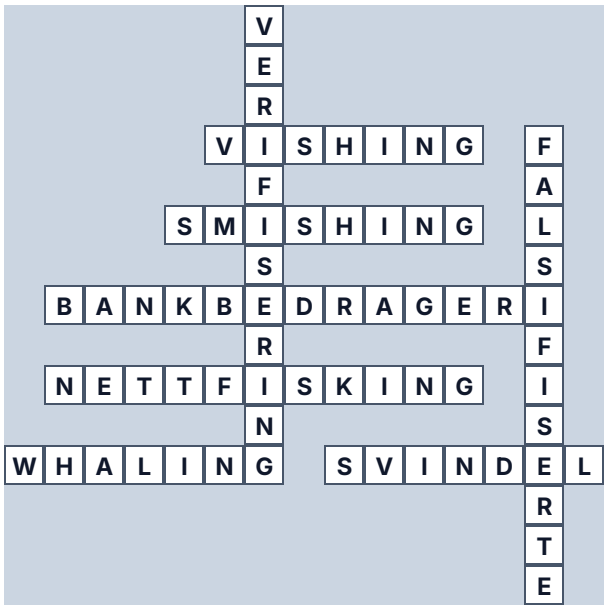
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

2 vannrett: VISHING Uredelige telefonsamtaler utformet for å stjele påloggingsopplysninger og kontodetaljer. (7 bokstaver)

4 vannrett: SMISHING Utsending av svindel-SMS for å stjele påloggingsopplysninger til mobilkontoer. (8 bokstaver)

5 vannrett: BANKBEDRAGERI Uredelig omdirigering av banktransaksjoner til kriminelle kontoer. (13 bokstaver)

6 vannrett: NETTFISKING Uredelige e-postkampanjer utformet for å stjele påloggingsopplysninger og passord. (11 bokstaver)

7 vannrett: WHALING Målrettede nettfiskingsangrep som har som mål å stjele påloggingsopplysninger fra toppledere (C-nivå). (7 bokstaver)

8 vannrett: SVINDEL Uredelig opplegg utformet for å stjele penger eller tilgang til påloggingsopplysninger fra ofre. (7 bokstaver)

LODDRETT

1 loddrett: VERIFISERING Bekreftelse av betalingsopplysninger via en pålitelig sekundær kontaktmetode. (12 bokstaver)

3 loddrett: FALSIFISERTE Etterlignet e-postavsender eller nettadresse utformet for å se legitim ut. (12 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. F S N E I K N I T G T — **NETTFISKING**
2. V S G N I H I — **VISHING**
3. V E E S N R R I G F I I — **VERIFISERING**
4. G H I L N W A — **WHALING**
5. A R S I E L I E F F T S — **FALSIFISERTE**
6. E I D S N L V — **SVINDEL**
7. G E R E B A A B I R N D K — **BANKBEDRAGERI**
8. S M H G S N I I — **SMISHING**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"OPPDAG NETTFISKING MED SKANNER OG VERIFISERING"

Fasit til casestudiene

A Casestudie 1: Forebygging av bedrageri med bedriftsoverføringer

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En økonomiavdeling mottar en hasteepost fra en forfalsket leverandøradresse som ber om at fremtidige fakturabetalinger sendes til et nytt rutenummer.
- Anbefalt strategi og løsning: Innfør en policy med dobbel autorisasjon for alle betalinger. Innfør verifisering utenfor båndet via et forhåndslagret telefonnummer, og blokker e-poster fra forfalskede domener i gatewayen.

B Casestudie 2: Nettfiskingshendelse med hvalfangst mot leder

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En leder klikket på en nettfiskingslenke som hevdet å inneholde et sikkert styremøtedokument, og skrev inn sin primære bedriftspålogging på en forfalsket portal.
- Anbefalt strategi og løsning: Isoler lederens enhet. Tilbakestill alle bedriftens øktnøkler og all legitimasjon. Gå gjennom tilgangslogger for dataeksfiltrering, og innfør maskinvarebasert MFA på alle innlogginger.