Navn: _____ Dato: _____ Poeng: _____

Forebygging av identitetstyveri og eiendeler Sikkerhetsguide

Lekkasjer av legitimasjon, MFA, overvåking av darknet, varsler om kredittsperre, sosial manipulering

LÆRINGSOVERSIKT: FOREBYGGING AV IDENTITETSTYVERI

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 forebygging og reduksjon av identitetstyveri. Du utforsker lekkasjer av legitimasjon, flerfaktorautentisering, overvåking av mørkenettet, varsler om kredittsperre og forsvar mot sosial manipulering.

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/identitetstyveri/

Din læringsveiledning for identitetsbeskyttelse

- Forstå risikoen for at legitimasjon eksponeres på fora på det mørke nettet.
- Innfør flerfaktorautentisering (MFA) og varsler om kredittsperre.
- Utform forsvar for bedriftens sikkerhet mot målrettede svindelforsøk med sosial manipulering.

INSTRUKSJONER FOR GUIDE OM IDENTITETSTYVERI

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

FOREBYGGING AV IDENTITETSTYVERI OG SIKRING AV EIENDELER (INNLEDNING)

Identitetstyveri utnytter lekket påloggingsinformasjon og svake innlogginger til å kapre personlige kontoer og bedriftskontoer. Innføring av MFA, kredittsperrer, skannere for det mørke nettet og rammeverkene SPF/DKIM/DMARC er et viktig forsvar mot digital etterligning.

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

Kontrollpunkt 1: Flervalgsutfordring

1 **1. Hva er hovedmetoden identitetstyver bruker for å stjele påloggingsopplysninger?**

- A. Å sende falske e-postvarsler som lurer brukere til å skrive inn passord på forfalskede portaler
- B. Å lytte til radiosendinger i nærheten av en brukers bedriftskontor
- C. Å defragmentere lagringsstasjonen på en brukers lokale server
- D. Å koble fra eksterne konfigurasjoner for nettverkssikkerhetskopiering

2 **2. Hvilken sikkerhetskontroll gir det sterkeste forsvaret mot lekkasje av påloggingsopplysninger?**

- A. Flerfaktorautentisering med maskinvarenøkler
- B. Å lage lange passord med nettleserens standardformater
- C. Å bytte e-postbrukernavn hver sjette måned
- D. Å slette lagret sporingshistorikk fra informasjonskapsler i nettleseren

3 **3. Hva representerer kredittfrysing?**

- A. Å låse kredittrapporter for å hindre tyver i å opprette uautoriserte lån
- B. Å slette transaksjonshistorikk fra bankkontoer i databaser
- C. Å deaktivere magnetstripelesere for kredittkort på skannere
- D. Å kryptere lokale databaseharddisker i hvile

4 **4. Hvorfor er overvåking av det mørke nettet nyttig?**

- A. Den varsler brukere hvis lekket legitimasjon dukker opp i ulovlige databaser
- B. Den hindrer aktiv skadevare i å kjøre i virtuelle sandkasser
- C. Den øker nettleserens rutingshastighet i virtuelle nettverk
- D. Den blokkerer forsøk på SQL-injeksjon mot databasen i bakkant

5 **5. Hva betyr sosial manipulering?**

- A. Å manipulere folk til å frivillig oppgi konfidensiell legitimasjon
- B. Å skanne bedriftens serverporter etter aktive sikkerhetshull
- C. Å sikkerhetskopiere systemets databasefiler til frakoblede harddisker
- D. Å rute nettverkspakker gjennom tre krypterte onion-noder

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Identitetstyveri rammer bare digitale kontoer på nett, ikke fysisk post.

○ Sant ○ Usant

7 Spørsmål 7

7. Å håndheve MFA på alle personlige kontoer blokkerer de fleste botangrep med gjenbruk av påloggingsopplysninger (credential stuffing).

○ Sant ○ Usant

8 Spørsmål 8

8. En kredittsperre blokkerer kredittsjekker, men hindrer deg i å få tilgang til din egen bankkonto.

○ Sant ○ Usant

9 Spørsmål 9

9. Passordbehandlere beskytter brukerne mot nettfisking ved å nekte å fylle ut passord automatisk på forfalskede domener.

○ Sant ○ Usant

10 Spørsmål 10

10. Nettfiskings-e-poster bruker ofte hastespråk for å utløse følelsesmessige, raske reaksjoner.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. Identitetstyver er ute etter personlige passord og brukerens _____ .
2. Varsling av brukere om databrudd avdekker _____ av private kontoer.
3. Å kreve en midlertidig kode for å logge inn kalles _____ -autentisering.
4. Å skanne hackerforum etter stjålne data kalles dark web- _____ .
5. Å blokkere uautoriserte kredittsjekker krever en _____ .
6. Å lære opp ansatte i å gjenkjenne nettfisking bygger et aktivt _____ for sikkerheten.

ORDBANK

FLERFAKTOR FORSVAR INNLOGGINGSDATA KREDITTSPERRE LEKKASJER
NETTFISKING OVERVÅKING SPOOFING

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble sikkerhetsbegreper

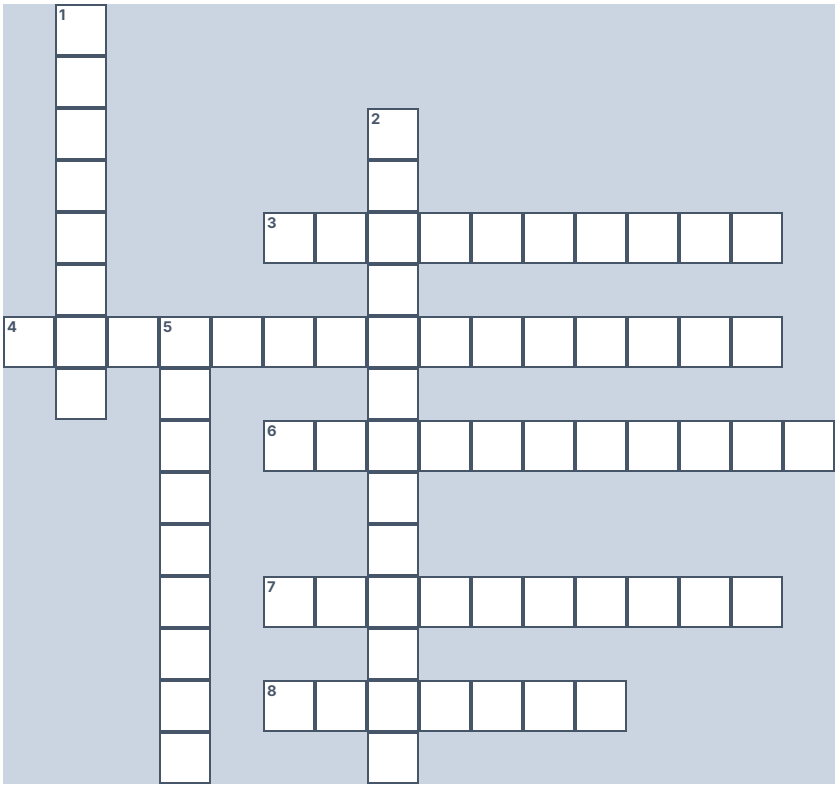
KOBLE DEFINISJONER

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

☐	1. LEGITIMASJON	A	Et sekundært verifiseringstrinn (for eksempel maskinvarenøkler) som beskytter kontopåloggинger.
☐	2. LEKKASJER	B	Å lage et falskt nettsted eller en falsk e-post som imiterer en legitim organisasjon.
☐	3. MFA	C	Begrensning av tilgang til kredittfiler for å hindre uredelige lånesøknader.
☐	4. OVERVÅKING	D	Uautorisert eksponering av private databaser som inneholder brukeres personlige poster.
☐	5. FRYS	E	Opplæring og tekniske kontroller som brukes for å beskytte mot identitetstyveri.
☐	6. FORSVAR	F	Å sende falske meldinger for å lure brukere til å gi fra seg påloggingsopplysninger.
☐	7. FORFALSKNING (SPOOFING)	G	Skanning av nettfora og hackerkanaler etter stjålne bedriftsdata.
☐	8. NETTFISKING	H	Brukernavn, passord og private tokens som brukes til å autentisere digitale identiteter.

Kontrollpunkt 5: Kryssord

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



VANNRETT

3. Sekundært verifiseringstrinn (for eksempel maskinvarenøkler) som beskytter kontoinnlogginger. (10)

4. Brukernavn, passord og private tokener som brukes til å autentisere digitale identiteter. (15)

6. Utsending av uredelige meldinger for å lure brukere til å gi fra seg påloggingsinformasjon. (11)

7. Skanning av nettforum og hackerkanaler etter stjålne bedriftsdata. (10)

8. Opplæring og tekniske kontroller som brukes til å beskytte mot identitetstyveri. (7)

LODDRETT

1. Å lage et falskt nettsted eller en falsk e-post for å etterligne en legitim organisasjon. (8)

2. Begrensning av tilgang til kredittfiler for å hindre uredelige lånesøknader. (13)

5. Uautorisert eksponering av private databaser som inneholder personlige brukeropplysninger. (9)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

3 vannrett: Sekundært verifiseringstrinn (for eksempel maskinvarenøkler) som beskytter kontoinnlogginger. (10 bokstaver):

4 vannrett: Brukernavn, passord og private tokener som brukes til å autentisere digitale identiteter. (15 bokstaver):

6 vannrett: Utsending av uredelige meldinger for å lure brukere til å gi fra seg påloggingsinformasjon. (11 bokstaver):

7 vannrett: Skanning av nettforum og hackerkanaler etter stjålne bedriftsdata. (10 bokstaver):

8 vannrett: Opplæring og tekniske kontroller som brukes til å beskytte mot identitetstyveri. (7 bokstaver):

LODDRETT

1 loddrett: Å lage et falskt nettsted eller en falsk e-post for å etterligne en legitim organisasjon. (8 bokstaver):

2 loddrett: Begrensning av tilgang til kredittfiler for å hindre uredelige lånesøknader. (13 bokstaver):

5 loddrett: Uautorisert eksponering av private databaser som inneholder personlige brukeropplysninger. (9 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

INNLOGGINGSDATA
LEKKASJER
FLERFAKTOR
OVERVÅKING
KREDITTSPERRE
FORSVAR
SPOOFING
NETTFISKING

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. INNLOGGINGSDATA
B. LEKKASJER
C. FLERFAKTOR
D. OVERVÅKING
E. KREDITTSPERRE
F. FORSVAR
G. SPOOFING
H. NETTFISKING

DEFINISJONER OG TILHØRENDE FELT	
	1. Utsending av uredelige meldinger for å lure brukere til å gi fra seg påloggingsinformasjon.
	2. Brukernavn, passord og private tokener som brukes til å autentisere digitale identiteter.
	3. Å lage et falskt nettsted eller en falsk e-post for å etterligne en legitim organisasjon.
	4. Opplæring og tekniske kontroller som brukes til å beskytte mot identitetstyveri.
	5. Skanning av nettforum og hackerkanaler etter stjålne bedriftsdata.
	6. Begrensning av tilgang til kredittfiler for å hindre uredelige lånesøknader.
	7. Uautorisert eksponering av private databaser som inneholder personlige brukeropplysninger.
	8. Sekundært verifiseringstrinn (for eksempel maskinvarenøkler) som beskytter kontoinnlogginger.

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. GGGNSNINDAI TLAO
2. ORFLFRKTAE
3. RKSEPREETIT RD
4. ONGIFSPO
5. JAERSKLEK
6. NVRKIOVÅGE
7. FAVROSR
8. ISGITNFENKT

Bonusaktivitet: Tenk raskt

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

1	Ting å gjøre hvis identiteten din er stjålet			
2	Ting du ikke bør dele på sosiale medier			
3	Ting du tar sikkerhetskopi av			
4	Kort eller ID-er i lommeboken din			
5	Dokumenter du bør beskytte			
6	Ting å gjøre etter en datalekkasje			
7	Grunner til å oppdatere programvare			
8	Informasjon en identitetstyv vil ha			
9	Enheter som kan hackes			
10	Steder dataene dine kan lekke fra			
11	Trygge vaner du kan begynne med i dag			
12	Tegn på at en datamaskin er infisert			
13	Måter å bevise hvem du er på			
14	Tegn på identitetstyveri			
15	Advarselstegn i en e-post			

Kontrollpunkt 8: Casestudier om cybersikkerhet

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

CASESTUDIE 1: BESKYTTELSE MOT IDENTITETSFORFALSKNING AV LEDERE



Scenario: En profilert toppleder har blitt rammet av domenenavn med skrivefeil (typosquatting) som etterligner vedkommendes private e-postadresse for å svindle kunder. Utform en plan for merkevarebeskyttelse.

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

CASESTUDIE 2: EKSPONERING AV BEDRIFTSLEGITIMASJON PÅ DARKNET



Scenario: Et dumpet datasett fra det mørke nettet inneholder flere hundre påloggingsopplysninger for selskapet som tilhører systemadministratorer. Utform en strategi for å redusere skadene.

Diskusjonsspørsmål: Skisser prosessen for å rydde opp i påloggingsopplysninger, og planlegg innføringen av en passordbehandler.

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

2	5	19	11	25	20	20		9	4	5	14	20	9	20	5	20	5	14
4	9	14		13	5	4		6	12	5	18	6	1	11	20	15	18	

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 identitetstyveri?

En forbrytelse der en angriper stjeler personlige opplysninger (som passord eller personnumre) for å utgi seg for å være en annen person og oppnå økonomisk vinning.

Q2: Hva er den vanligste årsaken til identitetstyveri?

Nettfisking er en av de viktigste måtene tyver får tak i passord på, ved å lokke brukere til falske, forfalskede nettsteder.

Q3: Hvordan beskytter flerfaktorautentisering (MFA) identiteter?

MFA krever et ekstra bevis (som en maskinvarenøkkel) for å logge inn, og hindrer angripere selv om de stjeler passordet ditt.

Q4: Hva er en kredittsperre?

En gratis tjeneste som hindrer kredittopplysningsbyråer i å dele kredittfilen din og stopper tyver fra å opprette nye lån i ditt navn. [2]

Q5: Hva er overvåking av det mørke nettet?

Programvare som sjekker hackerforum etter lekkede e-postadresser, passord og personlige opplysninger, og varsler deg hvis dataene dine er eksponert.

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

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

Q6: Hva betyr credential stuffing?

Automatiserte roboter som tester lekkede passordlister på hundrevis av nettsteder for å overta aktive kontoer.

Q7: Hvorfor er e-postforfalskning (spoofing) farlig?

Den lar angripere forfalske avsenderens navn i e-poster, slik at nettfiskingsmeldinger ser ut til å komme fra pålitelige kolleger.

Q8: Hvordan stopper passordbehandlere identitetstyveri?

De lagrer komplekse, unike passord for hver konto og nekter å fylle ut påloggingsinformasjon automatisk på falske nettfiske-domener.

Q9: Hva er målrettet nettfisking (spear phishing)?

Et svært målrettet nettfiskeangrep tilpasset med offerets navn og opplysninger for å øke sjansen for å lure det.

Q10: Hvordan skiller et kredittvarsel seg fra en kredittsperre?

Et varsel ber långivere om å verifisere identiteten din før de oppretter kontoer, mens en sperre blokkerer tilgangen til kredittfilen din fullstendig. [2]

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

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

Q1: Hvordan fører SIM-bytte (SIM swapping) til identitetstyveri?

Angripere overbeviser ansatte hos teleoperatøren om å overføre offerets telefonnummer til et nytt SIM-kort, slik at de kaprer SMS-baserte 2FA-koder.

Q2: Hvilken rolle har DMARC for å forhindre identitetstyveri?

DMARC lar domeneeiere blokkere forfalskede e-poster før de når innboksen, slik at falske e-poster ikke kan etterligne bedriftsdomener.

Q3: Hvorfor er syntetisk identitetstyveri vanskelig å oppdage?

Tyver kombinerer ekte personnumre med falske navn og fødselsdatoer for å bygge helt nye kredittprofiler og omgå grunnleggende svindelvarsler.

Q4: Hvordan utnytter databrokere personlige identiteter?

Datameglere samler offentlige registre, nettatferd og kjøpshistorikk for å sette sammen profildossierer, som kan lekke eller bli solgt.

Q5: Hvorfor anses SMS-basert MFA som sårbar?

SMS-trafikk er sårbar for avlytting, phishing og utnyttelser av SIM-bytte på operatørnivå.

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

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

Q6: Hva er en kredittfillås?

En kommersiell tjeneste som ligner på en kredittsperre, og som lar brukere låse eller låse opp kredittfilen sin umiddelbart via en mobilapp.

Q7: Hvordan bidrar datainnbrudd i selskaper til identitetstyveri?

Lekkede databaser avslører millioner av passord i klartekst og gir tyver rådataene som trengs for å utføre målrettet identitetssvindel.

Q8: Hva er risikoen ved å dele for mye i sosiale medier?

Å dele kjæledyrnavn, fødested og morens pikenavn offentlig gir tyver svarene på vanlige spørsmål for gjenoppretting av kontoer.

Q9: Hvordan beskytter biometrisk pålogging identitetsprofiler?

Biometri knytter påloggінger til trekk som fingeravtrykk eller ansikt. Når de holdes på enheten, er de vanskelige å stjele, men lagrede biometriske data kan lekke.

Q10: Hvordan bekjemper Red Flags Rule identitetstyveri?

En føderal forskrift som krever at finansinstitusjoner utvikler skriftlige programmer for å oppdage og reagere på varselsignaler om identitetstyveri.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

IdentityTheft.gov, drevet av FTC, lar ofre i USA rapportere identitetstyveri og få en personlig gjenopprettingsplan. [1]

2. SIKKERHETSINNSIKT

Maskinvaresikkerhetsnøkler er phishing-resistent MFA, den sterkeste formen for MFA som CISA anbefaler. [4]

3. SIKKERHETSINNSIKT

Kompromitterte passord er et vanlig inngangspunkt ved datainnbrudd og gir drivstoff til senere identitetsbedrageri.

4. SIKKERHETSINNSIKT

En kredittsperre er gratis ifølge føderal lov og hindrer långivere i å sjekke kredittfiler til den låses opp. [2]

5. SIKKERHETSINNSIKT

DMARC lar domeneeiere be e-postservere om å avvise eller sette i karantene forfalsket e-post som feiler kontrollene. [7]

6. SIKKERHETSINNSIKT

SIM-bytte (SIM swapping) lar hackere omgå SMS-basert tofaktorautentisering i nettbankportaler.

7. SIKKERHETSINNSIKT

Svindel med syntetisk identitet blander ekte og falske opplysninger, noe som gjør det vanskelig for långivere å oppdage.

8. SIKKERHETSINNSIKT

Mange gjenbruker det samme passordet på flere nettkontoer, så ett datainnbrudd kan avsløre flere av dem.

9. SIKKERHETSINNSIKT

Datameglere samler detaljerte dossierer om store mengder forbrukere, noe som skaper en konsentrert personvernrisiko.

10. SIKKERHETSINNSIKT

Å komme seg etter identitetstyveri kan ta måneder med arbeid, for eksempel å bestride belastninger og rette opp kredittrapporter.

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.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

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

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

Fasit: Kontrollpunkt 1 – flervalg

1 Spørsmål 1

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er hovedmetoden identitetstyver bruker for å stjele påloggingsopplysninger? → Å sende falske e-postvarsler som lurer brukere til å skrive inn passord på forfalskede portaler

2 Spørsmål 2

Riktig svar: A

MERKNAD TIL LÆREREN

Hvilken sikkerhetskontroll gir det sterkeste forsvaret mot lekkasje av påloggingsopplysninger? → Flerfaktorautentisering med maskinvarenøkler

3 Spørsmål 3

Riktig svar: A

MERKNAD TIL LÆREREN

Hva representerer kredittfrysing? → Å låse kredittrapporter for å hindre tyver i å opprette uautoriserte lån

4 Spørsmål 4

Riktig svar: A

MERKNAD TIL LÆREREN

Hvorfor er overvåking av det mørke nettet nyttig? → Den varsler brukere hvis lekket legitimasjon dukker opp i ulovlige databaser

5 Spørsmål 5

Riktig svar: A

MERKNAD TIL LÆREREN

Hva betyr sosial manipulering? → Å manipulere folk til å frivillig oppgi konfidensiell legitimasjon

Fasit: Kontrollpunkt 2 – sant eller usant

6 Spørsmål 6

Riktig svar: Usant

MERKNAD TIL LÆREREN

Identitetstyveri kan også starte frakoblet, for eksempel ved stjålet post eller stjålne dokumenter.

7 Spørsmål 7

Riktig svar: Sant

MERKNAD TIL LÆREREN

Å håndheve MFA på alle personlige kontoer blokkerer de fleste botangrep med gjenbruk av påloggingsopplysninger (credential stuffing).

8 Spørsmål 8

Riktig svar: Usant

MERKNAD TIL LÆREREN

Et kredittfrys stopper nye kredittsjekker, men påvirker ikke de eksisterende kontoene dine.

9 Spørsmål 9

Riktig svar: Sant

MERKNAD TIL LÆREREN

Passordbehandlere beskytter brukerne mot nettfisking ved å nekte å fylle ut passord automatisk på forfalskede domener.

10 Spørsmål 10

Riktig svar: Sant

MERKNAD TIL LÆREREN

Nettfiskings-e-poster bruker ofte hastespråk for å utløse følelsesmessige, raske reaksjoner.

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

H 1. LEGITIMASJON	D 2. LEKKASJER	A 3. MFA	G 4. OVERVÅKING
C 5. FRYS	E 6. FORSVAR	B 7. FORFALSKNING (SPOOFING)	F 8. NETTFISKING

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 INNLOGGINGSDATA	2 LEKKASJER	3 FLERFAKTOR	4 OVERVÅKING
5 KREDITTSPERRE	6 FORSVAR		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 H – NETTFISKING	2 A – INNLOGGINGSDATA	3 G – SPOOFING	4 F – FORSVAR
5 D – OVERVÅKING	6 E – KREDITTSPERRE	7 B – LEKKASJER	8 C – FLERFAKTOR

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare LEGITIMASJON, LEKKASJER og MFA med egne ord og gi et eksempel på hvert.

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

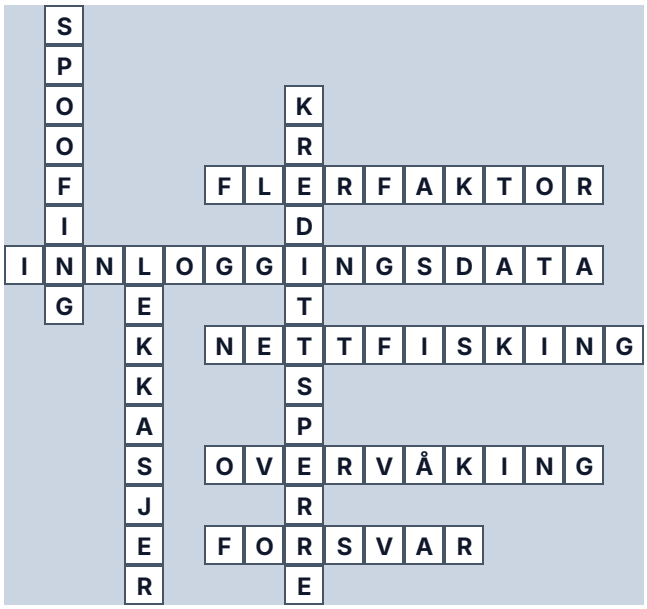
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

3 vannrett: FLERFAKTOR Sekundært verifiseringstrinn (for eksempel maskinvarenøkler) som beskytter kontoinnlogginger. (10 bokstaver)

4 vannrett: INNLOGGINGSDATA Brukernavn, passord og private tokener som brukes til å autentisere digitale identiteter. (15 bokstaver)

6 vannrett: NETTFISKING Utsending av uredelige meldinger for å lure brukere til å gi fra seg påloggingsinformasjon. (11 bokstaver)

7 vannrett: OVERVÅKING Skanning av nettforum og hackerkanaler etter stjålne bedriftsdata. (10 bokstaver)

8 vannrett: FORSVAR Opplæring og tekniske kontroller som brukes til å beskytte mot identitetstyveri. (7 bokstaver)

LODDRETT

1 loddrett: SPOOFING Å lage et falskt nettsted eller en falsk e-post for å etterligne en legitim organisasjon. (8 bokstaver)

2 loddrett: KREDITTSPERRE Begrensning av tilgang til kredittfiler for å hindre uredelige lånesøknader. (13 bokstaver)

5 loddrett: LEKKASJER Uautorisert eksponering av private databaser som inneholder personlige brukeropplysninger. (9 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. GGGNSNINDAITLAO — **INNLOGGINGSDATA**
2. ORFLFRKTAE — **FLERFAKTOR**
3. RKSEPREETITRD — **KREDITTSPERRE**
4. ONGIFSPO — **SPOOFING**
5. JAERSKLEK — **LEKKASJER**
6. NVRKIOVÅGE — **OVERVÅKING**
7. FAVROSR — **FORSVAR**
8. ISGITNFENKT — **NETTFISKING**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"BESKYTT IDENTITETEN DIN MED FLERFAKTOR"

Fasit til casestudiene

A Casestudie 1: Beskyttelse mot identitetsforfalskning av ledere

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En fremtredende toppleder har vært mål for typo-squattede domenenavn som imiterer vedkommendes personlige e-post for å lure kunder. Utform en plan for merkevarebeskyttelse.
- Anbefalt strategi og løsning: Registrer alle vanlige stavevarianter av lederens navn. Ta i bruk e-postautentiseringsprotokoller (DMARC, DKIM, SPF) for å hindre domeneforfalskning. Håndhev maskinvarebasert MFA på alle innlogginger for toppledelsen.

B Casestudie 2: Eksponering av bedriftslegitimasjon på darknet

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: Et datautslipp fra det mørke nettet inneholder flere hundre bedriftspåloggingsopplysninger som tilhører systemadministratorer i en bedrift. Utform en strategi for å redusere skadene.
- Anbefalt strategi og løsning: Gjennomfør tilbakestilling av passord for hele selskapet. Krev bruk av en passordbehandler for bedrifter. Håndhev MFA i alle systemportaler og sett opp kontinuerlige, automatiserte varsler om overvåking av det mørke nettet.