Navn: _____ Dato: _____ Point: _____

Forebyggelse af identitetstyveri i virksomheder

Lækager af loginoplysninger, MFA, overvågning af det mørke net, advarsler om kreditspærring, social engineering

OVERBLIK OVER FOREBYGGELSE AF IDENTITETSTYVERI

SIKRET

DATAKRYPTERING

256-bit AES-standard

OVERHOLDER KRAV

GLOBALE STANDARDER

GDPR- og CCPA-rammer

ZERO-TRUST

ADGANGSPOLITIK

Multifaktorgodkendelse

Velkommen! Denne opgavepakke fører dig gennem forebyggelse og håndtering af identitetstyveri. Du vil udforske lækkede loginoplysninger, flerfaktorgodkendelse, overvågning af det mørke net, kreditspærring og forsvar mod social manipulation.

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/identitetstyveri/

Din læringsplan for beskyttelse af identiteten

- Forstå risikoen, når loginoplysninger dukker op på fora på det mørke net.
- Indfør flerfaktorgodkendelse (MFA) og kreditspærring.
- Design virksomhedens forsvar mod målrettet social manipulation.

VEJLEDNING TIL GUIDEN OM IDENTITETSTYVERI

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 beskyttelse af identiteten. Slut af med bonusaktiviteten Tænk hurtigt.

FOREBYGGELSE AF IDENTITETSTYVERI OG SIKRING AF AKTIVER (INTRODUKTION)

Identitetstyveri udnytter lækkede loginoplysninger og svage logins til at overtage private konti og firmakonti. MFA, kreditspærring, scanning af det mørke net samt SPF, DKIM og DMARC er et afgørende forsvar mod digital efterligning.

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

Kontrolpunkt 1: Flervalgsopgave

1. Hvilken metode bruger identitetstyve oftest til at stjæle loginoplysninger?

- A. Falske e-mails, der lokker brugere til at taste adgangskoder på forfalskede sider
- B. At lytte til radioudsendelser nær brugerens kontor
- C. At defragmentere brugerens lokale serverdrev
- D. At afbryde eksterne backupopsætninger

2. Hvilken kontrol giver det stærkeste forsvar mod lækkede loginoplysninger?

- A. Flerfaktorgodkendelse med hardwarenøgler
- B. Lange adgangskoder i browserens standardformat
- C. Nyt e-mailbrugernavn hvert halve år
- D. Sletning af cookies og browserhistorik

3. Hvad er en kreditspærring?

- A. Låsning af kreditoplysninger, så tyve ikke kan optage lån i dit navn
- B. Sletning af bankens transaktionshistorik
- C. Deaktivering af magnetstribelæsere
- D. Kryptering af lokale databasediske i hvile

4. Hvorfor er overvågning af det mørke net nyttig?

- A. Den advarer, hvis dine lækkede loginoplysninger dukker op i ulovlige databaser
- B. Den forhindrer malware i at køre i sandkasser
- C. Den gør browseren hurtigere på virtuelle net
- D. Den blokerer SQL-injektion mod databaser

5. Hvad betyder social manipulation?

- A. At manipulere folk til frivilligt at afsløre fortrolige loginoplysninger
- B. At scanne firmaets serverporte for sårbarheder
- C. At tage backup af databasefiler på offline diske
- D. At sende pakker gennem tre krypterede onion-noder

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Identitetstyveri rammer kun digitale konti, ikke fysisk post.

○ Sandt ○ Falsk

7 Spørgsmål 7

7. MFA på alle private konti stopper de fleste automatiske angreb med lækkede adgangskoder.

○ Sandt ○ Falsk

8 Spørgsmål 8

8. En kreditspærring blokerer kredittjek, men spærrer også din adgang til din egen bankkonto.

○ Sandt ○ Falsk

9 Spørgsmål 9

9. Adgangskodeadministratorer beskytter mod phishing ved ikke at udfylde adgangskoder på forfalskede domæner.

○ Sandt ○ Falsk

10 Spørgsmål 10

10. Phishingmails bruger ofte et presserende sprog for at fremkalde hurtige, følelsesstyrede reaktioner.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. Identitetstyve går efter adgangskoder og brugernes _____ .
2. Advarsler om databrud viser, om private konti er ramt af _____ .
3. At kræve en midlertidig kode ved login kaldes _____ .
4. Når hackerfora gennemsøges for stjålne data, kaldes det _____ .
5. For at blokere uautoriserede kredittjek kræves en _____ .
6. Træning af medarbejdere i at genkende phishing opbygger et aktivt _____ .

ORDBANK MED FAGUDTRYK

DATAUDSLIP FORSVAR LOGINOPLYSNINGER MFA OVERVÅGNING PHISHING SPOOFING SPÆRRING

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

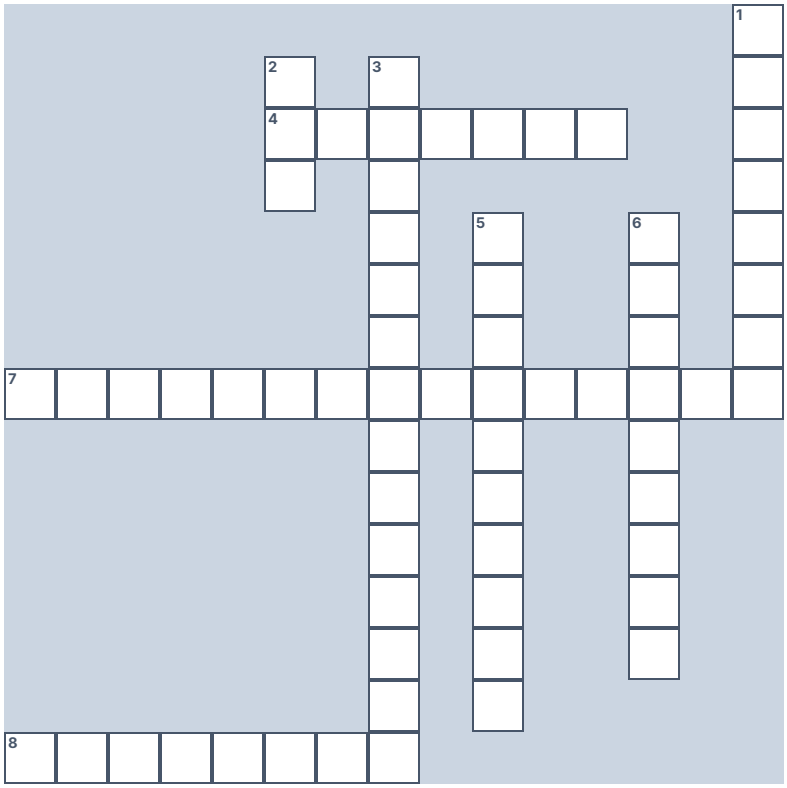
MATCH BEGREBER OG DEFINITIONER

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

☐	1. LOGINOPLYSNINGER	A	Ekstra kontroltrin (f.eks. hardwarenøgler), der beskytter logins.
☐	2. DATAUDSLIP	B	Et falsk websted eller en falsk e-mail, der efterligner en ægte organisation.
☐	3. MFA	C	Begrænset adgang til kreditoplysninger mod svigagtige låneansøgninger.
☐	4. OVERVÅGNING	D	Uautoriseret afsløring af databaser med personlige oplysninger.
☐	5. SPÆRRING	E	Træning og tekniske kontroller mod identitetstyveri.
☐	6. FORSVAR	F	Svigagtige beskeder, der lokker brugere til at udlevere loginoplysninger.
☐	7. SPOOFING	G	Scanning af fora og hackerkanaler for stjålne firmadata.
☐	8. PHISHING	H	Brugernavne, adgangskoder og private nøgler, der bekræfter en digital identitet.

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

4. Det, som træning af medarbejdere i at genkende phishing opbygger (7)

7. Gennemsøgning af hackerfora for stjålne oplysninger (15)

8. Svigagtige beskeder, der skal lokke brugere til at udlevere logins (8)

LODRETTE NØGLER

1. Et falsk websted eller en falsk e-mail, der efterligner en ægte afsender (8)

2. Krav om en ekstra kode eller nøgle ved login (3)

3. Blokering af kredittjek, så ingen kan optage lån i dit navn (14)

5. Når private oplysninger slipper ud af en database uden tilladelse (10)

6. Brugernavne og adgangskoder, som identitetstyve går efter (9)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

4 vandret: Det, som træning af medarbejdere i at genkende phishing opbygger (7 bogstaver):

7 vandret: Gennemsøgning af hackerfora for stjålne oplysninger (15 bogstaver):

8 vandret: Svigagtige beskeder, der skal lokke brugere til at udlevere logins (8 bogstaver):

LODRETTE NØGLER

1 lodret: Et falsk websted eller en falsk e-mail, der efterligner en ægte afsender (8 bogstaver):

2 lodret: Krav om en ekstra kode eller nøgle ved login (3 bogstaver):

3 lodret: Blokering af kredittjek, så ingen kan optage lån i dit navn (14 bogstaver):

5 lodret: Når private oplysninger slipper ud af en database uden tilladelse (10 bogstaver):

6 lodret: Brugernavne og adgangskoder, som identitetstyve går efter (9 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

LOGINDATA DATAUDSLIP MFA DARKWEBSCANNING KREDITSPÆRRING
FORSVAR SPOOFING PHISHING

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. LOGINDATA
B. DATAUDSLIP
C. MFA
D. DARKWEBSCANNING
E. KREDITSPÆRRING
F. FORSVAR
G. SPOOFING
H. PHISHING

DEFINITIONER OG MATCHFELTER
[ ] 1. Svigagtige beskeder, der skal lokke brugere til at udlevere logins.
[ ] 2. Brugernavne og adgangskoder, som identitetstyve går efter.
[ ] 3. Et falsk websted eller en falsk e-mail, der efterligner en ægte afsender.
[ ] 4. Det, som træning af medarbejdere i at genkende phishing opbygger.
[ ] 5. Gennemsøgning af hackerfora for stjålne oplysninger.
[ ] 6. Blokering af kredittjek, så ingen kan optage lån i dit navn.
[ ] 7. Når private oplysninger slipper ud af en database uden tilladelse.
[ ] 8. Krav om en ekstra kode eller nøgle ved login.

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. **DNIOLATAG**
2. **AFM**
3. **KÆRNPGRRES ITID**
4. **ONGIFSPO**
5. **LDPAASUDIT**
6. **NBIRESANGN DACKW**
7. **FAVROSR**
8. **SHHGPNII**

Bonusaktivitet: Tænk hurtigt

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

1	Ting at gøre, hvis din identitet stjæles			
2	Ting, du ikke bør dele på sociale medier			
3	Ting, du tager backup af			
4	Kort eller id'er i din pung			
5	Dokumenter, du skal passe på			
6	Ting at gøre efter et datalæk			
7	Grunde til at opdatere software			
8	Oplysninger, en identitetstyv vil have			
9	Enheder, der kan blive hacket			
10	Steder, dine data kan lække fra			
11	Sikkerhedsvaner, du kan starte i dag			
12	Tegn på, at en computer er inficeret			
13	Måder at bevise, hvem du er			
14	Tegn på identitetstyveri			
15	Advarselstegn i en e-mail			

Kontrolpunkt 8: Casestudier om cybersikkerhed

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

CASESTUDIE 1: BESKYTTELSE MOD EFTERLIGNING AF LEDERE



Scenarie: En kendt topchef er blevet ramt af domæner med stavefejl, der efterligner chefens e-mail for at snyde kunder. Design en plan til beskyttelse af brandet.

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

CASESTUDIE 2: FIRMALOGINS PÅ DET MØRKE NET



Scenarie: Et datadump på det mørke net indeholder flere hundrede firmalogins, der tilhører en virksomheds systemadministratorer. Design en plan for at begrænse skaden.

Diskussion: Beskriv oprydningen i loginoplysninger, og planlæg udrulning af en adgangskodeadministrator.

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

2	5	19	11	25	20		4	9	14		9	4	5	14	20	9	20	5	20

13	5	4		13	6	1

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 identitetstyveri?

En forbrydelse, hvor en angriber stjæler personlige oplysninger (som adgangskoder eller personnumre) for at udgive sig for en anden og tjene penge.

Q2: Hvad er den hyppigste årsag til identitetstyveri?

Phishing er en af de mest udbredte måder, tyve får fat i adgangskoder på, ved at lokke brugere ind på falske, forfalskede hjemmesider.

Q3: Hvordan beskytter flerfaktorgodkendelse (MFA) identiteten?

MFA kræver et ekstra bevis (som en hardwarenøgle) ved login og stopper angribere, selv hvis de har din adgangskode.

Q4: Hvad er en kreditspærring?

En gratis tjeneste, der forhindrer kreditbureauer i at dele dine oplysninger, så tyve ikke kan optage lån i dit navn. [2]

Q5: Hvad er overvågning af det mørke net?

Software, der tjekker hackerfora for lækkede e-mails, adgangskoder og oplysninger og advarer dig, hvis dine data dukker op.

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvad er credential stuffing?

Automatiske bots, der afprøver lister med lækkede adgangskoder på hundredvis af websteder for at overtage konti.

Q7: Hvorfor er forfalskede e-mails farlige?

Angribere kan forfalske afsenderen, så phishing ser ud til at komme fra betroede kolleger.

Q8: Hvordan stopper adgangskodeadministratorer identitetstyveri?

De gemmer stærke, unikke adgangskoder til hver konto og udfylder ikke oplysninger på falske domæner.

Q9: Hvad er spear phishing?

Et målrettet phishingangreb tilpasset med offerets navn og detaljer, så det er sværere at gennemskue.

Q10: Hvad er forskellen på en kreditadvarsel og en spærring?

En advarsel beder långivere bekræfte din identitet, før de opretter konti, mens en spærring helt blokerer adgangen til dine kreditoplysninger. [2]

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

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

Q1: Hvordan fører SIM-swap til identitetstyveri?

Angribere får teleselskabet til at flytte offerets nummer til et nyt SIM-kort og overtager dermed SMS-koderne.

Q2: Hvilken rolle spiller DMARC mod identitetstyveri?

Med DMARC kan domæneejere blokere forfalskede e-mails, så de ikke efterligner firmaets domæne i indbakkerne.

Q3: Hvorfor er syntetisk identitetstyveri svært at opdage?

Tyve kombinerer ægte personnumre med falske navne og fødselsdatoer og opbygger nye kreditprofiler, der slipper forbi almindelige advarsler.

Q4: Hvordan udnytter datamæglere personlige identiteter?

De samler offentlige oplysninger, adfærd på nettet og køb i profiler, som kan lække eller blive solgt.

Q5: Hvorfor anses MFA via SMS for sårbar?

SMS kan opsnappes, phishes og kapres med SIM-swap hos teleselskabet.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

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

Q6: Hvad er en kreditlås?

En kommerciel tjeneste som en spærring, hvor du med det samme kan låse og åbne dine kreditoplysninger i en app.

Q7: Hvordan giver databrud i virksomheder næring til identitetstyveri?

Lækkede databaser afslører millioner af loginoplysninger og giver tyve råmaterialet til målrettet svindel.

Q8: Hvad er risikoen ved at dele for meget på sociale medier?

Kæledyrs navne, fødesteder og mors pigenavn giver tyve svarene på almindelige sikkerhedsspørgsmål.

Q9: Hvordan beskytter biometrisk login identiteten?

Biometri knytter login til træk som fingeraftryk eller ansigter; opbevaret på enheden er de svære at stjæle, men lagrede biometriske data kan lække.

Q10: Hvordan bekæmper Red Flags Rule identitetstyveri?

En amerikansk regel, der kræver, at finansielle virksomheder har skriftlige programmer til at opdage og reagere på tegn på identitetstyveri.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

IdentityTheft.gov, som drives af FTC, lader ofre i USA anmelde identitetstyveri og få en personlig plan for genopretning. [1]

2. SIKKERHEDSINDSIGT

Hardwaresikkerhedsnøgler er phishing-resistent multifaktorgodkendelse (MFA), den stærkeste type MFA, som CISA opfordrer til. [4]

3. SIKKERHEDSINDSIGT

Kompromitterede adgangskoder er et almindeligt indgangspunkt ved databrud og giver næring til senere identitetssvindel.

4. SIKKERHEDSINDSIGT

En kreditspærring er gratis efter amerikansk lov og forhindrer långivere i at se kreditoplysninger, indtil den ophæves. [2]

5. SIKKERHEDSINDSIGT

DMARC lader domæneejere bede mailservere om at afvise eller sætte forfalskede e-mails, der ikke består kontrollerne, i karantæne. [7]

6. SIKKERHEDSINDSIGT

SIM-swap lader hackere omgå SMS-koder hos netbanker.

7. SIKKERHEDSINDSIGT

Syntetisk identitetssvindel blander ægte og falske oplysninger, hvilket gør det svært for långivere at opdage.

8. SIKKERHEDSINDSIGT

Mange genbruger den samme adgangskode på tværs af onlinekonti, så ét brud kan afsløre flere af dem.

9. SIKKERHEDSINDSIGT

Datamæglere samler detaljerede profiler om et stort antal forbrugere og skaber dermed en koncentreret risiko for privatlivet.

10. SIKKERHEDSINDSIGT

At komme sig efter identitetstyveri kan tage måneders arbejde, fx med at gøre indsigelse mod betalinger og rette kreditoplysninger.

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] 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

Facitliste: Kontrolpunkt 1 – Flervalg

1 Spørgsmål 1

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvilken metode bruger identitetstyve oftest til at stjæle loginoplysninger? → Falske e-mails, der lokker brugere til at taste adgangskoder på forfalskede sider

2 Spørgsmål 2

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvilken kontrol giver det stærkeste forsvar mod lækkede loginoplysninger? → Flerfaktorgodkendelse med hardwarenøgler

3 Spørgsmål 3

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er en kreditspærring? → Låsning af kreditoplysninger, så tyve ikke kan optage lån i dit navn

4 Spørgsmål 4

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvorfor er overvågning af det mørke net nyttig? → Den advarer, hvis dine lækkede loginoplysninger dukker op i ulovlige databaser

5 Spørgsmål 5

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad betyder social manipulation? → At manipulere folk til frivilligt at afsløre fortrolige loginoplysninger

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

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

UNDERVISNINGSNOTE

Identitetstyveri kan også begynde offline, fx med stjålen post eller stjålne dokumenter.

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

UNDERVISNINGSNOTE

MFA på alle private konti stopper de fleste automatiske angreb med lækkede adgangskoder.

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

UNDERVISNINGSNOTE

En kreditspærring stopper nye kreditvurderinger, men påvirker ikke dine eksisterende konti.

9 **Spørgsmål 9** — **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Adgangskodeadministratorer beskytter mod phishing ved ikke at udfylde adgangskoder på forfalskede domæner.

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

UNDERVISNINGSNOTE

Phishingmails bruger ofte et presserende sprog for at fremkalde hurtige, følelsesstyrede reaktioner.

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

H 1. LOGINOPLYSNINGER	D 2. DATAUDSLIP	A 3. MFA	G 4. OVERVÅGNING
C 5. SPÆRRING	E 6. FORSVAR	B 7. SPOOFING	F 8. PHISHING

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 LOGINOPLYSNINGER	2 DATAUDSLIP	3 MFA	4 OVERVÅGNING
5 SPÆRRING	6 FORSVAR		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 H – PHISHING	2 A – LOGINDATA	3 G – SPOOFING	4 F – FORSVAR
5 D – DARKWEBSCANNING	6 E – KREDITSPÆRRING	7 B – DATAUDSLIP	8 C – MFA

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare LOGINOPLYSNINGER, DATAUDSLIP og MFA med egne ord og give et eksempel på hvert begreb.

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

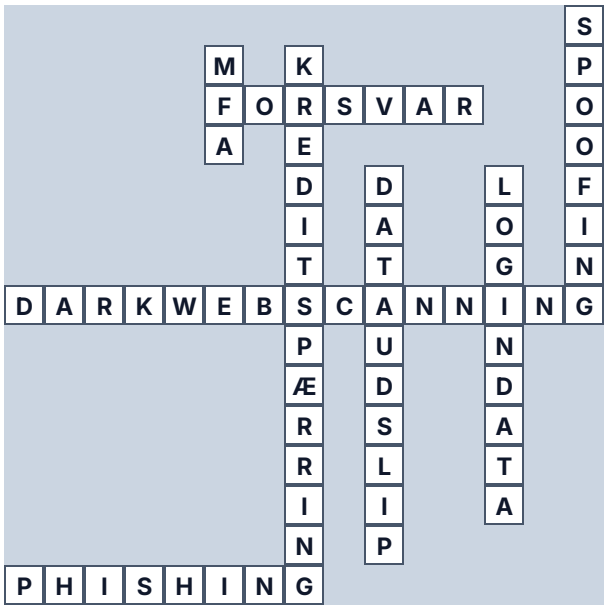
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

4 vandret: FORSVAR Det, som træning af medarbejdere i at genkende phishing opbygger (7 bogstaver)

7 vandret: DARKWEBSCANNING Gennemsøgning af hackerfora for stjålne oplysninger (15 bogstaver)

8 vandret: PHISHING Svigagtige beskeder, der skal lokke brugere til at udlevere logins (8 bogstaver)

LODRETTE NØGLER

1 lodret: SPOOFING Et falsk websted eller en falsk e-mail, der efterligner en ægte afsender (8 bogstaver)

2 lodret: MFA Krav om en ekstra kode eller nøgle ved login (3 bogstaver)

3 lodret: KREDITSPÆRRING Blokering af kredittjek, så ingen kan optage lån i dit navn (14 bogstaver)

5 lodret: DATAUDSLIP Når private oplysninger slipper ud af en database uden tilladelse (10 bogstaver)

6 lodret: LOGINDATA Brugernavne og adgangskoder, som identitetstyve går efter (9 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. D N I O L A T A G — **LOGINDATA**
2. A F M — **MFA**
3. K Æ R N P G R R E S I T I D — **KREDITSPÆRRING**
4. O N G I F S P O — **SPOOFING**
5. L D P A A S U D I T — **DATAUDSLIP**
6. N B I R E S A N G N D A C K W — **DARKWEBSCANNING**
7. F A V R O S R — **FORSVAR**
8. S H H G P N I I — **PHISHING**

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"BESKYT DIN IDENTITET MED MFA"

Facit til casestudier

A Casestudie 1: Beskyttelse mod efterligning af ledere

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En kendt topchef er ramt af domæner med stavefejl, der efterligner chefens e-mail for at snyde kunder.
- Anbefalet strategi og løsning: Registrér alle almindelige stavemåder af chefens navn. Brug DMARC, DKIM og SPF mod forfalskning af domænet, og kræv MFA med hardwarenøgle på alle ledelsens logins.

B Casestudie 2: Firmalogins på det mørke net

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: Et datadump på det mørke net indeholder flere hundrede logins, der tilhører en virksomheds systemadministratorer.
- Anbefalet strategi og løsning: Nulstil alle adgangskoder i virksomheden, og kræv en fælles adgangskodeadministrator. Indfør MFA på alle portaler, og opsæt løbende automatisk overvågning af det mørke net.