

Navn: _____

Dato: _____

Point: _____

Svindel online og social manipulation af endepunkter

Phishing, forfalskede domæner, vishing, supportsvindel, out-of-band-

OVERBLIK OVER SVINDEL ONLINE

SIKRET

DATAKRYPTERING

256-bit AES-standard

OVERHOLDER KRAV

GLOBALE STANDARDER

GDPR- og CCPA-rammer

ZERO-TRUST

ADGANGSPOLITIK

Multifaktorgodkendelse

Velkommen! Denne opgavepakke fører dig gennem forsvar mod svindel online. Du vil udforske falske phishing-sider, social manipulation, supportsvindel, svindel med overførsler og metoder til at bekræfte betalinger.

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.

Åbn VPN.com's guide til cybersikkerhed

URL: <https://www.vpn.com/cybersecurity/online-scams/>

Din læringsplan for beskyttelse mod svindel online

- Genkend tegn på supportsvindel og domæner med stavfejl.
- Indfør SPF, DKIM og DMARC mod forfalskede e-mails.
- Indfør bekræftelse ad en anden kanal for at forhindre svindel med firmaoverførsler.

VEJLEDNING TIL GUIDEN OM SVINDEL ONLINE

Besvar multiple choice- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden om beskyttelse mod svindel online.

BESKYTTELSE MOD SVINDEL ONLINE OG SOCIAL MANIPULATION (INTRODUKTION)

Svindel online udnytter menneskelig adfærd gennem phishing, falske support-pop-ups, vishing og svindel med overførsler. Bekræftelse af betalinger ad en anden kanal og domænereregler med SPF, DKIM og DMARC stopper social manipulation ved porten.

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

Kontrolpunkt 1: Multiple choice-udfordring

1 1. Hvad er det tydeligste tegn på supportsvindel?

- ☐ A. En pop-up, der påstår, at systemet er smittet, og kræver, at du ringer til et nummer
- ☐ B. En automatisk sikkerhedsopdatering fra en officiel kilde
- ☐ C. En adgangskodeadministrator, der ikke udfylder på et firmadomæne
- ☐ D. En backup, der kører i baggrunden på et eksternt drev

2 2. Hvilken teknik bruger forfalskede afsenderdomæner til at stjæle bankoplysninger?

- ☐ A. Phishing via e-mail
- ☐ B. Portscanning
- ☐ C. Indsprøjtning i hukommelsen
- ☐ D. Kryptografisk makulering

3 3. Hvad er svindel med overførsler?

- ☐ A. At narre ofre til at sende penge til falske firmakonti via social manipulation
- ☐ B. At kryptere databaser med ransomware
- ☐ C. At forespørge databaser med SQL-injektion
- ☐ D. At tage backup af filer på offline diske

4 4. Hvorfor laver svindlere falske webshops?

- ☐ A. For at stjæle kortoplysninger og betalingsdata fra købere
- ☐ B. For at hoste databaser til analyse af malware
- ☐ C. For at gøre DNS-flytninger hurtigere
- ☐ D. For at omgå geoblokering på offentligt wi-fi

5 5. Hvad betyder vishing?

- ☐ A. Phishing via telefonopkald for at stjæle loginoplysninger
- ☐ B. Scanning af lokale net for usikrede enheder
- ☐ C. Gendannelse af databaser efter et brud
- ☐ D. Kørsel af ukendt kode i sikre virtuelle beholdere

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Phishing rammer kun almindelige brugere, aldrig topledere.

☐

Sandt

☐

Falsk

7 Spørgsmål 7

7. Forfalskede domæner bruger ofte små stavefejl (som amaz0n.com) for at efterligne kendte brands.

☐

Sandt

☐

Falsk

8 Spørgsmål 8

8. Supportsvindel kan løses ved at give den, der ringer, fjernadgang.

☐

Sandt

☐

Falsk

9 Spørgsmål 9

9. Social manipulation udnytter frygt og tidspres for at omgå sikkerhedsregler.

☐

Sandt

☐

Falsk

10 Spørgsmål 10

10. Anmodninger om overførsler bør altid bekræftes ad en anden kanal.

☐

Sandt

☐

Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. Svigagtige e-mails, der narrer brugere, kaldes _____ .
2. Webadresser, der efterligner kendte brands, er _____ .
3. Telefonsvindel rettet mod bankoplysninger kaldes _____ .
4. En pop-up, der kræver betaling for at fjerne virus, er support- _____ .
5. En betalingsanmodning kræver out-of-band- _____ .
6. At omdirigere firmabetalinger til tyvenes konti er svindel med _____ .

ORDBANK MED FAGUDTRYK

FORFALSKEDE

OVERFOERSEL

PHISHING
VISHINGSMISHING
WHALING

SVINDEL

VERIFIKATION

Skriv dine svar her:

1.

2.

3.

4.

5.

6.

Kontrolpunkt 4: Match sikkerhedsbegreber

MATCH DEFINITIONER

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

PHISHING

A

Svigagtige e-mailkampagner, der skal stjæle logins og adgangskoder. (A)

FORFALSKET

B

Efterlignet afsender eller webadresse, der skal se ægte ud. (B)

VISHING

C

Svigagtige opkald, der skal stjæle logins og kontooplysninger. (C)

SVINDEL

D

Svigagtigt nummer, der skal stjæle penge eller adgang fra ofre. (D)

VERIFICATION

E

Bekræftelse af betalingsoplysninger ad en betroet, anden kanal. (E)

OVERFØRSEL

F

Svigagtig omdirigering af betalinger til kriminelles konti. (F)

WHALING

G

Måltrettet phishing mod topledere for at stjæle deres logins. (G)

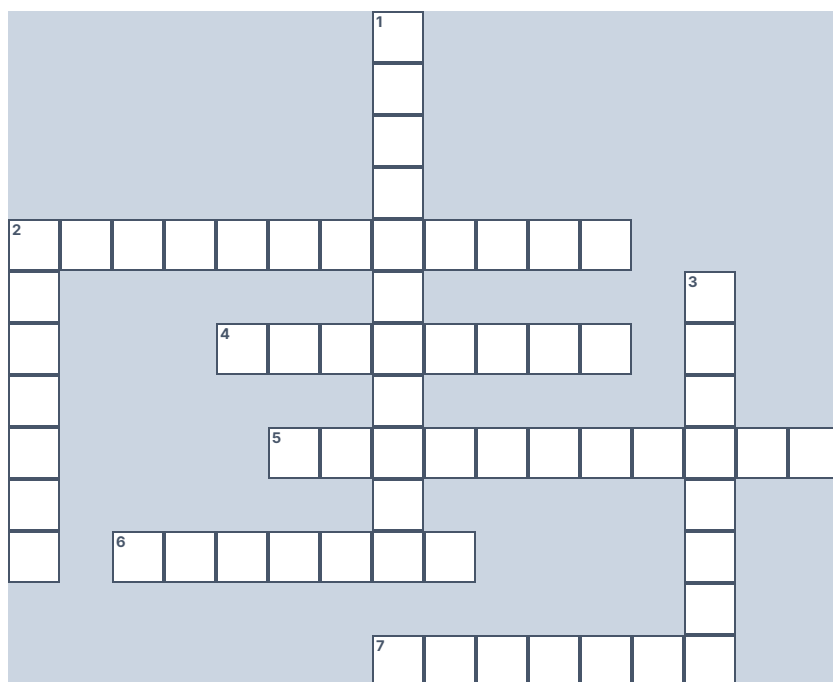
SMISHING

H

Svindel-sms'er, der skal stjæle logins til mobilkonti. (H)

Kontrolpunkt 5: Kryds og tværs

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



VANDRETTE NØGLER

- 2. Bekræftelse af en betaling ad en anden, betroet kanal (12)
- 4. Svigagtige e-mails, der skal narre brugere til at udlevere logins (8)
- 5. Bankbetaling, som svindlere omdirigerer til deres egne konti (11)
- 6. Et svigagtigt nummer, som en falsk support-pop-up er et eksempel på (7)
- 7. Målettet phishing mod topledere med stor beslutningsmagt (7)

LODRETTE NØGLER

- 1. Den slags webadresser, der efterligner kendte brands (11)
- 2. Telefonsvindel, der skal lokke bankoplysninger ud af ofre (7)
- 3. Svindel via sms med links til falske portaler (8)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

2 vandret: Bekræftelse af en betaling ad en anden, betroet kanal (12 bogstaver):

4 vandret: Svigagtige e-mails, der skal narre brugere til at udlevere logins (8 bogstaver):

5 vandret: Bankbetaling, som svindlere omdirigerer til deres egne konti (11 bogstaver):

6 vandret: Et svigagtigt nummer, som en falsk support-pop-up er et eksempel på (7 bogstaver):

7 vandret: Måltrettet phishing mod topledere med stor beslutningsmagt (7 bogstaver):

LODRETTE NØGLER

1 lodret: Den slags webadresser, der efterligner kendte brands (11 bogstaver):

2 lodret: Telefonsvindel, der skal lokke bankoplysninger ud af ofre (7 bogstaver):

3 lodret: Svindel via sms med links til falske portaler (8 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

PHISHING

FORFALSKEDE

VISHING
WHALINGSVINDEL
SMISHING

VERIFIKATION

OVERFOERSEL

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. PHISHING
- B. FORFALSKET
- C. VISHING
- D. SVINDEL
- E. VERIFIKATION
- F. OVERFØRSEL
- G. WHALING
- H. SMISHING

DEFINITIONER OG MATCHFELTER

- ☐ 1. Svigagtige e-mailkampagner, der skal stjæle logins og adgangskoder.
- ☐ 2. Efterlignet afsender eller webadresse, der skal se ægte ud.
- ☐ 3. Svigagtige opkald, der skal stjæle logins og kontooplysninger.
- ☐ 4. Svigagtigt nummer, der skal stjæle penge eller adgang fra ofre.
- ☐ 5. Bekræftelse af betalingsoplysninger ad en betroet, anden kanal.
- ☐ 6. Svigagtig omdirigering af betalinger til kriminelles konti.
- ☐ 7. Målrettet phishing mod topledere for at stjæle deres logins.
- ☐ 8. Svindel-sms'er, der skal stjæle logins til mobilkonti.

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. NSHPIGHI

5. EOKSREALFD
F

2. VSGNIHI

6. EIDSNLV

3. VEAKOTRINF
I

7. RFOVELSEEOR

4. GHILNWA

8. SMHGSNII

Kontrolpunkt 8: Casestudier om cybersikkerhed

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

CASESTUDIE 1: FOREBYGGELSE AF SVINDEL MED FIRMAOVERFØRSLER



Scenarie: En økonomiafdeling får en hastemail fra en forfalsket leverandøradresse, der beder om, at fremtidige betalinger sendes til et nyt kontonummer.

Diskussion: Beskriv reglerne for bekræftelse af overførsler, og angiv e-mail- godkendelser, der blokerer svindlen.

CASESTUDIE 2: WHALING MOD EN TOPLEDER



Scenarie: En leder klikkede på et phishinglink, der lovede et fortroligt bestyrelses- dokument, og tastede sine firmalogins på en forfalsket portal.

Diskussion: Beskriv håndteringen af hændelsen, og forklar, hvordan ledelsens logins revideres.

Sidste udfordring: 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. Afkodet cybersikkerhedsbesked:

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

Afkodet cybersikkerhedsbesked:

						18	9	14	7		20	9	12							
12	5	22	5	18	1	14	4	15	5	18	5	14		15	7		20	10	5	11

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z).

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del A)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q1: Hvad er svindel online?

Et svigagtigt nummer via digitale kanaler, der narrer ofre til at sende penge eller udlevere logins.

Q2: Hvad er det tydeligste tegn på phishing?

En besked med tidspres (som lukning af kontoen), der sender dig til et link, som ikke passer til det officielle domæne.

Q3: Hvad er typosquatting?

Registrering af domæner med typiske stavfejl af kendte brands (som amaz0n.com) til falske phishingssider.

Q4: Hvad er supportsvindel?

En pop-up, der påstår, at pc'en er smittet, og beder dig ringe og betale for falsk oprydning eller fjernsupport.

Q5: Hvad er vishing?

Phishing via telefonopkald, der narrer ofre til at udlevere bank- eller loginoplysninger.

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvad er svindel med overførsler?

Omdirigering af betalinger til svindlerkonti ved at udgive sig for leverandører eller ledere.

Q7: Hvad er whaling?

En meget målrettet form for spear phishing rettet mod værdifulde mål som topledere.

Q8: Hvad er smishing?

Svindel-sms'er med links til falske portaler eller pakkesporing.

Q9: Hvorfor er bekræftelse ad en anden kanal afgørende?

Den bekræfter betalingen ad en separat kanal (som et opkald) uden om en kompromitteret e-mailtråd.

Q10: Hvordan virker svindel med falsk deponering?

Svindlere laver en falsk deponeringsside, påstår at pengene er sikre, og stjæler købers indbetaling.

Kontrolpunkt 11: Avanceret FAQ om sikkerhed (del A)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og datacompliance.

Q1: Hvordan bruger svindlere BEC (kompromitteret firmamail) til svindel med overførsler?

De kaprer en medarbejders e-mailkonto, følger fakturatråde og sender nye betalingsoplysninger med svindlerkonti.

Q2: Hvad er risikoen ved IDN-homografangreb?

Tegn uden for ASCII, der ligner almindelige bogstaver (f.eks. kyrillisk 'a'), bruges til forfalskede domæner, der efterligner ægte brands.

Q3: Hvorfor er det vigtigt at undersøge e-mailens header?

Den viser afsendersserverens rigtige IP og resultatet af SPF/DKIM, så man kan se, om domænet er forfalsket.

Q4: Hvordan udnytter supportsvindlere fjernskrivebordsprogrammer?

De bruger AnyDesk eller TeamViewer til at koble sig på offerets enhed, installere malware og stjæle gemte adgangskoder.

Q5: Hvad er formålet med forskudssvindel?

At narre ofre til at betale gebyrer på forhånd for en stor gevinst, der ikke findes.

Kontrolpunkt 11: Avanceret FAQ om sikkerhed (del B)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og datacompliance.

Q6: Hvordan bruger svindlere sociale medier til målrettet phishing?

De kortlægger firmaets struktur og medarbejdernes navne og skriver overbevisende spear-phishingmails.

Q7: Hvorfor giver falske webshops store rabatter?

For at lokke købere til at taste kortoplysninger, som genbruges eller sælges på fora for kortsvindel.

Q8: Hvordan blokerer DMARC phishing?

DMARC beder mailservere afvise beskeder, der fejler SPF eller DKIM, så forfalskede e-mails ikke når indbakkerne.

Q9: Hvad er faren ved portaler, der høster logins?

Forfalskede sider, der ligner Microsoft 365 eller Google Workspace, og som stjæler logins, mens de tastes.

Q10: Hvordan anmelder og lukker sikkerhedsteams svindeldomæner?

Ved at sende beviser til registratorens abuse-adresse, hostingudbyderen og Google Safe Browsing.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

Phishing er startpunktet for over 90 % af svindel og sikkerhedsbrud i virksomheder.

2. SIKKERHEDSINDSIGT

Svindel via kompromitteret firmamail (BEC) koster over 2 milliarder dollar om året globalt.

3. SIKKERHEDSINDSIGT

Domæner med stavfejl registreres af svindlere få minutter efter store brandlanceringer.

4. SIKKERHEDSINDSIGT

Falsk teknisk support rammer især ældre og stjæler millioner i falske gebyrer.

5. SIKKERHEDSINDSIGT

Homografangreb ser ens ud i adresselinjen, medmindre browseren viser punycode.

6. SIKKERHEDSINDSIGT

Svindel-sms'er (smishing) åbnes oftere end phishingmails og stjæler logins hurtigere.

7. SIKKERHEDSINDSIGT

Whaling rammer lederes e-mail, fordi de kan godkende store overførsler.

8. SIKKERHEDSINDSIGT

Bekræftelse ad en anden kanal forhindrer over 95 % af tabene ved BEC-svindel.

9. SIKKERHEDSINDSIGT

Falske deponeringstjenester er en udbredt svindel ved handel med brugte domæner.

10. SIKKERHEDSINDSIGT

Google Safe Browsing blokerer titusindvis af nye svindelområder hver dag.

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] CISA. (2025). Cybersikkerhedsvarsler og -vejledninger.

<https://www.cisa.gov/news-events/cybersecurity-advisories>

[3] NIST. (2024). Special Publication 800-53: Sikkerheds- og privatlivskontroller.

<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

[5] NIST. (2023). Special Publication 800-88: Retningslinjer for sikker sletning af medier.

<https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>

[7] IETF. (2022). RFC 7519: Specifikation af JSON Web Token (JWT).

<https://datatracker.ietf.org/doc/rfc7519/>

[9] OWASP. (2024). Top 10 over sikkerhedsrisici i webapplikationer.

<https://owasp.org/www-project-top-ten/>

[2] GDPR. (2024). Databeskyttelsesforordningen (GDPR), officiel tekst.

<https://gdpr-info.eu/>

[4] NIST. (2023). Special Publication 800-61: Vejledning i håndtering af it-sikkerhedshændelser.

<https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

[6] IETF. (2021). RFC 8446: Specifikation af Transport Layer Security (TLS) 1.3.

<https://datatracker.ietf.org/doc/rfc8446/>

[8] Center for Internet Security (CIS). (2024). Kritiske sikkerhedskontroller.

<https://www.cisecurity.org/controls/cis-controls-list>

[10] OWASP. (2025). Application Security Verification Standard (ASVS).

<https://owasp.org/www-project->

Facitliste: Kontrolpunkt 1 – Multiple choice

1 Mæglerens rolle MÆGLING

Rigtigt svar: A

UNDERVISNINGSNOTE

Domænemæglere forhandler fortroligt for købere og sælgere for at opnå handler til markedspris. Kilde: ICANN Transfer Policy [Ref 1].

Domænemæglere forhandler fortroligt for købere og sælgere for at opnå handler til markedspris.

2 Diskret strategi ANONYMITET

Rigtigt svar: A

UNDERVISNINGSNOTE

Et diskret opkøb skjuler køberens identitet, så sælgeren ikke hæver prisen. Kilde: Escrow.com Protocol [Ref 7].

Et diskret opkøb skjuler køberens identitet, så sælgeren ikke hæver prisen.

3 Beskyttelse via deponering DEPONERING

Rigtigt svar: A

UNDERVISNINGSNOTE

En licenseret, uafhængig deponeringstjeneste opbevarer pengene sikkert, indtil ejerskiftet er bekræftet. Kilde: Escrow.com Protocol [Ref 7].

En licenseret, uafhængig deponeringstjeneste opbevarer pengene sikkert, indtil ejerskiftet er bekræftet.

4 Vurdering af domæner VURDERING

Rigtigt svar: A

UNDERVISNINGSNOTE

Korte .com-domæner på 2 bogstaver eller ét ord er yderst sjældne og lette at sælge. Kilde: WIPO UDRP Guide [Ref 3].

Korte .com-domæner på 2 bogstaver eller ét ord er yderst sjældne og lette at sælge.

5 Tvistløsning UDRP-POLITIK

Rigtigt svar: A

UNDERVISNINGSNOTE

ICANN's ensartede politik for domænetvister (UDRP) regulerer administrative varemærketvister. Kilde: WIPO Dispute Rules [Ref 2].

ICANN's ensartede politik for domænetvister (UDRP) regulerer administrative varemærketvister.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 Fortrolige NDA'er NDA'ER

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Professionelle domænemæglere arbejder under fortrolighedsaftaler for at beskytte køberens forretningsstrategi. Kilde: CIS Controls [Ref 8].

Professionelle domænemæglere arbejder under fortrolighedsaftaler for at beskytte køberens forretningsstrategi.

7 Levering via deponering DEPONERING

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Deponeringskonti udbetaler først midlerne, når køberen har verificeret den fulde overdragelse af domæneejerskabet. Kilde: Escrow.com-protokollen [Ref 7].

Deponeringskonti udbetaler først midlerne, når køberen har verificeret den fulde overdragelse af domæneejerskabet.

8 Digital ejendom AKTIVER

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Korte .com-domæner på to og tre bogstaver fungerer som værdifulde, likvide digitale ejendomsaktiver. Kilde: NIST's retningslinjer [Ref 9].

Korte .com-domæner på to og tre bogstaver fungerer som værdifulde, likvide digitale ejendomsaktiver.

9 Anonym forhandling STRATEGI

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Når en virksomhedskøber henvender sig direkte, hæver sælgere ofte prisen betydeligt. Kilde: WIPO's UDRP-guide [Ref 3].

Når en virksomhedskøber henvender sig direkte, hæver sælgere ofte prisen betydeligt.

10 EPP-autorisation EPP-KODE

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

EPP-koder er unikke sikkerhedskoder, som registratorer genererer for at godkende domæneoverførsler. Kilde: IETF RFC 5730 [Ref 4].

EPP-koder er unikke sikkerhedskoder, som registratorer genererer for at godkende domæneoverførsler.

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

A PHISHING	B FORFALSKET	C VISHING	D SVINDEL
E VERIFICATION	F OVERFØRSEL	G WHALING	H SMISHING

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 PHISHING	2 FORFALSKET	3 VISHING	4 SVINDEL
5 VERIFICATION	6 OVERFØRSEL		

DISKUSSIONSNOTER TIL UNDERVISERE

Trusselsbilledet:

Kontrollér, at eleverne forstår, hvordan malware, phishing og zero-day-angreb rammer og bryder netværkets forsvar.

Forsvarskontroller:

Understreg brugen af netværksfirewalls, sandkasseafvikling, adfærdsscannere og multifaktorgodkendelse (MFA).

Overholdelse af lovgivning:

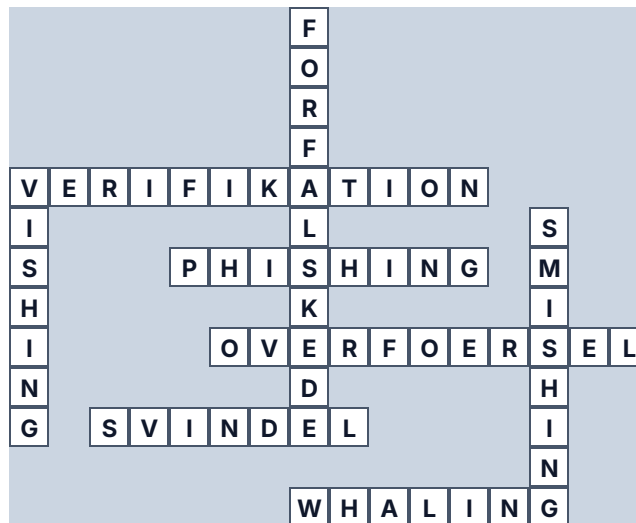
Fremhæv brugersamtykke, dataminimering, kryptering under lagring og transport samt globale rammer som GDPR og CCPA.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

2 vandret: VERIFIKATION Bekræftelse af en betaling ad en anden, betroet kanal (9,3)

4 vandret: PHISHING Svigagtige e-mails, der skal narre brugere til at udlevere logins (11,7)

5 vandret: OVERFOERSEL Bankbetaling, som svindlere omdirigerer til deres egne konti (13,8)

6 vandret: SVINDEL Et svigagtigt nummer, som en falsk support-pop-up er et eksempel på (15,5)

7 vandret: WHALING Målettet phishing mod topledere med stor beslutningsmagt (17,10)

LODRETTE NØGLER

1 lodret: FORFALSKED Den slags webadresser, der efterligner kendte brands (5,10)

2 lodret: VISHING Telefonsvindel, der skal lokke bankoplysninger ud af ofre (9,3)

3 lodret: SMISHING Svindel via sms med links til falske portaler (10,16)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. NSHPIHGI	PHISHING	5. EOKSREALFDF	FORFALSKEDE
2. VSGNIHI	VISHING	6. EIDSNLV	SVINDEL
3. VEAKOTRINFII	VERIFIKATION	7. RFOVELSEEOR	OVERFOERSEL
4. GHILNWA	WHALING	8. SMHGSNII	SMISHING

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"RING TIL LEVERANDOEREN OG TJEK"

Facit til casestudier om domænemægling

A

Casestudie 1: Forebyggelse af svindel med firmaoverførsler

[Underviserens løsning](#)

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: Økonomiafdelingen får en hastemail fra en forfalsket leverandøradresse, der beder om betaling til et nyt kontonummer.
- Anbefalet strategi og løsning: Kræv to godkendere til alle betalinger, bekræft via et gemt telefonnummer, og bloker forfalskede domæner ved porten.

B

Casestudie 2: Whaling mod en topleder

[Underviserens løsning](#)

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En leder klikkede på et phishinglink om et bestyrelses- dokument og tastede sine logins på en falsk portal.
- Anbefalet strategi og løsning: Isolér lederens enhed, nulstil alle sessioner og logins, gennemgå logfiler for dataudslip, og indfør MFA med hardwarenøgle.