Navn: _____ Dato: _____ Point: _____

Sikkerhed og kryptering på offentligt wi-fi

Man-in-the-middle-angreb, falske adgangspunkter, pakkesniffing, VPN-tunneler og HTTPS-kryptering.

OVERBLIK OVER SIKKERHED PÅ OFFENTLIGT WI-FI

SIKRET
DATAKRYPTERING
256-bit AES-standard

OVERHOLDER KRAV
GLOBALE STANDARDER
GDPR- og CCPA-rammer

ZERO-TRUST
ADGANGSPOLITIK
Multifaktorgodkendelse

Velkommen! Denne opgavepakke fører dig gennem sikkerhed på offentligt wi-fi. Du vil udforske ukrypterede net, man-in-the-middle-angreb (MitM), falske adgangspunkter, packet sniffing, VPN-tunneler og HTTPS under overførsel.

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/sikkerhed-offentlig-wifi/

Din læringsplan for sikkerhed på offentligt wi-fi

- Genkend risici på offentligt wi-fi som packet sniffing og falske adgangspunkter.
- Brug krypterede VPN-tunneler til data undervejs.
- Kræv HTTPS og sikre browserindstillinger for fjernmedarbejdere.

VEJLEDNING TIL GUIDEN OM SIKKERHED PÅ OFFENTLIGT WI-FI

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 sikker fjernadgang. Slut af med bonusaktiviteten Tænk hurtigt.

SIKKERHED PÅ OFFENTLIGT WI-FI OG BESKYTTELSE UNDERVEJS (INTRODUKTION)

Ukrypterede hotspots udsætter trafikken for packet sniffing og falske Evil Twin-net. Når trafikken tvinges gennem krypterede VPN-tunneler, og kun HTTPS tillades med HSTS, er sessionerne beskyttet mod aflytning på det lokale net.

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

Kontrolpunkt 1: Flervalgsopgave

1. Hvad er et man-in-the-middle-angreb (MitM)?

- A. At opsnappe og ændre kommunikation mellem to parter på et fælles net
- B. En teknik til at trække brugerdata ud af databaser
- C. At overbelaste servere med trafik
- D. At slette lokale harddiske

2. Hvad er et falsk adgangspunkt (Evil Twin)?

- A. Et ondsindet hotspot med samme netværksnavn (SSID) som et ægte net
- B. Et værktøj til at overvåge backups
- C. En sikker opsætning af en VPN-gateway
- D. En DNS-post med godkendte mailservere

3. Hvordan beskytter en VPN trafikken på offentligt wi-fi?

- A. Den pakker al trafik i en krypteret tunnel, så aflyttere ikke kan læse den
- B. Den blokerer automatisk alle indgående forbindelser
- C. Den ændrer netkortets MAC-adresse
- D. Den sletter cookies i browseren

4. Hvad er packet sniffing?

- A. At bruge hardware eller software til at opsnappe og logge pakker
- B. At scanne mapper for dubletter
- C. At begrænse læseadgang efter brugerroller
- D. At kryptere drev med AES-256

5. Hvad er HTTPS' rolle?

- A. At kryptere trafikken mellem browseren og webserveren
- B. At filtrere indgående e-mail ved porten
- C. Komprimering af billeder for hurtigere indlæsning
- D. At styre mapper på netværksdrev

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Brugere på et åbent offentligt net kan let opsnappe ukrypterede data.

○ Sandt ○ Falsk

7 Spørgsmål 7

7. Falske adgangspunkter (Evil Twins) er altid godkendt af administratorerne.

○ Sandt ○ Falsk

8 Spørgsmål 8

8. En VPN beskytter ikke mod packet sniffing på offentlige net.

○ Sandt ○ Falsk

9 Spørgsmål 9

9. HTTPS krypterer kun adressen og lader indholdet være ukrypteret.

○ Sandt ○ Falsk

10 Spørgsmål 10

10. Hotspots med WPA3 beskytter bedre end åbne net uden adgangskode.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. At opsnappe private adgangskoder på offentligt wi-fi kaldes _____ .
2. Analyse af rå pakker på et lokalt net kaldes packet _____ .
3. Et falsk hotspot, der efterligner hotellets wi-fi, er en _____ .
4. Sikker webtrafik undervejs kræver kryptering med _____ .
5. Kryptering af al trafik fra enheden sker med en _____ .
6. En krypteret forbindelse gennem offentlige net er en _____ .

ORDBANK MED FAGUDTRYK

ADGANGSPUNKT AFLYTNING EVIL TWIN FIREWALL HTTPS SNIFFING TUNNEL VPN

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

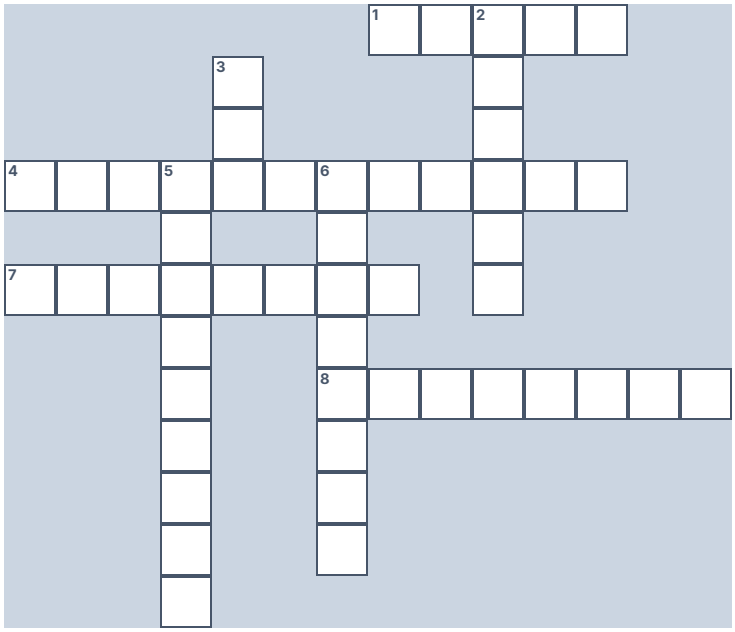
MATCH BEGREBER OG DEFINITIONER

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

☐	1. AFLYTNING	A	Moderne sikkerhedsstandard for wi-fi.
☐	2. SNIFFING	B	Sikker vej for data undervejs.
☐	3. EVIL TWIN	C	Filtrering af indgående trafik.
☐	4. HTTPS	D	Falsk hotspot, der efterligner et net.
☐	5. VPN	E	Aflæsning af trafik undervejs.
☐	6. TUNNEL	F	Opsnapning af datapakker.
☐	7. WPA3	G	Krypteret virtuelt privat netværk.
☐	8. FIREWALL	H	Sikker overførsel på nettet.

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

1. Protokol, der krypterer trafikken mellem browser og webserver (5)

4. Trådløs sender, som en Evil Twin udgiver sig for at være (12)

7. Falsk hotspot, der efterligner et ægte net med samme navn (8)

8. Barriere, der filtrerer indgående trafik (8)

LODRETTE NØGLER

2. Krypteret forbindelse gennem et offentligt net (6)

3. Tjeneste, der krypterer al trafik fra enheden i en tunnel (3)

5. At opsnappe andres adgangskoder og data på et offentligt net (9)

6. Packet …: opsnapning og analyse af rå datapakker (8)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

1 vandret: Protokol, der krypterer trafikken mellem browser og webserver (5 bogstaver):

4 vandret: Trådløs sender, som en Evil Twin udgiver sig for at være (12 bogstaver):

7 vandret: Falsk hotspot, der efterligner et ægte net med samme navn (8 bogstaver):

8 vandret: Barriere, der filtrerer indgående trafik (8 bogstaver):

LODRETTE NØGLER

2 lodret: Krypteret forbindelse gennem et offentligt net (6 bogstaver):

3 lodret: Tjeneste, der krypterer al trafik fra enheden i en tunnel (3 bogstaver):

5 lodret: At opsnappe andres adgangskoder og data på et offentligt net (9 bogstaver):

6 lodret: Packet …: opsnapning og analyse af rå datapakker (8 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

B A L B C Q Æ E M L Æ M Æ W L

E S E O K E J V O O F L S R H

O O N S T U W I V H I C U S Q

G I N U C Y E L V Ø R X C Å Y

N S U G L I Å T D O E E S S Z

I P T R C W B W A Å W P E N M

N T A E Q V E I F H A J D I T

T T S N F P J N U Å L U G F S

Y H Y F A N A S Q O L R W F Æ

L S L T W U D O Ø B G U Z I Z

F A D G A N G S P U N K T N K

A A T Å Ø Ø M H J O T L N G N

V Q I S S H Å A Q X G X C Ø T

Ø B I N Å H K P R P Z C N Å Ø

G Æ Q Y X M X R B P Y V N H X

ORDLISTE MED FAGUDTRYK

AFLYTNING SNIFFING EVILTWIN HTTPS VPN TUNNEL FIREWALL ADGANGSPUNKT

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. AFLYTNING
B. SNIFFING
C. EVILTWIN
D. HTTPS
E. VPN
F. TUNNEL
G. FIREWALL
H. ADGANGSPUNKT

DEFINITIONER OG MATCHFELTER

1. Barriere, der filtrerer indgående trafik.
2. Falsk hotspot, der efterligner et ægte net med samme navn.
3. Packet ...: opsnapning og analyse af rå datapakker.
4. Krypteret forbindelse gennem et offentligt net.
5. Trådløs sender, som en Evil Twin udgiver sig for at være.
6. At opsnappe andres adgangskoder og data på et offentligt net.
7. Tjeneste, der krypterer al trafik fra enheden i en tunnel.
8. Protokol, der krypterer trafikken mellem browser og webserver.

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. NTYFAINGL
2. LENVIWTI
3. NPV
4. ELLAWFIR
5. FINGFSNI
6. PHTST
7. ETNLNU
8. PGNNSTAGDK UA

Bonusaktivitet: Tænk hurtigt

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

1	Grunde til at opdatere software			
2	Enheder, der automatisk forbinder til wi-fi			
3	Oplysninger, du aldrig bør dele			
4	Sikkerhedsvaner, du kan starte i dag			
5	Måder at være sikker på en café			
6	Enheder, der kan blive hacket			
7	Ting, en hacker kan se på åbent wi-fi			
8	Tegn på et falsk wi-fi-net			
9	Alternativer til offentligt wi-fi			
10	Advarselstegn i en e-mail			
11	Ting, du ikke gør på offentligt wi-fi			
12	Steder med gratis wi-fi			
13	Måder at beskytte dine konti			
14	Tegn på, at en computer er inficeret			
15	Wi-fi-navne, der virker mistænkelige			

Kontrolpunkt 8: Casestudier om cybersikkerhed

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

CASESTUDIE 1: PACKET SNIFFING PÅ OFFENTLIGT WI-FI



Scenarie: En sælger på lufthavnens offentlige wi-fi opdager, at flere følsomme e-mails er lækket kort efter, at de blev sendt ukrypteret.

Diskussion: Analysér risiciene ved offentlige net, og beskriv en løsning med kryptering af trafikken.

CASESTUDIE 2: FORSVAR MOD FALSKE EVIL TWIN-HOTSPOTS



Scenarie: Angribere opsætter et falsk adgangspunkt ved navn 'CoffeeShop_Guest', der efterligner caféens hotspot og opsnapper trafikken fra intetanende gæster.

Diskussion: Beskriv, hvordan falske adgangspunkter opdages og blokeres.

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	18	21	7		1	12	20	9	4		22	16	14		16	29

15	6	6	5	14	20	12	9	7	20		14	5	20

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: Hvorfor er offentligt wi-fi usikkert?

Åbent offentligt wi-fi krypterer ikke trafikken i luften, så andre i nærheden kan opfange alle ubeskyttede data. [2]

Q2: Hvad er packet sniffing?

En sniffer opsnapper rå data på netværket og afslører ukrypterede adgangskoder og trafik.

Q3: Hvad er en Evil Twin?

Et falsk adgangspunkt, som hackere opsætter med samme navn og indstillinger som et betroet hotspot.

Q4: Hvordan beskytter en VPN mig?

Den sender trafikken gennem en krypteret tunnel og skjuler din surfing for aflyttere på nettet.

Q5: Beskytter HTTPS mig på offentligt wi-fi?

Ja, det krypterer de data, der udveksles mellem din browser og hjemmesiden, og en VPN tilføjer endnu et lag beskyttelse.

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvad er WPA3?

Den moderne Wi-Fi Protected Access-standard med stærkere kryptering og beskyttelse mod ordbogsangreb. [1]

Q7: Kan offentligt wi-fi sprede malware?

Ja, angribere kan opsnappe trafikken og indsætte skadelige downloads (drive-by downloads) i browseren.

Q8: Hvad er risikoen ved fildeling?

Er fildeling slået til, kan andre på nettet læse eller ændre dine mapper.

Q9: Hvad er en loginportal?

Den loginside, hoteller og caféer bruger til at give adgang, og som angribere kan forfalske.

Q10: Skal jeg slukke wi-fi, når jeg ikke bruger det?

Ja, så forbinder enheden ikke automatisk til ukendte net.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

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

Q1: Hvordan udnytter et MitM-angreb DNS?

En falsk router forfalsker DNS og sender browsere til phishingsider i stedet for de rigtige domæner.

Q2: Hvad er kapring af sessioner?

En angriber opsnapper en ukrypteret sessionscookie på wi-fi og bruger den til at springe login over.

Q3: Hvad er SSL stripping?

Et MitM-angreb, hvor HTTPS nedgraderes til ukrypteret HTTP, så logins kan læses.

Q4: Hvordan beskytter HSTS mod SSL stripping?

HTTP Strict Transport Security tvinger browseren til kun at bruge HTTPS og afviser ukrypteret HTTP. [3]

Q5: Hvad er en VPN med split tunneling?

En opsætning, hvor kun firmatrafik går gennem VPN'en, mens resten går direkte, hvilket kan give lækager.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

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

Q6: Hvorfor er WPA2 sårbar over for KRACK?

Key Reinstallation Attack udnytter WPA2's firevejshåndtryk til at dekryptere pakker uden adgangskoden.

Q7: Hvad er klientisolering?

En indstilling, der forhindrer enheder på nettet i at tale direkte sammen og dermed stopper lokal aflytning.

Q8: Hvordan bruger angribere falske DNS-servere?

Falske routere tildeler falske DNS-servere, så angriberen kan opsnappe og ændre alle opslag.

Q9: Kan en VPN skjule min MAC-adresse?

Nej. MAC-adresser er lokale identifikatorer på lag 2; brug i stedet din enheds indbyggede indstilling for tilfældig MAC-adresse (privat adresse).

Q10: Hvad er et angreb med falsk loginportal?

En angriber viser en falsk loginside på et falsk hotspot og stjæler logins under dække af gratis wi-fi.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

Fjernmedarbejdere bruger ofte wi-fi på caféer, hoteller og lufthavne, hvor de ikke kan styre netværkets sikkerhed.

2. SIKKERHEDSINDSIGT

Et Evil Twin-hotspot kan kopiere navn og MAC-adresse fra et betroet net og snyde enhederne.

3. SIKKERHEDSINDSIGT

Sniffere som Wireshark er gratis og kan vise ukrypterede HTTP-adgangskoder i klartekst.

4. SIKKERHEDSINDSIGT

WPA3 bruger Simultaneous Authentication of Equals (SAE) mod lokale brute force-angreb.

5. SIKKERHEDSINDSIGT

SSL stripping omgår HTTPS ved at opsnappe den første HTTP-omdirigering.

6. SIKKERHEDSINDSIGT

HTTP Strict Transport Security (HSTS)-svarheadere forhindrer browsere i at falde tilbage til ukrypterede HTTP-forbindelser. [3]

7. SIKKERHEDSINDSIGT

Når automatisk forbindelse slås fra, kobler telefoner sig ikke på falske net.

8. SIKKERHEDSINDSIGT

En VPN, der altid er slået til, sender al fjernmedarbejdernes trafik gennem firmaets firewalls.

9. SIKKERHEDSINDSIGT

Falske adgangspunkter kan uddele forfalskede DNS-svar og omdirigere måldomæner til phishing-servere.

10. SIKKERHEDSINDSIGT

Uden en VPN kan andre brugere på et åbent hotspot se, hvilke sider og servere din enhed kontakter.

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] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

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

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

Facitliste: Kontrolpunkt 1 – Flervalg

1 Spørgsmål 1

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er et man-in-the-middle-angreb (MitM)? → At opsnappe og ændre kommunikation mellem to parter på et fælles net

2 Spørgsmål 2

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er et falsk adgangspunkt (Evil Twin)? → Et ondsindet hotspot med samme netværksnavn (SSID) som et ægte net

3 Spørgsmål 3

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvordan beskytter en VPN trafikken på offentligt wi-fi? → Den pakker al trafik i en krypteret tunnel, så aflyttere ikke kan læse den

4 Spørgsmål 4

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er packet sniffing? → At bruge hardware eller software til at opsnappe og logge pakker

5 Spørgsmål 5

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er HTTPS' rolle? → At kryptere trafikken mellem browseren og webserveren

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Spørgsmål 6** — Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Brugere på et åbent offentligt net kan let opsnappe ukrypterede data.

7 **Spørgsmål 7** — Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Falsk: en Evil Twin er et uautoriseret hotspot, som en angriber opretter for at efterligne et rigtigt.

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

UNDERVISNINGSNOTE

Falsk: en VPN krypterer trafikken i en tunnel, så lokale sniffere ikke kan læse den.

9 **Spørgsmål 9** — Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Falsk: HTTPS krypterer hele HTTP-udvekslingen, inklusive URL-stien og sidens indhold.

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

UNDERVISNINGSNOTE

Hotspots med WPA3 beskytter bedre end åbne net uden adgangskode.

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

E 1. AFLYTNING	F 2. SNIFFING	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. TUNNEL	A 7. WPA3	C 8. FIREWALL

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 AFLYTNING	2 SNIFFING	3 EVIL TWIN	4 HTTPS
5 VPN	6 TUNNEL		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 G – FIREWALL	2 C – EVILTWIN	3 B – SNIFFING	4 F – TUNNEL
5 H – ADGANGSPUNKT	6 A – AFLYTNING	7 E – VPN	8 D – HTTPS

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare AFLYTNING, SNIFFING og EVIL TWIN med egne ord og give et eksempel på hvert begreb.

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

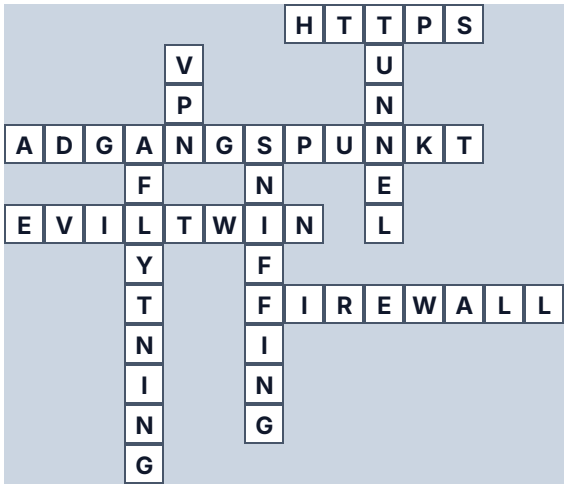
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

1 vandret: HTTPS Protokol, der krypterer trafikken mellem browser og webserver (5 bogstaver)

4 vandret: ADGANGSPUNKT Trådløs sender, som en Evil Twin udgiver sig for at være (12 bogstaver)

7 vandret: EVILTWIN Falsk hotspot, der efterligner et ægte net med samme navn (8 bogstaver)

8 vandret: FIREWALL Barriere, der filtrerer indgående trafik (8 bogstaver)

LODRETTE NØGLER

2 lodret: TUNNEL Krypteret forbindelse gennem et offentligt net (6 bogstaver)

3 lodret: VPN Tjeneste, der krypterer al trafik fra enheden i en tunnel (3 bogstaver)

5 lodret: AFLYTNING At opsnappe andres adgangskoder og data på et offentligt net (9 bogstaver)

6 lodret: SNIFFING Packet ...: opsnapning og analyse af rå datapakker (8 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1.	NTYFAINGL	AFLYTNING	5.	FINGFSNI	SNIFFING
2.	LENVIWTI	EVILTWIN	6.	PHTST	HTTPS
3.	NPV	VPN	7.	ETNLNU	TUNNEL
4.	ELLAWFIR	FIREWALL	8.	PGNNSTAGDKUA	ADGANGSPUNKT

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"BRUG ALTID VPN PÅ OFFENTLIGT NET"

Facit til casestudier

A Casestudie 1: Packet sniffing på offentligt wi-fi

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En sælger på lufthavnens wi-fi opdager, at følsomme e-mails er lækket kort efter, at de blev sendt ukrypteret.
- Anbefalet strategi og løsning: Kræv firmaets VPN på alle bærbare, tillad kun HTTPS i browseren, og bloker ukrypterede protokoller (som HTTP og FTP) i firewallen.

B Casestudie 2: Forsvar mod falske Evil Twin-hotspots

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: Angribere opsætter 'CoffeeShop_Guest', der efterligner caféens hotspot og opsnapper gæsternes trafik.
- Anbefalet strategi og løsning: Kontrollér adgangspunkternes BSSID, bloker forbindelser til åbne net, og kræv mobilt hotspot til følsomt arbejde.