Navn: _____ Dato: _____ Poeng: _____

Sikkerhet og kryptering på offentlig Wi-Fi

Man-in-the-middle-angrep, uautoriserte tilgangspunkter, pakkesniffing, VPN-tunneler og HTTPS-kryptering.

LÆRINGSOVERSIKT: SIKKERHET PÅ OFFENTLIG WI-FI

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 sikkerhet på offentlig Wi-Fi. Du skal utforske ukrypterte nettverk, man-in-the-middle-angrep (MitM), uautoriserte tilgangspunkter, pakkesniffing, VPN-tunneler og sikkerhet for HTTPS under overføring.

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/offentlig-wifi-sikkerhet/

Din læringsveiledning for sikkerhet på offentlig Wi-Fi

- Identifiser vanlige risikoer ved offentlig Wi-Fi, blant annet pakkesniffing og uautoriserte tilgangspunkter.
- Innfør krypterte VPN-tunneler for å sikre data under overføring.
- Håndhev HTTPS og sikre nettleserinnstillinger for ansatte som jobber eksternt.

INSTRUKSJONER FOR VEILEDNINGEN OM SIKKERHET PÅ OFFENTLIG WI-FI

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

SIKKERHET PÅ OFFENTLIG WI-FI OG BESKYTTELSE UNDER OVERFØRING (INNLEDNING)

Ukrypterte offentlige Wi-Fi-hotspots lar nettverkstrafikk ligge åpen for pakkesnusing og Evil Twin-forfalskning. Å tvinge trafikken gjennom sikre VPN-krypteringstunneler og håndheve HSTS-regler som bare tillater HTTPS, beskytter økter mot avlytting i det lokale nettverket.

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

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er et man-in-the-middle-angrep (MitM)?

- A. Å avskjære og endre kommunikasjon mellom to parter på et delt nettverk
- B. En teknikk for databaseuttrekk som retter seg mot brukerposter
- C. Å overbelaste webservere med forespørsler om nettverkstrafikk
- D. Å slette lagringsvolumer på den lokale harddisken

2. Hva er et uautorisert tilgangspunkt (Evil Twin)?

- A. Et ondsinnet Wi-Fi-aksesspunkt konfigurert med samme SSID som et legitimt nettverk
- B. Et administrasjonsverktøy som brukes til å overvåke databasesikkerhetskopier
- C. En sikker konfigurasjon av VPN-gateway
- D. En DNS-oppføring som kartlegger autoriserte e-postservere

3. Hvordan beskytter en VPN trafikk på offentlig Wi-Fi?

- A. Den pakker alle nettverkspakker inn i en kryptert tunnel, slik at de ikke kan leses av sniffere
- B. Den blokkerer automatisk alle innkommende tilkoblingsforespørsler
- C. Den endrer MAC-adressen til det fysiske nettverkskortet
- D. Den sletter mellomlagrede informasjonskapsler i nettleseren

4. Hva er pakkesniffing?

- A. Å bruke maskinvare- eller programvareverktøy til å fange opp og logge nettverkspakker
- B. Å skanne lokale kataloger etter dupliserte filer
- C. Å begrense lesetilgang til databasen basert på brukerroller
- D. Å kryptere lagringsstasjoner med AES-256-nøkler

5. Hva er rollen til HTTPS?

- A. Å kryptere øktrafikken mellom nettleseren og webserveren
- B. Å filtrere innkommende e-postmeldinger i gatewayen
- C. Å komprimere bilder for raskere sidelasting
- D. Å styre filstrukturer i nettverkstilkoblet lagring

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Tilkoblede brukere kan enkelt fange opp data i klartekst på åpne offentlige Wi-Fi-nettverk.

○ Sant ○ Usant

7 Spørsmål 7

7. Uautoriserte tilgangspunkter (Evil Twins) er alltid godkjent av nettverksadministratorer.

○ Sant ○ Usant

8 Spørsmål 8

8. En VPN er ineffektiv til å beskytte trafikk mot pakkesniffing på offentlige nettverk.

○ Sant ○ Usant

9 Spørsmål 9

9. HTTPS krypterer bare URL-stien og lar pakkenes nyttelast ligge i klartekst.

○ Sant ○ Usant

10 Spørsmål 10

10. Wi-Fi-hotspots som bruker WPA3-sikkerhet gir sterkere beskyttelse enn åpne nettverk uten passord.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. Å fange opp private passord på offentlig Wi-Fi er _____ av kommunikasjon.
2. Å analysere rå pakker på et lokalt nettverk bruker pakke- _____ .
3. Et falskt hotspot som etterligner et hotells Wi-Fi, er en _____ .
4. Å sikre nettrafikk under overføring krever kryptering med _____ .
5. Å kryptere all utgående nettverkstrafikk bruker en _____ .
6. En kryptert kommunikasjonsvei gjennom offentlige nettverk er en _____ .

ORDBANK

AVSKJÆRING BRANNMUR EVIL TWIN HTTPS SNIFFING TUNNEL VPN-KLIENT WPA-KRYPTERING

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble sikkerhetsbegreper

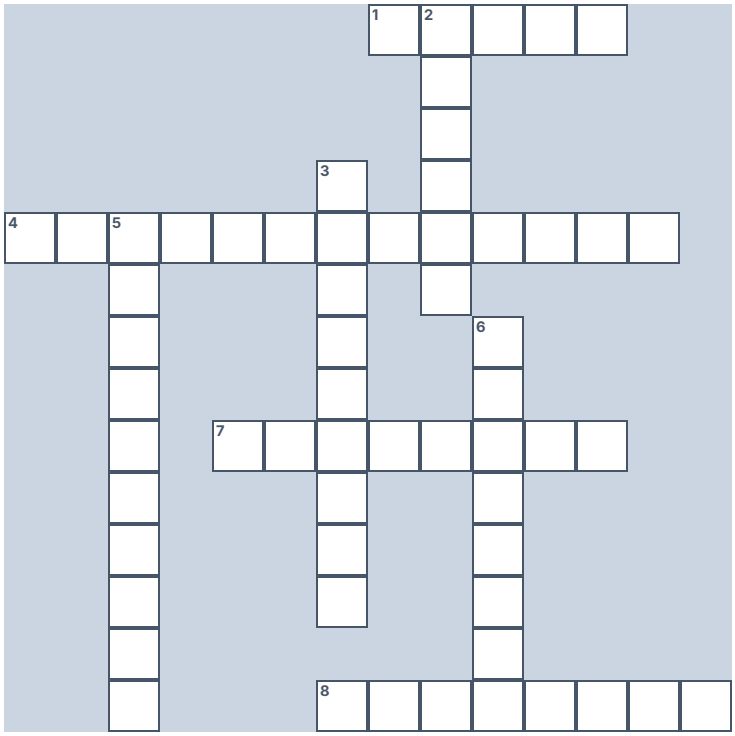
KOBLE DEFINISJONER

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

☐	1. AVLYTTING	A	Moderne sikkerhetsstandard for Wi-Fi.
☐	2. SNIFFING	B	Sikker datasti under overføring.
☐	3. EVIL TWIN	C	Filtrere innkommende trafikk.
☐	4. HTTPS	D	Uautorisert hotspot som imiterer Wi-Fi.
☐	5. VPN	E	Å lese trafikk under overføring.
☐	6. TUNNEL	F	Å fange opp nettverkspakker.
☐	7. WPA3	G	Kryptert virtuelt privat nettverk.
☐	8. BRANNMUR	H	Sikker nettoverføring.

Kontrollpunkt 5: Kryssord

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



VANNRETT

1. Sikker overføring av nettrafikk. (5)

4. Moderne sikkerhetsstandard for Wi-Fi (WPA3). (13)

7. Fanging av nettverksdatapakker. (8)

8. Filtrering av innkommende trafikk. (8)

LODDRETT

2. Sikker datasti under overføring. (6)

3. Kryptert virtuelt privat nettverk. (9)

5. Lesing av trafikk under overføring. (10)

6. Falskt hotspot som etterligner Wi-Fi. (8)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

1 vannrett: Sikker overføring av nettrafikk. (5 bokstaver):

4 vannrett: Moderne sikkerhetsstandard for Wi-Fi (WPA3). (13 bokstaver):

7 vannrett: Fanging av nettverksdatapakker. (8 bokstaver):

8 vannrett: Filtrering av innkommende trafikk. (8 bokstaver):

LODDRETT

2 loddrett: Sikker datasti under overføring. (6 bokstaver):

3 loddrett: Kryptert virtuelt privat nettverk. (9 bokstaver):

5 loddrett: Lesing av trafikk under overføring. (10 bokstaver):

6 loddrett: Falskt hotspot som etterligner Wi-Fi. (8 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

AVSKJÆRING SNIFFING EVILTWIN HTTPS VPNKLIENT TUNNEL
WPAKRYPTERING BRANNMUR

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. AVSKJÆRING
B. SNIFFING
C. EVILTWIN
D. HTTPS
E. VPNKLIENT
F. TUNNEL
G. WPAKRYPTERING
H. BRANNMUR

DEFINISJONER OG TILHØRENDE FELT
[ ] 1. Moderne sikkerhetsstandard for Wi-Fi (WPA3).
[ ] 2. Falskt hotspot som etterligner Wi-Fi.
[ ] 3. Fanging av nettverksdatapakker.
[ ] 4. Sikker datasti under overføring.
[ ] 5. Filtrering av innkommende trafikk.
[ ] 6. Lesing av trafikk under overføring.
[ ] 7. Kryptert virtuelt privat nettverk.
[ ] 8. Sikker overføring av nettrafikk.

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. **NRÆJVAIGKS** _____
2. **LENVIWTI** _____
3. **VILPETKNN** _____
4. **YNEATRGPIR WPK** _____
5. **FINGFSNI** _____
6. **PHTST** _____
7. **ETNLNU** _____
8. **NRNRBUMA** _____

Bonusaktivitet: Tenk raskt

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

1	Grunner til å oppdatere programvare			
2	Enheter som kobler seg automatisk til Wi-Fi			
3	Informasjon du aldri bør dele			
4	Trygge vaner du kan begynne med i dag			
5	Måter å være trygg på en kafé			
6	Enheter som kan hackes			
7	Ting en hacker kan se på åpent Wi-Fi			
8	Tegn på et falskt Wi-Fi-nettverk			
9	Alternativer til offentlig Wi-Fi			
10	Advarselstegn i en e-post			
11	Ting du ikke gjør på offentlig Wi-Fi			
12	Steder med gratis Wi-Fi			
13	Måter å beskytte kontoene dine på			
14	Tegn på at en datamaskin er infisert			
15	Wi-Fi-navn som virker mistenkelige			

Kontrollpunkt 8: Casestudier om cybersikkerhet

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

CASESTUDIE 1: BEGRENSNING AV PAKKESNUSING PÅ OFFENTLIG WI-FI



Scenario: En ekstern salgsleder som er koblet til et offentlig Wi-Fi-nettverk på en flyplass legger merke til at flere sensitive forretnings-e-poster lekkes kort tid etter at de er sendt i klartekst.

Diskusjonsspørsmål: Analyser risikoene ved offentlige nettverk, og skisser en løsning med kryptering av trafikk.

CASESTUDIE 2: FORSVAR MOT EVIL TWIN-HOTSPOT



Scenario: Angripere setter opp et uautorisert trådløst tilgangspunkt med navnet «CoffeeShop_Guest» som etterligner en ekte kafé-hotspot og fanger opp nettverkstrafikk fra intetanende gjester.

Diskusjonsspørsmål: Beskriv i detalj verifiseringstrinnene for å oppdage og blokkere uautoriserte tilgangspunkter.

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

11	18	25	16	20	5	18		20	18	1	6	9	11	11	5	14		16	29
15	6	6	5	14	20	12	9	7		23	9	6	9		13	5	4		
							22	16	14										

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: Hvorfor er offentlig Wi-Fi usikkert?

Åpent offentlig Wi-Fi krypterer ikke trafikken over luften, så andre i nærheten kan fange opp alle ubeskyttede data. [2]

Q2: Hva er pakkesniffing?

En pakkesniffer fanger opp rådata som flyter over et nettverksgrensesnitt og avslører passord i klartekst og trafikkdetaljer.

Q3: Hva er en Evil Twin?

Et uautorisert tilgangspunkt som er satt opp av hackere og etterligner navnet og innstillingene til et pålitelig lokalt Wi-Fi-aksesspunkt.

Q4: Hvordan beskytter en VPN meg?

Den ruter trafikken din gjennom en kryptert tunnel og skjuler nettleseraktiviteten din for sniffere i det lokale nettverket.

Q5: Beskytter HTTPS meg på offentlig Wi-Fi?

Ja, den krypterer dataene som utveksles mellom nettleseren din og nettstedet, og en VPN legger til enda et beskyttelseslag.

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

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

Q6: Hva er WPA3?

Den moderne standarden Wi-Fi Protected Access, som gir sterkere kryptering og beskyttelse mot frakoblede ordbokangrep. [1]

Q7: Kan offentlig Wi-Fi levere skadevare?

Ja, angripere kan avskjære trafikk og injisere ondsinnede nedlastingsforespørsler (drive-by-nedlastinger) i nettleserøkten din.

Q8: Hva er risikoen ved fildeling?

Hvis fildeling er aktivert, kan andre brukere på det offentlige nettverket lese eller endre den lokale mappekatalogen din.

Q9: Hva er en captive portal?

Innloggingssiden som hotell- og kafénettverk bruker for å gi internettilgang, og som noen ganger kan forfalskes av angripere.

Q10: Bør jeg slå av Wi-Fi når jeg ikke bruker det?

Ja, å slå av Wi-Fi hindrer enheten din i å koble seg automatisk til nettverk du ikke stoler på.

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

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

Q1: Hvordan utnytter et mann-i-midten-angrep DNS?

Ved å bruke DNS-forfalskning på en uærlig ruter for å lede målnettlesere til nettfiskingssider som ligner, i stedet for målets domener.

Q2: Hva er øktkapring?

En angriper som sniffer en ukryptert øktinfokapsel på offentlig Wi-Fi og importerer den for å omgå innlogging med legitimasjon.

Q3: Hva er SSL stripping?

Et mellommannsangrep (MitM) der en angriper nedgraderer en brukers sikre HTTPS-forespørsel til ukryptert HTTP og fanger opp innlogginger i klartekst.

Q4: Hvordan beskytter HSTS mot SSL stripping?

HTTP Strict Transport Security tvinger nettlesere til å koble til bare via HTTPS og avviser ukrypterte HTTP-reserveløsninger. [3]

Q5: Hva er en VPN med split tunneling?

En konfigurasjon som bare ruter bedriftstrafikk gjennom VPN-en mens offentlige internettdata sendes direkte, noe som kan medføre risiko for eksponering via lekkasjeveier.

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

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

Q6: Hvorfor er WPA2 sårbar for KRACK?

Key Reinstallation Attack utnytter WPA2-håndtrykket med fire trinn til å dekryptere pakker uten Wi-Fi-passordet.

Q7: Hva er klientisolering?

En sikkerhetsinnstilling i routeren som hindrer tilkoblede Wi-Fi-enheter i å kommunisere direkte med hverandre og blokkerer lokal sniffing.

Q8: Hvordan bruker angripere falske DNS-servere?

De konfigurerer useriøse rutere til å tildele falske DNS-servere til klienter, slik at de kan fange opp og skrive om alle webslag.

Q9: Kan en VPN skjule min lokale MAC-adresse?

Nei. MAC-adresser er lokale identifikatorer på lag 2; bruk enhetens innebygde MAC-randomisering (privat adresse) i stedet.

Q10: Hva er et angrep med forfalsket captive portal?

En angriper som er vert for en falsk autentiseringsportal på et uautorisert aksesspunkt for å stjele legitimasjon under dekke av gratis Wi-Fi-tilgang.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

Eksterne arbeidstakere bruker ofte Wi-Fi på kafeer, hoteller og flyplasser, der de ikke kan kontrollere nettverkets sikkerhet.

2. SIKKERHETSINNSIKT

Et Evil Twin-aksesspunkt kan kopiere det nøyaktige navnet og MAC-adressen til et pålitelig nettverk og forvirre enheter.

3. SIKKERHETSINNSIKT

Programvare for pakkesniffing som Wireshark er gratis og kan vise ukrypterte HTTP-passord i klartekst.

4. SIKKERHETSINNSIKT

WPA3-sikkerhet bruker Simultaneous Authentication of Equals (SAE) for å beskytte mot lokale brute force-angrep.

5. SIKKERHETSINNSIKT

SSL stripping-angrep omgår grunnleggende HTTPS-beskyttelse ved å avskjære innledende HTTP-omdirigeringer i gatewayen.

6. SIKKERHETSINNSIKT

Svarhoder for HTTP Strict Transport Security (HSTS) hindrer nettlesere i å falle tilbake til ukrypterte HTTP-tilkoblinger. [3]

7. SIKKERHETSINNSIKT

Å slå av «Auto-Connect» hindrer smarttelefoner i å koble til useriøse nettverk som ligner på ekte nettverk på offentlige steder.

8. SIKKERHETSINNSIKT

«Always-on»-konfigurasjoner for VPN i bedrifter tvinger all nettverkstrafikk fra ansatte som jobber eksternt gjennom bedriftens brannmurer.

9. SIKKERHETSINNSIKT

Uautoriserte tilgangspunkter kan dele ut forfalskede DNS-svar og omdirigere målrettede domener til phishing-servere.

10. SIKKERHETSINNSIKT

Uten et VPN kan andre brukere på et åpent hotspot se hvilke nettsteder og servere enheten din kontakter.

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] 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

Fasit: Kontrollpunkt 1 – flervalg

1 Spørsmål 1 — Riktig svar: A

MERKNAD TIL LÆREREN

Hva er et man-in-the-middle-angrep (MitM)? → Å avskjære og endre kommunikasjon mellom to parter på et delt nettverk

2 Spørsmål 2 — Riktig svar: A

MERKNAD TIL LÆREREN

Hva er et uautorisert tilgangspunkt (Evil Twin)? → Et ondsinnet Wi-Fi-aksesspunkt konfigurert med samme SSID som et legitimt nettverk

3 Spørsmål 3 — Riktig svar: A

MERKNAD TIL LÆREREN

Hvordan beskytter en VPN trafikk på offentlig Wi-Fi? → Den pakker alle nettverkspakker inn i en kryptert tunnel, slik at de ikke kan leses av sniffere

4 Spørsmål 4 — Riktig svar: A

MERKNAD TIL LÆREREN

Hva er pakkesniffing? → Å bruke maskinvare- eller programvareverktøy til å fange opp og logge nettverkspakker

5 Spørsmål 5 — Riktig svar: A

MERKNAD TIL LÆREREN

Hva er rollen til HTTPS? → Å kryptere øktrafikken mellom nettleseren og webserveren

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Spørsmål 6** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Tilkoblede brukere kan enkelt fange opp data i klartekst på åpne offentlige Wi-Fi-nettverk.

7 **Spørsmål 7** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Usant: en Evil Twin er et uautorisert hotspot satt opp av en angriper for å etterligne et ekte.

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

MERKNAD TIL LÆREREN

Usant: en VPN krypterer trafikk i en tunnel, så lokale avlyttere kan ikke lese den.

9 **Spørsmål 9** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Usant: HTTPS krypterer hele HTTP-utvekslingen, inkludert URL-stien og sideinnholdet.

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

MERKNAD TIL LÆREREN

Wi-Fi-hotspots som bruker WPA3-sikkerhet gir sterkere beskyttelse enn åpne nettverk uten passord.

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

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

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 AVSKJÆRING	2 SNIFFING	3 EVIL TWIN	4 HTTPS
5 VPN-KLIENT	6 TUNNEL		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 G – WPAKRYPTERING	2 C – EVILTWIN	3 B – SNIFFING	4 F – TUNNEL
5 H – BRANNMUR	6 A – AVSKJÆRING	7 E – VPNKLIENT	8 D – HTTPS

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare AVLYTTING, SNIFFING og EVIL TWIN 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

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

KRYSSORDLØSNING

							H	T	T	P	S			
								U						
								N						
						V		N						
W	P	A	K	R	Y	P	T	E	R	I	N	G		
		V				N		L						
		S				K			E					
		K				L			V					
		J		S	N	I	F	F	I	N	G			
		Æ				E			L					
		R				N			T					
		I				T			W					
		N							I					
		G				B	R	A	N	N	M	U	R	

LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

1 vannrett: HTTPS Sikker overføring av nettrafikk. (5 bokstaver)

4 vannrett: WPAKRYPTERING Moderne sikkerhetsstandard for Wi-Fi (WPA3). (13 bokstaver)

7 vannrett: SNIFFING Fanging av nettverksdatapakker. (8 bokstaver)

8 vannrett: BRANNMUR Filtrering av innkommende trafikk. (8 bokstaver)

LODDRETT

2 loddrett: TUNNEL Sikker datasti under overføring. (6 bokstaver)

3 loddrett: VPNKLIENT Kryptert virtuelt privat nettverk. (9 bokstaver)

5 loddrett: AVSKJÆRING Lesing av trafikk under overføring. (10 bokstaver)

6 loddrett: EVILTWIN Falskt hotspot som etterligner Wi-Fi. (8 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1.	N R Æ J V A I G K S	AVSKJÆRING	5.	F I N G F S N I	SNIFFING
2.	L E N V I W T I	EVILTWIN	6.	P H T S T	HTTPS
3.	V I L P E T K N N	VPNKLIENT	7.	E T N L N U	TUNNEL
4.	Y N E A T R G P I R W P K	WPAKRYPTERING	8.	N R N R B U M A	BRANNMUR

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"KRYPTER TRAFIKKEN PÅ OFFENTLIG WIFI MED VPN"

Fasit til casestudiene

A Casestudie 1: Begrensning av pakkesnusing på offentlig Wi-Fi

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En ekstern salgssjef som er koblet til et offentlig Wi-Fi-nettverk på en flyplass, legger merke til at flere sensitive forretnings-e-poster lekkes kort tid etter at de er sendt i klartekst.
- Anbefalt strategi og løsning: Pålegg bruk av en VPN-klient for bedrifter på alle eksterne arbeidsstasjoner. Håndhev nettleserutvidelser som bare tillater HTTPS, og blokker ukrypterte protokoller (som HTTP og FTP) i klientens brannmur.

B Casestudie 2: Forsvar mot Evil Twin-hotspot

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: Angripere setter opp et useriøst trådløst tilgangspunkt med navnet 'CoffeeShop_Guest' som etterligner en ekte kafés hotspot, og fanger opp nettverkstrafikk fra intetanende gjester.
- Anbefalt strategi og løsning: Revider BSSID-MAC-adressene til tilgangspunkter for å bekrefte nettverkets ekthet. Håndhev validering av klientens sikkerhetstilstand for å blokkere tilkobling til åpne nettverk, og krev mobile hotspots for sensitivt arbeid.