Namn: _____ Datum: _____ Poäng: _____

Säkerhet och kryptering på offentligt Wi-Fi

Man-in-the-middle-attacker, falska åtkomstpunkter, paketsniffning, VPN-tunnlar och HTTPS-kryptering.

LÄRANDEÖVERSIKT: SÄKERHET PÅ OFFENTLIGA WI-FI-NÄT

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom säkerhet på offentligt Wi-Fi. Du utforskar okrypterade nätverk, Man-in-the-Middle-attacker (MitM), falska åtkomstpunkter, paketsniffning, VPN-tunnlar och HTTPS-säkerhet vid överföring.

KONTROLLPUNKTER I ARBETSBLADET

- [ ] **Del 1-4: Behärska cybersäkerhet och hothantering.**
- [ ] **Del 5-7: Lös korsord och ordsökare.**
- [ ] **Del 8-9: Lös fallstudier och chifferutmaning.**
- [ ] **Del 10: Gå igenom sidorna med grundläggande och avancerade vanliga frågor.**
- [ ] **Del 11: Utforska 10 intressanta fakta från verkligheten.**
- [ ] **Bonus: utmaningen Tänk snabbt.**

Öppna VPN.com:s guide om cybersäkerhet

URL: https://www.vpn.com/sv/cybersakerhet/offentligt-wifi-sakerhet/

Din inlärningsplan för säkerhet på offentligt Wi-Fi

- Identifiera vanliga risker med offentligt Wi-Fi, inklusive paketsniffning och falska åtkomstpunkter.
- Inför krypterade VPN-tunnlar för att säkra data under överföring.
- Tillämpa HTTPS och säkra webbläsarinställningar för distansarbetare.

INSTRUKTIONER FÖR GUIDEN OM SÄKERHET PÅ OFFENTLIGA WI-FI-NÄT

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om säkerhet vid fjärråtkomst. Avsluta med bonusaktiviteten Tänk snabbt.

SÄKERHET PÅ OFFENTLIGA WI-FI-NÄT OCH SKYDD UNDER ÖVERFÖRING (INTRODUKTION)

Okrypterade publika Wi-Fi-hotspots lämnar nätverkstrafiken exponerad för paketsniffning och Evil Twin-förfalskning. Att tvinga trafiken genom säkra krypterade VPN-tunnlar och använda HSTS-regler med enbart HTTPS skyddar sessioner mot avlyssning i det lokala nätverket.

LÄS VARJE KONTROLLPUNKT NOGGRANT OCH VÄLJ ELLER SKRIV DET RÄTTA SVARET.

Kontrollpunkt 1: Utmaning med flerval

1. Vad är en Man-in-the-Middle-attack (MitM)?

- A. Att fånga upp och ändra kommunikation mellan två parter i ett delat nätverk
- B. En teknik för databasuttag som riktar in sig på användarposter
- C. Att överbelasta webbservrar med nätverkstrafikförfrågningar
- D. Att radera lokala hårddiskvolymer

2. Vad är en falsk åtkomstpunkt (Evil Twin)?

- A. En skadlig Wi-Fi-hotspot som konfigurerats med samma SSID som ett legitimt nätverk
- B. Ett administrationsverktyg för att övervaka databassäkerhetskopior
- C. En säker konfiguration av VPN-gateway
- D. En DNS-post som anger behöriga e-postservrar

3. Hur skyddar ett VPN trafik på offentligt Wi-Fi?

- A. Den lägger alla nätverkspaket i en krypterad tunnel så att sniffare inte kan läsa dem
- B. Den blockerar automatiskt alla inkommande anslutningsförfrågningar
- C. Den ändrar MAC-adressen på det fysiska nätverkskortet
- D. Den raderar cachade cookies i webbläsaren

4. Vad är paketsniffning?

- A. Att använda hårdvaru- eller programvaruverktyg för att fånga upp och logga nätverkspaket
- B. Att skanna lokala kataloger efter dubblettfiler
- C. Att begränsa läsbehörighet i databaser utifrån användarroller
- D. Att kryptera lagringsenheter med AES-256-nycklar

5. Vilken roll har HTTPS?

- A. Kryptering av sessionstrafiken mellan webbläsaren och webbservern
- B. Att filtrera inkommande e-postmeddelanden i gatewayen
- C. Att komprimera bilder för snabbare sidinläsning
- D. Att hantera filstrukturer i nätverksansluten lagring

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Anslutna användare kan enkelt fånga upp klartextdata i öppna offentliga Wi-Fi-nätverk.

○ Sant ○ Falskt

7 Fråga 7

7. Falska åtkomstpunkter (Evil Twins) är alltid godkända av nätverksadministratörer.

○ Sant ○ Falskt

8 Fråga 8

8. Ett VPN är ineffektivt för att skydda trafik mot paketsniffning i offentliga nätverk.

○ Sant ○ Falskt

9 Fråga 9

9. HTTPS krypterar bara URL-sökvägen och lämnar paketens nyttolast i klartext.

○ Sant ○ Falskt

10 Fråga 10

10. Wi-Fi-hotspots med WPA3-säkerhet ger starkare skydd än öppna nätverk utan lösenord.

○ Sant ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

Läs varje mening nedan och fyll i luckan med rätt term från ordbanken.

1. Att fånga upp privata lösenord på offentligt Wi-Fi kallas _____ av kommunikation.
2. Att analysera råa paket i ett lokalt nätverk sker genom _____ av paket.
3. En falsk hotspot som imiterar ett hotells Wi-Fi är en _____ .
4. Att skydda webbtrafik under överföring kräver kryptering med _____ .
5. Att kryptera all utgående nätverkstrafik sker med hjälp av en _____ .
6. En krypterad kommunikationsväg genom offentliga nätverk är en _____ .

ORDBANK

AVLYSSNING BRANDVÄGG EVIL TWIN HTTPS SNIFFNING TUNNEL VPN-TJÄNST WI-FI-STANDARD

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

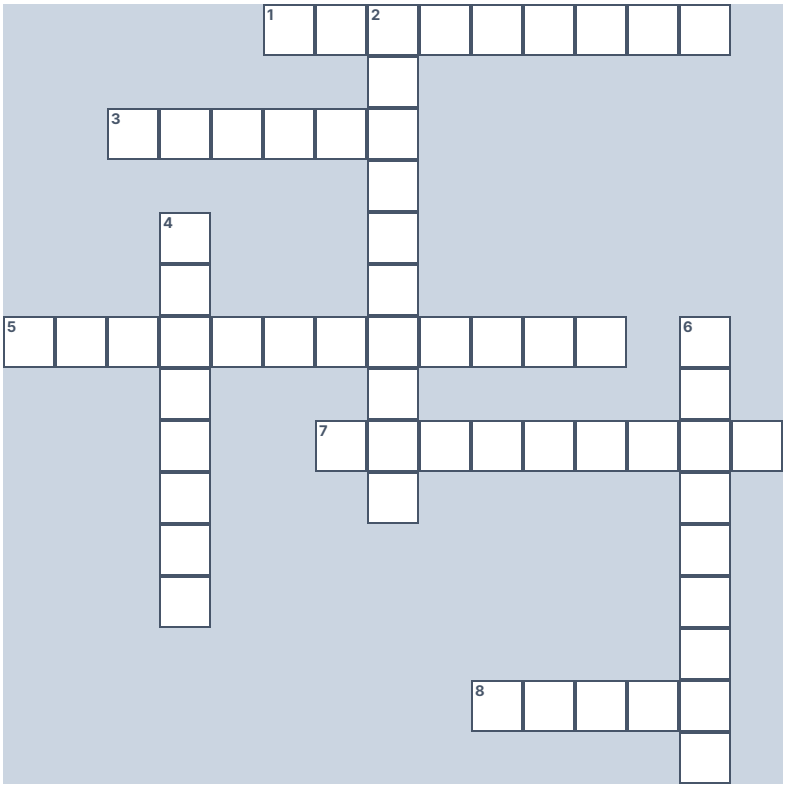
MATCHNING AV DEFINITIONER

Para ihop varje begrepp till vänster med rätt definition till höger genom att skriva motsvarande bokstav (A–H) i det ifyllbara fältet.

☐	1. AVLYSSNING	A	Modern säkerhetsstandard för Wi-Fi.
☐	2. SNIFFNING	B	Säker datasökväg under överföring.
☐	3. ILLASINNAD TVILLING	C	Filtrering av inkommande trafik.
☐	4. HTTPS	D	Falsk surfzon som imiterar Wi-Fi.
☐	5. VPN	E	Läsa trafik under överföring.
☐	6. TUNNEL	F	Att fånga nätverkspaket.
☐	7. WPA3	G	Krypterat virtuellt privat nätverk.
☐	8. BRANDVÄGG	H	Säker webböverföring.

Kontrollpunkt 5: Korsord

Lös korsordet genom att skriva bokstäver i de aktiva vita rutorna. Siffrorna motsvarar ledtrådarna nedan.



VÅGRÄTT

1. Filtrering av inkommande trafik. (9)

3. Säker datakanal under överföring. (6)

5. Modern säkerhetsstandard för Wi-Fi (WPA3). (12)

7. Insamling av nätverkets datapaket. (9)

8. Säker webböverföring. (5)

LODRÄTT

2. Läsning av trafik under överföring. (10)

4. Falsk hotspot som efterliknar ett Wi-Fi. (8)

6. Krypterat virtuellt privat nätverk. (9)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

Användare av skärmläsare och tangentbord kan skriva korsordssvaren direkt i textfälten nedan.

VÅGRÄTT

1 vågrätt: Filtrering av inkommande trafik. (9 bokstäver):

3 vågrätt: Säker datakanal under överföring. (6 bokstäver):

5 vågrätt: Modern säkerhetsstandard för Wi-Fi (WPA3). (12 bokstäver):

7 vågrätt: Insamling av nätverkets datapaket. (9 bokstäver):

8 vågrätt: Säker webböverföring. (5 bokstäver):

LODRÄTT

2 lodrätt: Läsning av trafik under överföring. (10 bokstäver):

4 lodrätt: Falsk hotspot som efterliknar ett Wi-Fi. (8 bokstäver):

6 lodrätt: Krypterat virtuellt privat nätverk. (9 bokstäver):

Kontrollpunkt 6: Dolt ordsök

Hitta de 8 viktiga ordförrådstermerna som är gömda i rutnätet nedan. Orden kan vara vågräta, lodräta eller diagonala.

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

ORDLISTA

AVLYSSNING SNIFFNING EVILTWIN HTTPS VPNTJÄNST TUNNEL
WIFISTANDARD BRANDVÄGG

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

Para ihop var och en av de 8 begreppen från ordsökningen med rätt definition genom att skriva bokstaven (A–H) på den tomma raden.

ORDLISTA

- **A. AVLYSSNING**
- **B. SNIFFNING**
- **C. EVILTWIN**
- **D. HTTPS**
- **E. VPNTJÄNST**
- **F. TUNNEL**
- **G. WIFISTANDARD**
- **H. BRANDVÄGG**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Modern säkerhetsstandard för Wi-Fi (WPA3).
2. Falsk hotspot som efterliknar ett Wi-Fi.
3. Insamling av nätverkets datapaket.
4. Säker datakanal under överföring.
5. Filtrering av inkommande trafik.
6. Läsning av trafik under överföring.
7. Krypterat virtuellt privat nätverk.
8. Säker webböverföring.

Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga begrepp och termer inom cybersäkerhet. Skriv dina svar i rutorna.

1. NNSSVAIGYL
2. LENVIWTI
3. VÄJPNTTSN
4. RNSFADTADWII
5. IFNGNFSNI
6. PHTST
7. ETNLNU
8. GDGBNRVÄA

Bonusaktivitet: Tänk snabbt

3 SVAR PER KATEGORI. DEN SOM FÖRST FYLLER I LISTAN VINNER.

1	Skäl till att uppdatera programvara			
2	Enheter som ansluter automatiskt till wifi			
3	Information du aldrig bör dela			
4	Säkra vanor du kan börja med i dag			
5	Sätt att vara säker på ett kafé			
6	Enheter som kan hackas			
7	Saker som en hackare kan se på öppet wifi			
8	Tecken på ett falskt wifi-nätverk			
9	Alternativ till offentligt wifi			
10	Varningstecken i ett e-postmeddelande			
11	Saker du inte gör på offentligt wifi			
12	Platser med gratis wifi			
13	Sätt att skydda dina konton			
14	Tecken på att en dator är infekterad			
15	Wifi-namn som verkar misstänkta			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

Tillämpa de begrepp du har lärt dig för att lösa de verkliga scenarierna nedan.

FALLSTUDIE 1: BEGRÄNSA PAKETAVLYSSNING PÅ OFFENTLIGT WI-FI



Scenario: En säljchef på distans som är ansluten till offentligt wifi på en flygplats märker att flera känsliga affärsmejl läcker kort efter att de skickats i klartext.

Diskussionsfråga: Analysera riskerna med offentliga nätverk och beskriv en lösning för kryptering av trafiken.

FALLSTUDIE 2: FÖRSVAR MOT EVIL TWIN-HOTSPOT



Scenario: Angripare sätter upp en falsk trådlös åtkomstpunkt med namnet "CoffeeShop_Guest" som efterliknar en äkta hotspot på ett kafé och fångar upp nätverkstrafik från intet ont anande gäster.

Diskussionsfråga: Beskriv i detalj verifieringsstegen för att upptäcka och blockera falska åtkomstpunkter.

Kontrollpunkt 9: Knäck chiffret

En cybersäkerhetsexpert skyddar nätverkstillgångar mot hotaktörer online. Använd bokstav-till-siffra-nyckeln nedan för att avkoda meddelandet genom att skriva de matchande bokstäverna på de tomma raderna.

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

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 Å=27 Ä=28 Ö=29

11	18	25	16	20	5	18	1		1	12	12		20	18	1	6	9	11
16	27		15	6	6	5	14	20	12	9	7	20		23	9	6	9	
						13	5	4		22	16	14						

Avkodat meddelande:

TIPS: VARJE SIFFRA MOTSVARAR BOKSTAVENS PLATS I ALFABETET (T.EX. 1 = A, 2 = B, 29 = Ö).

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del A)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q1: Varför är offentligt Wi-Fi osäkert?

Öppna offentliga Wi-Fi-nät krypterar inte trafiken i luften, så andra i närheten kan fånga upp alla oskyddade data. [2]

Q2: Vad är paketsniffning?

En paketsniffer fångar rådata som flödar över ett nätverksgränssnitt och avslöjar lösenord i klartext och trafikuppgifter.

Q3: Vad är en Evil Twin?

En oseriös åtkomstpunkt som hackare ställer upp och som imiterar namn och inställningar för en betrodd lokal Wi-Fi-hotspot.

Q4: Hur skyddar ett VPN mig?

Den routar din trafik genom en krypterad tunnel och döljer din surfaktivitet för sniffare i det lokala nätverket.

Q5: Skyddar HTTPS mig på offentligt Wi-Fi?

Ja, den krypterar de data som utbyts mellan din webbläsare och webbplatsen, och ett VPN lägger till ytterligare ett skyddslager.

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del B)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q6: Vad är WPA3?

Den moderna standarden Wi-Fi Protected Access, som ger starkare kryptering och skydd mot offline-ordlisteattacker. [1]

Q7: Kan offentligt Wi-Fi leverera skadlig kod?

Ja, angripare kan avlyssna trafik och injicera skadliga nedladdningsuppmaningar (drive-by-nedladdningar) i din webbläsarsession.

Q8: Vilken risk innebär fildelning?

Om fildelning är aktiverad kan andra användare på det offentliga nätverket läsa eller ändra din lokala mappkatalog.

Q9: Vad är en captive portal (inloggningsportal)?

Inloggningssidan som hotell- eller kafénätverk använder för att ge internetåtkomst, och som ibland kan förfalskas av angripare.

Q10: Ska jag stänga av Wi-Fi när jag inte använder det?

Ja, att stänga av Wi-Fi hindrar enheten från att automatiskt ansluta till icke betrodda nätverk.

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del C)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q1: Hur utnyttjar en man-in-the-middle-attack DNS?

Genom att använda DNS-spoofing på en falsk router för att styra målets webbläsare till nätfiskesidor som efterliknar de riktiga domänerna.

Q2: Vad är sessionskapning?

En angripare som sniffar en okrypterad sessionscookie på offentligt Wi-Fi och importerar den för att kringgå inloggning.

Q3: Vad är SSL-strippning?

En MitM-attack där en angripare nedgraderar en användares säkra HTTPS-förfrågan till okrypterad HTTP och fångar upp inloggningar i klartext.

Q4: Hur skyddar HSTS mot SSL-strippning?

HTTP Strict Transport Security tvingar webbläsare att ansluta endast via HTTPS och vägra okrypterade HTTP-reservlösningar. [3]

Q5: Vad är ett VPN med delad tunnel (split tunneling)?

En konfiguration som bara dirigerar företagstrafik genom VPN medan publika internetdata skickas direkt, vilket kan innebära risk för läckande vägar.

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del D)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q6: Varför är WPA2 sårbart för KRACK?

Key Reinstallation Attack utnyttjar WPA2:s fyrvägshandskakning för att dekryptera paket utan Wi-Fi-lösenordet.

Q7: Vad är klientisolering?

En routerinställning som hindrar anslutna Wi-Fi-enheter från att kommunicera direkt med varandra och blockerar lokal sniffning.

Q8: Hur använder angripare falska DNS-servrar?

De konfigurerar falska routrar som tilldelar klienter falska DNS-servrar, så att de kan avlyssna och skriva om alla webbuppslag.

Q9: Kan ett VPN dölja min lokala MAC-adress?

Nej. MAC-adresser är lokala identifierare på lager 2; använd i stället enhetens inbyggda inställning för MAC-randomisering (privat adress).

Q10: Vad är en förfalskningsattack mot en captive portal?

En angripare som är värd för en falsk autentiseringsportal på en oseriös hotspot för att stjäla inloggningsuppgifter under sken av gratis Wi-Fi-åtkomst.

Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

1. SÄKERHETSINSIKT

Distansarbetare använder ofta Wi-Fi på kaféer, hotell och flygplatser, där de inte kan kontrollera nätverkets säkerhet.

2. SÄKERHETSINSIKT

En Evil Twin-hotspot kan kopiera exakt samma namn och MAC-adress som ett betrott nätverk och förvirra enheter.

3. SÄKERHETSINSIKT

Programvara för paketsniffning som Wireshark är gratis och kan visa okrypterade HTTP-lösenord i klartext.

4. SÄKERHETSINSIKT

WPA3-säkerhet använder Simultaneous Authentication of Equals (SAE) för att skydda mot lokala brute force-attacker.

5. SÄKERHETSINSIKT

SSL-stripping-attacker kringgår grundläggande HTTPS-skydd genom att fånga upp första HTTP-omdirigeringarna i gatewayen.

6. SÄKERHETSINSIKT

Svarshuvuden för HTTP Strict Transport Security (HSTS) hindrar webbläsare från att falla tillbaka på okrypterade HTTP-anslutningar. [3]

7. SÄKERHETSINSIKT

Att stänga av ”Auto-Connect” hindrar smartphones från att ansluta till falska nätverk som liknar riktiga på offentliga platser.

8. SÄKERHETSINSIKT

Konfigurationer med 'always-on' VPN för företag tvingar all trafik från distansarbetare genom företagets brandväggar.

9. SÄKERHETSINSIKT

Falska åtkomstpunkter kan dela ut förfalskade DNS-svar och omdirigera måldomäner till nätfiskeservrar.

10. SÄKERHETSINSIKT

Utan en VPN kan andra användare på ett öppet hotspot se vilka webbplatser och servrar din enhet kontaktar.

Tekniska referenser och källor

Studieguiden och de interaktiva pusslen är sammanställda utifrån globala standarder från NIST och OWASP samt standarder för efterlevnad av dataskydd.

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[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

Facit: Kontrollpunkt 1 – Flerval

1 Fråga 1 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad är en Man-in-the-Middle-attack (MitM)? → Att fånga upp och ändra kommunikation mellan två parter i ett delat nätverk

2 Fråga 2 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad är en falsk åtkomstpunkt (Evil Twin)? → En skadlig Wi-Fi-hotspot som konfigurerats med samma SSID som ett legitimt nätverk

3 Fråga 3 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Hur skyddar ett VPN trafik på offentligt Wi-Fi? → Den lägger alla nätverkspaket i en krypterad tunnel så att sniffare inte kan läsa dem

4 Fråga 4 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad är paketsniffning? → Att använda hårdvaru- eller programvaruverktyg för att fånga upp och logga nätverkspaket

5 Fråga 5 — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vilken roll har HTTPS? → Kryptering av sessionstrafiken mellan webbläsaren och webbservern

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Fråga 6** — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Anslutna användare kan enkelt fånga upp klartextdata i öppna offentliga Wi-Fi-nätverk.

7 **Fråga 7** — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Falskt: en Evil Twin är en obehörig hotspot som en angripare sätter upp för att efterlikna en äkta.

8 **Fråga 8** — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Falskt: ett VPN krypterar trafiken i en tunnel, så lokala sniffers kan inte läsa den.

9 **Fråga 9** — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Falskt: HTTPS krypterar hela HTTP-utbytet, inklusive URL-sökvägen och sidans innehåll.

10 **Fråga 10** — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Wi-Fi-hotspots med WPA3-säkerhet ger starkare skydd än öppna nätverk utan lösenord.

Facit för ordförråd och bedömningsmall

Bedömningsmatris för läraren: Ge 1 poäng för varje korrekt matchning (totalt 8 poäng) och kontextbegrepp (totalt 6 poäng).

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

E 1. AVLYSSNING	F 2. SNIFFNING	D 3. ILLASINNAD TVILLING	H 4. HTTPS
G 5. VPN	B 6. TUNNEL	A 7. WPA3	C 8. BRANDVÄGG

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 AVLYSSNING	2 SNIFFNING	3 EVIL TWIN	4 HTTPS
5 VPN-TJÄNST	6 TUNNEL		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 G – WIFISTANDARD	2 C – EVILTWIN	3 B – SNIFFNING	4 F – TUNNEL
5 H – BRANDVÄGG	6 A – AVLYSSNING	7 E – VPNTJÄNST	8 D – HTTPS

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara AVLYSSNING, SNIFFNING och ILLASINNAD TVILLING med egna ord och ge ett exempel på varje.

Fallstudier:
Be eleverna att stödja sina rekommendationer med fakta från arbetsbladet, inte med antaganden.

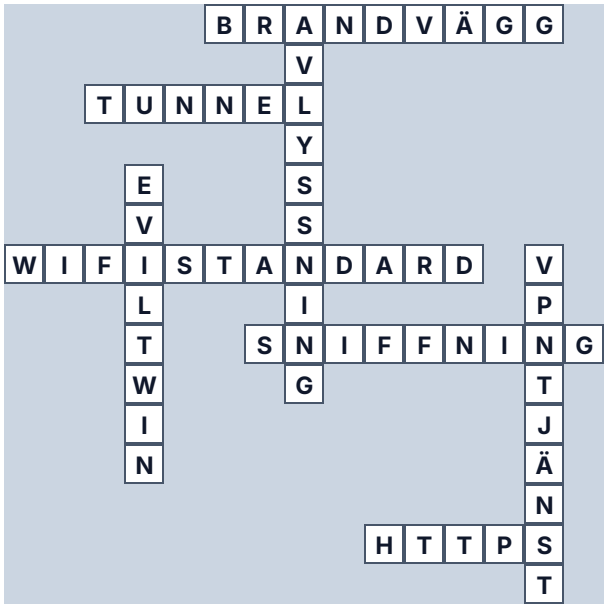
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

1 vågrätt: BRANDVÄGG Filtrering av inkommande trafik. (9 bokstäver)

3 vågrätt: TUNNEL Säker datakanal under överföring. (6 bokstäver)

5 vågrätt: WIFISTANDARD Modern säkerhetsstandard för Wi-Fi (WPA3). (12 bokstäver)

7 vågrätt: SNIFFNING Insamling av nätverkets datapaket. (9 bokstäver)

8 vågrätt: HTTPS Säker webböverföring. (5 bokstäver)

LODRÄTT

2 lodrätt: AVLYSSNING Läsning av trafik under överföring. (10 bokstäver)

4 lodrätt: EVILTWIN Falsk hotspot som efterliknar ett Wi-Fi. (8 bokstäver)

6 lodrätt: VPNTJÄNST Krypterat virtuellt privat nätverk. (9 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1.	N N S S V A I G Y L	AVLYSSNING	5.	I F N G N F S N I	SNIFFNING
2.	L E N V I W T I	EVILTWIN	6.	P H T S T	HTTPS
3.	V Ä J P N T T S N	VPNTJÄNST	7.	E T N L N U	TUNNEL
4.	R N S F A D T A D W I I	WIFISTANDARD	8.	G D G B N R V Ä A	BRANDVÄGG

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"KRYPTERA ALL TRAFIK PÅ OFFENTLIGT WIFI MED VPN"

Facit till fallstudierna

A Fallstudie 1: Begränsa paketavlyssning på offentligt Wi-Fi

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En säljchef på distans som är ansluten till ett offentligt Wi-Fi-nätverk på en flygplats märker att flera känsliga affärsmejl läcker kort efter att de skickats i klartext.
- Rekommenderad strategi och lösning: Kräv att en VPN-klient för företag används på alla distansarbetsstationer. Tillämpa webbläsartillägg som endast tillåter HTTPS och blockera okrypterade protokoll (som HTTP och FTP) i klientens brandvägg.

B Fallstudie 2: Försvar mot Evil Twin-hotspot

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: Angripare sätter upp en falsk trådlös åtkomstpunkt med namnet "CoffeeShop_Guest" som imiterar ett äkta kafés wifi och fångar upp nätverkstrafik från intet ont anande gäster.
- Rekommenderad strategi och lösning: Granska BSSID-MAC-adresserna för åtkomstpunkter för att verifiera nätverkets äkthet. Tillämpa validering av klientens hållning för att blockera anslutning till öppna nätverk och kräv mobila hotspots för känsligt arbete.