Navn: _____ Dato: _____ Poeng: _____

Anmeldelse av TunnelBear

Teknisk analyse av TunnelBear med hovedkontor i Canada, GhostBear-obfuskering, VigilantBear kill switch, årlige uavhengige sikkerhetsrevisjoner og null logging.

LÆRINGSOVERSIKT FOR TUNNELBEAR-ANMELDELSEN

ELEV
STUDENTSTATUS
Spor for nettverksforsvarere

SIKKER
TILKOBLINGSSTATUS
Beskytte datapakker

AKTIV
LEKKASJEBESKYTTELSE
DNS- og IPv6-lekkasjebeskyttelse

Velkommen! Dette aktivitetsheftet veileder deg gjennom en teknisk gjennomgang av TunnelBear. Du utforsker GhostBear-obfuskering, innstillinger for VigilantBear kill switch og validering av årlige sikkerhetsrevisjoner.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk VPN- og nettverkssikkerhetskonfigurasjoner.**
- [ ] **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 de beste VPN-ene

URL: https://www.vpn.com/no/vpn/tunnelbear/

Din læringsveiledning for TunnelBear

- Analyser den tekniske arkitekturen og krypteringsstandardene for TunnelBear Review.
- Konfigurer klientinnstillinger for å hindre lekkasjer av IP-, DNS- og WebRTC-trafikk.
- Sammenlign proprietære tunnelprotokoller med standardimplementeringer.

INSTRUKSJONER FOR TUNNELBEAR-ANMELDELSEN

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

GHOSTBEAR-OBFUSKERING OG ÅRLIG UAVHENGIG REVISJONSBEKREFTELSE

TunnelBear er kjent for årlige uavhengige sikkerhetsrevisjoner utført av Cure53. Selskapet har hovedkontor i Canada og tilbyr tilsløring av protokollen med GhostBear for å omgå DPI-sensurer, VigilantBear som beskyttelse mot tilkoblingslekkasjer, og ubegrenset antall enhetstilkoblinger.

(INTRODUKSJON)

TunnelBear er kjent for årlige uavhengige sikkerhetsrevisjoner utført av Cure53. Selskapet har hovedkontor i Canada og tilbyr tilsløring av protokollen med GhostBear for å omgå DPI-sensurer, VigilantBear som beskyttelse mot tilkoblingslekkasjer, og ubegrenset antall enhetstilkoblinger.

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

Kontrollpunkt 1: Flervalgsutfordring

1 **1. I hvilket land er TunnelBears selskap registrert?**

- A) Canada
- B) USA
- C) Sveits
- D) Tyskland

2 **2. Hva heter TunnelBears obfuskering for å omgå sensur?**

- A) GhostBear
- B) Chameleon
- C) Stealth
- D) ShadowSocks

3 **3. Hva heter TunnelBears innebygde kill switch-funksjon?**

- A) VigilantBear
- B) Secure Core
- C) NetShield
- D) SafePath

4 **4. Hvilket cybersikkerhetsselskap kjøpte TunnelBear i 2018?**

- A) McAfee
- B) Avast
- C) NortonLifeLock
- D) Kape Technologies

5 **5. Hvilken protokoll anbefaler TunnelBear for moderne høyhastighetstunneler?**

- A) WireGuard
- B) OpenVPN
- C) IKEv2
- D) PPTP

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. GhostBear kamuflerer VPN-metadata for å hjelpe til med å omgå brannmurer med dyp pakkeinspeksjon.

○ Sant ○ Usant

7 Spørsmål 7

7. TunnelBears gratisabonnement inkluderer ubegrenset månedlig surfedata.

○ Sant ○ Usant

8 Spørsmål 8

8. VigilantBear holder data trygge mens appen kobler til eller kobler til på nytt.

○ Sant ○ Usant

9 Spørsmål 9

9. TunnelBear var den første VPN-en for forbrukere som publiserte årlige offentlige sikkerhetsrevisjoner.

○ Sant ○ Usant

10 Spørsmål 10

10. Leverandøren opererer under streng jurisdiksjon etter panamansk lov.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. TunnelBear har hovedkontor i og drives fra _____ , som har strenge lover.
2. Tilsløringsteknologien drives av innstillingene for systemet _____ .
3. Beskyttelse mot lekkasjer på systemnivå styres av _____ -innstillinger.
4. VPN-leverandøren ble kjøpt av sikkerhetsutvikleren _____ i 2018.
5. Raske dataoverføringshastigheter oppnås via protokollen _____ .
6. Tradisjonelle klienttilkoblinger på skrivebordet bygger på protokollen _____ .

ORDBANK

CANADA GHOSTBEAR INGEN LOGGER MCAFEE OPENVPN REVISJON VIGILANTBEAR WIREGUARD

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble VPN- og nettverksbegreper

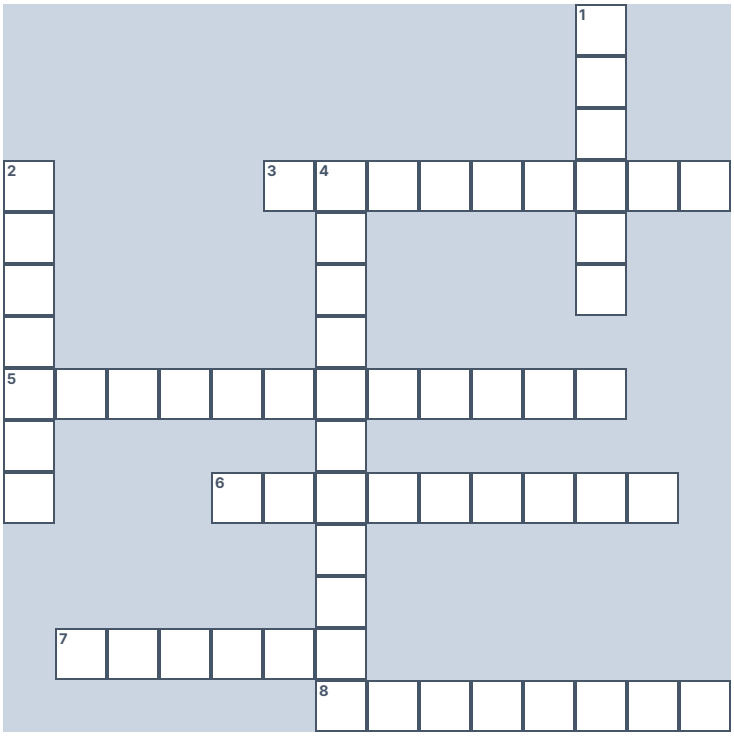
KOBLE DEFINISJONER

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

☐	1. CANADA	A	Personvernpolicy som forbyr lagring av trafikkhistorikk.
☐	2. GHOSTBEAR	B	Registreringsland og land for selskapets hovedkontor.
☐	3. VIGILANTBEAR	C	Sikkerhetsvurdering fra tredjepart som gjennomføres årlig.
☐	4. MCAFEE	D	Standard tunneleringsprotokoll med åpen kildekode som brukes på skrivebordet.
☐	5. WIREGUARD	E	Sikkerhetsmorselskap som kjøpte TunnelBear.
☐	6. OPENVPN	F	Protokoll med høy ytelse som bruker moderne kryptografi.
☐	7. REVISJON	G	Teknologi for omkoding av metadata som brukes til å omgå Deep Packet Inspection.
☐	8. NULL LOGGER	H	Innebygd kill switch som beskytter tilkoblinger når de faller ut.

Kontrollpunkt 5: Kryssord

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



VANNRETT

3. Høytytende protokoll som bruker moderne kryptografi (9)

5. Innebygd kill switch som beskytter tilkoblinger ved fall (12)

6. Teknologi for omskrambling av metadata som brukes til å omgå dyp pakkeinspeksjon (9)

7. Sikkerhetsselskapet som kjøpte TunnelBear (6)

8. Sikkerhetsvurdering fra tredjepart som gjennomføres årlig (8)

LODDRETT

1. Registreringsland og selskapets hovedkontor (6)

2. Standard tunnelprotokoll med åpen kildekode som brukes på skrivebordet (7)

4. Personvernpolicy som forbyr lagring av trafikkhistorikk (11)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

3 vannrett: Høytytende protokoll som bruker moderne kryptografi (9 bokstaver):

5 vannrett: Innebygd kill switch som beskytter tilkoblinger ved fall (12 bokstaver):

6 vannrett: Teknologi for omskrambling av metadata som brukes til å omgå dyp pakkeinspeksjon (9 bokstaver):

7 vannrett: Sikkerhetsselskapet som kjøpte TunnelBear (6 bokstaver):

8 vannrett: Sikkerhetsvurdering fra tredjepart som gjennomføres årlig (8 bokstaver):

LODDRETT

1 loddrett: Registreringsland og selskapets hovedkontor (6 bokstaver):

2 loddrett: Standard tunnelprotokoll med åpen kildekode som brukes på skrivebordet (7 bokstaver):

4 loddrett: Personvernpolicy som forbyr lagring av trafikkhistorikk (11 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

CANADA GHOSTBEAR VIGILANTBEAR MCAFEE WIREGUARD OPENVPN
REVISJON INGENLOGGER

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. CANADA
B. GHOSTBEAR
C. VIGILANTBEAR
D. MCAFEE
E. WIREGUARD
F. OPENVPN
G. REVISJON
H. INGENLOGGER

DEFINISJONER OG TILHØRENDE FELT

_____ 1. Standard tunnelprotokoll med åpen kildekode som brukes på skrivebordet.

_____ 2. Personvernpolicy som forbyr lagring av trafikkhistorikk.

_____ 3. Høytytende protokoll som bruker moderne kryptografi.

_____ 4. Registreringsland og selskapets hovedkontor.

_____ 5. Sikkerhetsvurdering fra tredjepart som gjennomføres årlig.

_____ 6. Teknologi for omskrambling av metadata som brukes til å omgå dyp pakkeinspeksjon.

_____ 7. Sikkerhetsselskapet som kjøpte TunnelBear.

_____ 8. Innebygd kill switch som beskytter tilkoblinger ved fall.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper om virtuelle private nettverk (VPN). Skriv svarene dine i svarboksene.

1. NCADAA
2. RILAVEAGTBNI
3. WUGIADERR
4. IONJSREV
5. ETHRBSGAO
6. EFMAEC
7. OPVNPNE
8. GORLGINNEGE

Bonusaktivitet: Tenk raskt

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

1	Land der du ville hatt TunnelBear-servere			
2	Ting TunnelBear kan skjule for nettverket ditt			
3	Situasjoner der en kill switch hjelper			
4	Sikkerhetsord du lærte i dette arbeidsarket			
5	VPN-protokoller du kjenner til			
6	Enheter du ville installert TunnelBear på			
7	Steder der du ville slått på TunnelBear			
8	Apper du ville brukt sammen med TunnelBear			
9	Tegn på at VPN-tilkoblingen din er treg			
10	Ting å sjekke før du kjøper en VPN			
11	Ord som beskriver en god VPN-app			
12	Knapper eller menyer i en VPN-app			
13	Strømmetjenester du ser på			
14	Data en VPN aldri bør lagre			
15	Funksjoner du leter etter i TunnelBear			

Kontrollpunkt 8: Casestudier om VPN og nettverk

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

CASESTUDIE 1: OMGÅ SENSUR



Scenario: En forsker som reiser gjennom en nasjon som blokkerer VPN-protokoller må få tilgang til forskningsmateriale.

Diskusjonsspørsmål: Hvilken TunnelBear-innstilling bør aktiveres for å omgå dyp pakkeinspeksjon (deep packet inspection)?

CASESTUDIE 2: USIKREDE OFFENTLIGE HOTSPOTS



Scenario: En ingeniør kobler til en åpen Wi-Fi-hotspot på en flyplass og opplever hyppige tilkoblingsbrudd.

Diskusjonsspørsmål: Hvordan beskytter VigilantBear ingeniørens enhet når tilkoblingen faller ut?

Kontrollpunkt 9: Knekk chifferet

En nettverksingeniør sikrer rutingkanaler og klienttunneler. 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

20 21 14 14 5 12 2 5 1 18 8 1 18

22 9 7 9 12 1 14 20 2 5 1 18

12 5 11 11 1 19 10 5 2 5 19 11 25 20 20 5 12 19 5

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del A)

Gå gjennom de vanligste spørsmålene og svarene om virtuelle private nettverk (VPN-er) og tunnelering.

Q1: Er TunnelBear trygg?

Ja, den bruker AES-256-kryptering og får appene sine revidert uavhengig hvert år. [1]

Q2: Hva er GhostBear?

GhostBear er en obfuskeringsfunksjon som skjuler VPN-trafikk for å omgå sensurblokkeringer.

Q3: Har den et gratisnivå?

Ja, TunnelBear tilbyr et begrenset gratisnivå med 2 GB månedlig båndbredde. [1]

Q4: Hvor har TunnelBear base?

TunnelBear har hovedkontor i Toronto i Canada, under kanadisk jurisdiksjon.

Q5: Hva er VigilantBear?

VigilantBear er TunnelBears innebygde kill switch som blokkerer lekkasjer når tilkoblingen faller ut.

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

Gå gjennom de vanligste spørsmålene og svarene om virtuelle private nettverk (VPN-er) og tunnelering.

Q6: Kan jeg koble til flere enheter?

Ja, betalte abonnement støtter ubegrenset antall samtidige tilkoblinger under én konto.

Q7: Støtter TunnelBear WireGuard?

Ja, WireGuard støttes for ytelsessterke og batterieffektive tilkoblinger.

Q8: Hva er deres policy om null logging?

TunnelBear logger ikke IP-adresser, DNS-spørringer eller brukernes nettaktivitet.

Q9: Hvem eier TunnelBear?

TunnelBear ble kjøpt opp av det store cybersikkerhetsfirmaet McAfee i 2018. [8]

Q10: Blokkerer den annonser?

TunnelBear fokuserer på kryptering; annonseblokkering er ikke innebygd i den primære VPN-klienten. [4]

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

Utforsk avanserte tekniske sider ved VPN-tunnelprotokoller, integrering av mobilklienter og utrulling i bedrifter.

Q1: Hvordan omgår GhostBear DPI?

Den får kryptert VPN-trafikk til å se ut som vanlig HTTPS, slik at DPI-filtre har vanskelig for å oppdage den.

Q2: Er Canada et 5-Eyes-land?

Ja, Canada er medlem av Five Eyes-alliansen, noe som reiser spørsmål om jurisdiksjon.

Q3: Hvordan blokkerer VigilantBear datalekkasjer?

Den blokkerer all inngående og utgående trafikk til VPN-tilkoblingen er gjenopprettet.

Q4: Hva kontrolleres i revisjonene deres?

Cure53 reviderer appkode, serverkonfigurasjoner, infrastruktur og kontroller for loggføring.

Q5: Kjører WireGuard innebygd?

Ja, TunnelBear-appene tilbyr WireGuard for raske og stabile tilkoblinger.

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

Utforsk avanserte tekniske sider ved VPN-tunnelprotokoller, integrering av mobilklienter og utrulling i bedrifter.

Q6: Finnes det spesialiserte P2P-servere?

Nei, P2P-trafikk støttes på alle globale servernoder uten begrensninger.

Q7: Forhindrer den WebRTC-lekkasjer?

Ja, klienten fanger opp og ruter WebRTC-forespørsler for å hindre eksponering av lokale IP-adresser.

Q8: Hvordan håndteres DNS-sikkerhet?

DNS-forespørsler rutes gjennom TunnelBears private, krypterte DNS-resolvere.

Q9: Kan jeg bruke den på Linux?

TunnelBear har ingen offisiell Linux-app; appene dekker Windows, macOS, iOS og Android. [5]

Q10: Hvordan isoleres faktureringsdatabaser?

Faktureringsposter lagres atskilt fra servertrafikkloggene for å bevare anonymiteten.

Del 11: 10 fakta om VPN fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om VPN-krypteringshastigheter, protokollrevisjoner, mobiltilkobling og fjernarbeid i bedrifter.

1. VPN-INNSIKT

TunnelBear har hovedkontor i Toronto i Canada og opererer under kanadisk jurisdiksjon. [2]

2. VPN-INNSIKT

Tjenesten ble kjøpt opp av McAfee i 2018 for å styrke sikkerhetsporteføljen deres. [3]

3. VPN-INNSIKT

GhostBear obfuskerer VPN-protokollens signaturer slik at de ser ut som vanlige HTTP/S-pakker. [4]

4. VPN-INNSIKT

VigilantBear fungerer som klientens kill switch for tilkoblingen på brannmurnivå. [4]

5. VPN-INNSIKT

Cure53 gjennomfører årlige offentlige revisjoner for å verifisere sikkerheten til appen og serverne. [6]

6. VPN-INNSIKT

Betalte abonnementer støtter et ubegrenset antall samtidige enhetstilkoblinger. [1]

7. VPN-INNSIKT

Nettverket bygger på AES-256-kryptering, den globale sikkerhetsstandarden. [1]

8. VPN-INNSIKT

Den støtter tunneler med protokollene OpenVPN, IKEv2 og WireGuard. [5]

9. VPN-INNSIKT

Det føres ingen logger over brukernes destinasjons-IP-adresser eller nettleserhistorikk.

10. VPN-INNSIKT

De tilbyr et leken brukergrensesnitt med bjørnetema som forenkler administrasjon av VPN.

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale tekniske standarder, spesifikasjoner og regelverk.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[1] TunnelBear, LLC. (2026). TunnelBear VPN - Apps on Google Play.

https://play.google.com/store/apps/details?id=com.tunnelbear.android&hl=en_US

[2] TunnelBear, LLC. (n.d.). TunnelBear: Safe and Fast VPN App - App Store.

https://apps.apple.com/us/app/tunnelbear-secure-vpn-wifi/id564842283

[3] TechCrunch. (2018). McAfee acquires VPN company TunnelBear.

https://techcrunch.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

[4] PCWorld. (2024). TunnelBear VPN review: It's just right for beginners.

https://www.pcworld.com/article/406999/tunnelbear-vpn-review-2.html

[5] CyberInsider. (2026). TunnelBear Review & Test Results 2026 — Pros and Cons.

https://cyberinsider.com/vpn/reviews/tunnelbear/

[6] Cure53. (2024). Pentest-Report TunnelBear VPN Clients & Servers 10-11.2023.

https://cure53.de/pentest-report_tunnelbear_2023.pdf

[7] Cure53. (2020). TunnelBear Security Assessment Summary 11.2019.

https://cure53.de/summary-report_tunnelbear_2019.pdf

[8] VentureBeat. (2018). McAfee acquires VPN provider TunnelBear.

https://venturebeat.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/

[9] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[10] Office of the Privacy Commissioner of Canada. (n.d.). The Personal Information Protection and Electronic Documents Act (PIPEDA).

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Fasit: Kontrollpunkt 1 – flervalg

1 **Spørsmål 1** — **Riktig svar: A**

MERKNAD TIL LÆREREN

I hvilket land er TunnelBears selskap registrert? → Canada

2 **Spørsmål 2** — **Riktig svar: A**

MERKNAD TIL LÆREREN

Hva heter TunnelBears obfuskering for å omgå sensur? → GhostBear

3 **Spørsmål 3** — **Riktig svar: A**

MERKNAD TIL LÆREREN

Hva heter TunnelBears innebygde kill switch-funksjon? → VigilantBear

4 **Spørsmål 4** — **Riktig svar: A**

MERKNAD TIL LÆREREN

Hvilket cybersikkerhetsselskap kjøpte TunnelBear i 2018? → McAfee

5 **Spørsmål 5** — **Riktig svar: A**

MERKNAD TIL LÆREREN

Hvilken protokoll anbefaler TunnelBear for moderne høyhastighetstunneler? → WireGuard

Fasit: Kontrollpunkt 2 – sant eller usant

6 Spørsmål 6

Riktig svar: Sant

MERKNAD TIL LÆREREN

Sant: GhostBear skjuler VPN-trafikk for å hjelpe den forbi dyp pakkeinspeksjon.

7 Spørsmål 7

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: gratisabonnementet gir 2GB surfedata hver måned.

8 Spørsmål 8

Riktig svar: Sant

MERKNAD TIL LÆREREN

VigilantBear holder data trygge mens appen kobler til eller kobler til på nytt.

9 Spørsmål 9

Riktig svar: Sant

MERKNAD TIL LÆREREN

Sant: TunnelBear sier at de var den første VPN-en for forbrukere som gjennomførte årlige offentlige tredjepartsrevisjoner.

10 Spørsmål 10

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: TunnelBear har base i Toronto og drives under kanadisk lov.

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

B 1. CANADA	G 2. GHOSTBEAR	H 3. VIGILANTBEAR	E 4. MCAFEE
F 5. WIREGUARD	D 6. OPENVPN	C 7. REVISJON	A 8. NULL LOGGER

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 CANADA	2 GHOSTBEAR	3 VIGILANTBEAR	4 MCAFEE
5 WIREGUARD	6 OPENVPN		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 F – OPENVPN	2 H – INGENLOGGER	3 E – WIREGUARD	4 A – CANADA
5 G – REVISJON	6 B – GHOSTBEAR	7 D – MCAFEE	8 C – VIGILANTBEAR

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare CANADA, GHOSTBEAR og VIGILANTBEAR med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

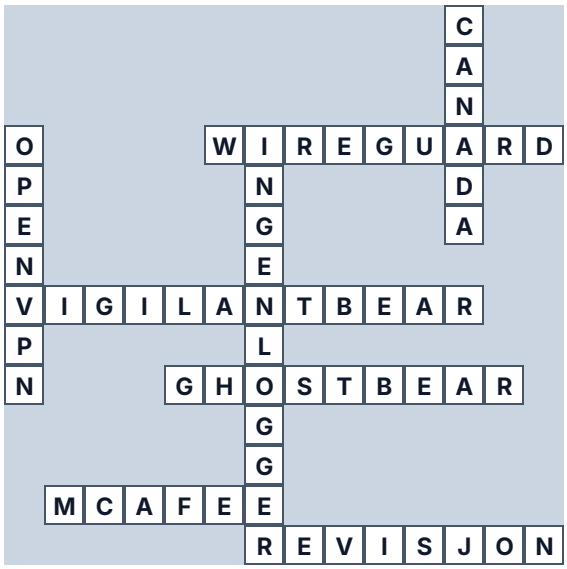
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

3 vannrett: WIREGUARD Høytytende protokoll som bruker moderne kryptografi (9 bokstaver)

5 vannrett: VIGILANTBEAR Innebygd kill switch som beskytter tilkoblinger ved fall (12 bokstaver)

6 vannrett: GHOSTBEAR Teknologi for omskrambling av metadata som brukes til å omgå dyp pakkeinspeksjon (9 bokstaver)

7 vannrett: MCAFEE Sikkerhetsselskapet som kjøpte TunnelBear (6 bokstaver)

8 vannrett: REVISJON Sikkerhetsvurdering fra tredjepart som gjennomføres årlig (8 bokstaver)

LODDRETT

1 loddrett: CANADA Registreringsland og selskapets hovedkontor (6 bokstaver)

2 loddrett: OPENVPN Standard tunnelprotokoll med åpen kildekode som brukes på skrivebordet (7 bokstaver)

4 loddrett: INGENLOGGER Personvernpolicy som forbyr lagring av trafikkhistorikk (11 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. N C A D A A — **CANADA**
2. R I L A V E A G T B N I — **VIGILANTBEAR**
3. W U G I A D E R R — **WIREGUARD**
4. I O N J S R E V — **REVISJON**
5. E T H R B S G A O — **GHOSTBEAR**
6. E F M A E C — **MCAFEE**
7. O P V N P N E — **OPENVPN**
8. G O R L G I N N E G E — **INGENLOGGER**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"TUNNELBEAR HAR VIGILANTBEAR LEKKASJEBESKYTTELSE"

Fasit til casestudiene

A CASESTUDIE 1: OMGÅ SENSUR

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En forsker som reiser gjennom et land som blokkerer VPN-protokoller, må få tilgang til forskningsmateriale.
- Anbefalt strategi og løsning: GhostBear må være aktivert for å kryptere VPN-pakkenes metadata, slik at trafikken ser ut som vanlig HTTPS-trafikk.

B CASESTUDIE 2: USIKREDE OFFENTLIGE HOTSPOTS

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En ingeniør kobler seg til et åpent Wi-Fi-hotspot på en flyplass og opplever hyppige brudd i tilkoblingen.
- Anbefalt strategi og løsning: VigilantBear fryser alle nettverksgrensesnitt og blokkerer lekkasjer av ukryptert trafikk til VPN-tunnelen er gjenopprettet.