Navn: _____ Dato: _____ Poeng: _____

Slik velger du en VPN Arbeidsark

Vurdering av VPN-leverandører, sikkerhetsstandarder, revisjoner og logging-policyer

OPPLÆRINGSOVERSIKT FOR VPN

ELEV
STUDENTSTATUS
Spor for nettverksforsvarere

SIKKER
TILKOBLINGSSTATUS
Beskytte datapakker

AKTIV
LEKKASJEBESKYTTELSE
DNS- og IPv6-lekkasjebeskyttelse

Velkommen! Dette aktivitetsheftet veileder deg gjennom de grunnleggende prinsippene i virtuelle private nettverk (VPN-er). Du utforsker hvordan krypterte tunneler sikrer dataene dine, hvordan nettverksprotokoller fungerer, og hvordan du identifiserer og begrenser personvernlekkasjer.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk VPN-begreper og -protokoller.**
- [ ] **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 VPN-veiledning

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

Din læringsveiledning for VPN

- Vurder leverandørens jurisdiksjon og policyer om ingen logging med tanke på personvern.
- Sammenlign tunnelprotokoller som WireGuard og OpenVPN med tanke på hastighet.
- Analyser sikkerhetsfunksjoner som kill switch og servernoder med bare RAM.
- Identifiser uavhengige sikkerhetsrevisjoner og prisplaner når du velger.
- Velg serverplasseringer ut fra behovet ditt for hastighet og opphevelse av geografiske blokkeringer.

INSTRUKSJONER FOR VALGARBEIDSARKET

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på valg av sikker VPN-infrastruktur. Avslutt med bonusaktiviteten Tenk raskt.

VELGE EN VPN (INNLEDNING)

Å velge riktig VPN krever at du ser forbi markedsføringsbløffen. En pålitelig leverandør må ha en dokumentert policy om ingen logging, sikre krypteringsprotokoller og klienter med åpen kildekode. Ved å vurdere sikkerhetsfunksjoner, jurisdiksjoner og hastighet kan du velge en VPN som passer dine behov for digital beskyttelse.

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

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er nøkkelfaktoren når du velger en sikker VPN-leverandør?

- A. Antall serverland
- B. En uavhengig revidert retningslinje om ingen logging
- C. Det laveste månedlige prisnivået
- D. Prangende reklamesponsorater

2. Hvilken VPN-protokoll gir den beste balansen mellom hastighet og mulighet for revisjon?

- A. PPTP (eldre)
- B. L2TP/IPSec
- C. Kun OpenVPN over TCP
- D. WireGuard

3. Hvorfor bør brukere unngå gratis VPN-er til sensitive aktiviteter?

- A. De er forbudt i USA
- B. De selger ofte nettleserhistorikken din
- C. De støtter ikke vanlig nettsurfing
- D. De krever spesialisert maskinvare for å koble til

4. Hva avgjør en leverandørs juridiske hjemland?

- A. Hastigheten på servertilkoblingen
- B. Hvilke typer enheter som støttes
- C. Lokale lover om datalagring og ransakingsordre
- D. Det visuelle temaet til klientapplikasjonen

5. Hva er hovedformålet med «kill switch»-funksjonen i en VPN-klient?

- A. Å blokkere internettilgang hvis VPN-tilkoblingen faller ut
- B. Å slette alle installerte programmer på enheten
- C. For å doble hastigheten på servertilkoblingen
- D. For å starte operativsystemet på nytt når det er inaktivt

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. En VPN beskytter enheten din mot nedlasting av skadevare og virusfiler.

○ Sant ○ Usant

7 Spørsmål 7

7. Uavhengige revisjoner fra selskaper som Deloitte bekrefter påstander om null logging.

○ Sant ○ Usant

8 Spørsmål 8

8. Lovene i leverandørens hjemland påvirker ikke personvernet for brukerdata.

○ Sant ○ Usant

9 Spørsmål 9

9. WireGuards kompakte kodebase er enklere å gjennomgå enn OpenVPNs.

○ Sant ○ Usant

10 Spørsmål 10

10. Gratis VPN-er selger ofte annonser eller sporer brukere for å dekke serverkostnadene.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. En uavhengig verifisert policy om _____ forplikter en VPN-leverandør til ikke å registrere nettlesehistorikken din.

2. Den moderne protokollen _____ gir høy hastighet og bruker en svært liten kodebase.

3. En sikkerhetsfunksjon som kalles _____ stanser all trafikk hvis VPN-tilkoblingen plutselig svikter.

4. Å vurdere leverandørens juridiske _____ avgjør om de er underlagt overvåkingsavtaler.

5. Å sikre servere med _____ disker hjelper til med å hindre at brukerdata blir værende etter en omstart.

6. Å verifisere en policy om null kunnskap krever en uavhengig _____ av sikkerheten fra anerkjente firmaer.

ORDBANK

GRATIS VPN | INGEN LOGGER | JURISDIKSJON | KILL SWITCH | RAM-BASERTE
REVISJON | SPLIT TUNNELING | WIREGUARD

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble nettverksbegreper

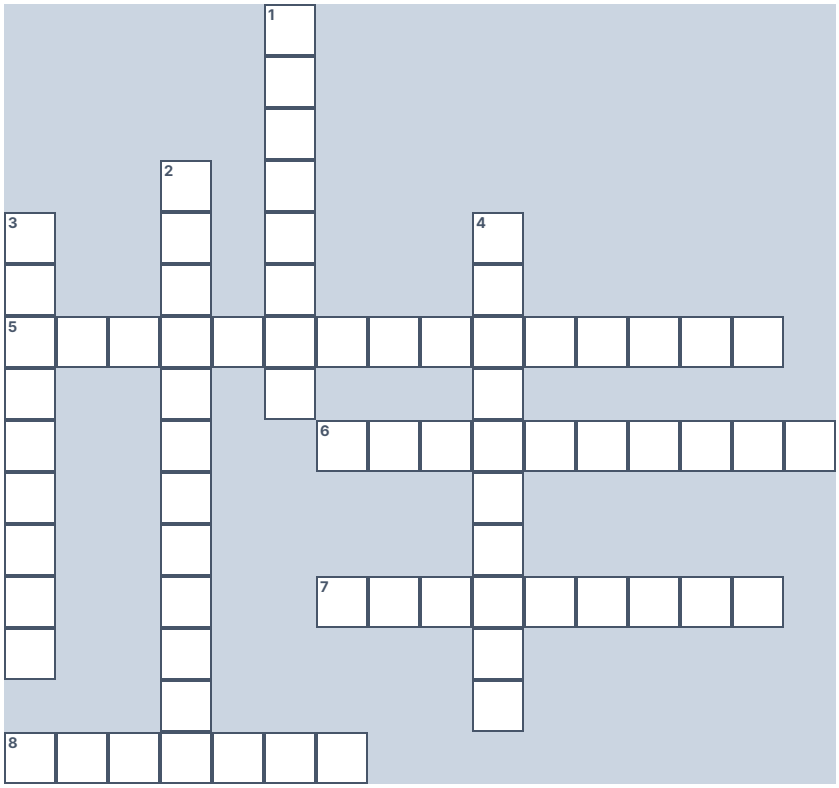
KOBLE DEFINISJONER

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

☐	1. WireGuard	A	Tilkoblingstjeneste med høy risiko som ofte tjener penger ved å logge og selge nettleserdata.
☐	2. Reviderte logger	B	Sikkerhetsmekanisme som blokkerer internettruting hvis den sikre tunnelen kobles fra.
☐	3. Jurisdiksjon	C	Internasjonal allianse for deling av etterretning mellom USA, Storbritannia, Canada, Australia og New Zealand.
☐	4. Kill switch	D	Maskinvareinfrastruktur som kjører på flyktig minne, slik at data ikke lagres på disk.
☐	5. Five Eyes	E	Det geografiske området som styrer VPN-leverandørens juridiske forpliktelser.
☐	6. Gratis VPN	F	Moderne, rask protokoll som bruker omtrent 4000 linjer med svært revisjonsvennlig kode.
☐	7. Servere med bare RAM	G	Moden, mye revidert protokoll med åpen kildekode og en langt større kodebase enn WireGuard.
☐	8. OpenVPN	H	Personvernpåstand bekreftet av uavhengige tredjeparts cybersikkerhetsfirmaer.

Kontrollpunkt 5: Kryssord

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



VANNRETT

5. Personvernpåstand verifisert av uavhengige cybersikkerhetsfirmaer fra tredjepart (15)

6. Maskinvareinfrastruktur som kjører helt på flyktig minne og hindrer datalagring (10)

7. Høyrisikotjeneste for tilkobling som ofte tjener penger ved å logge og selge nettleserdata (9)

8. Moden, mye revidert protokoll med åpen kildekode og en langt større kodebase enn WireGuard (7)

LODDRETT

1. Internasjonal etterretningsallianse mellom USA, Storbritannia, Canada, Australia og New Zealand (8)

2. Det geografiske området som styrer VPN-leverandørens juridiske forpliktelser (12)

3. Moderne, rask protokoll som bruker omtrent 4000 linjer svært reviderbar kode (9)

4. Sikkerhetsmekanisme som blokkerer internettruting hvis den sikre tunnelen kobles fra (10)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

5 vannrett: Personvernpåstand verifisert av uavhengige cybersikkerhetsfirmaer fra tredjepart (15 bokstaver):

6 vannrett: Maskinvareinfrastruktur som kjører helt på flyktig minne og hindrer datalagring (10 bokstaver):

7 vannrett: Høyrisikotjeneste for tilkobling som ofte tjener penger ved å logge og selge nettleserdata (9 bokstaver):

8 vannrett: Moden, mye revidert protokoll med åpen kildekode og en langt større kodebase enn WireGuard (7 bokstaver):

LODDRETT

1 loddrett: Internasjonal etterretningsallianse mellom USA, Storbritannia, Canada, Australia og New Zealand (8 bokstaver):

2 loddrett: Det geografiske området som styrer VPN-leverandørens juridiske forpliktelser (12 bokstaver):

3 loddrett: Moderne, rask protokoll som bruker omtrent 4000 linjer svært reviderbar kode (9 bokstaver):

4 loddrett: Sikkerhetsmekanisme som blokkerer internettruting hvis den sikre tunnelen kobles fra (10 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

WIREGUARD REVIDERTELOGGER JURISDIKSJON KILLSWITCH FIVEEYES
GRATISVPN RAMSERVERE OPENVPN

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. WIREGUARD
B. REVIDERTELOGGER
C. JURISDIKSJON
D. KILLSWITCH
E. FIVEEYES
F. GRATISVPN
G. RAMSERVERE
H. OPENVPN

	DEFINISJONER OG TILHØRENDE FELT
	1. Internasjonal etterretningsallianse mellom USA, Storbritannia, Canada, Australia og New Zealand.
	2. Moderne, rask protokoll som bruker omtrent 4000 linjer svært reviderbar kode.
	3. Moden, mye revidert protokoll med åpen kildekode og en langt større kodebase enn WireGuard.
	4. Høyrisikotjeneste for tilkobling som ofte tjener penger ved å logge og selge nettleserdata.
	5. Sikkerhetsmekanisme som blokkerer internettruting hvis den sikre tunnelen kobles fra.
	6. Maskinvareinfrastruktur som kjører helt på flyktig minne og hindrer datalagring.
	7. Det geografiske området som styrer VPN-leverandørens juridiske forpliktelser.
	8. Personvernpåstand verifisert av uavhengige cybersikkerhetsfirmaer fra tredjepart.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale VPN-begreper. Skriv svarene dine i de utfyllbare svarboksene.

1. UGEIWARDR
2. NUSDJJORKSII
3. EIFEYSEV
4. RREESEVRAM
5. VOIRGELERRGTEED
6. CSLITKIWHL
7. SGPNVTRIA
8. PNNOPVE

Bonusaktivitet: Tenk raskt

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

1	Ting en VPN kan skjule			
2	Ting som betyr mer enn prisen			
3	Steder å lese VPN-anmeldelser			
4	Ting en VPN ikke kan beskytte deg mot			
5	Spørsmål til et VPN-salgsteam			
6	Ting internettleverandøren din kan se			
7	Punkter på sjekklisten din når du velger en VPN			
8	Steder der du ville brukt en VPN			
9	Advarselstegn hos en VPN-leverandør			
10	Ord knyttet til personvern			
11	Ting du ville testet først			
12	Løfter en god VPN-leverandør gir			
13	Grunner til å bruke en VPN på reise			
14	Enheter som kan bruke en VPN			
15	Myter om VPN-er			

Kontrollpunkt 8: Casestudier om VPN

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

SARAH (STUDENT PÅ KAFÉ)

👷 «Hei! Jeg sitter på Coffee & Bytes. Der er det et usikret offentlig nettverk som heter «Free_Wi-Fi_No_Password». Jeg vil logge inn på skole-e-posten min og levere oppgaven min, men jeg er bekymret for hackere. Hva er risikoen ved å bruke dette nettverket uten en VPN, og hvordan sikrer en VPN dataene mine?»

ALEX (REISENDE STUDENT)

👷 «Å nei! Jeg reiser i utlandet i forbindelse med et prosjekt og prøver å se en biologidokumentar som ligger på en server i hjemlandet mitt. Men nettstedet sier «Denne videoen er ikke tilgjengelig der du befinner deg nå.» Hvorfor er jeg blokkert, og hvordan kan en VPN hjelpe meg å se den?»

Kontrollpunkt 9: Knekk chifferet

For å fullføre treningen i utvelgelsesveiledning må du dekryptere denne skjulte meldingen om valg av sikker infrastruktur.

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

19 1 13 13 5 14 12 9 7 14

18 1 16 16 15 18 20 5 14 5 4 9 14 5 13 5 4

5 20 19 9 11 11 5 18 20 19 25 19 20 5 13

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 potensielle kunder har om bruk av virtuelle private nettverk.

Q1: Hva er en VPN, og hvordan fungerer den?

Et virtuelt privat nettverk (VPN) krypterer internettforbindelsen din og ruter trafikken gjennom en sikker ekstern server. Dette maskerer den offentlige IP-adressen din og begrenser hva observatører på lokale nettverk og internettleverandøren din kan se om trafikk som rutes gjennom VPN-tunnelen.

Q2: Hvorfor bør jeg bruke en VPN?

En VPN beskytter ditt digitale personvern, sikrer tilkoblingen din på offentlige Wi-Fi-nettverk (som kafeer eller flyplasser), kan redusere aktivitetsbasert struping når internettleverandøren ikke kan identifisere typen kryptert trafikk, omgår geografiske begrensninger for å få tilgang til globalt innhold og bidrar til å sikre ressurser for fjernarbeid.

Q3: Gjør en VPN meg helt anonym på nett?

Nei. Selv om en VPN skjuler IP-adressen din og krypterer trafikk, kan du fortsatt spores via informasjonskapsler i nettleseren, aktive kontoer (som Google eller Facebook), nettleserens fingeravtrykk eller hvis VPN-leverandøren din logger dataene dine.

Q4: Vil en VPN gjøre internetthastigheten min tregere?

Ja, litt. Krypteringsprosessen og den fysiske avstanden til VPN-serveren gir ekstra ventetid og belastning. Effekten varierer med leverandør, protokoll, serveravstand, enhet og nettverksforhold.

Q5: Hvordan tjener den penger?

Sjekk forretningsmodellen. Abonnementer, freemium-nivåer og salg av data påvirker alle hvor mye du kan stole på en VPN, og en tjeneste som aldri samler inn dataene dine, kan ikke selge dem. Les personvernerklæringen først. [1]

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

Gå gjennom de vanligste spørsmålene og svarene potensielle kunder har om bruk av virtuelle private nettverk.

Q6: Kan jeg bruke en gratis VPN?

Gratis VPN-er kan være basert på reklame, begrensede funksjoner, bruksanalyse, datagrenser eller andre inntektsmodeller. Brukere bør gå gjennom leverandørens personvernerklæring, eierskap, revisjoner og forretningsmodell før bruk.

Q7: Hva er en policy om ingen logging («no-logs»)?

En retningslinje om ingen logging beskriver hvilke aktivitets- og tilkoblingsdata en leverandør sier at den ikke oppbevarer. Det nøyaktige omfanget varierer, så leserne bør gjennomgå retningslinjen og funnene fra uavhengige revisjoner.

Q8: Hvordan velger jeg den beste VPN-en?

Se etter revisjonsgodkjente policyer om ingen logging, sterke protokoller (WireGuard, OpenVPN), sikre serverplasseringer, høy hastighet, servere som kun bruker RAM, en kill switch-funksjon og jurisdiksjon utenfor etterretningsallianser (som 5/9/14 Eyes).

Q9: Kan jeg bruke en VPN på telefonen og smart-TV-en min?

Ja. Moderne VPN-leverandører tilbyr egne apper for iOS, Android, macOS, Windows, Linux og smart-TV-er, i tillegg til ruteroppsett som beskytter alle enhetene i hjemmenettverket ditt.

Q10: Hva er en Kill Switch?

En kill switch er en sikkerhetsfunksjon som automatisk kobler enheten din fra internett hvis VPN-tilkoblingen faller ut. Dette hindrer at ukrypterte data eller den virkelige IP-adressen din lekker ut.

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

Utforsk tekniske og strukturelle sider ved virtuelle private nettverk og sikre tunnelprotokoller.

Q1: Hva er forskjellen mellom WireGuard, OpenVPN og IKEv2?

WireGuard er en moderne, lettvekts protokoll (bare ca. 4000 kodelinjer) som gir høy hastighet og raske tilkoblingstider. OpenVPN er en svært sikker, velprøvd protokoll med åpen kildekode. IKEv2 er utmerket for mobile enheter fordi den kan koble til igjen raskt når du bytter nettverk.

Q2: Hva er dobbel VPN eller Multi-Hop-ruting?

Multi-hop ruter trafikken din gjennom to eller flere VPN-servere i rekkefølge. Dette gir et ekstra lag med kryptering og bidrar til å holde den virkelige IP-adressen din skjult for den andre serveren hvis én server blir kompromittert.

Q3: Hva er WebRTC-lekkasje, og hvordan forhindrer en VPN den?

WebRTC er en nettleserprotokoll som kan avsløre dine ekte lokale og offentlige IP-adresser selv når et VPN er aktivt. Premium VPN-er blokkerer eller forfalsker WebRTC-forespørsler i appene for skrivebord og mobil og i nettleserutvidelsene sine.

Q4: Hva er servere som kun bruker RAM, og hvorfor er de viktige?

Tradisjonelle servere skriver data til harddisker, som kan beslaglegges eller kompromitteres. Servere kun med RAM (diskløse) kjører helt i flyktig minne (RAM). Når serveren startes på nytt eller slås av, slettes data i minnet.

Q5: Hvordan omgår obfuskering VPN-blokkeringer?

Obfuskering (eller «Stealth VPN») skjuler VPN-trafikkpakker slik at de ser ut som vanlig HTTPS-nettrafikk (port 443). Dette bidrar til å komme forbi dyp pakkeinspeksjon (DPI), som myndigheter eller skole- og kontornettverk bruker for å blokkere VPN.

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

Utforsk tekniske og strukturelle sider ved virtuelle private nettverk og sikre tunnelprotokoller.

Q6: Hva er split tunneling, og når bør jeg bruke det?

Split tunneling lar deg velge hvilke apper som rutes gjennom den krypterte VPN-tunnelen, og hvilke som kobler seg direkte til internett. Bruk det til å rute sensitive bankapper gjennom VPN-en mens lokale spill kobler seg direkte, slik at du unngår forsinkelsen VPN-en legger til.

Q7: Hvordan fungerer Forward Secrecy (Perfect Forward Secrecy)?

PFS sørger for at det genereres en unik, midlertidig krypteringsnøkkel for hver eneste økt. Selv om en privat nøkkel skulle bli kompromittert i fremtiden, kan den ikke brukes til å dekryptere tidligere eller fremtidige økter, fordi de brukte uavhengige nøkler.

Q8: Hva er alliansene 5/9/14 Eyes, og hvorfor bør jeg bry meg?

Jurisdiksjon kan påvirke den juridiske prosessen en leverandør kan møte, men den praktiske personvernrisikoen avhenger også av hvilke data leverandøren beholder, den tekniske arkitekturen, eierskapet, åpenhetsrapportering og revisjonshistorikken.

Q9: Hva er beskyttelse mot DNS-lekkasjer?

DNS-lekkasjebeskyttelse tvinger enheten din til å sende oppslagsforespørsler for nettsteder (DNS-forespørsler) gjennom VPN-ens private, krypterte DNS-servere i stedet for internettleverandørens servere. Dette hindrer internettleverandøren din i å spore hvilke nettsteder du besøker.

Q10: Hvorfor bør man sjekke hvem som driver og støtter en VPN?

Omdømme har betydning. Undersøk selskapets eiere og ledere, se etter offentlige tredjepartsrevisjoner, og sjekk hva uavhengige sikkerhetseksperter og pressen sier, før du stoler på det. [1]

Del 11: 10 interessante fakta om VPN og innsikt fra virkeligheten

Gå gjennom disse verdifulle, virkelighetsnære fakta og innsiktene om historien, markedet og teknologien bak VPN-er.

1. FØRSTE VPN-PROTOKOLL

PPTP (Point-to-Point Tunneling Protocol), en tidlig VPN-protokoll fra en Microsoft-ledet gruppe på 1990-tallet, regnes nå som usikker, så moderne VPN-er bruker WireGuard eller OpenVPN. [1]

2. MARKEDSVERDSETTELSE

Det globale VPN-markedet har vokst raskt, drevet av økende behov for fjernarbeid og krav til bedriftssikkerhet.

3. WIREGUARD-REVOLUSJONEN

WireGuard har en svært strømlinjeformet kodebase som er utformet for effektivitet, noe som gjør det enklere å gjennomgå for sikkerhetssårbarheter enn tradisjonelle protokoller. [3]

4. STRENGE REVISJONSSTANDARDER

Ledende VPN-leverandører engasjerer firmaer som Deloitte, KPMG eller PwC til å kontrollere påstander om ingen logging, og sikkerhetsfirmaer som Cure53 til å teste appene og serverne sine. [4]

5. OPPRINNELSEN TIL 5 EYES-ALLIANSEN

Etterretningspartnerskapet Five Eyes mellom USA, Storbritannia, Canada, Australia og New Zealand vokste ut av alliertes samarbeid om signaletterretning under andre verdenskrig.

6. DYP PAKKEINSPEKSJON

Avanserte brannmurer bruker Deep Packet Inspection (DPI) for å analysere metadata i nettverkspakker og blokkere typiske kjennetegn ved VPN-tilkoblinger.

7. BEDRIFTSBRUK

Mange organisasjoner gir eksterne ansatte en VPN for å nå interne systemer som databaser, noe som gjør VPN-er til et vanlig sikkerhetsverktøy på arbeidsplassen.

8. DESENTRALISERTE VPN-ER

Desentraliserte VPN-er (dVPN-er) fordeler trafikken over et nettverk av noder drevet av likemenn (peers), noe som reduserer avhengigheten av én enkelt sentralisert leverandør.

9. ANONYMITET MED TOR MOT VPN

En VPN tunnelerer trafikk gjennom én enkelt leverandør, mens Tor (The Onion Router) sender trafikk gjennom tre frivillige reléer (inngang, mellomledd, utgang) for å maksimere personvernet. [5]

10. KOSTNADER VED DATABRUDD

Å kombinere en VPN med en nulltillit-tilgangsmodell, som kontrollerer hver bruker og enhet, hjelper organisasjoner med å beskytte data og begrense skadene ved datainnbrudd.

Tekniske referanser og kilder

Siterte publikasjoner, kryptografiske spesifikasjoner og offisielle dokumentstandarder som er brukt i dette arbeidsarket.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.

https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

Fasit: Vurdering av VPN-leverandører, sikkerhetsstandarder, revisjoner og loggingspraksis

1 **Retningslinjer for reviderte logger** PROTOKOLLER — **Riktig svar: B**

MERKNAD TIL LÆREREN

En uavhengig revidert retningslinje om ingen logging er den mest praktiske måten å kontrollere en leverandørs påstander om personvern uten kunnskap om brukerne. løynefallende markedsføring eller egne påstander er ikke tilstrekkelig.

2 **WireGuards overlegenhet** LATENS — **Riktig svar: D**

MERKNAD TIL LÆREREN

WireGuard gir moderne, rask tilkoblingsruting i kjerneområdet med en kompakt kodebase (ca. 4000 linjer), noe som gjør revisjoner svært effektive.

3 **Spørsmål 3** — **Riktig svar: B**

MERKNAD TIL LÆREREN

Gratis VPN-er må fortsatt betale for servere, og FTC advarer om at enkelte VPN-apper deler brukerdata med tredjeparter, for eksempel for å vise annonser.

4 **Juridiske jurisdiksjoner** RUTINGKONTROLLER — **Riktig svar: C**

MERKNAD TIL LÆREREN

Jurisdiksjon avgjør om VPN-en er underlagt overvåkingslover, lokale krav om datalagring og hemmelige stevninger fra myndighetene.

5 **Beskyttelse med Kill Switch** PERSONVERN — **Riktig svar: A**

MERKNAD TIL LÆREREN

Kill switch kutter umiddelbart rutingen til systemets nettverkskort hvis tunnelen faller ut, og hindrer lekkasje av virkelig IP og DNS.

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Begrensninger ved skadevare** IP-MASKERING — Riktig svar: Usant

MERKNAD TIL LÆREREN

En VPN gir en sikker, kryptert kanal, men den skanner ikke nyttelast eller filer. Antivirusprogramvare kreves for å blokkere skadevare.

7 **Uavhengig revisjon** HASTIGHETER — Riktig svar: Sant

MERKNAD TIL LÆREREN

Revisjonsrapporter verifiserer serverprogramvarens konfigurasjon, at oppsettet kun bruker RAM, og at det ikke finnes loggdatabaser.

8 **Spørsmål 8** — Riktig svar: Usant

MERKNAD TIL LÆREREN

Leverandører må følge lovene i hjemlandet sitt, som kan omfatte regler for datalagring og pålegg om å utlevere data de har.

9 **Størrelse på protokollens kodebase** BRANNMURER — Riktig svar: Sant

MERKNAD TIL LÆREREN

En mindre kodebase reduserer den potensielle angrepsflaten og gjør det enklere for sikkerhetsteam å verifisere protokollens integritet.

10 **Inntektsgenerering fra annonser** INGEN LOGGING — Riktig svar: Sant

MERKNAD TIL LÆREREN

Uten abonnementsavgifter er gratis VPN-er avhengige av datautvinning, trafikkprofilering og annonser som injiseres i nettleseren for å tjene penger.

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

F 1. WireGuard	H 2. Reviderte logger	E 3. Jurisdiksjon	B 4. Kill switch
C 5. Five Eyes	A 6. Gratis VPN	D 7. Servere med bare RAM	G 8. OpenVPN

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 INGEN LOGGER	2 WIREGUARD	3 KILL SWITCH	4 JURISDIKSJON
5 RAM-BASERTE	6 REVISJON		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 E – FIVEEYES	2 A – WIREGUARD	3 H – OPENVPN	4 F – GRATISVPN
5 D – KILLSWITCH	6 G – RAMSERVERE	7 C – JURISDIKSJON	8 B – REVIDERTELOGGER

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare WireGuard, Reviderte logger og Jurisdiksjon med egne ord og gi et eksempel på hvert.

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

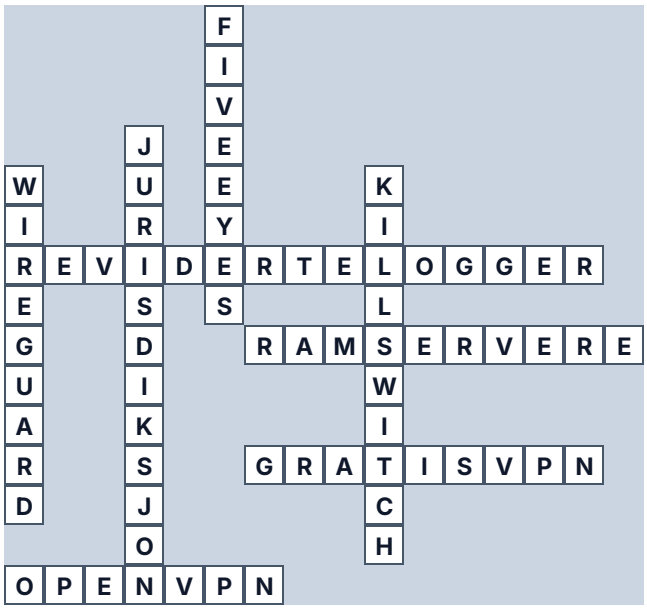
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

5 vannrett: REVIDERTELOGGER Personvernpåstand verifisert av uavhengige cybersikkerhetsfirmaer fra tredjepart (15 bokstaver)

6 vannrett: RAMSERVERE Maskinvareinfrastruktur som kjører helt på flyktig minne og hindrer datalagring (10 bokstaver)

7 vannrett: GRATISVPN Høyrisikotjeneste for tilkobling som ofte tjener penger ved å logge og selge nettleserdata (9 bokstaver)

8 vannrett: OPENVPN Moden, mye revidert protokoll med åpen kildekode og en langt større kodebase enn WireGuard (7 bokstaver)

LODDRETT

1 loddrett: FIVEEYES Internasjonal etterretningsallianse mellom USA, Storbritannia, Canada, Australia og New Zealand (8 bokstaver)

2 loddrett: JURISDIKSJON Det geografiske området som styrer VPN-leverandørens juridiske forpliktelser (12 bokstaver)

3 loddrett: WIREGUARD Moderne, rask protokoll som bruker omtrent 4000 linjer svært reviderbar kode (9 bokstaver)

4 loddrett: KILLSWITCH Sikkerhetsmekanisme som blokkerer internettruting hvis den sikre tunnelen kobles fra (10 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. U G E I W A R D R — **WIREGUARD**
2. N U S D J J O R K S I I — **JURISDIKSJON**
3. E I F E Y S E V — **FIVEEYES**
4. R R E E S E V R A M — **RAMSERVERE**
5. V O I R G E L E R R G T E E D — **REVIDERTELOGGER**
6. C S L I T K I W H L — **KILLSWITCH**
7. S G P N V T R I A — **GRATISVPN**
8. P N N O P V E — **OPENVPN**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"SAMMENLIGN RAPPORTENE DINE MED ET SIKKERT SYSTEM"

Fasit til casestudiene

A Scenario A: Sikkerhet på offentlige nettverk

SNIFFING OG KRYPTERING | Sarahs dilemma

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Risikoer: Pakkesniffing, avlytting av data og man-in-the-middle-angrep. Noen på det samme nettverket på kafeen kan fange opp innloggingsopplysningene hennes eller lekse-filen hennes.
- VPN-beskyttelse: Krypterer nyttelastene i nettverkspakkene, slik at avlyttet tunneltrafikk blir uleselig for passive snusere i det lokale nettverket når VPN-en er riktig konfigurert.

B Scenario B: Tilgang til blokkerte ressurser

GEOBLOKKERING OG IP-ADRESSER | Alex' dilemma

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Hvorfor blokkert: Strømmetjenesten bruker geoblokkering, som kobler reisendes lokale IP-adresse til hans fysiske land og blokkerer den basert på territoriell lisensiering.
- Slik hjelper VPN: Han maskerer sin virkelige posisjon ved å rute trafikken gjennom en server i hjemlandet sitt. Nettstedet ser en IP-adresse fra hjemlandet, og han får tilgang.