Navn: _____ Dato: _____ Poeng: _____

Darknet mot dypnett: sikkerhet og Forskjeller

Søkemotorindeksering, det dype nettet, Tor onion-ruting, nettverksanonymitet og risikoer

LÆRINGSOVERSIKT: DARKNET MOT DET DYPE NETTET

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 forskjellene mellom det dype nettet og mørkenettet. Du utforsker uindekserte databaser, onion-ruting i Tor-nettleseren, kryptografiske .onion-domener og sikkerhetsrisikoer for anonymitet.

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/mork-nett-vs-dypnett/

Din læringsveiledning for strategi for det dype nettet og mørkenettet

- Sammenlign det dype nettet (uindekserte databaser) med darknet (onion-tjenester).
- Forstå hvordan onion routing krypterer og videresender nettverkstrafikk.
- Vurder sikkerhetsrisikoene ved å besøke uverifiserte nettsteder på Tor-nettverket.
- Distribuer sikre gateway- og sandkasse-policyer for gjennomsøking av trusseletterretning.
- Analyser det kryptografiske adresseformatet til onion-tjenestedomener.

INSTRUKSJONER FOR GUIDEN OM DYPNETT OG DARKNET

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på personvern på det dype og mørke nettet. Avslutt med bonusaktiviteten Tenk raskt.

DATABASER PÅ DYPNETTET MOT LØKRUTING PÅ DARKNET (INNLEDNING)

Det dype nettet består av uindekserte sider bak passord og innlogginger, som private e-poster eller bedriftens nettbankportaler. Det mørke nettet er en delmengde av det dype nettet som er bevisst skjult, og som krever spesialiserte nettlesere (som Tor) og onion-nettverk for å få anonym tilgang.

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

Kontrollpunkt 1: Flervalgsutfordring

1. Hva skiller det dype nettet fra overflatenettet?

- A. Sider i dypnettet er ikke indeksert av offentlige søkemotorer
- B. Trafikk på det dype nettet er ulovlig og overvåkes av politiet
- C. Nettsteder på det dype nettet krever spesialiserte nettlesere som Tor for å nås
- D. Sider på det dype nettet laster alltid raskere enn sider på overflatenettet

2. Hvordan får man tilgang til det mørke nettet?

- A. Gjennom spesialiserte nettlesere som bruker onion-rutingnettverk
- B. Ved å konfigurere egne DNS-innstillinger på vanlige rutere
- C. Gjennom private søkekonsoller på overflatenettet som kun er for inviterte
- D. Ved å installere en vanlig nettleserutvidelse for reklameblokkering

3. Hvilken struktur utgjør den største delen av det dype nettet?

- A. Passordbeskyttede brukerdatabaser og private kontoer
- B. Ulovlige svartebørsfora der ulovlige varer omsettes
- C. Ukrypterte protokoller for peer-to-peer-fildeling
- D. Offentlige mellomlagerdatabaser i søkemotorer

4. Hva gjør Onion Routing med nettverkstrafikk?

- A. Den krypterer pakker og ruter dem via flere reléer
- B. Den øker nedlastingshastigheten ved å omgå noder hos internettleverandøren
- C. Den kobler maskinvarens serienumre til IP-oppføringer
- D. Den sletter informasjonskapsler i nettleseren etter hvert klikk

5. Hvilket domenesuffiks brukes utelukkende på Tor-nettverk?

- A. Den kryptografiske toppnivåendelsen .onion
- B. Den tradisjonelle kommersielle .com-endelsen
- C. Web3-endelsen .eth, basert på desentralisert blokkjede
- D. Landskode-teknologiendelsen .ai

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål (sant/usant) 6

6. Det dype nettet og det mørke nettet er det samme nettverkssegmentet.

○ Sant ○ Usant

7 Spørsmål (sant/usant) 7

7. Bedriftens intranettportaler er en del av det dype nettet.

○ Sant ○ Usant

8 Spørsmål (sant/usant) 8

8. Onion-ruting dekrypterer datapakker fullstendig i hver transittnode.

○ Sant ○ Usant

9 Spørsmål (sant/usant) 9

9. Tilgang til det mørke nettet utsetter enheter for høy risiko for skadevare.

○ Sant ○ Usant

10 Spørsmål (sant/usant) 10

10. Vanlige nettsøkemotorer gjennomsøker og indekserer onion-nettsteder.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. Private bankportaler befinner seg på det uindekserte segmentet kalt _____ .
2. Spesialiserte Tor-noder er vert for skjulte tjenester på _____ .
3. Tor-nettsteder bruker det kryptografiske toppdomenet _____ .
4. Kryptert trafikkføring i flere lag, slik Tor gjør det, kalles _____ .
5. Søkemotorer på overflatenettet gjennomsøker offentlig tilgjengelige _____ .
6. Onion-nettverk krypterer klientenes IP-adresser for å opprettholde _____ .

ORDBANK

ANONYMITET DARKNET DATABASE DYPNETT INDEKSERTE SIDER INNGANGSNODE ONION TOR-RUTING

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble sikkerhetsbegreper

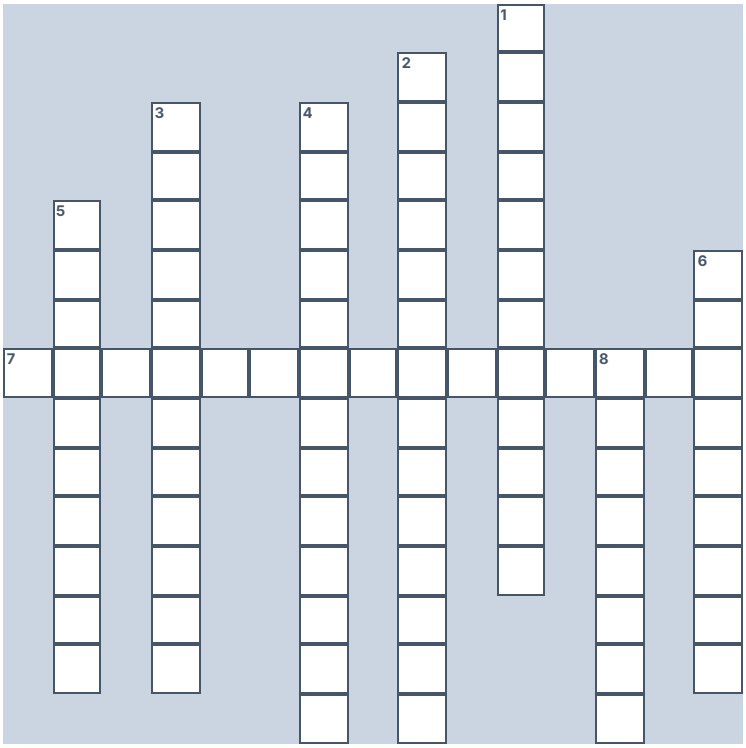
KOBLE DEFINISJONER

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

☐	1. Dypvev-segment	A	Kryptert nettverkssegment som bare er tilgjengelig via spesielle nettlesere.
☐	2. Portal på det mørke nettet	B	Kryptering av data i lag og videresending gjennom tre noder.
☐	3. Onion-endelse	C	Sikker lagring på baksiden som huser uindekserte systemposter.
☐	4. Tor-ruting	D	Kryptografisk toppnivådomenesuffiks som brukes i Tor-nettverk.
☐	5. Indekserte sider	E	Inngangsnoden som brukes for å få tilgang til Tor-nettverket.
☐	6. Brukeranonymitet	F	Innhold på det åpne nettet som er samlet inn og kan søkes i på Google.
☐	7. Privat database	G	Å holde klientenes offentlige IP-adresser skjult for servere.
☐	8. Inngangsport	H	Uindeksert nettinnhold som private innlogginger, e-poster og databaseposter.

Kontrollpunkt 5: Kryssord

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



VANNRETT

7. Overflatenett-innhold som er samlet inn og kan søkes på i Google (15)

LODDRETT

1. Inngangsnoden som brukes for å få tilgang til Tor-nettverket (12)

2. Uindeksert nettinnhold som private påloggінger, e-poster og databaseposter (14)

3. Kryptografisk toppdomenesuffiks som brukes på Tor-nettverk (12)

4. Kryptert nettverkssegment som bare er tilgjengelig via spesielle nettlesere (13)

5. Å holde klientenes offentlige IP-adresser skjult for servere (10)

6. Kryptering av data i lag og videresending gjennom tre noder (9)

8. Sikker lagring i bakkant som rommer uindekserte systemposter (8)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

7 vannrett: Overflatenett-innhold som er samlet inn og kan søkes på i Google (15 bokstaver):

LODDRETT

1 loddrett: Inngangsnoden som brukes for å få tilgang til Tor-nettverket (12 bokstaver):

2 loddrett: Uindeksert nettinnhold som private påloggінger, e-poster og databaseposter (14 bokstaver):

3 loddrett: Kryptografisk toppdomenesuffiks som brukes på Tor-nettverk (12 bokstaver):

4 loddrett: Kryptert nettverkssegment som bare er tilgjengelig via spesielle nettlesere (13 bokstaver):

5 loddrett: Å holde klientenes offentlige IP-adresser skjult for servere (10 bokstaver):

6 loddrett: Kryptering av data i lag og videresending gjennom tre noder (9 bokstaver):

8 loddrett: Sikker lagring i bakkant som rommer uindekserte systemposter (8 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

L A G Q L E P I D O C D I J B

A B Q T N S R N Y W D J Ø G Ø

T U H Æ Z A I D F T Y W P W L

R T E V I B U E N R P M E O U

O I A L N A R K I Ø N Q S N Z

P X N P N T Ø S S S E B L A T

T M O R G A O E B M T J E G O

E J N P A D Ø R C Å T Å D Ø R

N B Y O N Y Æ T N D S F N Q R

K Z M R G S Æ E I E E Ø E C U

R Z I N S F H S I Å G Z N D T

A Q T T N L Z I Æ T M M O Å I

D A E O O T Å D T N E H I U N

Y G T M D Z K E C Ø N D N C G

Ø Q X Å E Q Å R X W T B O I Y

ORDLISTE

DYPNETTSEGMENT DARKNETPORTAL ONIONENDELSE TORRUTING
INDEKSERTESIDER ANONYMITET DATABASE INNGANGSNODE

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. DYPNETTSEGMENT
B. DARKNETPORTAL
C. ONIONENDELSE
D. TORRUTING
E. INDEKSERTESIDER
F. ANONYMITET
G. DATABASE
H. INNGANGSNODE

DEFINISJONER OG TILHØRENDE FELT
1. Å holde klientenes offentlige IP-adresser skjult for servere.
2. Sikker lagring i bakkant som rommer uindekserte systemposter.
3. Kryptering av data i lag og videresending gjennom tre noder.
4. Uindeksert nettinnhold som private påloginger, e-poster og databaseposter.
5. Kryptert nettverkssegment som bare er tilgjengelig via spesielle nettlesere.
6. Kryptografisk toppdomenesuffiks som brukes på Tor-nettverk.
7. Inngangsnoden som brukes for å få tilgang til Tor-nettverket.
8. Overflatenett-innhold som er samlet inn og kan søkes på i Google.

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. MTSGTPYEEDNTEN
2. ENNEOLSIDENO
3. IDENESTSIERREDK
4. ASEABDAT
5. OTARPNLERTDAK
6. NROITTUGR
7. NNAIMTETYO
8. SNAOGEINNDNG

Bonusaktivitet: Tenk raskt

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

1	Grunner til å holde seg unna det mørke nettet			
2	Ting en søkemotor ikke kan finne			
3	Enheter som kan hackes			
4	Lovlige grunner til å bruke Tor			
5	Grunner til å oppdatere programvare			
6	Advarselstegn i en e-post			
7	Ting som selges ulovlig på det mørke nettet			
8	Personer du kan spørre om IT-hjelp			
9	Trygge vaner du kan begynne med i dag			
10	Ting å gjøre etter en datalekkasje			
11	Ting som hører til det dype nettet			
12	Nettsteder du bruker med innlogging			
13	Ord knyttet til anonymitet			
14	Informasjon du aldri bør dele			
15	Ting som ligger «under overflaten»			

Kontrollpunkt 8: Casestudier om cybersikkerhet

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

CASESTUDIE 1: IDENTIFISERING AV DATALEKKASJE



Scenario: En sikkerhetsrevisjon i et selskap avdekker at sensitive kundedatabaseposter omsettes på et onion-marked. Dataene er ikke indeksert på Google.

Diskusjonsspørsmål: Forklar hvilke deler av nettet som er involvert, og hvordan denne lekkasjen skjedde.

CASESTUDIE 2: ANONYMITET MOT RISIKO FOR SKADEVARE



Scenario: En analytiker vil sjekke trusseletterretningsstrømmer på et Tor-nettsted. Vedkommende laster ned Tor-nettleseren og åpner nettstedet.

Diskusjonsspørsmål: Vurder fordelene med anonymitet og skisser trinnene for å begrense skadevare.

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

2	5	22	1	18		1	14	15	14	25	13	9	20	5	20		13	5	4
19	9	11	11	5	18		15	14	9	15	14		18	21	20	9	14	7	

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: Hva er det dype nettet?

Det dype nettet består av alle nettsider som søkemotorer ikke kan indeksere, blant annet nettbank, e-postdatabaser og tidsskrifter bak betalingsmur.

Q2: Hva er dark web?

Det mørke nettet er en liten del av det dype nettet som er bevisst skjult og bare tilgjengelig gjennom spesialiserte nettlesere som bruker onion-nettverk.

Q3: Hvordan indekserer søkemotorer sider?

Søkemotorer kjører automatiserte programmer (spiders) som følger offentlige lenker og indekserer sider som ikke blokkerer gjennomsøking via robotdirektiver.

Q4: Hvorfor regnes nettbank som en del av det dype nettet (deep web)?

Nettbanker ligger bak påloggingsmurer og passord, noe som hindrer offentlige søkemotorer i å indeksere sider med kontoutskrifter.

Q5: Hva er løkruting (Onion Routing) i Tor-nettleseren?

Onion-ruting er en overføringsmetode som krypterer trafikk i lag og sender den gjennom flere reléer for å skjule brukernes IP-adresser.

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

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

Q6: Er det ulovlig å få tilgang til det mørke nettet?

Nei. Å få tilgang til det mørke nettet er lovlig i de fleste land, men det er forbudt å delta i ulovlige markedsplasser eller cyberaktiviteter.

Q7: Hvorfor er nettsteder på det mørke nettet trege å laste inn?

Trafikken rutes og dekrypteres gjennom minst tre globale reléer (inngang, midten, utgang), noe som øker overføringsforsinkelsen.

Q8: Hva betyr domeneendelsen .onion?

Det er et spesialisert toppdomenesuffiks som brukes i Tor-nettverk og peker til kryptografisk genererte adresser i stedet for vanlige DNS-servere.

Q9: Hvilke risikoer er knyttet til lenker på det mørke nettet?

Nettstedene har ingen sikkerhetsskanning, noe som utsetter brukere for høy risiko for skadevareinfeksjon, nettfiskingsskript og transaksjonssvindel.

Q10: Hvem skapte rutingprotokollen i Tor-nettverket?

Teknologien ble opprinnelig utviklet av U.S. Naval Research Laboratory på 1990-tallet for å beskytte myndighetenes kommunikasjon.

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

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

Q1: Hvordan beskytter mellomliggende noder anonymiteten i Tor?

Hver node dekrypterer bare ett lag med rutingdata og lærer bare det forrige og det neste hoppet, aldri både kilde og mål.

Q2: Hvilken rolle har utgangsnoden?

Utgangsnoden dekrypterer det siste krypteringslaget og sender trafikken videre til den offentlige målserveren eller onion-serveren.

Q3: Hva er en Tor-bridges-gateway?

Broer er uoppførte Tor-inngangsreléer som brukes til å omgå blokkeringer fra internettleverandører og sensur i regioner som begrenser tilgang til Tor-nettleseren.

Q4: Hvordan utnytter aktører på det mørke nettet kryptovaluta?

Aktører bruker anonyme kryptovalutaer til å gjennomføre økonomiske handler på mørke markedsplasser og omgår vanlige kontroller av banktransaksjoner.

Q5: Hvorfor klarer ikke vanlige søkemotorer å crawle dype databaser?

Søkerobotene kan ikke skrive inn påloggingsinformasjon, løse sikkerhets-CAPTCHA-er eller kjøre SQL-spørringsskript på baksiden som kreves for å få tilgang til dype databaser.

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

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

Q6: Hva er en katalogserver i Tor-nettverk?

Det er en pålitelig server som vedlikeholder listen over aktive inngangs-, mellom- og utgangsreléer som klienter bruker til å bygge rutingveier.

Q7: Hvordan utfører ondsinnede aktører snuking ved utgangsnoder (exit node sniffing)?

Uautoriserte utgangsnodeoperatører kan avskjære ukryptert HTTP-trafikk når den forlater Tor-nettverket, og stjele brukernavn og informasjonskapsler.

Q8: Hva er forskjellen mellom Tor og I2P?

Tor bruker en sentralisert reléfortegnelse og utgangsnoder for offentlig webtilgang, mens I2P bruker en desentralisert peer-to-peer-struktur for intern vertstjeneste.

Q9: Hvordan sporer politiet markedsplasser på det mørke nettet?

Myndigheter bruker blokkjedeanalyse, lokaliserer fysiske serveroppsett for hosting og gjennomfører lokkeoperasjoner for å identifisere operatørene.

Q10: Hvordan svekker DNS-lekkasje klientens anonymitet?

DNS-lekkasjer oppstår når DNS-forespørsler fra nettleseren sendes direkte via den lokale internettleverandøren i stedet for å rutes gjennom det krypterte Tor-nettverket.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

Det dype nettet er langt større enn det søkbare overflatenettet, siden mesteparten av innholdet ligger bak innlogginger og databaser.

2. SIKKERHETSINNSIKT

Det mørke nettet er en liten, bevisst skjult del av det dype nettet, som nås med verktøy som Tor.

3. SIKKERHETSINNSIKT

Tor-ruting krypterer datapakker tre ganger og skreller av krypteringslag som et løk ved hver relénode.

4. SIKKERHETSINNSIKT

Tor vokste ut av onion routing-prosjektet drevet av U.S. Naval Research Lab, og koden ble utgitt som fri programvare. [1]

5. SIKKERHETSINNSIKT

Onion-adresser er alfanumeriske strenger på 56 tegn som genereres kryptografisk fra offentlige nøkkelpar.

6. SIKKERHETSINNSIKT

Utgangsnoder kan lese trafikk i klartekst, noe som betyr at TLS/HTTPS fortsatt kreves på Tor for sikre øktdata.

7. SIKKERHETSINNSIKT

Intranettsider, skylagringsstasjoner og private databaser utgjør de største datalagringssegmentene på det dype nettet.

8. SIKKERHETSINNSIKT

Spesialiserte søkemotorer som DuckDuckGo driver onion-portaler som gir anonyme søk i Tor-nettverk.

9. SIKKERHETSINNSIKT

Over 2 millioner brukere kobler seg til Tor-nettverket hver dag for å omgå sensur og beholde personvernet i kommunikasjonen.

10. SIKKERHETSINNSIKT

Globale politiaksjoner (som Operation Bayonet) stenger store mørke markedsplasser ved å beslaglegge vertsmaskinvare.

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] Tor Project. (n.d.). Why is it called Tor?

https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?

https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.

https://metrics.torproject.org/userstats-relay-country.html

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

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

[5] 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

Fasit: Kontrollpunkt 1 – flervalg

1 **Søkeindeksering** DYPNETT Riktig svar: A

MERKNAD TIL LÆREREN

Sider på dypnettet ligger bak påloggingsmurer og databaser, noe som hindrer søkerobotter i å gjennomsøke dem.

2 **Tor-tilgang** DARKNET Riktig svar: A

MERKNAD TIL LÆREREN

Det mørke nettet består av skjulte onion-tjenester som bare er tilgjengelige gjennom nettlesere som Tor.

3 **Dype databaser** DATABASER Riktig svar: A

MERKNAD TIL LÆREREN

Passordbeskyttede kontoer og bedriftsoppføringer utgjør det største segmentet av det dype nettet.

4 **Onion-ruting** TOR-NETTVERKET Riktig svar: A

MERKNAD TIL LÆREREN

Onion-ruting krypterer datapakker i lag og videresender dem gjennom flere noder for anonymitet.

5 **Onion-domene** ENDELSE Riktig svar: A

MERKNAD TIL LÆREREN

Det kryptografiske domenesuffikset.onion ruter trafikk internt i Tor uten offentlig DNS.

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Nettsegmenter** STRUKTUR — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Det dype nettet omfatter alle uindekserte sider, mens det mørke nettet er et lite, kryptert onion-delsegment.

7 **Bedriftsintranett** DYPNETT — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Intranettsider ligger bak passordportaler og indekseres ikke, noe som betyr at de hører til det dype nettet.

8 **Lagkryptering** RELÉER — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Onion-reléer dekrypterer bare ett rutinglag for å beskytte brukerens anonymitet, aldri hele pakken.

9 **Eksponering for skadevare** TRUSLER — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Markedsplasser på darknet har ingen sikkerhetsfiltrering og medfører ekstremt høy risiko for skadevareinfeksjon.

10 **Spørsmål 10** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Vanlige søkemotorers crawlere bruker ikke Tor, så de kan ikke nå eller indeksere .onion-nettsteder.

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

H 1. Dypvev-segment	A 2. Portal på det mørke nettet	D 3. Onion-endelse	B 4. Tor-ruting
F 5. Indekserte sider	G 6. Brukeranonymitet	C 7. Privat database	E 8. Inngangsport

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 DYPNETT	2 DARKNET	3 ONION	4 TOR-RUTING
5 INDEKSERTE SIDER	6 ANONYMITET		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 F – ANONYMITET	2 G – DATABASE	3 D – TORRUTING	4 A – DYPNETTSEGMENT
5 B – DARKNETPORTAL	6 C – ONIONENDELSE	7 H – INNGANGSNODE	8 E – INDEKSERTESIDER

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare Dypvev-segment, Portal på det mørke nettet og Onion-endelse med egne ord og gi et eksempel på hvert.

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

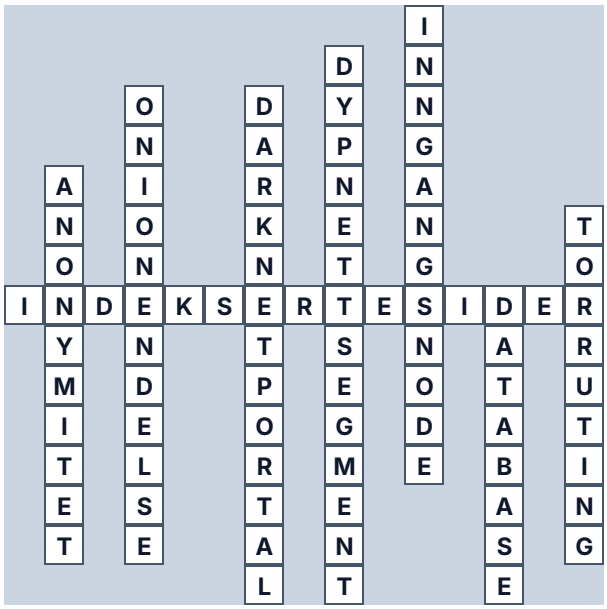
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

7 vannrett: INDEKSERTESIDER Overflatenett-innhold som er samlet inn og kan søkes på i Google (15 bokstaver)

LODDRETT

1 loddrett: INNGANGSNODE Inngangsnoden som brukes for å få tilgang til Tor-nettverket (12 bokstaver)

2 loddrett: DYPNETTSEGMENT Uindeksert nettinnhold som private påloggінger, e-poster og databaseposter (14 bokstaver)

3 loddrett: ONIONENDELSE Kryptografisk toppdomenesuffiks som brukes på Tor-nettverk (12 bokstaver)

4 loddrett: DARKNETPORTAL Kryptert nettverkssegment som bare er tilgjengelig via spesielle nettlesere (13 bokstaver)

5 loddrett: ANONYMITET Å holde klientenes offentlige IP-adresser skjult for servere (10 bokstaver)

6 loddrett: TORRUTING Kryptering av data i lag og videresending gjennom tre noder (9 bokstaver)

8 loddrett: DATABASE Sikker lagring i bakkant som rommer uindekserte systemposter (8 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. MTSGTPYEEDNTEN — **DYPNETTSEGMENT**
2. ENNEOLSIDENO — **ONIONENDELSE**
3. IDENESTSIERREDK — **INDEKSERTESIDER**
4. ASEABDAT — **DATABASE**
5. OTARPNLERTDAK — **DARKNETPORTAL**
6. NROITTUGR — **TORRUTING**
7. NNAIMTETYO — **ANONYMITET**
8. SNAOGEINNDNG — **INNGANGSNODE**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"BEVAR ANONYMITET MED SIKKER ONION RUTING"

Fasit til casestudiene

A Casestudie 1: Identifisering av datalekkasje

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En sikkerhetsrevisjon i et selskap oppdager at sensitive kundedatabaseposter handles på en onion-markedsplass. Dataene er ikke indeksert på Google.
- Anbefalt strategi og løsning: Involverte segmenter: Den private databasen tilhører det dype nettet (deep web: uindeksert, men sikkert). Markedsplassen som handler med de stjålne dataene, ligger på det mørke nettet (dark web: onion-nettverket). Slik skjedde det: Hackerne omgikk serverforsvaret, stjal databasen fra det dype nettet og la den anonymt ut på det mørke nettet for å unnslippe politiets sporing.

B Casestudie 2: Anonymitet mot risiko for skadevare

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En analytiker vil sjekke trusseletterretningsstrømmer på et Tor-nettsted. Vedkommende laster ned Tor-nettleseren og åpner nettstedet.
- Anbefalt strategi og løsning: Fordeler: Tor ruter trafikk gjennom tre noder og maskerer analytikerens IP-adresse i selskapet. Risikoer og tiltak: Lenker på det mørke nettet har ingen omdømmekontroll. Analytikere må kjøre Tor i isolerte virtuelle maskiner (VM-er), deaktivere JavaScript i Tor-innstillingene og unngå å laste ned filer for å beskytte bedriftsnettverket.