

Det mørke nettet:

- En del av internett der du kan opptre anonymt.
- Kun tilgang ved hjelp av en spesiell nettleser (Tor).
- Brukes ofte til kriminalitet, men også til legitime formål.



Sjekk selv: Er dine data til salgs?

I artikkelen forklarer vi også hvordan du kan sjekke din egen status på det mørke nettet. Eventuell lekket informasjon er garantert til salgs et sted der ute. Googles "Rapport om det mørke nettet" gir deg en oversikt, slik at du kan ta dine forholdsregler.

MARKEDET FOR KRIMINELLE:

Slik virker DET MØRKE NETTET

Du må ha en spesiell nettleser for å navigere på det mørke nettet, der det selges våpen, narkotika og kanskje også sensitiv informasjon om akkurat deg til høystbydende. Her får du en guidet tur.



Journalist
Steffen Nielsen

Det har aldri fristet å oppsøke den mørke delen av internett. Jeg hadde riktignok hørt rykter om en del av nettet som også kalles Dark Web, og hadde en vag forestilling om hva det er: En anonym del av internett der det foregår all verdens ulovligheter. Derfor var også lysten til å oppsøke det ganske begrenset. Nysgjerrigheten ble likevel vekket da jeg hørte om Google-verktøyet "Rapport om

det mørke nettet", som gir oversikt over steder på den delen av nettet der ens egne lekkede data kan være til salgs. Slike data lekkes gjerne etter et hackerangrep, og rapporten fra Google viste at både e-postadressen min og andre private opplysninger fantes opptil flere steder der ute i mørket. Det var bekymringsfullt, men det ga også et påskudd til å se nærmere på fenomenet.

Før jeg forteller mer om utflykten til den mørke siden, vil jeg oppklare noen misforståelser som jeg neppe var alene om. Jeg trodde for eksem-

pel at det mørke nettet handlet om vanlige, litt lurvete hjemmesider som ligger spredt rundt på nettet. Altså sider man kunne snuble over hvis man bladde langt nok ned i søkeresultatene til Google. Jeg trodde også at sider på det mørke nettet var tilgjengelige fra vanlige nettlesere, altså Chrome, Edge, Firefox og så videre, så lenge jeg kjente nettadressen. Dessuten trodde jeg at sider på det mørke nettet benyttet adresser som sluttet på .com og .no, som vanlige nettsider.

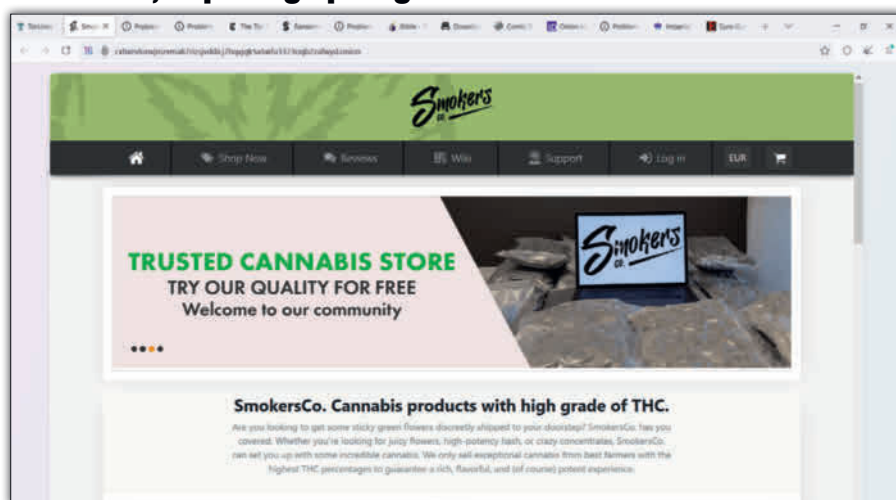
Så begynte jeg å lese meg opp på emnet. Det første jeg oppdaget var at man må bruke en bestemt nettleser som heter Tor, som ved første øyekast ligner en vanlig nettleser. Den kan lastes ned fra det vanlige nettet, før den åpnes og har et adressefelt øverst, som en hvilken som ▶

Hverdagen i en virtuell underverden

Besøket vårt på det mørke nettet sendte oss raskt til en rekke spennende hjemmesider. Denne delen av nettet benyttes først og fremst av lyssky elementer, og det er ikke grenser for hva som er til salgs. Lenkesamlinger tok oss til hundrevis av markedsplasser der våpen ble solgt side om side med leiemordere og hackerangrep.

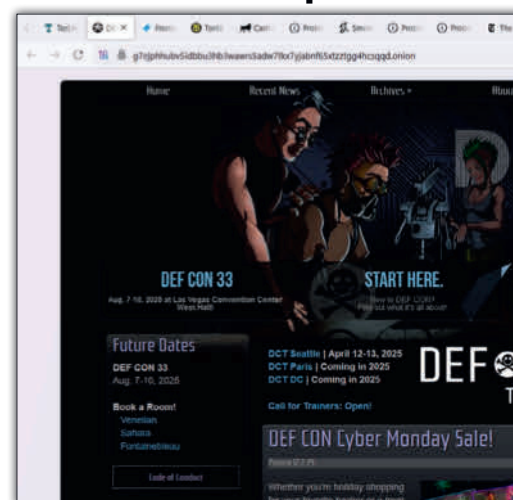
Det er likevel viktig å understreke at det mørke nettet er langt mer enn kriminalitet. Det har sin egen versjon av Wikipedia, sin egen Facebook og mange andre spesialutgaver av kjente hjemmesider og tjenester der man kan kommunisere uten å være redd for å bli identifisert av myndigheter, arbeidsgivere og andre autoriteter.

Narkotika, våpen og sprengstoff



En av de første koblingene vi klikket på, førte oss til denne hjemmesiden med salg av narkotika. Vi fant også raskt tilbud om våpen og sprengstoff ved ganske enkelt å klikke oss videre fra lenke til lenke.

Hackernes markedsplasse



Har du lurt på hvordan hackere kan utvikle skumle nye verktøy uten at myndighetene får nyss om det? En av grunnene er det

- ▶ helst nettleser. Det spesielle med Tor er at den skjuler IP-adressen din for omverdenen. Det skjer ved at den sender henvendelser til internett via en uoversiktlig omvei, slik at ingen vet at det er nettopp du som oppsøker den kontroversielle nettsiden. Det visste jeg fra før, men jeg hadde ikke forstått at Tor i praksis er den eneste inngangen til det mørke nettet.

Jeg visste heller ikke hva mitt neste trekk skulle være da jeg først hadde fått åpnet Tor. Hva skulle jeg skrive i adressefeltet for å komme videre? Igjen måtte jeg ty til det vanlige in-

ternett, der et Google-søk tok meg til forskjellige nettstedet med oversikt over sider på det mørke nettet.

Meterlange koblinger

Ved å se nærmere på adressene til disse sidene, oppdaget jeg en annen overraskende kjensgjerning om det mørke nettet. Lenker til nettsider er nemlig helt annerledes enn dem vi er vant til. Den første delen kan riktignok virke kjent. Adressen til Wikipedias mørke fetter starter for eksempel med bokstavene "Wik", men resten av koblingen er lang og intetsigende.

Her ser du for eksempel adressen til søkemotoren Ahmia: <http://juhanurmihxlp77nkq76byazcldyxcv32hlmov-fu2epvl5ankdibsot4csyd.onion>.

Legg merke til endelsen .onion, altså det engelske ordet for løk. Alle koblinger på denne delen av nettet slutter på .onion, mens resten av adressen hele tiden endres.

Oversiktssider med adresser

Jeg kopierte en kobling fra Google-oversikten til Tor, plasserte den i adressefeltet – og det var full klaff. Adressen var til en side med ytterli-

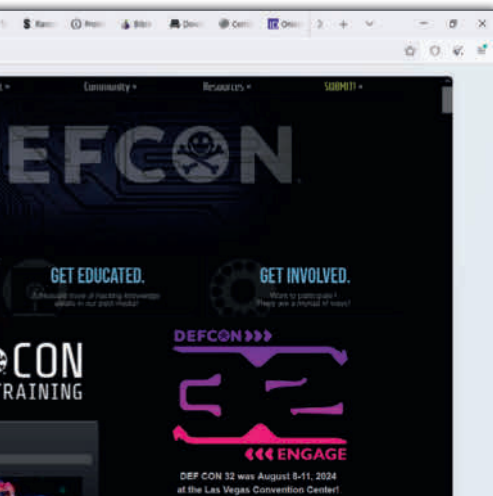
Fortsett på eget ansvar ...

I denne artikkelen har vi gitt et lite innblikk i hvordan det ser ut på det mørke nettet. Det er ikke ulovlig å besøke det og i praksis er det også helt trygt så lenge du kun opptrer som observatør. Derimot kan det være en ekstremt ubehagelig opplevelse hvis du er uoppmerksom og klikker på feil koblinger. Dette er nemlig også et sted der det utveksles barneporno og all verdens sadistiske videoer.

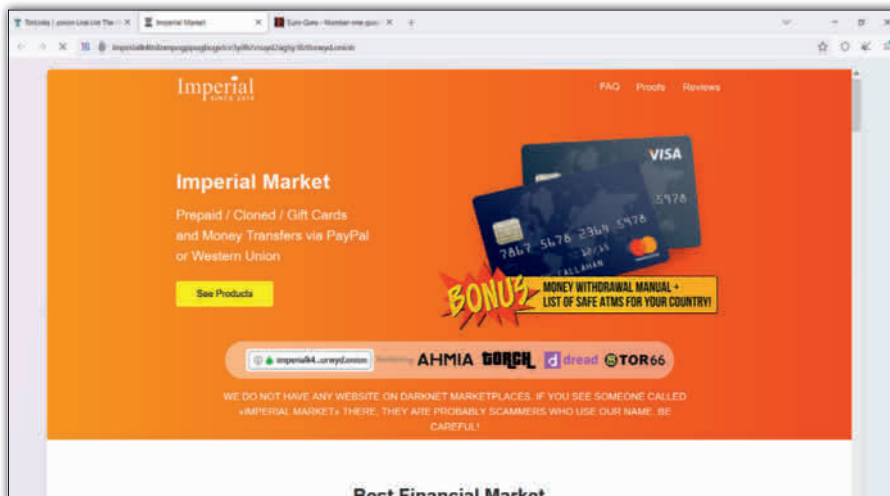
Her er en oversiktsside med lenker fordelt etter emne. Ulovlig innhold er bare noen museklikk unna.



Kredittkort og pass på billigsalg



mørke nettet, som er et sant paradys for svindlere og it-kriminelle. På denne siden kan man få inspirasjon og leie en hacker.



Har betalingsinformasjonen falt i feil hender fordi du for eksempel har vært utsatt for nettfiske eller fordi bankkortet ditt har blitt stjålet? Da er det nesten sikkert at informasjonen er til salgs. Kredittkort, pass og andre ID-dokumenter selges i stor stil.

gere koblinger til sentrale hjemmesider på det mørke nettet. Det viser seg at denne delen av nettet i høy grad er bygd opp rundt disse oversiktssidene. Søkemotorer er derimot mindre viktige. Kanskje du husker hvordan internett så ut på 90-tallet? Det mørke nettet minner på mange måter om datidens sider med lenkesamlinger, før søkemotorer som Google tok over.

Nå kunne jeg altså navigere fra lenkesamlingen og videre ut i mørket – og da ble det alvor. Jeg kom til sider med salg av våpen og narkotika, sider om bombeproduksjon, sider med

salg av kredittkortinformasjon og pass, og sider med hackerverktøy. Her dekkes alle kriminelle behov.

Et demokratisk lys i mørket

Det skal likevel sies at det mørke nettet også har positive sider. Fraværet av sporbarhet gjør det nemlig også til et frirom for opposisjonelle i diktaturer og andre steder der menneskerettigheter har trange kår.

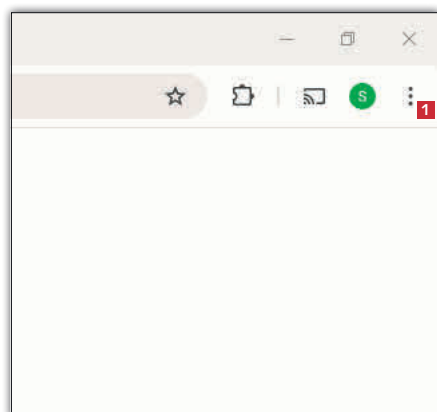
Også i vår del av verden spiller det mørke nettet en viktig rolle for folk som for eksempel vil varsle om maktmisbruk og korrupsjon. Du har sikkert hørt

om Wikileaks. Det mørke nettet inneholder en rekke lignende sider der man kan varsle uten å måtte være redd for represalier.

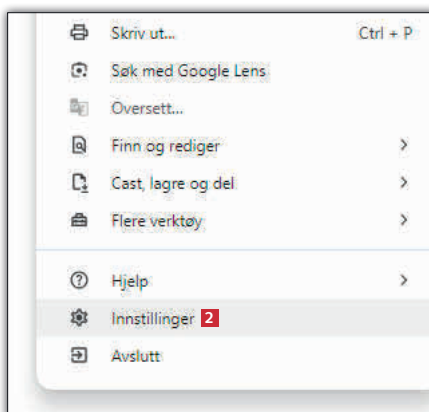
Etter noen timer på det mørke nettet hadde jeg dannet meg et bilde av hva det handler om. Det er ikke på noen måte et sted der man har lyst til å finne egne data lagt ut for salg. Nå har jeg lukket Tor og er tilbake i de trygge rammene til Chrome på den litt lysere delen av nettet. Og jeg vil strekke meg langt for å sikre egne data, slik at jeg ikke blir nok et produkt som er til salgs i mørket.

Hvordan ser du om dine data er til salgs?

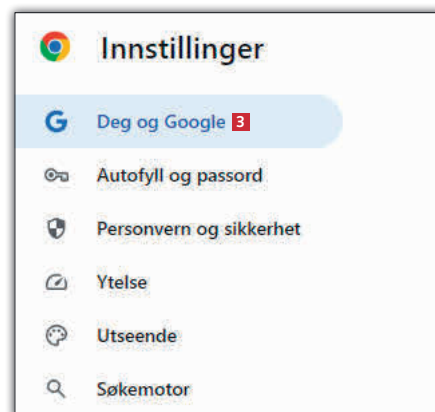
"Rapport om det mørke nett" er et godt Google-verktøy som lar deg finne ut om passordene dine er til salgs på det mørke nett. Er de det, bør du endre dem med det samme.



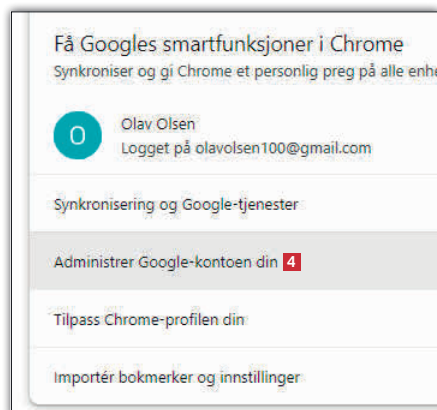
1 I Chrome klikker du først på de tre prikkene **1** øverst til høyre.



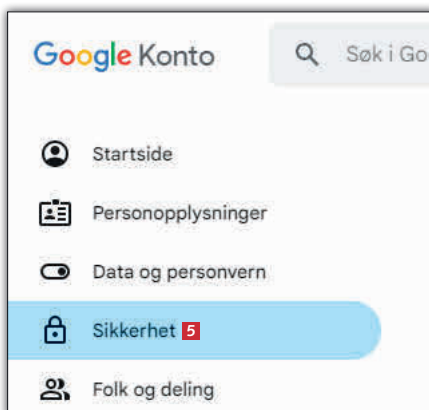
2 Deretter velger du **Innstillinger** **2**.



3 Nå velger du **Deg og Google** **3** til venstre i vinduet.



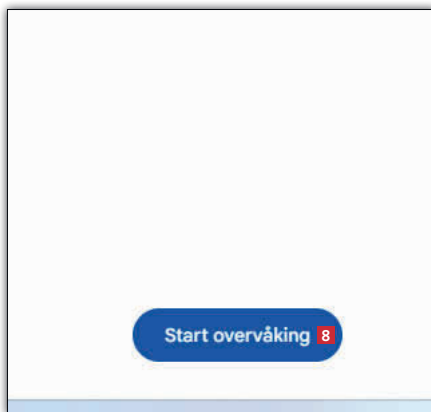
4 Klikk på **Administrer Google-kontoen din** **4**.



5 Til venstre velger du **Sikkerhet** **5**.



6 Bla ned til **Rapport om det mørke nett** **6**, og klikk på **Kom i gang** **7**.



7 Helt nederst i vinduet velger du **Start overvåking** **8**.



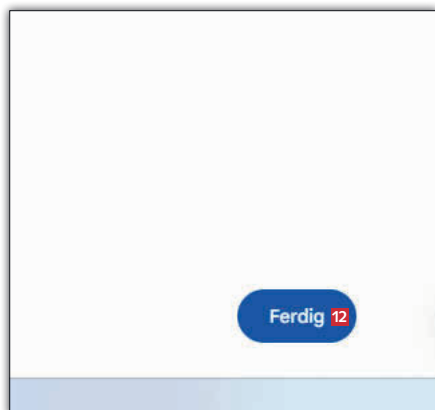
8 Sett hake ved **Velg alle** **9**. Da vil Google overvåke all informasjon som er knyttet til kontoen, for eksempel telefonnummeret ditt.



9 Helt nederst klikker du på **Tillat** **10**.



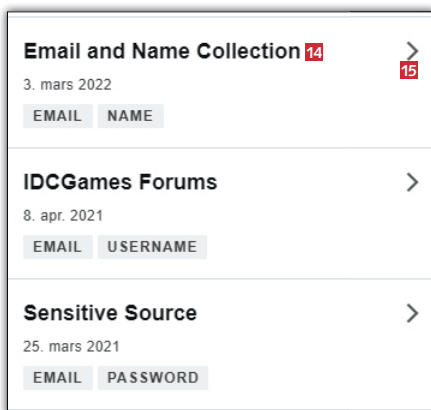
10 Hvis du vil legge til mer informasjon i overvåkingen, gjør du det ved å klikke på plusstegnet **11**.



11 Til slutt klikker du på **Ferdig** **12**.



12 Informasjonen innhentes, og du kan se den ved å klikke på **Se alle resultater** **13**.



13 Nå får du en liste over informasjon på det mørke nettet. Velg et punkt **14**, og klikk på pilen **15**.



14 Dermed får du en oversikt over hvilke av dine private opplysninger som er lekket, for eksempel passord **16**. Passord som vises her bør endres med det samme. Hvis det dukker opp mer informasjon på det mørke nettet, vil Google varsle deg via e-post.