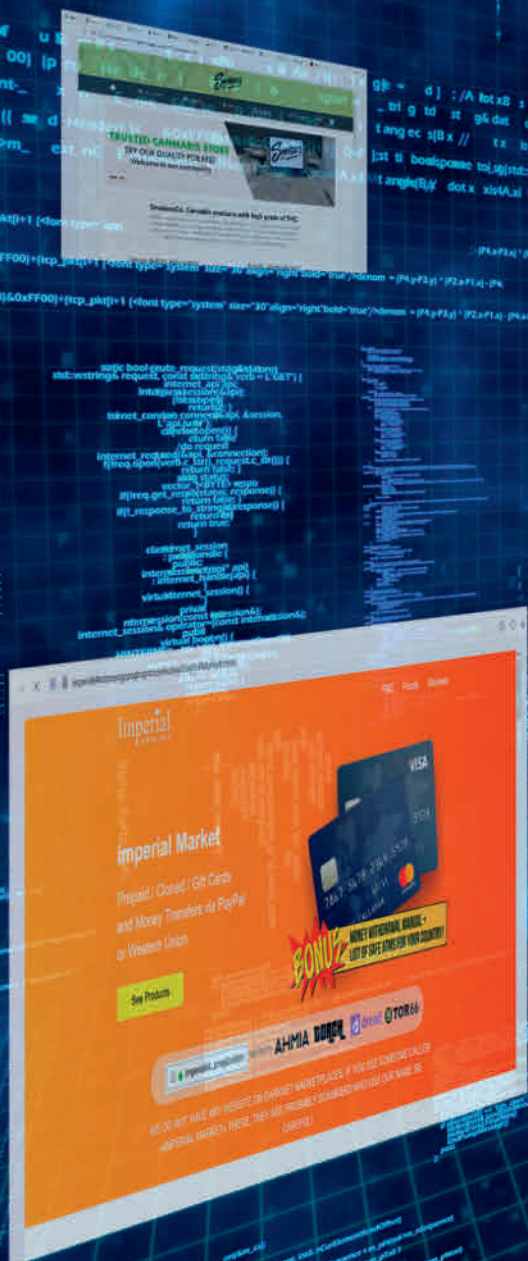


Det mørke internet:

- En del af nettet, hvor du kan optræde helt anonymt.
- Kan kun besøges ved hjælp af en særlig browser (Tor).
- Bruges i stor stil, men ikke udelukkende, af kriminelle.



Tjek selv: Er dine private data til salg?

I denne artikel forklarer vi også, hvordan du kan undersøge din egen rolle på det mørke net. Hvis personlige oplysninger er lækket, er de helt sikkert til salg et sted på mørkenettet. Googles Darkweb-rapport giver dig et overblik, så du kan sikre dig fremadrettet.

FORBRYDERNES HJEMMEBANE:

Sådan fungerer DET MØRKE INTERNET

Kun med en særlig browser kan du besøge det mørke internet, hvor våben, narkotika og måske også dine private oplysninger går til højestbydende. Vi viser dig rundt i mørket.



Journalist
Steffen Nielsen

Et besøg på det mørke internet havde aldrig rigtigt fristet mig. Jeg havde ganske vist hørt rygter om den lukkede del af nettet, også kendt som Dark Web, og havde en vag ide om, hvad det var: En anonym del af internettet, hvor der foregår alskens ulovligheder. Min lyst til aktivt at op-søge det var dog begrænset. Min nysgerrighed blev først pirret, da jeg hørte om Google-værktøjet Darkweb-

rapport, som leverer en oversigt over de steder på mørkenettet, hvor ens oplysninger er til salg. Det er typisk efter hackerangreb, at vores data risikerer at dukke op på det mørke internet. Min rapport hos Google viste således, at min mailadresse og andre private oplysninger florerede op til flere steder derude i mørket. Bekymrende. Men samtidig en anledning til at se nærmere på stedet.

Før jeg fortæller om mit besøg, vil jeg opsummere mine misforståelser om det mørke net. Misforståelser, som jeg næppe er alene om. Jeg tro-

ede fx, at det mørke internet blot var et udtryk for almindelige, skumle hjemmesider spredt rundt om på nettet. Altså hjemmesider, man kunne falde over, hvis man kom langt nok ned i listen over Googles søgeresultater. Jeg troede også, at jeg kunne finde sider fra det mørke internet i min normale Chrome-browser (eller i Firefox og Edge for den sags skyld), hvis blot jeg kendte adressen. Og jeg troede, at en hjemmeside på det mørke internet sluttede med .com og .dk, ligesom helt almindelige hjemmesider.

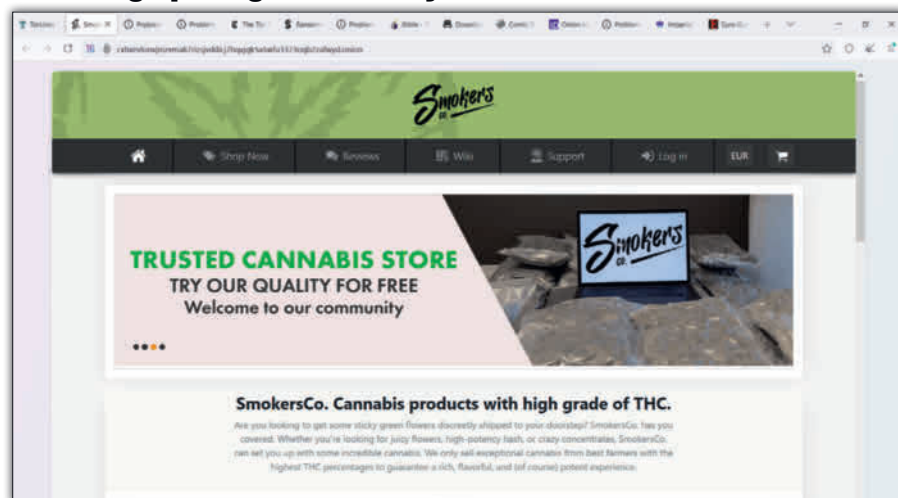
Så begyndte jeg at læse op på emnet. Det første, jeg fandt ud af, var, at man skal bruge en bestemt browser. Browseren hedder Tor, og ligner ved første øjekast Chrome og andre browsere. Den kan hentes fra det almindelige internet, hvorefter den ►

Sådan ser der ud på det mørke internet

Vores besøg på det mørke internet førte os i armene på en stribe spændende hjemmesider. Primært bruges mørkenettet af kriminelle kræfter, og det er ikke småting, som er til salg. Linksamlinger førte os i armene på hundreder af markedspladser, hvor våben blev solgt side om side med lejermordere og hackerangreb.

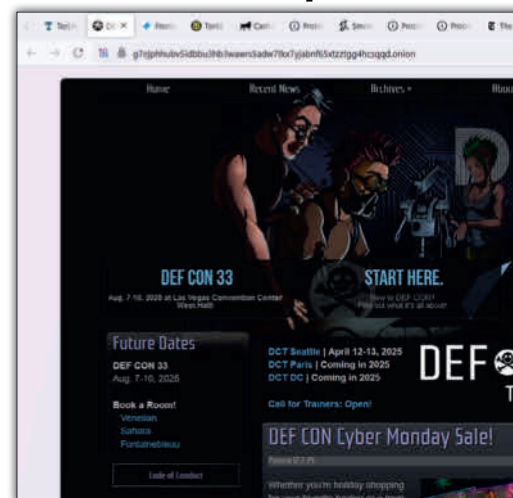
Det mørke internet er dog meget andet end kriminalitet. Mørkenettet har således sin egen Wikipedia, sin egen Facebook og mange andre specialudgaver af kendte hjemmesider, hvor man kan kommunikere uden at man behøver frygte at blive genkendt af myndigheder, arbejdsivere og andre autoriteter.

Våben og sprængstoffer falbydes



Et af de første links, som vi klikkede på ved vores besøg på det mørke net, førte os i favnen på denne hjemmeside med salg af narkotika. Vi fandt også hurtigt tilbud på våben og sprængstoffer ved simpelthen at klikke os videre fra link til link.

Hackernes markedsplads



Tænk du nogensinde over, hvordan hackere kan udvikle nye skumle værktøjer uden politiets indblanding? En af årsagerne

- åbner med et adressefelt øverst, som vi kender det. Tor-browserens særlige rolle er, at den hjælper med at skjule din pc's IP-adresse. Det sker ved, at den sender din henvendelse til internettet via en uoverskuelig omvej, så ingen er i stand til at vide, at det er netop dig, der besøger den kontroversielle hjemmeside. Alt dette vidste jeg i forvejen, men jeg havde ikke forstået, at Tor reelt var den eneste indgang til det mørke internet.

Da jeg nu havde åbnet Tor-browseren, vidste jeg igen ikke, hvad mit næste skridt skulle være? Hvad skulle

jeg skrive i adressefeltet for at komme videre? Igen måtte jeg ty til det almindelige internet, hvor en Google-søgning førte mig til forskellige sider med link-oversigter til hjemmesider på mørkenettet.

Alenlange mystiske links

Ved at næstudere disse links opdagede jeg en anden overraskende sandhed om det mørke net. Hjemmeside-links er helt og aldeles anderledes, end dem vi kender. Den første del af linket er måske nok genkendelig, fx begynder Wikipedias mørkenet-

udgave med bogstaverne "Wik". Den resterende del af linket er imidlertid både meget langt og tilfældigt. Linket til en søgemaskine ved navn Ahmia var således: <http://juhanurmihxlp-77nkq76byazclidyxcv32hlmovfu2ep-vl5ankdibot4csyd.onion>.

Bemærk endelsen .onion, som er det engelske ord for løg. Alle links på mørkenettet ender simpelthen på .onion og skifter i øvrigt hyppigt navn.

Oversigtssider med links

Jeg kopierede nu et link fra Chrome-browseren over i Tor, hvor jeg satte

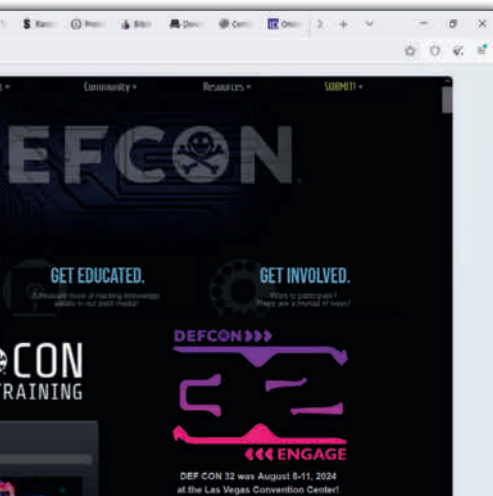
Indgang på eget ansvar

I denne artikel har vi givet dig et lille indblik i, hvordan der ser ud på det mørke internet. Det er fuldt lovligt at besøge det og i virkeligheden også helt sikkert, så længe du kun optræder som observatør. Til gengæld kan det godt være en barsk omgang, hvis du er uopmærksom og klikker på de forkerte links. Mørkenettet er blandt andet også hjemsted for udveksling af børneporno og alskens sadistiske videoer.

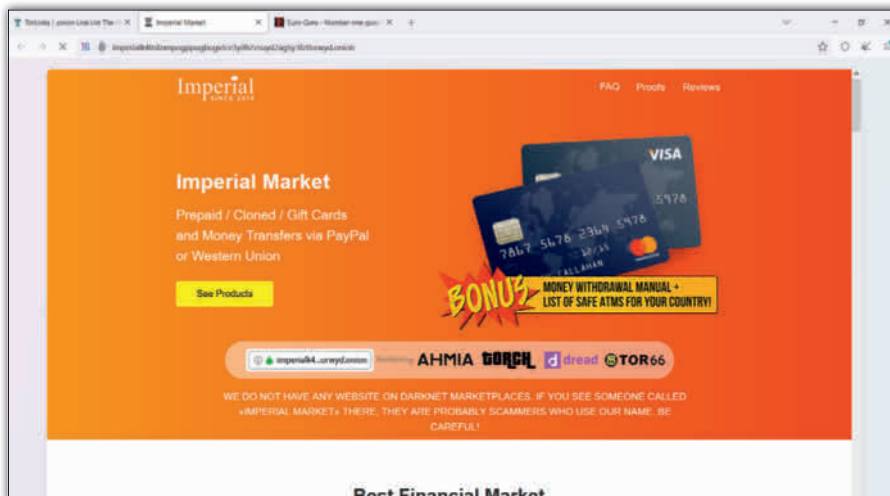
Her er en typisk oversigtsside med links fordelt på emne. Efter få klik støder man på ulovligt indhold.



Kreditkort og pas billigt til salg



er mørkenettet, som er et sandt paradis for svindlere og it-kriminelle. På den viste side kan man få inspiration og hyre en hacker.



Er dine kreditkortoplysninger faldet i de forkerte hænder, fordi du fx har været udsat for phishing eller dit kort er blevet stjålet? Så er der nærmest garanti for, at oplysningerne er til salg på mørkenettet. Kreditkort, pas og andre ID-dokumenter sælges i stor stil.

det ind i adressefeltet. Der var straks gevinst. Linket førte til en side med yderligere links til centrale hjemmeside på mørkenettet. Jeg fandt snart ud af, at mørkenettet i høj grad er bygget op omkring disse oversigtssider, hvorimod søgemaskiner spiller en mindre rolle. Måske husker du nettets allerførste år sidst i 1990'erne? Mørkenettet minder meget om den tids linksamlinger, før søgemaskiner som Googles blev dominerende.

Jeg bevægede mig fra link-oversigterne og videre ud i mørket. Det blev alvor. Jeg besøgte sider med våben-

og narkosalg. Sider om bombeproduktion. Sider med salg af kreditkortoplysninger og pas. Sider med hackerværktøjer. Mørkenettet er en perfekt legeplads for kriminelle.

Demokratisk lys på mørkenettet

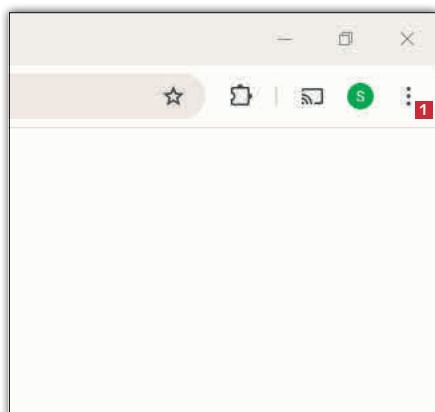
Mørkenettet viste sig dog også at rumme mere opmuntrende sider. Det er således et frirum for demokratiske kræfter i diktaturer og andre steder, hvor menneskerettigheder har trange kår. Også i vores del af verden har mørkenettet en funktion for personer, som vil lække hemmelige oplysning-

ger om fx magtmisbrug. Du har måske hørt om siden Wikileaks. På mørkenettet er der adskillige af dens slags sider, hvor man kan sladre uden at måtte frygte repressalier.

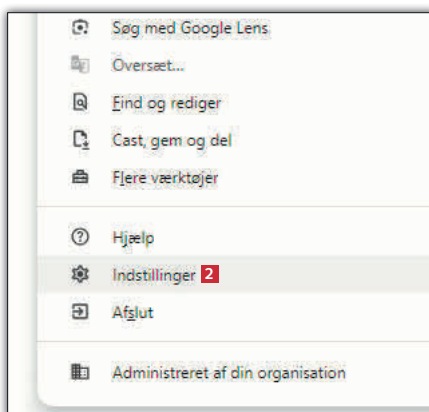
Efter få timer på mørkenettet havde jeg fået et godt indtryk af, hvad det er. Jeg fandt ud af, at det absolut ikke er et sted, hvor man har lyst til at have sine private oplysninger til salg. Jeg har nu lukket Tor-browseren ned, og er tilbage i Chromes trygge rammer på det kendte internet. Fast besluttet på at sikre mine data, så jeg ikke bliver endnu et salgsprodukt i mørket.

Find ud af om dine data sælges på mørkenettet

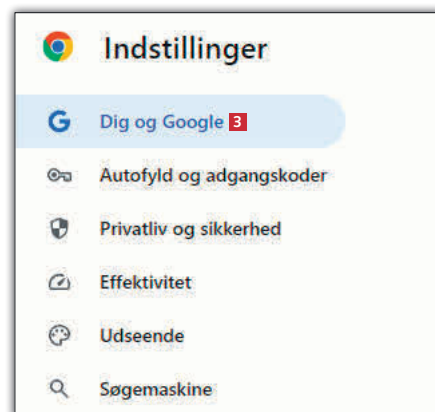
Darkweb-rapport er et fint Google-værktøj. Benyt det til at finde ud af, om dine kodeord er til salg på mørkenettet. Er det tilfældet, skal du snarest skifte dem, så dine konti ikke bliver hacket.



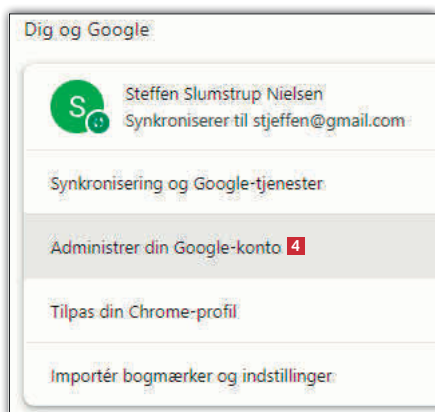
1 I Chrome klikker du først på de tre prikker **1** øverst til højre.



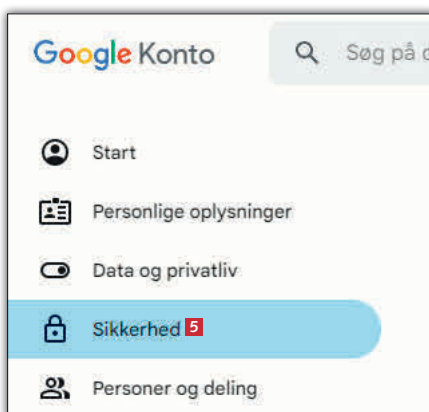
2 Vælg dernæst menupunktet **Indstillinger** **2**.



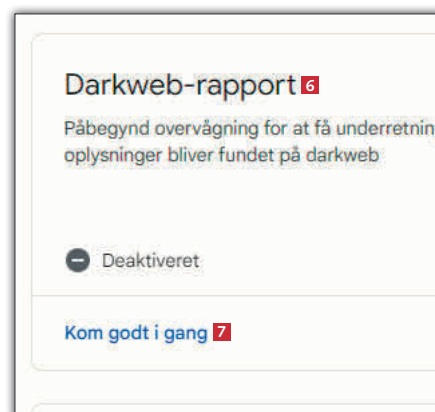
3 Til venstre i vinduet vælger du nu **Dig og Google** **3**.



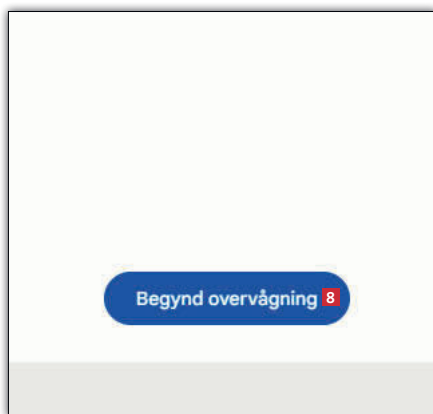
4 Derpå klikker du på **Administrer din Google-konto** **4**.



5 Til venstre vælger du **Sikkerhed** **5**.



6 Rul ned til **Darkweb-rapport** **6**, og klik på **Kom godt i gang** **7**.



7 Helt i bunden af vinduet vælger du **Begynd overvågning** **8**.



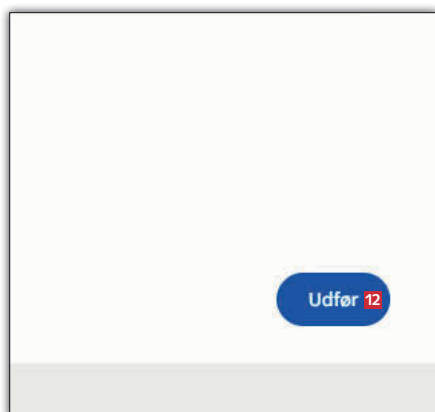
8 Sæt markering ved **Vælg alle** **9**. Så vil Google overvåge alle de oplysninger, som er knyttet til din konto, fx dit telefonnummer.



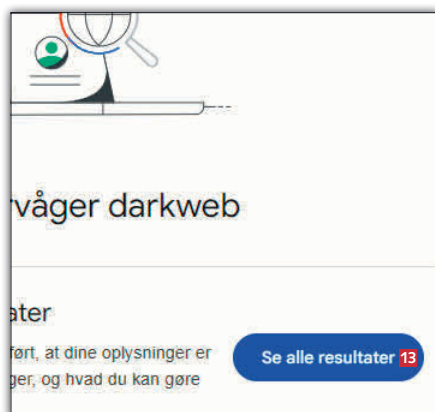
9 Helt i bunden klikker du på **Tillad** **10**.



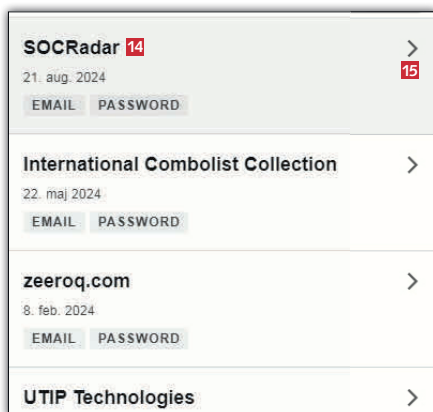
10 Hvis du vil føje flere oplysninger til overvågningen, kan du tilføje dem via plus-tegnene **11**.



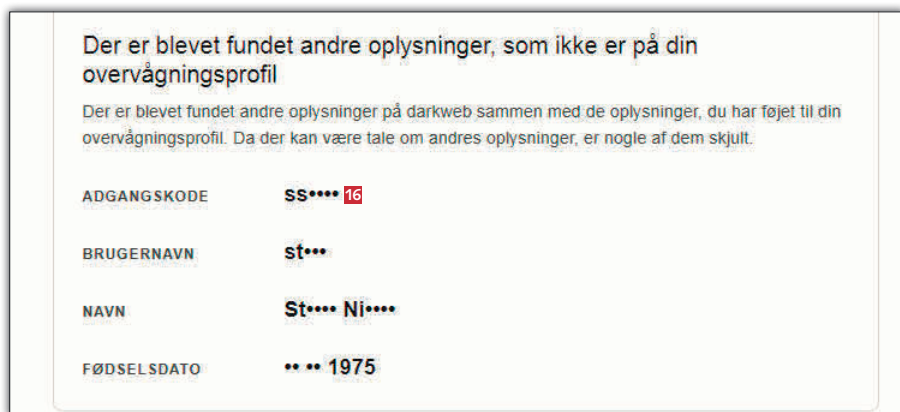
11 Endelig vælger du knappen **Udfør** **12**.



12 Oplysningerne indhentes. Se dem ved at klikke på **Se alle resultater** **13**.



13 En liste over dine oplysninger på mørkenettet vises. Vælg nu et punkt **14**, og klik på pilen **15**.



14 Nu kan du se, hvilke af dine oplysninger, der florerer på mørke-nettet fx adgangskoder **16**. Du bør straks skifte de viste koder hos de tjenester, hvor du har brugt dem. Hvis flere af dine oplysninger dukker op på mørkenettet i fremtiden, vil Google give dig besked på mail.