

Det mörka internet:

- En del av internet där du kan vara helt anonym.
- Kan bara besökas med hjälp av en speciell webbläsare.
- Används flitigt, men inte uteslutande, av kriminella.



Kontrollera: Finns din data till salu? ✓

I den här artikeln förklarar vi även hur du kan undersöka din egen roll på det mörka internet. Om din personliga information har läckt ut finns den till salu någonstans på de ljusskygga delarna av nätet. Googles Darkweb-rapport ger en översikt så du kan skydda dig.

DE KRIMINELLAS HEMMAPLAN

Så fungerar DET MÖRKA INTERNET

Det är bara med en speciell webbläsare som du kan besöka det mörka nätet där vapen, droger och kanske till och med din privata information säljs till högstbjudande. Vi visar dig runt i mörkret.



Journalist
Steffen Nielsen

Att besöka det mörka internet hade aldrig riktigt lockat mig. Jag hade hört rykten om den slutna delen av nätet, som på engelska kallas Dark Web, och hade en vag uppfattning om vad det var: En anonym del av internet där allehanda olagligheter äger rum. Min lust att aktivt söka upp den var däremot inte särskilt stor. Min nyfikenhet väcktes först när jag hörde talas om Google-verktyget

Darkweb Report som ger en översikt över platser på den mörka webben där din information är till salu. Det är vanligtvis efter en hackerattacker som våra uppgifter riskerar att dyka upp där. Min Google-rapport visade att både min mejladress och annan privat information flöt omkring på flera ställen där ute i mörkret. Minst sagt oroväckande, men samtidigt en anledning att ta en närmare titt.

Innan jag berättar om mitt besök vill jag sammanfatta några av mina missuppfattningar om den mörka webben. Missuppfattningar som jag

knappast är ensam om. Jag trodde till exempel att dark web bara var ett begrepp för vanliga, skumma webbplatser som ligger utspridda på internet. Webbplatser som man kunde snubbla över om man kom tillräckligt långt ner i listan över Googles sökresultat. Jag trodde att jag kunde hitta webbplatser från den mörka webben med min vanliga webbläsare Chrome (eller Firefox och Edge för den delen) om jag bara visste adressen. Och jag trodde att en webbplats på den mörka webben slutade med .com och .se, precis som vanliga webbplatser.

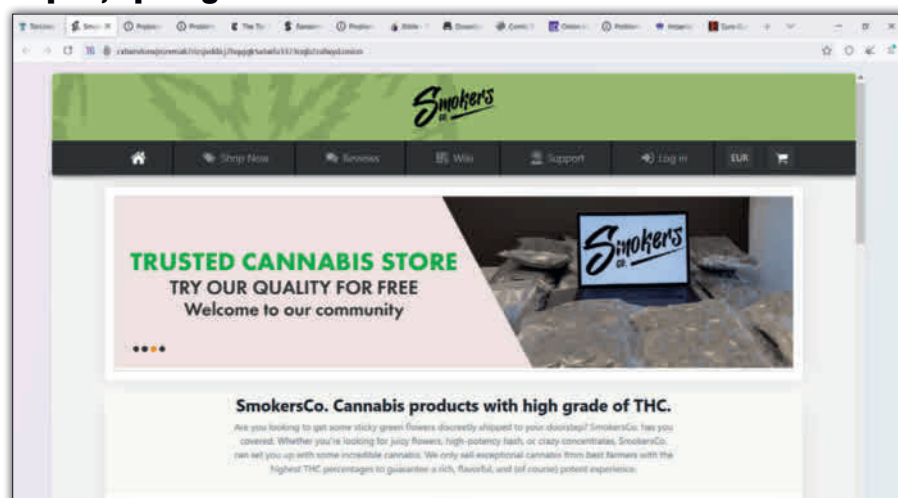
Sedan började jag undersöka. Det första jag insåg var att det behövs en specifik webbläsare. Den heter Tor, och vid första anblicken ser den ut som Chrome och de flesta andra webbläsare. Den kan hämtas från ▶

Så ser det ut på det mörka internet

Vårt besök på den mörka webben ledde oss till ett antal intressanta webbplatser. Den mörka webben används främst av kriminella krafter, och det är inte småsaker som är till salu. Länksamlingar ledde oss in i armarna på hundratals marknadsplatser där vapen såldes sida vid sida med lönnmord och hackerattacker.

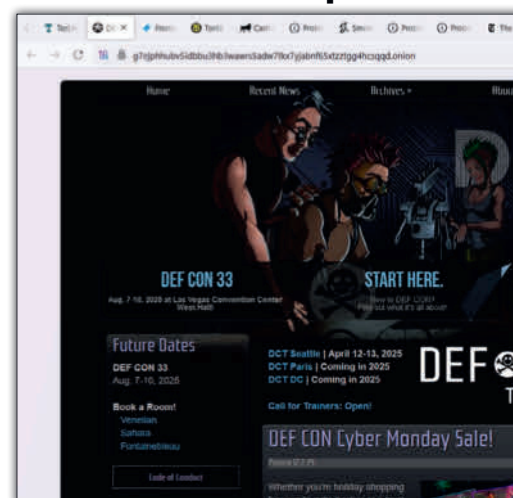
Men den mörka webben är mer än bara brottslighet. Den mörka webben har sitt eget Wikipedia, sitt eget Facebook och många andra specialiserade versioner av välkända webbplatser där man kan kommunicera utan att vara rädd för att bli igenkänd av myndigheter, arbetsgivare och andra auktoriteter.

Vapen, sprängmedel och narkotika



En av de första länkarna vi klickade på under vårt besök på Dark Web ledde oss till den här webbplatsen som säljer droger. Vi hittade också snabbt erbjudanden om vapen och sprängämnen genom att helt enkelt klicka oss vidare från länk till länk.

Hackarnas marknadsplats



Funderar du någonsin på hur hackare kan utveckla nya verktyg utan polisens inblandning? En av anledningarna är den

- det vanliga internet och har ett adressfält högst upp, som vi är vana vid. Tors speciella roll är att den hjälper till att dölja din dators IP-adress. Det gör den genom att skicka dina förfrågningar till internet via en obskyr omväg så att ingen ska kunna veta att det är just du som besöker kontroversiella webbplatser. Allt detta visste jag, men hade inte insett att Tor faktiskt var den enda ingången till Dark Web.

Nu när jag hade öppnat Tor visste jag återigen inte vad mitt nästa steg skulle vara? Vad skulle jag skriva i adressfältet för att komma vidare?

Återigen fick jag gå ut på det vanliga internet, där Google-sökningar ledde mig till sidor med länklister till webbplatser på den mörka webben.

Ändlösa mystiska länkar

Med dessa länkar upptäckte jag en annan överraskande sanning om den mörka webben. Webbplatslänkar är helt annorlunda än de vi känner till. Den första delen av länken kan gå att känna igen, till exempel börjar Wikipedias dark web-version med bokstäverna "Wik". Resten av länken är dock både fruktansvärt lång och

slumpmässig. Länken till sökmotorn som heter Ahmia såg till exempel ut så här: <http://juhanurmihxlp77nkq-76byazcldyxcv32hlmovfu2epvl5ank-dibsot4csyd.onion>.

Notera tillägget .onion, som är det engelska ordet för lök. Alla länkar på dark web slutar helt enkelt på .onion och byter namn ofta.

Översiktssidor med länkar

Jag testade att kopiera en länk från webbläsaren Chrome och klistrade in den i Tors adressfält. Utdelningen var omedelbar. Länken ledde till en

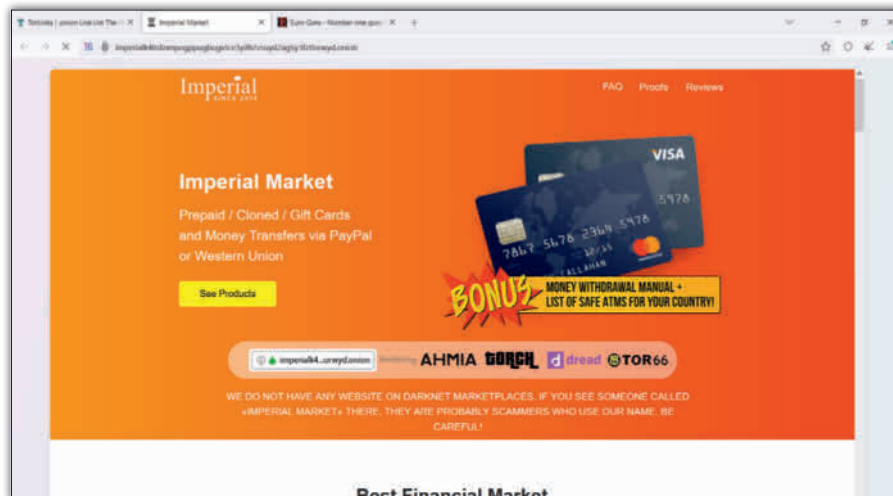
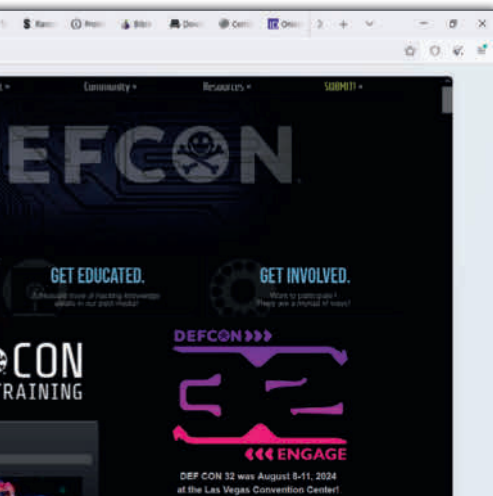
Besök helt på egen ansvar

I den här artikeln har vi gett dig en liten inblick i hur det mörka internet ser ut. Det är helt lagligt att besöka och faktiskt helt säkert så länge du bara agerar som observatör. Om du däremot inte är försiktig och klickar på fel länkar kan det bli en jobbig upplevelse. På det mörka internet förekommer bland annat ett stort utbyte av barnpornografi och många andra former av sadistiska videor.

Här är en typisk översiktssida med länkar som är organiserade efter ämne. Efter några klick kommer du till olagligt innehåll.



Kreditkort och pass till salu billigt



mörka webben, ett veritabelt paradys för bedragare och cyberbrottslingar. Här kan du både få inspiration och anlita en hacker.

Har din kreditkortsinformation hamnat i orätta händer på grund av nätfiske eller att ditt kort har blivit stulet? Då är det nästan garanterat att informationen finns till salu på det mörka internet. Kreditkort, pass och andra ID-handlingar säljs i stor skala.

sida som i sin tur presenterade ännu fler länkar till viktiga webbplatser på det mörka internet. Jag insåg snart att Dark Web till stor del är uppbyggd kring dessa översiktssidor, medan sökmotorer spelar en mindre roll. Du kanske kommer ihåg webbens tidiga år i slutet av 1990-talet? Den mörka webben är mycket lik den tidens länksamlingar, innan sökmotorer som Google blev dominerande.

Jag lämnade länklistorerna och gick in i mörkret. Det blev allvar väldigt snabbt. Jag besökte sajter som sålde vapen och droger. Webbplatser om

bombtillverkning. Webbplatser som sålde kreditkortsuppgifter och pass. Webbplatser med hackerverktyg. Det mörka internet är som den perfekta lekplatsen för kriminella.

Demokratiskt ljus på Dark Web

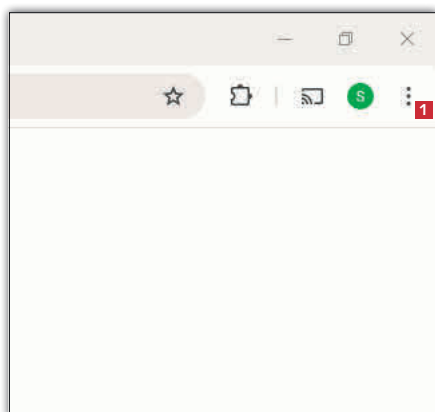
Men det mörka internet visade sig även ha mer uppmuntrande aspekter. Det är en fristad för demokratiska krafter i diktaturer och på platser där mänskliga rättigheter är en bristvara. I vår del av världen ger Dark Web en möjlighet för människor som vill läcka hemlig information om till exempel

maktmissbruk. Du kanske kommer ihåg webbplatsen Wikileaks? På det mörka internet finns det flera sådana sajter där man kan skvallra utan att vara rädd för repressalier.

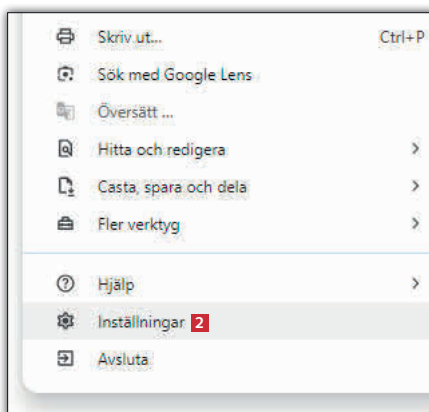
Efter några timmar på Dark Web hade jag en fått god uppfattning om vad det är. Jag insåg att det definitivt inte är en plats där man vill ha sin privata information till salu. Nu har jag stängt av Tor-webbläsaren och återvänt till tryggheten med Chrome på vanliga internet, fast besluten att skydda mina uppgifter så att jag inte blir en produkt till salu på Dark Web.

Ta reda på om du säljs på det mörka internet

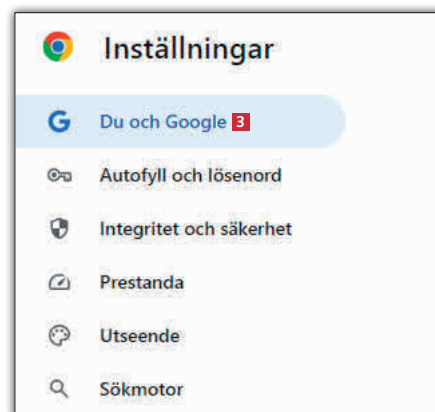
Darkweb-rapporten är ett bra Google-verktyg. Använd det för att ta reda på om dina lösenord är till salu på det mörka internet. Ändra dem i så fall så snart som möjligt innan dina konton blir hackade.



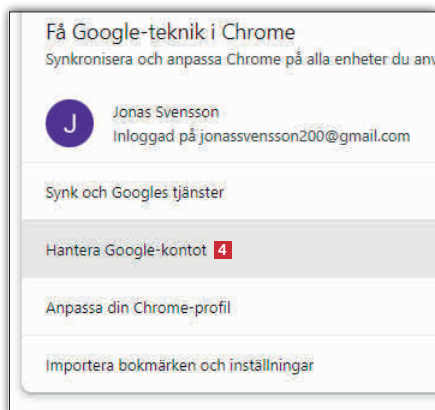
1 I Chrome klickar du först på de tre punkterna **1** uppe till höger.



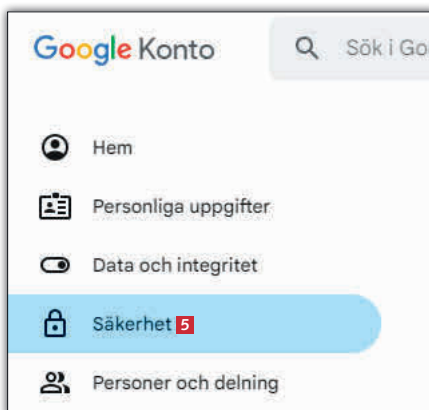
2 Välj sedan alternativet **Inställningar** **2**.



3 På vänster sida väljer du **Du och Google** **3**.



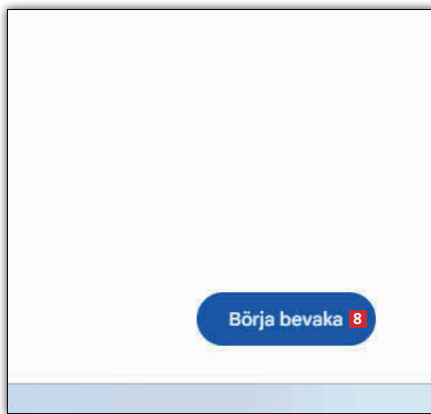
4 Klicka på **Hantera Google-kontot** **4**.



5 Till vänster väljer du **Säkerhet** **5**.



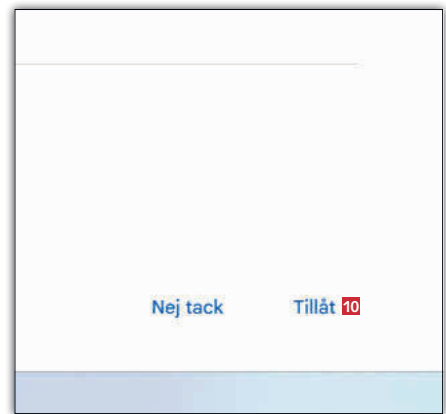
6 Bläddra till **Darknetrapport** **6** och klicka på **Kom igång** **7**.



7 Längst ner i fönstret väljer du **Börja bevaka** **8**.



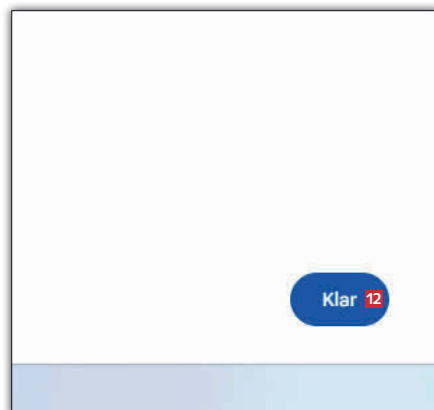
8 Markera alternativet som heter **Markera alla** **9**. Då kommer Google att övervaka all information som är kopplad till ditt konto, till exempel ditt telefonnummer.



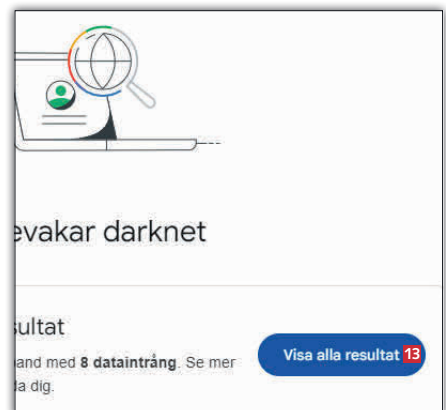
9 Längst ner klickar du på **Tillåt** **10**.



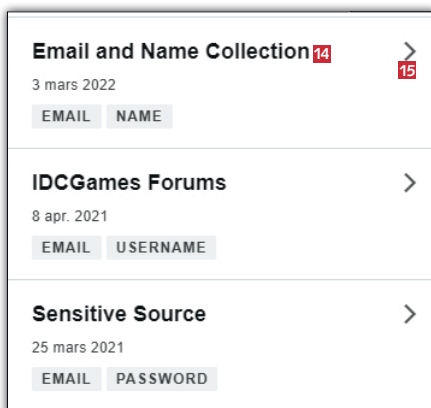
10 Vill du lägga till mer information i övervakningen kan du göra det med hjälp av plustecknen **11**.



11 Slutligen klickar du på knappen **Klar** **12**.



12 Informationen samlas in, och du kan se den genom att klicka på **Visa alla resultat** **13**.



13 En lista över din information på det mörka internet kommer att visas. Välj en punkt **14** och klicka på pilen **15**.



14 Nu kan du se vilken information om dig som finns på Dark Web, till exempel lösenord **16**. Du bör omedelbart ändra de visade lösenorden på de tjänster där du har använt dem. Om mer av din information dyker upp på det mörka internet i framtiden kommer Google att meddela dig via mejl.