

## Tällainen on "Dark web"

- Internetin osa, jossa voi toimia täysin anonyymisti
- Sivuilla vierailuun tarvitaan erityinen selain nimeltä Tor
- Käyttäjissä on paljon rikollisia – muttei pelkästään



## Tarkista itse: Ovatko tietosi kaupan?

Tässä artikkelissa kerromme myös, miten voit tutkia omaa tilan-  
nettasi pimeässä verkossa. Jos  
henkilötietojasi on vuotanut, ne  
ovat varmasti myynnissä dark we-  
bissä. Googlen Dark web -raportti  
antaa sinulle tilannekatsauksen,  
jotta pysyt tästedes turvassa.

RIKOLLISTEN TEMMELYSKENTTÄ:

# Näin toimii PIMEÄ VERKKO

**Pimeässä verkossa voi vierailla vain erityisellä selaimella. Siellä aseita, huumeita ja ehkä jopa yksityiset tietosi myydään häikäilemättä eniten tarjoavalle. Esittelemme nyt sen hämärät nurkat.**



**Toimittaja**  
Steffen Nielsen

Vierailu pimeässä verkossa ei ole koskaan oikein houkutellut minua. Olen toki kuullut huhuja verkon pimeästä puolesta, joka tunnetaan myös nimellä dark web, ja minulla on ollut epämääräinen käsitys siitä, millainen se on: internetin anonyymi kolkka, jossa tapahtuu kaikenlaista laitonta. Siihen tutustuminen ei ole liiemmin houkutellut. Uteliisuuteni heräsi, kun kuulin Googlen

työkalusta Dark web report. Se sisältää pimeän verkon paikat, joissa on myynnissä henkilökohtaisia tietoja. Tyypillisesti tavallisen käyttäjän tiedot ilmestyvät tarjolle pimeään verkkoon hakkerihyökkäyksen seurauksena. Google-raportti paljasti, että sähköpostiosoitteeni ja muut yksityiset tietoni liikkuvat useissa paikoissa pimeässä verkossa. Se oli huolestuttavaa, mutta myös hyvä syy tutkia asiaa tarkemmin.

Ennen raporttia vierailustani haluan kertoa lyhyesti harhakäsityksistäni liittyen pimeään verkkoon.

En liene ainoa, jonka kuva pimeästä verkosta on hieman vääristynyt. Luulin esimerkiksi, että dark web on vain nimitys tavallisille, hämärille verkkosivustoille, joita on hajallaan ympäri internetiä. Sivustoille, joihin voi törmätä, jos selaa Googlen hakutuloksia tarpeeksi pitkälle. Ajattelin myös, että voisin löytää pimeän verkon sivustoja tavallisella Chrome-selaimellani (tai Firefoxilla tai Edgellä), jos vain tietäisin osoitteen. Lisäksi kuvittelin, että pimeän verkon verkkosivujen osoitteet päättyvät .com- ja .fi-tunnuksiin, kuten tavallisten verkkosivujen.

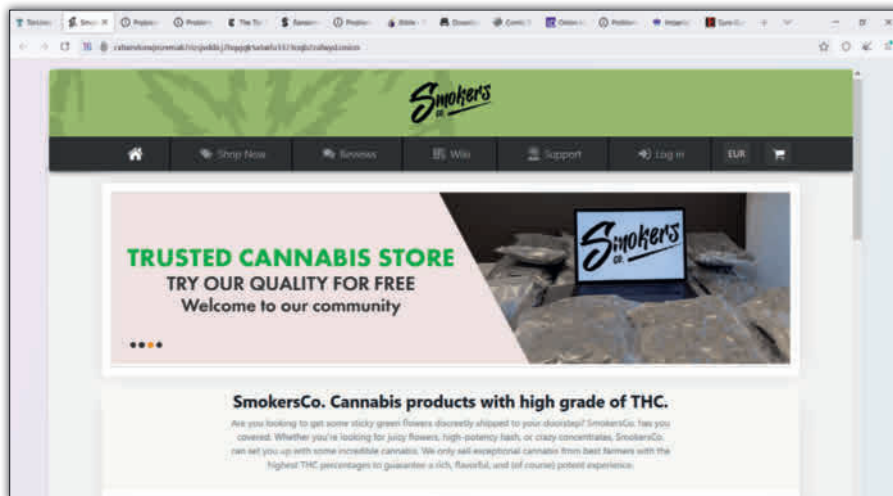
Sitten aloin perehtyä aiheeseen. Ensimmäisenä opin, että tarvitsin tietyn selaimen. Sen nimi on Tor, ja ensisilmäykseltä se muistuttaa Chromea ja muita selaimia. Selaimen voi ladata tavallisesta inter- ▶

# Tältä pimeässä verkossa näyttää

Vierailuni pimeässä verkossa johti minut useiden mielenkiintoisten verkkosivustojen äärelle. Pimeä verkko on ensisijaisesti rikollisten voimien käytössä, eikä siellä käydä mitään nappikauppaa. Linkkikokoelmat johdattivat minut sadoille markkinapaikoille, joilla oli myynnissä kaikkea aseista salamurhiin ja hakkerihyökkäyksiin.

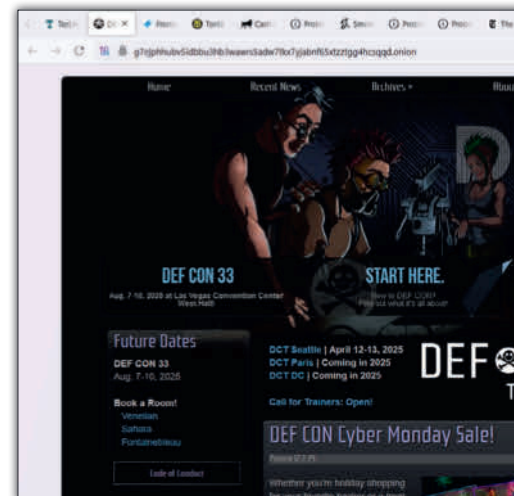
Pimeässä verkossa on kuitenkin tarjolla paljon muutakin kuin rikollisuutta. Siellä on muun muassa oma Wikipedia, oma Facebook ja monia muita tunnettujen verkkosivustojen erikoisversioita, joissa voi kommunikoida anonyymisti ja tyystin viranomaisten, työnantajien ja muiden tahojen ulottumattomissa.

## Tarjolla aseita ja räjähteitä



**Yksi ensimmäisistä linkeistä**, joita napsautin vieraillessani pimeässä verkossa, johti minut tälle huumeita myyvälle verkkosivustolle. Napsauttelemalla linkistä toiseen löysimme nopeasti myös tarjouksia aseista ja räjähteistä.

## Hakkereiden kauppapaikka



**Oletko koskaan miettinyt**, miten hakkerit pystyvät kehittämään uusia häijyjä työkaluja ilman poliisin puuttumista asiaan? Yksi syy

► netistä, ja kun ohjelman avaa, on yläreunassa tuttuun tapaan osoitekenttä. Tor-selaimen erityisyys piilee siinä, että se piilottaa tietokoneesi IP-osoitteen. Se tekee tämän lähettämällä kyselysi internetiin hämärää kiertotietä pitkin, jolloin kukaan ei voi tietää, että se olet juuri sinä, joka vieraillee kiistanalaisella verkkosivustolla. Tämän tiesin jo ennestään, mutta en ollut tajunnut Torin olevan likimain ainoa portti pimeään verkkoon.

Olin nyt saanut Tor-selaimen auki, mutten taaskaan tiennyt, mitä minun pitäisi tehdä seuraavaksi. Mitä minun

pitäisi kirjoittaa osoitepalkkiin päästääkseni eteenpäin? Jälleen kerran jouduin turvautumaan tavalliseen internetiin, jossa Google-haku johti minut verkkosivustoille, joilla oli linkkejä pimeän verkon kotisivuille.

### Salaperäisiä verkko-osoitteita

Tutkiessani näitä verkko-osoitteita huomasin toisenkin yllättävän asian pimeästä verkosta. Verkkosivujen osoitteet näyttivät täysin erilaisilta kuin meille tutut linkit. Linkin alkuosa saattaa olla tunnistettava, esimerkiksi Wikipedian pimeän verkon painos alkaa kirjaimil-

la Wik. Linkin loppuosa on kuitenkin sekä hyvin pitkä että sekava. Esimerkiksi Ahmia-nimisen hakukoneen osoite näytti tältä: <http://juhanurmihxlp77n-kq76byazcldyxcv32hlmovfu2epvl5ankdibst4csyd.onion>.

Huomaa verkkotunnus .onion, joka on englannin kielen sana sipulille. Kaikki pimeän verkon osoitteet päättyvät tunnukseen .onion, mutta muuten niiden nimet vaihtuvat usein.

### Linkkilistoja verkossa

Kopioin sitten linkin Chrome-selaimesta Toriin ja liitin sen osoiteriville.

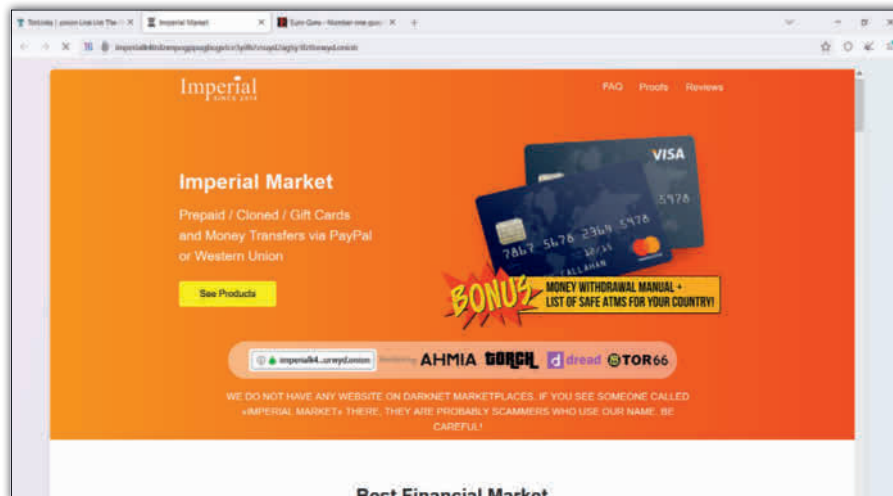
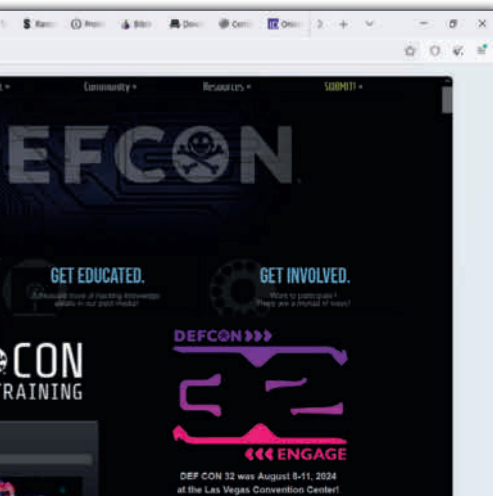
## Sisäänkäynti omalla vastuulla

Tässä artikkelissa raotamme hieman ovea pimeään verkkoon. Siellä vierailu on täysin laillista, ja itse asiassa myös turvallista, kunhan toimit vain tarkkaillijana. Huolimattomasti vääriä linkkejä napsautteleva voi kuitenkin äkkiä joutua ikävään paikkaan. Pimeässä verkossa kun on tarjolla muun muassa lapsipornoa ja kaikenlaisia sadistisia videoita.

**Tässä on tyypillinen linkkilista, jossa linkit on järjestetty aihepiireittäin. Laiton sisältö on vain muutaman napsautuksen päässä.**



## Halvalla passi ja luottokortti



on pimeä verkko, joka on huijareille ja verkkorikollisille todellinen paratiisi. Tältä sivulta sai hakea inspiraatiota ja palkata hakkerin.

**Ovatko luottokorttitietosi joutuneet vääriin käsiin, koska tietojasi on kalasteltu tai korttisi on varastettu? Silloin tietosi ovat lähes varmasti myynnissä pimeässä verkossa. Luottokortteja, passeja ja muita henkilöllisyystodistuksia myydään dark webissä laajamittaisesti.**

Se tuotti heti tulosta. Linkki johti sivulle, jossa oli lisää linkkejä pimeään verkon tärkeimmille verkkosivustoille. Tajusin pian, että pimeä verkko rakentuu pitkälti näiden linkkejä listavien sivustojen ympärille, ja hakukoneiden rooli on pienempi. Muistatko kenties internetin alkuvuodet 1990-luvun lopulla? Pimeä verkko muistuttaa kovasti linkkikokoelmia ajalta ennen Googlen kaltaisten hakukoneiden nousua suursuosioon.

Hyppäsin linkkilistoilta pimeyteen. Tunnelma muuttui heti. Kävin aseita ja huumeita myyvillä sivustoilla. Luot-

tokorttitietoja ja passeja myyvillä sivustoilla. Luin pommien valmistuksesta. Tarjolla oli myös hakkerityökaluja. Pimeä verkko on tosiaan täydellinen leikkikenttä rikollisille.

### Demokratian valo pimeydessä

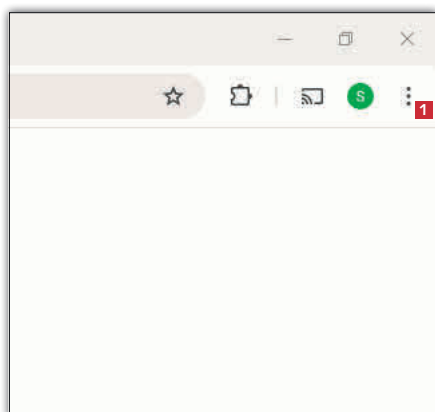
Pimeällä verkolla on kuitenkin rohkaisevampiakin puolia. Se on turvapaikka demokraattisille voimille diktaatuureissa ja muissa paikoissa, joissa ihmisoikeuksia poljetaan. Meidänkin maailmankolkassamme pimeä verkko mahdollistaa salaisten tietojen vuotamisen esimerkiksi vallan vä-

rinkäyttötapaauksissa. Olet ehkä kuulut Wikileaks-sivustosta. Se on vain yksi pimeään verkon monista sivustoista, joilla voi juoruilla ilman pelkoa vastapuolen kostotoimista.

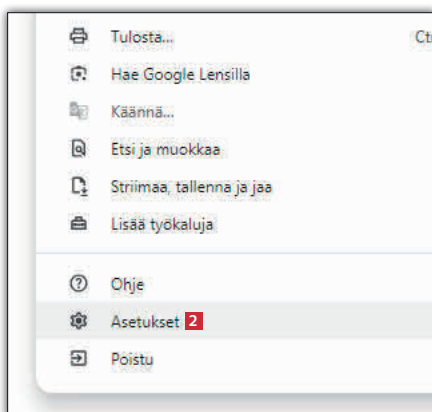
Muutaman tunnin jälkeen olin opinu tarpeeksi pimeästä verkosta. Ymmärsin, että se ei todellakaan ole paikka, jossa kukaan haluaa nähdä tietojan myynnissä. Olen nyt sulkenut Tor-selaimen ja palannut takaisin Chromen suojiin tuttuun internetiin. Kokemuksesta viisastuneena päätin suojata tietoni, ettei minusta tule pimeiden voimien kauppatavaraa.

# Selvitä kaupitellaanko tietojasi pimeässä verkossa

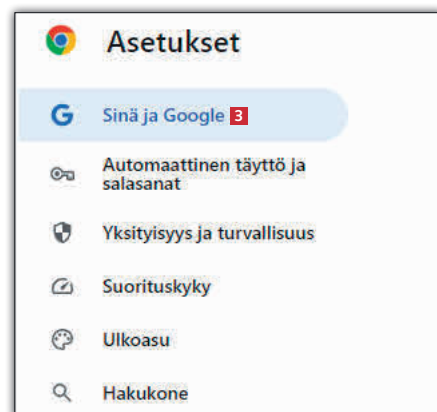
Dark web report on loistava Google-työkalu. Sillä voit selvittää, ovatko salasanasi myynnissä pimeässä verkossa. Mikäli niin on käynyt, vaihda ne mahdollisimman pian, ettei kukaan murtaudu tilillesi.



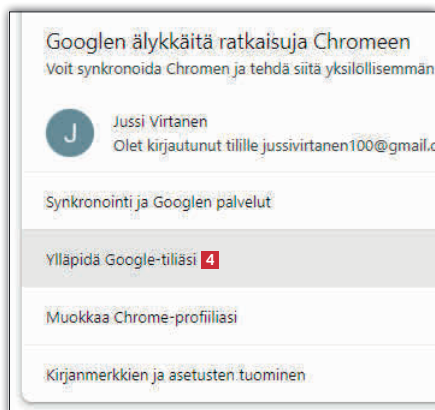
**1** Napsauta aluksi Chrome-selaimen oikeasta yläkulmasta kolmea pistettä **1**.



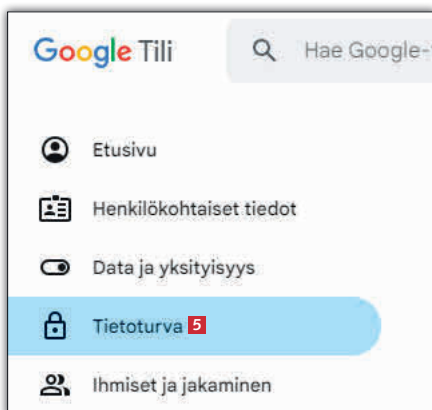
**2** Valitse valikosta kohta **Asetukset** **2**.



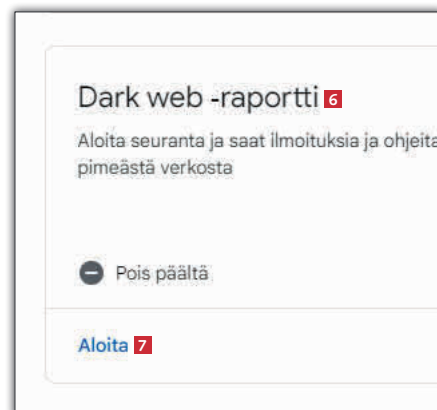
**3** Napsauta seuraavaksi ikkunan vasemmasta reunasta kohtaa **Sinä ja Google** **3**.



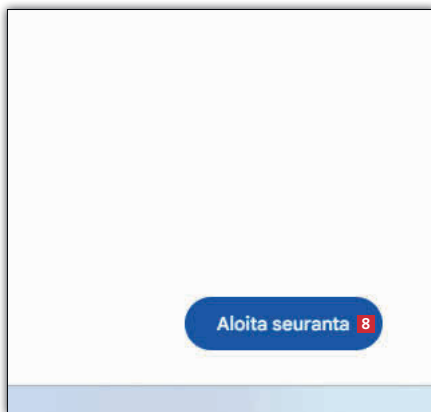
**4** Valitse sitten kohta **Ylläpidä Google-tiliäsi** **4**.



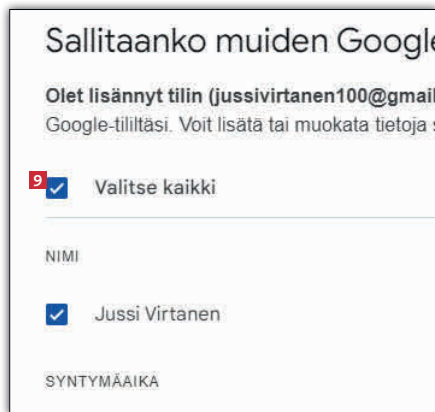
**5** Napsauta vasemmalta kohtaa **Tietoturva** **5**.



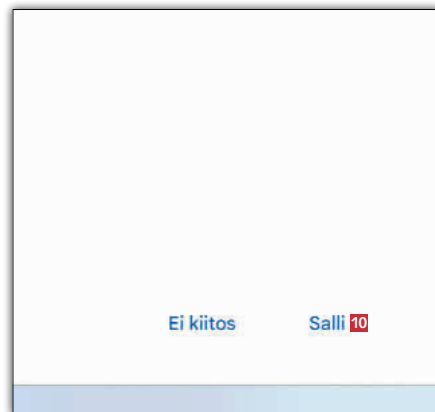
**6** Vieritä sitten sivua alas kohtaan **Dark web -raportti** **6** ja napsauta tekstiä **Aloita** **7**.



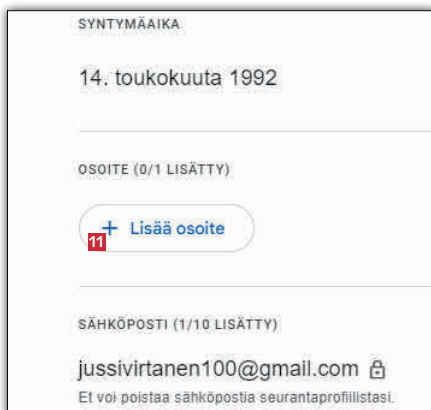
**7** Napsauta ikkunan alareunasta painiketta **Aloita seuranta** **8**.



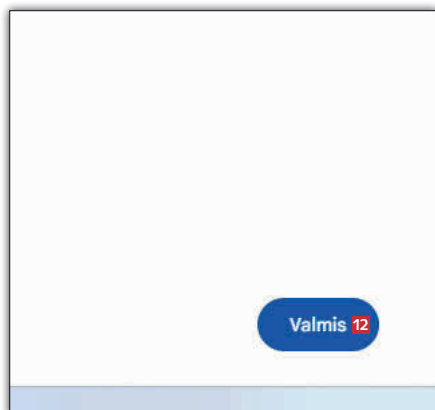
**8** Merkitse sitten kohta **Valitse kaikki** **9**. Näin Google ottaa huomioon kaikki Google-tiliin liitetyt tiedot, kuten puhelinnumeron.



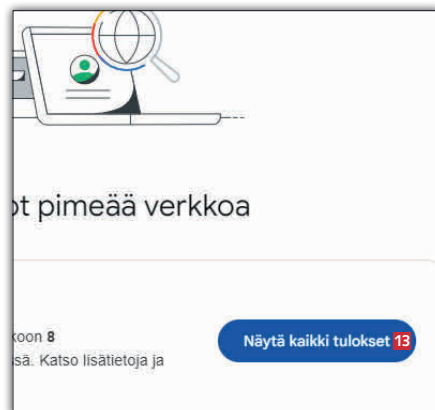
**9** Napsauta sivun alalaidasta kohtaa **Salli** **10**.



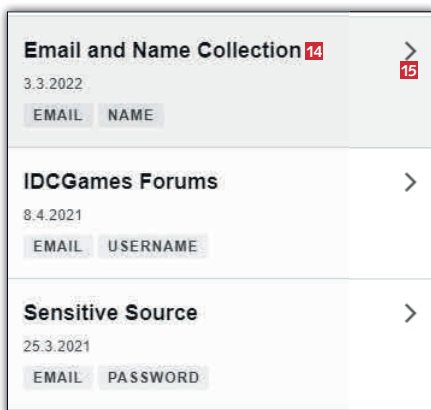
**10** Voit halutessasi lisätä tarkistukseen muita tietoja napsauttamalla plussamerkkiä **11**.



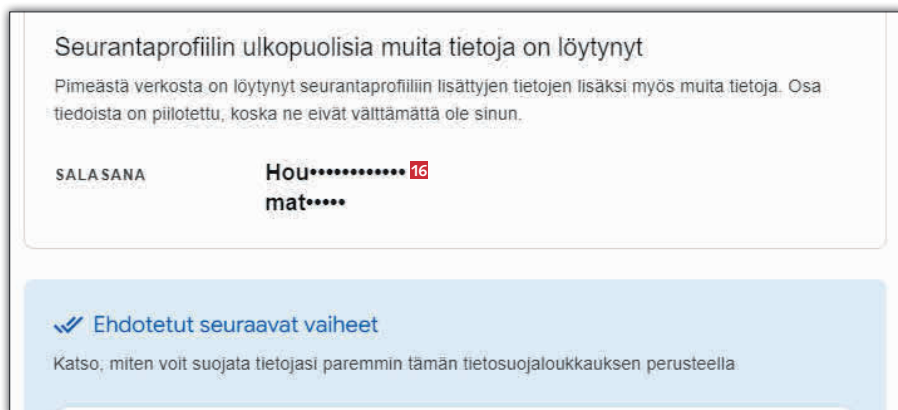
**11** Napsauta lopulta painiketta **Valmis** **12**.



**12** Työkalu hakee tiedot. Tarkista tiedot napsauttamalla painiketta **Näytä kaikki tulokset** **13**.



**13** Näet listan tiedoistasi dark webissä. Valitse jokin kohta **14** ja napsauta nuolta **15**.



**14** Nyt näet, mitkä tiedot ovat tarjolla pimeässä verkossa. Salasanat **16** ovat tyypillisiä tapauksia. Vaihda näkyvissä oleva salasana kaikissa palveluissa, joissa olet sitä käyttänyt. Vastaisuudessa Google ilmoittaa sinulle sähköpostitse, jos tietojasi ilmaantuu pimeään verkkoon.