Identiteettivarkaus

Kotimikron uutiskirje 13.10.2023

**Näin henkilöllisyytesi varastetaan verkossa**

Ennen vanhaan varkaiden piti saada käsiinsä passisi ja lompakkosi, jos he halusivat varastaa henkilöllisyytesi. Nykyään he vain keräävät tietosi sosiaalisesta mediasta ja sähköpostiisi lähetetyillä tietojenkalasteluviesteillä. Se voi tulla sinulle kalliiksi.

Identiteettivarkaudet voivat vaikuttaa sekä talouteesi että henkiseen hyvinvointiisi. Ensinnäkin rikolliset voivat tyhjentää tilisi, jos he saavat haltuunsa tarvittavat tiedot sinusta. Toiseksi yhteyden ottaminen velkojiin ja muihin huijauksen osapuoliin ja heidän vakuuttaminen siitä, ettet itse ole huijauksen takana, on uuvuttava tehtävä.

Internetin käytön yleistymisen myötä huijareilla on runsaasti uusia keinoja varastaa henkilöllisyytesi.

Miten identiteettivarkaudet sitten tapahtuvat verkossa ja mihin pitää kiinnittää erityistä huomiota, jotta niitä ei tapahdu sinulle?

**Mitä identiteettivarkaus tarkoittaa?**

Kun rikolliset varastavat henkilöllisyytesi, he esiintyvät sinuna taloudellisen hyödyn saamiseksi. Tämä voi tapahtua esimerkiksi ottamalla lainoja nimissäsi käyttämällä tietojasi tai hyödyntämällä niitä muihin kohdistuvissa huijauksissa.

Identiteettivarkaudet tapahtuvat yleensä siten, että rikolliset saavat tietoonsa henkilötunnuksen, maksukortin numeron tai valokuvia.

Henkilötietoja käytetään sen jälkeen sinun tai täysin keksityn henkilön esittämiseen esimerkiksi väärennetyssä Facebook-profiilissa.

Tämä voi johtaa siihen, että rikolliset ottavat lainaa nimissäsi tai pääsevät muulla tavoin käsiksi rahoihisi. Tietojasi voidaan käyttää myös muiden ihmisten huijaamiseen, jolloin rikolliset piiloutuvat tietojesi taakse esimerkiksi lähettäessään roskapostia tai tietojenkalasteluviestejä.

**Näin rikolliset varastavat henkilöllisyytesi**

Toisin kuin aiemmin, kun identiteettivarkaiden piti varastaa lompakkosi, henkilötodistuksesi tai maksukorttisi, nykyisessä modernissa digitaalisessa yhteiskunnassamme voit joutua identiteettivarkauden uhriksi, vaikka passisi ja luottokorttisi olisivatkin lukitussa laatikossa.

Nykyään huijarit voivat nimittäin päästä helposti käsiksi yksityisiin tietoihin esimerkiksi tietojenkalastelumenetelmillä, hakkeroimalla tietokoneita ja puhelimia ja sieppaamalla sosiaalisen median tietoja.

Jos et harkitse tarkasti, kuka voi nähdä esimerkiksi kuvia ja tietojasi, kuten syntymäpäiväsi, puhelinnumerosi ja osoitteesi Facebook-profiilissasi, ei-toivotut henkilöt voivat kerätä helposti paljon tietoa sinusta pelkästään sosiaalisen median kanavistasi.

**Monia huijataan yksityisessä verkkokaupassa**

Huijarit käyttävät erityisesti yksityishenkilöiden välistä verkkokauppaa henkilöllisyysvarkauksissa.

Huijarit esiintyvät kiinnostuneina ostajina tai myyjinä ja pyytävät sinua todistamaan henkilöllisyytesi lähettämällä valokuvan virallisesta henkilöllisyystodistuksestasi.

Kuvaa henkilökorteistasi, kuten passistasi tai sairausvakuutuskortistasi, käytetään lainan ottamiseen nimissäsi tai uuden, keskityn henkilön luomiseen.

Keksittyä henkilöä käytetään myöhemmin lisäpetosten tekemiseen.

**Näin vältät identiteettivarkaudet**

Huijarit hyödyntävät usein sosiaalista mediaa ja etenkin Facebook-profiileja, joista he varastavat profiilikuvia ja käyttävät niitä keksittyjen profiilien luomiseen.

Jos kuitenkin teet Facebook-profiilistasi yksityisen, jotta kaikki eivät näe tietojasi, huijareiden on vaikeampi varastaa henkilöllisyyttäsi.

Se tehdään seuraavasti:

1. Avaa Facebook ja napsauta profiilikuvaasi oikeassa yläkulmassa.

2. Valitse Asetukset ja yksityisyys.

3. Napsauta Tietosuojatarkistus ja käy läpi Facebookin yksilölliset ohjeet.

Älä myöskään koskaan jaa kuvia henkilöllisyystodistuksistasi, kuten passista, Kela-kortista tai muista vastaavista esimerkiksi verkkokaupan yhteydessä.

Kaiken kaikkiaan kannattaa olla varovainen arkaluonteisten tietojen jakamisen suhteen ja olla erityisen tarkkana, jos saat sähköpostiviestin, jossa sinua pyydetään syöttämään sosiaaliturvatunnuksesi, salasanasi tai maksutietosi.

Muista, että tietokoneesi on suojattu paremmin tietojenkalasteluyrityksiltä ja muilta digitaalisilta huijauksilta, jos olet asentanut siihen parhaat tietoturvaohjelmat. Ne nappaavat vaaratekijät kiinni, ennen kuin ne vahingoittavat tietokonettasi.

**Mitä teen, jos joudun identiteettivarkauden uhriksi?**

Jos huomaat joutuneesi identiteettivarkauden uhriksi, soita ensin pankkiin ja lukitse maksukorttisi.

Ota sitten yhteyttä poliisiin ja tee rikosilmoitus.

On myös suositeltavaa, että luot etukäteen luottokiellon, jotta rikollisten on vaikeampi ottaa lainaa nimissäsi. Suomessa voit tehdä sen muun muassa osoitteessa asiakastieto.fi.

Ota myös yhteyttä kaikkiin huijauksen osapuoliin. On erityisen tärkeää, että otat yhteyttä mahdollisiin luotonantajiin ja kerrot selkeästi, ettet ole ottanut lainaa itse, vaan että kyseessä on rikos.

On myös hyvä idea pyytää selvitystä siitä, miten sopimus on tehty, jonka voit sitten jakaa poliisille.

**Pitkätkin salasanat murretaan vaivatta: Ota parhaat neuvot onkeesi**

Tuore tutkimus osoitti, että jopa pitkät ja monimutkaiset salasanat voidaan murtaa. Itse asiassa onkin tärkeämpää vaihtaa salasanoja toistuvasti.

Me kaikki tiedämme perinteisen vinkin pitkistä ja monimutkaisista salasanoista.

Joka kerta, kun valitsemme uuden salasanan esimerkiksi verkkosivustolle, meitä muistutetaan siitä, että koodin on oltava vähintään kahdeksan merkkiä pitkä ja koostuttava numeroista, kirjaimista ja erikoismerkeistä. Emme yleensä saa luoda tiliä lainkaan, ellemme valitse vaadittua pitkää ja vaikeaa salasanaa.

Pitkä ja vaikeat salasanat ovat toki järkeviä, vaikka niitä on luonnostaan vaikeampi muistaa kuin yksinkertaisia salasanoja – kuten "12345678", jollaisia jotkut PC-käyttäjät suosivat edelleen.

Kun hakkerit yrittävät brute force -hyökkäystä – joka voidaan kääntää muotoon "yritä kunnes onnistut" - niin pitkä salasana riittää yleensä estämään murtautumisen.

Hakkereilta kuluisi yksinkertaisesti liikaa resursseja, jos he yrittäisivät arvata pitkää salasanaasi. Pitkät salasanat eivät aina auta Brute force -hyökkäys ei kuitenkaan ole ainoa hakkereiden käyttämä menetelmä.

Miljoonia salasanoja murretaan ja väärinkäytetään koko ajan, mutta se johtuu todennäköisemmin kahdesta muusta ilmiöstä: salasanavuodoista ja tietojenkalastelusta.

Näiltä tavoilta suojautuminen ei onnistu, vaikka olisitkin keksinyt hyvän ja pitkän salasanan, jossa on paljon erikoismerkkejä.

**Tutkimus: Lyhyet salasanat murretaan useimmin**

Tietoturvayhtiö Specops on analysoinut yli 800 miljoonaa vuotanutta salasanaa, ja selvä yhteys salasanan pituuteen paljastui. Lyhyet salasanat ovat yleisimpiä vuotaneiden salasanojen kokonaisuudessa.

Kokoelmassa oli kuitenkin yli 30 miljoonaa yli 15 merkin pituista vuotanutta salasanaa. Tämä on selvä merkki siitä, että salasanan pituus ei riitä, jos verkossa haluaa pysyä turvassa.

Vain pienessä osassa salasanojen murtoyrityksistä pitkästä salasanasta on todella hyötyä.

Salasanavuotoja ja tietojenkalastelua torjuessa on kuitenkin tärkeää, **ettet käytä samaa salasanaa useilla sivustoilla** vaan valitset uuden salasanan jokaiselle sivustolle, jolle rekisteröidyt. **Jos salasanasi vuotaa vääriin käsiin, niin hakkerilla on pääsy kaikkialle, jos olet käyttänyt samaa salasanaa.**

Jättiyritykset luopuvat salasanoista. Mieleen voi tulla, että kunpa salasanoja ei enää tarvittaisi, ja vaikuttaakin siltä, että voit vielä joskus hylätä ne. Muun muassa Google ja Microsoft pyrkivät luopumaan salasanoista ja panostamaan sen sijaan muihin tunnistautumismuotoihin, kuten kaksivaiheiseen tunnistautumiseen kirjautumissovelluksella [Google Authenticator](https://kotimikro.fi/tietoturva/pc-suojaus/nain-kaytat-google-authenticatoria) sekä [Microsoft Authenticator](https://www.microsoft.com/fi-fi/security/mobile-authenticator-app).

Jättiyritysten suunnitelmista voi lukea jutusta [Microsoft hylkää salasanat](https://kotimikro.fi/tietoturva/microsoft-hylkaa-salasanat).

- - - - - - - - - - - - - - - - - - - - -- - - - - - - - - - - - - - - - - - - - - - -- -

Kommentteja: Esa Maijala

**Yksi keino** henkilökohtaisen tietoturvan parantamiseksi on säännöllisesti vaihtaa käyttämiään salasanoja. Mutta jos salasanoja käyttäviä palveluita on kymmenittäin kuten minulla on, niin ei tule mieleenkään käydä kerran kuussa vaihtamassa salasanat. Meneehän siinä jo itsekin sekaisin.

**Kaksivaiheinen tunnistautuminen** tuntuu tällä hetkellä parhaalta suojalta hakkereita vastaan. Itse käytän molempia tunnistautumistapoja **Google Authenticator**ia sekä **Microsoft Authenticator**ia tärkeimmissä palveluissa kuten Facebook, Google tili ja kotisivujen hallintapaneeli. Molemmat ovat kännykkään ladattavia sovelluksia ja Android puhelimiin ne löytyvät Google Play:sta. Tunnistautuminen näiden avulla toimii siten, että kun tietokoneella on antanut käyttäjätunnuksen ja salasanan, pyytää tietokone sen jälkeen 6 numeroista koodia, joka annetaan kännykällä.

Kaksivaiheiseen tunnistautumiseen tietokoneella ei välttämättä tarvita näitä sovelluksia, vaan riittää, kun on kännykällä ko. palvelussa esim. Facebookissa, jolloin saa ilmoituksen sisäänkirjausyrityksestä ja vastaamalla siihen ”Kyllä” pääsee sisään.

Kun on kerran näin kirjautunut sisään, kyseiselle tietokoneelle tallentuu eväste, joka päästää sisään ilman kaksivaiheisuutta eli ko. työasema on luotettava. Sen sijaan hakkerin työasema ei ole, joten hakkerilta pääsy tyssää siihen, vaikka hän tietäisi käyttäjätunnuksen ja salasanan.

Mikäli ajat tietokoneella puhdistusohjelmaa, joka poistaa evästeet, on jälleen suoritettava kaksivaiheinen tunnistautuminen.

**Kolmas tapa** on käyttää salasanojen hallintaohjelmaa esim.LastPass, joka on maksullinen ohjelma. Siitä löytyy myös ilmainen lisäosa, jonka voi liittää Chrome selaimeen. Minulla ei ole tästä kokemusta. Voi olla käteväkin.

Huomattavaa parannusta tietoturvaan kännykällä antavat sormijälki- ja kasvotunnistautumistavat. Mutta olisivat jo kokonaan uuden jutun aiheita.

**Onko käyttäjätunnuksesi ja mahdollisesti salasanasi** vuotanut hakkereille esim. tietovuotapahtuman yhteydessä? Asian voi tarkistaa helposti ja nopeasti [Have I Been Pwned](https://haveibeenpwned.com/) -sivustolla. Kirjoita email address -kenttään sähköpostiosoitteesi, niin hetken kuluttua saat tiedon, onko sähköpostiosoitteesi vuotanut jonkin tietomurron yhteydessä. Mikäli salasanaa ei ole vaihdettu vuosiin, on se nyt syytä tehdä.

Eipä muuta kuin turvallisempaa huomista kaikille!

* Esa -