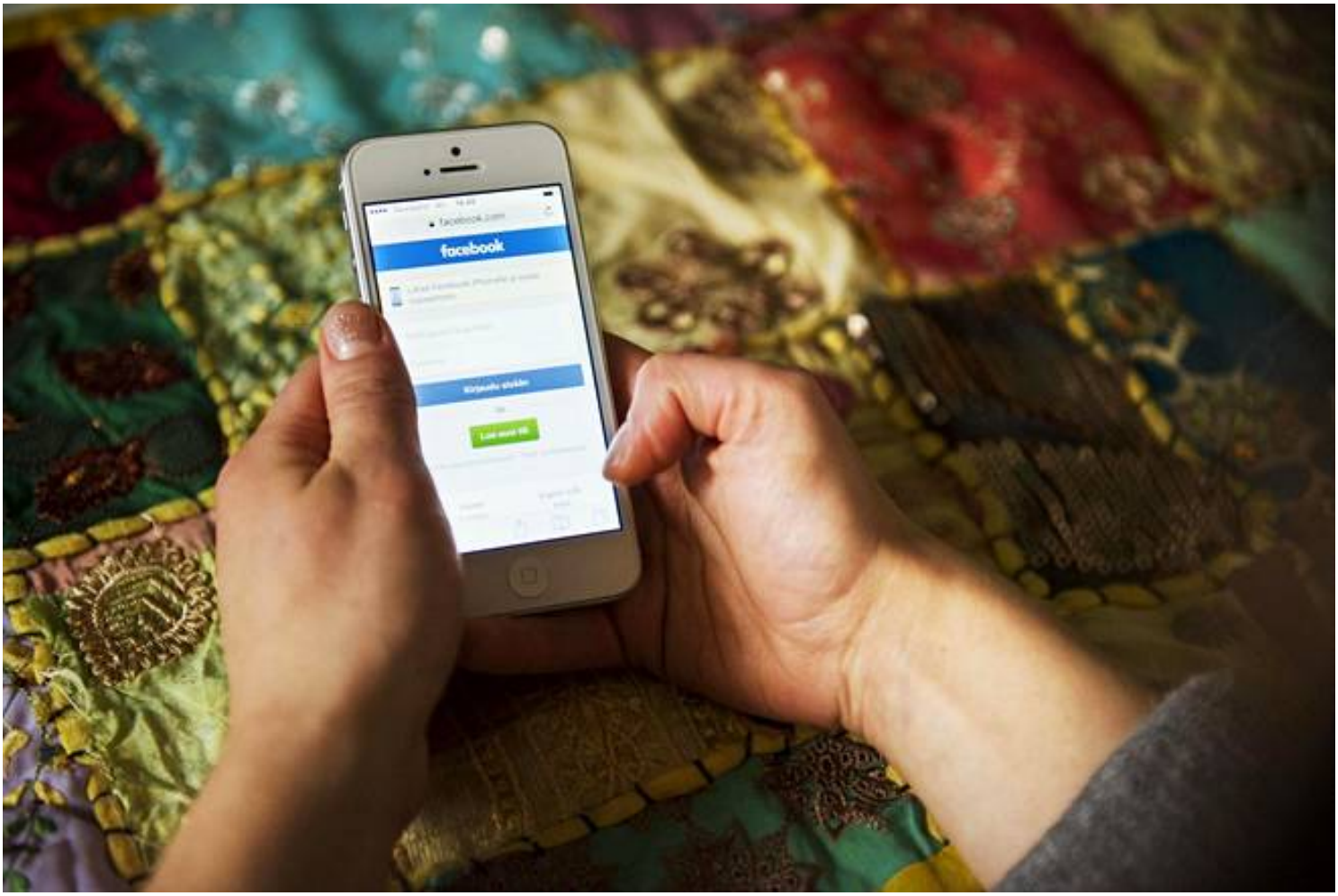
HYVINVOINTI: Useampi kuin joka toinen kärsii väsymyksestä – Kokosimme yhteen kaiken, mitä opimme unesta vuonna 2017

Kotimaa

Moni suomalainen käyttää salasanoja huolettomasti – Näin pärjäät vain kahdella salasanalla

Joka viides suomalainen käyttää vain yhtä tai kahta salasanaa, paljastaa tuore kyselytutkimus. Tietoturva-asiantuntija neuvoo muistamaan kaksi vahvaa salasanaa ja jättämään muut tietokoneen huoleksi.



Sähköisiin palveluihin, kuten Facebookiin, vaaditaan sähköpostiosoite, joka mahdollistaa palvelun salasanan nollaamisen. (KUVA: EMILIA KANGASLUOMA)

Toni Lehtinen HS

JOKA viides suomalainen käyttää vain yhtä tai kahta salasanaa sähköisissä palveluissa. Tieto selviää Bilendin tekemästä online-kyselytutkimuksesta, johon vastasi yhtiön paneelissa tuhat 18–75-vuotiasta suomalaista. Henkilötunnistautuminen verkossa -tutkimuksen tilasi teleoperaattorien yhteinen

Mobiilivarmenne-hanke.

Vain muutaman salasanan käyttäminen kasvattaa huomattavasti tietoturvariskiä.

”Sellaiset ihmiset, joilla on käytössä ainoastaan muutama salasana, eivät yleensä pidä kauhean tarkkaa kirjaa siitä, mihin he ovat kirjautumassa”, tietoturvallisuusjohtaja **Erka Koivunen** F-Securesta kertoo.

Huoleton salasanojen käyttö altistaa salasanankalasteluille.

”Kun henkilöllä ei ole ihan tarkkaa tietoa, mihin palveluun hän on kirjautumassa, kaikki salasanakyselyt, jopa kalastelut, vaikuttavat ihan järkeviltä”, Koivunen sanoo.

Kyselytutkimuksen mukaan valtaosalla suomalaisista on käytössään yli kolme salasanaa. 16 prosenttia vastanneista kertoi, että heillä on käytössään yli kymmenen salasanaa.

TÄMÄN vuoden aikana on paljastunut useita tietomurtoja, joiden seurauksena yli miljardin ihmisen salasanoja on päätynyt hakkereiden käsiin. Tietoturvayhtiö Splashdata selvitti viiden miljoonan hakkerien käsiin joutuneen salasanan perusteella yleisimmät käytetyt salasanat.

Yleisin salasana on 123456.

Verkkopalveluita käyttävällä kuluttajalla voi olla hallittavanaan kymmeniä salasanoja. Kuinka niistä kannattaa pitää huolta, niin ettei käytä samoja salasanoja jokaiseen palveluun?

Erka Koivunen neuvoo jakamaan salasanat tärkeysjärjestykseen niiden käytön mukaan.

”Jotkut käyttäjätunnukset ovat tärkeämpiä kuin toiset, ja niiden suojaamiseksi kannattaa käyttää vähän enemmän vaivaa. Hierarkian rakentamalla täytyy muistaa ainoastaan kaksi salasanaa, joiden pitää olla laadukkaita”, Koivunen painottaa.

YKSI tärkeä salasana on se, jota käytetään työnantajan ohjelmiin ja sähköpostiin. Aiemmin suositeltiin monimutkaisia salasanoja, mutta nyt suosituksena on vähintään 16 merkkiä pitkä salasana.

”Työnantajan salaisuuksien suojaamiseksi on syytä käyttää täysin eri salasanaa kuin yksityisasioissa”, Koivunen korostaa.

Seuraavaksi tärkein on niin sanotun master-sähköpostitilin salasana. Tämä tarkoittaa sitä yksityistä sähköpostia, jota käytetään muihin sähköisiin palveluihin kirjautumiseen. Sähköisiin palveluihin, kuten Facebookiin, vaaditaan sähköpostiosoite, joka mahdollistaa palvelun salasanan nollaamisen.

”Näin ollen palautussähköpostiosoitetta pitää suojata voimallisimmin. Jos se ja sen salasana päätyvät vääriin käsiin, henkilön kaikki kymmenet sähköiset palvelut voidaan kaapata”, Koivunen sanoo.

Kolmas salasanakategoria ovat erilaisten sähköisten verkkokauppojen ja palveluiden salasanat. Niihin Koivunen neuvoo käyttämään tietokoneen salasanageneraattoria tai erillistä salasanamanageriohjelmaa.

”Helpoimmalla pääsee, jos antaa tietokoneen sekä generoida salasanat että muistaa ne. Tietokoneen

voi antaa myös syöttää salasanat automaattisesti palveluihin. Nämä salasanat voi vaikka unohtaa tietoisena siitä, että ne pystyy tarvittaessa palauttamaan.”

Kannattaako salasanamanageriohjelmaan tallentaa tärkeitä salasanoja, eli master-sähköpostitilin tai työpostin salasanoja?

”Minä olen tallentanut sensitiivisiä salasanoja manageriohjelmaan, mutta olen tallentanut ne hieman muutettuina. Jos puhelimeni varastettaisiin, automaattinen salasanan syöttäminen ei antaisi täysin oikeaa salasanaa”, Koivunen neuvoo.

HENKILÖTUNNISTAUTUMINEN verkossa -tutkimuksen mukaan yli kolmasosa suomalaisista kirjoittaa salasanojaan edelleen muistiin. Muistiin kirjoittamista harrastavat varsinkin yli 65-vuotiaat. Koivunen ei kuitenkaan pidä muistiin kirjoittamista suurena riskinä.

”Jos salasanat ovat kotona piirongin laatikossa tai lompakossa mukana, niiden päätyminen käytettäväksi tietomurrossa on hyvin pieni [riski]. On huomattavasti epätodennäköisempää joutua asuntomurron tai ryöstön kohteeksi kuin tietomurtoyrityksen kohteeksi”, Koivunen sanoo.

Henkilötunnistautuminen verkossa -tutkimuksen mukaan suurin osa suomalaisista käyttää vahvaa sähköistä tunnistautumista viikoittain. Tämä tarkoittaa siis joko pankkien tarjoamaa Tupas-tunnistautumista tai operaattorien tarjoamaa Mobiilivarmennetta. Tupas-tunnukset on käytössä neljällä miljoonalla suomalaisella, ja Mobiilivarmennetta käyttää yli 200 000 suomalaista.

Verkkopankkitunnukset eli Tupas-varmenteet ovat yleisin vahva tunnistautumiskeino. (KUVA: SAMI KERO / HS)

Aiemmin Suomeen kaivattiin yhtenäistä sähköistä henkilökorttijärjestelmää, jollainen on käytössä esimerkiksi Virossa.

”Näyttää siltä, että Suomen hajautettu järjestelmä voi olla turvallisempi kuin yhtenäinen järjestelmä.

Viron järjestelmä jouduttiin sulkemaan, koska salausavaimet osoittautuvat viallisiksi. Sen seurauksensa koko järjestelmä oli alhaalla, kunnes avaimet oli saatu vaihdettua”, johtaja **Ari Hakala** Teliasta kertoo.

BIOMETRISISTÄ tunnisteista, kuten sormenjäljestä, kasvoista ja silmästä, on toivottu korvaajaa tulevaisuudessa avainlukujen ja salasanojen näpyttelylle. Passeissa on jo sormenjälki ja kasvot tunnisteena, ja uusimmat älypuhelimet käyttävät myös kasvojentunnistusta.

Hakala kehottaa suhtautumaan varauksella biometristen tunnisteiden käyttöön ennen kuin alalle saadaan tarvittavaa lainsäädäntöä ja säännöstöä. Hakkeroinnin riski on nykyään niin suuri, että tunnistautumispalveluita pitää miettiä vahingon minimoinnin kannalta.

”Biometristen tunnisteiden ympärillä on hypeä, jossa ei ole pohdittu tarpeeksi sen riskejä. Jos numeropohjaiset tiedot joutuvat vääriin käsiin, ne voidaan poistaa ja vaihtaa helposti tietojärjestelmistä”, Hakala sanoo.

Biometriset tunnisteet ovat kuitenkin ainutkertaisia, joten tietoturvayhtiöt joutuvat pohtimaan mitä tapahtuu, jos biometriset tunnisteet, kuten silmän iiriksen tiedot, hakkeroidaan ja ne leviävät maailmalle.

”Suljetaanko käyttäjä ikuisiksi ajoiksi pois järjestelmästä vai vaihdetaanko silmä”, Hakala kysyy.

Fakta
Hyvä salasana on 15–20 merkkiä pitkä

■ Tietoturvan suurimmat vaatimukset koskevat henkilökohtaisia sähköisiä palveluita, kuten pankki-, Kela- ja terveyspalveluita. Niihin kirjautumiseen voi käyttää joko Tupas-tunnuksia tai Mobiilivarmennetta. Tupas toimii tunnuksen, salasanan sekä vaihtuvan avainluvun yhdistelmällä. Mobiilivarmenne on matkapuhelimen sim-kortissa ja se tarvitsee puhelimen lisäksi salasanan.

■ Tärkeimpien salasanojen eli työsähköpostin ja yksityisen sähköpostitilin salasanojen pitää erota toisistaan. Niiden pitää olla mahdollisimman pitkät ja vaikeasti keksittävissä olevat.

■ Hyvä salasana on 15–20 merkkiä pitkä, ja se sisältää pieniä ja isoja kirjaimia, numeroita sekä erikoismerkkejä. Salasanassa kannattaa käyttää suomen kieltä.

■ Salasanan voi koostaa vaikka lauseesta, josta salasanaan käyttää vain sanojen ensimmäiset kirjaimet, joita on vähintään 15! Edellinen lause olisi salasanana: Svkvljskvsekjov15!

■ Jos kirjoitat salasanat muistiin paperille, älä kirjoita palvelun nimeä salasanan viereen.

■ Useat tietoturvayritykset tarjoavat salasanamanageriohjelmia, joihin voi tallentaa käyttämiään salasanoja. Ohjelmia ovat esimerkiksi F-securen Key sekä Last Pass ja Dashlane.