4.

SUOJAA VIRTUAALISET ARVOTAVARASI

Aivan kuten pidät huolta kotisi arvotavaroista, sinun tulee huolehtia myös virtuaalisesti tallentamistasi tiedoista, olipa kyse sitten pankkitiedoista, skannatusta passista, osoitteesta tai puhelinnumerosta. Kannattaa miettiä, mihin tallennat arvokkaimmat henkilötietosi, ja kuinka voit suojata niitä.

Pikapuhdistus on hyvä kikka, jos haluat tehdä muutamia nopeita parannuksia vaikkapa kahvitauolla. Etsi tiettyjä tietoja, jotka löytyvät sähköpostistasi tai muilta tileiltäsi, ja poista ne. Ota kohteeksi esimerkiksi skannattu henkilötodistus, pankkitiedot tai sairausvakuutustiedot. Jos tarvitset tietoja myöhemmin, voit aina ladata tiedot tai tulostaa ne ennen kuin poistat ne sähköpostitililtäsi.

Syväpuhdistus on perusteellisempi tapa, ja se on hyvä tehdä kerran vuodessa. Arkistoi kaikki tiedot sähköpostistasi tai sosiaalisen median tileiltä, lataa tiedot tietokoneellesi ja poista tilien sisältö aloittaaksesi uudelleen puhtaalta pöydältä.

Vinkki: Älä pelkästään poista. Tyhjennä myös roskakori ja tilapäiset tiedostot!

Voit itse valita, haluatko varmuuskopioida arkistot ja asiakirjat pilveen vai tallentaa ne ulkoiselle kiintolevylle tai USB-tikulle. Huolimatta siitä, miten tallennat, varmista, ettet menetä tietoja ja että salasanasi on vahva ja muistissasi.

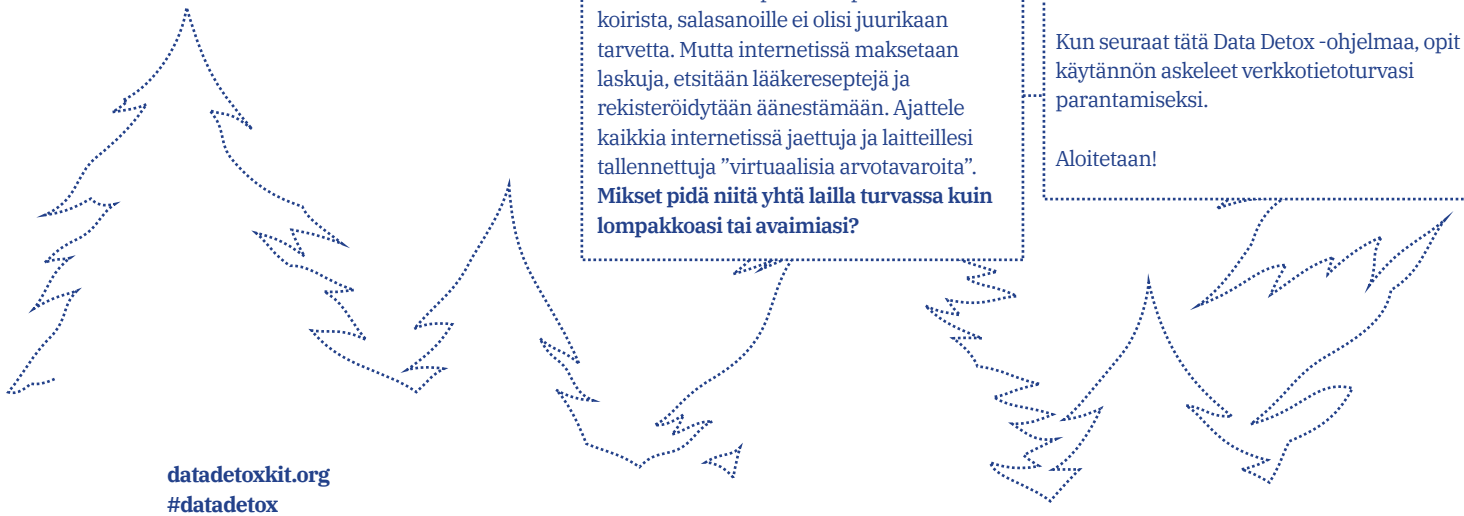
5.

VÄLITÄ VIESTIÄ!

On ehkä helppo unohtaa, että verkkoa kutsutaan ”verkoksi” syystä. **Olemme kaikki yhteydessä verkkoon** eri verkostojen kautta, ei vain ystävinä sosiaalisessa mediassa, vaan myös sähköpostitiliemme yhteystietojen ja verkossa jakamiemme valokuvien kautta. Kun suojaat tilisi, vahvistat salasanasi ja puhdistat tietosi, sinun lisäksesi myös muut hyötyvät. Toimintasi auttaa pitämään jokaisen, johon olet yhteydessä, hieman paremmassa turvassa.

Kun puhdistat sähköpostiasi ja sosiaalisen median tilejäsi, mieti, mitä muuta voisit poistaa ystäviäsi tai työtovereitasi auttaaksesi. Sisaresi pankkitiedot, toimistosi avainkoodi tai poikasi passin kopio ovat vain muutamia esimerkkejä tiedoista, joiden päätyminen vääriin käsiin voi aiheuttaa melkoista päänsärkyä.

Välitä viestiä! Digitaalisen turvallisuuden lisääminen on helppoa muutamaa perusvaihetta noudattamalla. Jaa tämä Data Detox ystävien, perheen tai työtovereidesi kanssa, jotta myös he voivat muuttaa tapojaan järkevällä tavalla.



DATA DETOX KIT

VAIHDA ASETUKSIASI

tietojesi turvaamiseksi

Jos internet olisi vain paikka, jossa jaetaan kuvia dinosauruspukuihin puetuista koirista, salasanoille ei olisi juurikaan tarvetta. Mutta internetissä maksetaan laskuja, etsitään lääkereseptejä ja rekisteröidytään äänestämään. Ajattele kaikkia internetissä jaettuja ja laitteillesi tallennettuja ”virtuaalisia arvotavaroita”. **Mikset pidä niitä yhtä lailla turvassa kuin lompakkoasi tai avaimiasi?**

On yksi yksinkertainen tapa vaikeuttaa muiden pääsyä virtuaalitavaroihisi: **älä tee salasanojen arvaamisesta liian helppoa.** Suurin osa ihmisistä ei tarvitse erityisiä teknisiä taitoja päästäkseen tileillesi. Tarvitaan vain muutama arvaus salasanoistasi tai automaattinen ohjelma.

Kun heillä on pääsy yhdelle tilille, he voivat kokeilla vaarantunutta salasanaa muille tileille, kerätä tietoja sinusta ja tottumuksistasi, ottaa haltuun omistamasi tilit tai jopa käyttää digitaalista identiteettiäsi.

Kun seuraat tätä Data Detox -ohjelmaa, opit käytännön askeleet verkkotietoturvasi parantamiseksi.

Aloitetaan!

Tuotteen takana
TACTICAL TECH

Tukijana
Firefox

datadetoxkit.org
#datadetox

1.

LUKITSE DIGITAALINEN OVESI

Laitteesi näytönlukitukset eli salasana, kuvio, sormenjälki tai kasvotunnistus ovat *parhaita suojautumiskeinoja sellaisia henkilöitä vastaan, jotka haluavat päästä käsiksi laitteeseesi. Lukituskeinoja on useita erilaisia, ja voi olla vaikea tietää, mikä niistä sopii parhaiten juuri sinulle.

Mikä tahansa lukitus puhelimessa, tabletissa tai tietokoneessa antaa sinulle paremman suojan kuin ei lukitusta ollenkaan. Ja aivan kuten erilaiset oveen laitettavat lukot, **jotkut näytönlukitukset ovat vahvempia kuin toiset.**

Vahvimpia ovat pitkät, yksilölliset salasanat. Jos käytät lukituksen avaamiseen salasanaa, sen tulisi sisältää kirjaimia, numeroita ja erikoismerkkejä.

Jos nykyisin avaat puhelimesi pyyhkäisemällä, voit lisätä tietoturvaasi asettamalla puhelimeesi pitkän salasanan. Vai käytätkö kuviolukitusta? Entä jos muuttaisit kuvion hiukan pidemmäksi? Onko PIN-koodisi 1234? Entä jos valitsisit uuden PIN-koodin pyöräyttämällä noppaa seitsemän kertaa ja pistämällä tuon koodin mieleesi helpon koodin sijasta? **Pieni muutos voi olla iso askel kohti laitteidesi parempaa hallintaa.**

2.

PÄÄSTÄ SISÄÄN VAIN HARVAT JA VALITUT

Huipputason salasanojen luominen on helppoa. Sinun tarvitsee vain noudattaa muutamia perusperiaatteita. Salasanan tulee olla:

Pitkä: **salasanoissa tulee olla vähintään kahdeksan merkkiä. Vielä vahvempi? 16–20 merkkiä**

Ainutlaatuinen: **jokaisen käyttämäsi salasanan – jokaisella sivustolla – tulisi olla erilainen**

Satunnainen: **salasanasi ei tulisi olla looginen eikä helposti arvattavissa. Salasanojen hallintaohjelmista on paljon hyötyä.**

Vahvimmissa salasanoissa yhdistellään kirjaimia, numeroita ja erikoismerkkejä. Tämä vanha neuvo toimii, ja sen avulla rakennat vahvemman ja vaikeammin arvattavan salasanan. Jotkin salasanajärjestelmät eivät valitettavasti anna käyttää erikoismerkkejä (kuten @ # $% - = +), mutta riittävän pitkä kirjainten ja numeroiden yhdistelmä on silti parempi kuin lyhyt.

Parasta tapa on käyttää **erillistä salasananhallintaa** kaikkien salasanojen luomiseen ja tallentamiseen. Turvallisuusasiantuntijoiden suosittelemat salasanojen hallintaohjelmat, kuten 1Password ja KeePassXC, ovat sovelluksia, joiden ainoa tarkoitus on suojata kirjautumistunnuksesi ja muita arkaluonteisia tietoja.

3.

LISÄÄ TOINEN AVAIN

Kaksivaiheisen todennuksen (two-factor authentication, 2FA) tai monivaiheisen todennuksen (multifactor authentication, MFA) asettaminen tarkoittaa, että vaikka joku löytäisi salasanasi, **hänellä ei todennäköisesti olisi tiedossa toista avainta, jota tarvitaan laitteen avaamiseen.**

Tutustu eniten käyttämiesi sivustojen ja sovellusten suojausasetuksiin nähdäksesi, voitko määrittää ylimääräisen avaimen. Aloita tärkeimmistä: kaikki pankkisovellukset tai sähköpostin kaltaiset palvelut, joita käytät muiden tiliesi palauttamiseen.

Google:
Kirjaudu sisään osoitteeseen myaccount.google.com → Tietoturva → 2-vaiheinen vahvistus → Aloita

Facebook:
valikko → Asetukset → Turvallisuus ja sisäänkirjautuminen → Käytä kaksivaiheista todennusta

Vinkki: Kun määrität uutta vahvistustasoa, sinun on valittava toinen tapa vahvistaa henkilöllisyytesi. Yritä välttää (puhelinnumeroosi lähetettävien) tekstiviestien käyttöä siltä varalta, että kadotat puhelimesi. Sähköposti on yleensä luotettavampi vaihtoehto.