# Tietoturva käyttäjän näkökulmasta

## Tietoturvan ylläpito

Yksi tärkeimmistä suojautumiskeinoista on riittävän monimutkainen salasana, joka yhdistelee sanayhdistelmiä, merkkijonoja tai numeroita (1). Sovellusten viimeisimpien päivityksien lataaminen on suositeltavaa, sillä niillä pyritään paikkaamaan ohjelmistosta löytyviä tietoturva-aukkoja. Monivaiheinen tunnistautuminen yhdistettynä edellä mainittuun on yksi tehokkaimmista suojauskeinoista, jota käytetään esimerkiksi pankkisovelluksissa ja muissa henkilökohtaisissa palveluissa. Myös henkilökohtaisten sähköpostiosoitteiden ja vastaavien tietojen luovuttamisesta kannattaa olla tarkkana, sillä niiden joutuminen vääriin käsiin voi aiheuttaa tietoturvariskin. (2)

## Minkä takia tietoturvasta huolehtiminen on tärkeää?

Monelle saattaa tulla yllätyksenä, kuinka paljon heillä on menetettävää, kun tulee kysymykseen henkilökohtainen tietoturva ja sen murtuminen. Murtautuja voi käyttää henkilökohtaisia laitteita sekä internet-yhteyttä vahingollisiin tekoihin.

Pahimmassa tapauksessa uhri menettää omaisuutensa, identiteettinsä tai muutoin arkaluontoisia tietoja voi päätyä vääriin käsiin. Myös maine saattaa olla uhattuna, jolloin vahinkojen korjaaminen voi osoittautua erittäin hankalaksi ja niillä voi olla pitkäkantoiset jälkiseuraukset. (2)

## Arkielämän esimerkki huonosta tietoturvasta

Vuosina 2018–2019 tapahtunut Psykoterapiakeskus Vastaamon tietovuoto on hyvä esimerkki erittäin huonosti toteutetusta tietoturvasta. Siinä ulkopuolinen urkkija pääsi käsiksi asiakkaiden huonosti suojattuihin henkilökohtaisiin tietoihin, joita hän koitti myöhemmin käyttää kiristyksen välineenä. Kiristäjä vaati 200–500 euroa uhreilta, jotta hän ei julkaisisi tietoja julkisesti. (3) Kuitenkin potilastiedot julkaistiin osittain myös internetin pimeillä markkinoilla eli Tor-verkossa. (4) Varastettujen tietojen määräksi vahvistettiin elokuussa 2023 yhteensä 33086 kpl (5). Tapaukselta olisi voinut välittyä, jos Vastaamon järjestelmän olisi ohjelmoinut ammattilainen eikä yrityksen toimitusjohtaja, joka on itseoppinut ohjelmoija. (4) Potilas tiedot olisi pitänyt suojata pseudonyymisesti niin että tietokannassa olevien henkilötietojen mukaan ei voi päätellä asiakkaan oikeaa nimeä. (5) Lisäksi tietokannan ylläpitoon käytettiin oletuskäyttäjätunnusta ja -salasanaa. Kiristäjä väitti myös löytäneensä tietokantapalvelimen Google- haulla ilman palomuuria. (6)

(7)

# A screenshot of a phone Description automatically generated

Lähteet

1. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-2-suojautuminen-uhkatekijoilta/salasanojen-turvallinen-kaytto/.
2. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla

3 https://yle.fi/a/3-11613667

4 https://yle.fi/a/3-11616210

5 <https://www.aamulehti.fi/rikos/art-2000009757940.html>

6 <https://www.wired.co.uk/article/finland-mental-health-data-breach-vastaamo>

7 https://materiaalit.triuvare.fi/artikkelit/mita-jokaisen-toimitusjohtajan-tulee-tietaa-tietoturvasta