

Muistilista salasanojen hyvästä hoitamisesta yliopiston omissa ja ulkopuolisissa palveluissa

15.11.2011/ KR

Uutiset verkkoon vuodetuista tunnuksista, sähköpostiositteista ja niiden salasanoista alkavat olla toistuvia. Äskeinen vuoto sisälsi puoli miljoonaa suomalaista sähköpostiosoitetta, mukana joukko yliopistomme sähköpostiositteita. Myös salasanoja on uhattu julkistaa.

Vaikka tietomurtojen onnistuttua ei käyttäjällä olekaan paljon tehtävissä, voi kaapatun ja julkistetun käyttäjätunnuksen omistaja estää pääsyn tunnukselleen vaihtamalla salasanaan ja tarkistamalla muutoinkin omaa sähköpostin ja salasanojen käytäntöä.

Palveluiden käyttöoikeus on yliopistossakin pääsääntöisesti ns. heikon tunnistuksen varassa, jolloin verrataan käyttäjän antamaa salasanaa palvelun salasanatiedostossa olevaan. Käyttäjä voi vaihtaa salasanaan epä säännöllisin väliajoin ja palvelu voi muistuttaa vaihdosta, mutta salana on pysyvä vaihtojen väliajan. Mitä useammin salasanaa vaihdetaan, sitä huonommin sen anastaja pääsee sitä hyödyntämään.

Lisäturvallisuutta palvelun käyttöoikeuksien tarkistamiseen saadaan vahvalla tunnistamisella, joka yleisimmin toteutetaan antamalla kiinteän salasanan lisäksi kertakäyttöinen merkkijono. Tämä on tuttua verkkopankeissa tai yliopiston etäkäyttäjän VPN-yhteyden avaamisessa.

Hyvä järjestelmä ei hyväksy huonosti valittua salasanaa ja pakottaa käyttäjän myös vaihtamaan salasanaan säännöllisin väliajoin. Käyttäjä voi itse vaihtaa salasanaan lisäksi milloin vain.

Hyvän salanan käytännön muistilistaa käyttäjälle

- **Käyttöoikeus ja salana ovat henkilökohtaisia, niitä ei saa luovuttaa kenellekään toiselle** henkilölle. Ethän anna pankkikorttisikaan tunnusta toiselle henkilölle.
- Se, joka luovuttaa toiselle yliopiston tunnuksensa salasanan, toimii yliopiston käytösääntöjen vastaisesti.
- Jos salana on annettu toiselle tai on epäily että salana on joutunut toisen henkilön haltuun, tulee salana vaihtaa välittömästi. Vaihda salana kohtuullisin välein normaalistikin.
- **Erota yliopiston palvelut ja yliopiston työtä tai opiskelua varten tarvittavat palvelut verkossa yksityisesti käyttämistäsi yleisöpalveluista.** Hanki yleisöpalveluiden käyttöä varten ulkoisen palvelutarjoajan sähköpostitunnus ja anna se niihin yhteystiedoksi tai käyttäjätunnuksiksi.
- **Ulkopuolisen palvelun tunnukselle pitää aina antaa eri salana kuin yliopiston käyttäjätunnukselle,** jotta ulkopuolisen tunnuksen kaappaaja ei sen avulla kykene saamaan pääsyä saman henkilön yliopistotunnukselle.
- Kaappaaja yrittää avata salasanatiedostojen sisältämät salakirjoitetut salanat koneellisesti erilaisia merkkijonoja sisältävien sanakirjojen avulla. Avatut tunnus/salasanaparit kaupataan muille rikollisille, joiden tavoite on saada haltuunsa tavallisten käyttäjien kautta tietoja, palvelimia tai työasemia.
- **Valitse salanasasi niin, että ne ovat vaikeita avata jopa koneellisesti.** Laadi salana näin: siinä on enemmän kuin 8 merkkiä eikä se ole minkään kielen sana, sen yksikkö tai monikko, ei taivutusmuotokaan; siinä on isojen ja pienten kirjainten lisäksi numeroita ja erikoismerkkejä. Jos palvelu sallii, käytä myös skandinaavisia aakkosia (äääÄÖ). (Mm. yliopiston VPN-palvelin ei hyväksy.)

- Jos sinulla on käytössä paljon ulkopuolisia pääsyoikeuden tarkistavia palveluita, koeta ryhmitellä palvelut saman tasoiisiin. Käytä tärkeille palveluille kullekin omaa salasanaa ja muille yhteisiä salasanoja. Näin eivät kaikkien palveluiden salasanat ole menetettyjä yhden palvelun kaappauksessa.
- Kun sinulla on useita käyttäjätunnuksia eri palveluihin, et voi muistaa niitä vaan yleensä täytyy kirjoittaa salasanat muistiin jonnekin. Talleta salasanalistasi paikassa, josta sivulliset ei sitä helposti saa.
- Kiellä selaimesta toiminto, joka tallettaa verkkopalveluihin annettavat salasanat. Hyvästikin ylläpidettyyn työasemaan voi päästä haittaohjelma, joka nuuskii koneeseen talletetut salasanat ja lähettää ne maailmalle. Jotkut palvelut myös antavat aloitussalasanan selväkielisenä sähköpostissa, joten tarkista silloin tällöin tiedostosi ja sähköpostisi hakusanoilla 'passwd, password, salasana' tms. ja varmistu että olet vaihtanut niissä mainitut salasanasi.

Ajankohtaisista tietoturvaloukkauksista uutisoiva Viestintäviraston sivu TietoturvaNyt!

<http://www.cert.fi/Tietoturvanyt.html>

Cert.fi: Salasanat vaihtoon ja sillä sipuli

<http://www.mtv3.fi/uutiset/it.shtml/2011/11/1438039/certfi-salasanat-vaihtoon-ja-silla-sipuli>

Yliopiston salasanakäytäntöohjeita:

Opiskelijan tietoturvaopas sivut 2-3,

http://www oulu.fi/tietohallinto/opiskelijoille/opus/Opiskelijan_tietoturvaopas_2009elokuu_netti.pdf

Salasanan vaihtaminen keskitetyissä palveluissa ja hyvän salasanan vaatimukset,

<http://www oulu.fi/tietohallinto/ohjeet/unix/salasanat.htm>

Käyttäjän tietoturvaopas, sivut 17-18,

http://www oulu.fi/tietohallinto/tietoturva/sisalto/kayton_ohjeet/VAHTI/Vahti_10_06.pdf