Salasanojen turvallinen käyttö
Salasanat ovat henkilökohtaisia

Olet henkilökohtaisesti vastuussa salasanojesi käytöstä, joten huolehdi salasanojesi turvallisuudesta asianmukaisella vakavuudella! Alla muutama salasanojen käyttöohje:

- Älä koskaan anna mitään salasanaasi **kenellekään toiselle henkilölle**!
- **Hyvä salasana ei sellaisenaan muodostu sanakirjasta löytyvästä sanasta.Useista sanoista ja merkeistä muodostuva salasana on jo paljon parempi!**
- **Salasanan tulisi olla vähintään 10 merkkiä pitkä, ja sen olisi hyvä sisältääisoja ja pieniä kirjaimia sekä numeroita ja erikoismerkkejä (esim. vMItmtvk13ekm!).** Huomaa myös, että näppäimistöllä vierekkäin olevien merkkijonojen käyttäminen on riski (esim. qwertyui1234).
- **Älä missään nimessä käytä yhtä ja samaa salasanaa monissa palveluissa**: jos käyttäisit samaa salasanaa ja käyttäjätunnusta kaikkialla, pahanilkinen henkilö voisi saada heikosti suojatun järjestelmän krakkeroimalla pääsyoikeuden myös hyvin suojattuihin järjestelmiin.
- Vaihda salasanasi myös säännöllisesti, vaikkei järjestelmä sinua siitä muistuttaisikaan.

Helsingin yliopiston käyttäjätunnuksen salasanaa ei saa käyttää yliopiston ulkopuolisissa verkkopalveluissa, sillä monien palveluiden tietoturva on puutteellinen. **Käyttämällä eri salasanaa jokaiseen palveluun minimoit vahingot mahdollisen tietoturvamurron sattuessa.** Muista lisäksi se, että kukaan HY:n tietojärjestelmien ylläpitäjä EI kysy sinulta salasanaasi missään yhteydessä (järjestelmien ylläpitäjät pystyvät hoitamaan työnsä ilman salasanaasi).

Hyvän salasanan ominaisuudet

Salasana on hyvä jos se on helposti muistettava, mutta muille mahdoton arvata tai saada kokeilemalla oikein. Perusajatuksena salasanan keksimisessä kannattaa pitää sitä, että**salasana ei saa olla minkään kielen sana**: mikäli valitsisit salasanaksesi luonnollisen kielen sanan (esimerkiksi *pallo* tai *kissa*), olisi pahantahtoisilla kriminaaleilla mahdollisuus saada salasana tietoonsa kokeilemalla koneellisesti *kaikkia* sanakirjoissa esiintyviä sanoja. **Lisäksi hyvin harva järjestelmä edes kelpuuttaa näin lyhyttä salasanaa.**

Yhdistelemällä useita sanoja saat vahvemman salasanan, mutta käytä luovuuttasi ja lisää sekaan muita merkkejä! Esimerkiksi ”lepakkomies” ei ole turvallinen salasana – etenkään jos kyseessä on suosikkihahmosi tai -baarisi. Sen sijaan yhdistelmä mallia ”Dosiilit#%8Poljennot” on jo huomattavan paljon vaikeampi murtaa.

Turvallisen salasanan keksiminen

Salasanan keksimisessä on syytä olla luova, jotta kukaan ei voisi keksiä salasanaasi päättelemällä. Keksi salasanaksi vaikkapa jonkin lause, jonka muistat helposti. Lauseessa on hyvä olla erisnimiä, jotka aloitetaan isoilla kirjaimilla, ja myös lukuja. Valitse sen jälkeen lauseen jokaisesta sanasta ensimmäinen kirjain ja muodosta kirjaimista salasana.

Esimerkki: Raimo palaa mielessään ex-tyttöystävänsä kanssa viettämäänsä aikaan keksien saman tien varsin turvallisen, alla kuvatun lauseen.

Asuin Paulan kanssa 5 vuotta Keskuskatu 15:ssä = APk5vK15

Useiden salasanojen hallinta ja säilytys

Salasanoja ei tulisi kirjoittaa paperille tai tietokoneella säilytettävään tiedostoon sellaisenaan, sillä paperin löytävä tai tietokoneen varastava henkilö saisi tällöin helposti pääsyn kaikkiin salasanalla suojaamiisi palveluihin. Koska useiden kymmenien salasanojen muistaminen on kuitenkin hankalaa, voit helpottaa salasanojen muistamista osittamalla salasanasi kaikille eri salasanoille yhteiseen, samaan alkuosaan sekä erilliseen loppuosaan.

ESIMERKKI: alla on Raimon salasanalista, joka antaa kuvan salasanojen osittamisesta. Huomaa, että Raimo käyttää salasanoissa hyväkseen aiemmin mainittua salasanaansa.

Koko salasana	**Yhteinen alkuosa**	**Erilliset loppuosat**	**Palvelu**
APk5bb68	APk5	bb68	Eräs Raimon käyttämä treffipalvelu
APk5i9z4	APk5	i9z4	Raimon käyttämä ilmainen Notmail-sähköpostipalvelu
APk5b6yz	APk5	b6yz	Raimon käyttämä ilmainen osakekurssipalvelu

Painamalla kaikille salasanoille yhteisen alkuosan mieleesi, voit kirjoittaa erilliset loppuosat vaikkapa paperille varsin turvallisemmin mielin. Säilytä salasanalistaasi kuitenkin aina huolellisesti, sillä joku voi – keinolla tai toisella – saada selville salasanojesi yhteisen osan.

Usein tietokoneen käyttäjä ajattelee, että hän on salasanallaan vastuussa ainoastaan omalla tietokoneellaan tai omassa henkilökohtaisessa kansiossa olevista tiedoistaan. Helppo salasana tai sen huolimaton säilyttäminen voi kuitenkin avustaa krakkeria pahanilkisessä toiminnassaan, joten myös sinun on tärkeää huolehtia salasanojesi turvallisuudesta.

Salasanojen turvallinen käyttö

Monet ihmiset ajattelevat, että vaikeasti keksittävä salasana yhdessä turvallisen säilytystavan kanssa ovat riittävä tae salasanan käytön turvallisuudesta. Näin ei kuitenkaan ole, sillä salasanojen käytön turvattomuuteen vaikuttavat mm. seuraavat tekijät:

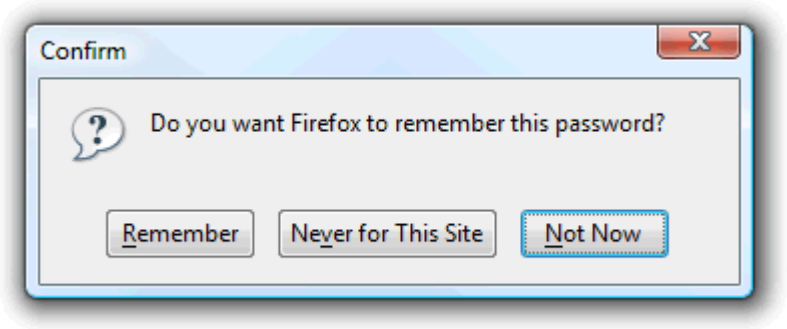
- Joku voi nähdä salasanasi syöttäessäsi sitä näppäimistölle.

- Joku voi asentaa käyttämääsi tietokoneeseen näppäimistön ”kuuntelulaitteen” eli ns. keyloggerin.

Erityisesti julkisissa nettikahviloissa ym. paikoissa kannattaa siis olla varovainen salasanoja käyttäessäsi: vaikka lukisit esimerkiksi sähköpostiasi tms. suojatussa yhteydessä (lisätietoa aiheesta seuraavassa luvussa), käyttämäsi tietokone voi olla turvaton käyttää!

Dalmatiassa lomaillessaan Raimo käy rakkaan ystävänsä Alisan kanssa nettikahvilassa, jonka tietoturvasta Raimolla ei ole varmuutta. Aavistaen tilanteen Raimo on edeltäkäsin ohjannut saamansa sähköpostin erääseen ilmaissähköpostiosoitteeseen, jonka salasana on muu kuin Raimon tavallisesti käyttämän sähköpostin salasana. Näin ollen Raimo voi lukea postinsa varsin turvallisin mielin.

Huomaa, että mm. useat verkkoselaimet tarjoavat mahdollisuuden käyttäjätunnusten ja salasanojen tallentamiseen. Kyseinen toiminto on kätevä, mutta siinä piilee myös tietoturvallisuusriskejä. Jos et lue selainohjelman näyttämiä viesti-ikkunoita tarkkaan, voit tallentaa salasanasi selaimeen jopa epähuomiossa. Seuraava kuva esittää selaimen viesti-ikkunaa, jossa ohjelma kysyy sinulta, haluatko tallentaa salasanasi selaimen muistiin.



Salasanojen tallentamistoimintoon liittyy myös muita riskejä. Tietyt haittaohjelmat osaavat tietokoneellesi päästessään sekä ”nuuskia” tallentamasi salasanat selainohjelmasta että lähettää salasanat haittaohjelman luoneelle krakkerille. Lisäksi samaa tietokonetta ja selainohjelmaa käyttävät ihmiset voivat lukea salasanasi selkokielisenä, jos heillä on pääsy selainasetuksiisi. Seuraava kuva havainnollistaa, kuinka salasanat on mahdollista lukea selkokielisenä Firefox-selaimen asetuksista käsin.

Lähde: