Näin syntyy turvallinen salasana – 11-vuotiaalla tytöllä huikea bisnes

Nopanheitto on taatusti satunnainen tapa muodostaa numerosarjoja. Ne muuntuvat puolestaan sanoiksi. *(KUVA: Sari Poijärvi)*

Julkaistu: 26.10.2015 12:58

TIETOTURVA **Noppaware on vähän tunnettu, verrattain turvallinen salasanojen luontimenetelmä, jonka 11-vuotias amerikkalaistyttö toi julkisuuteen.**

11-vuotias newyorkilaistyttö on perustanut oman **pikkubisneksen <http://www.dicewarepasswords.com/>**, jolla hän myy turvallisia salasanoja kahden dollarin kappalehintaan. Koululainen luo salasanat "diceware"-menetelmällä (termi kääntyy yleensä noppawareksi) ja lähettää kynällä paperille kirjoitetut salasanat kirjesalaisuuden piirissä olevalla kirjepostilla asiakkaille.

Bisnes syntyi "äidin laiskuudesta luoda monimutkaisia salasanoja".

Asiasta kirjoittaa **Ars Technica <http://arstechnica.com/business/2015/10/this-11-year-old-is-selling-cryptographically-secure-passwords-for-2-each/>**.

Dicewaressa on kyse salasanojen muodostamisesta sanalistoista sattumanvaraisesti noppaa heittämällä. Jokaisella listan sanaa vastaa viisinumeroinen luku välillä 11111–66666, ja viiden nopanheiton sarjalla listalta valikoituu yksi sattumanvarainen sana.

Toimenpide toistetaan kuusi kertaa, ja lopputuloksena syntyy viidestä luonnollisen kielen sanasta syntyvä salasana.

Noppawaren logiikka on siinä, että pitkät salasanat ovat hyvin vaikeita murtaa – etenkin, jos niitä höystää kevyesti esimerkiksi isoin alkukirjaimin tai sanojen välissä olevien merkein. Lisäksi salasana on helppo muistaa, koska se koostuu oikeista sanoista.

Noppawaresalasana on helppo luoda myös itse. IS heitti noppaa 30 kertaa ja sai numerosarjan **35146 36366 34364 12633 62551 35343**.

Englanninkielisestä sanalistasta <http://world.std.com/~reinhold/diceware.wordlist.asc> numerolla muodostuu salasana **kabul leyden jaw aug vale kind**.

Kai Puolamäen <http://www.iltasanomat.fi/haku/?search-term=Kai%20Puolam%C3%A4en> koostamasta **suomenkielisestä listasta <http://users.ics.aalto.fi/kaip/noppaware/noppaware-print.pdf>** sama numerosarja luo salasanan **kerron kohien [köhien] kaytko [käytkö] ansoja tahti kielsi**.

Tämän voi vaikkapa muotoilla muistisäännöksi, jossa "kerrotaan köhien tarina, jossa käydään ansaan tahdissa, vaikka se olisi kiellettyä". Virkkeessä ei ole järkeä, mutta se juuri tekee salasanasta vahvan.

Noppaware ei uusi ilmiö. Sen isänä pidetään **Arnold G. Reinholdia <http://www.iltasanomat.fi/haku/?search-term=Arnold%20G.%20Reinholdia>**, joka esitteli tekniikan **vuosia sitten <http://world.std.com/~reinhold/diceware.html>**. Newyorkilaistyttö teki tärkeän työn tuodessaan sen julkisuuteen, joten tämän bisnestä voi pitää tavallaan käänteentekevänä.

Noppawaren käyttö ei kuitenkaan estä tarvetta trimmata jokaisella palvelulle erillinen salasana. Turvallinenkin salasana muuttuu turvattomaksi, jos se päätyy tietomurrossa krakkereiden käsiin. Tällöin murtautujat voivat kokeilla sitä käyttäen pääsyä muihin järjestelmiin.

Uutista tarkennettu.