

Salasanat

Johdanto



Lähde: FlickR

Tärkein työkalu verkkopalveluun **tunnistautumisessa** on salasana, joka on usein ainoa suojautumiskeino ei-toivottuja tunkeutumisia vastaan, joilla voisi olla katastrofaalisia seurauksia.

Salasanat ovat kuitenkin huonosti hallittu työväline, sillä usein käytetään hyvin yksinkertaisia salasanoja, jolloin ne ovat helposti arvattavissa ja hakeroitavissa. On tärkeää osata pitää omat salasanat muistissa ja suojassa ulkopuolisilta.

■ Käyttäjän tunnistaminen

Tietokoneiden käyttämiseen liittyy usein käyttäjän tunnistaminen esimerkiksi internetissä. Yleisin

tunnistautumistekniikka perustuu

“käyttäjätunnus/salasana”-pariin. Riippuen tilanteesta, tunnus voi olla julkinen tai yksityinen, mutta se on usein heikosti suojattu. Salasana on työkalu, joka varmistaa perusturvallisuuden.

A screenshot of a web login interface. It features two text input fields: the top one is labeled "Admin ID" and the bottom one is labeled "Password". Below these fields is a button labeled "Login". The labels and button text are in a blue, slightly pixelated font.

Lähde: Flickr

■ Identiteettivarkaus

Wikipedian määritelmä:

"Identiteettivarkaus tarkoittaa toisen henkilötietojen kuten nimen tai henkilötunnuksen eli identiteetin oikeudetonta käyttöä. Usein varas pyrkii tekemään rahanarvoisia sitoumuksia toisen henkilön identiteetin nimissä."

Ongelma:

Tietoturvaloukkausten ja identiteettivarkauksen välisen yhteyden selvittäminen on haastavaa, koska identiteettivarkauksen uhrin eivät usein tiedä miten henkilötiedot on hankittu, eivätkä yksittäiset uhrin välttämättä havaitse identiteettivarkautta

Joten...

Tunnistusta pyytävien operaattoreiden tulee huolehtia salasanojen hallintaan liittyvistä lukuisista turvatoimista. Tämä on erittäin tärkeä asia, mutta siihen me itse voimme vähän vaikuttaa.

➔ Käytä salasanaa, jota ei ole helppo hakkeroida

- Vältä tavallisia salasanoja kuten 12345, qwerty, syntypäivä, sama salasana ja käyttäjätunnus jne.
- Salasanan tulee olla pitkä (vähintään 14 merkkiä)
- Salasanassa tulee olla isoja ja pieniä kirjaimia, numeroita, erikoismerkkejä jne
- Operaattorien tulisi tarjota turvatoimenpiteiden kuten rajoitetun määrän kirjautumisyrittäksiä, captcha esim kuvavarmennuksen avulla



Lähde: Flickr

■ Mutta...

Monilla ihmisillä on useita tilejä ja on tärkeää, että niissä käytetään eri salasanoja. Siksi niitä kaikkia on vaikea muistaa. Salasanojen kirjoittaminen paperillekin on omat riskinsä.

Miten ratkaista ongelma?

Tähän muistamisongelmaan voidaan käyttää seuraavia menetelmiä:

- Käytä lauseita salasanoina, ne on helppo muistaa, mutta vaikea arvata
- Käytä kaksivaiheisia tunnistautumismenetelmiä
- Käytä salasanojen hallintaohjelmaa

■ Lause salasananana

Sen sijaan, että tarvitsisi muistaa monimutkaisia salasanoja kuten "Mç9@X##Kl", on suositeltavampaa käyttää lauseita, jotka on helppo muistaa, mutta vaikea hakkeroida.

Esimerkki; syntymäpäivän ja -paikan sijaan voidaan käyttää lausetta "Syntynyt klo 11 torstaina". Tämä lause voi tai voi olla liittymättä käytettyyn palveluun (ei ilmeisellä tavalla).

Tämä mahdollistaa
monimutkaisen mutta
helposti muistettavan
salasanan!

■ Kaksivaiheinen tunnistaminen

Kaksivaiheisessa tunnistautumisessa henkilön identiteetti varmistetaan kahta eri tunnistautumismenetelmää hyödyntäen. Useimmiten tunnistautumiseen tarvitaan salasana ja tekstiviestinä käyttäjälle lähetetty koodi.

Tämän menetelmän heikko puoli on lisätietojen lähettäminen (puhelinnumero, vahvistus sähköpostilla tai maksukortilla, biometrinen tunnistus)

Huomaa!
Puhelinnumeron antaminen pankillesi
voi olla perusteltua, mutta
biometristen tietojen
nettiostoksen tekemiseksi ei ole!



Lähde: FlickrR

Salasanojen hallintaohjelmat

Riippumatta siitä miten luot omat salasanasi, niiden muistaminen on suurin haaste! Hyvä ratkaisu tähän voi olla salasanojen hallintaohjelmat.

Lähes kaikki selaimet tarjoavat mahdollisuuden salasanan tallennukselle. Tämä vaihtoehto yksinkertaistaa elämää, mutta voi olla vaarallinen. Jotkut selaimet, kuten Firefox, tallentavat salasanan oletuksena ja tekstimuodossa!

Jos todella haluat käyttää tätä vaihtoehtoa, paras tapa on käyttää pääsalasanaa, jonka avulla pääset hallinnoimaan muita salasanoja.

Salasanojen hallintaohjelmat (2)

Paras ratkaisu on käyttää ulkoista salasanojen hallintaohjelmaa. Tämä ohjelmisto on asennettava tietokoneeseen ja se hallitsee salasanojen muistamisen puolestasi. Ohjelmat enkryptaavat salasanat, joihin pääsee käsiksi vain pääsalasanan avulla, joka on tällöin ainoa salasana, joka tarvitsee muistaa.

Esimerkkejä ohjelmista: Lastpass, Onepassword, Dashlane, OsX:n oma Avainnippu jne.

Kyseiset ohjelmat ovat myös ilmaisia!



KIITOS!

Kysymyksiä?
