Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

- Salasanalausekkeet
- Salasanalausekkeiden turvallinen käyttö
- Lähteet

Salasanalausekkeet

Taustaa

Käytät salasanoja todennäköisesti päivittäin, tarvitset niitä sähköpostiin ja nettipankkiin kirjautumiseen tai voit käyttää salasanoja ostaaksesi jotain nettikaupasta tai kun haluat avata matkapuhelimesi. Salasanat voivat kuitenkin olla heikoin lenkkisi - jos joku saa ne haltuunsa, voidaan identiteettisi tai rahasi varastaa, tai varas voi päästä käsiksi henkilökohtaisiin tietoihisi. Tämän vuoksi hyvät salasanakäytännöt ovat tärkeitä kun suojelet itseäsi. Tässä uutiskirjeessä kerromme, kuinka voit luoda vahvoja ja helposti muistettavia salasanoja käyttämällä salasanalausekkeita (passphrase).

Vierastoimittaja

Guy Bruneau toimii seniorikonsulttina yrityksessä IPSS Inc., SANS-ohjaajana ja ISC-käsittelijänä. Guy:lla on SANS:n GSE ja hän on käynyt SANS:n Cyber Guardian ohjelman. Voit seurata häntä Twitterissä **@GuyBruneau** tai osoitteessa **handlers.sans.org/gbruneau**.

Salasanalausekkeet

Salasanojen osalta suurin haaste tänä päivänä on se, että kyberhyökkääjät käyttävät kehittyneitä menetelmiä “arvatakseen” salasanoja “brute force” menetelmällä ja nämä menetelmät muuttuvat kokoaika tehokkaammiksi. Tämä johtaa siihen, että salasanasi ovat helposti murrettavissa jos ne ovat heikkoja tai helppoja arvata. Itsesi suojaamiseksi tärkeintä on käyttää vahvoja salasanoja. Mitä enemmän merkkejä salasanassasi on, sitä vahvemmaksi se muuttuu ja sitä vaikeampi hyökkääjän on sitä arvata. Monimutkaisia ja pitkiä salasanoja voi kuitenkin olla vaikea muistaa ja siksi suosittelemme mieluummin salasanalausekkeiden käyttöä. Salasanalauseke on yksinkertainen lauseke tai lause, joka sinun on helppo muistaa, mutta sitä on vaikea hakkeroida. Alla on esimerkki.

Missä on Mannerheim?

Mikä tekee tästä salasalausekkeesta vahvan on se, että se on 20 merkkiä pitkä ja siinä on isoja kirjaimia ja erikoismerkkejä (muista, että välilyönnit, ääkköset ja kysymysmerkki lasketaan erikoismerkiksi). Voit tehdä omasta salasanalausekkeesta vielä vahvemman käyttämällä kirjainten sijaan numeroita ja symboleita, esimerkiksi “@”-merkkiä tai kirjaimen “O” sijaan numeroa “0”. Jos sovellus tai internetsivu rajoittaa salasanan merkkien pituutta, käytä aina suurinta sallittua pituutta.

© SANS Institute 2015

Salasanalausekkeet

Salasanalausekkeiden turvallinen käyttö

Myös salasanalausekkeita käytettäessä pitää noudattaa varovaisuutta, niiden käyttö ei auta jos vihamieliset tahot saavat kopioitua tai varastettua sen helposti.

Salasanalausekkeiden käyttö on yksi tehokkaimmista tavoista suojata verkkoidentiteettiäsi ja tietojasi.

1. Varmista, että käytät eri salasanalauseketta eri tileillä tai laitteilla. Älä esimerkiksi käytä samaa salasanalauseketta työ- tai pankkiasioihin kuin mitä käytät henkilökohtaisilla tileillä, kuten Facebookissa, YouTubessa tai Twitterissä. Tällä tavalla, jos yksi tileistäsi hakkeroidaan, muut ovat silti turvassa. Jos sinulla on monia salasanalausekkeita muistettavana (mikä on erittäin yleistä), harkitse salasanasovelluksen käyttöä. Kyseiset sovellukset tallentavat salasanasi turvallisesti ja tämän jälkeen sinun ei tarvitse muistaa salasanalauseketta kuin päätelaitteeseen ja salasanasovellukseen.

2. Älä koskaan kerro kenellekään salasanalausekkeitasi tai niiden keksimiseen käytettävää henkilökohtaista logiikkaasi. Muista, että salasanalauseke on salainen ja jos joku muu tietää sen, se ei enää ole salainen. Jos joku saa salasanalausekkeesi tietoonsa tai uskot, että se on vuotanut jonnekin, vaihda se välittömästi.

3. Aivan kuten salasanojen kanssa, älä käytä helposti arvattavia tai yleisesti käytettyjä salasanalausekkeita. Esimerkiksi lauseke “Parempi Pyy Pivossa” ei ole hyvä salasanalauseke, koska lause on niin yleisesti tunnettu.

4. Älä käytä julkisia tietokoneita, kuten hotellien tai kirjastojen koneita pankkiin tai työhön liittyviin palveluihin kirjautuessa. Kuka tahansa voi käyttää näitä samoja koneita, jolloin niissä saattaa olla haittaohjelmia, jotka kaappaavat kaikki näppäimistön painallukset. Kirjaudu verkkopankkeihin tai työhön liittyviin palveluihin vain luotetuilta koneilta tai mobiililaitteilta.

5. Noudata huolellisuutta jos internetsivut pyytävät sinua vastaamaan henkilökohtaisiin kysymyksiin. Näitä kysymyksiä käytetään salasanojen palauttamiseen, mutta ongelma näiden kanssa on se, että vastaukset niihin saattavat löytyä helposti myös internetistä tai Facebook-sivuiltasi. Jos vastaat näihin, niin varmista että käytät vain tietoa joka ei ole julkisesti saatavilla tai keksi kuvitteellisia vastauksia. Salasanasovellukset auttavat myös tämän tiedon tallentamisessa.

6. Monet verkkotilit tarjoavat nykyisin mahdollisuuden kaksivaiheiselle tunnestautumiselle. Kun otat tämän palvelun käyttöön, tarvitset salasanalausekkeen lisäksi aina jonkin toisen kirjautumiselementin, esimerkiksi matkapuhelimeen

© SANS Institute 2015

Salasanalausekkeet

lähetettävän koodin. Kaksivaiheisen tunnistautumisen avulla teet tiliesi käytöstä erittäin turvallisen ja näitä vaihtoehtoja on suositeltavaa käyttää kun mahdollista.

7. Mobiililaitteet käyttävät usein numeroita kirjautumiseen ja suojaukseen. Muista, että myös nämä ovat salasanoja ja mitä pidempi käyttämäsi numero on, sen turvallisempi se on. Monissa nykyaikaisissa mobiililaitteista, pääsykoodin voi myös vaihtaa oikeaan salasanalausekkeeseen.

8. Viimeisenä, kun et käytä jotain tiliä tai laitetta, muista aina sulkea, poistaa tai disabloida tili tai laite käytön jälkeen.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-uutiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa http://www.securingthehuman.org.

Elisa Appelsiini on korkean osaamisen IT-palvelutalo. Noin 400 IT-alan ammattilaisen voimin tuotamme monipuolisia ja tietoturvallisia tietotekniikkaan liittyviä pilvi-, työn tuottavuus-, konsultointi- ja ulkoistuspalveluja. Kehitämme myös asiakkaidemme liiketoimintaa tukevia sovelluksia ja tuotteita. Toimintamme perustuu syvään teknologiaosaamiseen ja aidosti asiakaslähtöiseen toimintaan.

Elisa Appelsiini is a comprehensive IT service provider owned by the leading provider of communications services in Finland, Elisa. Elisa Appelsiini helps its customers to enhance their business and increase competitiveness by offering high-end IT services in consulting, cloud, integration, software development and outsourcing.

Lähteet

Kaksivaiheinen tunnistautuminen:	http://www.securingthehuman.org/ouch/2013#august2013
Salasananhallintasovellukset:	http://www.securingthehuman.org/ouch/2013#october2013
Käyttäjän manipulointi:	http://www.securingthehuman.org/ouch/2014#november2014
Yleiset turvallisuustermit:	http://www.securingthehuman.org/resources/security-terms

Lisenssi

OUCH! julkaisijana toimii “SANS Securing The Human”-organisaatio ja jakelu tapahtuu Creative Commons BY-NC-ND 3.0 lisenssillä. Voit vapaasti jakaa tätä uutiskirjettä ja käyttää sitä osana tietoturvatietoisuusohjelmaasi kunhan et muokkaa uutiskirjettä. Käännös- ja lisätietoja varten, ota yhteys www.securingthehuman.org/ouch. Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus