Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Salasanalausekkeet

Taustaa

Käytät salasanoja todennäköisesti päivittäin; tarvitset niitä sähköpostiin ja nettipankkiin kirjautumiseen tai joudut käyttämään niitä ostaaksesi jotain nettikaupasta tai kun haluat avata matkapuhelimesi. Salasanat saattavat kuitenkin olla heikoin lenkkisi - jos joku saa ne haltuunsa, voidaan identiteettisi tai rahasi varastaa, tai varas voi päästä käsiksi henkilökohtaisiin tietoihisi. Salasanojen muistaminen ja laadukkaiden salasanojen luominen voi olla haasteellista ja tämän vuoksi hyvät salasanakäytännöt ovat äärimmäisen tärkeitä itsesi suojaamisessa. Tässä uutiskirjeessä kerromme, kuinka voit luoda vahvoja ja helposti muistettavia salasanoja käyttämällä salasanalausekkeita (passphrase).

Vierastoimittaja

My-Ngoc Nguyen on sertifioitu SANS kouluttaja ja Secured IT Solutions-yrityksen toimitusjohtaja. Hänellä on 14:sta vuoden ja useiden sertifiointien tuoma kokemus tietoturvaviitekehysten luomisesta, kehittämistä ja ylläpitämisestä lukuisilla eri aloilla. Löydät hänet Twitteristä: **@MenopN** ja LinkedInistä: My-Ngoc ”Menop” Nguyen.

Salasanalausekkeet

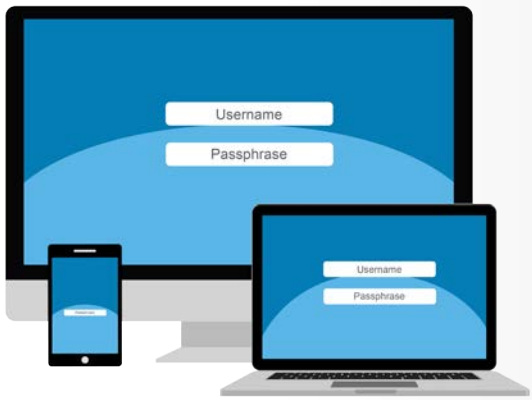
Salasanojen osalta suurin haaste tänä päivänä on se, että kyberhyökkääjät käyttävät jatkuvasti kehittyviä menetelmiä murtaakseen salasanoja esim. “brute force” menetelmällä. Tämä johtaa siihen, että salasanasi ovat helposti murrettavissa jos ne ovat heikosti laadittuja tai helppoja arvata ja siksi itsesi 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 murtaa tai arvata. Alla on esimerkki.

Pysy-Aina-Aallonharjalla
Kahviaika iltapäivällä 13:20

Näistä salasanalausekkeista tekee vahvan se, että ne ovat yli 20 merkkiä pitkä ja niissä on isoja kirjaimia sekä erikoismerkkejä (muista, että välilyönnit, ääkköset ja kysymysmerkki lasketaan erikoismerkiksi). Voit tehdä omasta salasanalausekkeesta vielä vahvemman käyttämällä kirjainten sijaan numeroita ja symboleita, esimerkiksi “@”-merkkiä

Salasanalausekkeet

tai kirjaimen “O” sijaan numeroa “0”. Jos sovellus tai internetsivu rajoittaa salasanan merkkien pituutta, käytä aina suurinta sallittua pituutta.



Salasanalausekkeet ovat yksinkertainen tapa luoda ja muistaa vahvoja salasanoja.

Salasanalausekkeiden turvallinen käyttö

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

1. Varmista, että käytät eri salasanalausekkeita eri tileillä ja laitteilla. Älä esimerkiksi käytä samaa salasanalauseketta työ- tai pankkiasioihin kuin mitä käytät henkilökohtaisilla tileillä, kuten Facebookissa, YouTubessa tai Twitterissä. Tässä tapauksessa, 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. Ainoa poikkeus on se, jos haluat kertoa salasanasi tutulle tai perheenjäsenelle hätätapauksia varten. Tässä tapauksessa kirjoita salasanat paperille, sijoita ne turvalliseen paikkaan ja kerro tästä paikasta vain henkilölle jolle haluat. Jos sinulle tapahtuu jotain tai tarvitset tunnuksia, pääset niihin käsiksi.
3. Älä käytä julkisia tietokoneita, kuten hotellien tai kirjastojen koneita pankkiin tai työhön liittyviin palveluihin kirjautuessa. Kuka tahansa voi käyttää näitä koneita, ja niissä saattaa olla haittaohjelmia, jotka esim. kaappaavat kaikki näppäimistön painallukset. Kirjaudu verkkopankkeihin tai työhön liittyviin palveluihin vain luotetuilta koneilta tai mobiililaitteilta.
4. 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

Salasanalausekkeet

joka ei ole julkisesti saatavilla tai keksi kuvitteellisia vastauksia. Salasanasovellukset auttavat myös tämän tiedon tallentamisessa.

5. Monet palvelut tarjoavat nykyisin mahdollisuuden kaksivaiheiselle tunnestautumiselle. Kun otat tämän palvelun käyttöön, tarvitset salasanalausekkeen lisäksi aina jonkin toisen kirjautumiselementin, esimerkiksi matkapuhelimeen lähetettävän koodin. Kaksivaiheisen tunnistautumisen avulla teet tiliesi käytöstä erittäin turvallisen ja tätä vaihtoehtoa on suositeltavaa käyttää aina kun mahdollista.
6. 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.
7. 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 securingthehuman.sans.org/ouch/archives.

Uutiskirjeen kääntäjä Kirill Filatov (KTM) on GIAC-sertifioitu tietoturvaa rakastava, kokenut IT-ammattilainen. Kirill turvaa tällä hetkellä Nebula Oy:n asiakkaiden liiketoimintaa konsultoimalla ja kehittämällä asiakkaiden tietoturvaviitekehyksiä ja toimintamalleja.

Lähteet

Salasananhallintasovellus: https://securingthehuman.sans.org/ouch/2015#october2015

Kaksivaiheinen tunnistautuminen: https://securingthehuman.sans.org/ouch/2015#september2015

Lock Down Your Login: https://lockdownyourlogin.com

SANS SEC301 – Viiden päivän kurssi kyberturvallisuuden perusasioista: https://sans.org/sec301

Lisenssi