Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Sosiaalinen Media

Yleiskatsaus

Sosiaalisen median sivustot, kuten Facebook, Twitter, Instagram ja LinkedIn ovat mahtavia resursseja, jotka mahdollistavat muiden kanssa kommunikoinnin, kanssakäymisen ja monimuotoisen sisällön jakamisen ympäri maailman. Kaikilla näillä sivustoilla piilee kuitenkin riskejä, jotka kohdistuvat, ei vain sinuun, vaan myös perheeseesi, ystäviisi ja työnantajaasi. Tässä uutiskirjeessä kerromme näistä vaaroista ja miten pystyt toimimaan turvallisesti eri sosiaalisen median foorumeilla.

Vierastoimittaja

Tanya Baccam on pitkän uran tehnyt turvallisuuskonsultti. Hän on kirjoittanut ja kouluttanut SANS:lla jo yli kymmenen vuotta, mm. kursseilla: SEC502, SEC542, SEC401, MGT414 ja AUD507. Voit seurata häntä Twitterissä **@tbaccam**.

Yksityisyys

Yleisin huolenaihe sosiaalisessa mediassa on riittävä yksityisyyden ja henkilökohtaisten tietojen suojaaminen. Tähän liittyviä mahdollisia uhkia ovat:

- **Vaikutus tulevaisuuteesi**: Monet yritykset etsivät tietoa sosiaalisesta mediasta osana rekrytointia. Nolot tai jopa rikolliset kuvat tai päivitykset riippumatta siitä kuinka vanhoja ne ovat saattavat estää ylenemisen, työpaikan saamisen tai pahimmassa tapauksessa johtaa jopa irtisanomiseen. Lisäksi nykyisin monet koulut ja yliopistot tekevät samanlaisia tarkistuksia sosiaalisesta mediasta. Yksityisyysasetukset eivät välttämättä suojele sinua tältä, koska kun ”pidät” jostain organisaatiosta tai liityt heidän seuraajakseen, monet statuspäivityksesi ja kuvasi saattavat muuttua heille näkyviksi vaikka yksityisyysasetukset alun perin tämän estäisivät.
- **Hyökkäykset sinua kohtaan**: Kyberhyökkääjät saattavat analysoida päivityksiäsi ja käyttää näitä sinua tai työnantajaasi vastaan. Jakamasi tieto saattaa myös toimia vastauksena salasanan nollaamiseen vaadittaviin itse asettamiisi ”henkilökohtaisiin kysymyksiin”. Tiedon avulla voidaan myös luoda kohdistettuja kalastelusähköposteja (keihästyshyökkäys=spear phishing), tai hyökkääjä voi käyttää saamaansa tietoa esiintyessään sinuna hyökätessään muita kohtaan. Lisäksi sosiaalisesta mediasta voi löytyä tietoja, jotka paljastavat reaalimaailman tietoja sinusta, kuten asuinpaikan tai työpaikan yhteystiedot.
- **Työnantajasi vahingoittaminen**: Rikolliset tai kilpailijat voivat käyttää työnantajaasi vastaan sitä luottamuksellista tietoa mitä olet jakanut verkossa yrityksestäsi. Lisäksi julkaisemasi päivityksesi saattavat vaikuttaa negatiivisesti työnantajan maineeseen. Varmista yrityksesi tietoturvapolitiikasta tai vastaavasta ohjeistuksesta ennen kuin tuotat internettiin sisältöä joka liittyy millään tavalla työhösi. Huomaa, että työnantajasi saattaa monitoroida sosiaalisen median käyttöä.

Sosiaalinen Media

Paras suojautumiskeino näiltä uhkatilanteilta on rajoittaa asioita, joita jaat internettiin. Yksityisyysasetukset suojaavat sinua tiettyyn rajaan asti, mutta ne ovat usein monimutkaisia ja muuttuvat jopa tietämättäsi. Asiat, joiden uskot olevan yksityisiä saattavat muuttua julkisiksi näiden asetusten muuttuessa. Muista, että tietosi ovat vain yhtä yksityisiä kuin niiden ihmisten yksityisyysasetukset, joiden kanssa jaat sisältöä. Mitä useammalle ihmiselle jaat tietoa, sen julkisemmaksi päivityksesi muuttuvat. Kannattaa aina lähteä siitä oletuksesta, että kaikki verkkoon tuottamasi sisältö saattaa muuttua julkiseksi ja jäädä verkkoon pysyvästi.

Viimeisenä, tarkkaile mitä tuttavasi postaavat sinuun liittyen. Jos huomaat, että sinusta on jaettu sellaista sisältöä mitä et halua julkisuuteen, pyydä sen jakajaa poistamaan kyseinen sisältö. Mikäli he eivät suostu, ota yhteyttä sosiaalisen median sivuston ylläpitäjiin ja pyydä heitä poistamaan sisältö. Toisaalta, ota omissa päivityksissäsi aina huomioon muut ihmiset ja se mitä sisältöä jaat heihin liittyen.



Sosiaalisen median sivustot ovat hauskoja ja vaikuttavia medioita, mutta varo mitä jaat ja kenelle.

Turvallisuus

Yksityisyyteen liittyvien huolien lisäksi, alla on lueteltu joitakin keinoja suojata sosiaalisen median tilejäsi ja verkkotoimintaasi.

- **Kirjautuminen**: Suojaa jokainen tilisi vahvalla, uniikilla salasanalla, äläkä jaa niitä kenellekään muulle. Lisäksi monet sivustot mahdollistavat vahvan kirjautumisen, kuten kaksivaiheisen tunnistautumisen, käytä näitä aina kun mahdollista. Älä käytä sosiaalisen median kirjautumistietojasi kirjautuessasi muille sivustoille, sillä jos käyttäjätietosi päätyvät vääriin käsiin, vaarantuvat kaikki muutkin sivustot.
- **Yksityisyysasetukset**: Jos käytät yksityisyysasetuksia, katselmoi ja testaa niitä säännöllisesti. Sosiaalisen media foorumit muuttavat usein yksityisyysasetuksiaan ja siksi niiden kanssa on helppo tehdä virheitä. Lisäksi, useat sovellukset ja palvelut sallivat sinun merkitä sijaintisi päivittämääsi sisältöön (geotagging). Tarkasta säännöllisesti nämä asetukset mikäli haluat pitää sijaintisi yksityisenä tietona.
- **Suojaus**: Sosiaalisessa mediassa käytetään usein HTTPS salausta turvaamaan yhteytesi sivustolle. Sivustot kuten Twitter ja Google+ aktivoivat HTTPS salauksen automaattisesti, kun taas muut sivustot voivat vaatia sinua aktivoimaan toiminnon manuaalisesti. Tarkista sosiaalisen median tiliesi käyttöasetukset ja aktivoi HTTPS ensisijaisena yhteytenä aina kun se on madollista.
- **Sähköposti**: Suhtaudu epäilevästi aina sähköposteihin, jotka näyttävät tulevan sosiaalisen media sivustoilta, kyberrikolliset saattavat käyttää näitä osana hyökkäystään. Turvallisin tapa vastata tällaisiin viesteihin on kirjautua suoraan sisälle sosiaalisen median tilillesi ja tämän jälkeen lukea ja vastata viesteihin sekä notifikaatioihin suoraan verkkosivulta.
- **Haitalliset linkit**: Muista varoa epäilyttäviä linkkejä ja mahdollisia huijauksia, joita muut ovat jakaneet sosiaalisessa mediassa. Rikolliset käyttävät usein sosiaalista mediaa levittääkseen omia hyökkäyksiään ja haitallista sisältöä. Vain koska joku tuttusi on jakanut sisällön tai lähettänyt sinulle viestin, ei tarkoita että se on tosiasiassa heiltä, sillä kyberrikollinen on

Sosiaalinen Media

saattanut ottaa heidän tilinsä haltuunsa. Jos ystäväsi tai perheenjäsenesi lähettää oudon viestin, jonka todenmukaisuutta et pysty varmistamaan (kuten, että heidät on ryöstetty ja he pyytävät sinulta rahaa), soita heille tai selvitä muilla keinoilla, että viesti on todellakin heiltä.

- **Mobiilisovellukset**: Useimmat sosiaalisen median sivustot tarjoavat mobiilisovelluksen, jolla voit käyttää kätevästi tiliäsi. Varmista, että lähde josta lataat sovelluksia on tunnettu ja luotettava sivusto ja, että älypuhelimesi on suojattu vahvalla salasanalla. Mikäli älypuhelimessasi ei ole lukitusta aktivoituna ja hukkaat sen, kuka tahansa pääsee käsiksi sosiaalisen median tileillesi puhelimesi kautta ja voi käyttää tilejäsi nimissäsi.

Sosiaalisen median sivustot ovat mahtava tapa kommunikoida ja pitää yhteyttä muihin. Jos noudatat uutiskirjeessämme listattuja vinkkejä, tulisi sinun pystyä turvallisin mielin nauttimaan sosiaalisen median hyödyistä. Oppiaksesi lisää siitä miten käytät sosiaalisen median foorumeita turvallisesti ja miten voit raportoida epäilyttävistä asioista, navigoi kyseisen sivuston turvallisuus-osioon.

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

Salasanalausekkeet:	http://www.securingthehuman.org/ouch/2015#april2015
Kaksivaiheinen tunnistautuminen:	http://www.securingthehuman.org/ouch/2013#august2013
Mobiilisovellusten turvallinen käyttö:	http://www.securingthehuman.org/ouch/2015#january2015
Kyberturvallisuusasioiden opettaminen lapsille:	http://www.securingthehuman.org/ouch/2015#june2015
Facebook turvallisuus:	https://www.facebook.com/safety

Lisenssi

 Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy

