Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Auta muita turvaamaan itsensä

Yleiskatsaus

Suurin osa meistä käyttää päivittäin luontevasti erinäisiä teknologiota ja useimmiten osaamme käyttää niitä suhteellisen turvallisesti. Jokaisella on varmasti tuttuja tai sukulaisia, joilla nämä asiat eivät ole hallussa niin hyvin ja on niitäkin joita teknologioiden käyttö ahdistaa. Kyberturvallisuuden ei tarvitse olla pelottavaa tai ahdistavaa, päinvastoin perusasiat ovat suhteellisen yksinkertaisia ja he todennäköisesti vain tarvitsevat vähän osaavan henkilön apua oikeanlaisten toimintatapojen ja alkeiden kanssa.

Vierastoimittaja

Randy Marchany (Twitter: **@randymarchany**) toimii tietoturvajohtajana Virginia Tech-yliopistossa ja sertifioituna SANS- ohjaajana.

Viisi yksinkertaista askelta

Alla on listattu viisi yksinkertaista askelta joita voit käyttää pohjana, kun keskustelet muiden kanssa heidän verkkokäyttönsä turvaamisesta. Uutiskirjeen lopussa on lisäksi listattu lähteitä joista saat lisätietoa alla mainituista asioista.

1. **Sosiaalinen hakkerointi**: Sosiaalinen hakkerointi on hakkereiden yleisesti käyttämä tekniikka, jossa huijataan tai ohjataan ihmisiä tekemään jotain mitä heidän ei pitäisi tai jota he eivät halua tehdä. Esimerkiksi jakamaan salasanansa, saastuttamaan laitteensa tai jakamaan luottamuksellista tietoa. Tämän tyyppisessä toiminnassa ei itsessään ole mitään uutta, erinäiset huijarit ovat jo tuhansien vuosien ajan käyttäneet samoja tekniikoita tavoitteidensa saavuttamisessa. Ainoa ero on, että tässä tapauksessa huijaaminen tapahtuu verkossa. Voit auttaa muita selittämällä yleisimmät tavat huomata sosiaalinen hakkerointiyritys, kuten kiireellisyyden tunteen luominen, liian hyvät tarjoukset tai epäjohdonmukaisuudet viesteissä. Kerro esimerkkejä sosiaalisesta hakkeroinnista, kuten kalasteluviesteistä tai kuuluisasta Microsoftin tekniset tuen puhelusta. Jos voit välittää vain yhden asian, niin yritä saada tuttusi ymmärtämään se, etteivät he antaisi salasanaansa koskaan kenellekään.
2. **Salasanat**: Vahvat salasanat ovat kriittisessä asemassa laitteiden ja tilien suojaamisen kannalta. Selitä perheenjäsenillesi miten vahvoja salasanoja luodaan esim. salasanalausekkeiden avulla ja auta heitä salasanojen

Auta muita turvaamaan itsensä

hallintaohjelman asentamisessa ja käytössä. Muista, että salasanan pitää olla eri jokaisella tilillä ja laitteella. Jos salasanojen hallintaohjelman käyttö aiheuttaa haasteita, opeta heidät kirjoittamaan salasanansa paperille ja säilyttämään paperia turvallisessa paikassa. Selitä myös miten kaksivaiheinen tunnistautuminen toimii, ja opeta sen käyttöönotto tärkeimmillä tileillä.

3. **Päivittäminen**: Järjestelmien ajan tasalla pitäminen ja päivittäminen on yksi tärkeimpiä asioita tietoturvan ylläpitämisessä. Tämä pätee kaikkiin tietokoneisiin ja mobiililaitteisiin, mutta lisäksi kaikkiin muihinkin laitteisiin, erityisesti niihin jotka ovat yhteydessä verkkoon, kuten reitittimet, pelikonsolit ja kaikki IoT-laitteet. Laitteissa kannattaa pitää päällä automaattista päivittämistä aina kun mahdollista.
4. **Anti-Virus**: Ihmiset tekevät virheitä, joskus klikkaamme jotain mitä ei olisi pitänyt tai asennamme jotain mikä on haitaksi laitteellemme. Anti-virus ohjelmat suojaavat meitä tällaisilta virheiltä. Vaikka nämä ohjelmat eivät estä kaikkia haittaohjelmia, ne pysäyttävät ja estävät suurimman osan yleisimmistä hyökkäyksistä. Tämän vuoksi kannattaa varmistaa, että kaikissa kotilaitteissa on asennettuna viimeisin versio anti-virus ohjelmasta ja että se päivittyy automaattisesti. Kannattaa myös käyttää anti-virus ohjelmien lisäominaisuuksia, kuten palomuureja ja selainsuojia.
5. **Varmistukset**: Kun kaikki muu pettää, varmistukset ovat yleensä ainoa keino palauttaa tietosi kyberhyökkäyksen tai inhimillisen virheen jälkeen. Varmista, että tuttusi ja perheenjäsenesi käyttävät automaattisia varmistuspalveluita. Usein yksikertaisin tapa on käyttää pilvipalveluita, jotka varmistavat laitteet ja tiedot automaattisesti säännöllisin väliajoin. Näiden palveluiden avulla varmistaminen ja myös palauttaminen on erittäin helppoa.

Auta muita turvaamaan itsensä jakamalla heidän kanssaan viisi helppoa askelta.

Lasten suojaaminen kodin ulkopuolella

Jos käytät teknologiaa sujuvasti, olet varmasti turvannut oman ja lapsesi verkkokäytön ja palvelut. Lapsesi kuitenkin käyvät kylässä kavereiden tai sukulaisten luona, jotka eivät välttämättä panosta tietoturvaan niin paljon. Voit turvata lastesi turvallisuuden tässä tapauksessa näillä yksinkertaisilla keinoilla:

- **Säännöt**: Varmista, että muut tietävät lapsellesi asettamista rajoista ja säännöistä. Jos olet määritellyt kuinka pitkään lapsesi saa olla kerrallaan verkossa tai pelata, kerro tämä, kun lapsi kyläilee muualla. Voit olla melko

Auta muita turvaamaan itsensä

varma, että lapsesi yrittää unohtaa määritellyt säännöt vierailun aikana, joten siihen ei kannata luottaa. Voit kirjoittaa säännöt ja ohjeet paperille ja antaa paperin lapselle mukaan hänen kyläillessään muualla.

- **Hallinta**: Jos lapsesi ymmärtää teknologiaa paremmin kuin sinä, hän saattaa käyttää osaamista hyväkseen. Lapsi saattaa pyytää tai hankkia itselleen pääkäyttäjätunnukset isovanhempien koneelle ja sitten tehdä koneella asioita mitä heidän ei ole tarkoitus tehdä, kuten asentaa pelejä joita hänen ei ole tarkoitus pelata. Varmista, että sukulaisesti ymmärtävät tämän, eivätkä anna lapsille mitään lisäoikeuksia tai päästä käyttämään koneita valvomatta.

Suosittele sukulaisille ja tuttaville liittymään OUCH! -uutiskirjeen tilaajiksi, jotta he saavat lisättyä tietoturvatietouttaan ja oppimaan lisää. Tätä uutiskirjettä julkaistaan kuukausittain 20:llä eri kielellä. Tilaa osoitteessa: https://securingthehuman.sans.org/ouch.

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

Sosiaalinen hakkerointi:	https://securingthehuman.sans.org/ouch/2017#january2017
Salasanalausekkeet:	https://securingthehuman.sans.org/ouch/2017#april2017
Salasanojen hallintaohjelma:	https://securingthehuman.sans.org/ouch/2017#september2017
Kaksivaiheinen tunnistautuminen:	https://securingthehuman.sans.org/ouch/2015#september2015
Varmistus ja palautus:	https://securingthehuman.sans.org/ouch/2017#august2017
Lasten verkkokäytön turvaaminen:	https://securingthehuman.sans.org/ouch/2017#may2017

Lisenssi

 Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley Käännös suomeksi: Kirill Filatov, Senior Security Consultant, Nebula Oy