Turvallisen kotoa käsin työskentelyn 5 tärkeintä askelta

Tiedämme, että kotoa käsin työskentely voi olla uutta joillekin teistä. Uuteen työympäristöön sopeutuminen voi tuntua jopa ylivoimaiselta. Yhtenä tavoitteistamme on varmistaa, että työskentely kotona sujuisi mahdollisimman turvallisesti. Käymme alla läpi viisi yksinkertaista keinoa, joilla turvallinen työskentely onnistuu. Parasta näissä ohjeissa on se, että työn suojaamisen lisäksi ne auttavat suojaamaan myös sinua ja perhettäsi luomalla kyberturvallisen kodin.

Sinä: Ensimmäisenä on syytä muistaa, että teknologia ei yksin voi täysin suojata ketään – sinä itse olet paras puolustuskeino. Hyökkääjät ovat oppineet, että usein paras keino saavuttaa tavoite on keskittyä ihmisiin tietokoneiden tai muiden laitteiden sijaan. Jos hyökkääjät haluavat saada käsiinsä salasanan, työhön liittyviä tietoja tai tietokoneen hallinnan, he yrittävät huijata uhrinsa antamaan ne, usein luomalla kiireen tunteen. Hyökkääjä voi esimerkiksi soittaa tekeytyneenä Microsoftin tekniseksi tueksi ja väittää työtietokoneen olevan saastunut. Tai ehkä hyökkääjä lähettää sähköpostia, jossa kertoo, että postipakettia ei voitu toimittaa, mikä saattaa saada uhrin napsauttamaan haittalinkkiä. Yleisimpiä manipulointihyökkäysten tunnusmerkkejä:

- Suuri kiireen tunne, joka luodaan pelottelemalla, uhkailemalla, kriisitilanteella tai tärkeän määräajan sulkeutumisella. Kyberhyökkääjät ovat taitavia luomaan vakuuttavia viestejä, jotka vaikuttavat tulevan luotettavilta organisaatioilta, kuten pankeilta, viranomaisilta tai kansainvälisiltä organisaatioilta.
- Painostus tietoturvakäytäntöjen tai -toimintatapojen ohittamiseen, tai tarjous, joka on liian hyvä ollakseen totta (ei, sinä et voittanut lotossa).
- Viesti, joka vaikuttaa tulevan ystävältä tai kollegalta, mutta jonka allekirjoitus, sävy tai sanavalinnat eivät kuulosta oletetulta lähettäjältä.

Paras puolustus tällaisia hyökkäyksiä vastaan olet sinä.

Kotiverkko: Lähes jokaisen kotiverkon perusta on langaton verkko (Wi-Fi-verkko). Sen avulla kaikki kodin laitteet voivat muodostaa yhteyden internetiin. Useimpia langattomia kotiverkkoja ohjaa reititin tai erillinen Wi-Fi-tukiasema. Molemmat niistä toimivat samalla tavalla: ne lähettävät langattoman signaalin, johon kodin laitteet muodostavat yhteyden. Tämä tarkoittaa, että langattoman verkon suojaaminen on avainroolissa kodin turvaamisessa. Suosittelemme seuraavia toimia verkon suojaamiseen:

- Langatonta verkkoa hallitsevan laitteen ylläpitäjän oletussalasana tulee muuttaa. Ylläpitäjän tilin kautta voi muuttaa langattoman verkon asetuksia.
- Varmista, että vain luotettavat henkilöt voivat muodostaa yhteyden langattomaan verkkoon. Se tehdään ottamalla käyttöön vahva suojaus. Tällöin langattomaan verkkoon voidaan liittyä vain salasanan avulla ja käyttäjien verkkotoiminta on salattua.
- Huolehdi, että langattoman verkon salasana on vahva ja että se eroaa ylläpitäjän salasanasta. Salasana tarvitsee syöttää kuhunkin laitteeseen kuitenkin vain kerran, sillä laitteet tallentavat ja muistavat salasanan.

Askarruttaako, kuinka toimet tehdään? Voit pyytää apua internetpalveluntarjoajalta tai etsiä tietoa palveluntarjoajan verkkosivustolta, tukiaseman mukana tulleista ohjeista tai valmistajan verkkosivustolta.

Salasanat: Kun verkkosivusto pyytää luomaan salasanan, siitä tulee luoda vahva. Mitä enemmän merkkejä salasanassa on, sitä vahvempi se on. Salasanalauseen käyttäminen on yksinkertaisimpia tapoja luoda vahva salasana. Salasanalause on kaikessa yksinkertaisuudessaan vain useista sanoista koostuva salasana, esimerkiksi "*mehiläinen hunaja bourbon*". Yksilöllisen salasanalauseen käyttäminen tarkoittaa eri salasanan käyttämistä kullakin laitteella ja verkkotilillä. Tällä tavoin yhden tilin vaarantuminen ei aseta muita tilejä ja laitteita vaaraan. Tuottaako kaikkien salasanojen muistaminen vaikeuksia?

Käytä salasananhallintaohjelmaa. Kyseessä on ohjelma, joka on suunniteltu tallentamaan turvallisesti kaikki salasanalauseet salatussa muodossa (ja niissä on paljon muitakin hyviä ominaisuuksia). Käyttöön tulee myös ottaa kaksivaiheinen todennus (kutsutaan myös esimerkiksi monivaiheiseksi

tunnistautumiseksi) aina kun mahdollista. Silloin käytössä on salasana, mutta mukaan lisätään toinen vaihe, esimerkiksi älypuhelimeen lähetettävä koodi tai sovellus, joka luo koodin. Kaksivaiheinen todennus on todennäköisesti tehokkain keino suojata verkkotilejä, ja sen käyttäminen on paljon helpompaa, kuin miltä saattaa kuulostaa.

Päivitykset: Huolehdi, että kaikki tietokoneet, mobiililaitteet, ohjelmat ja sovellukset ovat aina päivitettyinä uusimpiin ohjelmistoversioihin. Kyberhyökkääjät etsivät herkeämättä haavoittuvuuksia laitteidesi käyttämissä ohjelmistoissa. Kun haavoittuvuus löytyy, hyökkääjät käyttävät erikoisohjelmia haavoittuvuuksien hyödyntämiseen ja hakkeroivat käytössäsi olevat laitteet. Laitteiden ohjelmistot luoneet yhtiöt puolestaan uurastavat jatkuvasti korjatakseen haavoittuvuudet julkaisemalla päivityksiä. Varmistamalla, että tietokoneet ja mobiililaitteet asentavat päivitykset viipymättä, laitteiden hakkerointi vaikeutuu huomattavasti. Laitteet pysyvät ajan tasalla, kun automaattiset päivitykset kytketään päälle. Tämä sääntö sopii lähes kaikkiin laitteisiin, jotka on yhdistetty verkkoon, mukaan lukien työlaitteisiin, televisioon, itkuhälyttimiin, turvakameroihin, kotireitittimiin, pelikonsoleihin ja jopa autoihin.

Lapset/vieraat: Toimistolla joutuu harvoin huolehtimaan siitä, pääsevätkö lapset, vieraat tai muut perheenjäsenet käsiksi työtietokoneeseen tai muihin työlaitteisiin. On syytä pitää huolta, että perheenjäsenet ja ystävät ymmärtävät, etteivät he voi käyttää työlaitteita, sillä he saattavat vahingossa poistaa tai muokata tietoja tai pahimmassa tapauksessa saastuttaa laitteen tahattomasti.