Verkossa liikkujan työkalupakki

Toimi turvallisesti ja vastuullisesti

Viestintävirasto
Kyberturvallisuuskeskus

Sisällysluettelo

Aluksi

Verkossa liikkujan työkalupakki - Toimi turvallisesti ja vastuullisesti antaa vinkkejä ja ohjeita tavallisille internetin käyttäjille. Se voi toimia myös muistilistana verkon eri medioissa liikkuvalle.

Ensimmäisessä luvussa keskitytään siihen, kuinka kommunikoida muun muassa sosiaalisessa mediassa niin, ettei oma verkkojälki tuottaisi pahaa mieltä kenellekään viestinnän osapuolelle.

Aihetta jatketaan myös toisessa luvussa, jossa kerrotaan, kuinka internetissä liikkuva voi pitää hyvää huolta verkkominästään.

Kolmannessa luvussa taas käsitellään verkon kautta saapuvia yhteydenottoja, esimerkiksi sähköposteja, joiden liitteissä voi piillä tietoturvariskejä.

Viimeisessä, neljännessä luvussa kehotetaan pitämään omat laitteet ja ohjelmistot ajantasaisina, mikä onnistuu vain, jos päivityksistä tekee itselleen tavan.

Verkossa liikkujan työkalupakki on alun perin julkaistu Viestintäviraston Kyberturvallisuuskeskuksen www-sivuilla heinäkuussa 2015. Kokonaisuus kuuluu Kyberturvallisuuskeskuksen kuukausittain vaihtuviin Teema-artikkeleihin.

Verkossa liikkujan työkalupakin tarkoituksena on tarjota lukijoilleen 2010-luvulle päivitetty netiketti. Käsitellyt aiheet on valikoitu yhteistyössä Suomi 24:n kanssa.

1 Toimi niin, että voit olla verkkojäljestäsi ylpeä

Sosiaalisessa mediassa turvallisesti ja rehdisti käyttäytyvä ei kiusaa eikä mustamaalaa toisia. Hän myös ymmärtää, että elämä virtuaalimaailmassa ei pääty tähän hetkeen. Tästä syystä tunnekuohut, raivo ja rakkauspuuskat kannattaa jakaa muualla kuin internetissä.

Verkkoon jää aina jälki, eikä nimimerkkikään takaa anonyymiyttä. Esimerkiksi chat-palstalla häiriköivien nimimerkkien oikeat identiteetit on mahdollista selvittää.

1.1 Mieti vielä kerran

Kiukustuneena tai mustasukkaisena tehdyt jaot, kommentit ja väitteet voivat aiheuttaa paljon pahaa, vaikka alkuperäinen tarkoitus olisi ollut jotakin aivan muuta. Aluksi hauskalta tuntuva vitsi tai käytännön pila voi muuttua kunnianloukkaustapaukseksi, josta tekijä saa vastata poliisille.

Jos uskot, että olet asiastasi samaa mieltä myös lähitulevaisuudessa, olet valmis keskustelemaan aiheesta rakentavasti ja teeman julkinen pohdinta on mielestäsi tärkeää, asiasi voi olla somejaon arvoinen.

Kun jaat mielipiteitäsi tai tietoa yleensä, kerro myös lähteesi ja perustele kantasi. Lisäksi moniarvoisuus ja suvaitsevaisuus antavat hyvän perustan esimerkiksi keskustelulle, johon mahdollisimman moni voi osallistua - leimautumista tai vihapuhetta pelkäämättä.

1.2 Yrityksille annettu julkinen palaute ei aina ole totta

Suhtaudu epäillen esimerkiksi keskustelupalstalla annettuun yrityspalautteeseen, etenkin jos se poikkeaa selvästi valtavirrasta. Luotettavaa tietoa etsivä voi myös tarkistaa, millaisia muita kommentteja palautteen antaneen nimimerkin takaa löytyy.

Valitettavasti myös yritykset voivat mustamaalata toisiaan tai kehua palveluitaan julkaisemalla tekaistuja asiakaspalautteita tai -kokemuksia. On täysin mahdollista, että keksittyjen ja ilkeiden kommenttien vuoksi asiakkaita kaikkoaa tai jopa yrityksen liiketoiminta päättyy.

1.3 Täydellinen nettideitti ei tarvitse rahaa

Internetin treffipalvelut ja mobiilisovellukset tarjoavat helppoja tapoja tavata ihmisiä ja etsiä itselle seuraa. Suuret tunteet voivat saada nettideittaajan unohtamaan, että nimimerkin takana oleva ihminen ei välttämättä ole se, joksi itsensä esittää. Kuva, nimi ja elämäntarina voivat kaikki olla valetta, siksi vastapuoleen on hyvä rakentaa luottamusta vähitellen.

Älä siis jaa omia henkilökohtaisia tietojasi julkisesti. Harkitse tietojesi jakamista myös henkilölle, jota et ole koskaan tavannut. Puhelinnumero, nimi ja osoite voivat saada rikolliset liikkeelle, jopa vieraiksi kotiisi ja pankkitilillesi asti.

2 Huolehdi verkkominästäsi

Henkilökohtaisista tiedoistaan ja asioistaan, kuten henkilötunnuksesta, osoitetiedoista, puhelinnumerosta ja valokuvista, kannattaa olla tarkka niin verkossa kuin verkon ulkopuolellakin. Etenkin sosiaalisessa mediassa tulee muistaa, että vaikka kyse on henkilökohtaisesta profiilista, itse media on kuitenkin perusluonteeltaan julkinen.

Jos ulkopuoliset henkilöt pääsevät käsiksi toisen henkilökohtaisiin ja arkaluontoisiin tietoihin, on täysin mahdollista, että tietoja voidaan hyödyntää ilkeämielisesti. Tämä voi aiheuttaa uhrille vähintäänkin ylimääräistä vaivaa ja tahria hänen verkkomainettaan. Pahimmassa tapauksessa tietoja voidaan käyttää epärehellisiin tarkoituksiin, joista koituu harmia tietojen omistajalle vielä vuosienkin kuluttua.

Verkossa toimiessa on hyvä muistaa, että oma verkkominä tai verkkoidentiteetti rakentuu henkilötietojen lisäksi omasta verkkokäyttäytymisestä. Tällä tarkoitetaan henkilön kirjoituksia, kommentteja, tykkäämisiä sekä näihin liittyvää äänensävyä eri foorumeilla ja palveluissa.

Pikaistuksissaan saattaa tulla julkaisseeksi asioita, jotka myöhemmin haluaisi verkosta pois. On tärkeää pitää mielessä, että verkon muisti on lähes ikuinen: esimerkiksi pikaistuksissaan lähetetty kirjoitus, kommentti tai twiitti voi tulla vastaan vuosienkin kuluttua.

2.1 Mieti, mitä tietoja kerrot ja kenelle

Verkkopalveluiden ja sähköpostin välityksellä voit saada yhteydenottoja entuudestaan tuntemattomilta henkilöiltä. Lähettäjän todenperäisyyttä voi olla hankala arvioida, koska verkossa voi tekeytyä toiseksi ja näin harhauttaa toista viestinnän osapuolta.

Yksi kiusanteon muoto on esimerkiksi toisen henkilökohtaisten tietojen ja valokuvien jakaminen osana valeprofiilia. Henkilökohtaisten asioiden uteluihin kannattaakin vastata harkiten, etenkin jos kysyjä on vasta tavattu nettituttu.

Verkkopalveluissa kannattaa huomioida sekä ympäristön avoimuus että yksityisyys. Omien julkaisujen, kirjoitusten ja valokuvien kohderyhmiä voi rajoittaa koskemaan esimerkiksi vain ystäviä. Lisäksi verkkopalveluihin rekisteröityessä ja niitä käytettäessä kannattaa punnita, mitkä tiedot ovat oikeasti tarpeellisia palvelun toteuttamiseksi.

2.2 Älä julkaise muiden materiaalia ilman lupaa

Kun julkaistaan valokuvia, musiikkia ja videoita, on pidettävä huoli, että julkaisijalla on oikeus julkaisemaansa materiaaliin. Toisen materiaalin julkaiseminen omanaan voi aiheuttaa tekijänoikeusrikkomuksen.

Siispä, älä julkaise muista kirjoituksia tai kuvia, joita et haluaisi itsestäsikään julkaistavan. Yleisfiksulla toiminnalla ennaltaehkäisee monta harmia ja riitatilannetta.

3 Tarkastele saamiasi yhteydenottoja

Sähköpostiin, sosiaalisen median palveluihin ja muihin verkkopalveluihin saattaa tulla erikoisia ja epäilyttävän oloisia yhteydenottoja.

Yhteydenotot saattavat tulla entuudestaan tuntemattomilta, mutta myös omilta kavereilta ja kontakteilta. Kaikissa tapauksissa on syytä suhtautua varoen erilaisiin linkkeihin, liitetiedostoihin ja pyyntöihin. Myös omalta kaverilta tuleva epäilyttävä viesti voi olla osa huijausta, jos esimerkiksi hänen käyttäjätilinsä on joutunut vääriin käsiin.

3.1 Varmistu viestin aitoudesta ja lähettäjästä

Oletko varma, että saamasi sähköpostin lähettäjä ja lähettäjän osoite ovat aitoja? Sähköpostiosoitteen nimikenttä on helppo väärentää näyttämään joltain muulta, kuin mitä se todellisuudessa on. Jos viestin sähköpostiosoite tuntuu epäilyttävältä, kannattaa koko viestin sisältöönkin suhtautua epäilevästi. Epäilyttäviä viestejä ei tulisi lähettää eteenpäin mahdollisten vahinkojen minimoimiseksi.

Viestin aitoutta ei siis voi päätellä vain lähettäjän nimestä tai sähköpostiosoitteesta. Yritysten nimissä lähetetyistä viesteistä kannattaa tarkkailla esimerkiksi viestin ulkoasua ja kielioppia. Kielioppivirheet ja kömpelö grafiikka saattavat olla viitteitä tietoja kalastavista huijareista. Epäilys viestin aitoudesta pitäisi herätä myös, jos yrityksen nimi on entuudestaan tuntematon eikä vastaanottaja muista antaneensa yritykselle yhteystietojaan.

Yrityksen laillisuutta voi yrittää selvittää esimerkiksi yrityksen kotisivuilta, jos vain sellaiset on olemassa. Myös verkossa olevasta Patentti- ja rekisterihallituksen sekä verohallinnon Yritys- ja yhteisötietojärjestelmästä (YTJ) voi olla apua.

Käyttäjätunnuksia, salasanoja ja verkkopankkitunnuksia ei tule antaa sähköpostin tai puhelimen välityksellä, eivätkä yritykset niitä siten pyydäkään. Liian hyvältä vaikuttavat lupaukset ovat usein osa huijareiden taktiikkaa. Jos viestissä pyydetään tai luvataan rahaa, tulisi epäilyksen herätä.

3.2 Älä hätäile - Mieti ennen kuin klikkaat

Jos saamassasi yhteydenotossa on mukana linkki tai liitetiedosto, harkitse ennen kuin klikkaat. Jo näin yksinkertaisin keinoin pystyy parantamaan omaa verkkoturvallisuuttaan.

Linkin osoittamasta kohteesta voi ottaa selvää esimerkiksi laittamalla hiiren osoittimen linkin päälle, jolloin useimmat ohjelmat näyttävät linkin kohteen selainikkunassa tai sen alareunassa. Jos taas tutulta tullut sähköpostiviesti liitetiedostoineen on jostakin syystä epäilyttävä, varmista, että viesti on aito ennen kuin avaat liitetiedoston.

Tuntemattomilta ihmisiltä tulevia sähköpostin liitetiedostoja ei ylipäänsä tulisi avata. Myöskään tuntemattomien ihmisten yhteydenottoja ei tarvitse hyväksyä sosiaalisen median palveluissa, etenkään jos yhteydenotto on yhtään epäilyttävä.

4 Tee päivityksistä tapa

Ajantasaiset ohjelmistot ja työkalut ovat tärkeä osa omaa verkkoturvallisuutta. Ne myös tekevät mahdolliseksi viimeisimpien verkkopalveluiden käytön.

Ohjelmistot pysyvät ajantasaisina vain, jos niihin asentaa niin sanotut ohjelmistopäivitykset. Ne koostuvat turvallisuuteen, suorituskykyyn, ohjelmointivirheisiin ja toiminnallisuuteen liittyvistä parannuksista.

Suurin osa päivityksistä liittyy turvallisuuden parantamiseen. Jättämällä tietoisesti ohjelmistonsa ja laitteensa päivittämättä, käyttäjä altistaa itsensä ja laitteensa monille erityyppisille uhkille. Kannattaa pitää myös mielessä, että osa verkkopalveluista ei toimi, jos uusimmat ohjelmistoversiot ja -komponentit eivät ole käytössä. Vanha ohjelmistoversio voi estää verkkopalvelun käytön.

4.1 Mitä päivitetään?

Tärkeimpiin tietoturvapäivityksiin lukeutuvat:

- antivirus- ja turvallisuusohjelmien päivitykset
- webselaimet ja niiden liitännäiset
- käyttöjärjestelmät,
- ohjelmistot sekä
- mobiililaitteiden päivitykset.

Niin sanotuilla pienimuotoisilla päivityksillä parannetaan tietoturvaa ja suorituskykyä. Laajemmat päivityskokonaisuudet koskevat usein yleistä ohjelmistokehitystä, jolloin ohjelmisto saa uusia ominaisuuksia tai sen käyttöliittymää uudistetaan. Usein päivityspakettien yhteydessä mainitaan suurimmat kokonaisuudet, joita päivitys koskee.

Kun tuote tai laite tulee elinkaarensa päähän, sen valmistaja ei enää tuota siihen päivityksiä. Tällöin se tulee vaihtaa sellaiseen versioon tai täysin uuteen kokonaisuuteen, jonka kehitystä ja turvallisuutta tuetaan jatkossakin.

4.2 Miten päivitän?

Useimmat ohjelmat tarjoavat automaattisia päivityksiä, jolloin käyttäjän ei itse tarvitse huolehtia päivityspakettien etsimisestä. Samalla käyttäjä voi olla varma, että ajan tasalla olevat ohjelmistoversiot ovat käytössä ja päivitysten asentaminen ei unohdu.

Usein automaattinen päivitys tulee kytkeä päälle ohjelman asetuksista. Automaattiset päivitykset hakevat itse päivityksensä verkosta, mutta voivat vaatia myös käyttäjältä toimia päivitysten loppuun saattamiseksi. Tällöin laitteen ruudulle usein ilmestyy merkki-ikoni tai ikkuna ilmaisemaan, että uusi päivitys on saatavilla ja asennettavissa. Joissakin ohjelmissa päivitysikoni ilmestyy ruudulla näkyvään tehtäväpalkkiin ja vaatii käyttäjältä toimia päivityksen asentamiseksi. Järjestelmäpäivityksissä tietokone tai mobiililaite saattaa vaatia laitteen uudelleen käynnistämistä päivityksen jälkeen.

4.3 Päivityksillä voidaan myös huijata

On hyvä tietää, että joillakin haitallisilla verkkosivuilla voi saada näytölleen ponnahdusikkunoita, jotka varoittavat tietokoneelta löytyneestä viruksesta tai muistuttavat ohjelmistopäivityksestä.

Näitä selaimesta ponnahtavia ikkunoita ei kuitenkaan pidä klikata, vaikka ne ulkoasultaan muistuttaisivat käyttöjärjestelmän tai oheisohjelmistojen päivitysikkunoita. Jos päivitysilmoitus vaikuttaa epäilyttävältä, kannattaa vierailla ohjelmistovalmistajan kotisivuilla ja etsiä tietoa päivityksestä sen aitouden varmistamiseksi.

Yhteystiedot
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi