Matti Laakso

ARJEN DIGITURVAN TEHOKUURI

12 valmista blogikirjoitusta, joilla nostat henkilöstösi digiturvaosaamista

Lisää vinkkejä organisaatiosi digiturvallisuuden kehittämiseen löydät osoitteesta Tietojesiturvaksi.fi

Miksi tarvitset tämän tehokuurin?

Onko vastuullasi **henkilöstön digiturvaosaamisen ylläpitäminen?** Olet varmasti huomannut, että se on pitkäjänteistä ja työlästä tekemistä.

Tämä blogipaketti helpottaa arkeasi!

Tässä sinulle 12 valmista blogikirjoitusta, joiden avulla voit nostaa henkilöstön digiturvaosaamista. Tehokuuri sisältää koko vuoden blogijulkaisut yhdessä paketissa!

Tiedätkö kollegan, joka voisi hyötyä tehokuurista? Laita kopio menemään hänellekin!

Tekstejä voi käyttää vapaasti organisaation sisäisissä kanavissa.

Muokkaa, leikkaa, liitä, tiivistä tai täydennä ihan miten haluat. Tuo mukaan esimerkkejä omasta organisaatiostasi tai uutisista. Lisää kuvia ja omia huomioitasi.

Julkaise tekstit omalla nimelläsi, jolloin blogit ovat sinulta muille. Minun nimeäni ei tarvitse mainita! Jos haluat mainita nimeni, niin tee lähdeviittaus tähän julkaisuun.

Olisi kuitenkin kiva kuulla, missä kaikkialla **Arjen digiturvan tehokuuria** hyödynnetään. Laita samalla palautetta tulemaan. Yhteystiedot löytyvät blogistani Tietojesiturvaksi.fi

Terveisin

Matti

Sisältö

Missä järjestyksessä tekstit kannattaa julkaista?

Blogitekstit voi julkaista ihan missä järjestyksessä tahansa. Tässä kaksi ehdotusta:

1) Yleiskuvasta yksityiskohtiin

Jos haluat aloittaa julkaisun digiturvan yleiskuvasta ja edetä sitten yksityiskohtaisempiin aiheisiin, etene sisällysluettelon mukaisessa järjestyksessä.

2) Kuukausikohtainen teemajulkaisu

Osa blogiteksteistä sopii hyvin tiettyihin kuukausiin. Katso oheisesta listasta, mitä tekstiä suosittelen eri kuukausille ja miksi.

Tammikuu: Tietosuoja on suunnitelmallisuutta ja arjen tekoja. Tietosuojapäivää vietetään 28.1.

Helmikuu: Etätyöskentely ja matkustaminen. Matkustelun ja työn yhdistäminen.

Maaliskuu: Miksi ihminen on tietoturvan vahvin lenkki?

Huhtikuu: Etäkokoukset, puhelut ja keskustelut – huomioi nämä turvallisuusasiat.

Toukokuu: Arjen tietoturvan muistilista.

Kesäkuu: Mikä on toimitusjohtajahuijaus? Varoitus aiheesta ennen kesälomia.

Heinäkuu: Älypuhelin on tärkeä – suojele sitä!

Elokuu: Salasanat on arjen digiturvan perusta. Loman jälkeen salasana on usein unohtunut.

Syyskuu: Huijausviestin tunnistaminen – Mikä tekee viestistä epäilyttävän? Muistetaan nämä syksyn kiireissä.

Lokakuu: Tietoturvaosaaminen kasvaa yhteistyöllä! Suomessa Digiturvaviikko ja Euroopassa Kyberturvakuukausi.

Marraskuu: Miksi sähköposti on huono väline tiedon jakamiseen?

Joulukuu: Toimitilaturvallisuus on muutakin kuin digiä!

Vinkki: Tekstit on suunniteltu julkaistavaksi intrassa. Jos bloggaaminen ei sovi työpaikallesi, niin vaihda välinettä. Pilko tekstit pienempiin palasiin, niin saat muodostettua useampia sähköposteja tai yhteistyöalustoille sopivia julkaisuja.

1. Arjen tietoturvan muistilista

Tietoturva on todella tärkeä asia organisaatiomme toiminnan kannalta. Mutta miten sitten huolehdimme tietoturvasta arjen kiireiden keskellä? Miten pidämme tiedot, laitteet, järjestelmät ja ihmiset turvassa? Pääsemme pitkälle, kun muistamme perusasiat!

Arjen tietoturvan muistilista:

Työlaitteet

- Työlaitteet ovat vain minun käyttööni. Säilytän laitteita huolellisesti.
- Asennan päivitykset viipymättä.
- Salasanani ja käyttäjätunnukseni on eri töissä kuin vapaa-ajalla.
- Koneelta poistuessani painan Win+L
- Mobiililaitteessani on lukituskoodi.

Tiedot ja järjestelmät

- Avaan vain työtehtäviini liittyviä tietoja.
- Jaan käyttöoikeudet muille työtehtävien perusteella.
- Lähetän viestit turvapostilla tai muuten salattuna.
- Tunnistan epäilyttävän viestin. Tarkistan viestin aitouden lähettäjältä.
- Käytän vain työpaikkani hyväksymiä tallennuspaikkoja ja ohjelmistoja.
- Tietosuojaroskis on oikea paikka luottamuksellisten asiakirjojen hävittämiseen.

Työpaikan yhteiset käytännöt

- Noudatan puhtaan pöydän periaatetta: en säilytä henkilötietoja tai muita tärkeitä tietoja näkyvillä työpöydällä.
- Avaimet, kulkulätkät ja käyttäjätunnukset ovat henkilökohtaisia.
- Käytän henkilökorttia työpaikalla, jotta minut tunnistetaan.
- Vierailijani ovat minun vastuullani.
- Olen tarkkana, kuka näkee tai kuulee arkaluonteisia tietoja.
- Ilmoitan tietoturvahavainnot ja -ongelmat viipymättä esihenkilölle.

2. Salasanat on arjen digiturvan perusta

Salasanat ovat varmasti yksi IT- ja tietoturvamaailman puuduttavimmista puheenaiheista. Perusjuttujen lisäksi kerron ohessa muitakin näkökulmia, esim. mitä rikolliset tekevät salasanoilla ja mitä hyötyä unohtuneesta salasanasta on.

Salasanoilla on merkittävä rooli meidän kaikkien digiturvallisuudessa. Salasana-asioista puhutaan paljon, mutta tälle on hyvä syy: verkkorikolliset haluavat sinun salasanasi. Paluu työpaikalle on hyvä tilaisuus tarkastella omia ja työpaikan salasanakäytäntöjä.

Miksi rikolliset haluavat salasanoja?

Rikollinen haluaa muuttaa sinun käyttäjätunnuksesi rahaksi. Rikollinen hyödyntää kaapattuja käyttäjätunnuksia ja salasanoja rikosten valmistelussa ja toteuttamisessa. Rikollinen testaa:

Voiko kaapatulla salasanalla kirjautua esimerkiksi sähköpostiin?

Pääseekö samalla salasanalla muihinkin palveluihin?

Käyttääkö joku muu yrityksessä samaa salasanaa?

Rikollinen käyttää kaapattua tunnusta esimerkiksi huijauksiin ja tiedon keräämiseen. Hän voi myydä tunnukset toisille rikollisille, jotka esimerkiksi pyrkivät saamaan kiristyshaittaohjelman yrityksen järjestelmiin. On helpompi kirjautua sisään kuin hakkeroitua sisään.

Salasanat suojaavat sinua, muita työntekijöitä ja yrityksesemme tietojärjestelmiä rikollisilta.

Millaiset salasanakäytännöt sinulla on?

Mieti seuraavaksi näitä asioita omasta näkökulmastasi. Onko salasanasi:

- helppo muistaa,
- vaikea arvata, ja
- eri joka paikassa?

Vielä kun se sisältää erilaisia merkkejä eikä löydy sanakirjasta sellaisenaan, niin ollaan erittäin turvallisen salasanan äärellä!

Salasanan vaihtaminen esim. 6kk välein vaikuttaa siihen, että kerran varastettu tunnus ei toimi loputtomasti. Yksi varastettu salasana ei vaaranna muita palveluita, kun salasana on eri joka paikassa. Toiselta varastettu salasana ei vaaranna sinua, kun salasanasi on vaikea arvata.

Pitkä salasana – salalause – vaikeuttaa salasanan arvaamista ja teknistä murtamista.

Millaiset salasanakäytännöt meillä on?

Unohditko salasanasi? Hyvä! Nyt sinulla on mahdollisuus testata meidän käytäntöjä salasanoihin ja käyttäjätunnuksiin liittyen!

Pohdi:

- Keneltä pyydän apua, jos salasanojen kanssa on ongelmia?
- Onko minulla tarvittavien henkilöiden yhteystiedot saatavilla?
- Millä välineellä otan yhteyttä, jos en pääse kirjautumaan?
- Mistä tiedän, onko salasanan vaihtajat töissä tai lomalla?

Havaitsitko kehitettävää? Kerro havaintosi ja kehittämisideasi!

Jos epäilet rikollisten saaneen salasanasi, vaihda salasana heti. Ilmoita asiasta sen jälkeen välittömästi IT-tukeen.

Käyttäjätunnusta ja salasanaa on helpompi suojata, kun ottaa käyttöön monivaiheisen tunnistautumisen. Sitä kannattaa hyödyntää niin työpaikan kuin vapaa-ajankin palveluissa. Monivaiheisesta tunnistautumisesta käytetään myös nimitystä MFA (Multi-Factor Authentication) tai 2FA (Two-Factor Authentication).

Salasanat ovat arjen digiturvan perusta!

3. Huijausviestin tunnistaminen - mikä tekee viestistä epäilyttävän?

Huijausviestin tunnistaminen on tärkeä taito digimaailmassa. Jokaisen pitäisi onnistua siinä mahdollisimman hyvin. Huijausviestin tunnistaa, kun oppii havaitsemaan viestistä epäilyttäviä yksityiskohtia.

Mikä tekee viestistä epäilyttävän? Arvioi viestistä seuraavia asioita:

Viestin lähettäjä

Tunnistatko viestin lähettäjän?

Onko viestin lähettäjä sinulle tuttu vai tuntematon? Täsmääkö lähettäjän nimi ja hänen käyttämä sähköpostiosoite? Jos viestin lähettäjä väittää olevansa yrityksen työntekijä, mutta viesti on lähetetty työpaikan ulkopuolisesta sähköpostiosoitteesta, on syytä olla varuillaan. Lähettäjätiedolla yritetään myös herättää luottamusta. Kun viesti on lähetetty IT-tuen nimissä, niin viesti vaikuttaa luotettavammalta. Viestin lähettäjätietoon ei voi luottaa, koska lähettäjätieto voidaan väärentää.

Viestin odotettavuus

Odotatko tällaista viestiä juuri tältä lähettäjältä?

Odotatko yhteydenottoa ja liitteitä kollegalta? Pitäisikö asiakkaalta tulla linkki projektiin liittyen? Oletko sopinut pankin kanssa, että he ovat sinuun yhteydessä työsähköpostiisi?

Vetoaminen sinuun ja saamaasi hyötyyn

Yritetäänkö viestissä vedota sinuun tai luvataanko viestissä merkittävää hyötyä?

Huijausviestissä yritetään yleensä vedota sinuun, jotta sinut saadaan tekemään jokin haitallinen toimenpide. Sinun pitää esimerkiksi avata liitetiedosto tai linkki, täyttää tietosi jonnekin, toimittaa jokin asia esihenkilösi puolesta tms. Rikollisen käyttämä "Tässä pyytämäsi tiedostot" suorastaan houkuttelee avaamaan liitteitä. Tai sinua voidaan houkutella lunastamaan sinulle saapunut rahalähetys, kun kirjaudut verkkopankkitunnuksilla viestissä olevaan linkkiin.

Kiire ja pakollisuus

Edellytetäänkö viestissä kiireellisiä tai pakollisia toimenpiteitä?

Kiireeseen vetoaminen on yksi huijausviestien peruspilareista. Rikollinen haluaa luoda sinulle kiireen tuntua. Tämä voi tapahtua erilaisin keinoin. Esim. jos et uusi salasanaasi 24h aikana

tästä linkistä, käyttäjätunnuksesi suljetaan. Salattu sähköposti on luettavissa vain vähän aikaa. Lasku on erääntynyt ja pitää maksaa nopeasti. Jne.

Viestin kieliasu

Tunnistatko lähettäjän käyttämän kieliasun?

Käyttääkö viestin lähettäjä epäilyttävää kirjoitustyyliä? Jos olet tehnyt pitkään yhteistyötä joidenkin henkilöiden kanssa, niin saatat tunnistaa heidän kirjoitustyylinsä. Jos lähettäjä on tuttu, mutta kirjoitustyyli ei ole hänelle sopivaa, niin ole tarkkana.

Linkit

Millaisia linkkejä viestissä on?

Suhtaudu linkkeihin aina varauksella ja tarkista, millaista linkkiä olet avaamassa. Sähköpostissa näkyvä linkki ei välttämättä vie sinne, miltä teksti näyttää. Jos linkki vaikuttaa turvalliselta ja avaat sen, niin katso mitä linkistä oikeasti aukeaa. Tarkasta aina avautuneen sivuston www-osoite uudelleen ennen kuin syötät sinne tietoja tai lataat sieltä mitään. Jos viestin tai liitteen avaaminen vaatii kirjautumista, mieti mihin olet käyttäjätunnusta ja salasanaa syöttämässä. Oletko kirjautumassa tuttuun paikkaan? Linkki voi olla https-suojattu, mutta se ei tarkoita mitään. Rikollisetkin osaavat käyttää suojattuja yhteyksiä.

Liitteet

Millaisia liitteitä viestissä on?

Avaa liitetiedostot vain silloin, jos koko viesti vaikuttaa järkevältä ja liite sopii asiayhteyteen ja lähettäjään. Suhtaudu liitteisiin suurella epäilyksellä silloin, kun liitteen avaaminen edellyttää joidenkin suojatoimenpiteiden kytkemistä pois päältä. Esimerkiksi Excel-tiedostojen sisällä saattaa olla teksti, joka pyytää ajamaan komentoja tai poistamaan suojauksia käytöstä, jotta tiedoston sisältö voidaan näyttää oikein. Suhtaudu epäilevästi myös sellaisiin liitteisiin, jotka edellyttävät kirjautumista, jotta liitteen saa lopulta auki.

Roskapostia vai ei?

Onko viesti jäänyt roskapostisuodattimeen?

Jos viesti on jäänyt roskapostisuodattimeen, niin se on vahva signaali siitä, että viestiä pitää käsitellä varovaisesti. Automatiikka on huomannut viestissä huijausviestille tyypillisiä asioita, kuten esim. erikoisen lähettäjätiedon, haitallisen liitteen tai linkkejä muihin palveluihin.

Viestin ajankohtaisuus

Käsitelläänkö viestissä kiinnostavaa ajankohtaista aihetta?

Huijausviesteissä voidaan käyttää ajankohtaisia aiheita, jotka saavat mielenkiintosi heräämään. Tällöin et välttämättä suhtaudu viestiin epäilyttävästi. Huijausviestin sisällössä voidaan viitata esim. uusiin asioihin, kuten vaikkapa uuteen sähköpostijärjestelmään. "Kirjaudu uuteen järjestelmään tästä". Viestit voivat liittyä esim. Suomen ja muun maailman tapahtumiin. Jos viesti ei liity työasioihin, niin tulkitse se roskapostiksi.

Huijausviestin tunnistaminen ei aina ole yksinkertaista

Jos suomalaisen toimijan sähköpostitili on kaapattu, niin huijausviestin tunnistaminen on erittäin haastavaa. Tällöin vain viestin sisällöstä ja asiayhteydestä voi olla mahdollista päätellä, että kyseessä on huijaus. Valitettavasti joskus on jopa avattava linkki ennen kuin huomataan, että kyseessä on huijaus.

4. Miksi sähköposti on huono väline tiedon jakamiseen?

Sähköposti on perinteinen tiedonjakotapa. Työelämässä sähköpostilla on selkeitä etuja, mutta myös monia haittoja.

Hyvinä puolina on nopeus, toimivuus ja yksinkertaisuus. Tietoja saadaan liikkumaan hyvin helposti ja nopeasti paikasta toiseen. Sähköposti toimii erilaisilla laitteilla. Sähköpostijärjestelmä sisältää tietoa vuosien ajalta, jolloin vanhakin tieto on edelleen löydettävissä sähköpostin hakutoiminnolla.

Sähköpostin yhtensä suurimpana ongelmana on pidetty sitä, että sähköpostiliikenne kulkee yrityksestä toiseen salaamattomana. Kolmannen osapuolen on mahdollista salakuunnella viestiliikennettä. Onneksi viestit ja liitetiedostot voidaan nykyään kohtalaisen helposti suojata eri keinoin - tosin käytettävyyden kustannuksella.

Tieto voidaan lähettää vahingossa väärälle vastaanottajalle. Jälkikäteen on haastavaa selvittää, onko vastapuoli hyötynyt tiedosta jotenkin. Vastaanottajalle voidaan toki lähettää pyyntö väärän sähköpostin poistamisesta, mutta tämän varmentaminen voi olla käytännössä hankalaa.

Tieto monistuu useaan paikkaan. Kun lähetät tietoa ja liitteitä, niin ne päätyvät vastaanottajan sähköpostiin sekä sinun sähköpostisi Lähetetyt-kansioon. Tieto on siis kahdessa paikassa. Jos vastaanottajia on useita, niin kopioitakin on useita eri paikoissa. Tiedon tulostaminen tai tallentaminen työasemalle lisää kopioiden määrää entisestään.

Liitteen muokkaaminen muodostaa liitteestä uuden version. Tästä päädytään helposti versio-ongelmaan. Ei välttämättä ole täysin selvää, mikä on tuorein versio ja onko kaikilla tuorein versio käytettävissä.

Viestin edelleen lähettäminen (forward-toiminto) mahdollistaa ison viestiketjun siirtämisen sellaisenaan uudelle vastaanottajalle. Tässä voi helposti käydä niin, että uusi vastaanottaja saa vahingossa tietoa, joka ei ole hänelle tarkoitettu. Edelleen lähettäminen konkretisoi myös monistumiseen ja versio-ongelmiin liittyvät asiat.

Sähköpostiviestin lähettäjätietoon ja viestin sisältöön ei voi täysin luottaa. Lähettäjätieto on mahdollista väärentää, jolloin sähköposti näyttäisi tulevan luotettavalta taholta. Lisäksi käyttäjätunnusten kaappaukset ovat johtaneet siihen, että verkkorikolliset voivat viestiä toisen henkilön nimissä hänen oikealla käyttäjätunnuksellaan. Samalla verkkorikollisilla on pääsy samaisen työntekijän viestihistoriaan, pahimmillaan useiden vuosien ajalta.

Henkilötietojen käsittelyn ja tietosuojavelvoitteiden noudattamisen kannalta sähköposti on haastava väline. Rekisteröidyn oikeuksien toteuttaminen on ongelmallista, jos henkilötietolistoja kerääntyy eri sähköposteihin. Samalla henkilötiedot altistuvat erilaisille tietoturvariskeille, jotka voivat aiheutua esimerkiksi tiedon edelleen lähettämisestä tai sähköpostin käyttäjätunnuksen kaappaamisesta.

Asiakkaat ja yhteistyökumppanit eivät välttämättä pidä siitä, että jotakin asiaa käsitellään sähköpostin välityksellä. Heille voi olla tärkeää, että esimerkiksi kahdenkeskisistä asioista ei viestitä laisinkaan tavallisella sähköpostilla. On hyvä ensin sopia, miten tietoa vaihdetaan, jotta vältytään ylimääräiseltä mainehaitalta.

Tietoa voi jakaa sähköpostin sijasta fiksummin digitaalisten työtilojen, tiedostonjakopalveluiden tai verkkolevyjen kautta. Tällöin pääsyä tietoon on mahdollista rajoittaa käyttöoikeuksilla, eikä tietoa tule jaettua niin helposti väärille vastaanottajille. Jaossa oleva tieto on myös mahdollista poistaa, jos tiedosto on jaettu väärin tai jos tiedostojakoa ei enää tarvita. Versio-ongelmia ei pääse muodostumaan, kun muokkaukset tehdään aina jaossa olevaan tiedostoon.

5. Etätyöskentely ja matkustaminen

Töitä voi tehdä turvallisesti eri paikoissa, kun huomioidaan näihin työskentelypaikkoihin liittyvät erityispiireet. Ohessa on lähestytty asiaa kolmen näkökulman kautta:

Työskentely kotona

Kotona korostuu työntekijän oman osaaminen ja vastuu ympäristön ja laitteiden teknisestä suojaamisesta. Huomioitavaa:

- Tee työt työpaikan laitteilla. Käytä omia laitteita vain omien asioiden hoitamiseen.
- Suojaa laitteita fyysiseltä vahingolta. Sovi samassa taloudessa asuvien kanssa, että työlaitteisiin ei kosketa.
- Lukitse tietokone ja puhelin, kun poistut työpisteeltä.
- Säilytä laitteita suojassa työpäivän jälkeen.
- Varmista, että kotona käytössäsi oleva langaton WLAN-verkko on suojattu esimerkiksi WPA2-salauksella.
- Vaihda verkkolaitteen oletussalasana ja huolehdi verkkolaitteiden tietoturvapäivityksistä.
- Suojaa samalla tavalla myös kodin muut älylaitteet, jotta niiden mahdolliset tietoturvaongelmat eivät vaikuta työlaitteisiin.

Muualla työskentely

Ohessa asioita, jotka tulee huomioida, kun työskentelee muualla. Huomioitavaa:

- Harkitse tarkkaan, mihin työlaitteet voi jättää vartioimatta.
- Sammuta tai lukitse tietokoneesi, jos joudut poistumaan sen luota.
- Älä kiinnitä työkoneeseesi muilta saatuja virtalähteitä, USB-muisteja tai ulkoisia kovalevyjä.
- Pidä laite itselläsi - älä lainaa omaa työlaitettasi muille.
- Älä kirjaudu yrityksemme IT-palveluihin muiden laitteilta tai yleisillä koneilla kirjastossa, hotellissa jne.
- Käytä vain luotettavia WLAN-verkkoja. Vältä lentokentän, hotellin, kirjaston jne. yleisiä verkkoja.
- Käytä näytön tietoturvasuojaa.
- Puheääni kantautuu pitkälle. Huomioi tämä, kun puhut puhelimessa tai osallistut etäpalaveriin.

Menossa ulkomaille?

Matkalla ja ulkomailla työskentely on turvallista, kun huomioi aikaisemmin mainitut asiat kohdasta "Muualla työskentely" sekä seuraavat lisähuomiot:

- Harkitse tarkkaan, tarvitsetko kaikkia työlaitteita matkalle mukaan.
- Poista tai suojaa laitteilla olevat tiedot, jotka eivät saa vaarantua esim. jos kone katoaa.
- Tarkista lentoyhtiöltä, mitä laitteita voit ottaa lennolle mukaan.
- Tiedosta, että tulliviranomaisilla voi olla oikeus avata ja tutkia laitteesi osana turvatarkastusta.
- Havaitsitko jotain epäilyttävää laitteisiin tai käyttäjätunnuksiin liittyen? Ilmoita asiasta välittömästi IT-tuelle.
- Tutustu myös Suomen ulkoministeriön matkustusturvallisuutteen liittyvään sivustoon.

6. Etäkokoukset, puhelut ja keskustelut - huomioi nämä turvallisuusasiat

Etäkokoukset mahdollistavat uusia asioita ja helpottavat monen arkea. Samalla kokoustila laajenee toimistolta ihmisten koteihin ja muihin paikkoihin. Jotta keskusteluiden luottamuksellisuus säilyy, on hyvä varmistua muutamista asioista. Ohessa on lähestytty asiaa etäkokousten näkökulmasta, mutta samoja vinkkejä voi soveltaa myös kahdenkeskisiin keskusteluihin ja puhelinkeskusteluihin.

Valitse kokoustila käsiteltävien asioiden mukaan. Kaikki nykyiset kokoustilat eivät ole alun perin tarkoitettu kokoustiloiksi, jolloin huoneiden rakenteelliset ratkaisut vaikuttavat mm. äänieristykseen. Jos tiedät, että jonkin huoneen äänieristys on huono, niin tiedosta se. On myös hyvä tiedostaa, mihin suuntaan kokoustilan esitysmateriaali näkyy. Pahimmillaan luottamuksellista esitystä seurataan myös kadulta ja viereisestä rakennuksesta.

Tunnista kaikki osallistujat. Etäkokouksessa on ensin hyvä varmistaa, kenen kanssa ollaan keskustelemassa. Aivan minimissään pitää varmistaa, täsmääkö osallistujalista kutsuttuihin henkilöihin ja tunnistathan kaikki paikalla olevat. Jos joukossa on uusia tuttavuuksia, niin kysy rohkeasti keitä he ovat. Jos olet itse kutsunut mukaan ylimääräisiä henkilöitä, niin esittele heidät omatoimisesti. Lisää luottamusta saadaan sillä, että kaikki esittäytyvät kuvan kera. Näin voidaan myös varmistaa kuulostaako ja näyttääkö toinen osapuoli tutulta.

Kerro ketkä ovat samassa kokoustilassa sinun kanssasi. Tällöin muut etäosallistujat ovat tietoisia, että kaikki osallistujat eivät näy etäkokousjärjestelmän osallistujalistassa. Muiden osallistujien kertominen on hyvien tapojen mukaista, mutta vaikuttaa myös turvallisuuteen. Ei voi olla niin, että kesken keskusteluiden tai näytön jakamisen ilmenee, että luottamuksellinen tieto menee myös sellaisille henkilöille, joiden ei tiedetty olevan kokoustilassa.

Suosi etäkokouksissa kuulokkeita. Käyttämällä kuulokkeita varmistat, että muiden osallistujien puhe ei kantaudu sinun kauttasi ulkopuolisille. Jos ääni tulee tietokoneesi tai puhelimesi kaiuttimesta, voi äänen kuulla myös ulkopuoliset. Huomioi kuitenkin se, että oma puheäänesi voi kuulua myös ulkopuolisille, vaikka muiden puhe tuleekin omista kuulokkeistasi. Valitse siis kokoustila järkevästi. Lisäksi on hyvä tiedostaa, että jollakin muulla osallistujalla voi olla kaiuttimet käytössä, jolloin koko keskustelu kuuluu sitä kautta.

Suojaa oman laitteesi näyttö ulkopuolisilta. Oman näytön suojaaminen on erityisen tärkeää, kun kokoukseen osallistutaan esimerkiksi julkisessa tilassa tai junassa tms. Tietokoneen näytölle asetettava tietoturvakalvo rajaa näytön katselukulmaa niin, että vierustoveri ei näe näyttöäsi. Voit myös asettua istumaan kokoustilassa niin, että näyttöäsi ei nähdä.

Turvalliset etäkokoukset ovat mahdollisia, kun kaikki osallistujat toimivat yhdessä järkevästi.

7. Älypuhelin on tärkeä - suojele sitä!

Älypuhelimella on iso rooli jokaisen arjessa. Puhelin tekee arjesta sujuvampaa ja lisää turvallisuutta.

On tärkeää, että suojelemme tätä laitetta asianmukaisesti. Ohessa huomioita ja vinkkejä älypuhelimen turvalliseen käyttöön. Asioita voi soveltaa myös muihin mobiililaitteisiin, kuten tablet-tietokoneisiin.

Tiedosta älypuhelimen tärkeys ja toimi sen mukaisesti

Mieti mihin kaikkialle menetät pääsyn, jos puhelimesi hajoaa, katoaa tai varastetaan. Esimerkiksi jos käytät puhelintasi kaksivaiheisessa todennuksessa (MFA), niin saatat menettää hetkellisesti pääsyn näihin palveluihin. Puhelimen muistissa saattaa olla myös tietoja, tiedostoja tai kuvia, joita ei muualla ole. Huolehdi varmuuskopioista ja pidä käyttäjätunnukset tallella.

Mitä kaikkea ulkopuolinen saa haltuunsa, jos puhelimesi varastetaan? Entä mihin varas saa pääsyn puhelimesi kautta? Lukitse puhelin suojakoodilla, suojakuviolla tai sormenjälkitunnistuksella. Koodi on tärkeä suojamuuri ulkopuolisia vastaan. Harkitse myös viestien ja ilmoitusten piilottamista näytöltä. Jos menetät puhelimesi, niin tällöin ulkopuolinen ei pääse lukemaan ruudulta tärkeitä tietoja.

Harjoittele erikoistilanteiden varalle. Jos puhelimesi katoaa, miten löydät sen? Puhelimessa olevia paikannustoimintoja kannattaa testata - mielellään jo ennen puhelimen kadottamista. Entä jos yhtäkkiä tarvitset puhelimeen liittyvää käyttäjätunnusta ja salasanaa? Mistä ne löytyvät ja miten ne voi palauttaa? Työpaikan IT-tuella ei välttämättä ole keinoja päästä puhelimeen.

Sovelluksia vain tarpeen mukaan

Asenna laitteeseen vain työn tekemisen kannalta välttämättömät sovellukset. Ennen uuden sovelluksen asentamista on toki hyvä selvittää, onko laitteessa jo vastaava sovellus. Eli selvitä, tarvitsetko välttämättä mitään uutta sovellusta, vai pärjäisitkö laitteen omalla sovelluksella.

Asenna sovellukset aina virallisesta sovelluskaupasta. Selvitä etukäteen millaista sovellusta tarvitset, mitä vaihtoehtoja on olemassa ja millaisia arvosteluja sovellus on saanut. Kun tiedät minkä sovelluksen haluat, tarkista tarkkaan, että olet asentamassa oikean nimistä

sovellusta oikealta julkaisijalta. Pyri suosimaan tunnettuja ja yleisesti käytössä olevia sovelluksia. Niissä mahdollisesti ilmenevät ongelmat tulevat todennäköisesti nopeammin esille.

Sovelluksen käyttöoikeuspyyntöjä kannattaa pohtia hetki. Jos sovellus pyytää käyttöoikeutta esimerkiksi laitteen tiedostoihin tai kameraan, niin anna oikeudet vain, jos pyyntö on mielestäsi aiheellinen. Jos sovelluksella ei ole tarkoitus ottaa kuvia, niin kameran käyttöoikeuksia ei tarvita.

Poista ylimääräiset sovellukset, kun niille ei ole enää tarvetta.

Huijausviestit ovat riski myös älypuhelimissa

Huijausviesteihin liittyvät riskit ovat olemassa myös älypuhelimissa. Riskit voivat olla puhelimissa jopa suurempia, koska laitteen näkymät ovat rajatumpia tietokoneeseen verrattuna. Rikollisen lähettämän linkin takaa mahdollisesti löytyvä huijaussivusto voi näyttää puhelimessa uskottavammalta kuin tietokoneen nettiselaimessa.

Sähköpostilla saapuneen linkin todellisen www-osoitteen selvittäminen on puhelimessa riskialttiimpaa kuin tietokoneella. Esimerkiksi tietokoneen sähköpostiohjelmassa voi viedä hiiren kursorin linkin päälle, jolloin linkin oikea osoite näkyy. Puhelimessa linkkiä pitää painaa pitkään, jolloin linkin todellinen osoite tulee näkyville. Vahinkoklikkauksen riski on puhelimessa suurempi kuin tietokoneella.

Älypuhelimen erikoisuus on se, että huijausviestejä ja haitallisia linkkejä voi tulla myös tekstiviestillä. Koska viestit saapuvat perinteisenä tekstiviestinä, ei sähköpostijärjestelmän roskapostisuodatin pysty niitä pysäyttämään. Rikolliset voivat lähettää viestejä niin, että viestit saapuvat samaan viestiketjuun oikeiden viestien kanssa. Puhelimen kautta avattavien viestien ja linkkien kanssa tuleekin olla todella tarkkana.

8. Toimitilaturvallisuus on muutakin kuin digiä!

Toimitilojen turvallisuus muodostuu IT-asioiden lisäksi oikean maailman asioiden huomioimisesta sekä vieraanvaraisuudesta. Muistetaan viestiä toisillemme, kuka kukin on. Asiallinen kyseenalaistaminen nostaa turvallisuustasoa. Ei unohdeta perusasioita!

Puhtaan pöydän periaate

Puhtaan pöydän periaatteen idea on se, että työpöydällä ei säilytetä sellaista materiaalia, jota ei haluta muiden näkevän. Näitä ovat esimerkiksi muistiinpanot, sopimukset, salasanat jne. Pöydällä ei myöskään säilytetä helposti varastettavia tavaroita, kuten henkilökorttia, avaimia, USB-muisteja tai muita tallennusmedioita, puhelinta, rahoja jne. Laita paperit, laitteet ja läppäri lukittuun kaappiin viimeistään päivän päätteeksi.

Käytä henkilökorttia

Työntekijän henkilökortti auttaa hahmottamaan, kuka on työntekijä ja kuka vierailija. Kortti viestittää, että olet töissä täällä. Vaikka olemme samassa työpaikassa, emme välttämättä tunnista toisiamme, koska emme näe toisiamme niin usein. Uudet työntekijät eivät vielä tunne muita – muut ei tunne heitä.

Kokousta sopivassa paikassa ja sopivalla äänellä

Tiedosta mitä puhut ja missä. Valitse kokoustila käsiteltävien asioiden mukaan. Käytäväpalaverit on ihan OK arjen asioihin. Luottamuksellisemmissa asioissa on hyvä suosia suljettua tilaa. Huomioi, että tilojen äänieristys vaihtelee. Varmista, että kokousmateriaalit eivät näy ja kuulu ulkopuolisille.

Huolehdi vieraistasi

Ilmoita muille tai merkitse intraan, että sinulle on tulossa vieraita ja toimit vieraiden isäntänä/emäntänä. Ota vieraat vastaan ja anna heille vierailijan henkilökortti. Saata vieraat kokoustilaan ja näytä samalla, missä on WC:t yms. Vierailun päätteeksi kerää vierailijakortit pois ja saata vierailijat ulko-ovelle asti. Tällä toimintamallilla pyritään siihen, että muut työntekijät tunnistavat vierailijat eikä vierailijoiden ole tarvetta liikkua talossa yksinään. Se on myös vierailijalle mukavampi, kun hänestä pidetään huolta.

Ylimääräisiä henkilöitä ovella tai toimitiloissa?

Onko toimitilojemme ovella tai toimitiloissa henkilö, jota et tunnista? Kysy rohkeasti millä asialla henkilö täällä liikkuu. Tuntemattomia ei tule päästää sisälle. Jos henkilö on sellaisessa

tilassa, johon vierailla ei ole asiaa, niin saata hänet takaisin isännän/emännän luo. Jos vierailulle ei löydy pätevää syytä, niin saata vieras ulos asti.

IT-laitteet ilman omistajaa

Havaitsitko toimitiloissa ylimääräisiä IT-laitteita? Mainitse niistä IT-asiantuntijalle. Jos löydät tiloista USB-muistitikun, niin älä kytke sitä suoraan tietokoneeseen. Haittaohjelmia levitetään edelleen USB-muistien avulla. Toimita myös ilman omistajaa olevat kannettavat tietokoneet ja puhelimet IT-asiantuntijalle.

Muista myös muut turvallisuusasiat

Turvallisuus ei ole pelkkää digiä ja kyberiä. Yhtä tärkeää on tietää, missä on lähin poistumistie, ensiaputarvikkeet ja palosammuttimet - ja osata käyttää näitä tarvittaessa! Huolehdi perusasioista!

9. Mikä on toimitusjohtajahuijaus?

Toimitusjohtajahuijauksessa – tai pomohuijauksessa – rikollinen esiintyy yrityksessä johtavassa asemassa olevana henkilönä ja pyytää työntekijää tekemään jonkin toimenpiteen hänen puolestaan. Pyyntö voi liittyä esimerkiksi laskun maksamiseen tai tilisiirron tekemiseen.

Rikollisen tarkoituksena on saada rahaa liikkeelle. Verkkorikollinen luottaa siihen, että alainen tottelee pomon pyyntöjä, etenkin jos pyyntö tulee toimitusjohtajalta, talousjohtajalta tms. korkeassa asemassa olevalta henkilöltä.

Toimitusjohtajahuijauksiin liittyy usein seuraavia asioita:

- Pomo edellyttää sinulta nopeaa rahansiirtoa tai laskun maksua.
- Pyyntö saapuu sähköpostilla, pomon nimissä.
- Pomo vaatii, että asiaa käsitellään luottamuksellisena.
- Pomo ei voi antaa lisätietoja, hän vetoaa omaan kiireeseen.

Toimitusjohtajahuijauksessa rikollinen yrittää olla tuttavallinen ja herättää luottamusta. Sähköpostiviestissä lähettäjän nimi vaikuttaa tutulta ja viestissä puhutellaan juuri sinua. Rikollinen aloittaa viestinnän helpolla kysymyksellä: “Oletko käytettävissä?” tai “Oletko paikalla?” Näin rikollinen yrittää muodostaa keskusteluyhteyttä kanssasi. Jos vastaat viestiin jotain, niin todennäköisesti seuraavissa viesteissä rikollinen kertoo, mitä hän oikeasti haluaa.

Näin suojaudut toimitusjohtajahuijauksilta

Huomioi alla olevat asiat, etenkin loma-aikoina:

- Suhtaudu tilisiirtoihin ja laskuihin liittyviin pyyntöihin erityisellä huolellisuudella.
- Odotatko laskua? Kerro tämä etukäteen varahenkilöllesi.
- Unohda kiire, vaikka laskun väitetään olevan myöhässä.
- Keskustele tiimin kesken, mitä asioita toimitusjohtaja tai muu esihenkilö ei pyydä sähköpostilla.
- Muista arjen tietoturva: ole tarkkana liitteiden ja linkkien kanssa.
- Soita työkaverille varmistuspuhelu, jos jokin hänen pyyntönsä epäilyttää.
- Noudata organisaatiossa sovittua tapaa laskujen vastaanottamisesta ja maksamisesta.
- Ota yhteyttä organisaatiomme IT-asiantuntijaan, jos saat epäilyttäviä viestejä.

Muista: Kiireeseen vetoaminen ja yksittäisen henkilön painostus ovat merkittäviä tekijöitä toimitusjohtajahuijausten onnistumisessa!

10. Tietosuoja on suunnitelmallisuutta ja arjen tekoja

Tietosuojakeskusteluissa korostuvat usein tietomurrot ja hallinnolliset sakot. Valitettavasti ne hämärtävät tietosuojaa kokonaisuutena ja ohjaavat ajattelemaan aihetta kapeasti, ulkoisten asioiden kautta.

Tietosuoja muodostuu **suunnitelmallisuudesta ja arjen valinnoista.** Merkittävä määrä tietosuojatyötä tehdään ennen kuin yhtään henkilötietoa on kerätty.

Henkilötietojen tietoturvaloukkaukset ja tietomurrot pyritään välttämään hyvällä suunnittelulla ja toteutuksella. Hallinnolliset sakot johtuvat siitä, että suunnitelmallisuutta, tietosuojaperiaatteita ja rekisteröidyn oikeuksia ei ole noudatettu.

Suunnittelu luo pohjan tietosuojalle

Henkilötietojen käsittelyn suunnittelua voi toteuttaa esimerkiksi seuraavien kysymysten kautta:

- Mitä olemme tekemässä?
- Miksi tarvitsemme henkilötietoja?
- Millaisia henkilötietoja oikeasti tarvitsemme?
- Miten tietoja tullaan käsittelemään?
- Ketkä kaikki tietoja tulevat käsittelemään?
- Mille osapuolille tietoja tullaan luovuttamaan?
- Miten tietoa tullaan keräämään?
- Minne tarpeelliset tiedot tallennetaan?
- Kauanko tietoa on tarpeellista säilyttää?
- Miten tieto lopulta poistetaan eri paikoista?
- Miten ja missä henkilötietojen käsittelystä kerrotaan rekisteröidylle?
- Miten ohjeistan muita työntekijöitä, jotta suunnitelma muuttuu käytännön teoiksi?

Kaikki työntekijät eivät välttämättä joudu suunnittelemaan henkilötietojen käsittelyä työpaikalla, mutta jokaisella henkilötietoja käsittelevällä on merkittävä rooli tietosuojan toteutumisessa.

Tietosuoja on arjen tekoja

Suunnitelma muuttuu arjen teoksi usealla eri tavalla:

Noudata ohjeita!

Noudata henkilötietojen käsittelyyn liittyvää suunnitelmaa ja ohjeita. Kerää vain niitä henkilötietoja, joita oikeasti tarvitaan. Älä kerää lisätietoja varmuuden vuoksi. Tallenna tiedot sovittuun paikkaan. Käsittele ja avaa vain niitä tietoja, joita työssäsi tarvitset. Poista tiedot, kun niitä ei enää tarvita. Jos olet epävarma, miten henkilötietoja tulee käsitellä, niin pyydä lisää ohjeita!

Käytä sovittuja järjestelmiä

Käsittele henkilötietoja niissä järjestelmissä, jotka on kyseistä tehtävää varten hankittu.

Yksittäinen työntekijä ei saa käsitellä henkilötietoja esimerkiksi pilvipalveluissa tai muissa järjestelmissä, jos niiden käytöstä ei ole suunnitelmaa ja organisaatiossa tehtyä päätöstä.

Vältä turhia kopioita

Arjen tekeminen vaatii joskus, että henkilötiedoista tehdään listoja, joita käsitellään esim. taulukkolaskentaohjelmassa. Tallenna listaus sovittuun paikkaan. Vältä turhien kopioiden ottamista useaan paikkaan, esimerkiksi omalle koneelle, kotihakemistoon, yhteisille verkkolevyille tai sähköpostiin. Useampi kopio hankaloittaa henkilötietojen asianmukaista hallintaa ja altistaa tiedot myös erilaisille tietoturvariskeille.

Lähetä ja jaa tietoa turvallisesti

Henkilötiedon jakaminen muille tulee tehdä järkevästi ja turvallisesti. Älä lähetä tietoa perinteisellä sähköpostilla. Se muodostaa monia ongelmia. Perinteisessä sähköpostissa tieto liikkuu turvattomasti, tiedosta muodostuu turhia kopioita ja tieto saattaa päätyä väärälle vastaanottajalle. Jaa ennemmin linkki käyttöoikeuksilla rajattuun tiedostoon tai käytä turvasähköpostipalvelua.

Poista turhat tiedot

Henkilötiedot tulee lopulta poistaa, kun tiedolle ei ole enää tarvetta. Älä kuitenkaan poista tietoa heti, kun tieto on sinulle tarpeetonta. Noudata tässäkin organisaation ohjeita. Tiedoilla voi olla pitkiäkin säilytysaikoja. Varmista myös, hoitaako tietojärjestelmä tiedon poistamisen automaattisesti vai pitääkö sinun poistaa tietoa itse. Muista myös ne turhat kopiot! Paperinen materiaali toimitetaan tietosuojaroskikseen.

Auta rekisteröityä

Rekisteröidyllä on monia tietosuojaoikeuksia, mm. oikeus saada tietoa henkilötietojen käsittelystä ja tutustua omiin tietoihinsa. Jos rekisteröity pyytää tällaista, niin suhtaudu tilanteeseen asiakaspalveluhenkisesti. Noudata olemassa olevia ohjeita tai palaa asiaan, kun olet saanut organisaatiosta lisäohjeita.

Ilmoita havainnoista ja poikkeamista

Havaitsitko poikkeamia tai mahdollisia ongelmia henkilötietojen käsittelyyn, tietosuojaan tai tietoturvaan liittyen? Ilmoita tästä viipymättä eteenpäin. Nopean reagoinnin ansiosta isommilta ongelmilta on vielä mahdollista välttyä.

Suunnitelmallinen ja fiksu toiminta tekee henkilötietojen käsittelystä järkevää, vastuullista ja turvallista.

11. Tietoturvaosaaminen kasvaa yhteistyöllä!

Yrityksen työntekijöiden tietoturvatietoisuus eli tietoturvaosaaminen on tärkeä asia, josta pitää huolehtia jatkuvasti. Ilman tietoturvaosaamista yrityksen tietojen ja toiminnan turvaaminen sekä jatkuvuuden varmistaminen on arpapeliä.

Miten voimme yhdessä nostaa yrityksemme tietoturvaosaamista?

Digiturva liittyy meidän kaikkien työtehtäviin jollain tavalla. Tuo siis sinäkin digiturva osaksi arkea, oman tehtäväsi kautta. Keskustele työkavereidesi kanssa tietoturvasta, jaa kokemuksiasi ja esimerkkejä. Näin saamme levitettyä osaamista myös muille. Esittelen seuraavaksi muutamia tapoja, joilla tietoturvaosaamista voidaan konkreettisesti lisätä ja levittää.

Kybervartti – 15 min keskustelua digiturvasta

Kokeilkaa sellaista tapaa, että keskustelette jostain ajankohtaisesta digiturvallisuusaiheesta 10-15 minuuttia kuukausipalaverin alussa. Palaverin agendassa tätä osiota voi kutsua vaikkapa nimellä kybervartti.

Kirjatkaa keskustelusta talteen yksi havainto, oivallus, oppi, kysymys, kehitysidea tms. ja lähettäkää se heti eteenpäin allekirjoittaneelle. Keskustelun osallistujat oppivat yhdessä ja saavat uusia näkökulmia aiheeseen. Lisäksi saamme yhdessä koottua erilaisia tietoturvavinkkejä, keskustelunaiheita ja ajatuksia koko organisaatiolle.

Sisällytä digiturva ohjeisiin ja koulutuksiin

Pidätkö koulutuksia tai teetkö työssäsi ohjeita ja muita kaikille tarkoitettuja dokumentteja? Sisällytä ohjeisiin pari näkökulmaa myös tietoturvasta ja tietosuojasta! Kysy tarvittaessa lisävinkkejä esim. tietoturvasta, tietosuojasta, turvallisuudesta ja IT-asioista vastaavilta henkilöiltä. Kysy heiltä "Mitä tässä asiassa pitäisi huomioida tietoturvan kannalta?" Lopputuloksena ei ole tietoturvaohje, vaan ohje, joka sisältää myös tietoturvaa.

Kaikki voivat ylläpitää tietoturvakeskustelua

Oletko hankkimassa uutta IT-palvelua? Kysy palveluntarjoajalta, miten digiturvallisuus on huomioitu tässä palvelussa? Palveluntarjoajan vastausten perusteella on mahdollista oppia uutta. Samalla luodaan hyvää käytäntöä siitä, että tietoturvavastaavan ei tarvitse olla ainut, joka nostaa tietoturvakysymyksiä keskusteluun. Palveluntarjoajat, muut yhteistyökumppanit sekä omat työntekijätkin huomaavat, että meillä digiturva on kaikkien asia. Tämä luo hyvää kuvaa meistä ja nostaa osaamisestamme.

Toimitaan yhdessä esimerkillisesti

Me kaikki voimme edistää digiturvallisuutta toimimalla esimerkillisesti. Esimerkin voima korostuu erityisesti yrityksemme johdolla ja esihenkilöillä. Te viestitte omalla toiminnalla muille, miten asioihin pitää suhtautua. Kokeneemmat työntekijät puolestaan näyttävät uusille työntekijöille, miten talossa toimitaan.

Esimerkillisyys ei tarkoita mitään erityistä ja poikkeuksellisen hienoa, vaan ihan sitä arjen perustoimintaa. Meillä on tiettyjä sovittuja käytäntöjä - toimitaan niiden mukaisesti. Meillä on tietoturvaohjeet - noudatetaan niitä. Meillä on henkilökortit - käytetään niitä. Jne. Perusasioita.

Katsotaan digiturvallisuutta uuden työntekijän silmin

Uusi työntekijä on hyvässä tilanteessa - hänellä on lupa ihmetellä ja kysyä ihan mitä vaan. Mutta oikeastaan meidän kaikkien tulisi käyttäytyä kuin uusi työntekijä: jos jokin asia mietityttää tai ihmetyttää, niin uskalla kysyä.

Kysymällä voit saada aikaan keskustelun, jossa muutkin oppivat. Muut ovat saattaneet miettiä samaa asiaa, mutta eivät ole kehdanneet kysyä. Tai muut eivät välttämättä ole ajatelleet asiaa, kuten sinä.

Ihmetellään ja kysytään yhdessä!

12. Miksi ihminen on tietoturvan vahvin lenkki?

Ihmistä pidetään tietoturvan heikoimpana lenkkinä, mutta tämä on väärä lähtökohta. Päinvastoin. Sinulla on erittäin tärkeä rooli! Pystyt tekemään sellaisia havaintoja ja toimenpiteitä, joihin tietoturvaohjelmistot eivät kykene.

Käytetään esimerkkinä huijausviestejä.

Osaat arvioida kokonaisuutta

Olet työntekijänä olennaisessa roolissa, kun tunnistamme huijausviestejä. Sähköpostilaatikkoosi on päätynyt huijausviesti, jossa sinua pyydetään avaamaan liite tai linkki. Koska viesti on jo sähköpostilaatikossasi, se tarkoittaa, että tietoturvaohjelmisto ei ole onnistunut estämään viestiä.

Koulutusten kautta sinulla on ollut mahdollisuus oppia, millaisia huijausviestit ovat ja mitä niissä yleensä pyydetään tekemään. Pystyt arvioimaan mistä viesti on tullut, onko lähettäjä oikea, odotatko tällaista viestiä, onko asiayhteys oikea ja onko linkki tai liite luotettava.

Sinä pystyt arvioimaan kokonaisuutta ja tunnistamaan, onko viesti epäilyttävä.

Ilmoittaminen on tärkeä päätös

Ilmoitathan kaikista turvallisuuteen liittyvistä havainnoista? Ilmoittaminen on päätös. Kun päätät ilmoittaa havainnostasi, päätät samalla varoittaa muita. Se on päätös huolehtia yhteisestä turvallisuudesta.

Selkeästä huijausviestistä ilmoittaminen saattaa tuntua turhalta. Helposti ajattelee, että itsestäänselvyyksistä ei tarvitse ilmoittaa. Ilmoita silti, koska ilmoittaminen luo tärkeää tilannekuvaa. On hyvä ymmärtää, että samaa huijausviestiä ei välttämättä lähetetä kaikille työntekijöille. Älä huijaa itseäsi sillä, että joku muu on tästä jo ilmoittanut.

Ilmoittamalla tietoturvahavainnoista mahdollistat myös sen, että ongelmilta voidaan suojautua ennakkoon. Tai jo tapahtuneen vahingon vaikutukset saadaan minimoitua, kunhan toimitaan nopeasti. Kun ilmoitat, olet tehnyt päätöksen muiden auttamisesta.

Voimme oppia yhdessä

Työntekijät ja asiantuntijat voivat yhdessä tutkia ja arvioida ilmoitettua tietoturvahavaintoa (esim. huijausviestiä), jolloin molemmat osapuolet hyötyvät.

Työntekijä saa asiantuntijalta oppia siitä, mitkä asiat viestissä kertovat, onko kyseessä mahdollisesti huijausviesti vai ei. Työntekijä oppii esimerkiksi arvioimaan viestin lähettäjää, linkkejä ja viestin kontekstia. Samalla opit, millaisia huijausviestit voivat olla. Tai millainen viesti ei ole huijausviesti.

Asiantuntija oppii työntekijältä, millaisia viestejä työntekijät saavat. Asiantuntija saa tärkeää tilannetietoa, millaisia huijauksia juuri meidän yritykseen kohdistuu. Lisäksi asiantuntija oppii, miten erilaisiin viesteihin reagoidaan ja miten työntekijät tunnistavat ne huijausviesteiksi. Työntekijän ilmoitus ylläpitää asiantuntijankin osaamista!

Voimme opastaa toisiamme ja samalla oppia toisiltamme. Vahvistamme toinen toisiamme.

Osaat arvioida kokonaisuutta, ilmoittaa havainnoistasi ja opastaa muita.

Sinulla on tietoa, taitoa ja osaat toimia eri tilanteissa. Olet tietoturvan vahvin lenkki.

Toivottavasti blogiteksteistä oli sinulle ja organisaatiollesi iloa ja hyötyä!

Tiedätkö kollegan, joka voisi hyötyä tehokuurista?

Laita kopio menemään hänellekin!

Lisää vinkkejä organisaatiosi digiturvallisuuden kehittämiseen löydät osoitteesta Tietojesiturvaksi.fi

Matti Laakso, 2022
Tietojesiturvaksi.fi