Peruskyberturvallisuus

Arjessa ja vapaa-ajalla – koskee jokaista meitä

MPK

Miten valmistaudutaan kyberuhkiin?

- **Käytä harkintaa**
  - **Älä avaa epäilyttäviä sähköposteja tai klikkaa epäilyttäviä linkkejä ja liitetiedostoja**
  - **Älä vieraile haitallisilla verkkosivuilla, joiden turvallisuudesta et voi olla varma**
- **Tekninen torjunta**
  - **Aseta laitteisiin automaattiset päivitykset (tietokone, tabletti, puhelin)**
  - **Käytä virustorjuntaohjelmia**

Miten tunnistan mahdollisen hyökkäyksen?

- **Älä luota sähköpostissa näkyviin lähettäjän tietoihin (lähettäjän yhteystiedot, jotka ovat näkyvillä sähköpostia luettaessa), koska ne on helposti väärennettävissä.**
- **Vaikka sähköposti näyttää olevan lähetetty toisen työntekijän tai tunnetun yhteistyökumppanin nimissä, varsinainen lähettäjä saattaa olla kyberrikollinen.**
- **Tarvittaessa vahvista sähköpostin alkuperä puhelinsoitolla. Lisävarmistus pitäisi tehdä kaikissa tapauksissa, jotka liittyvät rahaan (pankkitili, …) tai muuhun luottamukselliseen tietoon.**
- **Jos sinulta kysytään puhelimitse luottamuksellista tietoa, vahvista aina soittajan henkilöllisyys. Voit tehdä tämän soittamalla kyselyn tehneen henkilön yrityksen vaihteeseen. Samaa tapaa voidaan käyttää myös vahvistamaan epäilyttävän sähköpostin lähettäjä.**

- **Älä hämäänny tiedosta, jota huijarilla saattaa olla. Useissa tapauksissa sähköpostit ja puhelinsoitot saattavat sisältää kollegoidesi nimiä sekä merkityksellistä ja ajankohtaista tietoa.**
- **Älä koskaan luovuta käyttäjätunnusta ja salasanaasi puhelimessa tai tuntemattomalla internet-sivustolla. Huomioi myös, että sähköpostien linkit eivät ole luotettavia, koska saatat joutua sivustolle, joka näyttää aidolta (pankkien kirjautumissivu tai muu sivusto, jossa pyydetään käyttäjätunnuksia)**
- **Käytä aina omia tai intranetin linkkejä. Älä myöskään paljasta mitään työhösi / yritykseen / yhteisöön liittyvää tietoa kenellekään ulkopuoliselle henkilölle, jonka henkilöllisyyttä ei voida vahvistaa.**

Kyberturvallisuus ja mobiililaitteet

- **Mobiililaitteiden monipuolistuneen käytön takia niihin kohdistuvat kyberturvallisuusuhat ovat lisääntyneet merkittävästi ja riskienhallinta on käynyt yhä haasteellisemmaksi.**
- **Harkitse tarkoin miten käytät matkapuhelintasi ja sen sovelluksia - vältä selailua epäilyttävillä verkkosivuilla välttyäksesi haittaohjelmilta.**
- **Älä koskaan myöskään lainaa puhelintasi tuntemattomille. Lukituskoodi ja automaattinen lukitus – aktivoi nämä toiminnot.**
- **Mobiilipalveluiden käytöstä – samat perussäännöt pätevät kuin tietokoneellakin toimittaessa, eli ei vierailla haitallisilla / tuntemattomille sivuilla, eikä klikkailla tuntemattomia linkkejä.**
- **Asenna aina uusimmat tietoturvapäivitykset – tai pyydä ystävääsi tekemään ne.**

- **Sovellukset – lataa luotettavista lähteistä, harkitse datan käyttö oikeuksia.**
- **Jos puhelin häviää - Pilvipalveluilla voit paikantaa, lukita ja tarvittaessa pyyhkiä puhelimen tiedot etänä.**
- **Puhelimen ostaminen ja myyminen Jos olet myymässä puhelinta Kytke puhelin pois kaikista pilvipalveluista (iCloud, OneDrive, sähköpostit…). Pyyhi puhelimen tiedot ja poista myös mahdolliset muistikortit. Palauta puhelimen tehdasasetukset.**
- **Jos olet ostamassa käytettyä puhelinta. Palauta puhelimen tehdasasetukset. Tarkista, ettei puhelin ole yhdistetty pilvipalveluihin, joihin tietosi voitaisiin siirtää.**
- **Lue mallikohtaiset ohjeet puhelinvalmistajien sivuilta**

Sosiaalinen media - tietojen kerääminen eri lähteistä ja niiden yhdistely

Kolme asiaa, joita sinun on hyvä harkita ennen kuin lisäät sisältöä sosiaaliseen mediaan (Facebook, Twitter jne).

1.) Sanotaan, että kaikki se mitä lisäät internetiin ei koskaan katoa. Asiat, mitkä sillä hetkellä vaikuttavat harmittomilta kertoa, voivat näyttäytyä eri valossa - jopa piinallisessa - kymmenen vuoden kuluttua. Käytä harkintaa myös lisätessäsi valokuvia, sillä ne voivat alkaa jopa 'elämään omaa elämäänsä' netissä, kuvia on helppo muokata toisiin käyttötarkoituksiin. Myös vanhempien tulisi tarkoin punnita, millaisia valokuvia he lisäävät lapsistaan sosiaaliseen mediaan.

2.) “Viimeinkin taukoa töistä ja loma Espanjan auringossa perheen kanssa". Tämä pieni harmiton ajankohtaisten kuulumisten kertominen sisältää tiedon, jota voidaan käyttää sinua vastaan. Kotiosoitteesi on jäljitettävissä, se voi löytyä jopa internetistä helposti ja varkailla on kokonainen viikko aikaa selvittää, mitä mielenkiintoista ja arvokasta anastettavaa sinulla on kotonasi

3.) Mainitset somessa, että etsit kauan kateissa ollutta sukulaistasi, joka asuu Australiassa. Yllättäen 'sukulainen' ottaa sinuun yhteyttä ja kertoo uskottavasti muistoja yhteisestä menneisyydestä ja lapsuudestanne. Kaikki tämä tieto on kerätty sosiaalisesta mediasta. "Riemukas jälleennäkeminen" odottaa teitä, kunhan vain lähetät vähän matkarahaa sukulaisellesi. Yhteenveto Sosiaalinen media on hyödyllinen ja tehokas kanava täynnä tietoa. Muista aina harkita hetki, millaista informaatiota olet sinne lisäämässä, oli se sitten tietoa sinusta itsestäsi tai yrityksestäsi.

Yllä mainitut esimerkit antavat sinulle osviittaa siitä, miten tietoja voidaan käyttää sinua vastaan.

EU:n uusi asetus henkilötietojen suojasta ja mitä se tarkoittaa sinulle

Tärkeimmät asetuksessa määritellyt EU-kansalaisen oikeudet:

- **Tietää, mitä tietoja sinusta kerätään tai on jo kerätty**
- **Nähdä, mitä tietoja sinusta on tallennettu**
- **Korjata sinusta tallennettua tietoa**
- **Pyytää tallennettujen tietojen poistamista**
- **Rajoittaa tallennetun tiedon jatkokäsittelyä**
- **Pyytää omien tietojen siirtoa tietojärjestelmästä toiseen (palveluntarjoajalta toiselle)**
- **Vastustaa, että tietojasi käytetään suoramarkkinointiin, tieteellisiin- tai profilointitarkoituksiin**

MPK