Kyberhygienian käsikirja

▶ Tee kyberturvallisuudesta itsellesi **rutiini**

KYMEN LAAKSON LIITTO

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Mikä ihmeen kyberturvallisuus?

Kyberturvallisuus tarkoittaa yrityksien ja organisaatioiden, mutta myös yksilöiden toimintaa, jonka avulla suojataan digitaalisia asioita, kuten järjestelmiä, laitteita ja käyttäjien tilejä.

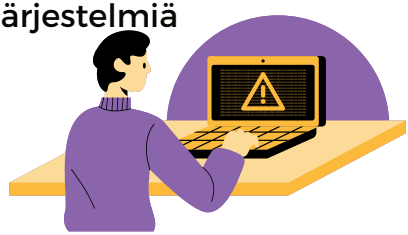
Yksinkertaistetusti idea on sama kuin fyysisten asioiden turvaamisessa.

Lukitsemme kotioven, koska haluamme suojella kotia ja sen sisällä olevia asioita ulkopuolisilta henkilöiltä – lukitsemme päätelaitteen, sillä haluamme suojella laitetta ja siinä olevia tietoja ulkopuolisilta henkilöiltä.

Kyberturvallisuus on jokaisen asia!

Kyberturvallisuus koskettaa **jokaista** meistä,

sillä jokaisella meistä on rooli digitaalisten asioiden turvaamisessa. On helppo ymmärtää, että rikolliset hyökkäävät teknisiä järjestelmiä kohtaan,
sillä niissä on teknisiä heikkouksia.



Joten on ymmärrettävää,
että meitä ihmisiäkin kohtaan hyökätään. Meissä ihmisissä on inhimillisiä heikkouksia, joita rikolliset osaavat käyttää hyväksi.

Olemme ihmisiä ja sen takia haavoittuvaisia inhimillisiä heikkouksia hyödyntäville kyberhyökkäyksille.

Kyberturvallisuus on **taito**, jossa voi, kannattaa ja pitää kehittyä.

Kuten kotioven kohdalla: ovi suojelee sisältöä suhteellisen tehokkaasti, jos se pidetään lukittuna. Huolimaton toiminta, kuten kotiavain maton alla tai oven auki jättäminen mahdollistaa pahantekijöille helpomman tien sisään.

Tunne kyberviholliseesi

Kyberuhat ovat uhkia kyberturvallisuudelle. Niitä voisi ajatella myös **kybervihollisina**, joita kohtaamme päivittäisessä tekemisessämme.

Yleisimpiä kyberviholliseesi ovat **tietojen kalastelijat** ja **käyttäjän manipuloijat**.

Tietojen kalastelija

Tietojen kalastelija on varmasti puhutuin ja tunnetuin kyberviholinen. Tietojen kalastelijat yrittävät huijata meidät avaamaan esimerkiksi haitallisen sähköpostilinkin tai liitetiedoston.

Heidän tavoitteensa on varastaa meidän tärkeitä tietojamme.

Nimitys tietojen kalastelu tulee siitä, että kyberviholinen yrittää narrata meitä erilaisilla syöteillä, jotta epähuomiossa tarttuisimme niihin.

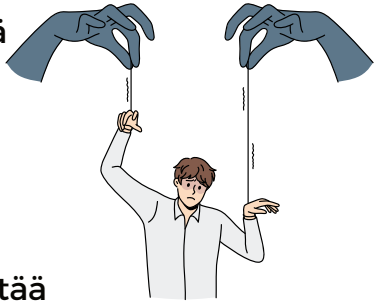
Kalastelijan syötit ovat erilaisia

Osa syöteistä on kaikille **samanlaisia**; niitä heitetään valtavasti tieto-verkkojen vesille ja toivotaan, että joku nappaisi niihin kiinni. Näitä ovat esimerkiksi spämmiviestit.

Osa syöteistä **räätälöidään** kohdetta varten; tällaiset syötit saavat todennäköisemmin kohteen antamaan tietonsa. Tällainen voi olla esimerkiksi väärennetty lasku.

Käyttäjän manipuloija

Käyttäjän manipuloija yrittää manipuloida meidät toimimaan heille suotuisalla tavalla. He hyödyntävät meidän inhimillisiä heikkouksiamme, eli esimerkiksi halua auttaa muita ihmisiä.



Käyttäjän manipuloijat ovat ovelia. He tietävät, mistä narusta pitää vetää, jotta kohde lankeaa heidän manipulointiinsa.

Käyttäjän manipuloijan työkalupakki on monipuolinen. Työkaluna voi olla esimerkiksi:

Huijausviesti

Manipuloija esiintyy viestissä esimerkiksi yrityksen toimitusjohtajana.

Esittäminen

Manipuloija voi tekeytyä korjaajaksi ja yrittää kävellä yrityksen tiloihin ilman, että kukaan pysäyttää häntä.

Haitallinen USB-tikku

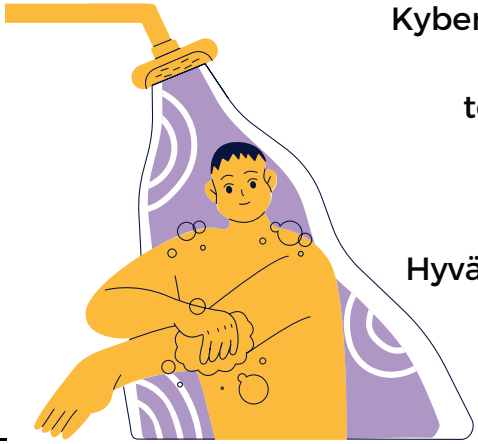
Manipuloija viljelee haitallisia USB-tikkuja näkyville paikoille ja toivoo, että joku liittäisi sellaisen koneeseensa.

Henkilökohtainen kyberhygienia

Kyberviholliset ovat siis ovelia ja tietävät, miten meitä ihmisiä huijataan. Tästä huolimatta heitä ei tarvitse pelätä. Asia on vähän sama kuin fyysisessä maailmassa, jossa kohtaamme erilaisia taudinaiheuttajia päivittäin. Ne hyökkäävät puolustuskykyämme vastaan ja suojaudumme niitä vastaan hyvällä hygienialla.

Kyberhygienian idea on sama kuin terveyshygienian.

Kyberhygienia tarkoittaa kyberturvallisuuden kehittämistä ja sen ylläpitämistä, eli omaa ja ympäristön kyberturvallisuutta edistetään säännöllisillä rutiineilla.



Kyberhygienian tekojen idea on olla yhtä tärkeitä ja yhtä helppoja kuin terveyshygienian. Käsien peseminen esimerkiksi hoituu itsestään, kun siitä on syntynyt meille rutiini.

Hyvän kyberhygienian avulla toimimme **turvallisesti arjessamme**.

NÄIN TEET KYBERHYGIENIASTA ITSELLESI RUTIININ

Kyberhygieniasta saa muodostettua itselleen rutiinin kiinnittämällä huomiota näihin: 1) **asenne** ja 2) **aloittaminen**.

1 Kyberhygienian idea on, että turvallisesta toiminnasta tulee osa päivittäistä tekemistä ja tämän takia asiaan tulisi kiinnittää huomiota. Kyberturvallisuus ei ole kaikille ykkösasia, mutta jokaisen tulee tästä huolimatta tiedostaa sen tärkeys ja tehdä **välttämätön**, jotta pysyy turvassa kyberuhkilta.

2 Toinen keskeinen asia on aloittaminen. Aloita pienillä teoilla, jotta kyberhygieniasta muodostuu **rutiini**. Voit esimerkiksi päättää, että jatkossa lukitset tietokoneesi aina, kun poistut sen luota. Toteuta tätä pientä asiaa ja vähitellen lisää siihen rinnalle muita tekoja, kuten salasanojen kanssa oikein toimiminen.

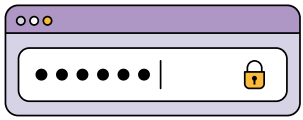
Kyberhygienia on siis näin yksinkertaista. Se vaatii kuitenkin oikeanlaista asennetta. Aloita pienestä ja pidä kyberhygienia osana päivittäistä rutiiniasi!

Pienillä teoilla on suuri vaikutus

Seuraavaksi käydään läpi viisi tapaa, joiden avulla voit parantaa ja ylläpitää hyvää kyberhygieniaa.

1

Toimi salasanojen kanssa oikein



Älä käytä samaa salasanaa eri palveluissa, äläkä koskaan jaa salasanaasi muiden kanssa. Muista käyttää tarpeeksi pitkää salasanaa (vähintään 16 merkkiä). Salalause on hyvä salasana, esimerkiksi **kissakiipesikatollekatsomaangorillaa**.

2

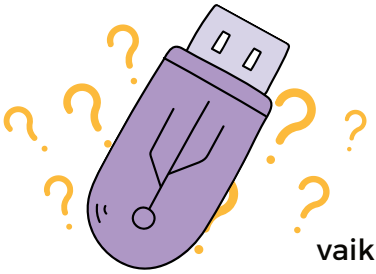
Mieti ennen kuin klikkaat

Älä klikkaa epäilyttäviä linkkejä tai avaa epämääräisiä liitetiedostoja. Linkki voi johtaa haitalliselle sivulle ja liitetiedosto voi ladata haittaohjelman laitteellesi.

3

Lukitse laitteesi

Ota rutiiniksi lukita tietokoneesi **aina** kun lähdet pois sen luota. Kyberviholinen voi kahvinhakureissunkin aikana ehtiä tekemään vakavia asioita tietokoneellesi.



4

Vältä vieraita laitteita

Maassa lojuva vieras USB-tikku voi vaikuttaa kiinnostavalta, mutta voit saada haittaohjelmatartunnan sellaisesta. Vältä siis vieraita laitteita, **äläkä ikinä liitä niitä koneeseesi.**

5

Kyseenalaista se, mitä näet ja kuulet

Älä usko kaikkea, mitä näet tai kuulet. Huijaussivustot näyttävät aidoilta, ääntä voidaan väärentää ja hyökkäys voi tulla myös tutun tahon nimissä. Nykypäivänä tulee olla kriittinen ja kyseenalaistaa se tieto, mitä kohtaa.

Kyberhygienia on siis ajattelutapa.

Nämä viisi tapaa on hyvä omaksua osaksi päivittäistä tekemistä – lista ei ole kuitenkaan täydellinen.

Enemmän kuin pelkästään tietyt tavat toimia, kyberhygieniassa tärkeintä on olla aktiivisesti tietoinen omasta toiminnasta ja **miettiä, onko se turvallista**.

Kyberturvallisuus ja työturvallisuus

Kyberturvallisuus on osa **työturvallisuutta**.

Molemmat näistä koskettavat kaikkia yrityksessä toimivia henkilöitä.

On toki selvää, että yrityksen johto on vastuussa kyberturvallisuuden ja työturvallisuuden toteutumisesta yrityksessä.

Jokaisen yrityksessä on kuitenkin hyvä huomioida, että huolimaton toiminta voi mahdollistaa kyberviholliselle **helpomman tien** yrityksen järjestelmiin.

Tällöin kyberviholliset voi vakavissa tapauksissa vaikuttaa jopa fyysiseen maailmaan. Vaikutukset voivat kohdistua siis myös työturvallisuuteen.

Älä ole helppo kohde kyberviholliselle!

Huolimaton toiminta tekee rikollisten elämästä helpompaa ja sitähän me emme halua. Turvallisella toiminnalla ylläpidetään omaa ja työelämässä koko työyhteisön turvallisuutta.

Älä siis ole helppo kohde kyberviholliselle,
vaan **pidä huolta kyberhygieniastasi**.

Tee rikollisten elämästä vaikeampaa
ja toimi kyberturvallisesti!

Tämä opas on **Satamalogistiikan kyberhygienia** -hankkeen tuottama käsikirja **Sinulle** turvallisempaan elämään tietoverkoissa, myös tulevaisuudessa.

Tekijät: Tuomas Heikkinen ja Vesa Tuomala