



Tietoturvan ABC

Hyvää kyberhygieniaa
työpäivään!



Kyberturvan tulevaisuus Kymenlaaksossa -hanke



KYMEN
LAAKSON
LIITTO



Euroopan unionin
osarahoittama

Tämä käsikirja auttaa sinua oppimaan ja kertaamaan digiturvan perusohjeet, jotta voit käyttää verkkoa ja laitteita turvallisemmin.

Sisällys

Mitä on kyberturva?	3
Miksi kyberturvallisuus on tärkeää?	4
Mihin varautua? - Tietojen kalastelu	5
Mihin varautua? - Sosiaalinen manipulointi	6
Sosiaalisen manipuloinnin pääpiirteet	7
Mihin varautua? - Haittaohjelmat	8
Hyvä kyberhygienia – Turvalliset toimintatavat arjessa	9
Kyberturvallisuus työpaikalla	10
Mitä teet jos epäilet kyberhyökkäystä?	11-12

Mitä on **kyberturva**?

Kyberturvallisuus tarkoittaa tapoja, joilla suojaamme tietomme, laitteemme ja järjestelmämme verkossa tapahtuvilta vahingoilta ja rikoksilta.

Samalla tavalla kuin lukitsemme kotioven tai tarkastamme, että kahvinkeitin on pois päältä, meidän täytyy suojata myös tietokoneet, puhelimet ja yrityksen järjestelmät.



Miksi **kyberturvallisuus** on **tärkeää**?

Hyvä kyberturva varmistaa tietojen turvassa pysymisen ja mahdollistaa jatkuvan toiminnan.

Tieto on arvokasta – se voi olla asiakastietoa, tuotantosalaisuuksia tai sopimuksia.

- Yritystietojen ja erityisesti sensitiivisten tietojen vuotamista kutsutaan tietovuodoksi.
- Yksityishenkilöllä esimerkiksi henkilötunnuksen vuotaminen voi altistaa identiteettivarkaudelle.

Rikolliset pyrkivät pääsemään useita eri kanavia kautta sisään yritysjärjestelmiin.

- Yleisin kanavista on ihminen, jota huijaamalla rikolliset mahdollistavat helpon pääsyn.



Kyberturvallinen toiminta on osa meidän kaikkien arkea, ja auttaa meitä suojautumaan näkymättömiä kyberuhkia vastaan.

Mihin **varautua?**

Tietojen kalastelu

Huijarit lähettävät sähköposteja tai viestejä, jotka näyttävät aidoilta.

Tavoite 📌

Saada sinut klikkaamaan linkkiä, avaamaan liite tai antamaan tunnuksesi.

Muista !

Suhtaudu varauksella viesteihin, jotka tulevat tuntemattomista lähteistä, painottavat kiirettä ja koittavat saada sinut klikkaamaan tai lataamaan jotain.

Tarkista lähettäjän osoite huolellisesti ja varmista henkilöllisyys jotain toista kautta kuin mistä viesti tai pyyntö on alunperin tullut, esim. soittamalla.

Älä koskaan anna tunnuksiasi, jos niitä pyydetään. Esimerkiksi viranomaiset eivät koskaan pyydä tunnuksiasi toimintaansa varten.

Mihin **varautua?**

Käyttäjän manipulointi (sosiaalinen manipulointi)

Rikolliset käyttävät **sosiaalista manipulointia** ihmisten “hakkeroinmiseen”. Esimerkiksi iso osa **kalastelu- ja huijausviesteistä** käyttää sosiaalista manipulointia hyväkseen.

Rikollinen yrittää saada sinut toimimaan haluamallaan tavalla – esimerkiksi 📵

- **Tekeytyy** IT-tueksi ja pyytää salasanaa.
- Yrittää tulla toimitiloihin ilman lupaa.
- Koittaa saada sinut **lataamaan** haitallisen tiedoston.

Muista !

- Suhtaudu suurella varauksella tietopyyntöihin.
- Älä päästä turvatiloihin tai vain henkilökunnalle tarkoitetuille alueille tuntemattomia sisään ilman lupaa.
- Jos laite on sinulle tuntematon tai löytyy oudosta paikasta (esim. muistitikku parkkipaikalla), älä liitä niitä tietokoneeseesi.

Sosiaalisen manipuloinnin pääpiirteet

Auktoriteetti — tekeytymällä esim. pomoksi, viranomaiseksi tai IT-tueksi.

Kiire tai paine — kiireellinen pyyntö, joka pyrkii ohittamaan kriittisen ajattelun.

Sosiaaliset siteet / miellyttävyys — kohtelias ja ystävällinen lähestymistapa madaltaa epäilyjä.

Vastavuoroisuus — tarjoamalla apua tai etuja koitetaan toinen saada antamaan vastapalvelus.

Sosiaalinen yhteenkuuluvuus — viesti antaa vaikutelman, että “muutkin tekivät näin”.



Mihin **varautua**?

Haikkaohjelmat

Haikkaohjelman tarkoituksena on **vahingoittaa, häiritä tai varastaa tietoja** tietokoneelta, puhelimelta tai verkosta. Haikkaohjelma voi toimia salassa, varastaa salasanojasi, salata tiedostosi lunnaita vastaan tai muuttaa laitteesi toimintoja.

Kuinka haikkaohjelmat leviävät? 📇

- Sähköpostin liitteet ja haitalliset linkit.
- Ladattavat tiedostot epäluotettavilta sivuilta tai torrentit/piratismi.
- Haitalliset mainokset (malvertising).
- Tuntemattomista USB-tikuista tai ulkoisista kovalevyistä.
- Haavoittuvuuksien (päivitysten puutteiden) hyväksikäyttö.
- Huijauksilla saatu pääsy (esim. troijalainen esittäen päivitystä tai työkalua).

Hyvä kyberhygienia – **turvalliset** tavat arjessa

Kyberhygienia on kuin käsienpesu: pieni teko, joka estää suuria ongelmia. Tee turvallisista tavoista rutiini.

1. Toimi salasanojen kanssa oikein

- Älä käytä samaa salasanaa eri paikoissa.
- Käytä pitkiä salasanoja (väh. 16 merkkiä).
- Luo salalause kuten
“kissakiipesikatollekatsomaangorillaa”.
- Käytä salasanojen hallintasovellusta.
- Ota käyttöön monivaiheinen tunnistautuminen (MFA/2FA).

2. Lukitse laitteesi

Lukitse tietokone ja puhelin aina, kun poistut työpisteeltä — vaikka vain kahville.

3. Mieti ennen kuin klikkaat

Jos viesti tai liite tuntuu oudolta, älä avaa sitä. Kysy IT-tuelta tai esimieheltä ennen kuin toimit.

4. Älä käytä vieraita laitteita

Älä koskaan liitä tuntemattomia muistitikkuja tai laitteita koneeseesi. Ne voivat sisältää haittaohjelmia.

5. Kyseenalaista

Älä usko kaikkea, mitä näet tai kuulet verkossa. Nykyään myös ääntä, kuvia ja videoita voidaan väärentää.

Kyberturvallisuus työpaikalla

Kyberturvallisuus on osa työturvallisuutta. Toimimalla turvallisesti voit ennaltaehkäistä riskejä ja suojella itseäsi, työkavereitasi sekä työpaikkaasi.

Työntekijän vastuu:

- Käytä yrityksen laitteita vain työasioihin.
- Säilytä salassa pidettävät tiedot huolellisesti.
- Ilmoita heti epäilyttävästä sähköpostista, laitteesta tai toiminnasta IT-tuelle.
- Noudata yrityksen tietoturvaohjeita.

Johdon vastuu:

- Tarjota turvalliset työvälineet ja koulutusta.
- Varmistaa, että kyberturvallisuus on osa yrityksen arkea.

Mitä teet jos epäilet kyberhyökkäystä?

**Jos epäilet, että työlaitteesi on
saastunut:**

Merkkejä voivat olla esim. tietokoneen hitaus, koneen tuulettimet ovat oudon äänekkäitä, työpöydälle ilmestyy lunnasvaatimus tai uusia kansioita.

Toimi näin:

1. Irrota laite verkosta mahdollisimman nopeasti:

- Katkaise Wi-Fi
- Irrota verkkokaapeli

2. Älä sammuta laitetta, ellet saa siihen ohjetta IT-tuelta. (Sammutus voi tuhota tutkittavaa tietoa.)

3. Ilmoita välittömästi IT-tuelle ja kerro, mitä tapahtui juuri ennen ongelmaa.

4. Älä avaa ohjelmia tai tiedostoja, äläkä liitä ulkoisia laitteita.

5. Odota ohjeita (IT voi eristää laitteen tai palauttaa varmuuskopioita).

Mitä teet jos epäilet kyberhyökkäystä?

Jos epäilet **salasanasi vuotaneen** tai **että tilisi on kaapattu**:

esim. tilillä näkyy outoa toimintaa, saat kirjautumisvahvistuksia, joita et tehnyt tai salasanasi ei enää toimi.

Toimi näin:

1. Ilmoita välittömästi IT-tuelle tai esihenkilölle.
2. Jos pääset käsiksi tiliisi, vaihda salasanat nopeasti ja laita kaksivaiheinen tunnistautuminen päälle viimeistään tässä vaiheessa.
3. Jos et pääse tilillesi Ilmoita työkavereille, että tilisi on mahdollisesti kaapattu ja varoita, että nimissäsi saattaa tulla kalasteluviestejä.

Kyberturvallisuus työpaikalla

Tilanne	Ensimmäinen toimenpide	Ilmoita
Epäilyttävä sähköposti	Älä klikkaa / älä vastaa	IT-tuki / esihenkilö
Haittaohjelmaepäily	Irrota laite verkosta	IT-tuki
Salasana vuotanut	Vaihda salasana turvalliselta laitteelta	IT-tuki
Some- tai käyttäjätili kaapattu	Vaihda salasana ja ilmoita	IT-tuki / viestintä

MUISTA!
Ilmoita mieluummin
turhaan kuin liian
myöhään.



Kyberkestävyyttä Kymenlaaksoon!

Katso lisää vinkkejä
oman & yrityksesi
tieto- ja kyberturvan
vahvistamiseen:

www.kyberasema.fi

Kyberturvan tulevaisuus Kymenlaaksossa -hanke



KYMEN
LAAKSON
LIITTO



Euroopan unionin
osarahoittama