



# Tietoturvan perusteet arjessa ja työelämässä

*Mallivastaus: sisällysluettelon, sivunumeroinnin ja kuvien rivityksen harjoitus*

Opiskelijan nimi

Opintojakso: TIE1

Syyskuu 2026

## Sisällysluettelo

|                                                   |   |
|---------------------------------------------------|---|
| 1 Johdanto.....                                   | 1 |
| 2 Tietoturvan perusteet.....                      | 2 |
| 2.1 Mitä tietoturvalla tarkoitetaan .....         | 2 |
| 2.2 Tietoturvan kolme osa-aluetta.....            | 2 |
| 3 Yleisimmät tietoturvauhat .....                 | 3 |
| 3.1 Haittaohjelmat .....                          | 3 |
| 3.2 Tietojenkalastelu.....                        | 3 |
| 3.3 Sosiaalinen manipulointi.....                 | 3 |
| 4 Suojautumiskeinot .....                         | 4 |
| 4.1 Salasanat ja tunnistautuminen .....           | 4 |
| 4.2 Ohjelmistopäivitykset ja suojausohjelmat..... | 4 |
| 4.3 Varmuuskopiointi.....                         | 4 |
| 5 Tietoturva organisaatioissa .....               | 5 |
| 5.1 Tietoturvapoliittikka .....                   | 5 |
| 5.2 Henkilöstön koulutus .....                    | 5 |
| 6 Yhteenveto .....                                | 6 |

# 1 Johdanto

Tietoturva on noussut viime vuosina yhä tärkeämmäksi taidoksi niin opiskelussa, työelämässä kuin arjessakin. Lähes kaikki toimimme päivittäin erilaisten digitaalisten palveluiden, laitteiden ja verkkojen parissa, ja jokainen näistä yhteyksistä voi olla myös mahdollinen riski. Tässä materiaalissa käydään läpi tietoturvan keskeisiä käsitteitä, yleisimpiä uhkia sekä keinoja, joilla riskejä voidaan pienentää.

Tämä on mallivastaus, jossa sivunumerointi alkaa vasta sisällysluettelon jälkeisestä sivusta numerosta 1, ja jossa kahta kuvaa on rivitetty tekstin sekaan eri tavoin: toinen "Tekstin tasossa" ja toinen "Tiivis"-rivityksellä.

## 2 Tietoturvan perusteet

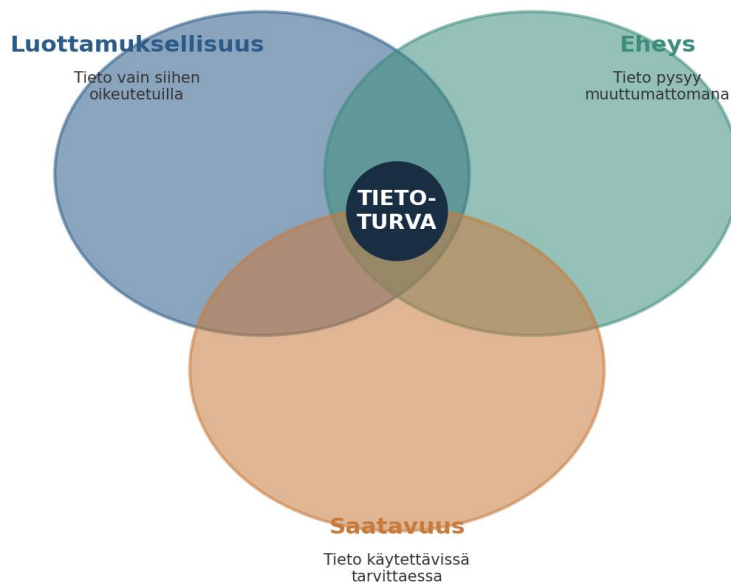
### 2.1 Mitä tietoturvalla tarkoitetaan

Tietoturvalla tarkoitetaan niitä toimenpiteitä, joilla suojataan tietoa, laitteita ja järjestelmiä luvattomalta käytöltä, muuttamiselta tai tuhoamiselta. Tavoitteena on varmistaa, että tieto on saatavilla oikeille henkilöille oikeaan aikaan, mutta ei kenellekään muulle. Tietoturva ei ole pelkästään tekninen kysymys, vaan siihen liittyy vahvasti myös ihmisten toiminta ja käyttäytyminen.

### 2.2 Tietoturvan kolme osa-aluetta

Tietoturvaa kuvataan usein kolmen käsitteen kautta: luottamuksellisuus, eheys ja saatavuus. Alla oleva kuva on lisätty asetuksella "Tekstin tasossa" (Rivitä teksti → Tekstin tasossa), jolloin kuva käyttäytyy kuin yksi iso tekstimerkki omalla rivillään eikä teksti kierrä sen ympärillä.

#### Tietoturvan kolme osa-aluetta



Kuva 1. Tietoturvan kolme osa-aluetta (rivitys: Tekstin tasossa).

Luottamuksellisuudella tarkoitetaan sitä, että tieto on vain siihen oikeutettujen henkilöiden käytössä. Eheys tarkoittaa, että tieto pysyy muuttumattomana ja luotettavana koko sen elinkaaren ajan. Saatavuudella puolestaan varmistetaan, että tieto ja palvelut ovat käytettävissä silloin, kun niitä tarvitaan.

## 3 Yleisimmät tietoturvauhat

### 3.1 Haittaohjelmat

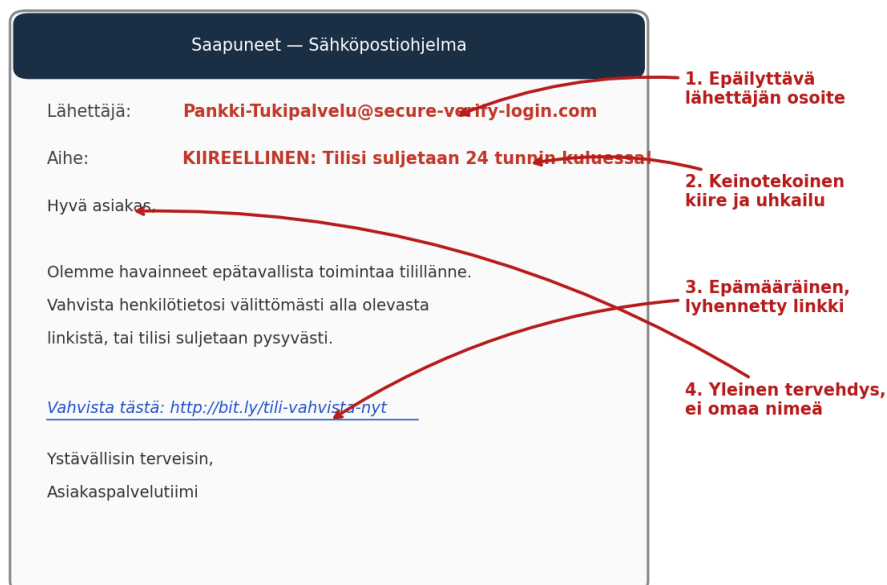
Haittaohjelmilla tarkoitetaan ohjelmistoja, jotka on suunniteltu vahingoittamaan laitetta, varastamaan tietoa tai häiritsemään järjestelmän normaalia toimintaa. Yleisimpiä haittaohjelmatyyppejä ovat virukset, madot, troijalaiset sekä kiristysohjelmat. Kiristysohjelmat ovat erityisen haitallisia, sillä ne salaavat käyttäjän tiedostot ja vaativat lunnaita niiden avaamisesta.

### 3.2 Tietojenkalastelu

Tietojenkalastelulla eli phishingillä tarkoitetaan huijausviestejä, joiden avulla yritetään saada käyttäjä luovuttamaan esimerkiksi salasanoja tai pankkitietoja. Viestit näyttävät usein aidoilta ja voivat jäljitellä tuttuja yrityksiä tai palveluita.

Tunnusmerkkejä ovat muun muassa kiireellisyyden korostaminen, epäilyttävät linkit sekä pyynnot syöttää henkilökohtaisia tietoja. Näiden tunnistaminen on tärkein yksittäinen keino suojautua tietojenkalastelulta.

#### Esimerkki tietojenkalasteluviestin tunnusmerkeistä



### 3.3 Sosiaalinen manipulointi

Sosiaalisella manipuloinnilla tarkoitetaan ihmisten psykologiseen käyttäytymiseen perustuvia huijausmenetelmiä, joilla pyritään saamaan uhri toimimaan hyökkääjän toivomalla tavalla. Tällaiset menetelmät voivat kohdistua esimerkiksi puhelimitse, sähköpostitse tai kasvojen tapahtuvaan viestintään, ja ne hyödyntävät usein luottamusta, kiirettä tai pelkoa.

## 4 Suojautumiskeinot

### 4.1 Salasanat ja tunnistautuminen

Vahva ja yksilöllinen salasana on yksi tehokkaimmista tavoista suojata omia tilejä. Suositeltavaa on käyttää eri palveluissa eri salasanoja sekä ottaa käyttöön kaksivaiheinen tunnistautuminen aina kun se on mahdollista. Kaksivaiheinen tunnistautuminen vaatii salasanan lisäksi toisen varmistuksen, esimerkiksi puhelimeen lähetettävän koodin.

### 4.2 Ohjelmistopäivitykset ja suojausohjelmat

Käyttöjärjestelmien ja sovellusten säännöllinen päivittäminen korjaa tunnettuja tietoturva-aukkoja, joita hyökkääjät voisivat muuten hyödyntää. Myös virustorjuntaohjelmiston ja palomuurin käyttö on suositeltavaa, sillä ne auttavat havaitsemaan ja estämään haitallista toimintaa ennen kuin se ehtii aiheuttaa vahinkoa.

### 4.3 Varmuuskopiointi

Säännöllinen varmuuskopiointi on tärkeä keino varautua tietojen menetykseen esimerkiksi laiterikon, varkauden tai kiristysohjelmahyökkäyksen sattuessa. Varmuuskopiot kannattaa tallentaa erilliselle tallennusvälineelle tai pilvipalveluun, jotta ne eivät tuhoudu samalla kertaa alkuperäisen aineiston kanssa.

## 5 Tietoturva organisaatioissa

### 5.1 Tietoturvapoliittikka

Monilla organisaatioilla on käytössään tietoturvapoliittikka, joka määrittelee yhteiset pelisäännöt tiedon käsittelylle ja laitteiden käytölle. Poliitikassa kuvataan esimerkiksi salasanaikäytännöt, etätyön tietoturvavaatimukset sekä toimintaohjeet tietoturvapoikkeamien varalle.

### 5.2 Henkilöstön koulutus

Koska suuri osa tietoturvapoikkeamista liittyy inhimillisiin virheisiin, henkilöstön säännöllinen kouluttaminen on keskeinen osa organisaation tietoturvaa. Koulutuksissa käydään läpi ajankohtaisia uhkia, kuten tietojenkalastelua, ja harjoitellaan tunnistamaan epäilyttäviä viestejä tilanteita.

Kuva 2. Tietoturvakoulutus organisaatiossa (rivitys: Neliö).



## 6 Yhteenveto

Tietoturva rakentuu teknisten ratkaisujen ja ihmisten toiminnan yhteisvaikutuksesta. Vahvat salasanat, ohjelmistopäivitykset, varmuuskopiointi sekä tietoisuus yleisimmistä uhkista muodostavat perustan, jonka avulla riskejä voidaan merkittävästi pienentää sekä yksityishenkilön että organisaation näkökulmasta. Tietoturva ei ole kertaluonteinen toimenpide vaan jatkuva prosessi, joka vaatii säännöllistä ylläpitoa ja päivittämistä.