Tietoturvallisuus

Miten suojaan tietokoneen ja matkapuhelimen?

Suojaa tietokone ja lähiverkko
Vastuusi tietosuojassa
Haittaohjelmista eroon
Älypuhelimet ja tabletit

KODIN TURVAOPAS
Ohjeita digitaaliseen arkeen
Turvallisuuskomitea

Porvoon Kansalliset Seniorit
Sakari Nikkanen kevät 2024

Suojaa tietokone ja lähiverkko

Tietoverkkojen käyttöön liittyy aina riskejä –
ei kannata liioitella/pelätä, vaan ottaa ne hallitaan

1. Pidä käyttöjärjestelmä, selain ja liitetyt laitteet päivitettynä
2. Pidä palomuuri päällä
3. Suojaa kodin lähiverkko
4. Pidä modeemi ja/tai reititin päivitettynä ja palomuuri päällä
5. Suojaa muut kodin älylaitteet
6. Hanki hyvä tietoturvaohjelma

Suojaa tietokone ja lähiverkko

Tietoverkkojen käyttöön liittyy aina riskejä –
ei kannata liioitella/pelätä, vaan ottaa ne hallitaan

1. Pidä kaikki käyttöjärjestelmät päivitettynä

- Tärkein suojatoimenpide
- Tulee päivityksiä, joissa ajantasaisia uusia suojauksia
- Laita automaattiset päivitykset päälle
- Windows 10/11, Crome/Edge, modeemi/reititin, sovellutukset…
- Katso, että päivitykset ovat aitoja

- Pyydä myyjää/asiantutijaa auttamaan tarvittaessa
- Hoida tietokoneen Asetuksien kautta (”Päivittäminen, suojaaminen”)

Suojaa tietokone ja lähiverkko

Tietoverkkojen käyttöön liittyy aina riskejä –
ei kannata liioitella/pelätä, vaan ottaa hallitaan:

2. Pidä päivitetty palomuuri päällä

- Estää haittaohjelmien pääsyn verkosta tietokoneelle

- Laita palomuuri päälle tietokoneen asetuksista (hae palomuuri)
- Laita myös modeemin ja/tai reitittimen palomuuri päälle
- Pidä palomuurit päällä jatkuvasti
- Päivitä palomuuriohjelmat uusimpiin versioihin

Suojaa tietokone ja lähiverkko

Tietoverkkojen käyttöön liittyy aina riskejä –
ei kannata liioitella/pelätä, vaan ottaa ne hallitaan

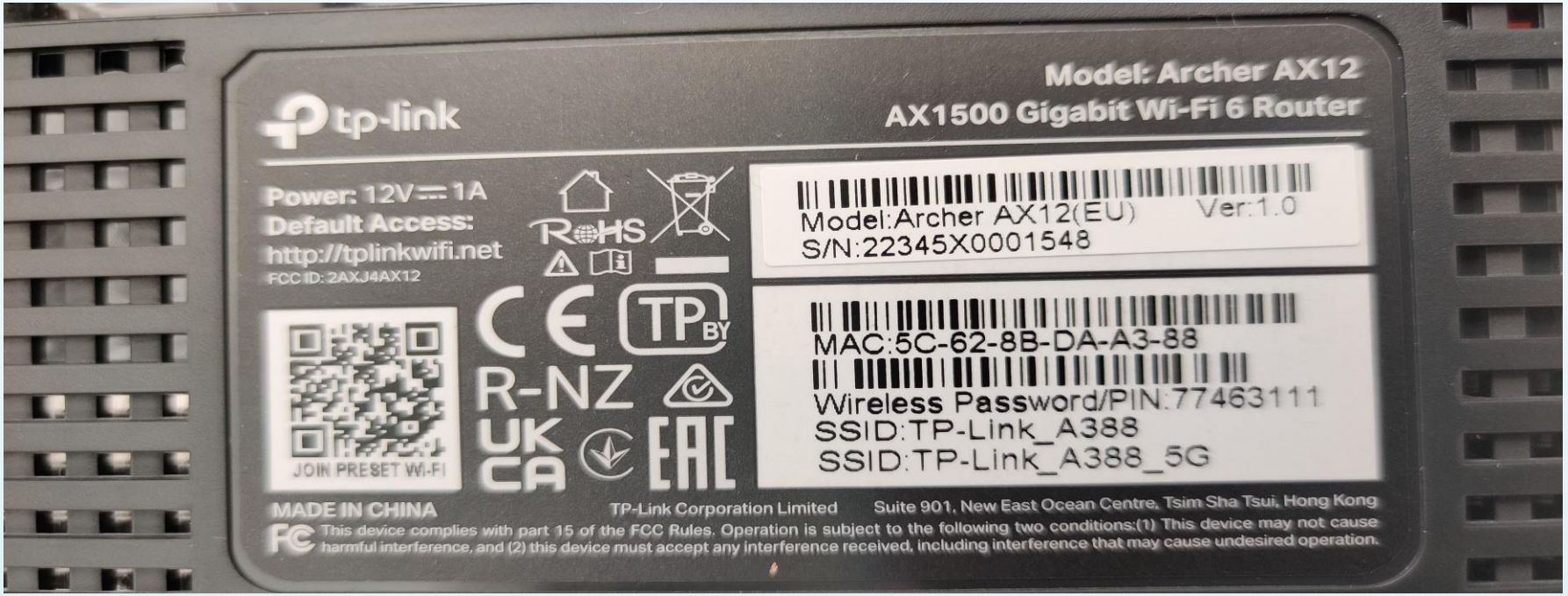
3. Suojaa kodin lähiverkko

- Radiosignaali reitittimestä kantaa jopa 100 m
- Pitää ehdottomasti suojata, avoin verkko on avoin kaikille

- Aseta oma PIN koodi, talleta PIN koodi huolellisesti
- Ota reitittimen takana olevasta tarrasta reitittimen osoite
- Muuta oletussalasana (Admin) omaksi salasanaksi

- Älä mene suojaamattomaan verkkoon ”Kahvilassa”
  - pyydä käyttäjätunnus ja salasana ja käytä suljettua verkkoa
  - Tyhjennä vieraan koneen selaushistoria

Reitittimen takatarra



Suojaa tietokone ja lähiverkko

Tietoverkkojen käyttöön liittyy aina riskejä –
ei kannata liioitella/pelätä, vaan ottaa ne hallitaan

4. Pidä modeemi ja/tai reititin päivitettynä ja palomuuri päällä

- Keskeinen turvatoimi massahakkeroinnille
- Estää haittaohjelmien pääsyn kodin tietoverkkoon

- Mene reitittimen hallintaohjelmaan ja varmista päivitys reititin
- Laita myös palomuuri päälle

- Joskus reititin ei päivity/ei pysty päivittämään – osta uusi.
- Pyydä tarvittaessa apua, esim. ostaessasi laitetta

Suojaa tietokone ja lähiverkko

Tietoverkkojen käyttöön liittyy aina riskejä –
ei kannata liioitella/pelätä, vaan ottaa ne hallitaan

5. Suojaa kodin muut älykoneet

- Monet koneet kytkeytyvät kodin tietoverkkoon ja sieltä.....
- Ulkopuolinen taho voi ottaa hallintaan kodinkoneet, jopa auton
- Yleensä hakkeri käyttää koneita palvelunestohyökkäyksiin

- Kysy ostaessa onko verkkoyhteys, pyydä tarvittaessa estämän
- Käyttäessäsi, suojaa kodinkoneet kuten tietokone
- Anna uusi pin koodi ja salasana sekä käyttäjätunnus

- Tämä on harvoin hyvin suojattu ja usein kaapattu etuoikeus
- Et tunnista helpolla tilannetta, verkko hitaus tai katkeilut

Suojaa tietokone ja lähiverkko

Tietoverkkojen käyttöön liittyy aina riskejä –
ei kannata liioitella/pelätä, vaan ottaa ne hallitaan

6. Hanki hyvä tietoturvaohjelma

- Netistä löytyy ilmaisia - varmista luotettavuus
- Nämä ohjelmat tunkeutuvat syvälle tietokoneeseen
- Riskit ovat suuret huonosta tai väärästä valinnasta
- Suosittelen kunnon tietoturvaohjelmia
  - Estävät tehokkaasti hyökkäykset
  - Päivittyvät ajantasaisesti
  - Varoittavat väärille sivuille menemisestä jne.
  - Roskapostisuojaus, varmuuskopiointi

- Kustannusten arvoinen hankinta ja merkitys tulee korostumaan mm. tekoälyn kautta
- Hävitä atk laitteesi huolella s.o. anna ammattilasien tehdä se

Tärkein tietosuoja olet sinä

Mikään tekniikka ei pysty suojamaan laitteita ja verkkoa, jos käyttäjä on huolimaton ja varomaton

1. Satsaa salasanoihin

- Salasanojen oikea käyttö on tärkein tietoturvallisuuden avain
- Tärkeimmät salasanat ovat:
  1. Sähköpostisi salasana
  2. Tietokoneesi salasana
  3. Salasanatiedoston salasana
- Käytä useita erilaisia salasanoja, tallenna ne turvallisesti
- Hyvä salasana:
  - PITKÄ, erikoismerkit, isoja ja pienet merkit jne
  - Suosi lauseita ja suomenkielisiä taivutettuja sanoja
  - Testaa murrettavuus (älä anna oikeita salasanoja)
- Ota salasanapalveluohjelma käyttöön
  - Varo väärää palvelutarjontaa

- https://yle.fi/aihe/artikkeli/2017/02/01/digitreenit-17-salasanakone-testaa-kuinka-nopeasti-salasana-murretaan
- Howsecureismypassword.net

Tärkein tietosuoja olet sinä

Mikään tekniikka ei pysty suojamaan laitteita ja verkkoa,
jos käyttäjä on huolimaton ja varomaton

1. Opettele sähköpostin turvallinen käyttö

Sähköpostien kautta leviää haittaohjelmat, huijaukset ja haitat

- Tarkista lähettäjä, nimi on helppo väärentää
  - Pistä hiiri töihin ja varmenna lähettäjän osoite
  - Suhtaudu kriittisesti myös tuttavaviesteihin, katso alkuperä
- Avaa sähköpostien linkit varovasti, älä anna mitään tietoja
  - Älä avaa tuntemattomien lähettäjien liitteitä
  - Varo liitteitä joissa päätee .COM tai .EXE tai .VBS tai .PIF
  - Mene palvelun oikeille sivuille **selaimen** kautta, vertaa osoite

- Järki hoi – älä jätä!
  - esim. pankki tai poliisi ei ota yhteyttä sähköpostilla

Tärkein tietosuoja olet sinä

Mikään tekniikka ei pysty suojamaan laitteita ja verkkoa,
jos käyttäjä on huolimaton ja varomaton

2. Pidä tietosi turvassa

Joskus tiedot vaan katoavat – näin käy kaikille

- Tieto voi joutua rikollisten käsiin: varastetaan tai lukitaan
  - Internetyhteys – tarvitseeko olla joka koneessa?
  - Hyvä tietoturva järjestettävissä, kaikkialla käytettävissä
- Pane päälle jatkuva varmuuskopiointi
  - Ota tiedostoistasi varmuuskopiot - USB, ulkoinen levy tai pilvi
  - Ulkoinen muistiväline ei saa olla aina kiinni koneessa
  - Älä laita vierasta muistitikkua kiinni koneeseen
- Pilvipalvelu on oikein käytettynä paras ratkaisu
  - Ei voi varastaa, ei pala, ei hajoa jne.
  - Esim. OneDrive, helppo ja edullinen

Haittaohjelmista eroon

Valitettavasti haittaohjelmia pääsee suojausten läpi aina.
Internet on tehokas ja edullinen väline levittää niitä.

3. Kiristysohjelmat

On vain ajan kysymys milloin kohtaat tämän

- Syy: lataat kiristysohjelman tavalla tai toisella koneeseesi
  - Ohjelma lukitsee koneen ja vaatii avausmaksua
  - Ohjelma uhkaa sinua jollain toimilla ja vaatii rahaa
- Yleensä pakotetaan pikatoimiin, jottei ”vahinko” suurene
  - Voi esiintyä poliisina, verottajana, pankkinasi
  - Pyydetään maksamaan sakko tai pankkitunnuksia jne.
  - Tekoälyllä luodut ihmiset
- Toimi harkitusti
  - Irrota kone verkosta, käynnistä virustorjuntaohjelma
  - Älä maksa lunnaita, ongelma ei yleensä poistu
  - Ilmoita poliisille, vie kone tarvittaessa puhdistettavaksi

Haittaohjelmista eroon

Valitettavasti haittaohjelmia pääsee suojausten läpi aina.
Internet on tehokas ja edullinen väline levittää niitä.

4. Vakoilu ja tietojen kalastelu

On vain ajan kysymys koska kohtaat myös tämän

- Vakoiluohjelmat keräävät tietoja käyttäjästä ja myyvät eteenpäin
  - Sniffer – tallentaa koneen ja internetin liikennettä
  - Keylogger – seuraa näppäinten painalluksia ja nauhoittaa ne
- Tartunnan voit saada esim.
  - Netistä ladatun ilmaisohjelman mukana
  - Tietojenkalasteluohjelmien kautta - tosi kova tarjous jne
  - Sähköpostilla, saastuneet nettisivut
- Toimi järkevästi:
  - Tunnista kalastelu, älä avaa postia saati sen liitteitä
  - Älä koskaan anna pankkitunnusta luottokorttia tai sp-osoitetta

Haittaohjelmista eroon

Valitettavasti haittaohjelmia pääsee suojausten läpi aina.
Internet on tehokas ja edullinen väline levittää niitä.

5. Tietokoneen kaappaus palveluestohyökkäykseen

Olet ehkä jo ollut auttamassa palvelunestoa

- Kaappausohjelma saadaan yleensä liitteiden mukana
  - Käytetään tietokonettasi lähettämään palvelupyyntöjä
  - Samalla kaapataan kaikki älylaitteet mukaan palveluestoon
- Tunnistat koneen oudosta käyttäytymisestä tai uhkaviestistä
- Jos epäilet kaappausta, irrota tietokone ja modeemi verkosta
  - Käynnistä virustorjuntaohjelma
  - Vie kone ammattilaisen puhdistettavaksi, ei onnistu itseltä
  - Älä maksa kiristäjälle – ilmoita poliisille

Älypuhelimet ja tabletit

Älypuhelin ei ole vaan puhelin, vaan mukana kulkeva Internetissä kiinni oleva tietokone.

Paljon tietoturvariskejä huonolla hoidolla

1. **Vaihda SIM kortin tunnusluku**
   - Vaihda SIM kortin tunnusluku puhelimella heti hankinnan jälkeen
   - Aseta pidempi kuin 4 numeroa, vaikeasti arvattava sarja
2. **Ota käyttöön puhelimen automaattinen lukitus**
   - Lyhyt sulkeutumisviive, estää tehokkaasti ei-toivotun käytön
3. **Suojaa puhelin suojakoodilla tai salasanalla**
   - Sormenjälkitunnistus on helppo ja varma tapa
   - SIM koodi suojaa pääsyn verkkoon - ei pääsyä puhelimeen
4. **Varkauden hallinta**
   - Lataa varkaudenhallinta sovellus puhelimeen (myös ilmaisia)
   - Voit paikallistaa puhelimen, lukita ja tyhjentää sen, kuvata varkaan

Älypuhelimet ja tabletit

Älypuhelin ei ole vaan puhelin, vaan mukana kulkeva Internetissä kiinni oleva tietokone.

Paljon tietoturvariskejä huonolla hoidolla

5. **Huolehti varmuuskopioinnista**
   - Pilvitallennus helpoin tapa, tiedot myös muiden atk laitteisesi käytössä
   - Puhelimen muistikortti yksin ei ole riittävä ratkaisu

6. **Käytä puhelinta fiksusti**
   - Varo puhelimesi lainaamista
   - Älä soita takaisin tuntemattomiin numeroihin
   - Tunnista huijaukset ja siirtymiset epävarmoille sivuille
   - Älä tallenna salasanoja puhelimeesi
   - Käytä puhelun ja viestien estoa
   - Hävitä puhelin järkevästi