TIETOTURVA

DIGITAIDOISTA VIRTAA – TEKOÄLYN KÄYTTÄMINEN JA TIETOTURVA

MIKSI TIETOTURVA ON TÄRKEÄÄ?

- Haasteet tietoturvan näkökulmasta
  - Tietovuodot
  - Hakkerointi
  - Tietojen manipulointi
  - Identiteettivarkaudet
  - Haittaohjelmat ja virukset
  - Palvelunestohyökkäykset

TURVALLISUUDEN PERUSASIOITA?

- Digilaitteiden suojaus
- Vanhentuneet ohjelmistot ja päivittäminen
- Salasanat ja käyttäjätunnukset
- Monikerroksiset suojausmenetelmät (MFA)
- Toimintaympäristön huomiointi (shoulder surfing)
- Toiminta verkossa (ssl-salaus, url-osoite)
- VPN, evästeet ja seurannan merkitys

DIGILAITTEIDEN SUOJAUS

- Virustorjunta ja palomuuri
  - Maksullisille vaihtoehdoille ei tarvetta, jos
    - Turvalliset verkkokäytännöt tiedossa
    - Huolellisuus linkkien ja liitetiedostojen kanssa
    - Verkkolataaminen tunnetuilta sivustoilta
    - Ohjelmistot ajantasalla

Jos noudatat hyviä tietoturvakäytäntöjä, Windows Defender on täysin riittävä useimmille yksityishenkilöille!

Maksullinen lisäturva saattaa olla hyödyllinen yrityskäytössä tai jos käsittelet arkaluontoista tietoa.

TURVALLISET VERKKOKÄYTÄNNÖT

HTTP (hypertext transfer protocol) on verkkoprotokolla, jossa tieto välittyy internetissä salaamattomana.

HTTPS (hypertext transfer protocol secure) on verkkoprotokolla, joka käyttää salausta (tls/ssl) suojatakseen tiedonvälityksen internetissä, mikä tekee siitä turvallisemman kuin http.

TURVALLISET VERKKOKÄYTÄNNÖT

URL-osoite on globaalisti uniikki

Domainpääte on URL-osoitteen lopussa oleva tunnuspääte (.fi .com .net .media .auto)

Vapaana oleva domain voidaan varata esimerkiksi webhotellipalvelusta. Esimerkki

TURVALLISET VERKKOKÄYTÄNNÖT

Sähköposti

Linkit sähköpostissa tai viestipalveluissa voivat johtaa tietoja kalastelevalle sivustolle.

Selvitä asiat vain suoraan **palveluntarjoajan sivustolta**.

Älä lähetä arkaluontoisia tietoja sähköpostitse.

TURVALLISET VERKKOKÄYTÄNNÖT

Salasana ~~tulee olla vähintään 8 merkkiä~~

Salasanan pituudeksi suositellaan vähintään 15 merkkiä (Kyberturvallisuuskeskus)

Salasanassa tulee käyttää vähintään yhtä erikoismerkkiä **()&@$** suuraakkosta ja numeroita. Erikoismerkeistä ***AltGr***-painikkeelliset ovat tehokkaampia.

Salasana voi olla salasanalause, jossa käytetään kahta sanaa. Turvallisuutta tehostaa murresanojen käyttö.

Joissain kriittisissä järjestelmissä erikoismerkeistä esimerkiksi huutomerkki ei ole sallittu sen runsaan käytön vuoksi.

ilakoiva395&Kantarelli

Tussahteleva4(3)kiwi

Virallinen3§9varaani

Toimitteleva564£vohveli

TURVALLISET VERKKOKÄYTÄNNÖT

Käyttäjätunnus (erityisesti WordPress)

Käyttäjätunnuksena voi käyttää mahdollisuuksien mukaan jotain, jota ei voida yhdistää omaan nimeen.

Voit lisätä siihen myös jonkin numeron tai numeroita.

Kiellettyjä käyttäjätunnuksia ovat esim. admin, administrator, ylläpito tai ylläpitäjä tai muu helposti arvattava.

TURVALLISET VERKKOKÄYTÄNNÖT

Tunnistautumisen menetelmät

Yksinkertainen tunnistautuminen
Heikoin tunnistautuminen käyttäjätunnuksella ja salasanalla

Kaksivaiheinen tunnistautuminen
Käyttäjän todennus toisella laitteella tai palvelulla.

Pankkitunnistautuminen
Vahva tunnistautuminen, jossa tunnistaudutaan pankkitunnistautumisella tai henkilökortilla.

OMA TOIMINTA

Shoulder Surfing eli olan yli surffaaminen tapahtuu helposti vaikka elokuvissa tai muissa julkisissa tiloissa digilaitteita selatessa. Varmistu, että yksityisiä tietojasi vuoda ympäristöön, kun selaat laitettasi.

Kirjautumistiedot kannattaa kirjoittaa ylös johonkin (voi tallentaa omalle koneelle tiedostoon, jos laitteen tietoturva on kunnossa. Suojaa salasanat kirjoittamalla ennen salasanaa esimerkiksi 5 merkkiä, jotka eivät kuulu salasanaan). Paras vaihtoehto on muistaa salasanat

QR-koodit: Tarkista QR-koodin lähde ennen skannausta. Jos se on peräisin tuntemattomasta tai epäilyttävästä lähteestä, vältä sen avaamista.

- QR-koodi voi sisältää linkin tietoja kalastelevalle sivustolle
- QR-koodit on skannattu, ne voivat käynnistää haittaohjelmien lataamisen ja asennuksen, mikä vaarantaa henkilökohtaiset tiedot.

OMA TOIMINTA

Ota kaksivaiheinen tunnistautuminen käyttöön kaikkialla missä se on mahdollista.

Käytä esimerkiksi Google Authenticator-sovellusta, jolla kaksivaiheinen tunnistautuminen voidaan ottaa käyttöön missä tahansa.