NEUVOJAN DIGITAIDOT 1

TIETOTURVA, DIGITURVALLISUUS

Tietoturvan määritelmä

Tietoturvalla tarkoitetaan tietojen, järjestelmien, palveluiden sekä tietoliikenteen suojaamista.

Tietoturva koskee kaikkia riippumatta tietojen käsittelytavasta: suullisesti, paperilla tai tietokoneella.

Kannattaa miettiä miten oma tietoturva parhaiten toteutuu. Kaikilla on ”salattavaa” ja menetettävää, vaikkei siltä ensin tuntuisikaan.

Tietoturvan yhteydessä puhutaan tiedon **luottamuksellisuudesta, eheydestä, käytettävyydestä** sekä **todentamisesta**.

Tietoturvan määritelmä

Milloin tieto on turvassa:

- **Luottamuksellisuus** – Tiedot eivät joudu vääriin käsiin ja tiedot vain sillä jolla oikeus niitä käyttää. Luottamuksellisuudella tarkoitetaan sitä, että tiedot ja järjestelmät ovat vain sellaisten henkilöiden käytettävissä, joilla on oikeus niiden käyttöön. Eli ulkopuolisille ei saa antaa mahdollisuutta lukea, muuttaa tai tuhota tietoja.
- **Todentaminen** - Todentaminen tarkoittaa osapuolten (henkilö tai järjestelmä) luotettavaa tunnistettavuutta. Todentamisessa käytetään esim. muuttuvia avaintunnuksia ja salasanoja.
- **Käytettävyys/saatavuus** – Käytettävyydellä tarkoitetaan sitä että tiedot ja palvelut ovat riittävän nopeasti ja turvallisesti saatavilla ja vain niihin oikeutettujen henkilöiden käytettävissä (esim. mitäs jos netti ei toimi?)
- **Eheys** – Eheys tarkoittaa sitä, että tietojen ja järjestelmien tulee olla luotettavia, oikeita ja ajantasaisia myös ongelmatilanteissa (laitteisto- tai ohjelmistoviat, poikkeustilanteet, inhimilliset virheet). Eheyteen voidaan vaikuttaa mm. tietojen päivittämisellä ja varmuuskopioinnilla. Tiedot paikkaansa pitäviä ja helposti löydettävissä .

Mikä on arvokasta tietoa?

- **Yksityiset tiedot**
  - Salasanat, käyttäjätunnukset
  - Terveys- ym. yksityiset tiedot
  - Tilitiedot

- **Muuten arvokkaat tiedot**
  - Salassa pidettävät tiedostot/ohjelmat
  - Paljon työtä/tietoa sisältävät tiedostot
  - Ainutlaatuiset tiedot
  - Valokuvat

- **Laitteet**
  - tietokoneet, tabletit, puhelimet
  - Kovalevyt, muistitikut…

Missä sitä tietoa sitten on?

LAITTEET

Tietokone, läppäri, tabletti, puhelin

CD/DVD/bluray, muistitikut, ulkoiset kovalevyt, Kamera ja sen muistikortit

PALVELUT

Sähköposti

Facebook ja sosiaalinen media yleensäkin, keskusteluryhmät, Chat ja muut pikaviestipalvelut

Omat ja muiden kotisivut

Kuvapalvelut, pilvitallennus ja varmuuskopiontipalvelut

PAPERIT

Salasanat, tunnuslukutaulukot

Lääkärintodistukset, takuupaperit, kuitit, sopimukset

Valokuvat, muistiinpanot

OMAT PUHEET

Hyvä tietoturva

- **Asenne**
  - Tiedon arvon ymmärtäminen
  - Riskien tiedostaminen ja siihen vakavasti suhtautuminen
- **Osaaminen**
  - Osataan huolehtia tietoturvasta
  - Varmuuskopiot, salasanat
  - Riskien minimointi ja kriittinen suhtautuminen mahdollisiin uhkiin
- **Tekniikka**
  - Huolehditaan laitteista ja ohjelmistoista
  - Virustentorjunta

Riskit

- **Käyttäjä itse**
  - Suurimmat riskit tietoturvalle johtuvat itse käyttäjästä
  - 80-90% tietoturvaongelmista johtuu käyttäjästä itsestään
  - Lapset, muut käyttäjät
  - Inhimilliset erehdykset
  - Ohjelmisto-ongelmat, laitteistovauriot

- **Muut**
  - 10-20% riskeistä
  - Kosteus, kuumuus, pöly, kolhut
  - Tulipalot, vesivahingot
  - Ilkivalta, varkaudet, murrot
  - Virukset ym.

Miksi?

- Ilkivalta
  - tietomurrossa voidaan varastaa ja poistaa tiedostoja, vahingoittaa tietokonetta jne
- Rahan ansaitseminen
  - hyökkääjä voi esimerkiksi muuttaa käyttämäsi tietokoneen roskapostia lähettäväksi palvelimeksi ja tällä tavoin ansaita rahaa tai kiristää sinua arkaluontoisilla tiedoilla
- Poliittiset tai ideologiset syyt
  - hyökkääjä voi käyttää tietokonetta esimerkiksi palvelunestohyökkäyksiin. Palvelunestohyökkäysten tarkoitus on estää tai hidastaa tietyn palvelun toimintaa
- Piratismi
  - hyökkääjä voi hyödyntää verkkoa tiedostojen laittomaan jakamiseen

Virukset

Troijalainen
- Sisältää käyttäjälle haitallisia ominaisuuksia, joista käyttäjä ei ole tietoinen. esim. etähallintaominaisuuksia.

Madot
- Liikkuvat itsenäisesti etsien saastutettavaksi kelpaavaa tietojärjestelmää.

Tiedostovirukset
- Tarttuvat ohjelmiin ja suorittavat jonkin toiminnon koneella.

Levykevirukset
- Koneen käynnistäminen viruksen sisältämältä levyltä tai muistitikulta aikaansaa virustartunnan.

Makrovirukset
- on ohjelmoitu jonkin ohjelman, kuten esimerkiksi Wordin/Excelin käyttämällä makrokielellä.

Mainos- ja vakoiluohjelmat

- pieniä ohjelmia jotka asentuvat koneelle joiltakin Internet-sivuilta.
- eivät tee tuhoja, mutta keräävät tietoja esimerkiksi mainontaa varten. Vakoiluohjelmat voivat kerätä myös salasanoja ja käyttäjätunnuksia.
- Älä hyväksy (klikkaa) mitään Internet-sivuilta esiin aukeavia sivuja, jotka pyytävät asentamaan ohjelmia tai päivityksiä
- Mieti hetki ennen kuin asennat uusia ohjelmia

Huijaustyyppejä

Käyttäjän manipulointi

- soitetaan esim. poliisin, pankin tai Microsoftin nimissä ja urkitaan tietoja – esim. tunnuslukuja

Phishing- eli urkintahuijaukset

- Tietojen kalastelua, eli pyrkimystä saada henkilökohtaisia tietoja väärennetyllä verkkosivulla – esim. väärennetty pankin sivusto. Jos epäilet verkkosivua tai sähköpostia huijaukseksi, tarkista ainakin ensin linkin osoite. Varo myös lähes identtiseksi valittuja osoitteita.

Nigerialaiskirjeet ja muut sähköpostin rahankerjuuviestit

Lotto- ja arpajaishuijaukset

- kerätään yleensä sähköpostiosoitteita

Huijausvaroitukset eli Hoax-viestit

- Vaikkapa väärennetty varoitus viruksesta ja kehotus jakaa viestiä eteenpäin, ohjeet voivat olla haitallisia -> älä lähetä hoax-viestejä eteenpäin tai vastaa niihin. Varo muutenkin kiertokirjetyyppisiä lähetyksiä.

Huijaustyyppejä

Pop up-ikkunat

- Selaimen avaamat pienoisikkunat. Monesti harmittomia ja ärsyttäviä mainoksia ym. mutta voivat myös sisältää haitallisia linkkejä. Älä klikkaa OK ym. painikkeita – voivat viedä sinut huijaussivustolle tms.
  Useimmat selaimet voi asettaa estämään Pop up-ikkunat.

Myyjän tai ostajan huijaaminen verkossa

- Osto/myyntipalstat, Tori.fi, Facebookin myyntipalstat jne
- Pyri selvittämään asioita myyjästä, kaupat kasvotusten, onko uusi profiili, onko aito kuva, postiennakko

Romanssihuijaukset

- rahaa nettirakkaalle tyyppiset huijaukset

Valelaskut

- enemmän yrityksille suunnattuja

Huijaussoitot

- pyrkivät saamaan sinut soittamaan takaisinpäin maksullisiin numeroihin

Ystävien/sukulaisten nimissä lähetetyt avunpyynnöt

Roskapostin välttäminen

- Katso minne kirjoitat sähköpostiosoitteesi.
  - Vältä kirjoittamasta osoitettasi oikeassa muodossa julkisille verkkosivuille.
- Vältä osallistumista turhiin arvontoihin ym
- Älä koskaan vastaa roskapostiviesteihin.
- Äläkä pyydä roskapostin lähettäjää poistamaan sähköpostiosoitettasi postituslistalta.
- Ota omasta sähköpostiohjelmasta kuvien automaattinen näyttäminen pois päältä.
  - Näistä jää tieto mainostajalle ja roskaposti lisääntyy entisestään.
- Jos joudut rekisteröitymään johonkin palveluun josta epäilet tulevan roska- tai mainospostia, tee tätä varten oma sähköpostiosoite, jota käytät vain tähän tarkoitukseen.
- Käytä aktiivisesti roskapostin suodatusta.

Hyvä tietoturva

- Salasanat
  - Hyvä salasana on riittävän pitkä ja monimutkainen. Käytä yhtä salasanaa vain yhdessä palvelussa. Äläkä kerro salasanojasi muille.
  - Älä kirjaudu esim. Facebook- tai Google-tunnuksilla palveluihin, älä kirjoita salasanojasi paperilapuille. Vaihda salasanoja välillä
- Klikkaile harkiten
  - Sähköpostin liitetiedostot voivat sisältää haittaohjelmia tai haitallisia linkkejä.
  - Jos et varmasti tunne lähettäjää tai epäilet linkin/liitteen aitoutta, älä klikkaa
  - Haitallisia linkkejä liikkuu myös sosiaalisessa mediassa, internetsivustoilla ja tekstiviesteissä
  - Lähtihän sähköposti varmasti oikeaan osoitteeseen
- Vältä huijaukset
  - Jos jokin tarjous kuulostaa liian hyvältä ollakseen totta, se todennäköisesti on huijaus.
  - Yksikään vastuullinen henkilö, yritys tai viranomainen ei kysy esimerkiksi salasanojasi tai pankkitunnuksiasi puhelimitse tai sähköpostilla.
- Käytä kaksivaiheista tunnistautumista
  - Ottamalla käyttöön kaksivaiheisen tunnistautumisen teet tiliesi varastamisesta huomattavasti vaikeampaa.
  - Salasanan lisäksi puhelimeen lisäkoodi
- Muista varmuuskopiot
  - Varmuuskopioi tärkeimmät tietosi. Käytä esimerkiksi ulkoista kovalevy/muistitikkuja tai pilvitallennusta.
    Mielellään molempia.

Hyvä tietoturva

- Huolehdi virustorjunnasta
  - Windowsissa on oma virustorjunta **Defender** joka on varsin hyvä.
  - Ei välttämättä kuitenkaan ole huono idea tutkia myös kaupallisia vaihtoehtoja – niistä löytyy myös muita ominaisuuksia – kuten automaattinen varmuuskopiointi
- Ohjelmien päivittäminen
  - Pidä käyttämäsi ohjelmat ym. päivitettynä!
- Muista myös
  - Älä jätä tietotekniikkaa esim. autoon näkyville
  - Muista vanhan tietokoneen kovalevyn totaalinen tyhjennys/tuhoaminen
  - Puhelimen suojaus
  - Varovasti julkisilla koneilla
    - välimuistin ja selaustietojen poisto
    - muista myös ottaa muistitikkusi talteen
    - Muista kirjautua ulos palveluista
- Kaikki ei ole sähköistä!
  - Hanki silppuri ja tuhoa paperit joissa esim. henkilötietoja
  - Mieti mitä puhut

Sosiaalinen media

- Älä käytä samaa salasanaa kun esim. sähköpostissa
- Yksityisyysasetukset: ehkä et halua koko maailman näkevän päivityksiäsi
- Mieti mistä tykkäät ja mihin ryhmiin kuulut: mainonta!
- Mieti mitä jaat
  - Valokuvat (muista myös tekijänoikeudet)
  - Sijaintitiedot
  - Mitä kerrot kavereista
  - Ota vastuu tekemisistäsi
- Älä käytä tunnuksiasi muualle kirjautumisen
- Vältä ketjuviestejä

Välimuisti ja selaustiedot

- Selaimet tallentavat sivuhistoriaasi, lomakkeiden täyttötietoja, kirjautumistietojasi, mahdollisesti salasanojasi
- Jos olet muulla kuin omalla tietokoneella muista poistaa tiedot
- Muista myös kirjautua ulos kaikilta tileiltäsi (Esim. Google-tili tai Facebook)

- Chrome: Kolme pistettä -> Asetukset -> Tietosuoja ja Turvallisuus -> Poista selaustiedot

- Edge: Kolme pistettä -> Asetukset -> Tietosuoja, haku ja palvelut -> Tyhjennä selaustiedot

- Vieraalla koneella kannattaa myös käyttää Incognito/InPrivate-ikkunaa selaamiseen.
  - Kun suljet ikkunan, tietokone ei tallenna: hakuja, välilehtiä, sisäänkirjautumistietoja tai evästeitäsi.
  - Se ei kuitenkaan estä internet-palveluntarjoajaasi, viranomaisia tai hakkereita pääsemästä käsiksi haluamiinsa tietoihin.

VPN ja Salasanaohjelmat

- VPN piilottaa kaikki tekemisesi netissä yhdistämällä sinut eri palvelimeen ja määrittämällä sinulle uuden IP-osoitteen
  - Virtual Private Network, virtuaalinen erillisverkko
  - Ulkopuolisille voi vaikuttaa että olet ihan eri maassa
  - Yle Digitreenit: VPN

- Salasanaohjelmat – ohjelma pitää salasanasi muistissa, sinun tarvitsee vain muistaa sen salasana
  - LastPass

- Yle Digitreenit: Salasanaohjelmat

Tietovuodot/Tietomurrot

- **Kun hakkeri on päässyt käsiksi yritysten tai palveluiden tietoihin.**
  - Usein tietoja myydään tai julkaistaan. Joskus tiedot voivat olla hyvinkin arkaluontoisia! Vrt. Vastaamo

- **Identiteettivarkaudet**
  - Identiteettivarkaus tapahtuu, kun joku käyttää henkilötietojasi kuten nimeä ja henkilötunnustasi luvatta. Yleensä tavoitteena on saavuttaa rahallista hyötyä.
    - Rikosuhripäivystys-ohjeet

Suoramarkkinoinnin kieltäminen

- **Suoramarkkinointia voi rajoittaa:**
  - Ilmoittamalla markkinointikiellosta suoraan markkinoijalle tai myyjälle, jolloin kielto koskee kyseistä yritystä
  - Kieltämällä nimi- ja osoitetietojen luovutuksen viranomaisten ylläpitämistä tietojärjestelmistä
  - Ilmoittautumalla suoramarkkinoinnin rajoituspalveluun. Palvelut voivat olla maksullisia.

- Eikä niitä rukseja joka ruutuun!

- Kilpailu- ja kuluttajavirasto
- Suomen Asiakkuusmarkkinointiliitto (ASML)

Henkilötietolaki

- Henkilötietolaissa on säädetty rekisteröidyille seuraavat oikeudet:
  - Tiedonsaantioikeus: rekisterinpitäjä on velvollinen antamaan tietoja henkilötietojesi käsittelystä niitä kerättäessä, koska käsittelyn edellytetään olevan avointa.
  - Tarkastusoikeus: sinulla on oikeus käyttää tarkastusoikeutta kun haluat tietää, mitä tietoja sinusta on tallennettu eri rekistereihin. Näin voit myös varmistaa, että sinusta rekisteröidyt tiedot ovat oikeita.
  - Oikeus saada tietonsa korjatuiksi: sinulla on oikeus vaatia rekisterinpitäjää korjaamaan rekisterissä oleva virheellinen tieto.
  - Kielto-oikeus: sinulla on oikeus kieltää rekisterinpitäjää käyttämästä sinua koskevia tietoja tiettyihin tarkoituksiin, esimerkiksi koneelliseen suoramarkkinointiin.

  - Jos sinulla on kysyttävää henkilötietojesi käsittelystä, ota yhteyttä ensiksi asianomaisen rekisterin ylläpitäjään. Rekisterinpitäjän on laadittava pitämästään henkilörekisteristä rekisteriseloste, josta ilmenee esim. tietojen käyttötarkoitus ja mihin tietoja luovutetaan. Seloste on pidettävä jokaisen saatavilla.
  - Jos ei asia näin selviä, voit ottaa yhteyttä tietosuojavaltuutetun toimistoon. Ja jos on rikottu henkilötietolakia tai rikoslakia, voit pyytää poliisia selvittämään asiaa

GDPR

- Tietosuojadirektiivi, General Data Protection Regulation
  - Henkilötiedot käsittävät kaikki tiedot jotka liittyvät luonnolliseen henkilöön. Henkilötietoja ovat mm. henkilön nimi, sähköpostiosoite, sekä digitaaliset tiedot kuten IP-osoitteet ja mobiililaitteiden tunnukset.
  - Yritysten ja ym. organisaatioiden on pyydettäessä pystyttävä antamaan yksityishenkilölle kaikki ne tiedot, jotka yrityksellä on hänestä. Käyttäjälle on myös tarjottava selkeästi mahdollisuus hyväksyä tai kieltää tietojen kerääminen.
  - Ajatuksena on ettei tietoa kerätä jollei se ole tarpeellista. Rekisterinpitäjän on rekisteriselosteessa kerrottava mihin tietoja käytetään ja miten tietojen turvallisuus on varmistettu.
  - Direktiivin rikkomisesta voidaan määrätä merkittävät sakot, jopa 20 miljoonaa euroa tai 4% liikevaihdosta

Turvallinen nettishoppailu

1. Osta vain luotettavista verkkokaupoista
2. Tarkista toistuvat maksut – muista tarkistaa palveluehdot!
3. Jotkut verkkokaupat pyytävät lupaa maksutietojesi tallentamiseen. Ellei tämä ole välttämätöntä, maksutietoja ei kannata luovuttaa.
4. Käytä luottokorttia, kun teet verkko-ostoksia, PayPal
5. Varmista, että tiedonsiirto on suojattu asianmukaisesti. Suojatun tiedonsiirtoyhteyden tunnistaa osoiterivillä näkyvästä lukkosymbolista. Vältä verkkokauppojen tekemistä sivustoilla, jotka eivät käytä vahvan tunnistamisen todentamispalveluja
6. Tallenna aina kaikki verkko-ostoksiin liittyvät asiakirjat
7. Jos et osta mitään tiettyä tuotetta tai palvelua, älä lähetä korttitietojasi.
8. Kun ostat jotakin verkosta toiselta henkilöltä, älä lähetä myyjälle etukäteen rahaa
9. Älä lähetä rahaa tuntemattomille henkilöille
10. Älä koskaan lähetä korttisi numeroa, PIN-koodia tai muita kortin tietoja kenellekään sähköpostilla

Sähköinen asiointi

- Tunnistautuminen julkisiin ja muihin palveluihin
  - Pankkien verkkopankkitunnukset, suosituin
  - Mobiilivarmenne – operaattoreiden tunnistusmenetelmä, Sim-kortilla, maksullinen
  - Henkilökortin kansalaisvarmenne
    - Tarvitsee kortinlukijan, ohjelman ja henkilökohtaiset tunnusluvut
    - Pitää erikseen aktivoida

- Suomi.fi
  - Kirjaudutaan em. keinoilla
  - Kirjautuminen julkishallinnon palveluin

Testaa itsesi!

- Testaapa huviksesi:

- Ovatko tietosi vuotaneet nettiin? (F-secure)
- Vastaava englanniksi

- Salasanan vahvuus (Yle)
- Ja vielä muutama englanniksi

Sähköinen asiointi

- Tunnistautuminen julkisiin ja muihin palveluihin
  - Pankkien verkkopankkitunnukset, suosituin
  - Mobiilivarmenne – operaattoreiden tunnistusmenetelmä, Sim-kortilla, maksullinen
  - Henkilökortin kansalaisvarmenne
    - Tarvitsee kortinlukijan, ohjelman ja henkilökohtaiset tunnusluvut
    - Pitää erikseen aktivoida

- Suomi.fi
  - Kirjaudutaan em. keinoilla
  - Kirjautuminen julkishallinnon palveluin

Lisäoppia netistä

- Salasanat haltuun
- Helsingin Yliopiston tietoturvaohjeet opiskelijoille
- Poliisin vinkit
- Danske Bankin tietoturvasanastoa
- Poliisin lista sähköpostihuijauksista
- Ylen lista huijauksista
- Kilpailu- ja kuluttajavirasto
- Salasanavinkkejä
- Kuluttajaliitto
- F-Secure