Suomen Yrittäjäopisto

Euroopan unionin osarahoittama

# Yksin- ja pienyrittäjän tieto- ja cyberturva ABC –verkkovalmennus osa II.

**3.10.24**

## Tervetuloa!

**https://www.syo.fi/digialy-kayttoon-hanke/**

Valmennus on osa Suomen Yrittäjäopiston toteuttamaa Digiäly käyttöön –hankkeen toimenpiteitä. Hanke on EU:n osarahoittama.

# Koulutuksen sisältö

- Työskentele turvallisesti toimistolla, tien päällä ja etänä
- Pilvipalveluiden turvallinen käyttö
- Sosiaalisen median turvallinen käyttö
- Varautumiskeinot kyberuhkiin
- Mistä saa tukea kyberturvallisuuden vahvistamiseen?

*Kouluttaja: Arttu Ronkainen, tietoturva-asiantuntija, Opsec Oy*

# Työskentele turvallisesti toimistolla, tien päällä ja etänä

- Turvalliset yhteydet julkiseen verkkoon
- Turvalliset etäyhteydet
- Päätelaitteiden suojaus
- Fyysinen turvallisuus

# Turvalliset yhteydet julkiseen verkkoon

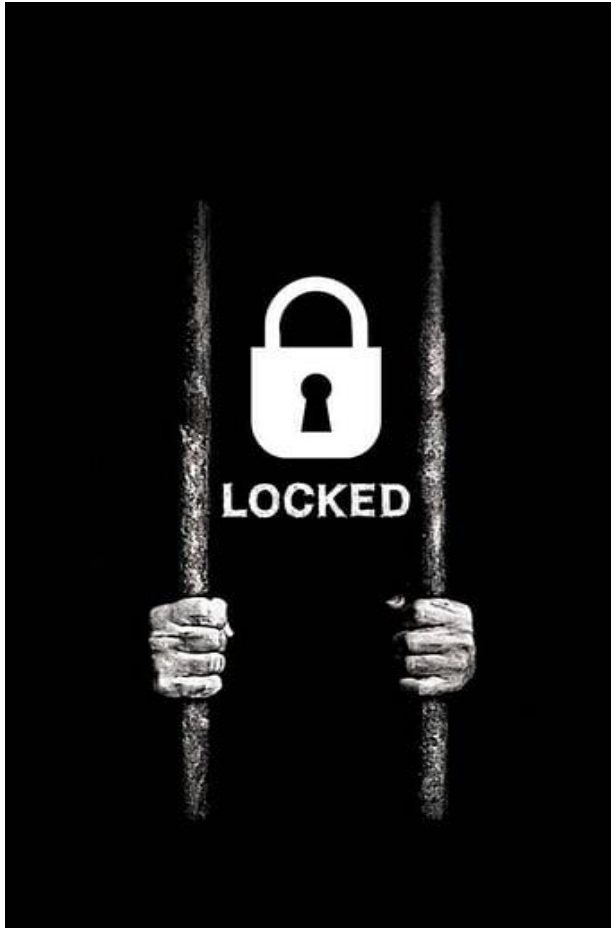
- Älä käytä julkisia suojaamattomia verkkoja
  - Salasanattomissa verkoissa liikenne liikkuu oletuksena salattuna, jolloin samassa verkossa olevat voivat seurata liikennettä.
- Suosi salasanalla suojattuja verkkoja
  - Käytä luotettavien tahojen tarjoamia salasanalla suojattuja verkkoja
- Kotimaassa operaattorien mobiiliverkot ovat hyvä vaihtoehto
  - Yleensä paras vaihtoehto jakaa oman puhelimen verkko työkoneeseen

# Turvalliset etäyhteydet

- Älä käytä salaamattomia tai haavoittuvaisia etäyhteyksiä
  - Valitse luetettavan toimittajan palvelu, jota ylläpidetään säännöllisesti
- Huolehdi järjestelmien päivityksistä
  - Haavoittuvuudet yhteyksissä paikataan päivityksillä, jolloin etäyhteydet pysyvät tietoturvallisina
- VPN-yhteydet ovat hyvä ratkaisu etäyhteyksiin
  - Mikäli käytössä on VPN-ratkaisu esim toimiston verkkoon on se hyvä tapa käyttää resursseja etänä

# Päätelaitteiden suojaus

- Suojaa laitteet asettamalla PIN-koodin kysely, lukituskoodi ja automaattinen lukitus päälle.
- Älä luovuta laitteita muiden käyttöön
  - Laitteille on helppo asentaa haitta- tai vakoiluohjelmia huomaamattomasti
- Salaa päätelaitteesi, jotka sisältävät luottamuksellista tietoa Käytä esim. käyttöjärjestelmän salausta (Bitlocker tai Filevault)
  - Laitteen hukkuessa salauksella varmistetaan, ettei laitteen tietoja saada luettua selväkielisenä tallennustilasta

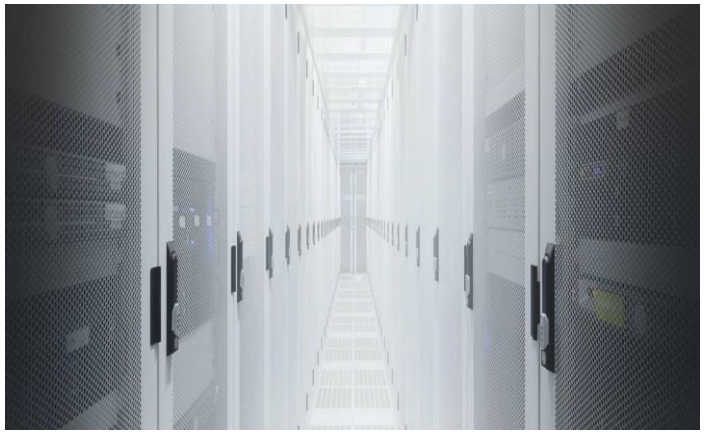


# Fyysinen tietoturvallisuus

- Käytä yksityisyydensuoja näyttökalvoa kun työskentelet julkisilla paikoilla
- Älä puhu luottamuksellisia asioita puhelimessa asiankuulumattomien kuullen esimerkiksi junassa tai linja-autossa
- Ole erityisen huolellinen laitteiden ja papereiden säilytyksestä, kun työskentelet tienpäällä

# Pilvipalveluiden turvallinen käyttö

- Lue aina palvelun käyttöehdot ja niiden muutokset
- Tarkista kuka omistaa palvelussa olevan tiedon ja mikä on tiedon elinkaari
- Pidä huolta tietojen varmuuskopioinnista
- Tarkista palvelun tietoturvallisuus hankintavaiheessa
- Pidä huolta käyttäjätunnusten suojauksesta
- Käytä kaksivaiheista tunnistautumista aina kun se on mahdollista
- Mitä jos palveluntarjoajalle tulee käyttökatko?



# Sosiaalisen median turvallinen käyttö

- Sosiaalinen media tarjoaa erinomaiset kanavat tunnettavuuden kasvattamiseen ja markkinointiin
- Erottele aina yrityksen tilit erilleen
- Muista että esiinnyt aina vähintäänkin yrityksen epävirallisena edustajana, jos mainitset yrityksesi tai työpaikkasi henkilökohtaisessa profiilissasi
- Käyttäjätunnusten turvallisuus
- Suhtaudu aina kriittisesti sosiaalisessa mediassa saamiisi yhteydenottoihin

# Varautumiskeinot kyberuhkiin

- Päätelaitteiden turvallisuus
- Sähköposti ja viestintä
- Salasanat ja identiteetti
- Tiedon varmistaminen

# Päätelaitteiden turvallisuus

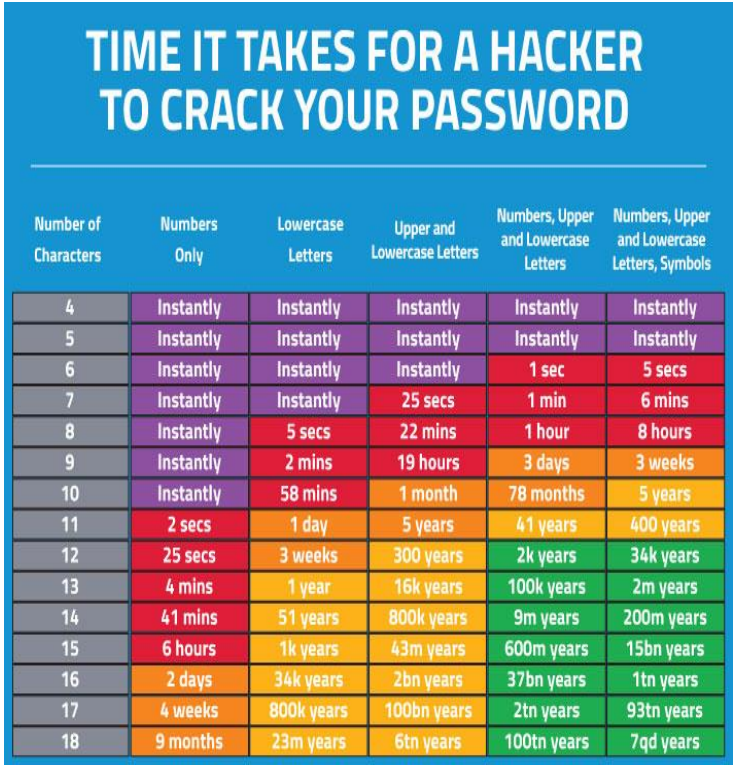
- Huolehdi päätelaitteiden päivityksistä
  - Päivityksillä paikataan laitteessa/ohjelmistoissa havaitut haavoittuvuudet.
- Suojaa laitteesi tietoturvauhilta tietoturvasovelluksella ja palomuurilla
- Huolehdi laitteiden tietoturvasta niiden koko elinkaaren ajan
  - Tarkista päivitysten ja tietoturva-asetusten toiminta säännöllisesti
- Poista laitteet käytöstä asianmukaisesti
  - Laitteen poistuessa käytöstä tyhjennä laite joko fyysisesti tai ohjelmallisesti. Laitteen voi myös kierrättää kumppanilla, joka tuhoaa laitteen tiedot.

# Sähköposti ja viestintä

- Sähköposti on yleisin tietomurtojen ja vuotojen alkupiste
- Ole tarkkana luottamuksellisen tiedon lähettämisessä
  - Varmista että viesti on lähtemässä oikealle vastaanottojalle ja että vastaanottaja on oikeutettu tietoon.
- Käytä tarvittaessa esimerkiksi salattua sähköpostia
- Valitse käyttöösi turvalliset pikaviestimet
  - Tarkista että pikaviestimen liikenne on salattua päästä päähän
- Erottele yrityksen viestintävälineet henkilökohtaisista viestintävälineistä

# Salasanat ja identiteetti

- Käytä vahvoja salasanoja tai salasanalauseita
  - Hyvä salasana on vähintään 10 merkkiä pitkä ja sisältää kirjaimia, numeroita ja erikoismerkkejä.
- Käytä aina eri palveluissa eri salasanoja. Voit käyttää apuna salasanamanageria
- Käytä monivaiheista tunnistautumista aina kun se on mahdollista
- Hallitse käyttöoikeuksia (Vähimpien oikeuksien periaate, Erilliset Admin tunnukset)



TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|---|---|---|---|---|---|
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | 1 sec | 5 secs |
| 7 | Instantly | Instantly | 25 secs | 1 min | 6 mins |
| 8 | Instantly | 5 secs | 22 mins | 1 hour | 8 hours |
| 9 | Instantly | 2 mins | 19 hours | 3 days | 3 weeks |
| 10 | Instantly | 58 mins | 1 month | 78 months | 5 years |
| 11 | 2 secs | 1 day | 5 years | 41 years | 400 years |
| 12 | 25 secs | 3 weeks | 300 years | 2k years | 34k years |
| 13 | 4 mins | 1 year | 16k years | 100k years | 2m years |
| 14 | 41 mins | 51 years | 800k years | 9m years | 200m years |
| 15 | 6 hours | 1k years | 43m years | 600m years | 15bn years |
| 16 | 2 days | 34k years | 2bn years | 37bn years | 1tn years |
| 17 | 4 weeks | 800k years | 100bn years | 2tn years | 93tn years |
| 18 | 9 months | 23m years | 6tn years | 100tn years | 7qd years |

# Tiedon varmistaminen

- Tietojen varmuuskopioinnilla varaudutaan vahinkojen, laiterikkojen tai haittaohjelmien varalle.
- Mitä tietoja varmuuskopioidaan?
  - Varmuuskopioi ainakin kriittiset tiedot
- Kuinka usein varmuuskopiot otetaan?
  - Kuinka tuoreen varmuuskopion tarvitset tietojen hävitessä.
- Missä varmuuskopioita säilytetään?
- Kauanko varmuuskopioita säilytetään?
  - Huolehdi että varmuuskopiot ovat erillään fyysisesti käytössä olevasta tiedosta sekä suojassa esim. kiristyshaittaohjelmalta
- Laita päälle järjestelmien logien tallennustoiminnot.

# Mistä saa tukea kyberturvallisuuden vahvistamiseen?

- ***Kyberturvallisuuskeskuksen uutiskirjeet***, *tai* ***RSS-syötteet***
- Kyberturvallisuuskeskuksen ohjeet ja oppaat organisaatioille ja yrityksille
- Palveluntarjoajat

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

opsec

## OHJEITA ORGANISAATION JOHDOLLE

- Toiminta kiristyshaittaohjelmatilanteessa - johdon ohje
- Kyberturvallisuus ja yrityksen hallituksen vastuu -opas
- Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - ohje johdolle ja asiantuntijoille

## MICROSOFT 365 -PALVELUIHIN LIITTYVIÄ OHJEITA

- Näin suojaat Microsoft 365 -palvelusi
- Toimi näin Microsoft 365 -tilin tietomurron sattuessa
- M365-tietomurroissa hyödynnetään yhä useammin AiTM-tietojenkalastelutekniikkaa

## TOIMINTAOHJEITA KYBERHYÖKKÄYSTILANTEISTA TOIPUMISEEN

- Toimintaohje - tietomurto
- Toimintaohje – kiristyshaittaohjelma
- Toimintaohje – palvelunestohyökkäys
- Toimintaohje – toimitusketjuhyökkäys
- Toimintaohje - vuotaneet käyttäjätunnukset
- Toimintaohje - pilviympäristöjen poikkeamanhallinta

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

**Pienyritysten kyberturvallisuusopas**

Traficomin julkaisuja
228/2020

# Kysymyksiä?

**Arttu Ronkainen**
Tietoturva-asiantuntija
p. 0201 210 359
arttu.ronkainen@opsec.fi

**OPSEC OY**
Tiedekatu 2, 60320 Seinäjoki
p. 020 198 6690, info@opsec.fi
www.opsec.fi