Pienyrityksen tietoturvakoulutus

LAB University of Applied Sciences

Kyberturvalliset ekosysteemit Etelä-Karjalassa hanke

Vipuvoimaa EU:lta 2014–2020

ETELÄ-KARJALAN LIITTO

Euroopan unioni
Euroopan aluekehitysrahasto

LAB University of Applied Sciences

Sisältö

- Tietoturva
- Päätelaitteiden suojaus
- Päivitykset
- Virustorjunta
- Salasanakäytännöt
- Monivaiheinen tunnistautuminen
- Tietojenkalastelu
- Haittaohjelmat
- Tietoturvan muistilista henkilöstölle

LAB University of Applied Sciences

Tietoturva

- Tietoturvan osat ovat sekä teknisiä että hallinnollisia
  - Saatavuus – tieto on saatavilla, kun sitä tarvitaan
  - Luottamuksellisuus – ulkopuoliset eivät pääse tietoon käsiksi
  - Eheys – tietoa ei ole muokattu (ulkopuolisten toimesta)

- Tietoturvakäytännöillä pyritään varmistamaan että tarvittavat tiedot ovat saatavilla oikeille henkilöille oikeaan aikaan, mutta muut eivät niitä pääse näkemään tai muokkaamaan

- Tämä koskee niin fyysistä- kuin virtuaalistamaailmaa
  - Olan yli katselu vs. tietomurto
  - Tai laitteiden/papereiden varastaminen

- **Tietoturva ei ole vain teknistä, vaan mitä suurimmissa osin ihmisten toimintatapoja.**

LAB University of Applied Sciences

Tietoturva

- Tarkoittaa toiminnan kannalta välttämättömien laitteiden, ohjelmien ja tiedostojen käsittelyyn liittyviä turvallisia toimintatapoja.
- Siitä huolehtiminen ehkäisee tietomurtoja, suojaa yrityksen toiminnan kannalta arkaluontoista materiaalia ja varmistaa ettei käyttäjän tietoja pääse ulkopuolisen haltuun.
- Mahdolliset poikkeamat (incidents) tulisi tunnistaa, toimia ennaltaehkäisevästi ja välttää vahingot.
- Mikäli jotain epäilyttävää tapahtuu, tulisi siitä raportoida pikemmiten yrityksen johdolle, jotta voidaan minimoida kaikki mahdolliset haitat ja uhkat.
- Lainsäädäntö muuttumassa; GDPR voimassa nyt ja sakkoja isoille yrityksille (tulevaisuudessa saattaa joutua maksamaan isojakin sakkoja)

LAB University of Applied Sciences

Päätelaitteiden suojaus

- Päätelaite, eli tietoliikenneverkkoon kytkettävä laite
  - Näitä ovat mm. puhelin, tabletti ja kannettava tietokone
- Tulisi suojata ulkopuolisilta käyttäjiltä
  - Tämä onnistuu esimerkiksi henkilökohtaisella käyttäjätunnuksella, koodilla tai sormenjälkitunnistuksella
- Mitä voi käydä?
  - Ulkopuolinen taho pääsee tarkastelemaan päätelaitetta ja sen sisältämiä tietoja

LAB University of Applied Sciences

Päätelaitteiden suojaus

- Erityisen tärkeää olisi suojata päätelaitteet, jotka mukana yrityksen ulkopuolella liikuttaessa
  - Näille laitteille mielellään tupla tai jopa triplasuojaus
    - Eli PIN koodin lisäksi vielä sormenjälki- tai kasvojentunnistus

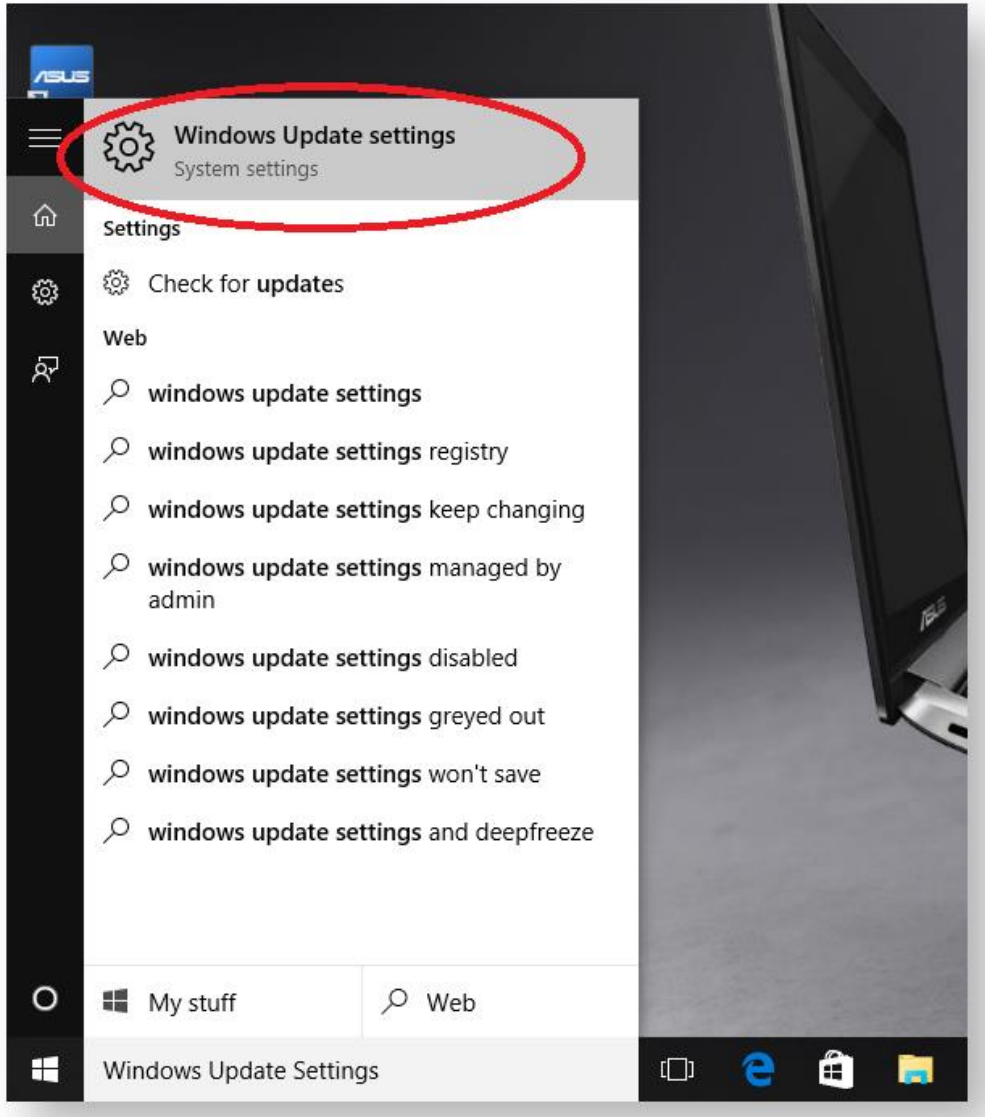
- Laitteilla oleva arkaluontoinen sisältö salattava erikseen
  - Esimerkiksi asiakastiedot erillisen suojauksen takana
  - Yrityksen toiminnan kannalta tärkeät sovellukset erillisen suojauksen takana
  - Tietosuojakalvo vähentää riskiä, että ulkopuolinen näkee näytön sisällön
  - Kovalevyjen salaus estää varastetun laitteen sisällön lukemisen

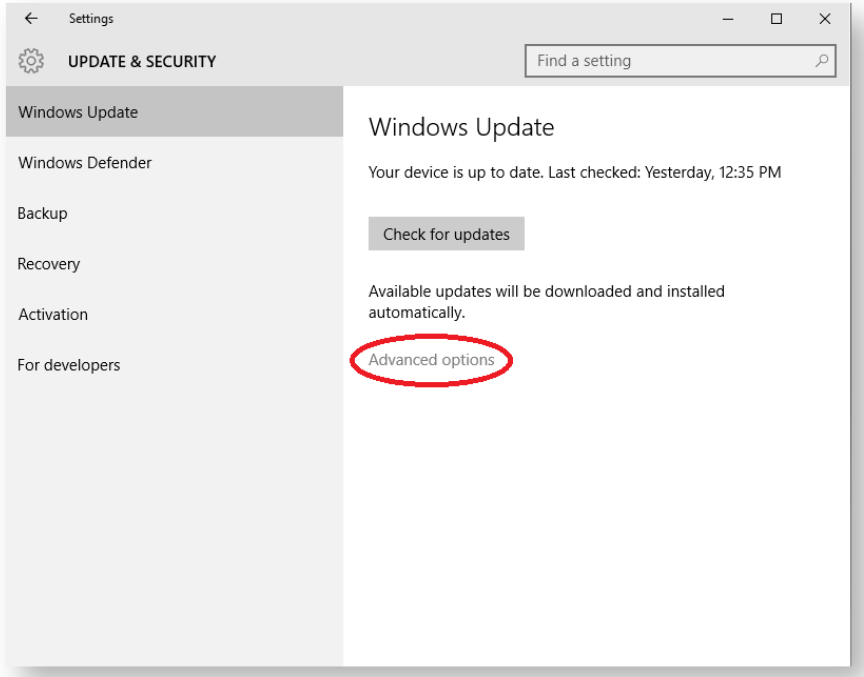
- Mitä voi käydä?
  - Asiakas voi saada laitteen haltuunsa ja päästä käsiksi suojaamattomiin tietoihin

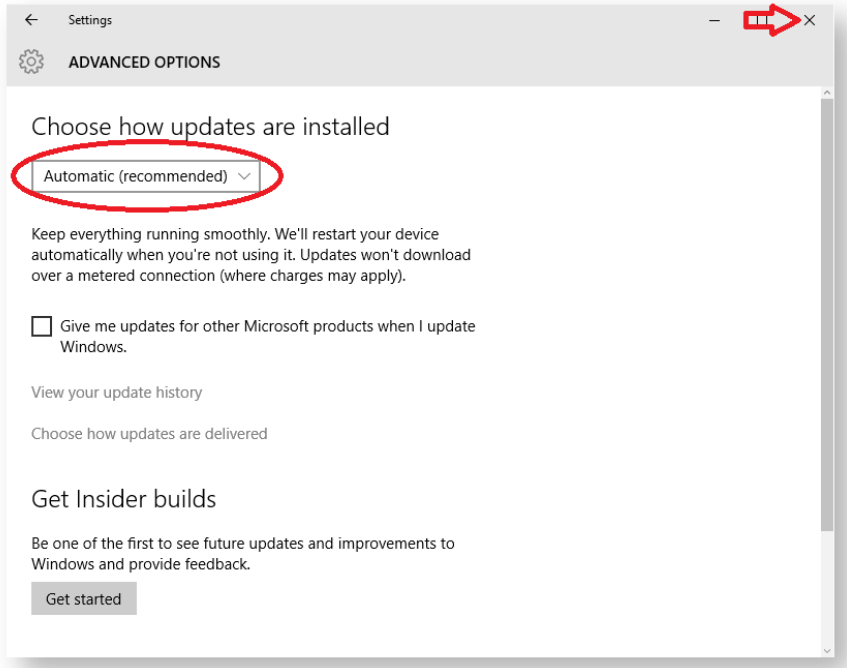
LAB University of Applied Sciences

Päivitykset

- Päätelaitteiden käyttöjärjestelmät, ohjelmat, ohjelmistot, applikaatiot jne. päivitettävä uusimpaan versioon
  - Päivitykset automaattisiksi
  - Suojaa poistamalla tai tukkimalla tietoturva-aukkoja
- Tarkista että päivityksiä on saatavilla!
  - Valmistaja tarjoaa päivityksiä vain tietyn aikaa
  - Erityisesti mobiililaitteiden päivitykset loppuvat nopeasti (muutamassa vuodessa).
- Mitä voi käydä?
  - Päivittämätön versio voi sisältää tietoturva-aukkoja, joiden kautta ulkopuolinen henkilö pääsee päätelaitteeseen ja sitä kautta tietoihin käsiksi


Windows Update settings
System settings
Settings
Check for updates
Web
windows update settings
windows update settings registry
windows update settings keep changing
windows update settings managed by admin
windows update settings disabled
windows update settings greyed out
windows update settings won't save
windows update settings and deepfreeze
My stuff
Web
Windows Update Settings


Settings
UPDATE & SECURITY
Find a setting
Windows Update
Windows Defender
Backup
Recovery
Activation
For developers
Windows Update
Your device is up to date. Last checked: Yesterday, 12:35 PM
Check for updates
Available updates will be downloaded and installed automatically.
Advanced options


Settings
ADVANCED OPTIONS
Choose how updates are installed
Automatic (recommended)
Keep everything running smoothly. We'll restart your device automatically when you're not using it. Updates won't download over a metered connection (where charges may apply).
Give me updates for other Microsoft products when I update Windows.
View your update history
Choose how updates are delivered
Get Insider builds
Be one of the first to see future updates and improvements to Windows and provide feedback.
Get started

LAB University of Applied Sciences

Virustorjunta

- Virustorjuntaohjelma estää haittaohjelmien pääsyn päätelaitteelle
  - Tarkistaa asennettavat sovellukset sekä skannaa laitteen säännöllisesti
    - Ilmoittaa käyttäjälle mahdollisesta vaarasta

- Mitä voi käydä?
  - Ilman virustorjuntaohjelmaa käyttäjä saattaa huomaamattaan asentaa laitteelle haitallisia sovelluksia tai ohjelmia
    - Haittaohjelma voi aiheuttaa erilaista haittaa päätelaitteelle riippuen sen tarkoitusperästä

LAB University of Applied Sciences

Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 9/14/2023 4:35 PM (quick scan)
0 threats found.
Scan lasted 3 minutes 0 seconds
63934 files scanned.

Quick scan

Scan options

Allowed threats

Protection history

LAB University of Applied Sciences

Salasanakäytännöt

- Käyttämällä vahvaa salasanaa voidaan ehkäistä ja estää tietomurtoja
  - Vahva salasana on yli 12 merkkiä pitkä, sisältää sekä pieniä että isoja kirjaimia, numeroita ja erikoismerkkejä
  - Salasanan ei tulisi sisältää sanoja tai olla lause, jotta sitä ei pysty arvaamaan
  - Salasanoja ei tulisi kirjoittaa ylös tai tallentaa päätelaitteelle
  - Samaa salasanaa ei tulisi käyttää muualla

- Mitä voi käydä?
  - Heikon salasanan pystyy arvaamaan tai murtamaan, jolloin ulkopuolinen voi päästä käsiksi päätelaitteeseen ja/tai käyttäjätiliin sekä niiden tietoihin
  - Mikäli samaa salasanaa on käytetty useassa paikassa, voi hyökkääjä päästä salasanan selvitettyään näihin kaikkiin järjestelmiin.

LAB University of Applied Sciences

Ilmaiset työkalut › F-Secure Strong Password Generator

Vahva salasanageneraattori

Luo itsellesi vahva salasana F-Securen ilmaisella salasana-generaattorilla

4Yk$sOs,j]=6 Kopioi **Luo uusi**

Salasana on VAHVA! Vahvista sitä tekemällä siitä vielä pidempi ja moni-mutkaisempi.

abc ☑ ABC ☑ 123 ☑ #$& ☑

Salasanan pituus: 12

4r5lu;X)Uoa2 Kopioi **Luo uusi**

Salasana on VAHVA! Vahvista sitä tekemällä siitä vielä pidempi ja moni-mutkaisempi.

_@Q,lAoOK7K@ Kopioi **Luo uusi**

Salasana on VAHVA! Vahvista sitä tekemällä siitä vielä pidempi ja moni-mutkaisempi.

F-Secure, 2023

LAB University of Applied Sciences

Monivaiheinen tunnistautuminen

- Monivaiheinen tunnistautumisella (Multi Factor Authentication MFA) tarkoitetaan käyttäjätunnuksen ja salasanan lisäksi tapahtuvaa erillisellä sovelluksella tai koodilla tunnistautumista
  - Esimerkiksi kirjautuessa pilvipohjaiseen palveluun uudesta laitteesta tai osoitteesta edellytetään käyttäjätunnuksen ja salasanan lisäksi erillistä sähköpostiin lähettyä PIN koodia
  - Monivaiheinen tunnistaminen ehkäisee ja suojaa käyttäjätunnuksia vaikeuttamalla niiden kaappaamisyrityksiä
- Mitä voi käydä?
  - Käyttäjätunnuksen ja salasanan selvittäminen avaa pääsyn järjestelmään
  - Ilman monivaiheista tunnistamista käyttäjätili saatetaan kaapata hyödyntämällä ”Unohditko salasanan?” –toimintoa
    - Päästään käsiksi käyttäjätietoihin ja mahdollisesti yrityksen tietoihin

LAB University of Applied Sciences

Kyberturvallisuuskeskus, 2023

LAB University of Applied Sciences

Tietojenkalastelu

- Tietojenkalastelulla, eli phishingillä, tarkoitetaan tietojen varastamista naamioitujen viestien ja linkkien avulla.
  - Viestit lähetetään yleensä aidon kuuloisesta osoitteesta tai jopa tekstiviestien tapauksessa lähettäjänä näkyy esimerkiksi pankki, lähettipalvelu tai palveluntarjoaja
  - Linkistä avautuva sivu muistuttaa oikeaa sivua
  - Usein nämä kuitenkin tunnistaa linkkien osoitteesta
  - Myös puhelimitse voidaan yrittää kalastella tietoja

- Mitä voi käydä?

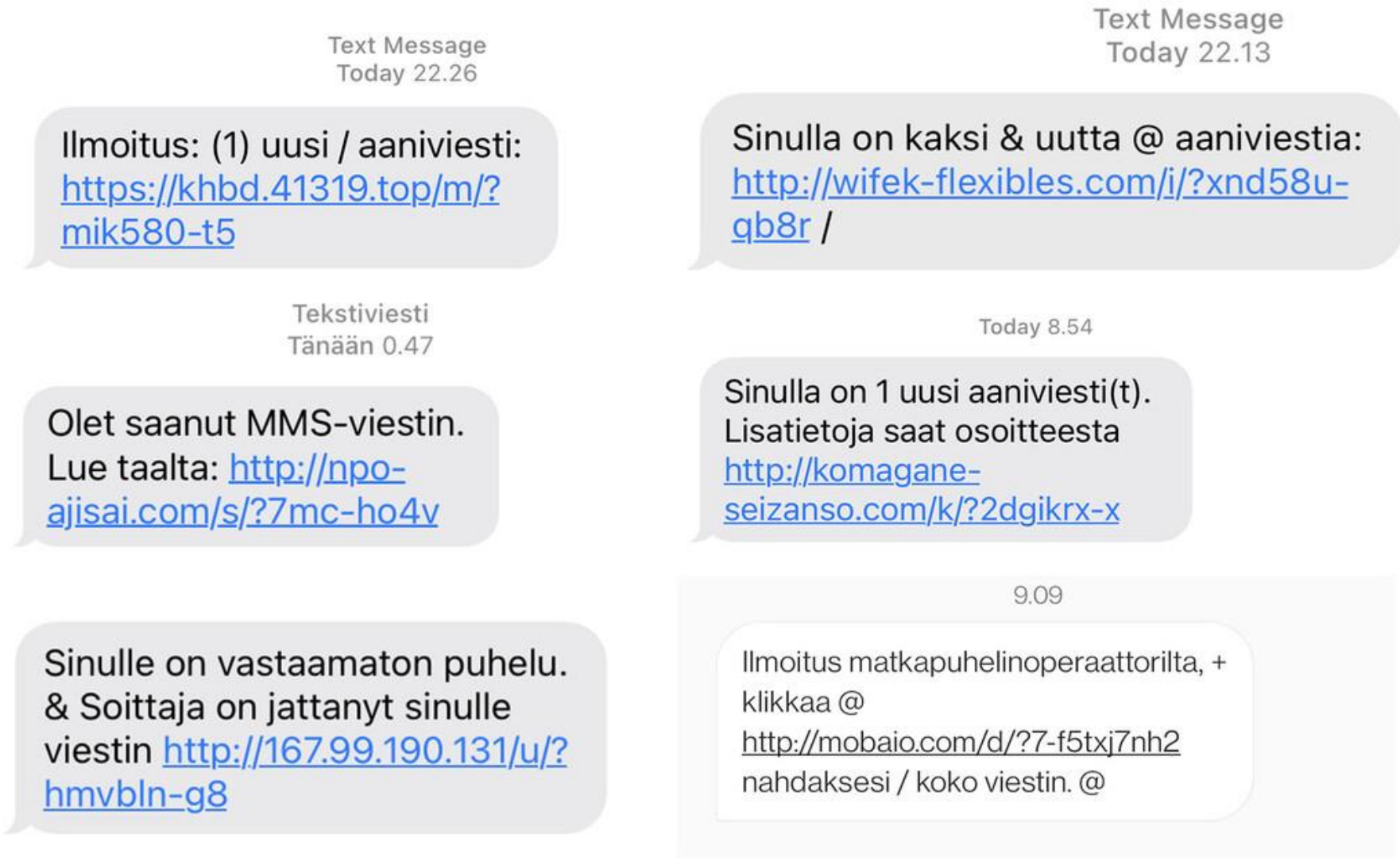
  -> Käyttäjä erehtyy avaamaan linkin

  -> ohjaa huijaussivustolle

  -> pyytää käyttäjää kirjautumaan palveluun

  -> varastaa käyttäjän tiedot

FluBot –nimisen haittaohjelman lähettämiä tekstiviestihuijauksia



Kyberturvallisuuskeskus, 2022

Luottamuksellinen / Konfidentiellt / Confidential

Aihe / Ämne / Subject

Perintä

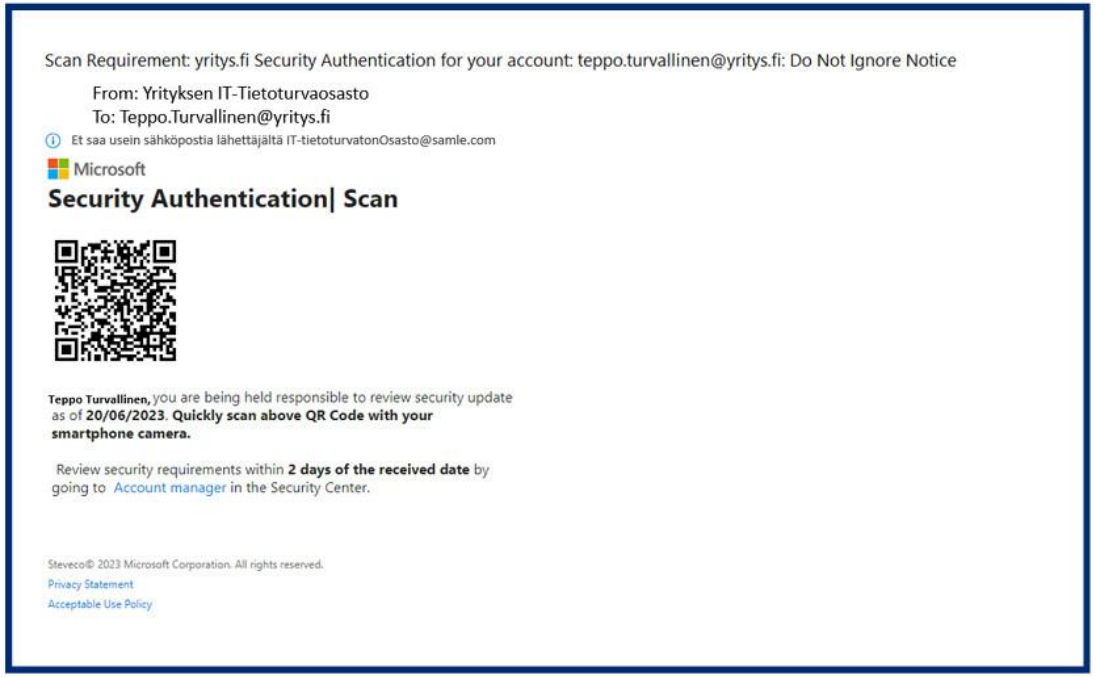
Avaa viesti tästä / Öppna meddelandet / Open message

Olet saanut luottamuksellisen viestin. Viesti avataan ja siihen voidaan vastata yläpuolella olevasta linkistä. Yhteys on suojattu TLS-salauksella. Turvallisuussyistä viestin lukemista on rajoitettu ja se voidaan lukea korkeintaan 14 päivän ajan.

Du har fått ett konfidentiellt meddelande. Meddelandet kan öppnas och svaras på från länken ovanför. Förbindelsen är skyddad med TLS-kryptering. Av säkerhetsskäl är läsningen begränsad och meddelandet kan läsas i högst 14 dagar.

You have received a confidential message. The message can be opened and replied to from the link above. The connection is protected with TLS encryption. Due to security reasons reading of the message is limited and can be read for 14 days at most.

Esimerkkejä sähköpostikalastuviesteistä



Scan Requirement: yritys.fi Security Authentication for your account: teppo.turvallinen@yritys.fi: Do Not Ignore Notice

From: Yrityksen IT-Tietoturvaosasto
To: Teppo.Turvallinen@yritys.fi

Et saa usein sähköpostia lähettäjältä IT-tietoturvatonOsasto@samle.com

Microsoft

Security Authentication| Scan

Teppo Turvallinen, you are being held responsible to review security update as of **20/06/2023**. **Quickly scan above QR Code with your smartphone camera.**

Review security requirements within **2 days of the received date** by going to Account manager in the Security Center.

LAB University of Applied Sciences

Haittaohjelmat

- Haittaohjelmalla tarkoitetaan ohjelmaa, jonka tarkoitus on joko aiheuttaa vahinkoa tai varastaa tietoa
  - Vakoiluohjelmat, jotka vakoilevat päätelaitteen tai käyttäjän toimintaa
  - Kiristysohjelmat, jotka lukitsevat päätelaitteen ja vaativat maksamaan lukituksen purkamisesta
  - Troijalaiset, jotka ujuttavat itsensä laitteelle toisen tiedoston tai latauksen yhteydessä

- Mitä voi käydä?
  - Haittaohjelma voi hidastaa tai jopa estää päätelaitteen toiminnan
  - Haittaohjelma voi varastaa ja jakaa käsiinsä saamaa tietoa
  - Haittaohjelma voi myös ajaa hyökkääjän koodia esim. osana palvelunestohyökkäystä

LAB University of Applied Sciences

Haittaohjelmat

- Haittaohjelmien välttämiseksi
  - Älä asenna mitään ylimääräistä (työlaitteella ainoastaan töissä tarvittavat ohjelmat)
    - Erilliset päätelaitteet töihin ja henkilökohtaiseen käyttöön
  - Asenna ohjelmia ainoastaan virallisista lähteistä
    - Sovelluskaupat
    - Sovelluksen tekijän sivut
    - Ei siis hakukoneiden linkeistä!
    - Eikä varsinkaan saapuneiden viestien linkeistä!

Wana Decryptor, 2017

LAB University of Applied Sciences

Tietoturvan Muistilista

- Päätelaitteiden suojaaminen
- Salasanakäytännön noudattaminen
- Monivaiheinen tunnistautuminen
- Virustorjunnan käyttäminen
- Päivityksistä huolehtiminen
- Haittaohjelmien tunnistaminen
- Tietojenkalasteluyrityksien torjuminen
- Yrityksen tietoturvasta huolehtiminen

- Ole varovainen etenkin henkilötietoja käsitellessä
- Tarkasta viestin lähettäjä ennen viestin avaamista
- Älä tee hätäisiä päätöksiä
- Suojaa ja suojele päätelaitteita aktiivisesti
- Kysy esimieheltä mikäli epäröit

LAB University of Applied Sciences

Lähteet

- https://www.kyberturvallisuuskeskus.fi/fi
- https://www.microsoft.com/fi-fi
- https://www.f-secure.com/en
- https://www.kaspersky.fi/
- https://answers.syr.edu/display/ITHELP

- Tietoturvaopas pienyritykselle

KIITOS!

LAB University of Applied Sciences

Vipuvoimaa EU:lta 2014–2020

ETELÄ-KARJALAN LIITTO

Euroopan unioni
Euroopan aluekehitysrahasto