

12.45 Digiturvavartti – tarkoitettu meille kaikille 19.4.2023

Kimmo Rousku ja Juha Kirves
Digi- ja väestötietovirasto



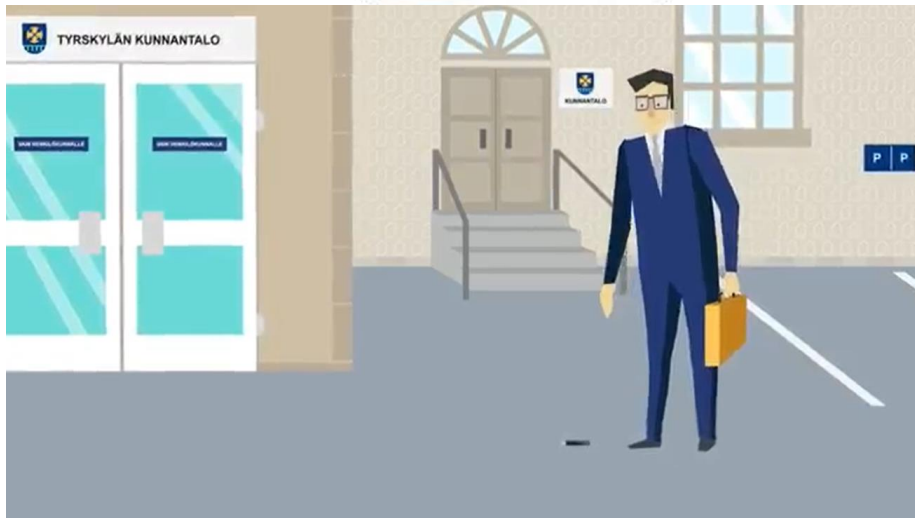
**DIGI- JA
VÄESTÖTIETO-
VIRASTO**





Digiturvavartti

- Ajankohtaiset uhat digimaailmassa
 - Muutama case-esimerkki ja pari vinkkiä
- Ota käyttöön kaksivaiheinen tunnistautuminen!
- Uuden Digiturma vai digiturva koulutusvideon julkaisu – tänään aiheena **"Tartuttaako tikku"**



Ajankohtaisia uhkia ja kuinka suojautua niiltä



DIGI- JA VÄESTÖTIETOVIRASTO

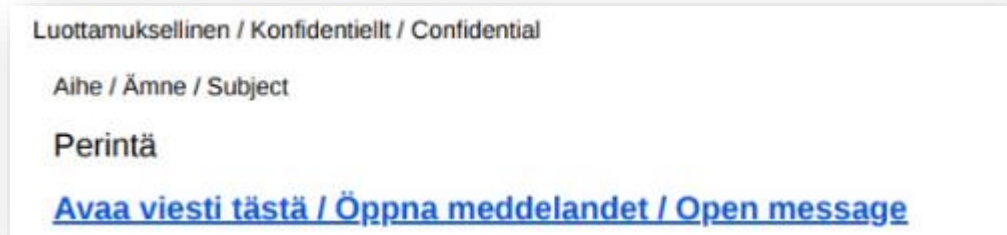
Sähköpostissa on kaksi vaaraa eessä:

1) Viestissä mukana oleva **liitetiedosto**

- Microsoft Office-asiakirjat
- PDF-asiakirjat



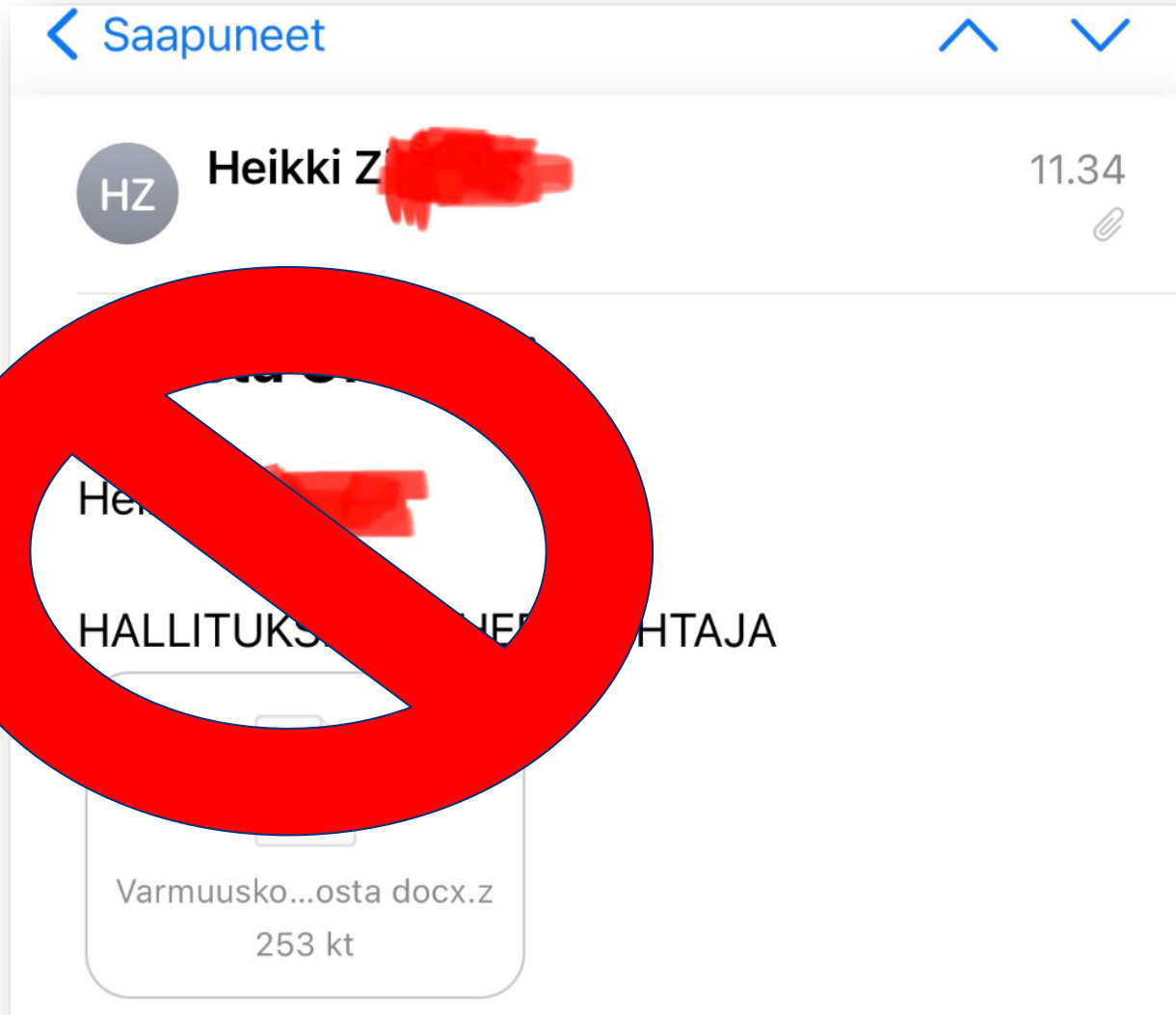
Tällä hetkellä verkkorikolliset pyrkivät naamioimaan nämä luotettavalta taholta tuleviksi.



2) **Nettilinkki** siirtyä verkkorikollisen hallinnassa olevalle sivustolle tai pyyntö kirjautua heidän hallinnassa olevaan palveluun.



Case-esimerkki – ikävä liitetiedosto



Security vendors' analysis	Do you want to automate checks?
AhnLab-V3	⚠ Trojan.Win.NSISInject.R5...
ALYac	⚠ Gen:Variant.Babar.170764
Arcabit	⚠ Trojan.Garf.Gen.6 [many]
Avira (no cloud)	⚠ HEUR/AGEN.1337962
BitDefender	⚠ Trojan.Garf.Gen.6
BitDefenderTheta	⚠ Gen:NN.ZexaF.36132.dm...
Cynet	⚠ Malicious (score: 99)
DeepInstinct	⚠ MALICIOUS
Emsisoft	⚠ Trojan.Garf.Gen.6 (B)
eScan	⚠ Trojan.Garf.Gen.6
F-Secure	⚠ Heuristic.HEUR/AGEN.13...
Fortinet	⚠ W32/ShellcodeRunner.CA!tr
GData	⚠ Gen:Variant.Babar.170764
Google	⚠ Detected
Ikarus	⚠ Trojan-Spy.FormBook
Kaspersky	⚠ UDS:Trojan.Win32.Strab....
MAX	⚠ Malware (ai Score=83)
McAfee-GW-Edition	⚠ BehavesLike.Generic.dc
Microsoft	⚠ Trojan:Win32/Woreflint.A!cl
Rising	⚠ Trojan.Generic@AI.88 (RD...
Sangfor Engine Zero	⚠ Suspicious.Win32.Save.ins
SentinelOne (Static ML)	⚠ Static AI - Suspicious Arc...
Sophos	⚠ Generic ML PUA (PUA)
Trellix (FireEye)	⚠ Trojan.Garf.Gen.6
VIPRE	⚠ Trojan.Garf.Gen.6
ZoneAlarm by Check Point	⚠ UDS:Trojan.Win32.Strab....



Varo tätä sähköpostia: "Älä edes avaa saati tulosta"

Sähköpostin liitetiedostona leviävää haittaohjelmaa ei kannata päästää tietokoneelle.

➔ JAA



Haittaohjelma on suunnattu Windows-tietokoneita vastaan. KUVA: COLOURBOX

Henrik Kärkkäinen

12.4. 8:28

– Älä edes avaa saati  tulosta "Varmuuskopio tuomioistuimen kopiosta docx.z" -viestiä, koska se on täynnä pahuutta eli sisältää haittaohjelman, Rousku kirjoittaa.

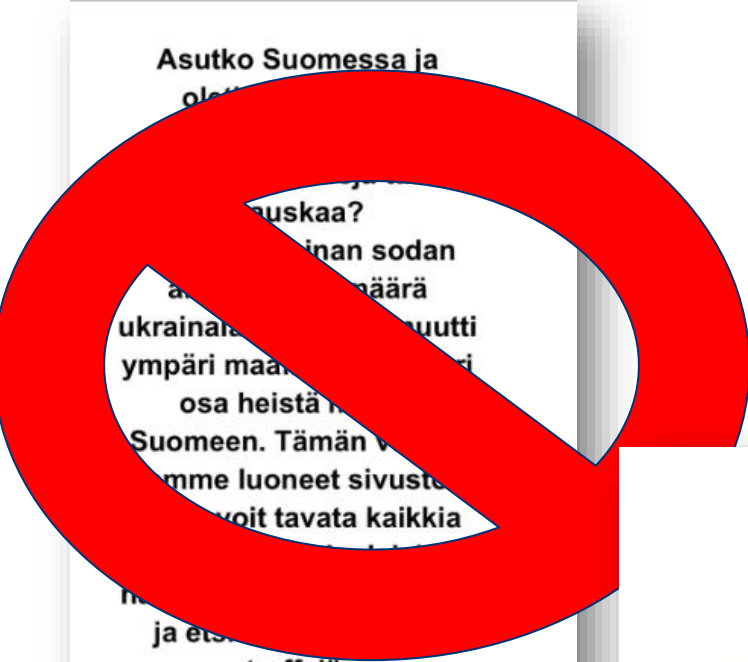
Virustotalin mukaan kyse on muun muassa Trojan.Garf.Gen.6- eli Garfield-nimellä tunnetusta haittaohjelmasta. Se osaa muun muassa varastaa pankkitietoja, sähköpostien kirjautumistietoja, selaimeen tallennettuja salasanoja sekä selaustietoja. Asennuttuaan se osaa vältellä virustutkia.

Lue lisää: Nämä ovat vaarallisimmat tiedostot – hakkeri kertoo, miten kannattaa suojautua

Kehotus tulostaa tiedosto perustuu siihen, että Microsoft-muotoiset asiakirjat aukeavat suojatussa tilassa, jolloin niihin upotetut haittaohjelmat eivät aktivoitu. Niiden tulostaminen aktivoi tiedostojen muokkaustilan, jolloin mukana oleva haittaohjelma käynnistyy.



Case-esimerkki – vaarallinen ”deittipalvelu”



Yli 200 000 muutti Suomeen, minkä vuoksi olemme luoneet sivun, jossa voit tavata sinkkuja ukrainalaisia naisia ja esitellä heille ympäri Suomea! Sivustollamme on yli 70 000 naimatonta ukrainalaista naista, jotka ovat kiinnostuneita juttelemaan ja seurustelemaan tänään tanskalaisten kanssa! Rekisteröidy tänään ja löydä itsesi maailman kaunein nainen! Ukrainan naiset!

Security vendors' analysis

Do you want to automate checks?

AutoShun

⚠ Malicious

CMC Threat Intelligence

⚠ Malicious

Seclookup

⚠ Malicious



Verkkorikollisten tietojenkalasteluyrityksiä – turvapostiksi naamioidut viestit

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.

**Tunnetun
yrityksen
logo**

Oikeista turvaposteista ei saa aueta kirjautumisikkunaa esimerkiksi Microsoft sähköposti tai muuhun palveluun!

Soita viestin lähettäjälle ja varmista aitous!



Päivitä älylaitteesi!

< Yleiset

Ohjelmistopäivitys

Päivitä automaattisesti

Päällä >



iOS 16.4.1

Apple Inc.

Ladattu

Tämä päivitys sisältää tärkeitä virheenkorjauksia ja suojauspäivityksiä iPhoneille, mm. seuraavat:

- Työntävä käsi -emojeiden ihonvärin vaihtoehdot eivät näkyneet.
- Siri ei vastannut joissakin tilanteissa.

Jotkin ominaisuudet eivät välttämättä ole saatavilla kaikilla alueilla tai kaikissa Apple-laitteissa. Tietoja Applen ohjelmistopäivitysten suojaussisällöstä löytyy osoitteesta

<https://support.apple.com/kb/HT201222>

HAAVOITTUVUUS 5/2023 CVSS 8.8 CVE-2023-28205, CVE-2023-28206 ¹

Kriittisiä haavoittuvuuksia Applen tuotteissa - päivitä heti

Päivitetty 13.04.2023 16:35 – Julkaistu 11.04.2023

Uusia ja kriittisiä päivityksiä Applen iOS, macOS Ventura, macOS Monterey, macOS Big sur ja iPadOS-laitteissa, sekä Safari verkkoselaimessa. Päivitykset tulee asentaa välittömästi, sillä hyväksikäyttöä on havaittu maailmalla.

Apple on korjannut menneellä viikolla aikaistetun päivitysaikataulun mukaisesti kaksi 0-päivähaavoittuvuutta (eng. zero day).

CVE-2023-28205 haitalliseksi muotoiltu verkkosisältö on mahdollistanut mielivaltaisen ohjelmistokoodin suorittamisen laitteella ilman käyttäjän hyväksyntää.

CVE-2023-28206 on mahdollistanut mielivaltaisen ohjelmistokoodin suorittamisen käyttöjärjestelmän ytimen (eng. kernel) oikeuksilla.



Ethän lainaa (pankki-/palvelu-) tiliäsi muille?

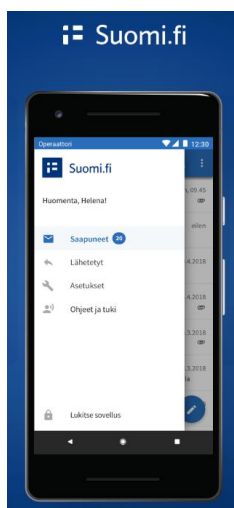
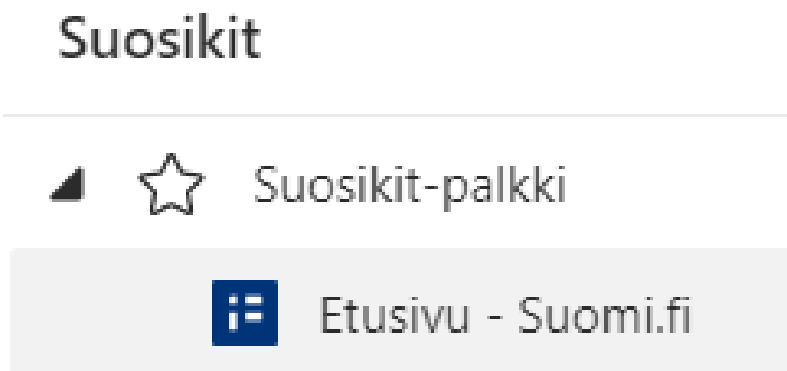


- Etenkin nuoria saatetaan houkutella **lainaamaan esimerkiksi pankkitiliä**, jota verkkorikolliset käyttävät sitten esimerkiksi rahojen kierrättämiseen.
 - Sama koskee myös erilaisten palveluiden tilejä, näihin ei tule antaa pääsyä muille ja ovat aina myös palvelun ehtojen vastaista – pankkitilien osalta jopa rangaistavaa
- Tämä, kuten muut edellä olevat ovat niitä asioita, joista kannattaisi **perheen ja sukulaisten kanssa** muistaa nostaa keskusteluissa esille!
- Ja jos **edes** epäily rikoksesta tai väärinkäytöksestä, yhteys **a)** pankki ja **b)** poliisille rikosilmoitus

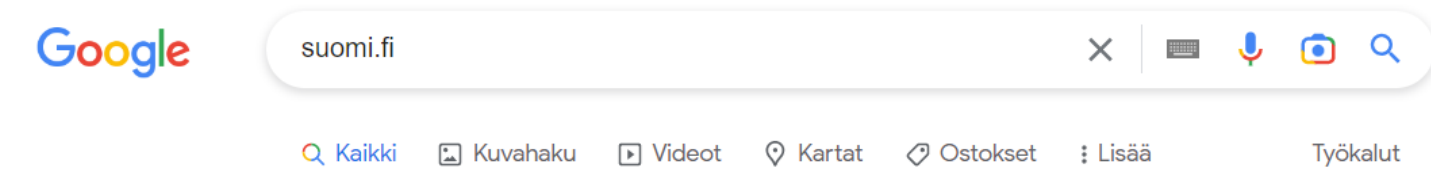


Kolme vinkkiä palveluihin kirjautumiseksi

1) Tallenna tärkeät sivusto suosikeiksi ja käynnistä aina sieltä:



3) Käytä älylaitteen appsia, jos sellainen on tarjolla!



2) Älä googlaa osoitteita!



Kuusi muuta vinkkiä:



- Käytä kaksivaiheista tunnistautumista aina kun se on saatavilla!
- **Älä kirjaudu SMS-tekstiviesteissä** saapuvien linkkien kautta mihinkään palveluun verkkopankkitunnuksillasi.
- ”Hei äiti” -WhatsApp viestit, joissa lapseksi tai joku kaveriksesi tekeytynyt rikollinen taho kertoo uuden numeron tai pyytää lähettämään puhelimeesi tulleen SMS-viestin tai muita tietoja sekä kenties pyytää **myöhemmin rahaa tai vahvistamaan laskun**.
- Sijoita varasi ainoastaan **luotettavien tahojen kautta**, älä esimerkiksi mainoksien kautta. Älä googlaa ”kryptovaluutta rikas”
- **Nettiromanssi** on mahdollisuus, mutta se voi viedä sydämen ohella rahat! Sekä romauttaa luottamuksen muihin ihmisiin 😞
- Älä salli **kenenkään asentaa etäkäyttöohjelmaa** tai älä asenna itse, ellet tiedä varmasti, mitä olet tekemässä!



Testaa digiturvan perusosaaminen Digiturvallinen elämä -testin avulla

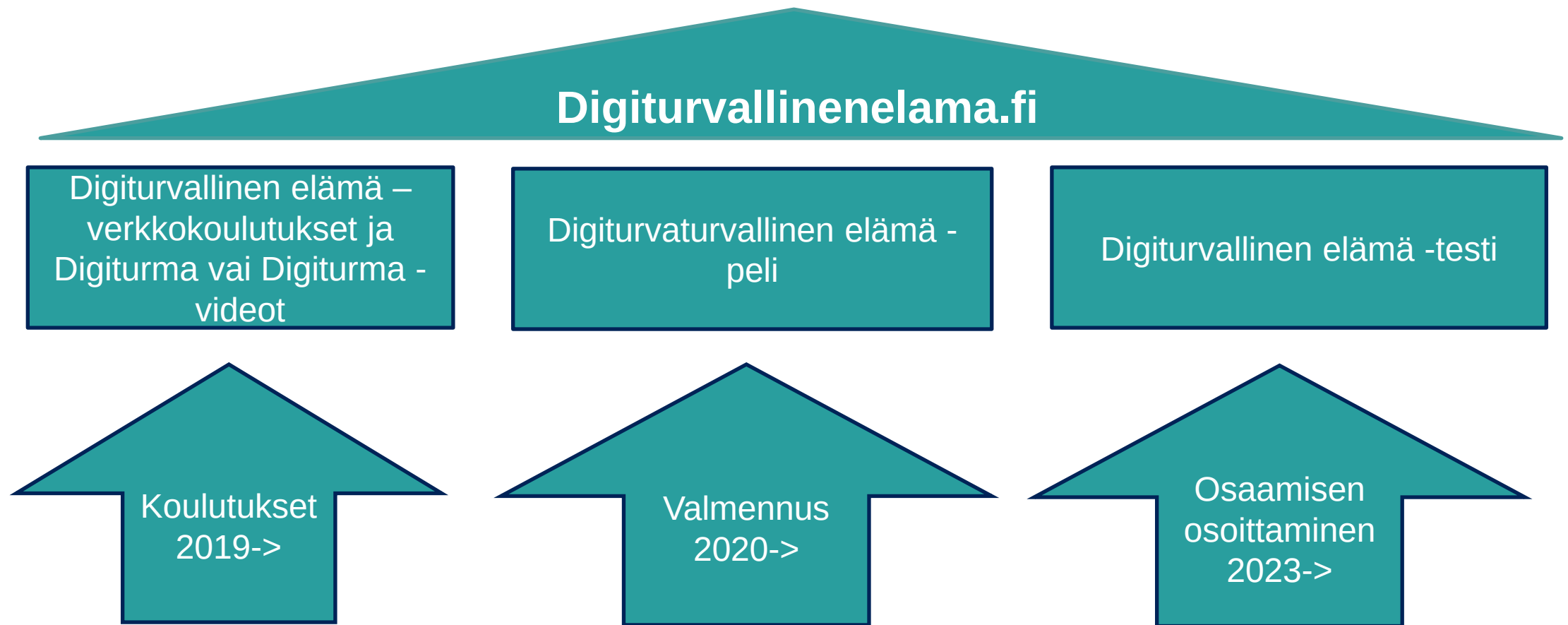
Juha Kirves



**DIGI- JA
VÄESTÖTIETO-
VIRASTO**



Digiturvallinen elämä -koulutuskokonaisuus -



Digiturvallinen elämä -sivusto

<https://digiturvallinenelama.fi> – uusi verkkotunnus!

Kaikki Digiturvallinen elämä-sisältö yhdessä paikassa!

Tilaa Digiturvallinen elämä –tarroja organisaatiosi käyttöön

Lataa Digiturvallinen elämä –julisteita organisaatiosi käyttöön! (Salasanat ja huijausviestit)

Sivusto toimii myös englanniksi ja ruotsiksi



Henkilöstölle suunnatut koulutukset (1/2)

Digiturvallinen työelämä
(RUO saatavilla, ENG
saatavilla)

- <https://www.eoppiva.fi/koulutukset/digiturvallinen-tyoelama/>

Toimi turvallisesti
digimaailmassa (RUO
saatavilla, ENG
saatavilla)

- <https://www.eoppiva.fi/koulutukset/toimi-turvallisesti-digimaailmassa/>

Tietosuoja ABC +
Tietosuoja ABC 2020
(RUO saatavilla, ENG
saatavilla)

- <https://www.eoppiva.fi/koulutukset/tietosuoja-abc-julkishallinnon-henkilostolle/>



Henkilöstölle suunnatut koulutukset (2/2)

Digiturvallisuus kuntien
luottamushenkilöille (RUO
saatavilla, ENG saatavilla)

- <https://www.eoppiva.fi/koulutukset/digiturvallisuus-kuntien-luottamushenkiloille>

Digiturvallisuus hyvinvointialueiden
luottamushenkilöille (RUO
saatavilla, ENG saatavilla)

- <https://www.eoppiva.fi/koulutukset/digiturvallisuus-hyvinvointialueiden-luottamushenkiloille/>

Tietosuoja ABC 2 – tietosuojaan
(RUO saatavilla, ENG saatavilla)

- <https://www.eoppiva.fi/koulutukset/tietosuojaan-abc-syvemmalle-tietosuojaan/>

Turvallisuusluokitellut asiakirjat
(RUO saatavilla, ENG saatavilla)

- <https://www.eoppiva.fi/koulutukset/turvallisuusluokitellut-asiakirjat/>



Koulutukset asiantuntijoille ja johdolle

Turvaa digitaalinen toiminta
häiriötilanteissa (ENG +
RUO)

- <https://www.eoppiva.fi/koulutukset/turvaa-digitaalinen-toiminta-hairiotilanteissa>

Digiriskien hallinta (ENG +
RUO)

- <https://www.eoppiva.fi/koulutukset/riskienhallinta-digimaailmassa>

Digitaalinen turvallisuus
järjestykseen arkkitehtuurin
(ENG + RUO) avulla (Uusi!)

- <https://www.eoppiva.fi/koulutukset/digitaalinen-turvallisuus-jarjestykseen-arkkitehtuurin-avulla/>

Julkri – arvioi ja kehitä
tietoturvallisuutta (Uutuus!)

- <https://www.eoppiva.fi/koulutukset/julkri-arvioi-ja-kehita-tietoturvallisuutta>



Digiturma vai Digiturva -lyhytvideot

1		Vaarat viestissä – Digiturma vai digiturva – osa 1 DVV 0.54
2		Huolellisuutta henkilötiedoissa – Digiturma vai digiturva – osa 2 DVV 0.59
3		Suojaa sähköpostit – Digiturma vai digiturva – osa 3 DVV 1.14
4		Uskomaton uutinen – Digiturma vai digiturva – osa 4 DVV 1.14
5		Tuntematon tikapuilla – Digiturma vai digiturva – osa 5 DVV 1.14
6		Luotatko laskuun? – Digiturma vai digiturva – osa 6 DVV

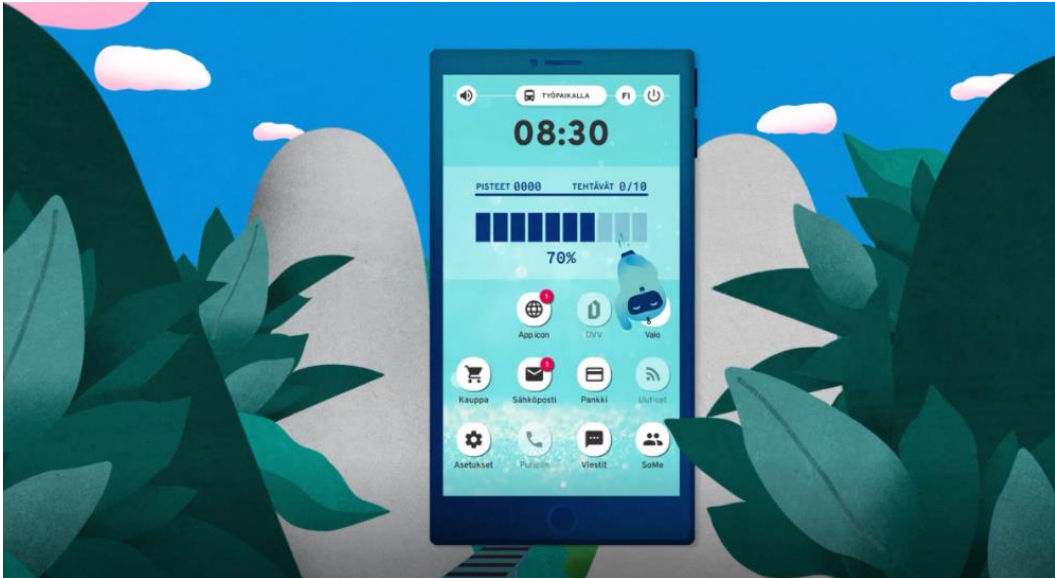
- Lyhytvideoiden sarja tarjoaa keinoja arjen digiturvan parantamiseen työssä ja vapaa-ajalla.
- Opi tunnistamaan digiturvallisuutta uhkaavat tilanteet ytimekkäiden ja hauskojen videoiden avulla.
- Hetken miettiminen ratkaisee, menetkö kohti digiturmaa vai digiturvaa.
- Ota käyttöön kätevä soittolista:
https://youtube.com/playlist?list=PL1_EIQ-Ddub-gVbetAX0qKVPhcdf-ar3



Digiturvallinen elämä -peli



Digiturvallinen elämä -peli pähkinänkuoressa



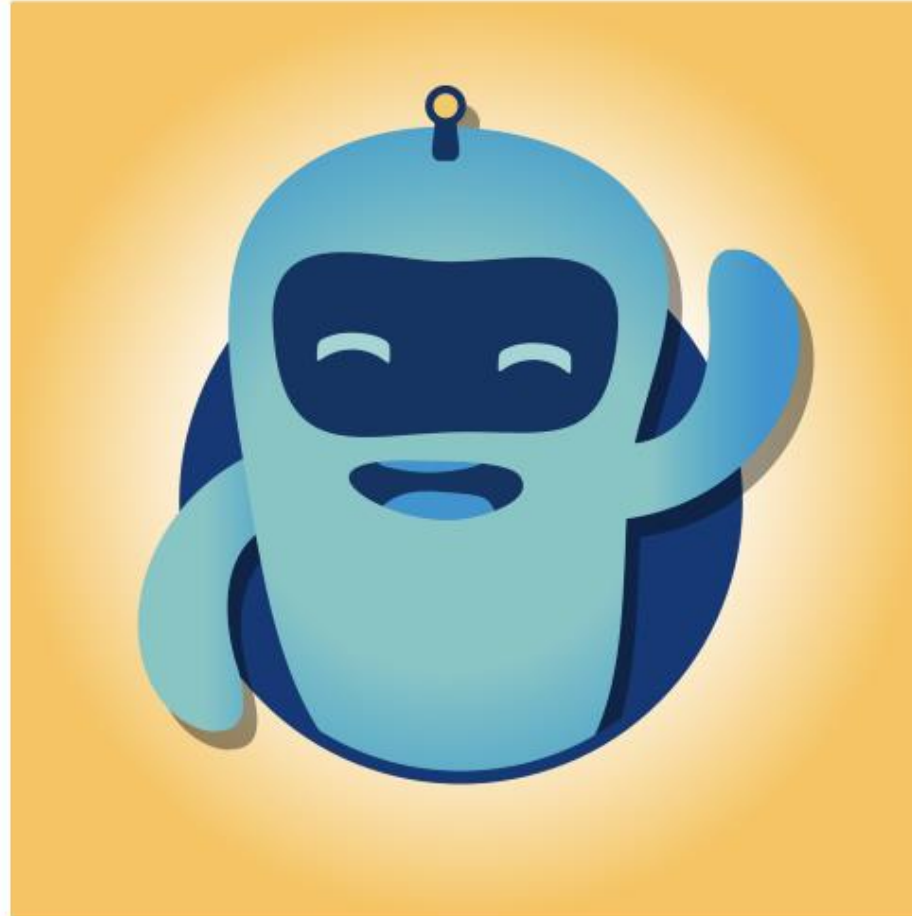
- Ohjaa kuvitteellisen Tyrskylän kunnan työntekijöitä läpi kymmenen digiturvatilanteita täynnä olevan päivän läpi!
- Noin 70 tehtävää!
- Helppo tapa valmentautua itse tai valmennuttaa henkilöstä digiturvasasioissa.
- Englannin- ja ruotsinkieliset versiot!



Ladattavissa IOS ja Android -laitteille!

Google Play:

<https://play.google.com/store/apps/details?id=fi.dvv.digiturvaelama>



App Store:

<https://apps.apple.com/app/id1514065267>



Digiturvallinen elämä -testi (1/3)

- Tapa osoittaa henkilökohtainen perustason digiturvaosaaminen.
- Mitä opin:
 - Pysähdyt miettimään toimintaa digiturvallisuuden kannalta.
 - Kiinnität huomiota tietojen luokitteluun, tilojen, laitteiden ja palveluiden käyttöön työssä ja vapaa-ajalla.
 - Otat tietoturvan ja tietosuojan huomioon viestinnässä.
 - Olet valppaana huijausyritysten ja muun kyberrikollisuuden varalta.



Digiturvallinen elämä -testi (2/3)

- Kehitetty yhdessä VAHTI-asiantuntijaryhmien ja HAUS:n kanssa.
- Julkaistu ensimmäisessä vaiheessa valtionhallintoon.
- Tällä hetkellä testissä on 20 kysymystä, joista arvotaan 15.
- Mahdollisuus täydentää kysymyspatteristoa esimerkiksi haastavimmilla kysymyksillä.



Digiturvallinen elämä –testi (3/3)

- Valtionhallinnossa organisaatioilla on mahdollisuus seurata suorituksia eOppiva-palvelun kautta.
- Muille on suorituksesta ladattavissa todistus.
- Saatavilla kaikille nyt:
<https://www.eoppiva.fi/koulutukset/digiturvallinen-elama-testi/>
- Löytyy myös haulla Digiturvallinen elämä -testi eOppivasta.





DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi