

TIETOJENKALASTELOVIESTIEN TUNNISTAMINEN JA KÄSITTELY



WINNOVA
LÄNSIRANNIKON KOULUTUS OY

Sisälllys

Kuvaus.....	2
Pikaohje.....	2
Sähköpostin tarkastus.....	2
Miten toimia, jos tunnukset on kalastettu?.....	2
Katso minne URL-osoitteen linkki viittaa	3
Tarkastele viestiä kokonaisuutena.....	5
Tarkista lähettäjän todellinen osoite	6
Ilmoita tietojenkalasteluyrityksestä.....	7
Outlookin työpöytäversio	7
Outlookin selainversio	7
Painikkeiden käyttö.....	7
Ilmoita tietojenkalasteluyrityksestä.....	7
Ilmoita viestistä	7
Turvatieto sivu	8
Sähköpostin sääntöjen tarkastaminen	8
Tee ilmoitus.....	8
Opiskelijat	8
Henkilökunta.....	8
Lähteet	8
Näin suojaudut nettihuijaukselta.....	8
Tietojenkalastelu ja epäilyttävä käytös.....	8
Tietojen kalastelulta suojautuminen	8
Näin tunnistat tietojenkalastelun eli verkkourkinnan (phishing)	8

Kuvaus

Jokainen on törmännyt, joskus epäilyttävään sähköpostiin, jolla yritetään saada sinut luovuttamaan luottamuksellista tietoa huijarille. Yleensä tietojenkalasteluviestin tunnistaa helposti oudosta lähetysosoitteesta, kirjoitusvirheistä tai epäilyttävästä sisällöstä. Nykyään viestit voidaan toteuttaa todella uskottavan näköiseksi, joka hankaloittaa kalasteluviestien tunnistamista. Uskottavimmissa viesteissä huijari voi hyödyntää verkosta löytyvää tietoa, kuten etu- ja sukunimeä. Koska tietojenkalastelun toteuttaminen on helppoa ja tehokasta se on todella yleistä.

Tietojenkalastelu eli verkkourkinta (phishing) on tietotekniikassa esiintyvää rikollista toimintaa. Sen avulla pyritään saamaan haltuun luottamuksellisia tietoja, kuten henkilö- tai tilitietoja, esiintymällä tiedon saantiin oikeutettuna tahona. Käyttäjille yleisimmin saapuneet phishing-viestit ovat olleet olevinaan sähköpostitse tulevia salasananakysely liittyen jonkun järjestelmän vaihtumiseen tai ne on merkattu luottamukselliseksi ja sinulla on rajoitettu aika avata linkki.

Kaikkiin linkin sisältäviin viesteihin on suhtauduttava varauksella varsinkin, jos niiden sisällössä on jotakin vähänkin odottamatonta.

Pikaohje

Sähköpostin tarkastus

- Katso minne URL-osoitteen linkki viittaa.
- Tarkastele viestiä kokonaisuutena:
 - Kirjoitusvirheet.
 - Odotatko sähköpostia kyseiseltä henkilöltä?
 - Kiireellisyyden tunne?
 - Jos tunnet lähettäjän, soita ja varmista!
- Jos epäilet saaneesi tietojenkalasteluviestin käytä Outlookissa olevaa **”Ilmoita tietojenkalasteluyrityksestä”** painiketta.
- Asiasta ei tarvitse ilmoittaa tietohallintoon.

Miten toimia, jos tunnukset on kalastettu?

Jos olet klikannut linkkiä tietojenkalasteluviestissä **ja syöttänyt tunnuksesi**, toimi näin:

- Vaihda salasanasi **heti** osoitteessa <https://passwordreset.microsoftonline.com/>
- Tarkista:
 - Turvatieto sivu <https://mysignins.microsoft.com/security-info>
Varmista, että siellä on **vain sinun lisäämäsi tunnistautumistavat.**
Poista muut!
 - **Onko sähköpostiisi lisätty uusia sääntöjä?**
Esim. kaikki Saapuneet kansion viestit ohjataan johonkin muuhun kansioon tms.
Poista kaikki ne mitä et tunnista tai mistä et ole varma!
 - Onko sähköpostisi kautta lähetetty kalasteluviestejä muille?
- Käytä Outlookissa olevaa **”Ilmoita tietojenkalasteluyrityksestä”** painiketta.
- Tee ilmoitus:
Opiskelijat: **Kerro asiasta vastuukouluttajalle**
Henkilökunta: **Ilmoita asiasta tietohallintoon**, joko puhelimitse tai [WinNovan asiointiportaaliin](#).

Katso minne URL-osoitteen linkki viittaa

Lähettilä: [redacted]@winnova.fi>

Lähetetty: torstai 13. huhtikuuta 2023 13.32

Aihe: VL: Postia

WINNOVA

Luottamuksellinen / Konfidentiellt / Confidential

Aihe / Ämne / Subject

KYSYMYKSET

Alkuperäinen URL-osoite:

https://[redacted].podia.com/

Avaa linkki napsauttamalla tai napauttamalla.

[Avaa viesti / Öppna meddelandet / Open message](#)

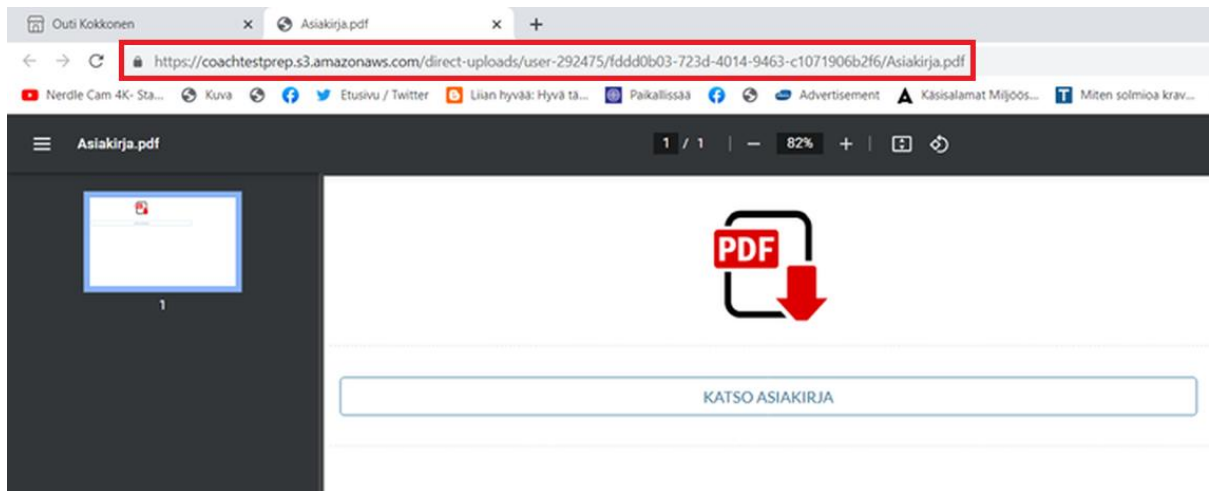
Olet saanut luottamuksellisen viestin. Viesti on suojattu ja siihen voidaan vastata yläpuolella olevasta linkistä. Yhteys on suojattu TLS-salauksella. Turvallisuussyistä viestin lukemista on rajoitettu ja se voidaan lukea korkeintaan 30 päivän ajan.

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 30 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 30 days at most.

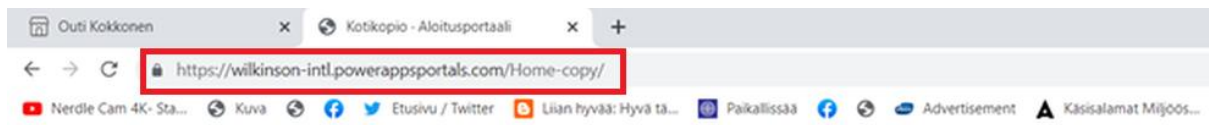
Yllä on kuva huijausviestistä. Tässä ohjeessa kuvattu esimerkki koskee Microsoft Outlookin työpöytäsovellusta, mutta useimmat sähköpostiohjelmat toimivat samaan tapaan.

1. **Siirrä hiiren osoitin linkin päälle.** Tässä tapauksessa "[Avaa viesti / Öppna meddelandet / Open message](#)" on linkki. Linkki on aina se kohta viestistä, jota viestin lähettäjä kehottaa klikkaamaan.
2. Kun hiiren osoitin on linkin päällä, ilmestyy Outlookissa URL-osoite näkyville hiiren osoittimen viereen. Joissakin sähköpostiohjelmissa URL-osoite ilmestyy näkyville esimerkiksi alapalkkiin tai johonkin muuhun kohtaan. Joissakin ohjelmissa myös linkin saa näkyville klikkaamalla sitä hiiren kakkospainikkeella.
3. **Katso URL-osoitetta** ja erityisesti yllä olevassa kuvassa punaisella ympyröityä osaa. **Se ei viittaa esim. toimialueeseen winnova.fi** tai johonkin muuhun selkeästi tunnistettavaan, luotettavaan kohteeseen. Linkki johtaa siis tuntemattomalle sivustolle, joka todennäköisesti antaa mahdollisuuden kirjautua käyttäjätunnuksellasi ja salasanallasi. Jos "kirjautut", salasanasi ja käyttäjätunnuksesi päätyy rikollisten haltuun.
4. Jos olet erehdyksessä klikannut linkkiä, näet osoitteen selaimen osoiterivillä.



Kun tästä klikkaa vielä Katso asiakirja linkkiä päästään "Kirjautumissivulle".

Ao. esimerkkikuvan sivu näyttää päällisin puolin normaalilta kirjautumissivulta, mutta kiinnitä huomiota selaimen osoiterivillä näkyvään osoitteeseen.



Microsoft
Kirjaudu sisään

Sähköposti tai puhelin

Salasana

Etkö pääse tilillesi?

Seuraava

Kirjautumisvaihtoehdot

Tarkastele viestiä kokonaisuutena

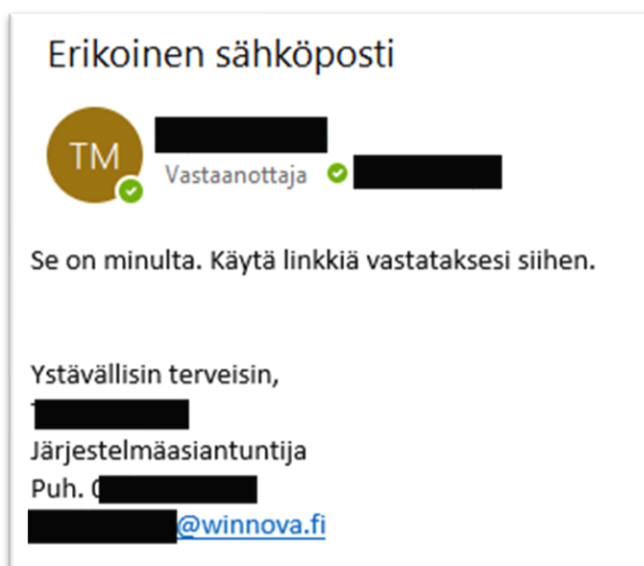
- Jos viestissä yritetään painostaa kiireellisyyteen, kannattaa tilanne rauhoittaa. Kiireellisyyden luominen on yleinen tapa huijauksissa ohjata sinua tekemään jotain ajattelematta.
- Odotatko sähköpostia kyseiseltä henkilöltä tai lähettäjältä? Vaikka ei ole epätavallista saada sähköpostia uudesta sähköpostiosoitteesta, on tärkeää tarkastella viestiä ennen kuin teet mitään jatkotoimenpiteitä.
- Tarkasta onko viesti esim. edelleen lähetetty. Tämän näkee siitä, jos otsikossa lukee VL: tai FWD: merkintä.

Lähettäjä: [REDACTED]@winnova.fi>

Lähetetty: torstai 13. huhtikuuta 2023 13.32

Aihe: VL: Postia

- Aiemmin kalasteluviesteissä oli kirjoitusvirheitä tai viesti oli kirjoitettu huonosti ja tämä viittasi huijaukseen, mutta nykyisenä tekoälyaikana viestit ovat usein oikeinkin hyvää suomea.
- Jos tunnet sähköpostin lähettäjän, mutta olet epävarma viestistä, **ota yhteyttä häneen puhelimitse** varmistaaksesi, että hän on lähettänyt sähköpostin ja se on asiallinen. Mikäli tili on kaapattu, pystyy rikollinen vastaamaan kaikkiin sähköpostiviesteihin:



Tarkista lähettäjän todellinen osoite

From: Metropolia University of Applied Sciences <james666@usan.edu.pe>

Sent: Wednesday 1. June 2022 16.20

To: Matti Meikäläinen <Matti.Meikalainen@metropolia.fi>

Subject: Last notification

Joskus tietojenkäsitteily onnistuu lähettämään sähköpostin niin, että lähettäjän osoite näyttää oikealta. Vaikka tarkistaisitkin lähettäjän osoitteen, se ei ole taivastietoa viestin aitoudesta. Usein viestit tulevat kuitenkin sellaisesta osoitteesta, joka ei kuulu väitettylle lähettäjälle. Näet osoitteen sähköpostiviestin yläpuolelta, kuten kuvassa (oikea osoite on merkitty punaisella).

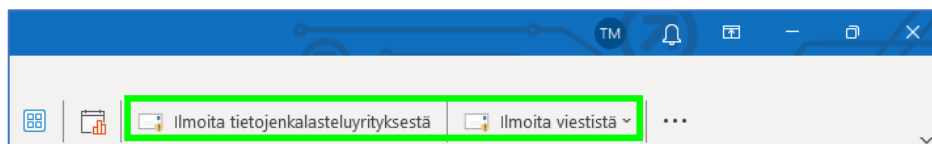
Esimerkissä lähettäjän nimenä on "Metropolia University of Applied Sciences". Kun katsot tarkemmin lähettäjän osoitetta, huomaat, että se ei päätty @metropolia.fi, joka olisi oppilaitoksen sähköpostin oikea loppuosa.

Jos osoite viittaa toiseen lähettäjään kuin mitä lähettäjän nimessä väitetään, on viesti todennäköisesti huijaus. Joskus kuitenkin myös lähettäjän osoite on mahdollista väärentää, tai **viestejä on voitu lähettää murretulta sähköpostitililtä**. Siksi lähettäjän osoite voi näyttää myös aidolta, vaikka kyseessä olisi huijausviesti. Tästä syystä on tärkeää aina tarkastella viestiä myös aiemmin neuvotuilla tavoilla.

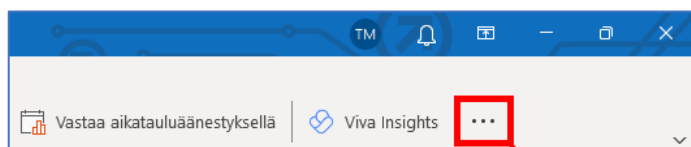
Ilmoita tietojenkalasteluerytyksestä

Outlookiin työpöytä- ja selainversiosta löytyy **Ilmoita tietojenkalasteluerytyksestä** ja **Ilmoita viestistä** painikkeet. Näitä painikkeita käyttämällä voit lähettää tietoja sähköpostista Microsoftille, jotta he voivat parantaa tietojenkalastelu- ja roskapostisuodatintaan. Näistä jää myös merkintä Defender järjestelmään, jotta niitä voidaan tutkia myöhemmin.

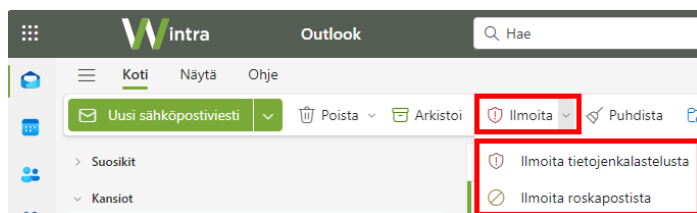
Outlookin työpöytäversio



Mikäli painikkeet eivät näy valikossa, ne ovat piilossa **lisää komentoja** eli ... painikkeen takana.



Outlookin selainversio



Painikkeiden käyttö

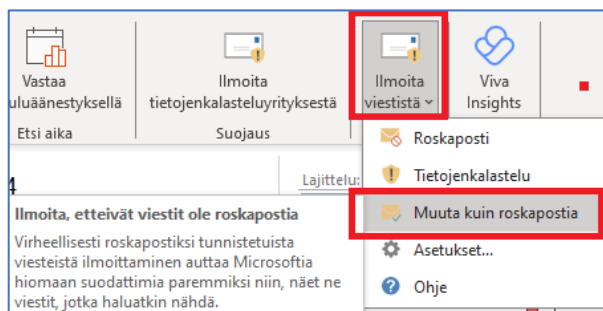
Ilmoita tietojenkalasteluerytyksestä

Valitse epäilyttävä sähköposti ja valitse **"Ilmoita tietojenkalasteluerytyksestä"**.

Ilmoita viestistä

Valitse viesti ja valitse **"Ilmoita viestistä"**. Voit valita, onko viesti **roskapostia** vai **tietojenkalastelua**.

Mikäli viesti on roskapostikansiossa ja se ei mielestäsi ole roskapostia, niin voit ilmoittaa Microsoftille sen olevan **muuta kuin roskapostia**.



Turvatieto sivu

[Oma tili](#) sivuilta löydät [Turvatieto](#) sivun. Sivulta voit tarkastaa käyttämäsi monivaiheisen tunnistautumisen menetelmät.

Tarkasta ja poista ne, joita et tunnista.

Voit myös poistaa kaikki ja lisätä ne uudelleen.

Sähköpostisääntöjen tarkastaminen

Outlookin työpöytäversiossa valitse **Tiedot** välilehti. Valitse oikealta puolelta kohta **Sääntöjen ja ilmoitusten hallinta**.

Outlookin Web versiossa löydä säännöt **lisää vaihtoehtoja** kohdasta eli kolmen pisteen takaa ... ja sieltä kohta **Säännöt** → **Sääntöjen hallinta**.

Tarkasta säännöt ja poista ne, joita et tunnista.

Tee ilmoitus

Jos epäilet, että tunnuksesi on kalastettu, tee ilmoitus. On parempi olla varma asiasta, kuin joutua huijauksen kohteeksi. Mahdollisimman aikainen ilmoitus tietojenkalastelusta auttaa tietohallintoa estämään tietojenkalastelun jatkumisen.

Opiskelijat

Kerro asiasta vastuukouluttajalle ja hän välittää tiedon tietohallintoon.

Henkilökunta

Ota yhteys tietohallintoon, joko puhelimitse tai tekemällä ilmoitus [WinNovan asiointiportaaliin](#).

Lähteet

Näin suojaudut nettihuijaukselta

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta>

Tietojenkalastelu ja epäilyttävä käytös

<https://support.microsoft.com/fi-fi/office/tietojenkalastelu-ja-ep%C3%A4ilytt%C3%A4v%C3%A4-k%C3%A4yt%C3%B6s-0d882ea5-eedc-4bed-aebc-079ffa1105a3>

Tietojen kalastelulta suojautuminen

<https://support.microsoft.com/fi-fi/windows/tietojen-kalastelulta-suojautuminen-0c7ea947-ba98-3bd9-7184-430e1f860a44>

Näin tunnistat tietojenkalastelun eli verkkourkinnan (phishing)

<https://wiki.metropolia.fi/pages/viewpage.action?pageId=62195969>