Terveys- ja hyvinvointialojen opintokokonaisuus

Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa

OPETUS- JA KULTTUURIMINISTERIÖ
UNDERVISNINGS- OCH KULTURMINISTERIET

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

06A – Tietojenkalastelu ja tekoäly

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Terminologia

- Huijaus / Huijausviesti (Hoax)
- Tietojenkalastelu (Phishing)
- Tekoäly (Artifical Intelligence (AI))
- Syväväärennös (Deepfake)
- Hakkeri (Hacker)
- Edistynyt jatkuva uhka (Advanced Persistent Threat (APT))
- Avoimienlähteiden tiedustelu (Open Source Intelligence (OSINT)
- Sosiaalinen vaikuttaminen (Social Engineering)

jamk

Tietojenkalastelu (Phishing)

Kuvailu

- Tietojenkalastelun avulla verkkorikolliset varastavat henkilötietoja, kuten puhelinnumeroita sekä pankki- ja henkilötunnuksia. Tämän lisäksi verkkorikollisia kiinnostavat ihmisten kirjautumistiedot eli käyttäjätunnukset ja salasanat, joiden avulla voidaan kirjautua erilaisiin palveluihin.
    - Yleensä tietojenkalastelu tapahtuu väärennettyjen verkkosivujen avulla. Näillä luotettavilta näyttävillä sivuilla käyttäjät huijataan antamaan tietonsa rikollisille. Tietoja voidaan sitten käyttää käyttäjätilien kaappauksiin tai jopa identiteetti-varkauksiin.
- Tietojenkalastelun avulla voidaan myös tartuttaa haittaohjelmia laitteellesi. Haittaohjelmat naamioidaan kiinnostavaksi sisällöksi, kuten tärkeiksi asiakirjoiksi tai viihdyttäväksi sisällöksi — vaikkapa kissavideoiksi. (Troijalainen haittaohjelma)
- Koska tietojenkalastelussa hyödynnetään viestejä, kuten sähköposteja, kohteiden huijaamiseen, kannattaa kiinnittää huomiota itse viesteihin sekä niiden sisältöön.
    - Tietojenkalastelu- eli phishing-viestit voivat usein olla automaattisella kääntäjällä käännettyjä. Tästä syystä tietojenkalastelu-viestit sisältävät usein kirjoitusvirheitä tai niiden ulkoasu on epäilyttävä.

Lähde: https://www.f-secure.com/fi/articles/what-is-phishing, viitattu 20.12.2024

jamk

Tietojenkalastelu (Phishing)

Yleisimmät erilaiset muodot

- Yleisiä tietojenkalastelun muotoja ovat muun muassa spear phishing eli kohdennettu tietojenkalastelu, smishing ja vishing.
- Kohdennettu tietojenkalastelu eli spear phishing
  - Spear phishing -huijauksen kohteena voi olla yksityishenkilöiden lisäksi organisaatioita sekä niiden johtohenkilöitä. Kun kyseessä on kohdettaan varten räätälöity, kohdennettu tietojenkalastelu, voi huijausta olla paljon vaikeampi tunnistaa kuin tavanomaisessa tietojenkalastelussa.
- Tekstiviestihuijaukset eli smishing
  - Hyödyntää joko teksti- tai pikaviestipalveluita kalastelun välineenä. Verkkorikolliset voivat myös ujuttaa olemassaoleviin viestiketjuihin omia, haitallisia viestejään. Tällöin voi olla vaikea tunnistaa esimerkiksi postin tai lähettipalvelun viestin perään ilmestynyttä huijausviestiä. Myös smishing-viestit sisältävät sähköpostien tapaan linkkejä, jotka ohjaavat huijaus-sivustoille.
- Huijauspuhelut eli vishing
  - Nimi tulee sanoista "voice" ja "phishing". Puheluiden soittajat voivat esiintyä pankin tai muun luotettavan tahon nimissä. Yleisiä ovat myös yritysten tai kohteen työnantajan IT-tuen nimissä tehtävät huijauspuhelut. Näiden tarkoituksena on saada huijauksen uhri asentamaan etähallintaohjelma tietokoneelleen.

Lähde: https://www.f-secure.com/fi/articles/what-is-phishing, viitattu 20.12.2024

jamk

Tietojenkalastelu (Phishing)

Puolustautumis- ja tunnistamiskeinoja

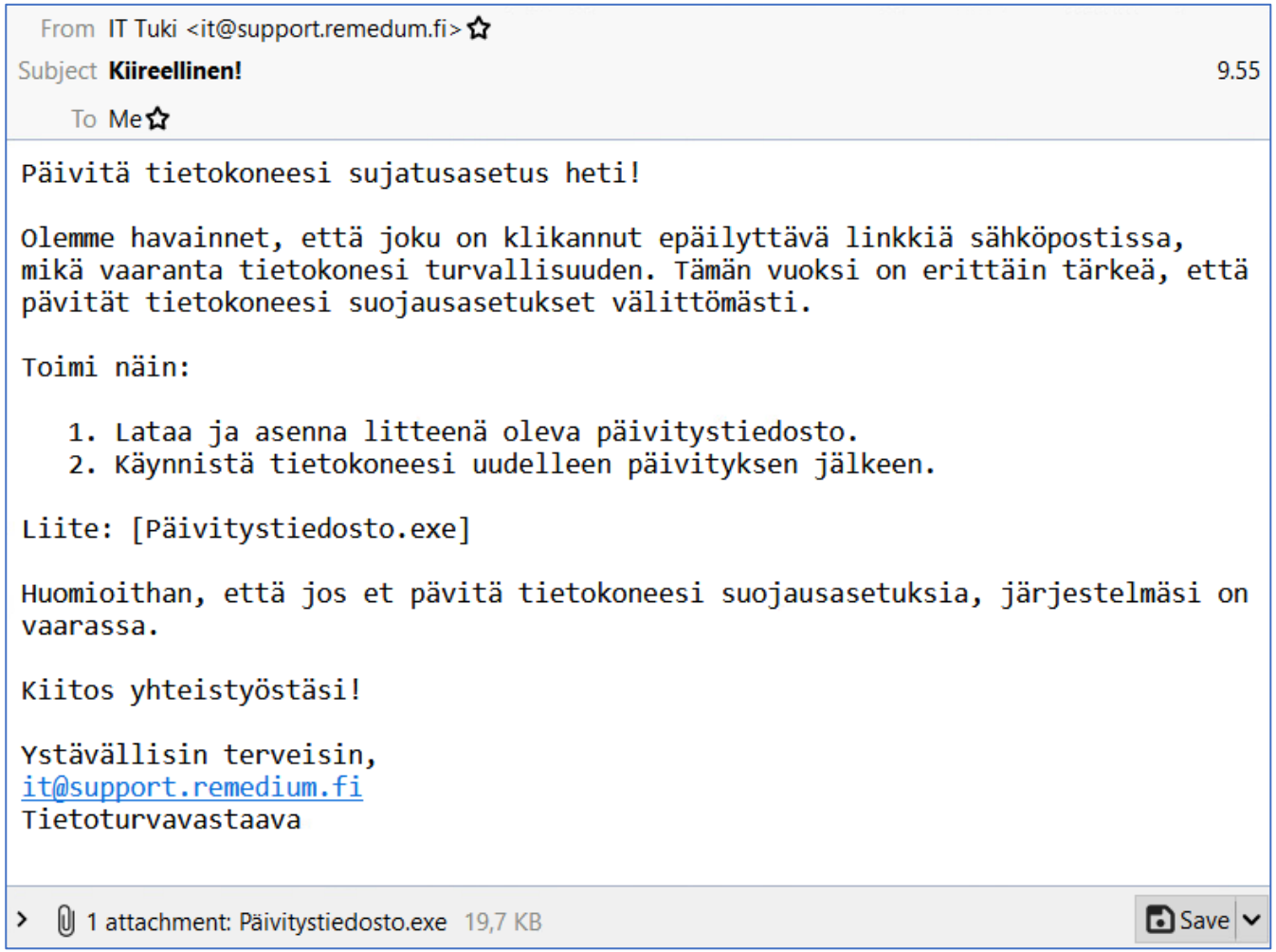
- Tietojenkalastelussa käyttäjää voidaan pyytää kirjoittamaan yksityisiä tietoja huijauslomakkeeseen. Älä siis tee mitään epäilyttävässä viestissä pyydettyä toimenpidettä, kuten anna henkilökohtaisia tietojasi, avaa liitetiedostoja tai asenna ohjelmia, joiden turvallisuudesta et ole varma.
- Rikolliset tietävät hyvin, että kohde saattaa odottaa jotakin toimitusta, kuten internetin välityksellä tilattua pakettia verkkokaupasta. Ja vaikka tietojenkalastelun uhri ei odottaisikaan mitään postissa, on aina mahdollista, että joku haluaa lähettää lahjan postitse.
- Tyypillisimpiä tietojenkalastelukeinoja ovat sähköpostiin lisättävät liitteet ja linkit. Tietojenkalasteluhyökkäyksiä voidaan lähettää myös teksti- tai pikaviesteinä, esimerkiksi WhatsAppin, Messengerin tai muiden vastaavien palveluiden välityksellä.
- Kalasteluviestin uskottavuutta kasvattaa, jos kyseessä on yleisesti luotettava ja tunnettu taho. Varsin usein huijauksia lähetetäänkin jonkin ison ja luotettavan brändin tai muun nimekkään yrityksen nimissä.
- Tietojenkalasteluviesteissä vedotaan usein asian kiireellisyyteen. Jos sinua pyydetään toimimaan nopeasti, suhtaudu viestiin epäilyksellä.
    - Jos asialla olisi aidosti kiire, sinua tuskin lähestyttäisiin sähköpostitse tai tekstiviestin välityksellä. Varsinkaan pankit ja luottokorttiyhtiöt eivät koskaan pyydä vahvistamaan korttitietoja, pankkitunnuksia tai muitakaan tietoja sähköpostitse.
- Aina kun kohtaat jotakin epäilyttävää, kysy itseltäsi: onko tämä realistista ja odotettavissa? Luotatko lähteeseen? Voitko vahvistaa lähteen aitouden esimerkiksi internethaulla tai puhelulla lähettäjälle?

Lähde: https://www.f-secure.com/fi/articles/what-is-phishing, viitattu 20.12.2024

jamk

Phishing sähköposti esimerkkejä

- Huomaatko sähköpostissa olevia ns. Punaisia lippuja (red flags), jotka voisivat herättää epäilyksiä.
- Seuraavalta kalvolta löydät vastaukset



From IT Tuki <it@support.remedum.fi>

Subject **Kiireellinen!** 9.55

To Me

Päivitä tietokoneesi sujatusasetus heti!

Olemme havainnet, että joku on klikannut epäilyttävä linkkiä sähköpostissa, mikä vaaranta tietokonesi turvallisuuden. Tämän vuoksi on erittäin tärkeä, että pävität tietokoneesi suojausasetukset välittömästi.

Toimi näin:

1. Lataa ja asenna litteenä oleva päivitystiedosto.
2. Käynnistä tietokoneesi uudelleen päivityksen jälkeen.

Liite: [Päivitystiedosto.exe]

Huomioithan, että jos et pävitä tietokoneesi suojausasetuksia, järjestelmäsi on vaarassa.

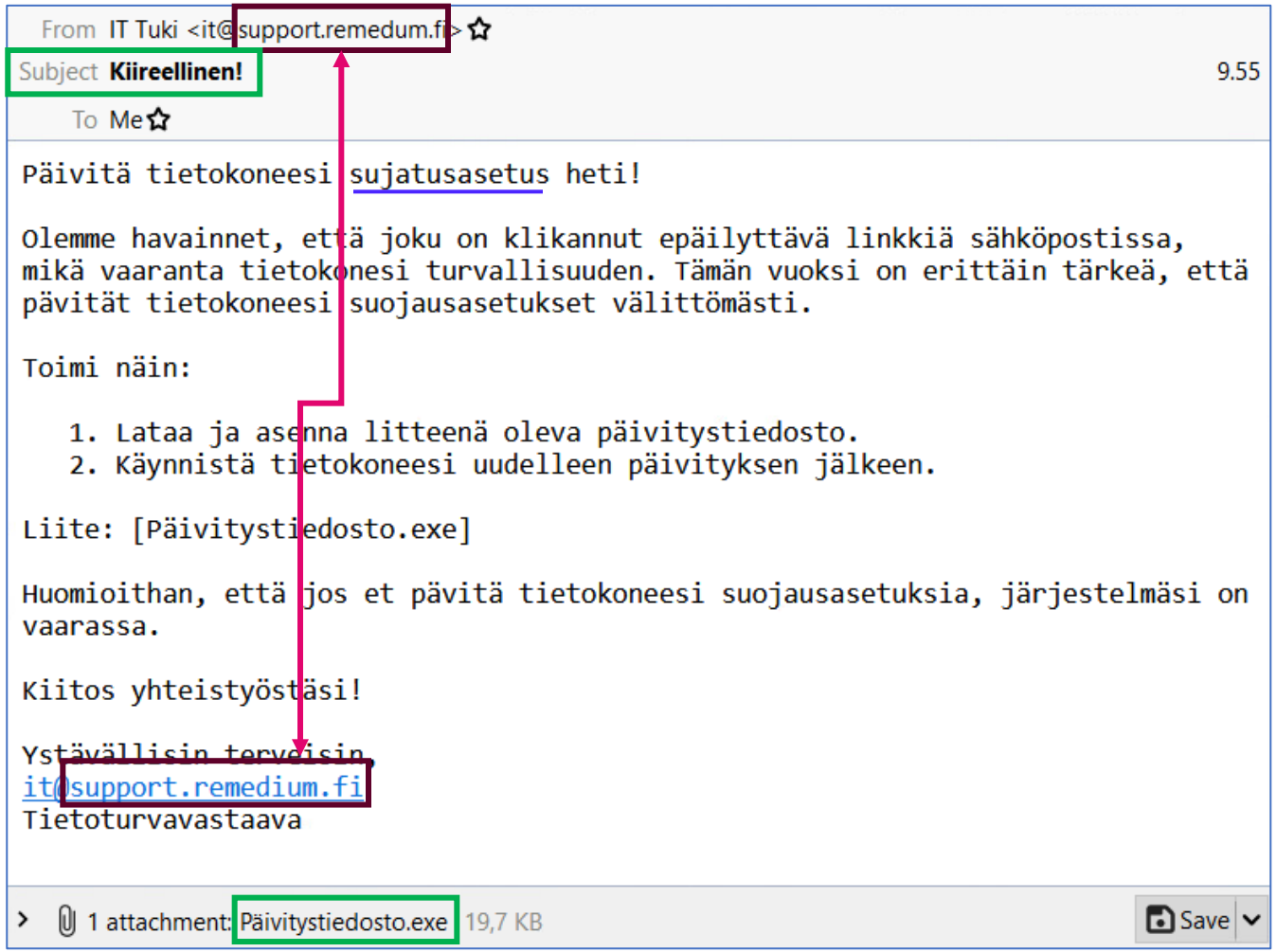
Kiitos yhteistyöstäsi!

Ystävällisin terveisin,
it@support.remedium.fi
Tietoturvavastaava

1 attachment: Päivitystiedosto.exe 19,7 KB Save

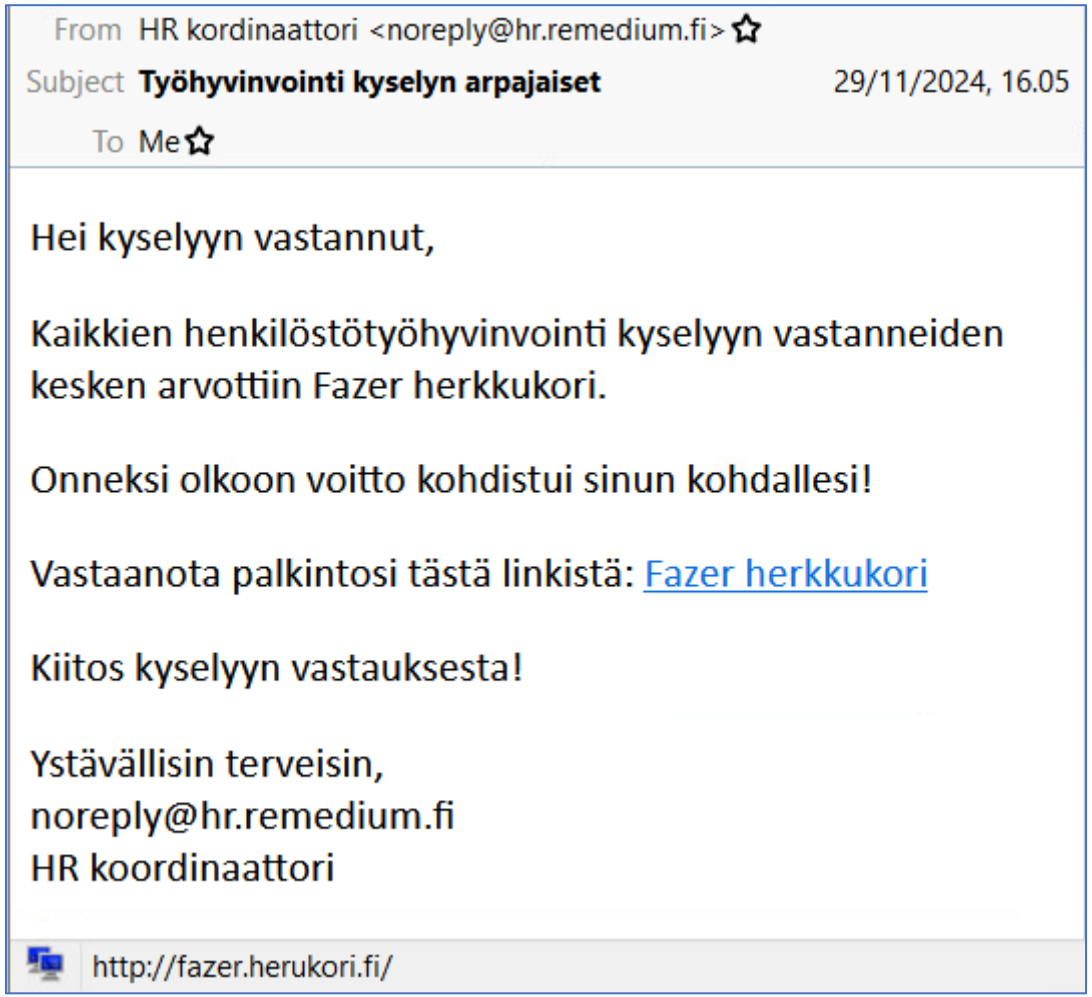
Phishing sähköposti esimerkkejä

- Sähköpostin lähettäjä ei täsmää sähköpostin allekirjoitukseen.
- Usein tietojenkalasteluvi esteissä viitataan kiireeseen tavalla tai toisella
- Usein viesteissä saattaa olla kirjoitusvirheitä (nykyään kielimallit oikovat näitä toki entistä paremmin)



Phishing sähköposti esimerkkejä

- Huomaatko sähköpostissa olevia ns. Punaisia lippuja (red flags), jotka voisivat herättää epäilyksiä.
- Seuraavalta kalvolta löydät vastaukset


From HR kordinaattori <noreply@hr.remedium.fi>
Subject **Työhyvinvointi kyselyn arpajaiset** 29/11/2024, 16.05
To Me

Hei kyselyyn vastannut,

Kaikkien henkilöstötyöhyvinvointi kyselyyn vastanneiden kesken arvottiin Fazer herkkukori.

Onneksi olkoon voitto kohdistui sinun kohdallesi!

Vastaanota palkintosi tästä linkistä: Fazer herkkukori

Kiitos kyselyyn vastauksesta!

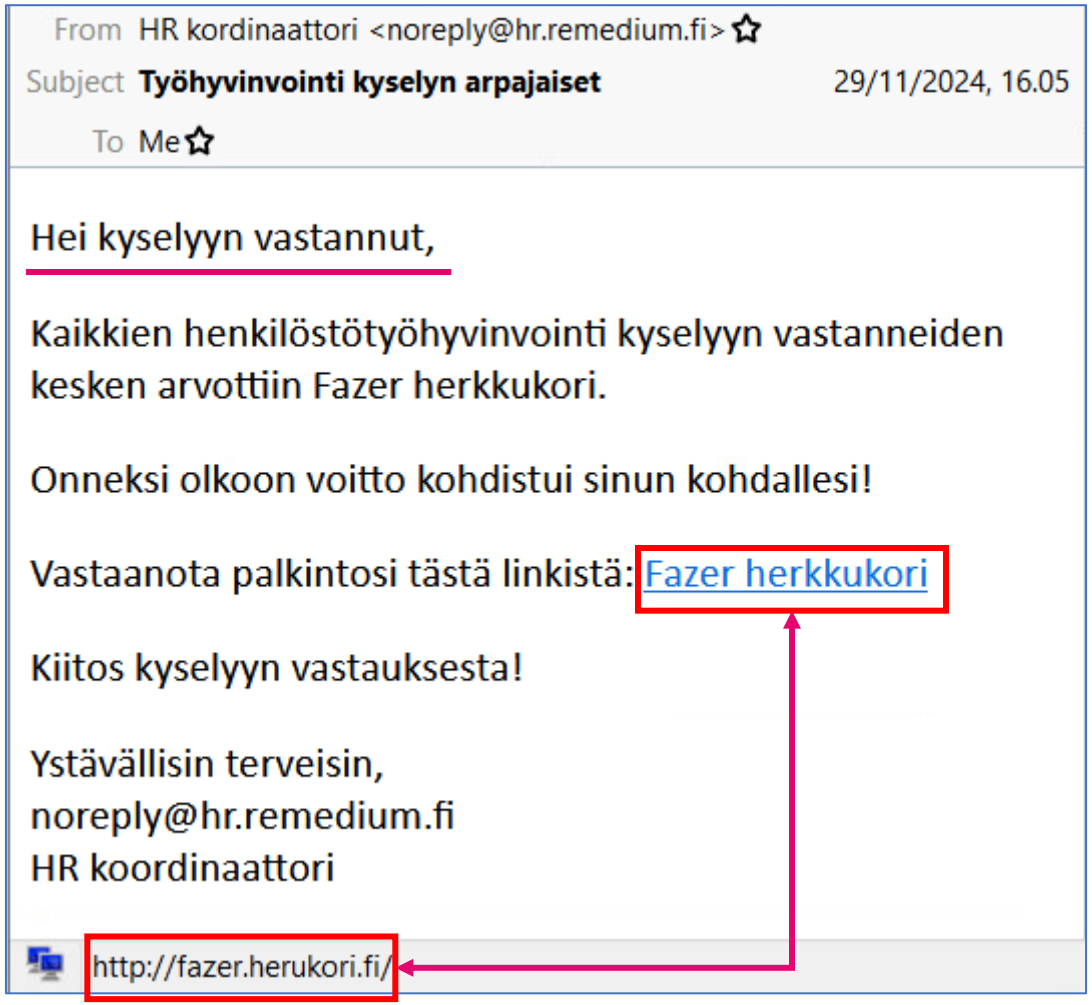
Ystävällisin terveisin,
noreply@hr.remedium.fi
HR koordinaattori

http://fazer.herukori.fi/

jamk

Phishing sähköposti esimerkkejä

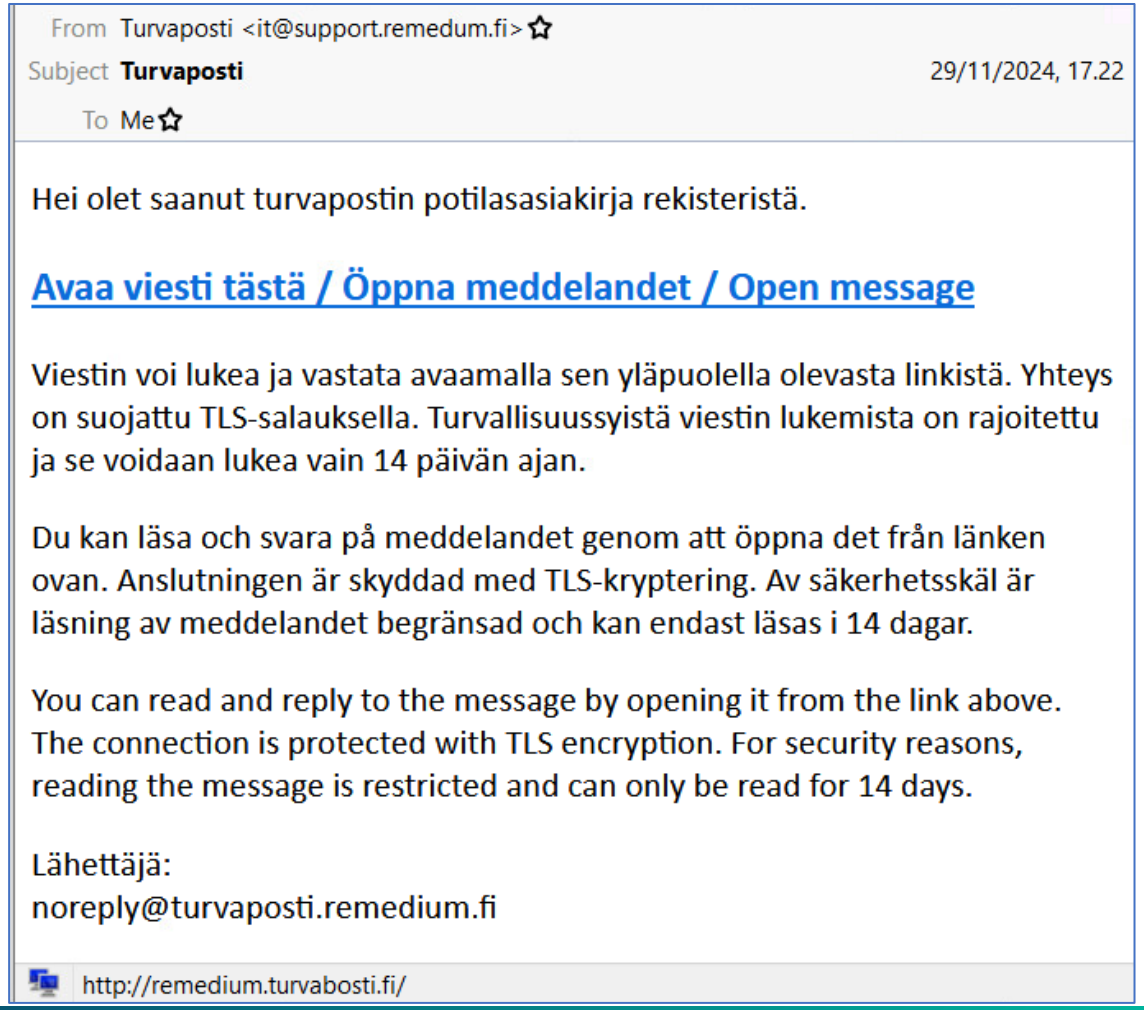
- Usein tietojenkalasteluviesteissä vastaanottaja jätetään mainitsematta, jolloin sama viesti voidaan kohdistaa suureen massaan, tietämättä edes kenelle viesti lähtee.
- Tämän viestin linkki, ei täsmää linkin nimeen ja URL (eli verkko)-osoitteeseen.
- Vaikka lähettäjä voi näyttää ja jopa ollakin aito, tämä voi silti olla tietojenkalastelua



jamk

Phishing sähköposti esimerkkejä

- Huomaatko sähköpostissa olevia ns. Punaisia lippuja (red flags), jotka voisivat herättää epäilyksiä.
- Seuraavalta kalvolta löydät vastaukset



From Turvaposti <it@support.remedum.fi>

Subject **Turvaposti** 29/11/2024, 17.22

To Me

Hei olet saanut turvapostin potilasasiakirja rekisteristä.

Avaa viesti tästä / Öppna meddelandet / Open message

Viestin voi lukea ja vastata avaamalla sen yläpuolella olevasta linkistä. Yhteys on suojattu TLS-salauksella. Turvallisuussyistä viestin lukemista on rajoitettu ja se voidaan lukea vain 14 päivän ajan.

Du kan läsa och svara på meddelandet genom att öppna det från länken ovan. Anslutningen är skyddad med TLS-kryptering. Av säkerhetsskäl är läsning av meddelandet begränsad och kan endast läsas i 14 dagar.

You can read and reply to the message by opening it from the link above. The connection is protected with TLS encryption. For security reasons, reading the message is restricted and can only be read for 14 days.

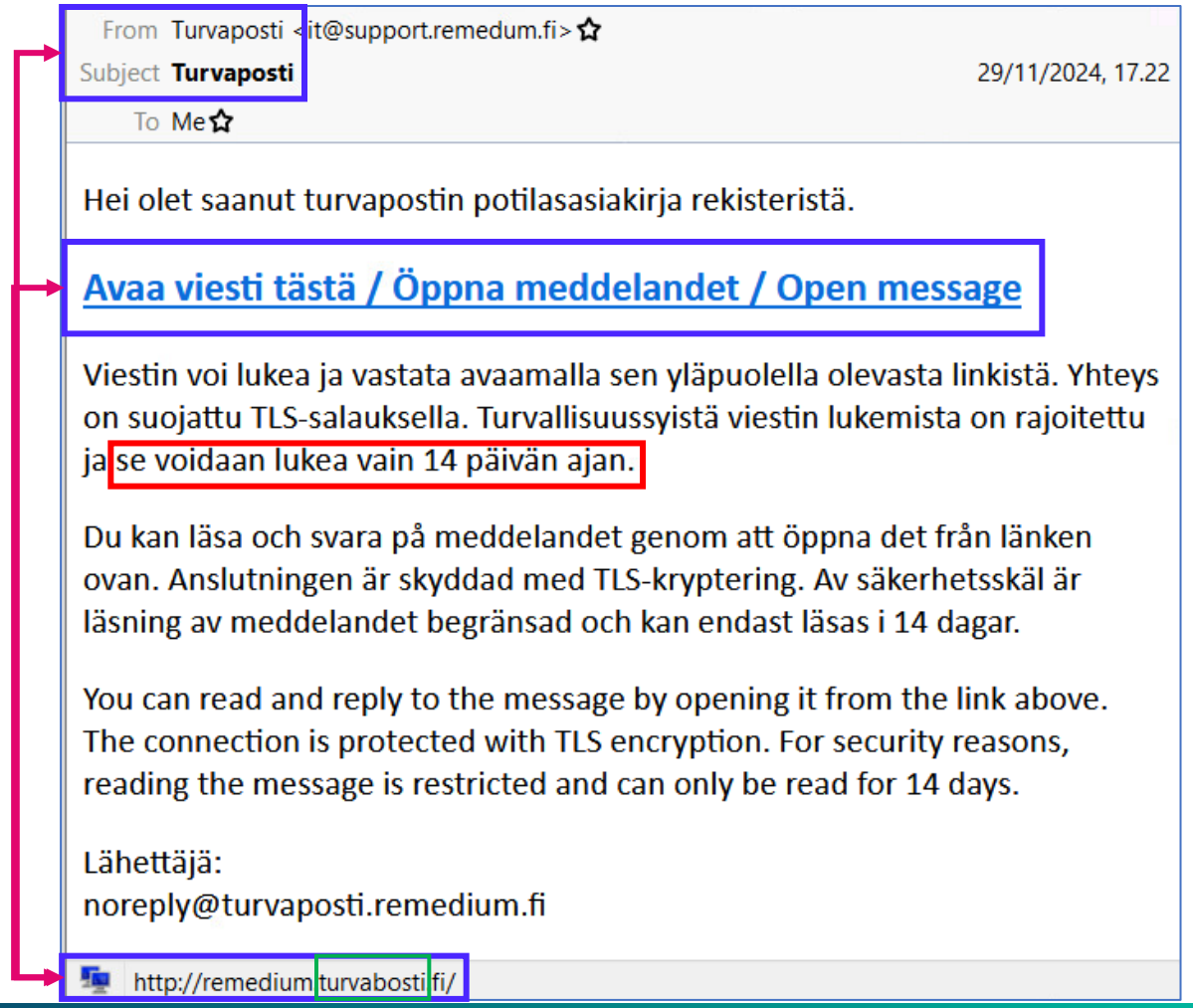
Lähettäjä:
noreply@turvaposti.remedium.fi

http://remedium.turvabosti.fi/

Phishing sähköposti esimerkkejä

- Linkeissä on tärkeintä tarkistaa minne se vie. Sähköpostiohjelmistoista riippuen, linkki näkyy eri tavalla, tässä tapauksessa postin alareunassa.

- Jälleen on viitattu myös kiireeseen



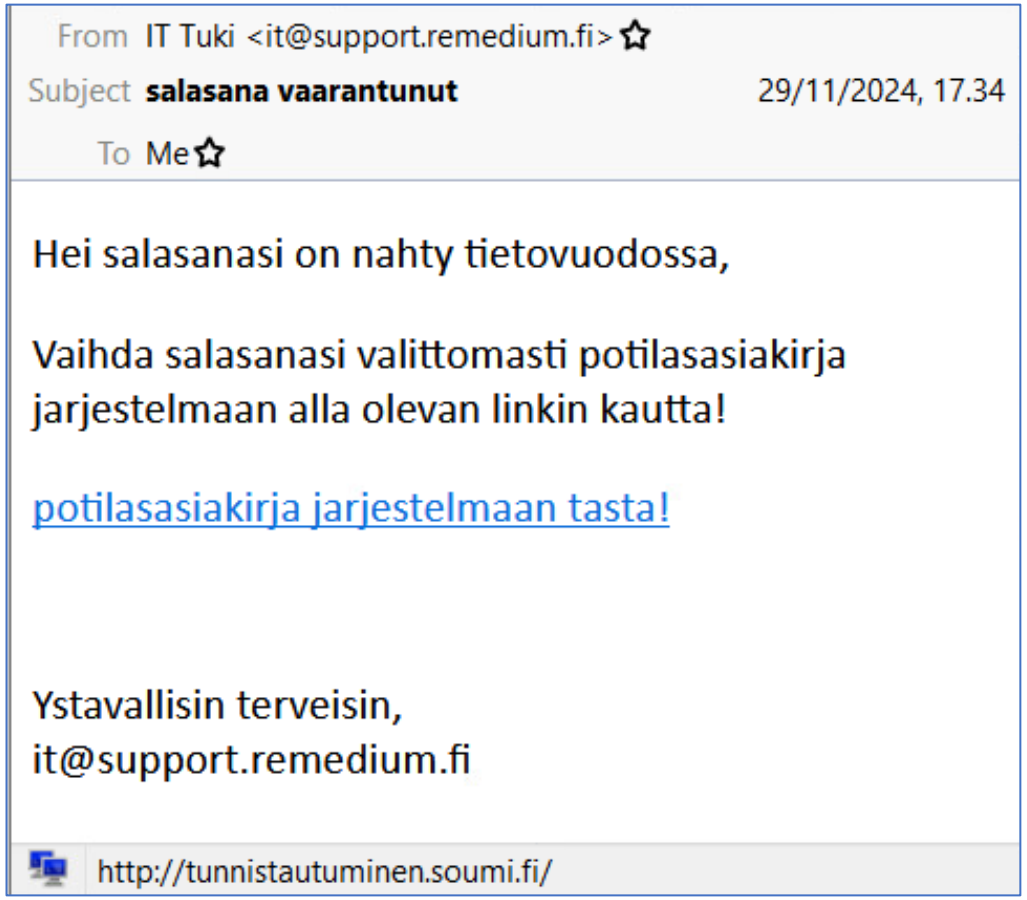
- Knoppitieto: URL (eli verkko-osoite) määräytyy seuraavasti:
- http:// <- kertoo protokollan (verkkosivu)
- remedium. <- kertoo **ali**sivun
- turvabosti. <- kertoo **pää**domainin
- fi. <- kertoo alueen tai sivun myöntäjän (Suomi)

- Näissä sivuissa on oleellisin tieto katsoa nimenomaan päädomainia, koska sillä voi olla mitä tahansa alidomaineja

jamk

Phishing sähköposti esimerkkejä

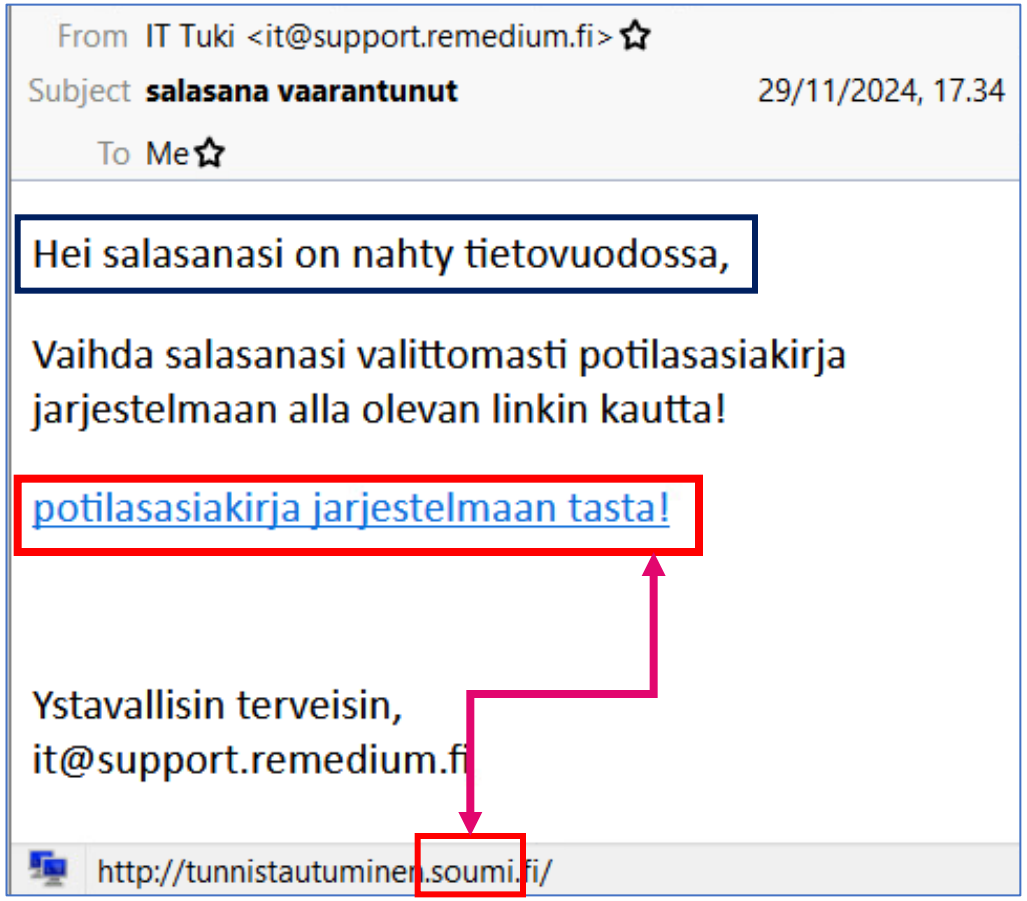
- Huomaatko sähköpostissa olevia ns. Punaisia lippuja (red flags), jotka voisivat herättää epäilyksiä.
- Seuraavalta kalvolta löydät vastaukset



jamk

Phishing sähköposti esimerkkejä

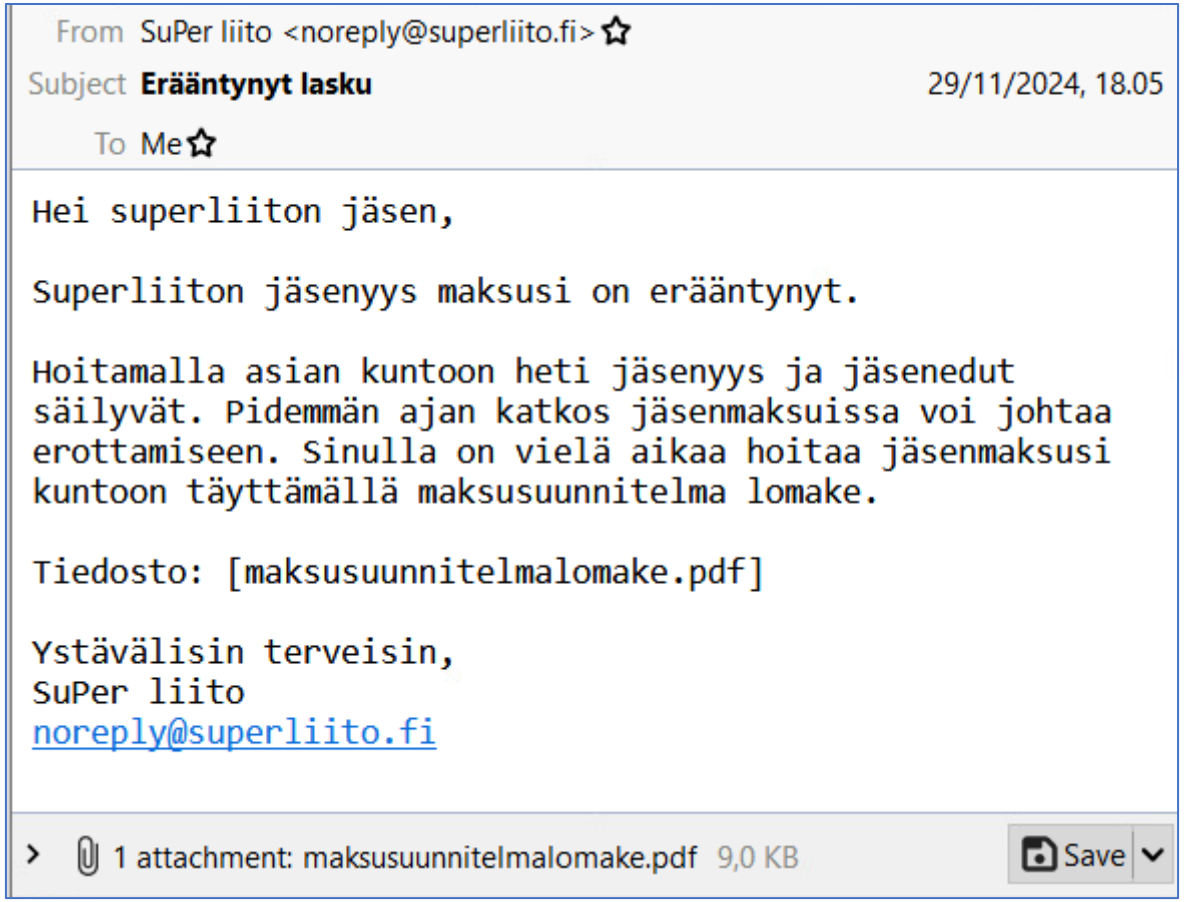
- Viestissä ei ole mainittu vastaanottajaa.
- Tässä viitataan kiireeseen
- Koko viestistä puuttuu ns. Skandit, eli pohjoismaiset aakkoset (å,ä,ö)
- Tunnistautumissivu vie soumi.fi osoitteeseen



jamk

Phishing sähköposti esimerkkejä

- Huomaatko sähköpostissa olevia ns. Punaisia lippuja (red flags), jotka voisivat herättää epäilyksiä.
- Seuraavalta kalvolta löydät vastaukset


From SuPer liito <noreply@superliito.fi>

Subject **Erääntynyt lasku** 29/11/2024, 18.05

To Me

Hei superliiton jäsen,

Superliiton jäsenyys maksusi on erääntynyt.

Hoitamalla asian kuntoon heti jäsenyys ja jäsenedut säilyvät. Pidemmän ajan katkos jäsenmaksuissa voi johtaa erottamiseen. Sinulla on vielä aikaa hoitaa jäsenmaksusi kuntoon täyttämällä maksusuunnitelma lomake.

Tiedosto: [maksusuunnitelmalomake.pdf]

Ystävälisin terveisin,
SuPer liito
noreply@superliito.fi

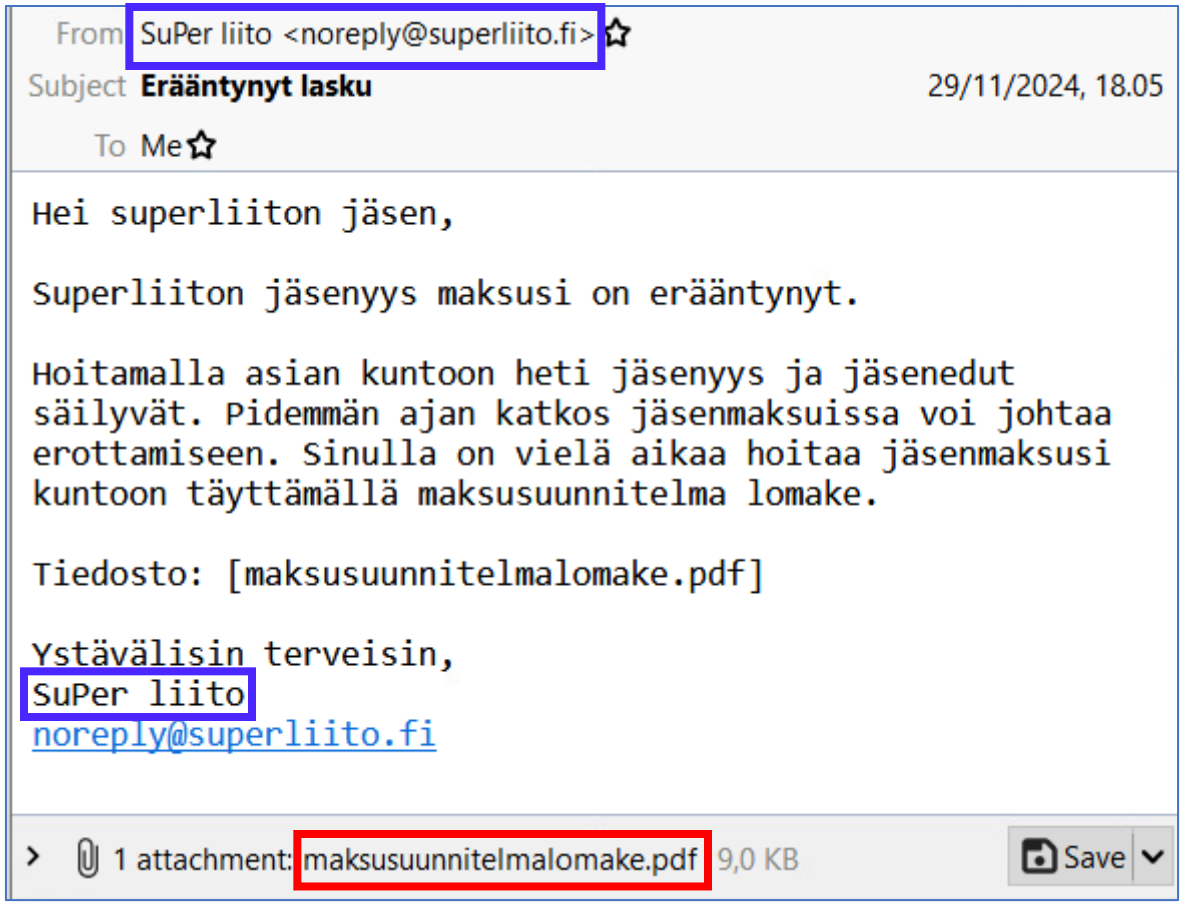
1 attachment: maksusuunnitelmalomake.pdf 9,0 KB Save

jamk

Phishing sähköposti esimerkkejä

- Jälleen vastaanottaja on kohdistamaton.

- Lähettäjä on SuPer liito (eikä esim. Super liitto)
  - Tässä voi toki olla osittain kysymys perinteisemmästä huijauksesta, kuin vain ja ainoastaan verkkohuijauksesta, jos joku olisi rekisteröinyt samankaltaisen nimen, joka taipuu identtisesti


From SuPer liito <noreply@superliito.fi>
Subject **Erääntynyt lasku** 29/11/2024, 18.05
To Me

Hei superliiton jäsen,

Superliiton jäsenyys maksusi on erääntynyt.

Hoitamalla asian kuntoon heti jäsenyys ja jäsenedut säilyvät. Pidemmän ajan katkos jäsenmaksuissa voi johtaa erottamiseen. Sinulla on vielä aikaa hoitaa jäsenmaksusi kuntoon täyttämällä maksusuunnitelma lomake.

Tiedosto: [maksusuunnitelmalomake.pdf]

Ystävälisin terveisin,
SuPer liito
noreply@superliito.fi

1 attachment: maksusuunnitelmalomake.pdf 9,0 KB Save

jamk

Tekoäly mukana huijauksissa

- Etenkin generatiivisen tekoälyn myötä. Tekoälyä voidaan käyttää mm. luomaan ääntä huijauspuheluihin, väärentämään videoita ja kuvia sekä tuottamaan tekstiä huijausviesteihin. Tekoälyn yleistyminen vaatii kuluttajilta entistä parempaa kriittistä medialukutaitoa.
- Suomen kieli on aiemmin karsinut suomalaisiin kohdistuvia huijausyrityksiä, mutta tekoälyn kehityksen myötä huijausyritysten kohdentaminen meille on entistä helpompaa. Huijauksia ei myöskään voi enää yhtä helposti tunnistaa esimerkiksi kielioppivirheistä, koska tekoäly mahdollistaa entistä vakuuttavampien käännösten tekemisen.
- Generatiivinen tekoäly voi oppia uusia asioita sille syötetystä datasta (tiedosta) ja osaa myös luoda sen pohjalta uutta tietoa.
    - Tulevaisuudessa saatamme kohdata yhä kehittyneempiä huijauksia, joissa esimerkiksi läheisen ääntä on kopioitu huijaustarkoituksessa väärennettyyn ääniviestiin.

Lähde: https://www.kuluttajaliitto.fi/materiaalit/tekoalyhuijaukset/, viitattu 20.12.2024

jamk

Tekoäly mukana huijauksissa

Syväväärennös (Deepfake)

- Tekoälyn avulla voidaan tehdä ”syväväärennöksiä” eli erittäin aidon ja realistisen näköisiä videoita, joilla näyttää esiintyvän tuttu henkilö.
- Tämä on kuitenkin huijausta. Ääntä ja kuvaa voidaan poimia esimerkiksi sosiaalisessa mediassa julkaistuista videoista.
- Myös kotimaisia syväväärennöksiä on tehty, tässä kaksi esimerkkiä
  - https://www.is.fi/digitoday/tietoturva/art-2000010677237.html
  - https://yle.fi/a/3-10955498
- Kenties tunnetuin ulkomainen video löytyy Youtubesta:
  - https://www.youtube.com/watch?v=cQ54GDm1eL0
    - **Varoitus!** Sisältää karkeaa kielenkäyttöä

Lähde: https://www.kuluttajaliitto.fi/materiaalit/tekoalyhuijaukset/, viitattu 20.12.2024

jamk

Tekoäly mukana huijauksissa

Äänipuhelut

- Huijarit voivat tuottaa tekoälyn avulla vakuuttavan kuuloista ääntä ja laittaa sen sanomaan mitä haluavat. Huijauksiin voidaan myös väärentää tietyn henkilön ääntä. Toisin kuin perinteiset huijaussoitot, tekoäly mahdollistaa myös vuorovaikutteisen keskustelun.
- Työntekijöihin voidaan kohdistaa huijaussoitto, jossa toimitusjohtaja pyytää kiireellisesti siirtämään rahaa.
  - Ääntä voidaan väärentää esimerkiksi hyödyntämällä sosiaaliseen mediaan ladattuja videoita. Lyhytkin videopätkä voi riittää.
- Samaa teknologiaa käytetään myös huijareita vastaan, tästä esimerkki O2: Daisy
  - https://news.virginmediao2.co.uk/o2-unveils-daisy-the-ai-granny-wasting-scammers-time/
  - Tämän esimerkin avulla voidaan saada hyvä käsitys siitä mihin teknologia pystyy myös huijareiden päässä

Lähde: https://www.kuluttajaliitto.fi/materiaalit/tekoalyhuijaukset/, viitattu 20.12.2024

jamk

Tekoäly mukana huijauksissa

Miten tunnistaa piirteitä?

- Montako sormea ihmisellä on?
- Onko eläimellä tai ihmisellä kaikki raajat tallessa tai ylimääräisiä raajoja?
- Näyttävätkö ihmisen hiukset, kulmakarvat ja/tai parta pehmeiltä ja utuisilta?
- Onko iho kuin muovailuvahaa?
- Liikkuvatko ihmisen suu ja silmät luonnollisesti videolla?
- Onko kuvassa elementtejä, jotka muistuttavat siveltimen vetoja, kuten viereisen kuvan kissan viikset?

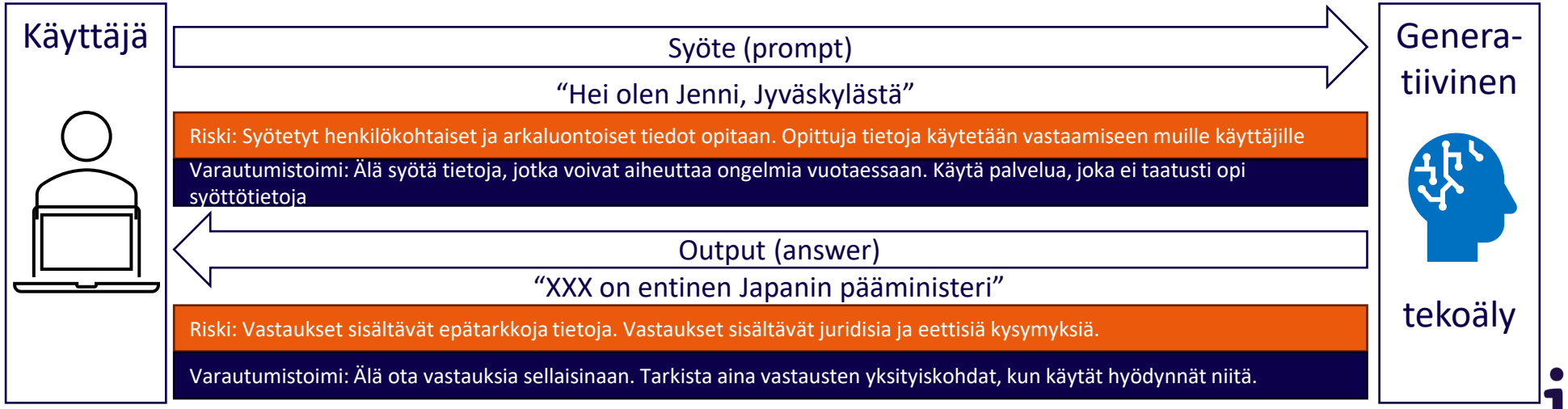
Lähde: https://www.kuluttajaliitto.fi/materiaalit/tekoalyhuijaukset/, viitattu 20.12.2024

jamk

Tekoäly mukana huijauksissa

Tekoälyn käytön riskejä

- Generatiivisen tekoälyn käytössä on kaksi pääasiallista riskiä: tietovuodot ja virheelliset tiedot.
  - Tietovuotoja voi tapahtua, jos käyttäjän syöttämää tietoa käytetään tekoälyn oppimateriaalina, jolloin se voi päätyä muiden käyttäjien saataville. Siksi henkilötietoja tai potilastietoja ei tulisi syöttää tekoälylle.
  - Toinen riski on virheellisten tai epäasiallisten tietojen tuottaminen, kuten harhat, tekijänoikeusrikkomukset, syrjintä ja puolueellisuus. Käyttäjien tulee olla tietoisia näistä riskeistä ja tarkistaa tekoälyn tuottamien tietojen paikkansapitävyys ja lainmukaisuus ennen niiden käyttöä.



Lähde: https://www.nttdata.com/global/en/insights/focus/security-risks-of-generative-ai-and-countermeasures, viitattu 20.12.2024

Huijaukset

Kokemuksista

- Tyypillisiä tietojenkalasteluun liittyviä uhkia sote-kentällä on mahd. liitetiedostot ja linkit, jotka sähköpostiin liitettyinä saatetaan klikata auki kaiken kiireen ja ns. sähköpostiruuhkankin vuoksi.
- Herkästi saattaa sattua inhimillisiä virheitä siis, kun on työkuormaa, kiirettä, melua eikä esim. IT-ohjeistuksia ehkä ehditä lukea tai niihin perehtyä.

jamk

Huijaukset

Pohdintaa

- Milloin viimeksi olet vastaanottanut epäilyttäviä sähköposteja?
  - Oliko kyseessä linkki, liitetiedosto vai jokin muu taktiikka?
- Oletko käyttänyt työ- tai opiskelutehtäviin generatiivista tekoälyä?
  - Oletko huomioinut tietosuojan?
  - Oletko huomannut virheitä vastauksissa?
- Miksi tietojenkalastelut ja huijaukset ovat niin yleisiä?

- Linkki aiheesta Samsung kieltää generatiivisen tekoälyn käytön, sisäisen tietovuodon johdosta:
  - https://techcrunch.com/2023/05/02/samsung-bans-use-of-generative-ai-tools-like-chatgpt-after-april-internal-data-leak/

jamk

Tekoälystä avuksi

Lääkärilehden artikkeli “Tekoäly kirjaa, lääkäri hoitaa“

- Artikkeli "Tekoäly kirjaa, lääkäri hoitaa" käsittelee tekoälyn käyttöä lääkärien vastaanotoilla Länsi-Uudellamaalla ja Pohjois-Pohjanmaalla. Tekoälysovellukset, kuten AIDocLog, hyödyntävät ChatGPT 4o -kielimallia ja Azuren puheentunnistusta, jotta lääkärit voivat keskittyä potilaisiin samalla kun tekoäly hoitaa kirjaukset. Sovellukset tekevät äänitteistä tekstimuotoisia transkriptioita ja luonnostelevat kirjaukset, jotka lääkäri lopuksi tarkistaa ja hyväksyy
  - Kyberturvallisuuden näkökulmasta on tärkeää huomioida seuraavat seikat:
    - **Tietosuoja**: Asiakastietoja käsitellään paikallisesti hyvinvointialueen verkossa, eikä niitä siirretä ulkopuolisille palvelimille. Tämä vähentää tietovuotojen riskiä
    - **Äänitteiden käsittely**: Äänitteitä ei tallenneta, vaan ne käsitellään reaaliajassa. Tämä minimoi arkaluontoisten tietojen väärinkäytön mahdollisuudet
    - **Kielimallien koulutus**: Tekoälyn käsittelemää asiakastietoa ei käytetä kielimallien kouluttamiseen, mikä suojaa potilaiden yksityisyyttä
- Tekoäly tuo paljon hyviä asioita, mutta asiayhteydessä huijaukset ja kyberturvallisuus koulutusmateriaalina, näkökulma on tämänlainen
  - Muista tekoälyn käytön kriittisyys ja parhaat käytänteet

Lähde: https://www.laakarilehti.fi/terveydenhuolto/tekoaly-kirjaa-laakari-hoitaa/, viitattu 14.4.2025

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

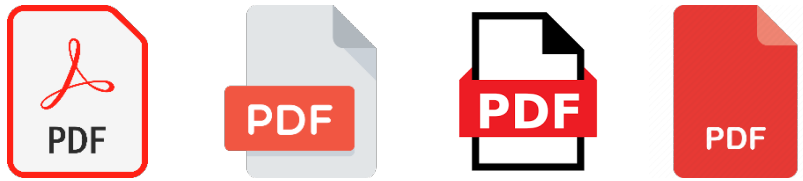
06B – Tiedostoliitteet

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Tiedostoliitteet ja tiedostopäätteet

Testi

- Mikä seuraavista on PDF tiedostopäätteen ikoni?

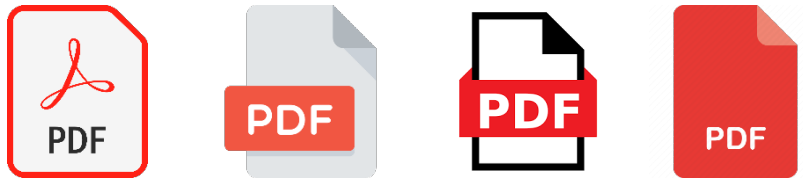


A B C D

Tiedostoliitteet ja tiedostopäätteet

Testi

- Mikä seuraavista on PDF tiedostopäätteen ikoni?



A B C D

- Oikea vastaus on, että riippuu. Kaikki nämä ovat oikein. Tietokoneelle asennettu PDF-lukija määrittää vakio ikonin.

jamk

Tiedostoliitteet ja tiedostopäätteet

Kuvaus

- Tiedostopääte on tietokoneessa tiedoston nimeen liittyvä mutta siitä pisteellä erotettu, useimmiten kolmikirjaiminen tunnusosa, jonka avulla erityyppiset tiedostot erottuvat toisistaan.
  - Esimerkiksi .txt tiedostonimen lopussa osoittaa, että kyseessä on tekstitiedosto, kun taas tiedostopäätteet .png, .gif ja .jpg viittaavat erityyppisiin kuvatiedostoihin. Usein myös eri ohjelmien omiin tiedostomuotoihin liittyy tunnusmerkillinen tiedostopääte.
- Windows käyttöjärjestelmä vaatii tiedostopäätteen, jotta se osaa suorittaa tiedoston tai avata sen oikealla ohjelmalla.
- Tunnistatko seuraavat tiedostopäätteet?
  - ZIP
  - JPG tai JPEG
  - GIF
  - EXE
  - PDF
  - DOC tai DOCX
  - MP4

Lähde: https://fi.wikipedia.org/wiki/Tiedostomuoto, viitattu 20.12.2024
Lähde: https://fi.wikipedia.org/wiki/Tiedostop%C3%A4%C3%A4te, viitattu 20.12.2024

jamk

Tiedostoliitteet ja tiedostopäätteet

Yleisimmät tietojenkalasteluun liittyvät tiedostomuodot

1. ZIP, 7z ja RAR arkistointitiedostot
    - Nämä tiedostot sisältävät tiedostoja sisällänsä ja näihin voi asettaa salasanan. Mikäli arkistolla on salasana, silloin esimerkiksi sähköpostin automaattinen haittaohjelma tutka ei pääse tutkimaan sisältöä. Erityisesti salasanalla salattuihin arkistointitiedostoihin tulee varautua erityisen kriittisesti tästä syystä. Monet uhkatoimijat käyttävät näitä vaikkapa houkuttelevalla nimellä varustettuna haittaohjelmien levitykseen, esimerkkinä **Love_You0891.zip** tai **Loveletter.zip**

2. Microsoft Office tiedostot
    - Erityisesti MSWord dokumentit (DOC, DOCX, **DOCM**), ja MSExcel laskentataulukot (XLS, XLSX, **XLSM**), ja muut Microsoft Office tiedostot ovat suosittuja, sillä näitä ohjelmistoja käytetään monissa töissä päivittäin. Mikäli tiedostopääte on tuo **M** päättyinen tai sisältää **M** kirjaimen, usein kyseessä on tiedosto, joka sisältää ”makroja”. Makro on pala koodia, joka voi teoriassa suorittaa mitä vain. Makroja käytetään myös rehellisiin toimenpiteisiin suorittaman monenlaista automaatiota, eteenkin Excel taulukoissa se on tyypillistä, mutta varmista että luotat lähettäjään, jos vastaanotat makrotetun tiedoston, makro voi esimerkiksi ladata ja asentaa haittaohjelman taustalla. Nämä ovat monesti naamioitu vaikkapa sopimuksiksi, verotiedotteiksi tai kiireellisiksi viesteiksi ylemmältä johdolta.

3. PDF tiedostot
    - Moni tuntee Microsoft Office tiedostojen vaaroista, mutta saattavat olla tietämättömämpiä PDF tiedostoista, jolla voidaan myöskin luoda ja ajaa ajettavaa koodia. Monet rikolliset myöskin piilottavat dokumentteihin tiedostojenkalastelulinkkejä joissa pyritään saamaan luottokorttitiedot ”turvalliselle” sivulle kirjautumalla.

Lähde: https://www.kaspersky.com/blog/top4-dangerous-attachments-2019/27147/, viitattu 20.12.2024

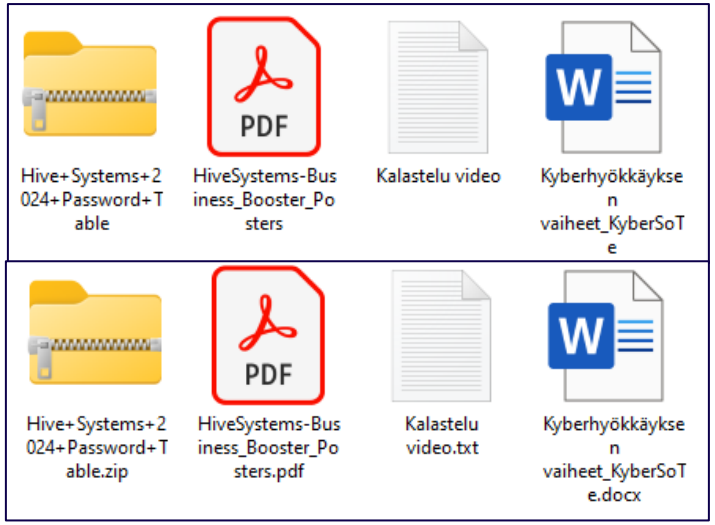
jamk

Tiedostoliitteet ja tiedostopäätteet

Puolustautumiskeinoja ja ongelmia

- Windows käyttöjärjestelmä vakiona piilottaa tunnetun tiedostopäätteen ja näyttää vain ikonin. (Ylemmässä kuvassa on tiedostopäätteet piilotettuina)

- Voit kytkeä tiedostopäätteiden näkyvyyden päälle, jolloin näet todelliset tiedostopäätteet. (Alemmassa kuvassa tiedostopäätteet ovat näkyvissä)

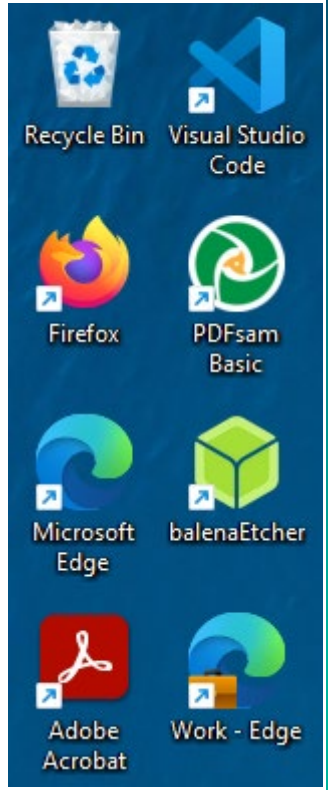


- Haaste: Kuinka montaa tietokonetta (fyysiset ja virtuaaliset) käytät päivittäin tai viikoittain? Onko kaikissa samat asetukset? (Esim. Työpaikka, neuvotteluhuoneen tietokone, koti, kannettava tietokone, mummolan tietokone, lapsen tietokone yms.)

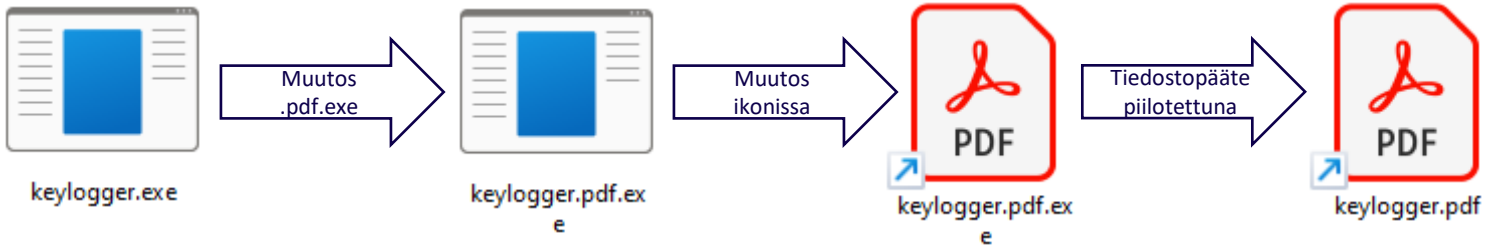
jamk

Tiedostoliitteet ja tiedostopäätteet

Puolustautumiskeinoja ja ongelmia



- Käynnistystiedostot tukevat Windows ympäristöissä ohjelmien omia logoja, ohjelman ikonin voi valita vapaasti millaiseksi vain.
- Ongelmaksi muodostuu, se että uhkatekijät voivat yrittää naamioida haittaohjelmalle ikonin, jonka käyttäjä tunnistaa turvalliseksi.
- **Huom!** Tiedostopäätteen piilottaa käyttäjä, ei uhkatoimija. Uhkatoimija voi varautua tai olettaa käyttäjän hyödyntävän tätä.



- Tässä muodostetaan haittaohjelma.exe, jolle annetaan lisänimi .pdf.exe, vaihdetaan logo ja lopussa käyttäjä on jo laittanut tiedostopäätteen piiloon.
  - (Realismin puutteena, tässä tehtiin vain pikakuvake, mutta samanlailla ohjelmaan voidaan upottaa itse ikonitieto oikean uhkatoimijan toimiessa.)

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

06C – Uhkatoimijat

Lähteet:

https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

https://www.ibm.com/think/topics/threat-actor

https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Uhkatoimijat

Uhkatoimija	Motiivit	Kohteet
Kyberrikolliset	Taloudellinen hyöty, maineen parantaminen	Henkilötiedot, yritysdata, rahoituslaitokset
Sisäpiiriläiset	Taloudellinen hyöty, kosto tai kiristetty henkilö	Organisaation sisäinen data, järjestelmät
Valtiolliset toimijat	Vakoilu, poliittiset, taloudelliset tai sotilaalliset tavoitteet	Julkisen ja yksityisen sektorin verkostot
Haktivistit	Poliittiset, sosiaaliset tai ideologiset syyt	Julkiset ja yksityiset organisaatiot
Terroristijärjestöt	Häirintä, rekrytointi	Viestintäkanavat, rekrytointialustat
Jännityksenhakijat	Huvin vuoksi, teknisen osaamisen kehittäminen	Satunnaiset kohteet, haavoittuvat järjestelmät

jamk

Tyypillisimmät uhat ja tekijät

Uhka	Tyypilliset uhkatekijät	Tyypillinen kohde
Tietojenkalastelu (Phishing)	Kyberrikolliset, hakkerit	Yksityiset, yritykset
Kiristyshaittaohjelmat (Ransomware)	Kyberrikolliset	Yritykset, terveysala
Haittaohjelmat (Malware)	Kyberrikolliset, hakkerit, valtiolliset toimijat	Yksityiset, yritykset
Vakoilu (Spy)	Valtiolliset toimijat	Yritykset, hallitukset
Sisäpiiriuhat (Insider Threat)	Sisäpiiriläiset	Yritykset
Hajautetut palvelunesto hyökkäykset (DDoS-hyökkäykset)	Hakkerit, jännityksenhakijat	Yritykset, palveluntarjoajat
Sosiaalinen manipulointi (Social Engineering)	Hakkerit, kyberrikolliset	Yksityiset, yritykset
Identiteettivarkaudet	Kyberrikolliset	Yksityiset
Rekrytointi	Terroristijärjestöt	Yksityiset

Esimerkki tapaus

Change Healthcare

- **Tapahtuma:** Change Healthcare joutui merkittävän kiristyshaittaohjelmahyökkäyksen kohteeksi. Hyökkäyksessä kyberrikolliset onnistuivat lukitsemaan organisaation tiedostot ja vaativat lunnaita niiden vapauttamiseksi
- **Vaikutukset:**
  - **Potilastiedot:** Hyökkäys vaaransi potilastietojen luottamuksellisuuden ja saatavuuden.
  - **Toiminnan häiriöt:** Hyökkäys aiheutti merkittäviä häiriöitä terveydenhuollon palveluiden toiminnassa, mikä vaikutti potilaiden hoitoon ja organisaation päivittäiseen toimintaan.
  - **Taloudelliset menetykset:** Organisaatio kärsi taloudellisia menetyksiä sekä suoraan lunnaiden maksamisesta että epäsuorasti toiminnan keskeytyksistä ja maineen menetyksestä johtuen.
- **Opit:**
  - **Tietoturvakäytännöt:** Tapaus korostaa vahvojen tietoturvakäytäntöjen ja -protokollien merkitystä terveysalalla.
  - **Varautuminen:** Organisaatioiden tulee varautua mahdollisiin kyberhyökkäyksiin ja kehittää valmiussuunnitelmia, jotka auttavat minimoimaan hyökkäysten vaikutukset.
- Tämä tapaus on hyvä esimerkki siitä, kuinka kyberrikolliset voivat kohdistaa hyökkäyksiä terveysalaan ja kuinka tärkeää on suojata potilastietoja ja varmistaa terveydenhuollon palveluiden jatkuvuus

Lähde: https://www.csoonline.com/article/3484304/the-cyber-assault-on-healthcare-what-the-change-healthcare-breach-reveals.html, viitattu 9.4.2025

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

06D – Sosiaalinen vaikuttaminen (Social engineering)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sosiaalinen vaikuttaminen

Kuvaus

- Sosiaalinen manipulointi on tekniikka, jossa hyödynnetään ihmisten luottamusta ja tietämättömyyttä tietojen hankkimiseksi tai järjestelmien murtautumiseksi.
- Sosiaalisen manipuloinnin määritelmä:
  - Sosiaalinen manipulointi tarkoittaa ihmisten manipulointia psykologisten tekniikoiden avulla, jotta he paljastavat arkaluonteisia tietoja tai suorittavat tiettyjä toimia.
    - Se on merkittävä uhka tietoturvalle.

Lähde: Practical Social Engineering ja Learn Social Engineering, viitattu 9.4.2025

jamk

Sosiaalinen vaikuttaminen

Pretexting ja Baiting

- **Pretexting** tarkoittaa tekaistujen tarinoiden tai valheiden käyttöä, jotta uhri paljastaa arkaluonteisia tietoja.
  - Esimerkiksi esittäytyminen pankkivirkailijaksi.

- **Baiting** on tekniikka, jossa uhri houkutellaan paljastamaan tietoja tai lataamaan haittaohjelmia tarjoamalla houkuttelevaa sisältöä, kuten ilmaisia ohjelmia tai musiikkia.

Lähde: Practical Social Engineering ja Learn Social Engineering, viitattu 9.4.2025

jamk

Sosiaalinen vaikuttaminen

Tailgating ja Quid Pro Quo

- **Tailgating** tarkoittaa luvattoman henkilön pääsyä suojattuun tilaan seuraamalla luvallista henkilöä sisään.

- **Quid Pro Quo** on tekniikka, jossa tarjotaan palvelusta tai tietoa vastineeksi arkaluonteisista tiedoista.

Lähde: Practical Social Engineering ja Learn Social Engineering, viitattu 9.4.2025

jamk

Sosiaalinen vaikuttaminen

Impersonation ja Dumpster Diving

- **Impersonation** tarkoittaa toisen henkilön esittämistä, jotta saadaan pääsy arkaluonteisiin tietoihin tai tiloihin.

- **Dumpster Diving** on tekniikka, jossa hyökkääjä etsii roskista asiakirjoja tai tietoja, joita voidaan käyttää hyökkäyksissä
  - Nimenmukaisesti, tämä voi tapahtua roskalavalta, mutta pitää sisällään muitakin fyysisen pääsyn kohteita (paperinkeräysastiat ym.), SER-lavan sisällöt (muistitikut tai muut tallennusvälineet ym.).

Lähde: Practical Social Engineering ja Learn Social Engineering, viitattu 9.4.2025

jamk

Sosiaalinen vaikuttaminen

Shoulder Surfing ja Elicitation

- **Shoulder Surfing** tarkoittaa arkaluonteisten tietojen urkkimista katsomalla uhrin olkapään yli.

- **Elicitation** on tekniikka, jossa hyökkääjä käyttää keskustelutaitojaan saadakseen uhrin paljastamaan tietoja

Lähde: Practical Social Engineering ja Learn Social Engineering, viitattu 9.4.2025

jamk

Sosiaalinen vaikuttaminen

Honey Trap ja Watering Hole

- **Honey Trap** on tekniikka, jossa hyökkääjä houkuttelee uhrin luottamukselliseen suhteeseen saadakseen tietoja.

- **Watering Hole** on hyökkäys, jossa haittaohjelma sijoitetaan uhrin usein vierailemaan verkkosivustoon.

Lähde: Practical Social Engineering ja Learn Social Engineering, viitattu 9.4.2025

jamk

Sosiaalinen vaikuttaminen

Yhteenveto ja johtopäätökset

- Sosiaalinen manipulointi on merkittävä uhka, mutta tietoisuuden lisääminen ja oikeat suojautumiskeinot voivat vähentää riskiä.

- Ole valppaana ja suojaa tietosi.
  - Muista, että tieto on paras puolustus.

jamk

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences