VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Valtteri Missonen

TIETOJENKALASTELU –

MUODOT, VAIKUTUKSET JA SUOJAUTUMINEN

Tekniikka

2024

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Valtteri Missonen
Opinnäytetyön nimi	Tietojenkalastelu – Muodot, vaikutukset ja suojautuminen-
Vuosi	2024
Kieli	suomi
Sivumäärä	53
Ohjaaja	Jukka Matila

Tämän opinnäytetyön aiheena on tietojenkalastelu, joka muodostaa yhden suurimmista kyberuhista nykyaikaisessa digitaalisessa maailmassa. Tietojenkalastelu tarkoittaa tilannetta, jossa hyökkääjä yrittää huijata käyttäjän luovuttamaan arkaluonteisia tai henkilökohtaisia tietoja petollisiin tarkoituksiin.

Tietojenkalastelu voi tapahtua eri muodoissa, kuten sähköpostitse, tekstiviestitse, puhelimitse tai QR-koodien avulla ja voivat aiheuttaa vakavia seurauksia, kuten taloudellisia menetyksiä, toiminnallisia häiriöitä ja mainevahinkoja. Tämän vuoksi on tärkeää, että yksilöt ja organisaatiot ovat tietoisia tästä uhasta ja toteuttavat asianmukaiset suojatoimenpiteet tietojenkalastelun torjumiseksi. Tähän kuuluvat muun muassa käyttäjien koulutus, haittaohjelmien torjuntaohjelmistot, laitteiden ja sovellusten päivitykset sekä vahvat salasanat ja monivaiheinen todennus.

Tässä opinnäytetyössä käydään ensiksi läpi, mitä tietojenkalastelu todellisuudessa on, sen eri muodot, niiden vaikutukset ja keinot suojautua niitä vastaan. Tämän jälkeen analysoidaan yrityksille tehtyjä tietojenkalastelusimulaatioita ja selvitätään mitkä piirteet tietojenkalasteluviesteissä saavat käyttäjän avaamaan viestin, vierailemaan viestin sisältämissä linkeissä tai antamaan jopa tietojansa.

Avainsanat tietojenkalastelu, kyberuhka, kyberrikollisuus, tietoturva

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikka

ABSTRACT

Author	Valtteri Missonen
Title	Phishing – Forms, effects and protection
Year	2024
Language	Finnish
Pages	53
Name of Supervisor	Jukka Matila

The topic of this thesis is phishing, which is one of the biggest cyber threats in the modern digital world. Phishing refers to a situation where an attacker attempts to deceive a user into disclosing sensitive or personal information for fraudulent purposes.

Phishing can occur in various forms, such as through email, text messages, phone calls, or QR codes, and can result in serious consequences such as financial losses, operational disruptions, and reputational damage. Therefore, it is important for individuals and organizations to be aware of this threat and implement appropriate countermeasures to combat phishing. These may include user education, anti-malware software, device and application updates, as well as strong passwords and multi-factor authentication.

In this thesis, we will first go through what phishing is, the different forms of phishing, effects, and ways to defend against phishing attacks. Then we analyze phishing simulations conducted for companies and investigate which features in phishing messages prompt users to open the message, visit the links contained within the message, or even provide their information.

Keywords phishing, cyber threat, cybercrime, cybersecurity

SISÄLLYS

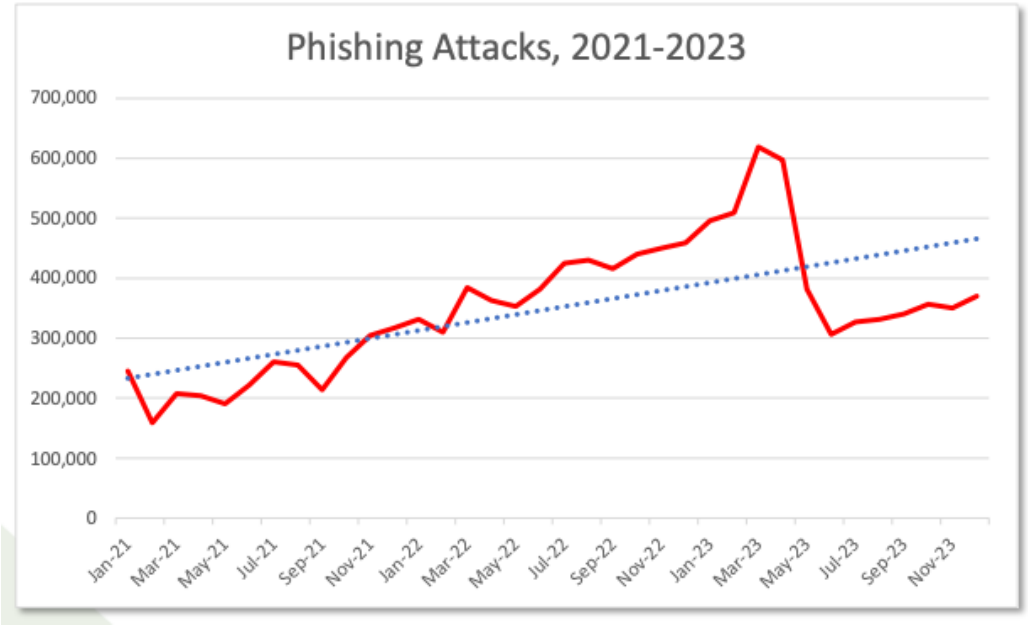
KUVALUETTELO

ERITYISSANASTO

APWG	Anti-Phishing Working Group
Domain	Verkkotunnus eli domain on sivuston osoite
Hakkeri	Tietojärjestelmiin murtautuva henkilö
Sosiaalinen manipulointi	Manipulointitekniikka, jossa käytetään hyväksi inhimillisiä virheitä yksityisten tietojen, pääsyoikeuksien tai muiden arvokkaiden tietojen tai asioiden hankkimiseen
URL	Uniform Resource Locator, tarkoittaa verkkosivuston osoitetta
QR-koodi	Ruutukoodi on kaksiulotteinen kuviokoodi, johon on koodattu informaatiota

1 JOHDANTO

Tietojenkalasteluhyökkäykset ovat yksi suurimmista uhista yrityksille tänä päivänä, ja hyökkäykset ovatkin yleistyneet vuosi vuodelta (APWG, 2024; Luse & Burkman, 2021). Siksi työntekijöitä pidetään ensimmäisenä puolustuslinjana tai päinvastoin - heikoimpana lenkkinä turvallisuusketjussa. Toisin sanoen ihmiset ovat tällä hetkellä suurin uhka yrityksille (Al-Mohannadi ja muut, 2018). Tietojenkalasteluyritysten onnistumisprosentti on kasvanut vuosien varrella, joten on tärkeää, että työntekijät ovat hyvin koulutettuja ja tietoisia tietojenkalasteluhyökkäysten muodoista ja vaikutuksista (Alharthi & Regan, 2020; APWG, 2024). Koska kyberrikolliset keksivät jatkuvasti uusia luovia tapoja huijata ihmisiä, on herännyt kysymys siitä, miten yritysten, heidän työntekijöidensä ja verkkojensa sensitiivistä tietoa voidaan suojata paremmin (Vayansky & Kumar, 2018). Kuvasta 1 voidaan nähdä todenettujen hyökkäysten kasvu vuodesta 2021 vuoteen 2023.



Kuva 1. Todennetut tietojenkalastuhyökkäykset 2021–2023 (APWG, 2024)

Sähköposti on ollut yritysten pääasiallinen viestintäväline jo vuosien ajan, mikä tarkoittaa, että vastaanotettujen, luettujen ja lähetettyjen viestien määrä kasvaa joka vuosi ja se on kasvanut vielä enemmän COVID19-pandemian aikana, joka alkoi vuonna 2020. Lisäksi maailmanlaajuinen pandemia on jättänyt jälkensä tietoturvan alalle. Ihmisille on muodostunut entistä enemmän tavaksi työskennellä kotona tai muissa todennäköisesti vähemmän suojatuissa verkkoympäristöissä kuin toimistossa. (Ramadan ja muut, 2021.)

Lisäksi tietojenkalasteluhyökkäykset kehittyvät vuosi vuodelta ja siksi on tärkeää, että yritykset kouluttavat työntekijöitään tietojenkalastelun uhista, seurauksista ja lisäävät heidän turvallisuustietoisuuttaan. Yksi lähestymistapa on järjestää säännöllisiä turvallisuuskoulutuksia, jotka voivat auttaa päivittämään tietoa kyberrikollisten käyttämistä uhista ja tekniikoista. (Vayansky & Kumar, 2018.)

Toinen tapa, joka yleensä täydentää tietoisuutta kyberuhista, on yrityksen IT-osaston tai muun vastaavan palveluntarjoajan tekemät todelliset simuloidut tietojenkalasteluhyökkäykset. Simuloitujen hyökkäysten avulla yritykset testaavat ja voivat nähdä, kuinka hyvin heidän työntekijänsä ovat valmistautuneet tällaisiin hyökkäyksiin. Simulaatiot auttavat myös räätälöimään tietoturvakoulutukset, jotka sopivat paremmin tietylle yritykselle tai jopa erillisille ihmisryhmille. Tässäkin työssä analysoidaan yrityksille tehtyjä sähköpostitse toteutettuja tietojenkalastelutestejä ja pyritään saamaan selville, mitkä piirteet testeissä saivat käyttäjän vierailemaan sähköpostissa sisältämässä linkissä ja jopa antamaan mahdollisesti jotakin tietoja. (uSecure n.d..)

1.1 Opinnäytetyön tavoite

Tämän opinnäytetyön tavoitteena on tarjota kattava tietopaketti tietojenkalastelun monimuotoisesta maailmasta. Työssä käydään läpi erilaisia tietojenkalastelun tekniikoita, kuten sähköpostihuijauksia ja verkkosivujen kloonauksia. Työssä käsitellään myös näiden hyökkäysten mahdollisia seurauksia

niin yksilön kuin organisaationkin näkökulmasta, jotta voidaan ymmärtää niiden vaikutukset paremmin.

Ennen kaikkea työssä keskitytään kuitenkin siihen, miten tietojenkalastelulta voidaan suojautua ja mitä käytännön toimenpiteitä voidaan toteuttaa lisäämään tietoturvaa verkossa. Työn tarkoituksena on toimia oppaana niille, jotka haluavat parantaa tietoisuuttaan tietojenkalastelusta ja vahvistaa puolustustaan tämänkaltaisia hyökkäyksiä vastaan.

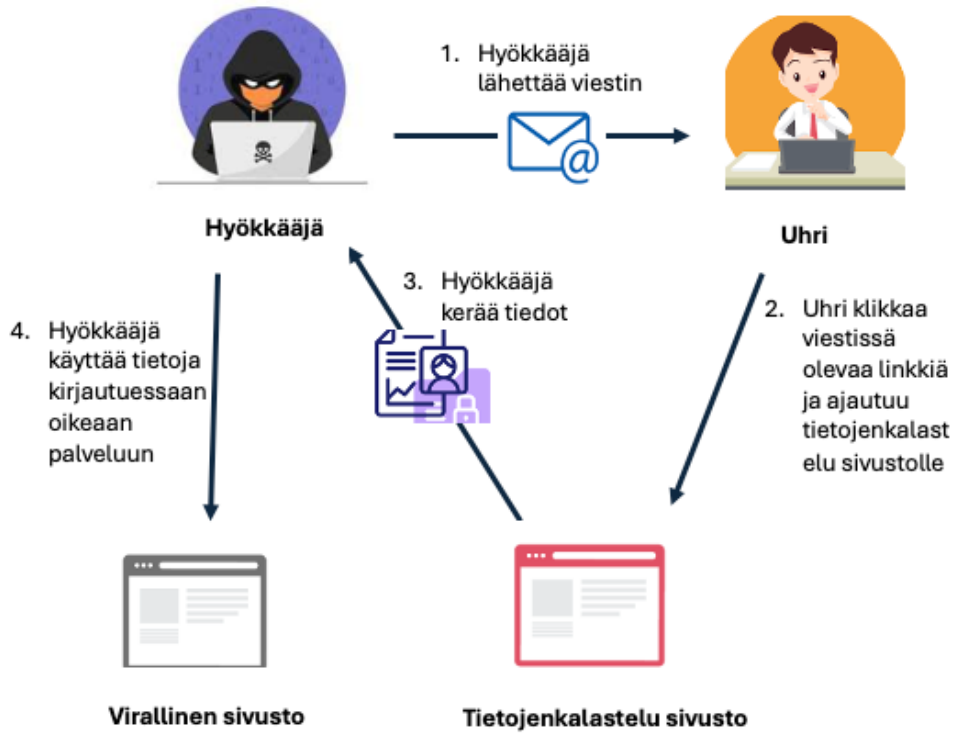
1.2 Opinnäytetyön rakenne

Ensin tässä työssä perehdytään yleisesti tietojenkalasteluun ja tarkastellaan tietojenkalastelun eri muotoja, jotka voivat vaihdella hienovaraisista sähköposteista ja verkkosivuista massiivisiin huijauksiin ja identiteettivarkauksiin. Seuraavaksi pureudutaan syvemmälle tietojenkalastelun vaikutuksiin, jotka voivat ulottua yksilön henkilökohtaisista tietovuodoista aina organisaatioiden laajamittaiseen tietoturvakriisiin. Kuitenkaan pelkä uhkien tunnistaminen ei riitä. Tämän työn keskeinen painopiste on myös tarjota käytännön ohjeita ja strategioita tietojenkalastelun torjumiseksi. Työn tavoitteena on opettaa lukija tunnistamaan huijaukset, suojaamaan henkilökohtaisia tietoja ja kehittämään hyviä tietoturvakäytäntöjä, jotka auttavat pysymään turvassa digitaalisessa maailmassa.

Opinnäytetyön kolmannessa luvussa tarkastellaan uSecuren uPhish -ohjelmalla luotuja tietojenkalastelutestejä oikeille yrityksille ja pyritään saamaan selville mitkä piirteet viesteissä ovat saaneet kohdehenkilön luottamaan testissä luotuun sisältöön ja vierailemaan viestien sisältämässä linkissä ja jopa antamaan henkilökohtaisia tietoja. Lopuksi työ sisältää johtopäätökset, joka sisältää yhteenvedon työstä ja työn havannoista. Tässä osiossa peilataan simulaatioissa ja koulutustilanteissa saatuja tuloksia työn teoriaan.

2 TIETOJENKALASTELU

Tietojenkalastelu eli phishing tarkoittaa tilannetta, jossa kyberhyökkääjä yrittää huijata käyttäjän avaamaan haitallisen linkin tai sähköpostiliitteen naamioimalla ne kiinnostavaksi sisällöksi. Kuvassa 2 on esitetty tyypillinen tietojenkalasteluhyökkäyksen toiminta malli. Tällaisten hyökkäysten tarkoituksena on yksilön harhauttaminen luottamuksellisen tai henkilökohtaisen tiedon paljastamista varten petollisiin tarkoituksiin. (F-Secure, n.d. a.) Tällaisten hyökkäysten havaitseminen ja niiden torjuminen on haastavaa niiden hyödyntämän ihmiskäyttäytymisen vuoksi (Kaushalya ja muut, 2018).



Kuva 2. Tietojenkalasteluhyökkäyksen toimintaperiaate

Verkostojen ja turvallisuustoimenpiteiden kehitys saa kyberrikolliset turvautumaan yhä enemmän sosiaaliseen manipulointiin ohittaakseen tekniset suojaukset ja hyödyntääkseen haavoittuvia käyttäjiä (Alharthi & Regan, 2020). Tutkimukset

ovat yhtä mieltä siitä, että sisäiset käyttäjät, erityisesti työntekijät, ovat suurin uhka yrityksille tahattomasti tartuttamalla järjestelmiä toimillaan, kuten epäilyttävien verkkosivustojen selaamisella tai tartunnan saaneiden tiedostojen lataamisella (Al-Mohannadi ja muut, 2018; Kaushalya ja muut, 2018).

2.1 Tietojenkalastelun historia ja kehitys

Tietojenkalastelu ei ole uusi ilmiö, vaan pikemminkin nykyaikainen mukautus vanhaan huijaus- ja petostekniikkaan. Termin "tietojenkalastelu" keksivät 1990-luvun puolivälissä hakkerit, jotka käyttivät sähköpostin väärentämistä ja sosiaalista manipulointia varastaakseen salasanoja ja pääsykoodeja online-käyttäjiltä, erityisesti America Onlinen (AOL), tuolloin suositun Internet-palveluntarjoajan, käyttäjiltä. Termi johdettiin sanasta "kalastus", koska hakkerit "kalastivat" uhreja lähettämällä heille syöttisähköposteja. (Whitty, 2018.)

Siitä lähtien tietojenkalastelu on kehittynyt ja monipuolistunut hienostuneisuuden, mittakaavan ja kohteiden suhteen. Tietojenkalasteluhyökkäyksistä on tullut realistisempia ja vakuuttavampia. Niissä käytetään kehittyneitä tekniikoita, kuten verkkotunnuksen väärentämistä, verkkosivustojen kloonausta ja haittaohjelmia luomaan väärennettyjä verkkosivustoja ja sähköposteja, jotka jäljittelevät aitojen verkkosivustojen ja sähköpostien ulkoasua. Myös tietojenkalasteluhyökkäykset ovat yleistyneet ja laajentuneet; ne kohdistuvat yksityishenkilöiden lisäksi myös yrityksiin, hallituksiin ja muihin organisaatioihin eri sektoreilla ja toimialoilla. Tietojenkalasteluhyökkäysten tavoitteet ovat myös laajentuneet henkilökohtaisten ja taloudellisten tietojen varastamisesta tilien ja verkkojen vaarantamiseen, kiristysohjelmien ja muiden haittaohjelmien levittämiseen sekä vakoiluun ja sabotaasiin. (APWG, 2024.)

2.2 Syitä tietojenkalastelun yleisyyteen

Ei ole olemassa yhtä vastausta siihen, miksi tietojenkalastelu on niin yleistä, vaan pikemminkin yhdistelmä tekijöitä, jotka tekevät siitä houkuttelevan ja tehokkaan

tekniikan verkkorikollisille. Vivitecin (n.d) mukaan neljä yleisintä syytä sille, miksi tietojenkalasteluhyökkäykset ovat yleistyneet, ovat: lisääntynyt etätyöskentely, organisaation heikentynyt valvonta, tietojenkalastelumuotojen jatkuva kehitys ja edulliset kustannukset.

Viimeisen parin vuoden aikana huomattava osa organisaatioista on joutunut siirtymään etä-/hybridityömalleihin. Vaihto mahdollisti toiminnan jatkumisen keskeytyksettä, mutta hajallaan oleva työvoima ja mobiilipäätepisteet toivat omat haasteensa. Yksi suurimmista ongelmista oli haavoittuvuuksien näkyminen hakkereille, jotka käyttivät niitä nopeasti hyväkseen tietojenkalasteluhyökkäysten kautta. (Vivitec, n.d..)

Pyrkiessään pysymään pinnalla globaalin kriisin keskellä monet yritykset jättivät kyberturvallisuuden kokonaan huomioimatta. Kiire etätöihin tarkoitti sitä, että yritykset olivat huolissaan henkilöstönsä saamisesta toimintakuntoon ja unohtivat turvallisuuden tämän prosessin aikana. Tämä johti esimerkiksi riittämättömiin tietoturvatyökaluihin ja työntekijöiden koulutuksen puutteeseen. Ihmiset ovat tottuneet työskentelemään henkilökohtaisilla laitteillaan suojaamattomissa verkoissa. Tällaiset virheet avasivat oven kyberrikollisille. (Spector, 2022.)

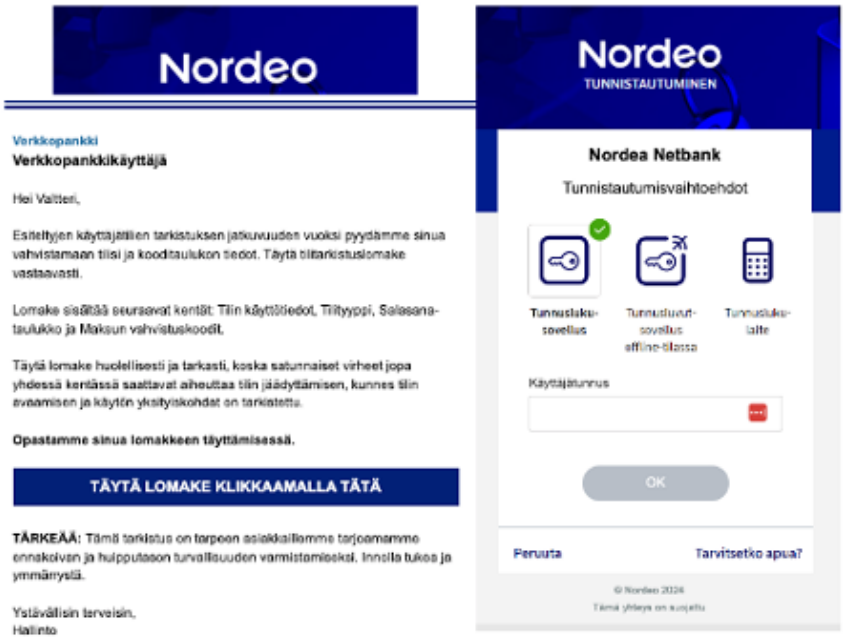
Kyberrikolliset pyrkivät jatkuvasti paljastamaan ja hyödyntämään yrityksien pienimpiäkin puutteita. Tämän lisäksi pimeässä verkossa on saatavilla useita edullisia tietojenkalastelutyökaluja, joiden avulla jopa ei-tekniset ihmiset voivat ryhtyä toteuttamaan erilaisia tietojenkalasteluhyökkäyksiä. Käytännössä jokainen, joka osaa luoda sähköpostiviestin voi toteuttaa tietojenkalasteluhyökkäyksiä vain arpomalla vastaanottajan osoitteen. (Vivitec, n.d..)

2.3 Tietojenkalastelun muodot

Puhuttaessa tietojenkalastelusta tarkoitetaan yleensä sähköpostipohjaisia hyökkäyksiä, joissa rikolliset käyttävät erilaisia tekniikoita harhauttaakseen käyttäjiä uskomaan viestin olevan peräisin luotettavalta lähteeltä, kuten esimerkiksi pankilta,

viranomaisilta tai vaikka työkaverilta. Tyypillisesti tietojenkalastelulla pyritään saamaan haltuun arkaluonteisia tietoja, kuten käyttäjätunnukset, salasanat ja luottokorttitiedot. (Bhardwaj ja muut, 2020.)

Tietojenkalasteluhyökkäykset ovat muuttuneet monimutkaisemmiksi, ja kyberrikolliset käyttävät vuosi vuodelta kehittyneempiä tekniikoita luodakseen väärennettyjä, mutta luotettavien verkkosivustojen näköisiä sivustoja ja vakuuttavia sähköposteja. Kalasteluviesteissä on usein logoja ja grafiikkaa arvostetuista yrityksistä, mikä tekee niistä aidon näköisiä (katso kuva 3). Prosessi sisältää yleensä linkin, joka ohjaa uhrin väärennetylle verkkosivustolle, jossa häntä pyydetään antamaan henkilökohtaisia tietoja. (Vayansky & Kumar, 2018.)



Kuva 3. Esimerkki tietojenkalastelusähköpostista

Tietojenkalasteluviestin pystyy tunnistamaan hyvin sen sisällöstä. Tällaiset viestit saattavat usein sisältää kirjoitusvirheitä tai niiden ulkoasu voi vaikuttaa epäilyttävältä, mikä voi johtua esimerkiksi automaattisesta käännöksestä. Virallisilta ja luotettavilta tahoilta saaduissa viesteissä yleensä pyritään välttämään

kirjoitusvirheitä ja noudattamaan brändin visuaalista tyyliä, joten nämä poikkeamat voivat viitata huijaukseen. Usein tällaiset huijausviestit voidaan tunnistaa jo niiden otsikoista tai epäilyttävästä lähettäjän sähköpostiosoitteesta. (Elisa, 2021.)

Vaikka monet osaavatkin jo tunnistaa epäilyttävät tietojenkalasteluyritykset sähköpostitse sekä huijaukseen käytettävät verkkosivut, eivät ne ole ainoat tietojenkalastelun muodot. Yleisiä tietojenkalastelun muotoja ovat muun muassa kohdennettu tietojenkalastelu eli spear phishing, tekstiviestitse tapahtuva smishing ja puhelimitse tapahtuva vishing. (F-Secure, n.d. a.)

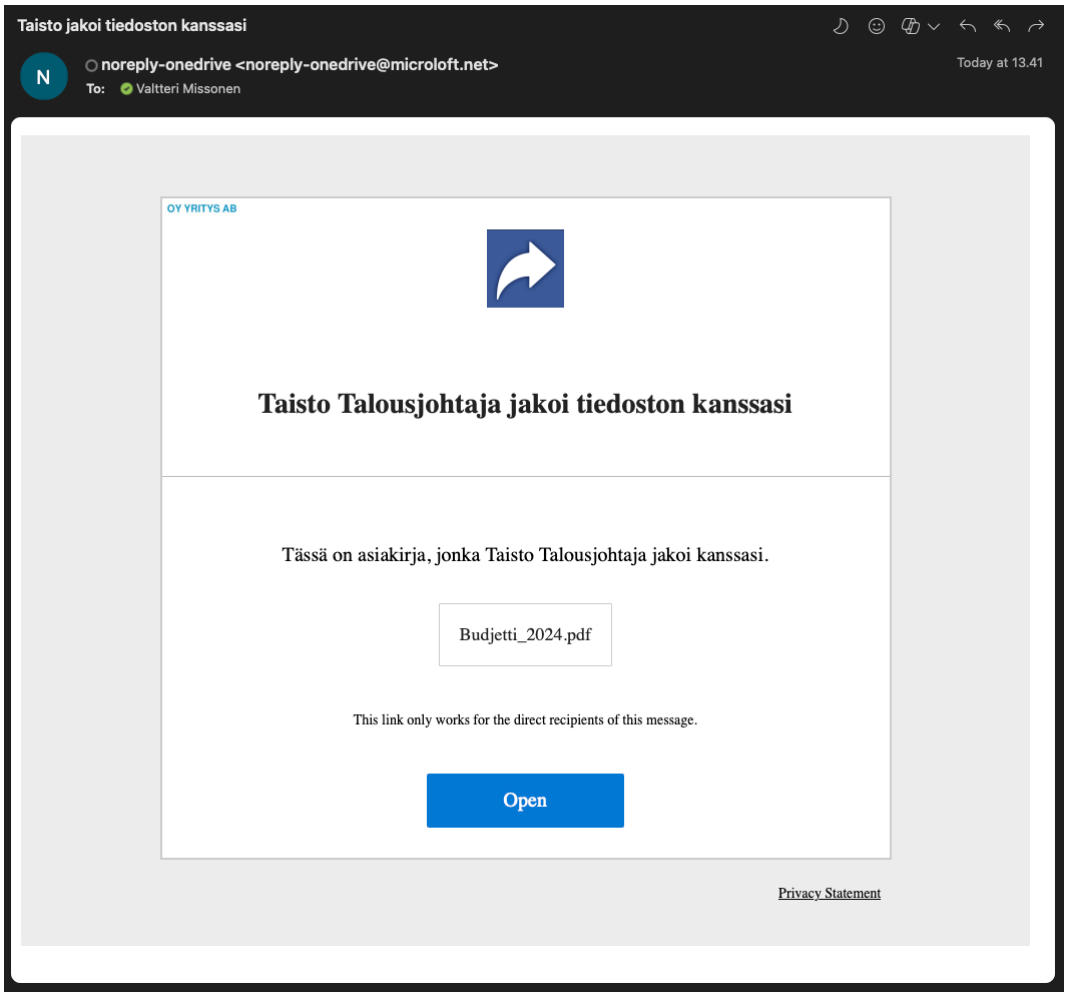
2.3.1 Kohdennettu tietojenkalastelu

Kohdennettu tietojenkalastelu eli spear phishing on edistyksellisempi ja hienovaraisempi muoto tietojenkalastelusta, joka perustuu tarkkaan kohdistamiseen ja yksilölliseen lähestymistapaan. Tässä hyökkäystavassa hyökkääjät investoivat aikaa ja vaivaa tutkiakseen potentiaalisia uhrejaan syvällisesti ennen hyökkäystä. Tämä perusteellinen tutkimus mahdollistaa sen, että hyökkääjät voivat kustomoida huijausviestinsä ja muut toimensa niin, että ne vaikuttavat mahdollisimman aidoilta ja houkuttelevilta uhreille. (Vayansky & Kumar, 2018.) Kuvassa 4 on esitetty esimerkki tällaisesta kohdennetusta hyökkäysviestistä.

Tämäntyyppinen hyökkäys vaatii yleensä useita vaiheita ja huolellista suunnittelua. Aluksi hyökkääjien on kerättävä tietoja uhreistaan eri lähteistä, kuten sosiaalisen median profiileista, verkkosivuilta ja julkisista tietokannoista. Tämän jälkeen he voivat käyttää tätä tietoa luodakseen houkuttelevia huijausviestejä tai muita huijausviestintävälineitä, jotka saavat uhrit luottamaan ja reagoimaan vastaanotettuun viestiin. (Fortinet, n.d..)

Kohdennetun tietojenkalasteluhyökkäyksen kohteena olevat tiedot voivat vaihdella tilitiedoista ja salasanoista henkilökohtaisiin tai yrityssalaisuuksiin, ja sen seurauksena hyökkäykset voivat aiheuttaa laajoja taloudellisia vahinkoja ja

henkilökohtaisia haittoja uhreille. Tämän vuoksi on äärimmäisen tärkeää, että yksilöt ja organisaatiot ovat tietoisia tästä uhasta ja toteuttavat asianmukaiset suojatoimenpiteet tietoturvansa vahvistamiseksi ja suojaamiseksi. (Fortinet, n.d..)



Kuva 4. Esimerkki kohdennetusta tietojenkalastelusta

2.3.2 Valastelu

Valastelu eli whaling on tietojenkalastelun muoto, jota kutsutaan myös toimitusjohtajapetokseksi. Valastelu on kohdennettu hyökkäys, jossa hyödynnetään sosiaalisen manipuloinnin tekniikoita korkean tason johtohenkilöiden harhauttamiseksi, jotta he paljastaisivat arkaluonteisia tietoja tai suorittaisivat luvattomia liiketoimia. Valasteluhyökkäykset toteutetaan yleensä sähköpostitse, jossa

verkkorikolliset luovat viestejä, jotka näyttävät tulevan luotettavalta lähteeltä, kuten toimitusjohtajalta tai talousjohtajalta. Sähköpostiviestit sisältävät usein kiireellisiä tilisiirtopyyntöjä tai ohjeita, jotka vaativat välitöntä toimintaa, kuten varojen siirtämistä tai arkaluonteisten tietojen jakamista. (Kaspersky, n.d. a.)

Kohdennettu tietojenkalasteluhyökkäys ja valasteluhyökkäys eroavat toisistaan siten, että valastelussa kohteena on yleensä vain yksi henkilö. Tämä henkilö on korkean profiilin toimija organisaatiossa, josta löytyy verkosta paljon tietoa, jota voidaan käyttää häntä vastaan, esimerkiksi yrityksen toimitusjohtaja. Kohdennetun tietojenkalasteluhyökkäyksen kohteena voi olla kuka tahansa organisaatiossa toimiva henkilö, joka täyttää tekijän kriteerit. Kohde voi olla esimerkiksi kuka tahansa, jolla on pääsy yrityksen sisäisiin tietoihin. (Trustpair, 2023.)

2.3.3 Tekstiviestihuijaus

Tekstiviestihuijaus eli smishing on tietojenkalastelun muoto, jossa käytetään nimensä mukaisesti tekstiviestejä huijaamaan ihmisiä luovuttamaan henkilökohtaisia tai taloudellisia tietojaan. Termi on tekstiviestien (SMS) ja tietojenkalastelun (phishing) yhdistelmä. Tekstiviestihuijaus on kasvava uhka, kun yhä useammat ihmiset käyttävät mobiililaitteitaan verkkotapahtumiin. Smishing-viestit näyttävät usein tulevan laillisista lähteistä, kuten pankeista, valtion virastoista tai verkkopalveluista, ja ne sisältävät yleensä kiireellisyyden tunteen tai palkkion, joka houkuttelee vastaanottajia napsauttamaan linkkiä, soittamaan numeroon tai vastaamaan tiedoillaan. Nämä linkit tai numerot voivat kuitenkin johtaa haitallisiin verkkosivustoihin tai puhelinlinjoihin, jotka voivat varastaa käyttäjän tietoja, asentaa haittaohjelmia tai veloittaa maksuja. (Norton, 2024a.) Kuvassa 5 on esimerkki tekstiviestihuijauksesta, joka on lähetetty Postin nimissä.

Kuva 5. Esimerkki tekstiviestihuijauksesta

Tekstiviestihuijauksen voi tunnistaa useista merkeistä. Yksi tärkeimmistä on epäilyttävä lähettäjän numero tai nimi. Jos viesti tulee tuntemattomalta tai epäilyttävältä lähettäjältä ja sisältää pyyntöjä jakaa henkilökohtaisia tietoja, kuten pankkitietoja tai salasanoja, on syytä olla varovainen. Lisäksi huijauksissa usein luvataan liian hyvältä kuulostavia tarjouksia tai vaaditaan nopeaa toimintaa kiireellisen tilanteen luomiseksi. On myös tarkkailtava viestin kieltä ja kielivirheitä sekä epäilyttäviä linkkejä. Niitä ei koskaan kannata klikata, jos on epävarma viestin luotettavuudesta. Jos epäilee viestin aitoutta, on aina turvallisinta varmistaa asia suoraan henkilöltä tai organisaatiolta sen virallisilta verkkosivuilta tai asiakaspalvelusta ennen toimimista. Lisäksi voi raportoida epäilyttävistä viesteistä operaattorille tai viranomaisille niiden selvittämiseksi ja muiden madollisien huijauksien estämiseksi. (F-Secure, n.d. b.)

2.3.4 Äänikalastelu

Äänikalastelu eli vishing edustaa perinteisen kalastelun kehittynyttä muotoa, jossa hyödynnetään äänipohjaista viestintää yksilöiden harhauttamiseksi ja luvattoman pääsyn saamiseksi sensitiivisiin tietoihin tai taloudellisiin varoihin (Securityweek,

2020). Äänikalastelussa hyökkääjä toimii eri kanavien, kuten puhelinsoittojen, ääniviestien ja VoIP-palvelujen kautta esiintyen laillisena toimiana, kuten pankkina, viranomaisena tai teknisen tuen henkilöstönä. Hyökkääjät käyttävät sosiaalisen manipulaation taktiikoita saadakseen uhrin paljastamaan luottamuksellista tietoa, kuten tilitunnuksia, henkilöllisyystunnisteita tai luottokorttitietoja kiireellisen tilanteen tai houkuttelevien tarjousten varjolla. Automaattisten äänijärjestelmien käyttö tai luotettavana viranomaisena esiintyminen lisää uskottavuutta tehostaen näin äänihyökkäystä (F-Secure, n.d. c.)

Äänikalaseteluhuijauksen tunnusmerkit ovat kiire ja pelottelutaktiikat, yllättävät puhelut ilman odotusta, pyynnöt arkaluontoisten tietojen vahvistamiseksi puhelimitse, kuten sosiaaliturvatunnukset tai pankkitilin tiedot ja huono äänenlaatu tai taustamelu. Virastoista tai yrityksistä ei koskaan pyydetä tällaisia tietoja yllättäen puhelimitse, ja jos epäilys herää, paras toiminta on tarkistaa soittajan todellisuus virallisten yhteystietojen avulla ennen kuin jakaa mitään henkilökohtaisia tai taloudellisia tietoja. (Norton, 2024b.)

2.3.5 Deepfake

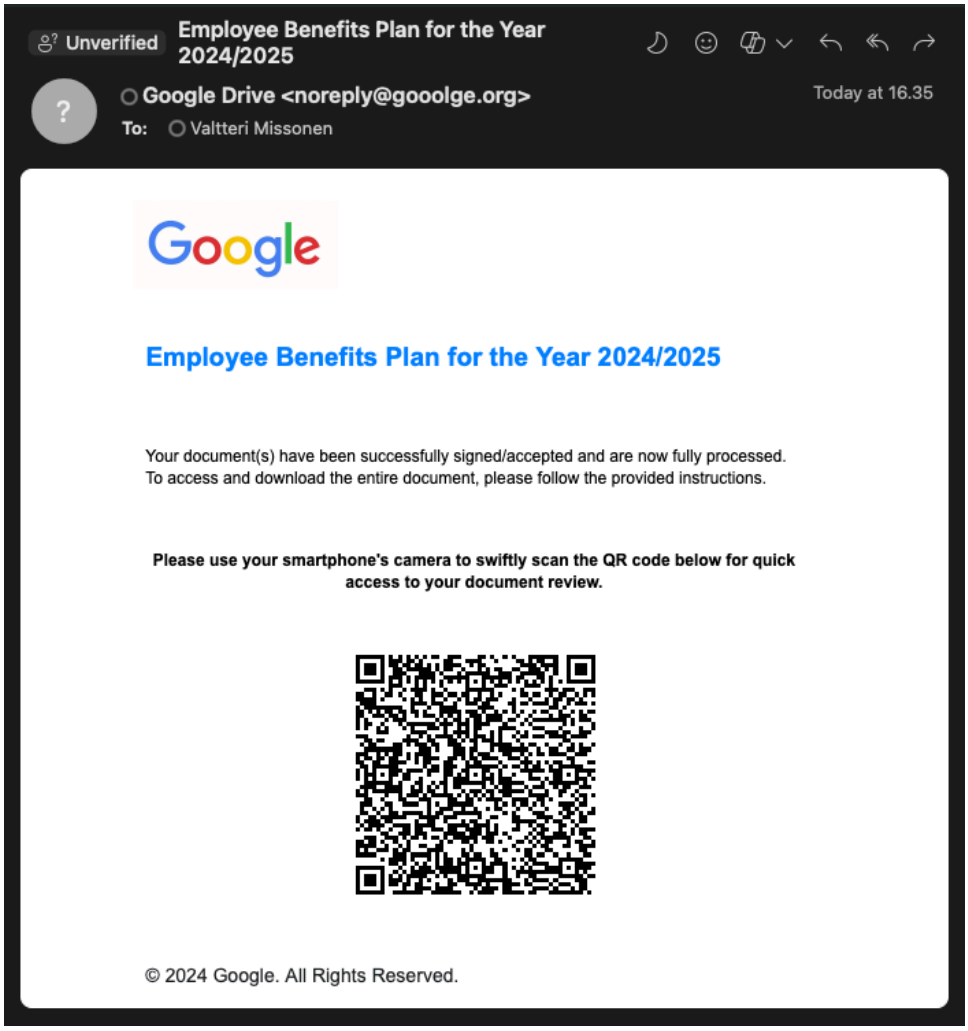
Tekoäly tuo kyberrikollisuuden markkinoille uudenlaiset huijaustyypit. Yksi nopeiten lisääntyvistä tietojenkalastelun muodoista ovat ns. deepfake-huijaukset. Deepfake-teknologia luo aidolta vaikuttavaa ääni-, kuva- ja videomateriaalia halutusta henkilöstä. Materiaali tuotetaan yhdistämällä tai muuttamalla olemassa olevaa materiaalia koneoppivan tekoälyn avulla. Se on suunniteltu saamaan vastaanottajan uskomaan, että materiaali esittää todellisia tapahtumia tai henkilöitä, vaikka näin ei ole. (TBOIJ, 2024.)

Näitä tekniikoita käytetään usein manipuloimaan tai vääristämään sisältöä, jolloin henkilöt voivat vaikuttaa sanovan tai tekevän jotain, mitä he eivät todellisuudessa ole sanoneet tai tehneet. Deepfake-huijaukset voivat olla erityisen vaarallisia, koska ne voivat levitä nopeasti ja aiheuttaa vahinkoa henkilöiden maineelle, levittäessään väärää tietoa tai vääristeltyä sisältöä. (TBOIJ, 2024.)

2.3.6 QR-koodi

Toinen nopeasti yleistyvä tietojenkalastelun muoto on QR-koodien avulla tehtävät tietojenkalastelu huijaukset. QR-koodien käyttö kasvoi merkittävästi koronapandemian aikana, kun monet ravintolat ja yritykset ottivat ne käyttöön kontaktien vähentämiseksi. Tämän seurauksena myös QR-koodien väärinkäyttö huijauksissa yleistyi. QR-koodien avulla toteutettavassa tietojenkalastelussa, jota kutsutaan myös quishingiksi, houkutellaan käyttäjiä skannaamaan QR-koodi älypuhelimella tai tabletilla. QR-koodien skannaus on helppoa, koska lähes kaikissa älypuhelimissa ja tableteissa on sisäänrakennettu kamera, joka pystyy lukemaan QR-koodeja. (Kyberturvallisuuskeskus, 2023.)

QR-koodikalastelussa hyökkääjät lähettävät harhaanjohtavia sähköposteja, jotka muistuttavat aitoja markkinointiviestejä usein luotettavilta tahoilta, kuten rahoituslaitoksilta, ja kehottavat vastaanottajia toimimaan välittömästi. Näissä sähköposteissa on QR-koodeja (katso kuva 6), jotka johtavat huijaukseen tarkoitettuihin verkkosivustoihin, joilla pyydetään arkaluonteisia tietoja tai käynnistetään haittaohjelman lataaminen. Vaikka sähköpostikalastelun tunnistamisesta ja raportoinnista on paljon tietoa ja koulutusta, QR-koodien kalastelu on suhteellisen vähän tunnettu ilmiö, mikä tekee siitä houkuttelevan vaihtoehdon kyberrikollisille, koska QR-koodeja käytetään laajasti myös eri julkisissa tiloissa, kuten sanomalehdissä, aikakauslehdissä ja mainoksissa. (TechTarget, 2024.)



Kuva 6. Esimerkki QR-koodi huijauksesta

On ensisijaisen tärkeää olla varovainen QR-koodeja skannatessaan, erityisesti jos ne ovat peräisin epäilyttävistä lähteistä. QR-koodeja tulisi käsitellä samalla tavalla kuin hyperlinkkejä, sillä ne voivat johtaa käyttäjän huijaussivustoille tai muihin vaarallisiin kohteisiin. Ennen QR-koodin skannaamista on viisasta arvioida viestin aitous ja harkita, onko QR-koodi todella odotettu tai tarpeellinen. Erityisesti jos QR-koodi on saapunut tekstiviestillä tai sosiaalisen median kautta, on suositeltavaa vahvistaa sen lähde. Tämä voidaan tehdä suoraan yhteydenoton avulla lähettäjään esimerkiksi puhelimitse tai muulla viestintävälineellä. (Kyberturvallisuuskeskus, 2023.)

2.4 Tietojenkalasteluhyökkäyksen vaikutukset

Kuten muillakin rikollisilla toiminnoilla, myös tietojenkalasteluhyökkäyksillä on onnistuessaan erilaisia seurauksia ja vaikutuksia. Onnistunut hyökkäys voi aiheuttaa merkittäviä taloudellisia menetyksiä, toiminnallisia häiriöitä ja mainevahinkoja yrityksille ja yksityishenkilöille.

2.4.1 Taloudelliset menetykset

Tietojenkalastelun aiheuttamat taloudelliset menetykset voivat olla suoria ja välillisiä. Suorat menetykset ilmenevät usein siten, että hyökkääjät käyttävät varastettuja tietoja tehdäkseen haitallisia ostoksia tai muuta taloudellista toimintaa. Tämä voi myös aiheuttaa yritykselle suuria rahallisia menetyksiä, kun se joutuu korvaamaan petoksista kärsineiden asiakkaiden menetykset. (CybSafe, 2023.)

Välilliset taloudelliset menetykset voivat olla vieläkin haitallisempia. Yrityksen tai jopa yksityishenkilön on käytettävä resurssejaan tutkintoihin, vahinkojen korjaamiseen ja tietoturvatoimenpiteisiin. Näihin kuuluvat muun muassa tietoturvajärjestelmien päivitykset, henkilöstön koulutus tietojenkalastelun tunnistamiseksi ja välttämiseksi sekä mahdollisesti oikeudelliset kustannukset, jos tietoturvaloukkauksen seurauksena tulee oikeusjuttuja. (CybSafe, 2023.)

2.4.2 Toiminnalliset häiriöt

Kun epäillään tietojenkalasteluhyökkäystä tai sellainen havaitaan, yrityksen on usein reagoitava nopeasti ja suljettava järjestelmiään väliaikaisesti. Tämän toimenpiteen tarkoituksena on estää mahdollisia lisävahinkoja ja suojella arkaluonteisia tietoja. Valitettavasti tämä toimenpide voi johtaa liiketoiminnan keskeytymiseen, kun tärkeitä järjestelmiä ei voida käyttää normaalisti. Liiketoiminnan keskeytyminen voi aiheuttaa merkittävää tuottavuuden laskua ja häiritä normaaleja toimintoja, mikä puolestaan voi johtaa asiakkaiden menetyksiin ja taloudellisiin tappioihin. (Wallarm, n.d..)

Lisäksi on tärkeää huomata, että onnistunut tietojenkalasteluhyökkäys voi antaa hyökkääjälle mahdollisuuden sulkea yrityksen järjestelmiä. Tämä voi olla erityisen haitallista, koska se voi pidentää liiketoiminnan keskeytymistä ja vaikeuttaa normaalin toiminnan palauttamista. Hyökkääjä voi esimerkiksi vaatia lunnaita tietojen ja toimintojen vapauttamiseksi tai yksinkertaisesti haluta aiheuttaa tuhoa ja häiriöitä yritykselle. (Wallarm, n.d..)

2.4.3 Mainevahingot

Tietojenkalasteluhyökkäysten aiheuttamat taloudelliset menetykset ovat selkeitä, mutta yhtä tuhoisa vaikutus on mainevahingoilla, joista on puhuttu vähemmän. Tietojenkalasteluhyökkäykset voivat horjuttaa organisaation mainetta ja luottamusta, mikä voi johtaa pitkäaikaisiin seurauksiin. (Stage2Data, n.d..)

Ensinnäkin tietojenkalasteluhyökkäyksen paljastuminen voi aiheuttaa luottamuksen menetyksen asiakkaiden ja sidosryhmien keskuudessa. Kun asiakkaat kokevat, että heidän henkilötietonsa tai taloudelliset tietonsa ovat vaarassa, he saattavat menettää luottamuksensa yritykseen. Tämä voi johtaa asiakkaiden menetyksiin ja vaikeuttaa uusien asiakkaiden hankkimista tulevaisuudessa. Lisäksi sidosryhmät, kuten sijoittajat ja yhteistyökumppanit, saattavat menettää luottamuksensa organisaatioon, mikä voi vaikuttaa negatiivisesti yrityksen maineeseen ja pitkän aikavälin menestykseen. (Infosec, 2020.)

Toiseksi tietojenkalasteluhyökkäyksen paljastuminen voi aiheuttaa mainehaittaa, joka voi levitä laajalle ja vaikuttaa organisaation brändiin ja uskottavuuteen. Kun tietovuoto saa laajaa julkisuutta mediassa tai sosiaalisessa mediassa, voi se aiheuttaa vakavia vaurioita organisaation maineelle. Asiakkaat ja yleisö voivat pitää organisaatiota huolimattomana tai epäluotettavana tietoturvansa suhteen, mikä voi vaikuttaa negatiivisesti organisaation brändiin ja tuotteiden tai palveluiden myyntiin. Lisäksi organisaatio voi joutua käyttämään merkittäviä resursseja maineen palauttamiseen ja vahinkojen korjaamiseen, mikä voi aiheuttaa lisää taloudellisia menetyksiä ja hidastaa liiketoiminnan kasvua. (Infosec, 2020.)

2.5 Tietojenkalasteluhyökkäyksen kohteeksi joutuminen

Tietojenkalasteluhyökkäyksen jälkeen uhrit saattavat ihmetellä, mitä toimenpiteitä tulisi toteuttaa, kun on joutunut tällaisen hyökkäyksen kohteeksi. On olemassa useita toimenpiteitä, joita voidaan tehdä, jotta voidaan lievittää hyökkäyksen aiheuttamia vahinkoja, estää muiden ihmisten joutumisen samanlaisen huijauksen uhreiksi ja jopa suojata uhri tulevilta hyökkäyksiltä.

Ensimmäinen askel on ymmärtää, miten hyökkäys tapahtui. Tämä voi edellyttää tutkimusta, kuten saapuneen tietojenkalastelusähköpostin tai muun viestin tarkastelua, mahdollisesti epäilyttävien URL-osoitteiden tai IP-osoitteiden tarkistamista erilaisista lokitiedostoista sekä sen selvittämistä tarkasti, mitä tietoja ja yksityiskohtia saattaa olla vaarassa. On myös suositeltavaa tarkistaa kaikki tilit, jotka saattavat olla yhteydessä varastettuihin tietoihin mahdollisen epäilyttävän toiminnan varalta. (Kaspersky, n.d. b.)

Toinen askel on katkaista hyökkäyksen kohteeksi joutuneen laitteen yhteys Internetiin. Joissakin tapauksissa hyökkäykset voivat liittyä haittaohjelmiin, joten laitteen yhteys on katkaistava välittömästi (OnSecurity, 2020).

Kolmas vaihe on vaihtaa kaikki mahdollisesti vaarantuneet salasanat ja suorittaa haittaohjelmien skannaus laitteelle. Hyökkäyksen tavoitteena on usein manipuloida uhreja antamaan arkaluontoisia tietoja, joten salasanojen vaihtaminen on välttämätöntä. Haittaohjelmien skannaus auttaa havaitsemaan ja poistamaan mahdolliset haittaohjelmat laitteelta. On myös tarkistettava, että käytössä on kaksivaiheinen todennus. Se lisää ylimääräisen turva-askeleen vaatien toisen todennusmuodon, kuten sormenjäljen tai kertakäyttöisen salasanan. Kaksivaiheinen todennus tekee kyberrikollisille vaikeammaksi pääsyn tilille, vaikka heillä olisikin kirjautumistiedoti. (Proofpoint, 2023.)

Seuraavaksi on tärkeää ottaa yhteyttä mahdollisesti osallisena olleeseen yritykseen ja mahdollisesti myös ilmoittaa hyökkäyksestä viranomaisille. Aidot yritykset

saattavat usein olla tietämättään mukana tietojenkalasteluhyökkäyksissä, joten on tärkeää ilmoittaa tapahtuneesta yritykselle. Tällä tavoin yritys voi ryhtyä toimenpiteisiin tulevien hyökkäysten estämiseksi ja varoittaa asiakkaitaan huijauksista (Kaspersky, n.d. b).

Lopuksi uhrien tulisi olla valppaina mahdollisten identiteettivarkauksien varalta. Jotkut hyökkäykset pyrkivät varastamaan henkilökohtaisia tietoja, jotta hyökkääjä voi ryhtyä identiteettivarkauksiin. Uhrien tulisi tarkkailla epäilyttäviä taloudellisia tapahtumia ja muita merkkejä mahdollisesta identiteettivarkaudesta ja tarvittaessa tehdä asiasta ilmoitus asianmukaisille viranomaisille (Proofpoint, 2023).

2.6 Tietojenkalasteluhyökkäyksiltä suojautuminen

Aivan kuin multakin uhilta, niin myös tietojenkalasteluhyökkäyksiltä on mahdollista suojautua. Suojautumistoimenpiteitä voidaan kohdentaa käyttäjiin tai käytettävissä oleviin laitteisiin. Henkilöstöön kohdennettavia toimenpiteitä ovat esimerkiksi erilaiset tietoisuutta lisäävät koulutukset ja laitteistoon kohdistuvia ovat järjestelmien ja ohjelmien pitäminen päivitettyinä.

Käyttäjien tietoisuutta voidaan kasvattaa erilaisilla koulutuksilla. Ensimmäinen tärkeä suojautumisen aste on ymmärtää, mitä tietojenkalastelu on ja tunnistaa tällaiset hyökkäykset. Usein voi olla vaikeaa erottaa aito viesti ja kalasteluyritys. Siksi on tärkeää suhtautua jokaiseen sähköpostiin varovaisesti, erityisesti niihin, jotka sisältävät linkkejä, liitetiedostoja tai arkaluonteisten tietojen pyyntöjä. (Kaspersky, n.d. c.)

Tietojenkalasteluhyökkäyksiä voi olla vaikea havaita, koska niissä käytetään usein kehittyneitä tekniikoita jäljittelemään laillisten lähteiden ulkonäköä ja sävyä (Vayansky & Kumar, 2018). On kuitenkin joitakin merkkejä, jotka voivat auttaa tunnistamaan ja välttämään tietojenkalasteluhyökkäyksiä.

Ensimmäiseksi on tärkeää tarkistaa lähettäjän sähköpostiosoite. Tietokalasteluviesteissä käytetään yleensä väärennettyjä tai samannäköisiä osoitteita, jotka

yrittävät jäljitellä alkuperäistä lähdettä. Tietojenkalastelijat voivat esimerkiksi käyttää verkkotunnusta, jossa on korvattu jokin osoitteen merkeistä samankaltaisella merkillä tai lisätty ylimääräisiä merkkejä, kuten @gmai1.com tai @gooogle.com, niitä on hankala huomata kiireen keskellä. (Kaspersky, n.d. c.)

Toinen asia, johon on tärkeätä kiinnittää huomiota, on viestin sisältö. On hyvä miettiä, kuulostaako viesti lähettäjältä. Tietojenkalasteluviestit voivat sisältää kirjoitus- tai kielioppivirheitä, epämääräisiä tai persoonattomia tervehdyksiä ja epäjohdonmukaisia tai yhteensopimattomia logoja tai fontteja. Viesteissä käytetään usein kiireellistä tai uhkaavaa kieltä, kuten "Tilisi on jäädytetty" tai "Tunnuksiesi voimassa olo päättyy pian" painostamaan henkilöä toimimaan nopeasti ja ajattelematta. (F-Secure, n.d. a.)

Kolmas asia, johon on äärimmäisen tärkeää kiinnittää huomiota, ovat viestin sisältämät linkit ja liitteet. Tietojenkalastelusähköpostit tai -viestit voivat sisältää linkkejä tai liitteitä, jotka näyttävät johtavan aitoihin verkkosivustoihin tai asiakirjoihin, mutta todellisuudessa sisältävät haitallisia tiedostoja tai ohjaavat vastaanottajan haitallisille sivustoille. Ennen kuin napsauttaa linkkiä tai avaa liitteen, tulee viedä hiiren osoitin linkin päälle ja tarkistaa, vastaako URL-osoite tai tiedostonimi odotettua lähdettä. (McAfee, 2023.)

Viimeinen tärkeä vaihe on tarkistaa viestin sisältämä pyyntö. Tietojenkalasteluviesteissä saatetaan pyytää antamaan tai vahvistamaan henkilökohtaisia tai taloudellisia tietoja, kuten salasanoja, luottokorttinumeroita tai pankkitilitietoja. Lailliset lähteet eivät kuitenkaan koskaan pyydä tekemään niin sähköpostitse tai viestillä. Pyyntö on aina tarkistettava ottamalla yhteyttä lähteeseen suoraan toisen kanavan, kuten puhelimen tai virallisen verkkosivuston, kautta. (Kaspersky, n.d. c.)

Kun kohtaa epäilyttävän viestin postilaatikossa, on ensisijaisen tärkeää toimia välittömästi. Erityisesti jos kyseessä on kalasteluviesti, joka on lähetetty työsähköpostiin, on ratkaisevan tärkeää ilmoittaa siitä myös yrityksen IT-osastolle. Tällä toimenpiteellä varmistetaan, että organisaati pysyy ajan tasalla mahdollisista

tietojenkalasteluriskeistä ja osaa tarvittaessa suojautua niitä vastaan. Yhteistyö IT-osaston kanssa voi myös auttaa tunnistamaan samankaltaisia huijausyrityksiä tulevaisuudessa ja välttämään niitä tehokkaasti. (Norton, 2022.)

Lisäksi – oli kyse sitten työ- tai henkilökohtaisesta sähköpostista –, on suositeltavaa ilmoittaa mahdollisista tietojenkalasteluhuijauksista myös sähköpostipalveluntarjoajalle. Tämä voi olla ratkaiseva askel tietoturvallisuuden varmistamiseksi, sillä sähköpostipalveluntarjoajat voivat ottaa tarvittavat toimenpiteet huijausyrityksen torjumiseksi ja estää vastaavien viestien saapumisen muiden käyttäjien postilaatikoihin. Vaikka ilmoitusprosessi vaihtelee palveluntarjoajan mukaan, sen merkitys on korvaamaton turvallisuuden ja vastatoimien kannalta. (Kaspersky, n.d. c.)

Toinen keino, jonka avulla käyttäjä voi merkittävästi vähentää riskiä joutumasta tietojenkalastelun uhriksi, on huolehtia, että käytössä on vahvat salasanat ja monivaiheinen todennus (MFA). Nämä ovat kulmakiviä tietojenkalastelun torjunnassa nykyaikaisessa digitaalisessa maailmassa. Vahvat salasanat ovat ensisijainen puolustuslinja, joka estää hakkereita pääsemästä käyttäjätilien kimppuun. Kun salasana on riittävän pitkä ja monimutkainen, sen arvaaminen tai murtaminen on äärimmäisen vaikeaa. Tämä vähentää merkittävästi riskiä tietojenkalastelun onnistumiselle. Lisäksi monivaiheinen todennus tuo ylimääräisen turvakerroksen, joka vaatii käyttäjän todentamaan itsensä useamman kuin yhden tekijän avulla, kuten salasanan lisäksi esimerkiksi tekstiviestin tai mobiilisovelluksen kautta lähetetyn koodin. Tämä vaikeuttaa huomattavasti hakkereiden pääsyä käyttäjätilille, vaikka he saisivatkin haltuunsa salasanan. Yhdessä vahva salasana ja monivaiheinen todennus muodostavat tehokkaan suojan tietojenkalastelua vastaan, suojaavat käyttäjien tietoja ja parantavat merkittävästi tietoturvaa verkossa. (Norton, 2022.)

Käyttäjien tietoisuuden lisäämisen lisäksi on tärkeää myös tärkeää tehdä suojaustoimia käytössä oleviin laitteisiin. Tällaisia keinoja ovat esimerkiksi koneelle

asennettavat haittaohjelmien torjuntaohjelmat ja laitteiden sekä sovellusten pitäminen päivitettyinä.

Haittaohjelmien torjuntaohjelmisto on olennainen puolustusväline monenlaisten kyberuhkien torjunnassa. Se on suunniteltu tunnistamaan ja neutraloimaan hienovaraisetkin haittaohjelmat, tarjoten jatkuvasti päivittyvän suojan viruksia, troijalaisia ja muita uhkia vastaan. Yhdistämällä palomuurin, roskapostin suodatuksen ja haittaohjelmien torjunnan yhteen pakettiin, käyttäjä voi tarjota lisäsuojaa järjestelmälleen ja estää vahingossa klikattujen vaarallisten linkkien aiheuttamia uhkia. Näiden integroitujen ratkaisujen avulla käyttäjä voi vahvistaa tietoturvaansa ja suojata laitteistonsa kalasteluyrityksiltä ja muilta haittaohjelmilta, mikä tarjoaa mielenrauhaa jatkuvasti muuttuvassa digitaalisessa maisemassa. (Kaspersky, n.d. c.)

Lisäksi laitteiden ja sovellusten päivitykset ovat korvaamaton osa tietoturvan ylläpitämistä tänä päivänä, erityisesti suojautumisessa tietojenkalastelua vastaan. Päivitettyjen järjestelmien turvapäivitykset tukkivat haavoittuvuuksia toimien digitaalisina kilpinä, jotka estävät haitallisten hyökkäysten pääsyn järjestelmiin. Lisäksi päivitykset tarjoavat käyttäjille lisäominaisuuksia ja parannuksia, jotka auttavat tunnistamaan ja torjumaan tietojenkalasteluyrityksiä, kuten haitallisia verkkosivustoja ja epäilyttäviä linkkejä. Tämä edistää aktiivista tietoturvakulttuuria ja käyttäjien tietoisuutta digitaalisista uhista. Näin ollen päivitysten säännöllinen suorittaminen on olennaista tietoturvan varmistamiseksi ja tietojenkalastelun torjumiseksi tehokkaasti. (Norton, 2022.)

Aktiivinen osallistuminen epäilyttävien viestien havaitsemiseen ja ilmoittamiseen on ratkaisevan tärkeää digitaalisen turvallisuuden kannalta. Lisäksi on olennaista pitää laitteet ja sovellukset päivitettyinä sekä hyödyntää haittaohjelmien torjuntaohjelmaa, jotta varmistetaan vahva suojautuminen haitallisia uhkia vastaan. Näiden toimenpiteiden yhdistäminen luo vankan puolustuksen digitaalista turvallisuutta uhkaavia riskejä vastaan.

3 TIETOJENKALASTELUSIMULAATIOT

Kuten aiemmin mainittiin, niin yksi tehokas tapa täydentää yksilön tietoisuutta kyberuhkista on simuloidut tietojenkalasteluhyökkäykset, jotka yrityksen IT-osasto tai vastaava palveluntarjoajan toteuttavat. Nämä simuloidut hyökkäykset ovat todellisia tilanteita jäljitteleviä skenaarioita, joissa pyritään testaamaan organisaation valmiutta ja reagointikykyä tietojenkalasteluyrityksiin.

Tietojenkalastelutestaus tarjoaa yrityksille arvokkaan mahdollisuuden arvioida niiden haavoittuvuutta tietojenkalasteluhyökkäyksille. Tämä tapahtuu simuloiduissa ympäristöissä, jotka pyrkivät jäljittelemään todellisia tietojenkalastelutilanteita mahdollisimman tarkasti.

Lisäksi tietojenkalastelutestaus auttaa organisaation henkilöstöä tunnistamaan tietojenkalastelun merkit ja reagoimaan niihin asianmukaisesti. Simuloidut hyökkäykset tarjoavat käytännön harjoittelutilaisuuksia, joissa henkilöstö voi oppia tunnistamaan epäilyttäviä viestejä, linkkejä tai liitetiedostoja ja oppia, miten toimia, jos he epäilevät joutuneensa tietojenkalasteluyrityksen kohteeksi.

3.1 Tietojenkalastelutestien tavoitteet

Testien päätavoite on arvioida organisaatioiden valmiutta tunnistaa ja torjua tietojenkalasteluhyökkäyksiä. Tietojenkalastelutestauksen avulla pyritään löytämään mahdollisia haavoittuvuuksia organisaatioiden tietoturvaprosesseissa ja -järjestelmissä, jotka voisivat altistaa ne tietojenkalastelulle. Tämä voi sisältää esimerkiksi heikkouksia sähköpostijärjestelmissä, käyttäjien tietoisuuden puutteita tietojenkalastelun merkeistä tai puutteita käyttäjien koulutuksessa tietoturvakäytäntöjen suhteen.

Lisäksi tietojenkalastelutestaus tarjoaa arvokkaan mahdollisuuden kouluttaa organisaation henkilöstöä tunnistamaan tietojenkalasteluyrityksiä ja reagoimaan niihin asianmukaisesti. Henkilöstön koulutus on avainasemassa tietoturva-

hyökkäysten torjunnassa, ja tietojenkalastelutestaus auttaa testaamaan, kuinka hyvin koulutus on omaksuttu ja toteutettu käytännössä.

Säännöllinen testaaminen ja tulosten analysointi ovat olennainen osa tietojenkalastelutestausta. Näiden toimien avulla voidaan kehittää ja parantaa organisaation tietoturvatoimenpiteitä tietojenkalastelun torjumiseksi. Tulosten perusteella voidaan tunnistaa toistuvia haavoittuvuuksia ja kehittää tehokkaampia strategioita niiden torjumiseksi.

Tavoitteena on myös arvioida organisaation alttiutta tietojenkalastelulle ja kehittää riskienhallintastrategioita tietojen turvallisuuden varmistamiseksi. Tehokas tietojenkalastelutestaaminen auttaa ylläpitämään luottamusta organisaation ja sen kykyyn suojata arkaluonteisia tietoja. Luottamuksen ylläpitäminen on keskeistä liiketoiminnan jatkuvuuden kannalta, sillä se vaikuttaa suoraan asiakkaiden ja sidosryhmien luottamukseen organisaatiota kohtaan.

3.2 Tietojenkalastelutestien toteutus

Tässä työssä tarkastellaan uSecuren uPhish-työkalulla tehtyjen testien tuloksia. Testiryhmälle suoritettiin kolme erilaista testiä, joista jokainen testi suoritettiin yhteensä kolme kertaa. Vaikka testeissä tehtiin aina muutamia pieniä muutoksia, säilytettiin pohja samanlaisena jokaisessa testissä. Näistä testeistä kaksi toteutettiin ennen tietojenkalastelukoulutusta ja yksi koulutuksen jälkeen. Yhteensä testeissä käytettiin 108 kohdehenkilön testituloksia seitsemästä eri organisaatiosta.

On oleellista huomata, että tässä tutkimuksessa keskitytään testitulosten yleiseen analysointiin ja niiden kokonaisvaikutukseen. Vaikka jokaiselle yritykselle suoritettiin omat analyysit, ne eivät sisälly tämän tutkimuksen sisältöön. Tarkoituksena on saada kokonaiskuva siitä, millaiset viestit saavat tietojenkalasteluviestin vastaanottajan lataamaan viestissä olevan liitteen tai vierailemaan viestin sisältämässä linkissä ja mahdollisesti antamaan tietonsa eteenpäin. Tämän avulla pyritään

ymmärtämään paremmin, kuinka tietoisia ja varovaisia ihmiset ovat tietojenkalasteluyritysten tunnistamisessa ja miten he reagoivat tällaisiin tilanteisiin.

3.3 Testituloksien analysointi

Tulosten analysoinnissa hyödynnettiin uSecuren portaaliin kerättyä dataa testituloksista. Analyysi suoritettiin kolmella eri tasolla, jotka olivat viestin avaaminen (matala riski), linkin klikkaaminen (keskisuuri riski) ja tiedoston lataaminen tai tietojen antaminen (suuri riski). Näiden eri riskitasojen avulla voitiin arvioida testin osallistujien alttiutta erilaisille tietojenkalasteluyrityksille ja heidän käyttäytymistään eri vaiheissa.

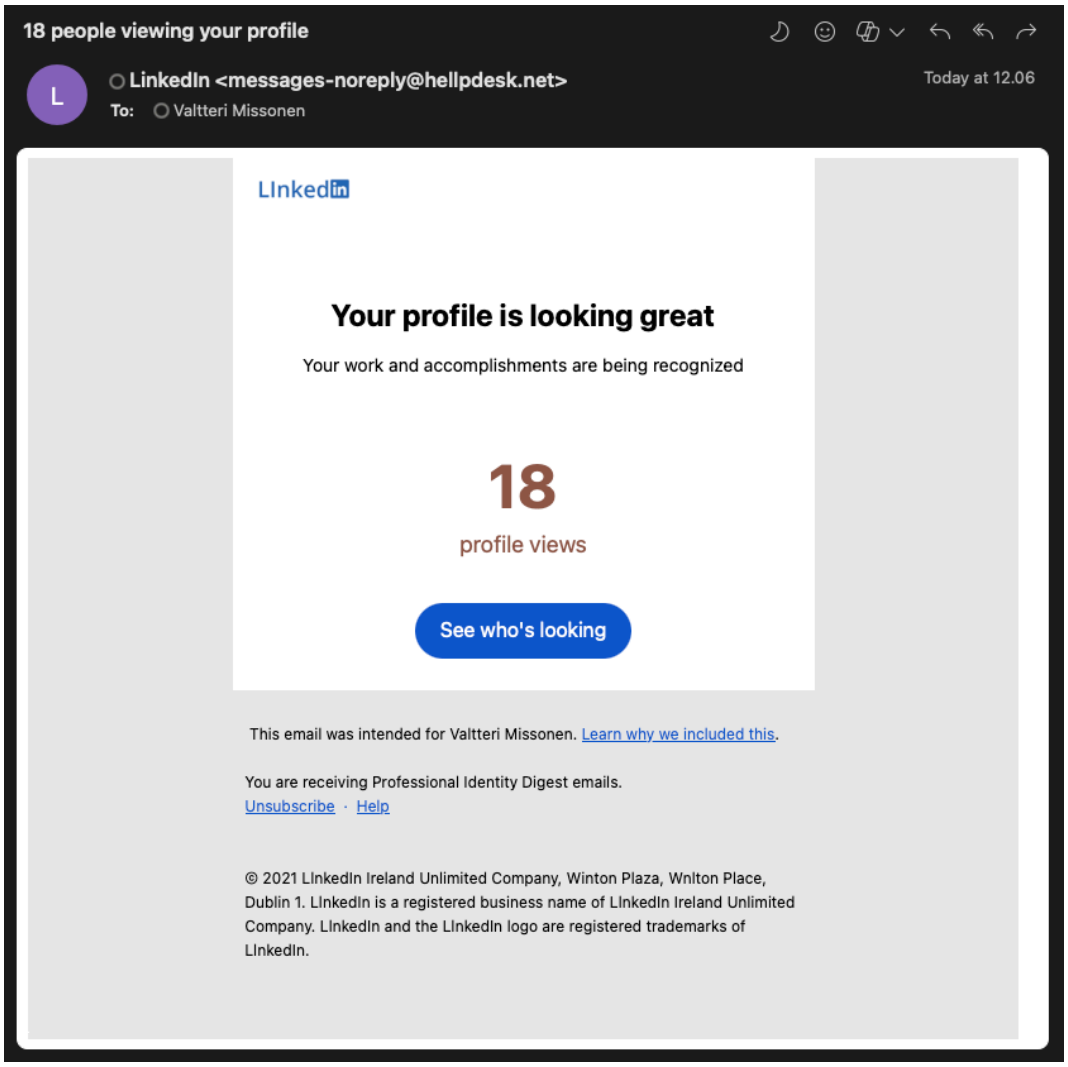
Lisäksi analyysissa otettiin huomioon koulutustilanteista saadut havainnot ja palaute, jotka toimivat täydentävinä tietolähteinä. Koulutustilanteista esiin nousseet asiat tarjosivat lisävalaistusta testituloksiin ja auttoivat ymmärtämään syvemmin osallistujien reaktioita ja havaintoja tietojenkalastelutestien aikana. Näiden kahden eri datalähteen yhdistäminen mahdollisti tulosten laajemman tulkinnan ja ymmärtämisen.

Kokonaisuudessaan tämä monipuolinen lähestymistapa analyysiin varmisti, että tulokset olivat perusteltuja, luotettavia ja kattavia. Tämä auttoi saamaan syvällisemmän käsityksen tietojenkalasteluyritysten tehokkuudesta ja osallistujien tietoturvakäyttäytymisestä, mikä puolestaan tarjosi arvokasta tietoa tietoturvakoulutuksen kehittämiseen ja turvallisuustoimenpiteiden suunnitteluun.

3.4 LinkedIn-testi

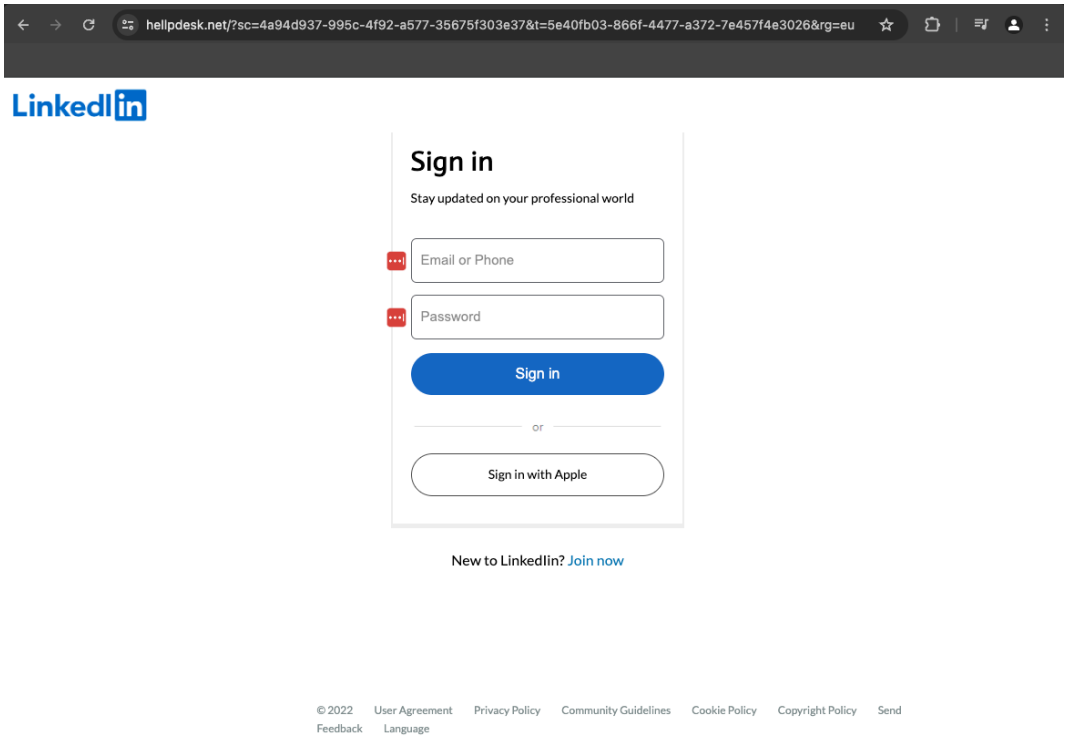
Ensimmäinen toteutetuista tietojenkalastelutesteistä ja koulutuksen osa keskittyi sosiaalisen median ilmoituksiin. Tämä testi oli vaikeusasteelta helpoimmasta päästä ja odotuksena oli, että kohdehenkilöt selviävät tästä testistä hyvin. Tässä testissä simuloitiin tilannetta, jossa LinkedIn-teemaisen sähköpostin ja kirjautumissivun avulla pyrittiin herättämään vastaanottajan kiinnostus omalla LinkedIn-profiilillaan havaittuun vierailumäärään. Sähköpostiviestissä luotiin houkutteleva

kuvitteellinen tilanne, jossa vastaanottajaa kehotettiin avaamaan linkki tutkiakseen tarkemmin profiilinsa vierailutilastoja (kuva 7).



Kuva 7. LinkedIn-testin sähköpostiviesti

Testin olennainen osa oli kiinnittää huomiota sähköpostiviestin lähettäjän osoitteeseen ja varmistaa sen aitous ennen linkin avaamista. Tässä testissä oli osoitteena käytetty ”hellpdesk.net” domain päätteistä osoitetta. Sähköpostiosoitteessa epäilystä olisi pitänyt herättää osoitteen sisältämä kirjoitusvirhe ”hellp” ja puuttuvat viittaukset LinkedIniin. Viestissä oleva linkki ohjasi käyttäjän kirjautumissivulle, joka näytti ulkoisesti aidoilta LinkedIn-kirjautumissivuilta (kuva 8).

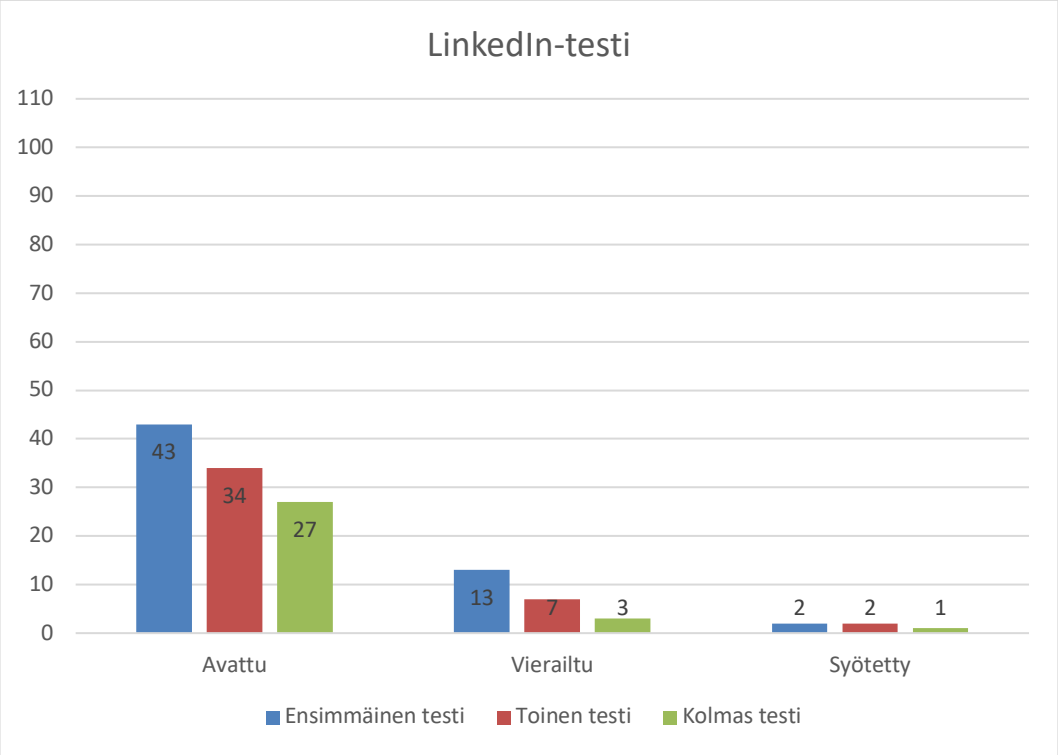


Kuva 8. LinkedIn-testin kirjautumissivu

Kirjautumissivulla oli keskeistä kiinnittää huomiota sivun URL-osoitteeseen (hellpdesk.net), joka antoi merkkejä siitä, että sivusto ei ollut aito, vaan pikemminkin suunniteltu tietojenkalasteluun.

3.4.1 Tulokset

Alla olevasta kuvasta (kuva 9) nähdään simulaation tuloksia. Kuvasta näkyy jokaisen testin avattujen viestien, linkkien klikkauksen ja tietojen syöttämisen määrät. Taulukosta voidaan verrata testien tuloksia keskenään ja huomata millainen kehittyminen tietojenkalasteluviestien tunnistamisella kohdehenkilöillä on ollut testien välillä.



Kuva 9. LinkedIn-testin tulokset

Aluksi voidaan huomata, että viestien avaamisen määrä on laskenut jokaisen testin osalta. Tämä osoittaa, että kehitystä on tullut käyttäjien varovaisuuteen ja tietoisuuteen mahdollisista uhkista. Ensimmäisen testin aikana viestejä avattiin 43 kappaletta, mikä laski toisessa testissä 34:ään ja edelleen 27:ään kolmannessa testissä. Vaikka nämä luvut osoittavat vähenevää trendiä, on huomattava, että viestien avaaminen on edelleen merkittävää. Se voi viitata siihen, että käyttäjät eivät vielä täysin ymmärrä tietojenkalastelun riskejä tai että joissain tapauksissa houkuttelevat otsikot tai sisältö houkuttelevat käyttäjiä avaamaan viestin varoituksista huolimatta. On myös mahdollsita, että jotkin sähköpostisovellukset merkitsevät viestin avatuksi vain selailemalla viestejä kansiossa.

Toiseksi linkissä vierailujen määrä on myös laskenut. Ensimmäisen testin aikana linkissä vierailtiin 13 kertaa, mikä laski seitsemään kertaan toisessa testissä ja vain kolmeen kertaan kolmannessa testissä. Tämä viittaa siihen, että käyttäjät ovat

oppineet tunnistamaan epäilyttäviä linkkejä ja vähentäneet altistumistaan mahdollisille haitallisille verkkosivustoille.

Kolmanneksi, tietojen syöttämisen määrä on myös laskenut koulutuksen jälkeen. Vaikka lasku ei ole yhtä merkittävä kuin viestien avaamisen tai linkkeihin vierailun määrän lasku, se silti osoittaa, että koulutus on auttanut käyttäjiä olemaan varovaisempia antamansa tietojen suhteen. On kuitenkin tärkeää huomata, että yhdenkin tietojen syöttämisen tapauksessa riski on edelleen olemassa, ja tämä voi olla kohdealue tuleville koulutuksille ja parannustoimille.

3.4.2 Kohdehenkilöiden huomiot testistä

Käyttäjän valinnoista, miten hän toimi saatuun testiviestiin voidaan saada erinomaista tietoa siitä, mikä viesteissä sai henkilön toimimaan juuri kuten toimi. Koulutuksessa esiin tulleet huomiot siitä, miksi käyttäjä ei avannut viestiä, klikannut linkkiä tai antanut tietoja, olivat seuraavanlaisia:

1. *“Tällaisia viestejä tulee paljon”:* Käyttäjä tunnistaa yleisen taktiikan ja välttää avaamasta viestejä, joissa on epäilyttäviä tai tuntemattomia lähettäjiä.
2. *“Minulla ei ole LinkedIniä”:* Koska käyttäjällä ei ole kyseistä palvelua, hän epäilee viestin aitoutta ja päättää olla reagoimatta siihen.
3. *“En uskonut, että määrä on oikea”:* Käyttäjä epäilee viestissä ilmoitettua määrää tai tarjousta ja päättää olla antamatta tietoja.
4. *“Huomasin epäilyttävän lähettäjän”:* Käyttäjä kiinnittää huomiota lähettäjän epäilyttävään nimeen tai sähköpostiosoitteeseen ja välttää viestin avaamista.
5. *“Huomasin sivun URL-osoitteen oudoksi”:* Käyttäjä kiinnittää huomiota linkin kohdesivun URL-osoitteeseen ja tunnistaa sen epäilyttäväksi tai epäaitoksi.

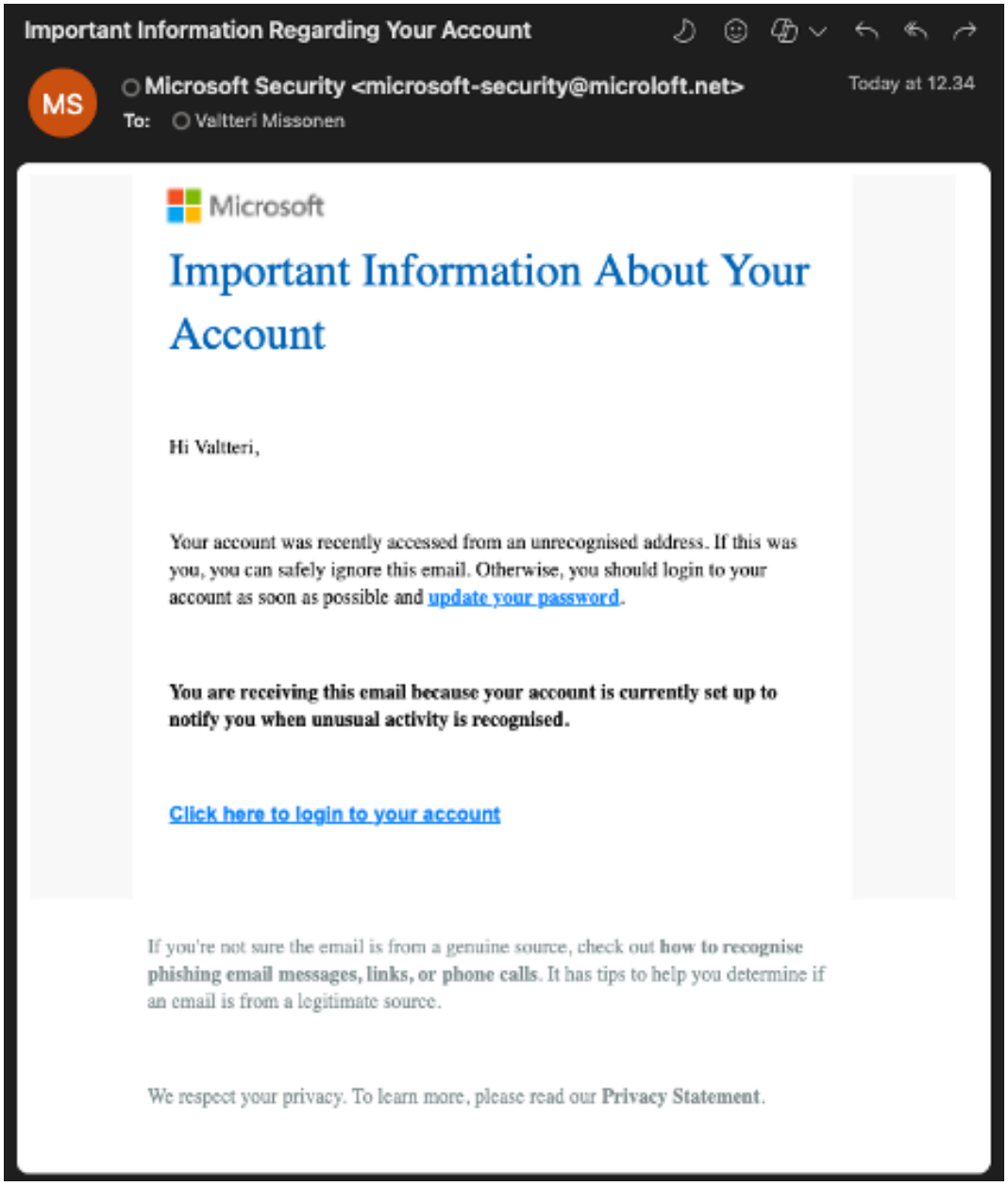
6. *"En käytä työosoitetta LinkedInissä":* Käyttäjä huomaa, että hänen LinkedIn-tilinsä ei ole yhteydessä työsähköpostiin, mikä lisää epäilyjä viestin aitoudesta.

Puolestaan taas syyt siihen, miksi käyttäjä avasi sähköpostiviestin, klikkasi linkkiä tai antoi tietoja olivat, seuraavanlaisia:

1. *"Sähköpostiohjelmani merkitsi sen itse luetuksi":* Käyttäjä saattaa vain selata viestejään ja sähköpostiohjelma merkitsee viestin automaattisesti luetuksi.
2. *"En vain osannut epäillä, että olisi huijausta":* Käyttäjä ei havainnut mitään epäilyttävää viestissä tai linkissä ja luotti sen aitouteen.
3. *"Kiinnostukseni heräsi isosta vierailijamäärästä":* Käyttäjä voi tuntea kiinnostusta mainitun suuren vierailijamäärän vuoksi ja haluaa tarkistaa linkin sisällön tai tarjouksen.

3.5 Microsoft salasana -testi

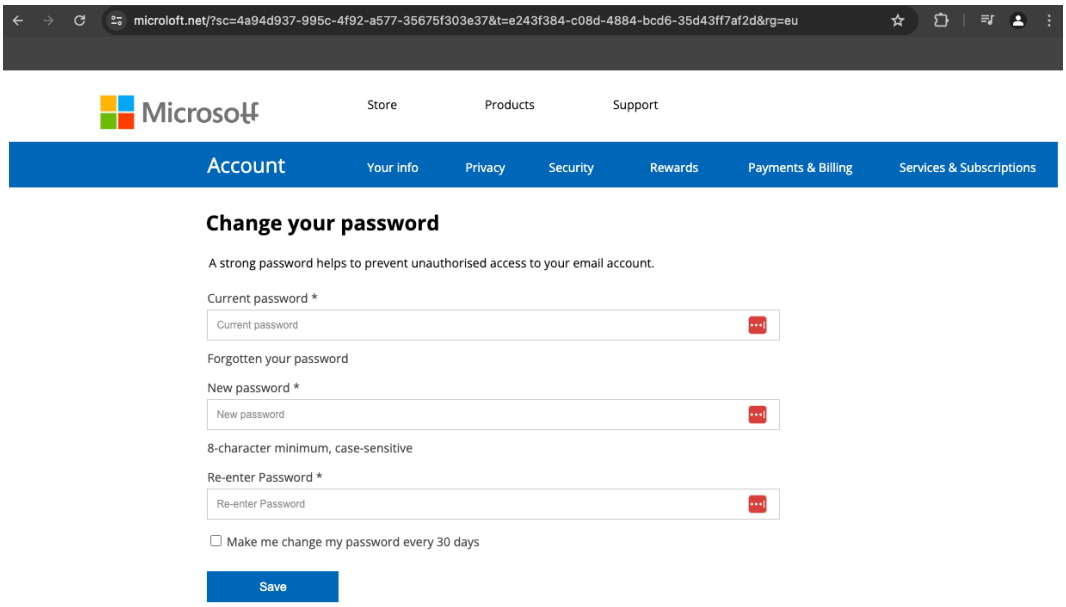
Toinen tietojenkalastelutesti toteutettiin simuloimalla Microsoftin ilmoitus epäilyttävästä toiminnasta käyttäjän tilillä (kuva 10). Testin tavoitteena oli herättää kohdehenkilön huoli ja saada hänet toimimaan nopeasti reaktion seurauksena ja vaihtamaan salasana, jolloin kuviteltu hyökkääjä saisi tietoonsa oikean salasanan. Viestissä oli tärkeää kiinnittää huomiota sähköpostin lähettäjän osoitteen päätteeseen, joka oli microloft.net. Tämän epäilyttävän osoitteen ja viestin aiheuttaman reaktion tarkoituksena oli hämmentää vastaanottajaa ja saada hänet luulemaan viestin olevan aito Microsoftilta.



Kuva 10. Microsoft salasana -testin sisältämä viesti.

Kun kohdehenkilö klikkasi linkkiä sähköpostiviestissä, hänet ohjattiin sivulle, jossa käyttäjän tulisi määrittää uusi salasana (kuva 11). Tässä testissä käyttäjän tuli kiinnittää huomiota sivun URL-osoitteeseen, joka oli myös microloft.net. Lisäksi kirjautumissivulla näkyi virheellinen Microsoftin logo, jossa kirjaimet ”f” ja ”t” olivat väärinpäin sanan lopussa. Tämä oli tarkoitettu herättämään epäilyksiä sivuston

aitoudesta ja varoittamaan kohdehenkilöä mahdollisesta tietojenkalasteluyrityksestä.

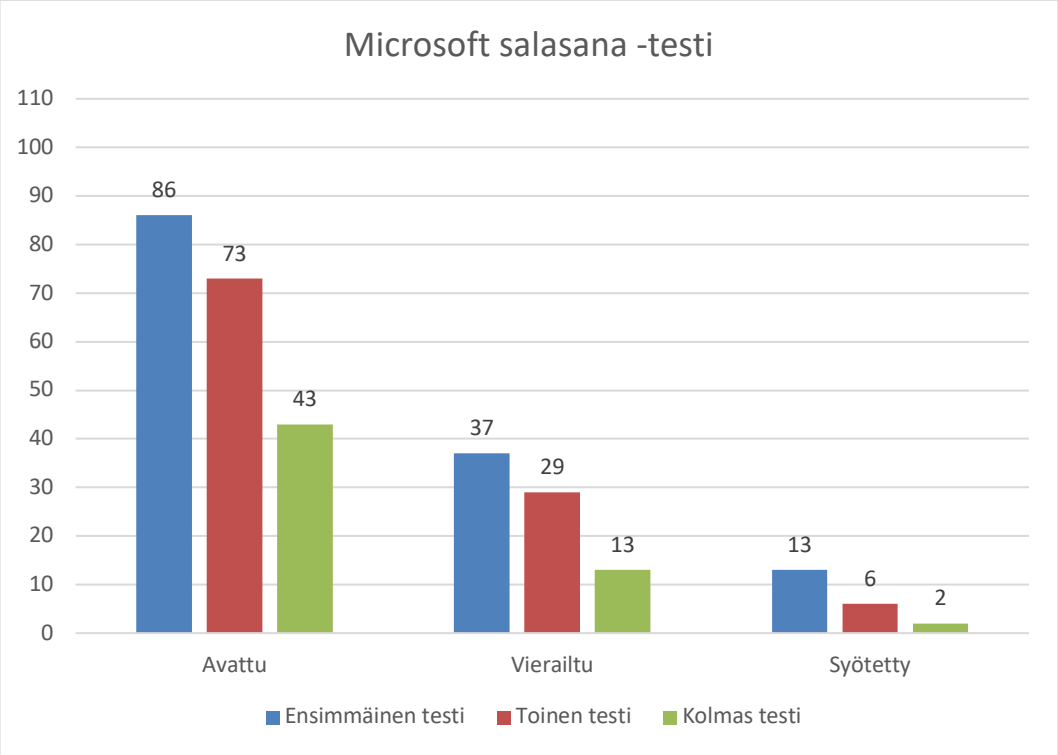


Kuva 11. Microsoft salasana -testin salasanan vaihtosivu.

Testin tarkoituksena oli osoittaa, kuinka tietojenkalastelijat pyrkivät hyödyntämään ihmisten hätääntymistä ja kiireellisyyden tunnetta saadakseen heidät toimimaan nopeasti ja antamaan arkaluonteisia tietoja. Lisäksi testi korosti tarvetta olla tarkkaavainen ja tietoinen epäilyttävistä merkeistä sähköpostiviesteissä ja verkkosivustoilla, jotta voidaan suojautua tällaisilta huijauksilta ja turvata henkilökohtaiset tiedot.

3.5.1 Tulokset

Kuvassa 12 esitetään simulaation tuloksia. Siitä nähdään jokaisen testin osalta avattujen viestien, linkkien klikkausten ja tietojen syöttämisen määrät. Kuvan avulla voidaan vertailla testien tuloksia keskenään ja havaita, kuinka kohdehenkilöiden kyky tunnistaa tietojenkalasteluviestit on kehittynyt testien välillä.



Kuva 12. Microsoft salasana -testin tulokset.

Viestien avaaminen on laskenut jokaisen testin välillä. Ensimmäisessä testissä viestejä avattiin 86 kappaletta, toisessa 73 kappaletta ja kolmannessa 43 kappaletta. Tämä osoittaa käyttäjien varovaisuuden lisääntymistä ja tietoisuuden kasvua potentiaalisista uhkista. Viestien suuri avaamisen määrä ei ole yllätys, sillä testin olikin tarkoitus kiinnittää enemmän huomiota kuin aiemman LinkedIn-testin.

Linkkien avaus määrä on myös laskenut jokaisen testin välillä. Ensimmäisessä testissä vierailuja oli 37, toisessa 29 ja kolmannessa 13. Tämä viittaa siihen, että käyttäjät ovat oppineet tunnistamaan epäilyttäviä linkkejä ja vähentäneet altistumistaan mahdollisille haitallisille verkkosivustoille. Huomionarvoista on myös se, että ensimmäisessä ja toisessa testissä vain kaksi henkilöä oli vieraillut sivustolla kummassakin testissä.

Tietojen syöttämisen määrä on myös laskenut jokaisen testin välillä, mikä on myönteinen merkki. Ensimmäisessä testissä tietoja syötettiin 13 kertaa, toisessa kuusi kertaa ja kolmannessa kaksi kertaa. Vaikka lasku ei ole yhtä merkittävä kuin viestien avaamisen tai linkkeihin vierailun määrän lasku, se silti osoittaa, että käyttäjät ovat oppineet olemaan varovaisempia antamasta tietoja.

3.5.2 Kohdehenkilöiden huomiot testistä

Käyttäjien palautteesta ja havainnoista voidaan erottaa useita syitä sille, miksi he eivät avanneet viestiä, klikanneet linkkiä tai antaneet tietoja:

1. *”Olin varma, ettei viesti ole aito, vaikka en kiinnittänytkään siihen erityistä huomiota”:* Käyttäjä tuntee jo etukäteen epäilyttävän viestin ja välttää avaamasta sitä.
2. *”Meidän oma IT-osastomme ilmoittaa aina näistä asioista, meidän ei tarvitse huolehtia”:* Käyttäjä luottaa yrityksen IT-tiimin aktiiviseen rooliin tällaisissa asioissa ja odottaa sen hoitavan tietoturvauhkien torjunnan.
3. *”Huomasin epäilyttävän lähettäjän”:* Käyttäjä kiinnittää huomiota epäilyttävään lähettäjään ja päättää olla reagoimatta viestiin.
4. *”Huomasin sivustolla olevan Microsoftin logossa virheen”:* Käyttäjä havaitsee virheen sivuston logossa, mikä herättää epäilyksiä sen aitoudesta.
5. *”Huomasin sivun URL-osoitteen oudoksi”:* Käyttäjä kiinnittää huomiota epäilyttävään URL-osoitteeseen ja päättää olla luottamatta sivustoon.
6. *”Sivusta tuli vain huono tunne”:* Käyttäjä tuntee epämukavuutta tai epävarmuutta sivuston tai viestin suhteen, joten hän päättää olla reagoimatta viestiin.

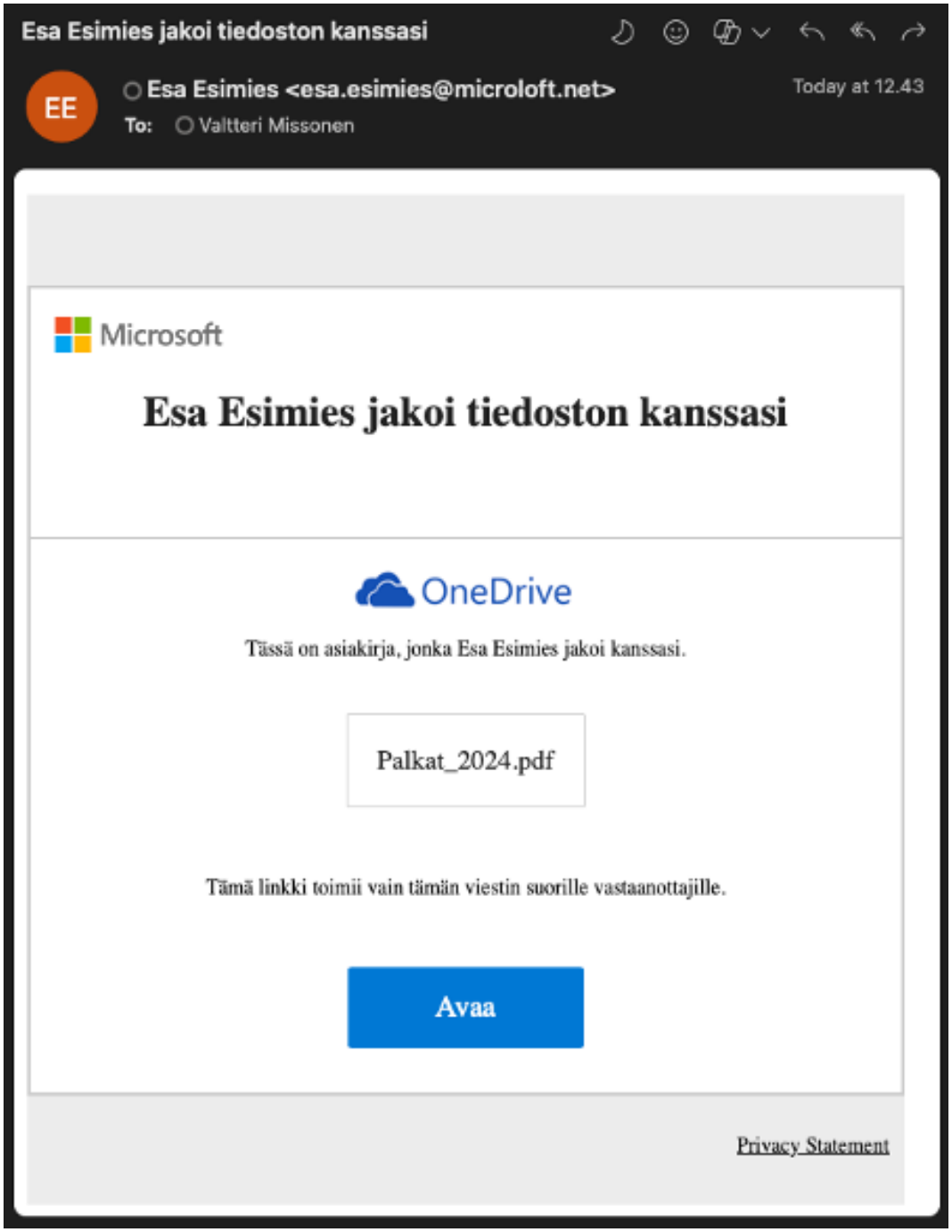
Puolestaan taas syitä sille, että miksi käyttäjä avasi sähköpostiviestin, klikkasi linkkiä tai antoi tietoja, olivat seuraavanlaisia:

1. *”Sähköpostiohjelmani merkitsi sen itse luetuksi”:* Käyttäjä saattaa vain selata viestejään ja sähköpostiohjelma merkitsee viestin automaattisesti luetuksi.
2. *”Viesti vaikutti realistiselta”:* Käyttäjä pitää viestiä uskottavana ja aidolta vaikutelmaltaan, joten hän päättää luottaa viestin sisältöön.
3. *”Viesti tuli kiireen keskellä, enkä osannut siinä vaiheessa epäillä sen aitoutta”:* Käyttäjä ei kiinnitä tarpeeksi huomiota viestin aitouteen kiireen keskellä.
4. *”En vain osannut epäillä yhtään”:* Käyttäjä ei havaitse mitään epäilyttävää viestissä tai linkissä ja luottaa sen aitouteen.

3.6 OneDrive-testi

Tietojenkalastelutesti keskittyi kolmannessa testissä Microsoft OneDriven tiedostonjakoon. Testin luotettavuutta lisättiin käyttämällä testissä yrityksen sisäisen esihenkilön nimeä, mikä herätti kohteen luottamusta viestiä kohtaan (kuva 13). Lisäksi jaettu tiedosto liittyi palkka-asioihin, minkä tarkoituksena oli herättää kohteen mielenkiinto ja lisätä todennäköisyyttä klikata Avaa-painiketta. Tässä testissä käytettiin jokaisella kolmella eri kerralle eri henkilön nimeä ja eri liitettä, mutta viestin pohja ja käytetty domain ja URL-osoite pysyivät samoina kaikissa kolmessa testissä. Testi oli suunniteltu vaikeaksi ja luotiin vaikuttamaan mahdollisimman aidolta, jotta kohteet olisivat alttiimpia toimimaan huijauksen mukaisesti.

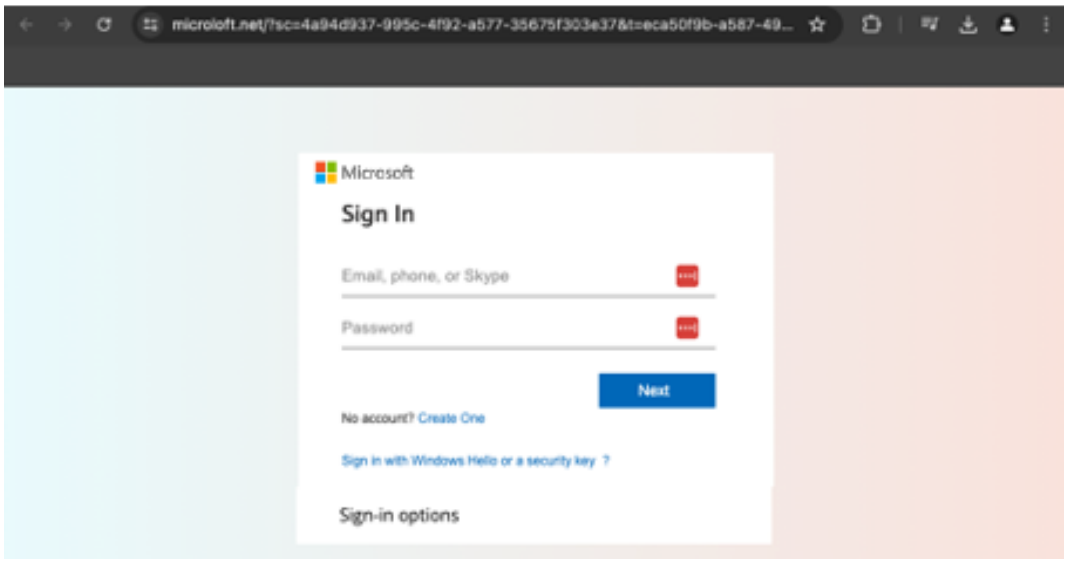
Testin tarkoituksena oli houkutella henkilö klikkaamaan Avaa-painiketta ja syöttämään Microsoft-kirjautumistietonsa väärennetylle sivustolle. Sähköpostiviestissä oli tärkeää kiinnittää huomiota sähköpostin lähettäjän osoitteeseen, joka oli keksitty osoite etunimi.sukunimi@microloft.net, joka poikkesi todellisesta organisaation osoitteesta.



Kuva 13. OneDrive-testin sisältämä viesti

Jos käyttäjä klikkasi viestin sisältämää Avaa-painiketta, hänet ohjattiin väärennetylle Microsoftin kirjautumissivustolle. Samoin kuin itse viestissä, niin

kirjautumissivulla oli tärkeää kiinnittää huomiota sivuston URL-osoitteeseen, joka oli myös microloft.net (kuva 14).

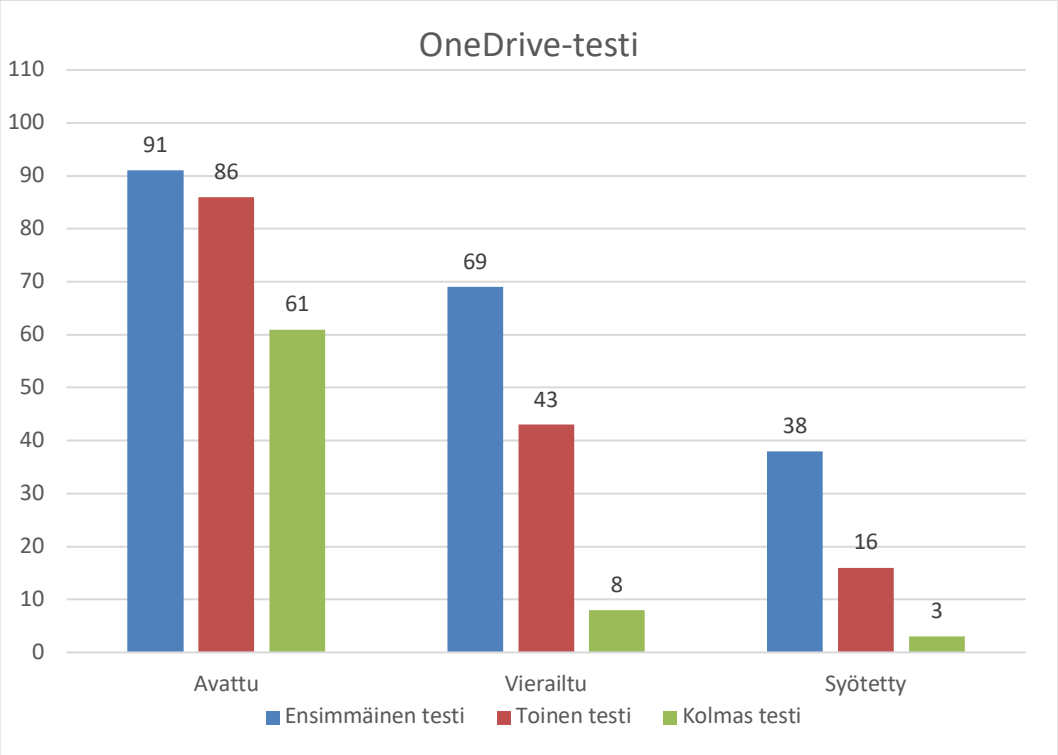


Kuva 14. OneDrive-testin kirjautumissivu.

Tällaiset tietojenkalastelutestit korostavat tarvetta olla varovainen ja tarkkaavainen verkossa vastaanotettujen viestien ja linkkien suhteen. Tarkoituksena testissä oli myös osoittaa henkilöille, kuinka aidon näköisiä viestit voivat todellisuudessa olla.

3.6.1 Tulokset

Kuva 15 näyttää simulaation tuloksia. Siitä ilmenee avattujen viestien, linkkien klikkausten ja tietojen syöttämisen määrä kussakin testissä. Kuvan avulla voidaan vertailla testien tuloksia keskenään ja havaita, kuinka kohdehenkilöiden kyky tunnistaa tietojenkalasteluviestit on kehittynyt testien välillä.



Kuva 15. OneDrive-testin tulokset.

Ensimmäisessä testissä viestejä avattiin 91 kappaletta, toisessa 86 kappaletta ja kolmannessa 61 kappaletta. Huomattavaa on, että viestien avaamisen määrä on laskenut jokaisen testin välillä. Vaikka avattujen viestien määrä on edelleen korkea, osoittaa se käyttäjien varovaisuuden lisääntymistä ja tietoisuuden kasvua tietojenkalastelun riskistä.

Linkkien vierailun määrä on myös laskenut jokaisen testin välillä. Ensimmäisessä testissä vierailuja oli 69, toisessa 43 ja kolmannessa kahdeksan. Tämä viittaa siihen, että käyttäjät ovat oppineet tunnistamaan epäilyttäviä linkkejä ja vähentäneet altistumistaan potentiaalisille haitallisille verkkosivuille.

Tietojen syöttämisen määrä on myös laskenut jokaisen testin välillä, mikä on myönteinen merkki. Ensimmäisessä testissä tietoja syötettiin 38 kertaa, toisessa 16 kertaa ja kolmannessa kolme kertaa. Vaikka lasku ei ole yhtä merkittävä kuin

viestien avaamisen tai linkkeihin vierailun määrän lasku, se silti osoittaa, että käyttäjät ovat oppineet olemaan varovaisempia antamiensa tietojen suhteen.

Huomionarvoista on, että ensimmäisessä ja toisessa testissä 18 henkilöä oli vieraillut sivustolla kummassakin testissä ja heistä neljä olivat antaneet tietoja kummassakin testissä. Koulutuksen jälkeen vain yksi henkilö oli vieraillut joko ensimmäisessä tai toisessa ja kolmannessa testissä linkissä, mutta viimeisessä testissä tietoja syöttäneet olivat täysin uusia uhreja.

3.6.2 Kohdehenkilöiden huomiot testistä

Tämän testin osalta tekijät sille, miksi käyttäjä ei avannut tai antanut tietojaan testissä, olivat seuraavanlaisia:

1. *"Meillä ei lähetetä yleisiä ilmoituksia OneDriven kautta tai ylipäätään sähköpostilla":* Käyttäjä tunnistaa viestin epätavalliseksi ja poikkeavaksi normaalista käytännöstä, mikä herättää epäilyksiä sen aitoudesta.

2. *"Lähettäjän sähköpostiosoite ei ollut oikea":* Käyttäjä kiinnittää huomiota epäilyttävään sähköpostiosoitteeseen, mikä lisää epäilyjä viestin aitoudesta.

3. *"Huomasin sivun URL-osoitteen oudoksi":* Käyttäjä havaitsee epäilyttävän URL-osoitteen, mikä viittaa sivuston epäaitouteen.

4. *"Kirjautumissivu ei vaikuttanut ihan oikealta":* Käyttäjä huomaa kirjautumissivun epäilyttävyyden ja päättää olla antamatta tietojaan.

Tämän testin osalta taas syitä sille, miksi käyttäjä avasi viestin, painoi viestin sisältämää linkkiä tai antoi tietoja olivat seuraavanlaisia:

1. *"Sähköpostiohjelmani merkitsi sen itse luetuksi":* Käyttäjä saattaa vain selata viestejään ja sähköpostiohjelma merkitsee viestin automaattisesti luetuksi.

2. *"Viesti vaikutti ihan aidolta ja viestin graafinen ilme oli samanlainen kuin oikea viesti":* Käyttäjä pitää viestiä uskottavana sen ulkoisen ilmeen ja sisällön perusteella.

3. *"Lähettäjän nimi sai minut luottamaan viestiin":* Käyttäjä luottaa "lähettäjään" ja pitää viestiä aitona sen perusteella.

4. *"Kaikki vaikutti vain aidolta, joten en vain osannut epäillä yhtään":* Käyttäjä ei havaitse mitään epäilyttävää viestissä tai linkissä ja luottaa sen aitouteen.

5. *"Olemme puhuneet töissä liitteen aiheesta niin oletin, että tämä liittyy oikeasti siihen":* Käyttäjä olettaa viestin liittyvän aiempaan keskusteluun aiheesta työpaikalla ja avaa sen olettaen sen olevan aito.

3.7 Testien tulosten yhteenveto

Tietojenkalastelutestien tulokset paljastavat mielenkiintoisia piirteitä niiden tehokkuudesta ja käyttäjien käyttäytymismalleista. Testien tuloksien ja koulutuksessa ilmenneiden huomioiden perusteella voidaan tehdä seuraavanlaisia päätelmiä erilaisten tietojenkalasteluviestien toimivuudesta:

Bulkkiviestit, jotka on suunnattu mainontaan, sosiaalisen median ilmoituksiin ja vastaaviin yleisiin viesteihin, eivät yleensä tuota toivottua tulosta. Tällaiset viestit harvoin saavat ihmisiä toimimaan nopeasti, joten vastaanottajille jää aikaa tutkia viestiä tarkemmin ja huomata sen epäaitouden merkit. Ihmisillä on jo hyvä yleinen tietoisuus siitä, kuinka heitä pyritään huijaamaan tällaisten massaviestien avulla, mikä tekee niistä vähemmän tehokkaita.

Toisaalta tietojenkalasteluviestit, jotka liittyvät käyttäjän turvallisuuteen tai henkilökohtaisiin tietoihin, voivat olla huomattavasti vaarallisempia. Tällaiset

viestit saattavat herättää vastaanottajissa pelonomaisen reaktion, joka saa heidät toimimaan nopeasti ja vaistonvaraisesti. Vaikka vastaanottajat saattavat olla tietoisia tällaisten viestien tarkoituksesta, pelko omasta turvallisuudesta voi ohittaa järjen.

Testien tuloksista voidaan myös päätellä, että ihmisten luottamus toisiin ihmisiin on usein suurin syy sille, miksi he lankeavat tietojenkalasteluyrityksiin. Kun viesti näyttää ulkoisesti aidolta, erityisesti kun se on yhdistetty organisaation luotettavan henkilön nimeen, vastaanottajat saattavat jättää huomiotta viestissä olevat varoitusmerkit ja antaa tietonsa huijareille. Tämä korostaa luottamuksen haavoittuvuutta tietojenkalasteluyrityksissä ja tarvetta lisätä tietoisuutta ja koulutusta tunnistamaan huijausyritykset.

Yhteenvetona voidaan todeta, että koulutuksella oli positiivinen vaikutus käyttäjien käyttäytymiseen tietojenkalastelusimulaatioissa. Viestien avaamisen, linkkien vierailun ja tietojen syöttämisen määrät laskivat kaikissa kolmessa testissä, mikä osoittaa, että käyttäjät ovat oppineet tunnistamaan ja välttämään potentiaalisia uhkia. Kuitenkin vaikka parannusta on tapahtunut, jatkotoimenpiteitä tarvitaan edelleen käyttäjien tietoisuuden ja varovaisuuden lisäämiseksi tietojenkalastelun torjunnassa.

4 JOHTOPÄÄTÖKSET

Tämän työn tarkoituksena oli tarjota kattava näkemys tietojenkalastelun eri muodoista, niiden vaikutuksista ja ennen kaikkea keinoista suojautua niitä vastaan. Työssä tarkasteltiin tietojenkalastelun historiaa, kehitystä ja yleisyyttä sekä erilaisia tietojenkalastelun muotoja, kuten kohdennettua tietojenkalastelua, tekstiviestihuijausta, äänikalastelua, deepfakea ja QR-koodia. Lisäksi työssä käsiteltiin tietojenkalasteluhyökkäyksen vaikutuksia, jotka voivat olla taloudellisia, toiminnallisia ja maineellisia sekä esitettiin käytännön ohjeita ja strategioita tietojenkalastelun torjumiseksi. Lopuksi työssä tarkasteltiin suoritettuja tietojenkalastelutestejä oikeille yrityksille ja pyrittiin saamaan selville, mitkä piirteet viesteissä saivat kohdehenkilön luottamaan testissä luotuun viestiin ja vierailemaan viestin sisältämässä linkissä ja jopa antamaan henkilökohtaisia tietoja.

Työn tulokset osoittivat, että tietojenkalastelu on monimutkainen ja monimuotoinen ilmiö, joka edellyttää jatkuvaa valppautta ja tietoisuutta käyttäjiltä. Tietojenkalasteluhyökkäykset voivat olla hyvin vakuuttavia ja realistisia, ja niissä voidaan hyödyntää erilaisia tekniikoita ja kanavia huijata ihmisiä. Tietojenkalasteluhyökkäykset voivat aiheuttaa vakavia vahinkoja niin yksilöille kuin organisaatioille, ja niiden torjuminen vaatii sekä teknisiä että inhimillisiä toimenpiteitä.

Yksi keskeinen havainto oli se, että tietojenkalastelun tehokkuus riippuu viestin sisällöstä ja muodosta. Yleiset massaviestit ovat harvoin tehokkaita, kun taas viestit, jotka herättävät pelkoa tai luovat kiireen tunteen, voivat olla vaarallisempia ja saavat vastaanottajan toimimaan harkitsemattomasti.

Toinen tärkeä havainto oli se, että ihmisten luottamus toisiin ihmisiin voi olla heidän haavoittuvin kohtansa tietojenkalastelussa. Kun viesti näyttää ulkoisesti aidolta ja se on liitetty organisaatiossa työskentelevän luotettavan henkilön nimeen, vastaanottajat saattavat luottaa siihen sokeasti, vaikka viestissä olisikin viitteitä epäaitoudesta.

Tietojenkalastelutestauksen avulla voidaan arvioida organisaatioiden valmiutta ja reagointikykyä tietojenkalasteluyrityksiin sekä kouluttaa henkilöstöä tunnistamaan ja välttämään tietojenkalastelua. Tietojenkalastelutestien tulokset osoittivat, että koulutus ja harjoittelu ovat tehokkaita keinoja parantaa tietoturvaa ja vähentää tietojenkalastelun riskiä.

Työn johtopäätöksenä voidaan todeta, että tietojenkalastelu on merkittävä ja kasvava uhka digitaalisessa maailmassa ja se vaatii jatkuvaa huomiota ja toimintaa. Tietojenkalastelun torjuminen edellyttää sekä teknisiä että inhimillisiä toimenpiteitä, jotka ovat yhteydessä toisiinsa. Tietojenkalastelun tunnistaminen ja välttäminen on ensisijaisesti ihmisten vastuulla, mutta he tarvitsevat myös asianmukaisia työkaluja ja koulutusta tietoturvansa vahvistamiseksi. Tietojenkalastelutestaus on yksi tehokas tapa kouluttaa ja testata henkilöstöä tietojenkalastelun tunnistamisessa ja välttämisessä. Tietojenkalastelutestaus auttaa myös kehittämään ja parantamaan organisaation tietoturvatoimenpiteitä tietojenkalastelun torjumiseksi. Tietojenkalastelun torjuminen on jatkuva prosessi, joka edellyttää säännöllistä päivittämistä ja seurantaa, jotta voidaan pysyä ajan tasalla tietojenkalastelun kehityksestä ja muodoista.

LÄHTEET

Alharthi, D. & Regan, A. (2020). *Social Engineering Defense Mechanisms: A Taxonomy and a Survey of Employees' Awareness Level.* Journal of Information Security, Vol.13 No.4. https://doi.org/10.1007/978-3-030-52249-0_35

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M. & Musa, A. (2018). *Understanding Awareness of Cyber Security Threat among IT Employees.* 2018 6th International Conference on Future Internet of Things and Cloud Workshops. http://dx.doi.org/10.1109/W-FiCloud.2018.00036

APWG. (2024). Phishing activity trends report, 4th quarter 2023. Noudettu 13.3.2024 osoitteesta https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N. & Arthi, S. (2020). *Why is phishing still successful?* Computer Fraud & Security, 2020(9). https://doi.org/10.1016/S1361-3723(20)30098-1

CybSafe. (2023). How phishing has catastrophic effects on organizations. Noudettu 25.3.2024 osoitteesta https://www.cybsafe.com/blog/how-can-phishing-affect-a-business/

Elisa. (2021). Neljä keinoa tunnistaa kalastelu. Noudettu 21.3.2024 osoitteesta https://elisa.fi/ideat/epailetko-saaneesi-huijausviestin-4-keinoa-tunnistaa-kalastelu/

Fortinet. (n.d.). Spear Phishing: What It Is and How to Protect Yourself. Noudettu 14.3.2024 osoitteesta https://www.fortinet.com/resources/cyberglossary/spear-phishing

F-Secure. (n.d. a). Mitä on tietojenkalastelu? Noudettu 12.3.2024 osoitteesta https://www.f-secure.com/fi/articles/what-is-phishing

F-Secure. (n.d. b). What is Smishing? Noudettu 16.3.2024 osoitteesta https://www.f-secure.com/en/articles/what-is-smishing

F-Secure. (n.d. c) What is “voice phishing”? Noudettu 20.3.2024 osoitteesta https://www.f-secure.com/en/articles/what-is-vishing

Infosec. (2020). Phishing: Reputational damages. Noudettu 27.3.2024 osoitteesta https://www.infosecinstitute.com/resources/phishing/reputational-damages/

Kaspersky. (n.d. a). What is a Whaling Attack? Noudettu 14.3.2024 osoitteesta https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack

Kaspersky. (n.d. b). I’m a phishing victim! What do I do now? Noudettu 6.4.2024 osoitteesta https://www.kaspersky.com/resource-center/threats/handling-phishing-attacks

Kaspersky. (n.d. c). All About Phishing Scams & Prevention: What You Need to Know. Noudettu 19.4.2024 osoitteesta https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

Kaushalya, S. A. D. T. P., Randeniya, R. M. R. S. B. & Liyanage, A. D. S. (2018). *An Overview of Social Engineering in the Context of Information Security*. 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences. https://doi.org/10.1109/ICETAS.2018.8629126

Kyberturvallisuuskeskus. (2023). QR-koodin käyttö tietojenkalastelussa yleistyy. Noudettu 20.3.2024 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/qr-koodin-kaytto-tietojenkalastelussa-yleistyy

Luse, A. & Burkman, J. (2021). *Gophish: Implementing a Real-World Phishing Exercise to Teach Social Engineering*. Journal of Cybersecurity Education, Research and Practice, 2020(2).

McAfee. (2023). Phishing Email Examples: How to Recognize a Phishing Email? Noudettu 19.4.2024 osoitteesta https://www.mcafee.com/learn/phishing-email-examples-how-to-recognize-a-phishing-email/

Norton. (2024a). What is Smishing? Noudettu 16.3.2024 osoitteesta https://us.norton.com/blog/emerging-threats/smishing

Norton. (2024b). What is vishing? Tips to spot and avoid voice phishing scams. Noudettu 20.3.2024 osoitteesta https://us.norton.com/blog/online-scams/vishing

Norton. (2022). How to protect against phishing: 18 tips for spotting a scam. Noudettu 21.4.2024 osoitteesta https://us.norton.com/blog/how-to/how-to-protect-against-phishing

OnSecurity. (2020). What to do when you've been phished and how to deal with it? Noudettu 6.4.2024 osoitteesta https://www.onsecurity.io/blog/what-to-do-when-youve-been-phished/

Proofpoint. (2023). What to Do If You Respond to a Phishing Email? Noudettu 6.4.2024 osoitteesta https://www.proofpoint.com/us/blog/email-and-cloud-threats/what-do-after-responding-phishing-email

Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A. & Dessouky, M. M. (2021). *Cybersecurity and Countermeasures at the Time of Pandemic.* Journal of Advanced Transportation. https://doi.org/10.1155/2021/6627264

Securityweek. (2020). The Evolution of Phishing: Welcome “Vishing”. Noudettu 20.3.2024 osoitteesta https://www.securityweek.com/evolution-phishing-welcome-vishing/

Spector (2022). Why is Phishing Getting More Frequent? Noudettu 13.3.2024 osoitteesta https://www.spector.ie/blog/why-is-phishing-getting-more-frequent/

Stage2Data. (n.d.). What damage can phishing cause to your business? Noudettu 27.3.2024 osoitteesta https://stage2data.com/what-damage-can-phishing-cause-to-your-business/

TBOIJ. (2024). What is a deepfake – and how are they being used by scammers? Noudettu 20.3.2024 osoitteesta https://www.thebureauinvestigates.com/stories/2024-03-07/what-is-a-deepfake-and-what-are-the-different-types/

TechTarget. (2024). QR code phishing. Noudettu 20.3.2024 osoitteesta https://www.techtarget.com/whatis/definition/QR-code-phishing

Trustpair. (2023). Whaling vs Spear Phishing: what are the differences? Noudettu 14.3.2024 osoitteesta https://trustpair.com/blog/whaling-vs-spear-phishing/

uSecure. (n.d.). What is a phishing simulation test? Noudettu 14.3.2024 osoitteesta https://blog.usecure.io/what-is-a-phishing-simulation-test

Vayansky, I. & Kumar, S. (2018). *Phishing – challenges and solutions*. Computer Fraud & Security, 2018(1). https://doi.org/10.1016/S1361-3723(18)30007-1

Vivitec. (n.d.). 4 Reasons Phishing Is Getting More Frequent. Noudettu 13.3.2024 osoitteesta https://vivitec.net/4-reasons-phishing-is-getting-more-frequent/

Wallarm. (n.d.). Phishing Attack. Noudettu 25.3.2024 osoitteesta https://www.wallarm.com/what/types-of-phishing-attacks-and-business-impact

Whitty, M. (2018). *Do you love me? Psychological characteristics of romance scam victims.* Cyberpsychology, Behavior, and Social Networking, 21(2).