Tietojenkalasteluviestien kieli ja vaikuttamisen keinot

Aiheen esittely

Tietojenkalastelu verkossa on lisääntynyt usean vuoden ajan. Kybertuvallisuuskeskuksen tilannekeskuksessa käsiteltyjen tietojenkalastelutapausten määrä kasvoi vuodesta 2019 vuoteen 2020 52 %, ja kaikenlaisten keskuksen tietoon tulleiden tietoturvaloukkausten määrä kasvoi kokonaisuudessaan 100 % vuodesta 2019 vuoteen 2020. (Traficom 2019, 35; Traficom 2020, 17). Edelleen jo lokakuuhun 2021 mennessä oli Kyberturvallisuuskeskukselle ilmoitettujen pankkitunnusten kalastelutapausten määrä kasvanut 65 prosentilla edellisvuoteen verrattuna. Onnistuneiden kalastelujen myötä suomalaiset olivat menettäneet 8,4 miljoonaa euroa. (Kyberturvallisuuskeskus 2021.)

Tietojenkalastelu (engl. *phishing*) tarkoittaa, että joku yrittää vilpillisesti saada haltuunsa salaisia tai arkaluonteisia tietoja tekeytymällä luotettavaksi tahoksi (Myers toim. 2007: 1). Kalastelijat esiintyvät laillisen yrityksen tai instituution työntekijänä ja käyttävät väärin tekijänoikeuden alaisia tuotteita ja toteuttavat identiteettivarkauksia (Cate toim. 2007: 671–672). Tietojenkalasteluhyökkäyksiä on tehty 1990-luvulta asti, vaikka Suomessa niitä on alkanut näkyä vasta 2000-luvun alkupuolella (Haapanen 2006, Myers toim. 2007: 2).

Tietojenkalastelu on rikollista toimintaa, joka koskettaa mitä todennäköisimmin jokaista verkossa asioivaa ihmistä riippumatta siitä, millaisilla sivustoilla asioi. Koska tietojenkalastelu on yleistä ja vahingollista, keräsin pro gradu -tutkielmaani (N.N.) varten sähköpostitse lähetetyistä tietojenkalasteluviesteistä aineiston, jota tarkastelin kielen näkökulmasta. Tavoitteena oli selvittää, millaista tietojenkalasteluviestien kieli on ja millä keinoin viestien vastaanottajaan yritettiin vaikuttaa. Selvitin myös, mihin suomenkielinen lukija kiinnittää huomiota viestin aitoutta pohtiessaan. Tutkimuskysymykseni olivat seuraavat: 1) Millaisia normeista poikkeavia piirteitä sähköpostitse lähetettyjen tietojenkalasteluviestien kieli sisältää? 2) Millä keinoilla vastaanottaja yritetään saada toimimaan tietojenkalastelijan toiveiden mukaisesti? 3) Mihin suomenkielinen lukija kiinnittää huomiota viestin aitoutta pohtiessaan? Tutkielma sijoittuu forensisen lingvistiikan eli forensisen kielentutkimuksen alueelle, josta kerron myöhemmin lisää.

Analysoitavia tietojenkalasteluviestejä sain Kyberturvallisuuskeskukselta, kahdelta pankilta, Verohallinnolta ja sosiaalisen median kautta yksityishenkilöiltä. Erittelin viestien

kielenpiirteitä ja keinoja, joilla viestin vastaanottajaan yritettiin vaikuttaa. Lisäksi koostin sosiaalisen median ja tuttavien avulla toisen aineiston, joka valotti sitä, millä perusteilla viestien lukijat tekevät johtopäätöksiä viestien aitoudesta. Lähetin vapaaehtoisille vastaajille viisi viestiä, joista osa oli huijausviestejä ja osa aitoja. He vastasivat minulle ja kertoivat, mitkä viesteistä olivat heidän mielestään huijausviestejä ja miksi he niin ajattelivat. Tässä havaintotekstissä kerron ensin, miten tietojenkalastelu liittyy kielitieteeseen, ja sen jälkeen kerron tiivistetysti analyysini tuloksista ja huomioistani. Aiheesta kiinnostuneet voivat lukea yksityiskohtaisemman kuvauksen aineistosta ja havainnoista pro gradu -tutkielmastani (N.N.).

Tietojenkalastelun aiempi tutkimus ja kalasteluviestien tyypilliset piirteet

Tietojenkalasteluviestien kielen tutkiminen on rikollisen toiminnan välineenä toimivan kielen tutkimista ja näin ollen forensista lingvistiikkaa. Forensinen lingvistiikka eli forensinen kielentutkimus on yksi soveltavan oikeuslingvistiikan osa-alue (Salmi-Tolonen toim. 2008: 376). Suomessa forensiseen lingvistiikkaan liittyvää tutkimusta on tehty toistaiseksi melko vähän[1]. Englanninkielisissä maissa tutkitaan ja käytetään forensista lingvistiikkaa Suomea laajemmin. Käyttöä tukee muun muassa kielialueen suuruus.

Forensista lingvistiikka ei ole nimeltä mainiten juurikaan hyödynnetty tietojenkalastelun tutkimuksessa, mutta yksittäistapauksia löytyy. Judith Tabron (2016) tutki huijauspuheluita forensisen lingvistiikan näkökulmasta ja huomasi, että suljetut kysymykset, puheenaiheen kontrolloiminen ja epätarkka kerronta ovat huijauspuheluille tyypillisiä piirteitä. Chisom Nlebedum (2017) vertaili maisterin opinnäytteessään nigerialaisten huijausviestien kielenpiirteitä aitojen pankkiviestien kieleen. Forensisen kielentutkimuksen avulla hän pystyi osoittamaan Nigeriassa käytetyn englannin kielen vaikutuksen huijausviesteissä. Hän huomasi myös, että syntaktisten rakenteiden avulla luotiin uhkaava tunnelma. (Nlebedum 2017: 101–102.) Tietojenkalasteluviestejä ja muita huijausviestejä on tutkittu kyllä lingvistiikan näkökulmasta suhteellisen pitkään kansainvälisesti. Esimerkiksi Martin Gill on tutkinut sitä,

[1] Roosa Rentola (2017) selvitti Poliisiammattikorkeakoulun opinnäytteessään, mitä forensinen lingvistiikka on, miten alaa on hyödynnetty ulkomailla ja Suomessa ja miten sitä voitaisiin hyödyntää tulevaisuudessa enemmän. Oma pro gradu -tutkielmani (N.N.), johon tämä teksti perustuu, tarkasteli tietojenkalasteluviestien kielenpiirteitä, vastaanottajaan vaikuttamisen keinoja ja sitä, millä perusteilla viestien vastaanottajat tekivät päätelmiä viestien luotettavuudesta. Harri Uusitalo (2019) hyödynsi forensisen lingvistiikan menetelmiä tutkiessaan Aitolahden koodeksiin sisältyvää lainsuomennosta. Annukka Junni tutki pro gradu -tutkielmassaan (2020) forensisen kääntäjän toimijuutta rikostutkinnassa. Forensiseen lingvistiikkaan perehtynyt ja alaa harjoittava erityisasiantuntija Ulla Tiililä on käsitellyt forensista kielentutkimusta Kielikellossa (Tiililä 2014).

miten autenttisuus saavutetaan nigerialaiskirjeissä. Tutkimuksensa perusteella hän loi listan ominaisuuksista, jotka vaikuttavat siihen, tulkitaanko teksti autenttiseksi eli luotettavaksi. Ominaisuudet ovat johdonmukaisuus, määrä, spontaanius, vakuuttavuus ja sopivuus sekä sitoutuminen. (Gill 2013: 413–415.)

Tutkimukset ovat osoittaneet, että tietojenkalasteluviesteillä on joitakin tyypillisiä yhteisiä piirteitä, vaikka viestit olisivat taiten tehtyjä. Esimerkiksi kalasteluviestien vastaanottajaa ei yleensä tervehditä nimellä, vaan häntä puhutellaan yleisesti, kuten *Arvoisa asiakas.* Myös lähettäjän tiedot ovat usein epämääräisiä ja epätäsmällisiä, eikä viestistä selviä välttämättä lainkaan, kuka lähettäjä on ja miten häneen voidaan olla yhteydessä. Hyvänkin viestin kielenkäyttö on usein horjuvaa. (Fincher & Hadnagy 2015: 13, 23.)

Tietojenkalasteluviesteissä on yleensä linkkejä, jotka eivät liity väitettyyn lähettäjään tai aiheeseen. Joskus viestin kaikki linkit ovat epäluotettavia, ja toisinaan luotettavien linkkien sekaan on piilotettu vain yksi huijaussivuston linkki. (Fincher & Hadnagy 2015: 13, 26.) Huijaussivustolle vievä linkki voidaan myös muokata näyttämään virallisen sivuston linkiltä (Myers 2007: 17). Viestien uskottavuutta lisätään joskus käyttämällä aitoja tavaramerkkejä, logoja ja kuvia vastaamaan väitetyn lähettäjän visuaalista ilmettä (Fincher & Hadnagy 2015: 13, 26).

Yritysten käyttämillä palomuureilla, salausohjelmilla ja tunnistamisen muodoilla ei lopulta ole paljonkaan merkitystä, jos tietokoneen käyttäjä lankeaa huijaukseen (Hong 2012: 74). Tietojenkalastelijat pyrkivätkin heikentämään vastaanottajan arviointikykyä herättämällä tunteita, kuten pelkoa tai innostusta. Tunnereaktioita voidaan voimistaa esimerkiksi esiintymällä auktoriteettina tai asettamalla aikarajoja toiminnalle. (Fincher & Hadnagy 2015: 15, 64; Ozkaya 2018, 102.)

Aineiston esittely ja sen käsittelyn kuvaus

Tutkimukseni hyödyntää kahta aineistoa. Aineistojen avulla tarkastelin sitä, millaista tietojenkalasteluviestien kieli on, miten vastaanottajaan yritetään vaikuttaa ja millä perusteella suomenkielinen vastaanottaja tekee päätelmiä viestien aitoudesta. Ensimmäinen aineistoni koostuu sähköpostitse lähetetyistä tietojenkalasteluviesteistä. Toinen osa on tuotettu kommenteista, joita vapaaehtoiset vastaajat kirjoittivat heille lähettämieni aitojen ja huijausviestien pohjalta. Seuraavaksi kerron tarkemmin aineistonkeruusta ja sen käsittelystä.

Tarkastelin vuosina 2018–2019 sähköpostitse lähetettyjä tietojenkalasteluviestejä, joita sain Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksesta (65 viestiä), S-Pankilta (16 viestiä), Nordealta (10 viestiä), Verohallinnolta (3 viestiä) ja yksityishenkilöiltä (27 viestiä). Kyberturvallisuuskeskukselta saadut viestit olivat aiheiltaan monipuolisia, sillä heille ilmoitetaan kaikenlaisista tietoturvaloukkauksista. Pankit ja Verohallinto taas olivat saaneet asiakkailtaan viestejä, joiden väitetty lähettäjä oli kyseinen organisaatio. Yksityishenkilöt lähettivät minulle itse vastaanottamiaan ja huijausviesteiksi tulkitsemiaan sähköpostiviestejä sosiaalisessa mediassa julkaisemani ilmoituksen vuoksi. Kaiken kaikkiaan sain yli 120 suomenkielistä tietojenkalasteluviestiä, joiden pohjalta muodostui 53 viestin tutkimusaineisto. Rajasin aineistosta lomakkeet, vahvasti visuaalisuuteen nojaavat viestit ja viestit, joissa oli niin vähän tekstiä, että tekstianalyysi ei olisi ollut järkevää tai mahdollistakaan. Lisäksi poistin aineistostani kaikki tuplakappaleet, joita oli eri lähteistä saamieni viestien joukossa. Koska tietojenkalasteluviestejä lähetetään usein massoille, on luonnollista, että eri tahoiltakin saaduissa viesteissä on runsaasti päällekkäisyyksiä.

Lopullinen tietojenkalasteluviestiaineistoni koostui 37 pankkien nimissä lähetetystä, kahdesta Verohallinnon nimissä lähetetystä, yhdeksästä Office 365 -palvelussa levinneestä ja viidestä muusta tietojenkalasteluviestistä. Tutkimusmenetelmäksi valikoitui aineistolähtöinen sisällönanalyysi, joka ohjasi tekstien systemaattiseen ja objektiiviseen tarkasteluun (Tuomi & Sarajärvi 2018: 104–105). Luin tietojenkalasteluviestejä tarkastellen niiden rakennetta, sanastoa, tyyliä, tunnelmaa ja sisältöä. Viestien välillä oli monia yhteisiä piirteitä, joita niputtamalla loin yläkategorioita löydöksilleni. Tarkastelin viestejä verraten niiden kieltä sekä suomen yleiskielen normeihin että luonnollisiin normeihin. Erittelin ja analysoin tietojenkalasteluviesteistä sitten suomen yleiskielen normien vastaisuuksia eli kielioppinormien vastaisuuksia, tarkastelin toistuvia kielellisiä piirteitä, joista teoriakirjallisuuskin luokitteli useimmat kalasteluviestien ominaispiirteiksi ja analysoin keinoja, joilla viestin vastaanottajaan yritettiin vaikuttaa. Erottelin löydökset aineistosta, luokittelin ne ja nimesin niiden perusteella ylä- ja alakategoriat.

Analyysini kahdeksi yläkategoriaksi muodostui *normeista poikkeava kieli tietojenkalasteluviesteissä* ja *vaikuttamisen ja vakuuttamisen keinot tietojenkalasteluviesteissä*. Normeista poikkeavat piirteet määrittelin löydösten perusteella viideksi alakategoriaksi: 1) kielioppinormeista poikkeaminen, 2) huomioita lauserakenteista ja puhuttelusta, 3) omituiset ja virheelliset sanavalinnat, 4) tyylinvaihto ja asiaankuulumaton sisältö, 5) sisällölliset ristiriidat ja muut huomiot. Vaikuttamisen ja vakuuttamisen keinot

määrittelin viiteen alakategoriaan: 1) auktoriteettiin vetoaminen, 2) seuraus ja houkutus, 3) hoputtaminen, 4) muunlainen painostava tunnelma, 5) tulevan yhteydenoton valmistelu.

Vertasin löydöksiäni keskenään sekä määrällisin että laadullisin keinoin. Tarkastelin löydöksiä sitä vasten, mitä yleiskielen ja virkakielen normeista ja konventioista on kirjoitettu (mm. Hiidenmaa 2000 & 2005; Lauerma toim. 2012; Tiililä 2015), millaiset suomen kielioppinormit ovat ja mitä suostuttelusta ja käyttäjän manipuloinnista (engl. *social engineering*) on kirjoitettu (mm. Cialdini 2013; Fincher & Hadnagy 2015; Jokinen 2016).

Tietojenkalasteluviestien lisäksi tarkastelin sitä, mihin suomenkieliset lukijat kiinnittävät huomiota pohtiessaan viestien aitoutta. Lähetin 23 vapaaehtoiselle vastaajalle viisi viestiä, joista kolme oli huijausviestejä ja kaksi luotettavia, aitoja viestejä. Vastaajat tiesivät, että osa viesteistä oli aitoja ja osa huijausviestejä, mutta he eivät tienneet huijausviestien jakaumaa, vaan yrittivät itse miettiä, mitkä viesteistä olivat huijausviestejä ja millä perusteella. Liitin kaikki tarkasteltavat viestit sähköpostiviestiin, johon kirjoitin ohjeet (liitteet 1–6). Tehtävänä oli kuvailla, mikä viesteissä herätti epäilyn tai toisaalta vakuutti sen aitoudesta. 23 vastaajan kommenteista syntyi aineisto, jossa perusteltiin viestien aitoutta tai vilpillisyyttä. Vastaajina oli sekä lähipiirini henkilöitä että heidän kauttaan saavutettuja ihmisiä. Vastaajien syntymävuodet ja koulutustaustat vaihtelivat suuresti.

Esimerkkianalyysi tietojenkalasteluviestin piirteistä

Seuraavaksi esittelen yhden esimerkin tietojenkalasteluviestistä käymällä läpi sen kielellisiä piirteitä ja vaikuttamisen keinoja. Tässä esimerkkitapauksen läpikäynnissä hyödynnän myös Martin Gillin (2013: 413–415) mallia. Tietokonevälitteiseen viestintään liittyy muita medioita enemmän epävarmuutta viestien tarkoitusperistä, mahdollisesta rikollisesta toiminnasta ja haittaohjelmien lataamisesta. Gill on tutkinut sitä, miten autenttisuus saavutetaan nigerialaiskirjeissä ja huomannut, että autenttisuuteen vaikuttavat johdonmukaisuus, määrä, spontaanius, vakuuttavuus ja sopivuus sekä sitoutuminen. Määrällä Gill tarkoittaa, että jos jokin asia toistuu tarpeeksi usein muuttuen kaavamaiseksi, se menettää autenttisuuden vaikutelmansa. Esimerkiksi ylikorostettu vakuuttelu ja ylitsepursuava kiittely vähentävät viestin uskottavuutta. Myös huijausviestien lukumäärä vaikuttaa niiden tulkintaan. Jos vastaanottaja saa yhden odottamattoman viestin tuntemattomalta, vaikuttaa se autenttisemmalta kuin, jos hän saa lukuisia samalla rakenteella tehtyjä viestejä. Spontaanius vahvistaa vilpittömyyden vaikutelmaa. Kun viestijä joutuu yllättävään tilanteeseen, hänen

uskotaan reagoivan suunnittelemattomasti ja näin ollen rehellisesti. Huijausviestien lähettäjä voi vaikuttaa rehelliseltä, jos hän esimerkiksi paljastaa itsestään tai yrityksestään jotakin arkaluontoista. Vakuuttavuus ja sopivuus tarkoittavat Gillin mukaan sitä, miten viestissä sanotaan asioita ja miten sopiva vaikkapa viestintäkanava on suhteessa väitettyyn lähettäjään. Sitoutuminen liittyy vuorovaikutukseen, jossa lähettäjäkeskeisyyden sijaan keskitytään vastaanottajaan niin, että syntyy vuorovaikutuksellinen ja sitouttava suhde. (Emt.: 413–415.)

Käyn seuraavaksi läpi valitsemani tietojenkalasteluviestin piirteitä ja vaikuttamisen keinoja. Esimerkkitapauksen jälkeen, seuraavassa luvussa, täydennän kokonaiskuvaa tietojenkalasteluviesteistä esittelemällä aineistoni muiden viestien piirteitä. Kerron myös lyhyesti tutkimusaineistoni toisen osan muodostavista kommenteista ja niiden pohjalta tekemistäni huomioista.

Käyn Nordean nimissä lähetetyn tietojenkalasteluviestin läpi rivi riviltä huomioiden myös Gillin (2013: 413–415) mallia. Kalasteluviestiä lähetettiin ainakin alkuvuodesta 2019. Se on kirjoitettu hyvällä suomen kielellä, eikä se erotu yhtä räikeästi aidosta asiakasviestinnästä kuin monet tökerömmät kalasteluviestit, mikä tekee siitä mielenkiintoisen tarkastelukohteen. Olen lisännyt rivinumerot havaintojen esittämisen helpottamiseksi.

1 Hyvä asiakas

2 Nordea:n asiakkaana on tärkeää olla tietoinen palveluitamme ja tuotteitamme koskevista
3 muutoksista. Haluamme tarjota asiakkaillemme mahdollisimman turvallisen virtuaalisen
4 ympäristön.

5 Tarkastus osoittaa, että useista sähköpostiviesteistä huolimatta käytät edelleen vanhentuneella
6 tekniikalla varustettua korttia.

7 **Hae uutta korttia**
8 Sinulla on mahdollisuus hakea uutta korttia ilmaiseksi 25.7. asti. Tämän päivämäärän jälkeen
9 veloitamme jokaisesta uudesta kortista 19,99.

10

11 Hae uutta korttia klikkaamalla tästä.

12

13 **Ehkäise petoksia**
14 Koska olemme viime aikoina altistuneet korttipetoksille, olemme päättäneet kehittää uuden
15 kortin ennaltaehkäisevässä tarkoituksessa.

16 Uusi kortti täyttää tiukemmat turvallisuusvaatimukset ja antaa sinulle mahdollisuuden käyttää
17 uusia ominaisuuksia.

18 Oletamme näin ollen, että olet tietoinen tästä asiasta.

19

20 Ystävällisin terveisin
21 Nordea

Viestin väitetty lähettäjä on pankki, joka on auktoriteettiasemassa viestin vastaanottajaan – asiakkaaseen – nähden. Viestin muodollinen rakenne on selkeä. Se alkaa ja päättyy asialliseen tervehdykseen, se on jaettu napakoihin kappaleisiin ja sisältää aiheeseen johdattelevat alaotsikot. Viestin keskelle sijoitettu linkki (r. 11), joka veisi tietojenkalastelusivulle, on peitetty suomenkielisen virkkeen alle.

Viesti alkaa kohteliaalla – joskin tietojenkalasteluviesteille tyypillisesti kohdistamattomalla – tervehdyksellä. Ensimmäisessä virkkeessä (r. 2) on viestin ainoa kielioppivirhe eli turhaan kaksoispisteillä taivutettu *Nordea:n*. Kyseisellä kirjoitustavalla voi olla myös käytännöllinen peruste. Kaksoispisteen edelle voidaan vaihtaa helposti toisen yrityksen nimi, jos viestipohjaa halutaan käyttää uudestaan. Virke (r. 2) vetoaa myös vastaanottajan velvollisuudentuntoon. Sen sijaan, että pankki kertoisi haluavansa tiedottaa muutoksista, se esittää, että on asiakkaan tehtävä olla tietoinen muutoksista. Puhuttelun epäsuorasti syyllistävä tyyli ei sovi väitettyyn lähettäjään – samoin kuin ei sovi sekään, että viestintäkanavana on sähköposti. Gillin (2013: 414–415) esittelemä sopivuus horjuu jo viestin alussa ja heikentää autenttisuuden vaikutelmaa.

Viestin toinen virke (r. 3–4) antaa ymmärtää, että viestissä on kyse virtuaalisen ympäristön turvallisuudesta. Koska viestin väitetty lähettäjä on pankki, virtuaalisen ympäristön voidaan olettaa tarkoittavan esimerkiksi verkkopankkia tai muuta pankkiasiointia verkossa. Seuraavassa kappaleessa (r. 5–6) puhe kääntyy kuitenkin korttiin. Kortilla voi toki maksaa verkossa, mutta se, miten uusi tekniikka tekisi asioinnista turvallisempaa, jää kertomatta. Tietojen puutteellisuus ja ristiriitaisuus heikentävät viestin johdonmukaisuutta ja siten uskottavuutta (Gill 2013: 413–414). Samalla viesti jatkaa vastaanottajan velvollisuudentuntoon vetoamista ja siirtyy sinuttelemaan vastaanottajaa. Nordea sinuttelee asiakkaitaan virallisessa viestinnässään (ks. www.nordea.fi), mutta puhuttelun muuttaminen kesken viestin tekee virkkeestä erityisen painokkaan. Vastaanottajassa herätetään epäilys omaa toimintaansa kohtaan: vastaanottaja on laiminlyönyt pankkiasioittensa hoitoa jo pitkään.

Seuraavaksi, riveillä 8 ja 9, luodaan tietojenkalastelulle tyypillinen kiireentuntu. Vastaanottajaa hoputetaan toimimaan nyt, kun se on vielä ilmaista. Ilmoitetun hinnan perästä puuttuu valuuttayksikkö. Vaikka kortin maksullisuus voi kummastuttaa, myöhemmin tilattavan kortin hinta on melko maltillinen ja näin ollen jopa uskottava. Gillin (2013: 414)

mukaan liioittelu heikentää autenttisuuden vaikutelmaa, joten maltillisuus voi vaikuttaa vilpittömältä. Viesti jatkaa tyypillisen tietojenkalasteluviestin kaavaa ja kehottaa seuraavaksi vastaanottajaa klikkaamaan linkkiä. Linkki on peitetty tekstillä, joka on samalla kehotus (r. 11).

Linkin jälkeen viesti perustelee vielä uuden kortin käyttöönottoa. Lähettäjä paljastaa, että pankki on altistunut viime aikoina petoksille (r. 14–15). Tässä käytetään hyväksi Gillin (2013: 414) esittämää spontaaniutta. Lähettäjä paljastaa itsestään arkaluontoista tietoa ja näyttäytyy yllättäen haavoittuvana ja avoimen rehellisenä. Uuden kortin on määrä ehkäistä tulevia petoksia, mutta sen enempää petoksista kuin kortin uusista ominaisuuksistakaan ei kerrota (r. 16–17). Viestin viimeinen virke (r. 18) ohjaa ajatukset jälleen vastaanottajan velvollisuuksiin. Vain asiakas voi tehdä päätöksen toiminnasta, ja se on tehtävä nopeasti. Onko asiakas valmis ottamaan vastuun pankkiasioittensa laiminlyönnistä johtuvista petoksista?

Muita huomioita aineiston viesteistä sekä vastaanottajien päätelmistä

Yllä kuvattu Nordean nimissä lähetetty kalasteluviesti on muihin aineistoni viesteihin verrattuna yksi taitavimmin tehdyistä. Sen kieli on laadukasta, eikä se sorru liiallisuuksiin. Viesti on maltillinen lopputervehdystä myöten, vaikka vetoaakin vastaanottajan tunteisiin. Esimerkiksi Kielitoimiston ohjepankin mukaan *ystävällisin terveisin* on hyvä valinta virallisen kirjeen lopputervehdykseen. Välimerkkejäkään ei lopputervehdyksessä kuulu käyttää. (Kielitoimiston ohjepankki.) Monet tietojenkalasteluviestit ovat puhuttelussaan tökerömpiä ja kielellisesti heikompia. Seuraavaksi esittelenkin muita aineistoni viestien ominaisuuksia.

Jokaisessa aineistoni 53 tietojenkalasteluviestistä oli vähintään yksi kielivirhe. Yleisiä olivat astevaihteluun ja persoonan ilmaisemiseen liittyvät virheet, yhdyssanavirheet, kirjoitusvirheet, isoihin alkukirjaimiin ja välimerkkeihin liittyvät virheet. Osa virheitä saattaa olla tahallisia. Tietojenkalastelijat leikittelevät joskus kielellä hämätäkseen roskapostisuodattimia tai vastaanottajaa. Esimerkiksi pieneltä *l*-kirjaimelta näyttävä merkki voikin olla iso *i*-kirjain (*paypaI.com*). (Scams & swindles 2006: 188.)

Aineistoni viesteissä oli keskenään identtisiä virkkeitä ja jopa kappaleita. Osa viestien sisällöistä oli löydettävissä oikeiden pankkien tai muiden tahojen verkkosivuilta. Näin ollen voidaan olettaa, että tietojenkalasteluviestien kirjoittajat koostavat viestinsä toisinaan oikeiden

yritysten tekstien ja jo lähetettyjen tietojenkalasteluviestien pohjalta. Samat lauserakenteisiin liittyvät ongelmat toistuivat eri viesteissä. Esimerkeissä 1, 2 ja 3 on yhtenevä rakenne, vaikka sanavalinnat eroavat toisistaan jonkin verran. Virkerakenne on samankaltainen, verbien rinnastaminen ontuu samalla tavalla (*on hyväksyttävä ja päivittää*), omistusliite puuttuu *tiedot*-sanasta ja jokaisessa on sama virheellisesti yhteen kirjoitettu *ajantasalle*.

(1) Verkkopankissa tietoturvapäivitysten vuoksi verkkopalvelujen käyttäjien on hyväksyttävä päivitys ja päivittää yhteystiedot ajantasalle.

(2) S-Pankin päivityksissä järjestelmäpäivitysten vuoksi verkkopalvelujen käyttäjien on hyväksyttävä järjestelmäpäivitys ja päivittää tiedot ajantasalle.

(3) Verkkopankissa järjestelmäpäivitysten vuoksi verkkopalvelujen käyttäjien on hyväksyttävä järjestelmäpäivitys ja päivittää yhteystiedot ajantasalle.

Viestiaineiston kierrättäminen selittää luultavasti myös sen, miksi joissakin viesteissä tyyli vaihtelee huomattavasti. Useassa aineistoni viestissä kömpelö tai sekava kieli muuttui erinomaiseksi yleiskieleksi kesken viestin tai jopa kesken virkkeen. Alla oleva esimerkki (4) havainnollistaa kyseistä ilmiötä. Viestin alkuosa on kömpelö. Siinä on astevaihteluvirhe ja yhdyssanavirhe (*asiakaamme* ja *ajantasalle*), verbien rinnastaminen ei toimi (*käyttäjien on hyväksyttävä tietoturvapäivitys ja päivittää yhteystiedot*), omistusliite puuttuu (*yhteystiedot*) ja piste puuttuu virkkeiden välistä (*tästä Prosessi*). Esimerkistä kursivoitu tekstijakso taas on tyypillistä, virheetöntä virkakieltä, joka löytyy tismalleen samanlaisena Säästöpankin henkilötietojen käyttöä ja tietosuojaa käsittelevältä verkkosivulta (Säästöpankki 2019).

(4) Hyvä asiakaamme, Verkkopankissa tietoturvapäivitysten vuoksi verkkopalvelujen käyttäjien on hyväksyttävä tietoturvapäivitys ja päivittää yhteystiedot ajantasalle. Päivitä tietosi ja tee tietoturvapäivitys tästä Prosessi järjestelmän ja tietojen päivittämiseksi on tehty mahdollisimman helpoksi ja sujuvaksi.

Käsittelemme rekistereissämme kaikkien asiakkaidemme tietoja samojen käsittely- ja tietoturvaperiaatteiden mukaisesti. Kaikkien asiakkaidemme tiedot ovat esimerkiksi pankkisalaisuuden, vakuutussalaisuuden tai vastaavan salassapitovelvoitteen alaisia tietoja riippumatta siitä, onko kyse henkilö- vai yritysasiakkaasta. Tietojen luovuttaminen on mahdollista vain asiakkaan antaman suostumuksen tai lain perusteella.

Sekä alkutervehdyksen että lopetuksen suurpiirteisyys on tietojenkalasteluviesteille tyypillinen piirre (esim. Fincher & Hadnagy 2015: 13, 23). Personoimattomuus antaa kalastelijoille mahdollisuuden lähettää sama viesti massoille. Analyysissani tekemäni huomiot

tukivat ajatusta viestin personoimattomuudesta ja lähettäjää koskevien tietojen puutteellisuudesta. Myös sanavalinnat kiinnittivät huomiota. Jotkut olivat selkeästi englannin kielestä muunnettuja (*deaktivointiin*), ja osa sanavalinnoista (*sydämellisesti Nordea.fi*) pisti hämmentävästi silmään virkakielen ja asiakasviestinnän kontekstissa – etenkin, kun viestin vastaanottajaa oli juuri uhattu tilin sulkemisella. Sanavalintoihin liittyviä ristiriitoja syntyi, kun viestin aihe tai lähettäjä ei vastannut viestin sisältöä. Esimerkiksi erään pankkiviestin lähettäjäkentässä luki *Yhteystietojen päivitys*, mutta viestissä puhuttiin verkkopankin järjestelmäpäivityksestä. Toisessa aiheeksi oli kirjoitettu *Tilausvahvistus tunnuslukulaite*, vaikka viestissä vasta kehotettiin laitteen tilaamiseen – ei suinkaan vahvistettu tilausta.

Tietojenkalastelijoiden tyypillinen tavoite on, että viesti saa vastaanottajan avaamaan viestissä olevan linkin. Aineistoni viesteissä oli käytetty erilaisia vastaanottajaan vaikuttamisen keinoja. Lähes kaikkien viestien lähettäjä – esimerkiksi pankki tai Verohallinto – oli auktoriteettiasemassa vastaanottajaan nähden. Auktoriteettien pyynnöillä voidaan olettaa olevan vahva perusta. Viesteissä vedottiin monesti myös itse auktoriteettilähettäjää ohjaavaan lakiin tai direktiiviin. Pankkien nimissä lähetetyissä viesteissä perusteltiin muutoksia esimerkiksi rahanpesulailla ja PSD2-direktiivillä.

Useimmissa tietojenkalasteluviesteissä esitettiin, että ohjeiden noudattamattomuudesta seuraa jotakin ikävää. Pankkien nimissä lähetetyissä kalasteluviesteissä uhattiin yleensä pankkipalveluiden rajoittamisella tai katkaisemisella. Office 365 -palvelussa levinneiden viestien yleisin uhkaus oli sähköpostitilin menettäminen. Monesti seurauksilla pelottelu erottaa tietojenkalasteluviestit muusta viestinnästä ja voi paljastaa viestin huijaukseksi. Kalastelijat haluavatkin viestin vastaanottajan toimivan nopeasti ennen kuin hän ehtii kyseenalaistaa viestin aitoutta. Aineistoni kalasteluviesteissä painostettiin asettamalla aikarajoja ja antamalla suoria kehotuksia toimia nopeasti. Runsas kolmasosa aineistoni viesteistä sisälsi selvän aikarajan tai hoputtavan sanallisen ohjeen, kuten esimerkeissä 5 ja 6.

> (5) Jos vastausta ei vastaanoteta *48 tunnin kuluessa*, käyttöoikeutesi keskeytetään automaattisesti
>
> (6) S-Pankin internetpalvelujen käyttö edellyttää, että käyttäjä tekee päivityksen *viipymättä*.

Viidessä kalasteluviestissä rauhoiteltiin etukäteen, että kone saattaisi toimia normaalia hitaammin päivityksen jälkeen tai että luvattujen rahojen saaminen voisi kestää tavallista

kauemmin erinäisistä väitetyn normaaleista syistä johtuen. Selitysten tavoite saattoi olla se, ettei henkilökohtaisia tietoja luovuttanut uhri alkaisi epäillä tilannetta ja ryhtyisi välittömästi turvatoimenpiteisiin. Ehkä päivityslinkiksi väitettyä linkkiä painanut asiakas olikin tietämättään ladannut haittaohjelman, jonka seurauksena tietokone toimi hitaasti.

Osatutkimuksessani tarkastelin vastaanottajien päätelmiä heille lähetettyjen viestien vilpillisyydestä ja vilpittömyydestä. Keskeisin tulos oli, että kyselyyn (liite 1) vastanneet ihmiset eivät kiinnittäneet huomiota niinkään kielioppivirheisiin, vaan perustelivat päätelmiään viestien tunnelmalla ja sisällöllä. Kielivirheistä mainitsi jokaisen viestin kohdalla korkeintaan neljäsosa vastaajista. Alla olevasta taulukosta (1) näkyy, miten vastaajien päätelmät jakautuivat kunkin viestin kohdalla.

Viesti	Arveli aidoksi (lkm)	Arveli huijaukseksi (lkm)	Epäröi (lkm)
Huijaus Nordea		23	
Huijaus S-Pankki	1	17	5
Huijaus K-Market		20	3
Aito Osuuspankki	21		2
Aito K-Citymarket	23		

Taulukko 1. Vastaajien päätelmät viestien aitoudesta.

Yksi vapaaehtoisille lähetetyistä viesteistä oli tässäkin kirjoituksessa aiemmin esitelty Nordean nimissä lähetetty tietojenkalasteluviesti. Vastaajien huomion herätti erityisesti viestin kieli ja painostava sävy. Osa vastaajista kuvaili kielen matkivan virkakieltä siinä täysin onnistumatta (esimerkit 7 ja 8). Vastaajat eivät kuitenkaan osanneet eritellä sitä, mikä kielenkäytössä ei toiminut.

(7) käytetään jargon-kieltä jota pankki käyttäisi, mutta jokin tekstissä ei ole niin sujuvaa kuin aidossa viestissä

(8) Tää jotenkin yrittää imitoida sellaista lainopillista kapulakieltä, jotta vaikuttaisi jotenkin uhkaavammalta ja varmaan sitten jonkun tylyn tyylin kautta pakottaisi toimintaan.

Viisi vastaajaa kiinnitti huomiota siihen, että ilmoitetun hinnan perästä puuttui valuuttayksikkö. Suurin osa vastaajista huomautti, että viestissä painostettiin painamaan

linkkiä tietyn ajan sisällä. Vastaajien joukossa ihmeteltiin, miksi vanhentuneella tekniikalla olevan kortin vaihtaminen olisi asiakkaan vastuulla. Suurpiirteisyys ja tietojen puutteellisuus lisäsi epäuskottavuutta. Samoin kommentoitiin viestintäkanavaa – sopivampana kanavana olisi pidetty puhelimella soittamista tai viestintää verkkopankissa. Kukaan vastaajista ei veikannut Nordean nimissä lähetettyä viestiä aidoksi viestiksi, mutta sen kuvailtiin olevan tietojenkalasteluviestiksi yllättävän hyvä. Vastaajilla oli siis jonkinlainen ennakkoajatus siitä, millainen tyypillinen tietojenkalasteluviesti olisi.

Yhteenveto ja jatkotutkimuksen tarve

Vaikka aineistoni viestit olivat pääsääntöisesti ymmärrettäviä, useissa viesteissä oli vaikeaselkoisia virkkeitä ja asiaankuulumattomia tekstiosioita. Viestien välillä oli runsaasti yhteisiä tekstiosioita yksittäisistä lauseista useisiin kappaleisiin. Osa teksteistä löytyi virallisten tahojen sivuilta. Leikkaa–liimaa-tyylinen viestintä oli johtanut monesti vaikeaselkoisuuteen ja viestien sisällöllisiin ristiriitoihin.

50 viestissä oli linkki, jota viestissä ohjattiin painamaan. Linkit olivat joko sellaisenaan näkyvillä tai ne oli peitetty tekstillä tai toisella, luotettavaksi osoitteeksi naamioidulla internetosoitteella. Linkkien painamisen merkitystä voimistettiin yleensä uhkailemalla ikävillä seurauksilla. Jotta harkinnalle jäisi vain vähän aikaa, useimmissa viesteissä painostettiin nopeaan toimintaan. Kalasteluviestien väitetyt lähettäjät olivat auktoriteetteja, joiden viestinnän vaikuttavuutta saatettiin vahvistaa esimerkiksi vetoamalla lakeihin ja direktiiveihin. Kyselytutkimukseni vastaajat huomioivat herkästi viestien tunnelmaa ja yhdistivät esimerkiksi vaatimisen ja aikarajojen asettamisen nimenomaan tietojenkalasteluun. Osatutkimukseni perusteella voidaan sanoa, että tietojenkalasteluviestejä tunnistetaan melko hyvin ainakin silloin, kun niitä osataan etsiä. Vain yksi vastaaja arvioi huijausviestin aidoksi, vaikka epäröijiä olikin enemmän (ks. taulukko 1 aiemmin).

Huolimatta siitä, että jokainen aineistoni kalasteluviesti poikkesi vähintään kerran suomen yleiskielen kielioppinormeista, viestien analyysi paljasti, etteivät läheskään kaikki kalasteluviestien tuntomerkit ole puhtaasti kielellisiä. Kalasteluviestien tunnusomaisten piirteiden havaitseminen vaatii viestien tarkastelua eri konteksteissa ja ajankohtaisiin tapahtumiin verraten. Viestin vastaanottajakaan ei aina kiinnitä huomiota yksittäiseen kielivirheeseen, kuten kyselytutkimukseni osoitti.

Tietojenkalastelu – muiden verkkohuijausten joukossa – on ollut aiempaakin runsaampaa kuluneen kahden vuoden aikana, kun työskentely ja sosiaalinen toiminta on siirtynyt koronapandemian takia kokonaisvaltaisemmin verkkoon. Muun muassa Postin nimissä on lähetetty tekaistuja saapumisilmoituksia, jotka ovat ohjanneet viestin vastaanottajan aidolta näyttävälle sivulle, jolla on vaadittu verkkopankkitunnuksilla tunnistautumista (Posti 2021). Myös esimerkiksi Finnairin, pankkien ja Microsoftin nimissä on kalasteltu tietoja, joiden avulla on onnistuttu siirtämään tuhansia euroja yksityishenkilöiden tileiltä (esim. Kemppi 2021, Kärkkäinen 2021).

Suomenkielisten kalasteluviestien kieltä ja vastaanottajien päätelmiä tutkimalla saadaan tietoa, joka auttaa tunnistamaan kalasteluviestejä aiempaa tehokkaammin ja ymmärtämään, mikä saa vastaanottajan luottamaan kalasteluviestiin. Mitä paremmin ymmärretään kalasteluun lankeamisen syitä, sitä täsmällisemmin voidaan tiedottamalla ja kouluttamalla estää niihin lankeaminen. Kielenpiirteiden tutkiminen auttaa luomaan myös entistä toimivampaa automatiikkaa tietojenkalastelun tunnistamiseksi.

Lähteet

CATE, FRED H. 2007: Liability for phishing. – Markus Jakobsson & Steven Myers (toim.): *Phishing and countermeasures. Understanding the increasing problem of electronic identity theft* s. 671–686. Wiley-Interscience cop. Verkkokirja.

CIALDINI, ROBERT B. 2013: *Influence. Pearson new international edition.* Pearson Education Limited 2014.

FINCHER, MICHELE – HADNAGY, CHRISTOPHER 2015: *Phishing dark waters. The offensive and defensive sides of malicious e-mails.* Indiana: John Wiley & Sons, Inc. 2015.

GILL, MARTIN 2013: Authentication and Nigerian letters. – Susan C. Herring, Dieter Stein & Tuija Virtanen (toim.): *Pragmatics of computer-mediated communication* s. 411–436. Handbook of pragmatics 9. Berlin: De Gruyter Mouton.

HAAPANEN, MINNA 2006: Mitä tarkoittaa phishing? *Kielikello* 3/2006. Kysyttyä-palsta. https://www.kielikello.fi/-/mita-tarkoittaa-phishing- (16.4.2019)

HIIDENMAA, PIRJO 2000: Poimintoja virkakielen rekisteristä. – Vesa Heikkinen, Pirjo Hiidenmaa & Ulla Tiililä: *Teksti työnä, virka kielenä* s. 35–62. Kotimaisten kielten tutkimuskeskuksen julkaisuja 116. Helsinki: Gaudeamus.

HIIDENMAA, PIRJO 2005: Näkökulmia yleiskieleen. *Kielikello 4/2005* s. 5–11. https://www.kielikello.fi/-/nakokulmia-yleiskieleen (4.2.2019)

HONG, JASON 2012: The state of phishing attacks. *Communications of the ACM* 55 (1) s. 74–81.

JOKINEN, ARJA 2016: Vakuuttelevan ja suostuttelevan retoriikan analysoiminen. – Arja Jokinen, Kirsi Juhila, Eero Suoninen*: Diskurssianalyysi. Teoriat, peruskäsitteet ja käyttö* s. 337–368. Tallinna: Vastapaino.

JUNNI, ANNUKKA 2020: *Rikos, rangaistus ja kääntäjä jossain siellä välissä? Forensisen kääntäjän toimijuus rikostutkinnassa*. Englannin kääntämisen pro gradu -tutkielma. Helsingin yliopisto. https://helda.helsinki.fi/bitstream/handle/10138/314316/Junni_Annukka_Pro_gradu_2020.pdf?sequence=3&isAllowed=y (18.10.2020)

KEMPPI, JANIKO 2021: Älä lankea tuoreeseen Finnair-huijaukseen: ”Lähettäjän tarkoitusperiä emme varmuudella tiedä”. *Mikrobitti* 22.1.2021. https://www.mikrobitti.fi/uutiset/ala-lankea-tuoreeseen-finnair-huijaukseen-lahettajan-tarkoitusperia-emme-varmuudella-tieda/f9a04846-55e7-4543-8133-f158cf5dbeca (15.2.2021)

KIELITOIMISTON OHJEPANKKI: *Kirjeen lopetus*. http://www.kielitoimistonohjepankki.fi/ohje/147 (9.12.2021)

KÄRKKÄINEN, HENRIK 2021: Someväitteiden mukaan Vastaamo-uhrien pankkitilejä tyhjennetty – todellisuudessa kyse lienee kierosta huijauksesta Nordean ja OP:n nimissä. *Ilta-Sanomat* 1.2.2021. https://www.is.fi/digitoday/tietoturva/art-2000007776104.html (15.2.2021)

KYBERTURVALLISUUSKESKUS 2021: *TIETOTURVA NYT!* Verkkopankkitunnuksien kalastelu jyrkässä nousussa – tällä viikolla kasvua yli 70 %. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkkopankkitunnuksien-kalastelu-jyrkassa-nousussa-talla-viikolla-kasvua-yli-70 (2.12.2021)

LAUERMA, PETRI 2012: Kieli. – Vesa Heikkinen, Eero Voutilainen, Petri Lauerma, Ulla Tiililä & Mikko Lounela (toim.): *Genreanalyysi – tekstilajitutkimuksen käsikirja* s. 51–54. Helsinki: Gaudeamus Oy.

MYERS, STEVEN 2007: Introduction to phishing. – Markus Jakobsson & Steven Myers (toim.): *Phishing and countermeasures. Understanding the increasing problem of electronic identity theft* s. 1–29. Wiley-Interscience cop. Verkkokirja.

NLEBEDUM, CHISOM JOSEPH 2017: *Dear valued customer: A forensic-linguistic analysis of scam texts.* Master’s thesis. University of Lagos, Nigeria. https://www.academia.edu/37276641/Dear_Valued_Customer_A_Forensic_Linguistic_Analysis_of_Scam_Texts (20.3.2021)

N.N.

OZKAYA, ERDAL 2018: *Learn social engineering.* Packt Publishing 2018. E-kirja: an O’Reilly Media Company 2019.

POSTI 2021: Postin nimissä liikkeellä huijausviestejä – älä reagoi, älä klikkaa yllättäviä linkkejä, katso myös Poliisin ohjeet. *Postin tiedote* 29.1.2021. https://www.posti.fi/fi/asiakastuki/tiedotteet/20201008_huijausviestitiedote (15.2.2021)

RENTOLA, ROOSA 2017: *Forensinen lingvistiikka. Kielentutkimuksen hyödyntäminen esitutkinnassa ja tuomioistuimessa*. Poliisiammattikorkeakoulun opinnäytetyö.

SALMI-TOLONEN, TARJA 2008: Forensista lingvistiikkaa – kielentutkimuksen juridisia sovelluksia. – Richard Foley, Tarja Salmi-Tolonen, Iris Tukiainen & Birgitta Vehmas (toim.): *Kielen ja oikeuden kohtaamisia. Heikki E.S. Mattilan juhlakirja* s. 375–394. Helsinki: Talentum.

SCAMS & SWINDLES 2006: *Scams & swindles. Phishing. Spoofing. ID theft. Nigerian advance schemes. Investment frauds. False sweetheart. How to recognize and avoid financial rip-offs in the internet age.* Silver Lake Publishing.

SÄÄSTÖPANKKI 2019: *Henkilötietojen käyttö ja tietosuoja.* https://www.saasto-pankki.fi/fi-fi/pankit-ja-konttorit/avain-saastopankki/yhteystiedot/henkilotietojen-kaytto-ja-tieto-suoja (2.10.2019)

TABRON, JUDITH L. 2016: *Linguistic features of phone scams: A qualitative survey*. 11th annual symposium of information assurance (ASIA '16). https://www.academia.edu/27716708/Linguistic_Features_of_Phone_Scams_A_Qualitative_Survey (26.3.2021)

TIILILÄ, ULLA 2014: Verbaaliset sormenjäljet – kielentutkimus huijausten ja rikosten tutkinnassa. *Kielikello* 4/2014. https://www.kielikello.fi/-/verbaaliset-sormenjaljet-kielentutkimus-huijausten-ja-rikosten-tutkinnassa (24.3.2021)

TRAFICOM 2019: *Tietoturvan vuosi 2018.* Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Julkaistu 5.2.2019. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan_vuosi_%2018_aukeamat.pdf (3.10.2019)

TRAFICOM 2020: *Tietoturvan vuosi 2019.* Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Julkaistu 19.2.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_tietoturvanvuosi_2019_WEB_aukeamittain.pdf (8.10.2020)

TRAFICOM 2021: *Tietoturvan vuosi 2020.* Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Julkaistu 11.2.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf (18.8.2021)

TUOMI, JOUNI – SARAJÄRVI, ANNELI 2018: *Laadullinen tutkimus ja sisällönanalyysi.* 3. laitos. Tammi.

UUSITALO, HARRI 2019: *Tausta, tekijä ja kieli. Filologinen tutkimus Aitolahden koodeksin lainsuomennoksesta.* Väitöskirja. Turun yliopiston kieli- ja käännöstieteiden laitos.: http://urn.fi/URN:ISBN:978-951-29-7669-0 (24.3.2021)

UUSITALO, MINNA 2019: *Kalasteluviestintä ilmiönä ja kiireellisyyden kokemuksen vaikutus huijauksen onnistumiseen.* Pro gradu -tutkielma. Jyväskylän yliopiston informaatioteknologian tiedekunta. http://urn.fi/URN:NBN:fi:jyu-201903181889 (10.4.2021)

LIITTEET

Liite 1

Moi!

Tässä on liitteenä viisi sähköpostia. Ensin ohjeistus:

- Kuvittele, että olet kyseessä olevan pankin tai kaupan asiakas.
- Viiden viestin joukossa on sekä aitoja viestejä että huijausviestejä. Lue viestit ja kerro, mitkä viesteistä vaikuttavat huijausviesteiltä, mitkä aidoilta ja **miksi**. Kuvaile hieman, **mikä viestissä herättää epäilysi tai toisaalta vakuuttaa sen aitoudesta**. Sinun ei tarvitse osata analysoida tekstiä sen kummemmin. Voit esimerkiksi merkata kokonaisen virkkeen ja sanoa, että se tuntuu oudolta.
- Linkit (sekä aidot että huijaussivustojen) on poistettu, jotta tekisit päätelmäsi muihin asioihin liittyvien havaintojen perusteella.
- Vastaanottajien sähköpostiosoitteet ja nimet on poistettu tai muokattu muotoon ”Xxxxx Xxxxx” anonymiteetin takia. Myös lähettäjien sähköpostiosoitteet ja viestien otsikot on poistettu, koska niitä ei ollut kaikissa viesteissä siinäkään vaiheessa, kun sain ne analysoitavakseni.

Liite 2

Hyvä asiakas

Nordea:n asiakkaana on tärkeää olla tietoinen palveluitamme ja tuotteitamme koskevista muutoksista. Haluamme tarjota asiakkaillemme mahdollisimman turvallisen virtuaalisen ympäristön.

Tarkastus osoittaa, että useista sähköpostiviesteistä huolimatta käytät edelleen vanhentuneella tekniikalla varustettua korttia.

Hae uutta korttia
Sinulla on mahdollisuus hakea uutta korttia ilmaiseksi 25.7. asti. Tämän päivämäärän jälkeen veloitamme jokaisesta uudesta kortista 19,99.

Hae uutta korttia klikkaamalla tästä.

Ehkäise petoksia
Koska olemme viime aikoina altistuneet korttipetoksille, olemme päättäneet kehittää uuden kortin ennaltaehkäisevässä tarkoituksessa.

Uusi kortti täyttää tiukemmat turvallisuusvaatimukset ja antaa sinulle mahdollisuuden käyttää uusia ominaisuuksia.

Oletamme näin ollen, että olet tietoinen tästä asiasta.

Ystävällisin terveisin
Nordea

Liite 3

Hei!

Hyvä asiakaamme,

Verkkopankissa tietoturvapäivitysten vuoksi verkkopalvelujen käyttäjien

on hyväksyttävä päivitys ja päivittää yhteystiedot ajantasalle.

Päivitä tietosi ja tee tietoturvapäivitys tästä

Prosessi järjestelmän ja tietojen päivittämiseksi on tehty

mahdollisimman helpoksi ja sujuvaksi.

Käsittelemme rekistereissämme kaikkien asiakkaidemme tietoja samojen käsittely- ja tietoturvaperiaatteiden mukaisesti.

Kaikkien asiakkaidemme tiedot ovat esimerkiksi pankkisalaisuuden,

vakuutussalaisuuden tai vastaavan salassapitovelvoitteen alaisia tietoja riippumatta siitä, onko kyse henkilö- vai yritysasiakkaasta.

Tietojen luovuttaminen on mahdollista vain asiakkaan antaman suostumuksen tai lain perusteella.

Ilman päivitystä pankkipalveluita voidaan joutua rajoittamaan.

Rajoitukset perustuvat 01.01.2018 voimaan tulleeseen uuteen rahanpesulakiin.

Rajoitukset koskevat maksukortteja ja verkkopankkia tai muuta tilin käyttöä.

Terveisin

Asiakaspalvelu

S-pankki

Liite 4

[viestin saajan nimi muutettu muotoon Xxxxx Xxxxx]

Hei Xxxxx Xxxxx,

Arvomme K-Marketin lahjakortin – osallistu kilpailuun!

Yhteistyökumppanimme järjestää arvonnan, jossa voit voittaa 1,000€ arvoisen lahjakortin K-Markettiin.

Sinun tulee vain täyttää osallistumistiedot, vastata muutamiin kysymykseen ja voitto voi olla sinun.

Tähän kilpailuun kannattaa osallistua heti, sillä palkinto arvotaan pian.

K-Marketista saat ostokset edullisesti, joten 1,000€ lahjakortilla voit ostella tuotteita mielin määrin. Saat itse päättää miten käytät lahjakortin – sen voi käyttää myös osissa.

Onko sinulla varaa jäädä tästä kilpailusta paitsi?

Osallistu kilpailuun tästä.

Liite 5

Saat uuden OP-Visa Credit/Debit-kortin

Hyvä asiakkaamme,

uudistamme luotolliset OP-Visa-korttimme varmistaaksemme, että saat jatkossakin nykyaikaisia ja monipuolisia korttipalveluita sekä maksamisen ratkaisuja. Myös sinulle on pian tulossa uusi kortti.

Ota uusi korttisi heti käyttöön

Saat uuden korttisi valitsemasi toimitustavan mukaan postitse kotiin tai konttoriin. Korttisi saapuu noin kuukauden kuluessa. Lähetämme sinulle vielä erillisen tekstiviestin, kun korttisi on matkalla. Otathan uuden kortin käyttöösi heti sen saatuasi.

OP-Visa-luottosi siirtyy uudelle kortille

Korttisi uusiutuessa uusi ja vanha korttisi näkyvät op.fi:ssä ja OP-mobiilissa. Vanhan korttisi OP-Visa-luotto ja mahdollinen avoin luottosaldo siirretään uudelle kortillesi. Uuden kortin myötä myös OP-Visa-luottosi laskutustiedot muuttuvat. Lisätietoja tästä ja korttiuudistuksestamme löydät täältä.

Ystävällisin terveisin,

OP-Korttiyhtiö Oyj

Liite 6

Hyvä asiakkaamme,

Mitä mieltä olet ruokaosastostamme? Missä asioissa olemme hyviä ja mitä pitäisi parantaa?

Olisi hienoa, jos vastaisit kyselyyn 8.9.2019 mennessä oheisella linkillä.

Osallistu napsauttamalla tätä

Kaikkien K-Citymarketien kyselyyn vastanneiden kesken arvotaan viidelle vastanneelle 20000 LisäPlussa-pistettä, joiden arvo on 100 euroa. Arvonta suoritetaan 10.9.2019 ja voittajille ilmoitetaan henkilökohtaisesti. Jos voittajaa ei tavoiteta virheellisten yhteystietojen vuoksi, arvotaan uusi voittaja. Kaikkia tietoja käsitellään luottamuksellisesti, eikä henkilötietojasi yhdistetä tutkimukseen.

Kiitos avustasi ja onnea arvontaan!

Terveisin

Marko Strand
Kauppias
K-Citymarket Tampere Lielahti

Osoitelähde: K-Plussan asiakastiedosto, Kesko Oyj, Helsinki, PL 1, 00016 Kesko, Y-0109862-8.
Tiedoston tietosuojaselosteeseen pääset tästä: https://www.plussa.com/Mika-on-K-Plussa/#Sopimusehdot

Jos et halua enää vastaanottaa kyselyitä ja tutkimuksia K-Plussalta, klikkaa sivulle https://www.plussa.com/tutkimuskielto. Mikäli sinulla on kysyttävää tästä tutkimuksesta, voit ottaa yhteyttä Plussan asiakaspalveluun chatilla osoitteessa https://www.plussa.com/asiakaspalvelu/ tai soittamalla numeroon 010 19 8604 (ma-pe 9-21, la 10-15). Puhelun hinta on pvm tai mpm.

Tämän palvelun tuottaa www.Questback.com - Questback Essentials