Tietojenkalasteluviestien kieli ja vaikuttamisen keinot

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 2007: 1). Kalastelijat esiintyvät laillisen yrityksen tai instituution työntekijänä ja käyttävät väärin tekijänoikeuden alaisia tuotteita ja tekevät identiteettivarkauksia (Cate 2007: 671–672). Tietojenkalastelu-hyökkäyksiä on tehty 1990-luvulta asti, vaikka Suomessa niitä on alkanut esiintyä vasta 2000-luvun alkupuolella (Haapanen 2006, Myers 2007: 2).

Tietojenkalastelu on rikollista toimintaa, joka saattaa koskettaa jokaista verkossa asioivaa ihmistä riippumatta siitä, millaisilla sivustoilla käy. Koska tietojenkalastelu on yleistä ja vahingollista, halusin tarkastella sitä pro gradu -tutkielmassani. Keräsin tutkielmaa 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, millä perustein suomenkielinen lukija tekee päätelmiään viestien aitoudesta. Tutkimuskysymykseni olivat seuraavat: 1) Millaisia normeista poikkeavia piirteitä sähköpostitse lähetettyjen tietojenkalasteluviestien kieli sisältää? 2) Millä keinoilla vastaanottaja yritetään saada toimimaan tietojenkalastelijan toiveiden mukaisesti? ja 3) Mihin suomenkielinen lukija kiinnittää huomiota viestin aitoutta pohtiessaan? Tutkielma sijoittuu forensisen lingvistiikan alaan, jota käsittelen myöhemmin tarkemmin.

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.

Tietojenkalastelun aiempi tutkimus ja kalasteluviestien tyypilliset piirteet

Tietojenkalasteluviestien kielen tutkiminen on rikollisen toiminnan välineenä toimivan kielen tutkimista ja näin ollen

forensista lingvistiikkaa. Forensinen lingvistiikka on yksi soveltavan oikeuslingvistiikan osa-alue (Salmi-Tolonen 2008: 376). Suomessa forensiseen lingvistiikkaan liittyvää tutkimusta on tehty toistaiseksi melko vähän.[1] Esimerkiksi englanninkielisissä maissa tutkitaan ja käytetään forensista lingvistiikkaa Suomea laajemmin. Käyttöä tukee muun muassa kielialueen suuruus.

Forensista lingvistiikkaa ei ole tutkimussuuntauksen nimeltä mainiten juurikaan hyödynnetty tietojenkalastelun tutkimuksessa, mutta yksittäistapauksia löytyy. Tabron (2016) on tutkinut huijauspuheluita forensisen lingvistiikan näkökulmasta ja esittänyt, että suljetut kysymykset, puheenaiheen kontrolloiminen ja epätarkka kerronta ovat huijauspuheluille tyypillisiä piirteitä. Nlebedum (2017) on vertaillut nigerialaisten huijausviestien kielenpiirteitä aitojen pankkiviestien kieleen ja osoittanut, miten Nigeriassa käytetty englanti vaikuttaa esimerkiksi syntaktisten piirteidensä myötä huijausviestien luonteeseen (mts. 101–102). Tietojenkalasteluviestejä ja muita huijausviestejä on kuitenkin tutkittu lingvistiikan näkökulmasta suhteellisen pitkään. Esimerkiksi Gill (2013) on tutkinut sitä, miten autenttisuuden vaikutelma saavutetaan nigerialaiskirjeissä. Tutkimuksensa perusteella hän on luonut listan ominaisuuksista, jotka vaikuttavat siihen, tulkitaanko teksti autenttiseksi eli luotettavaksi. Näitä ovat johdonmukaisuus, määrä, spontaanius, vakuuttavuus, sopivuus sekä sitoutuminen. (Mas. 413–415.)

Aiemmat 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. Parhaimmillaankin viestien kielenkäyttö on usein horjuvaa niin oikeinkirjoituksen kuin sisältöjensäkin osalta. (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. Huijaussivustolle vievä linkki voidaan myös muokata näyttämään virallisen sivuston linkiltä. Viestien uskottavuutta lisätään joskus käyttämällä aitoja tavaramerkkejä, logoja ja kuvia vastaamaan väitetyn lähettäjän visuaalista ilmettä. (Myers 2007: 17; 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.)

1. Rentola (2017) on kuvannut Poliisiammattikorkeakoulun opinnäytteessään, mitä forensinen lingvistiikka on, miten alaa on hyödynnetty ulkomailla ja Suomessa ja miten sitä voitaisiin hyödyntää tulevaisuudessa enemmän. Oma pro gradu -tutkielmani (Haapasalo 2019), johon tämä teksti perustuu, tarkasteli tietojenkalasteluviestien kielenpiirteitä, vastaanottajaan vaikuttamisen keinoja ja sitä, millä perusteilla viestien vastaanottajat tekivät päätelmiä viestien luotettavuudesta. Uusitalo (2019) on hyödyntänyt forensisen lingvistiikan menetelmiä tutkiessaan Aitolahden koodeksiin sisältyvää lainsuomennosta. Aitolahden koodeksi on käsikirjoitus, joka sisältää kuningas Kristofferin lain suomennoksen lisäksi erilaisia ruotsinkielisiä tekstejä 1600-luvulta. Junni on tutkinut pro gradu -tutkielmassaan (2020) forensisen kääntäjän toimijuutta rikostutkinnassa. Forensiseen lingvistiikkaan perehtynyt ja alaa harjoittava erityisasiantuntija Ulla Tiililä taas on käsitellyt forensista kielentutkimusta esimerkiksi *Kielikellossa* (Tiililä 2014).

Kalasteluviestit tutkimuksen aineistona

Tutkimukseni hyödyntää kahta aineistoa. Ensimmäinen aineistoni koostuu sähköpostitse lähetetyistä tietojenkalasteluviesteistä. Toinen osa on koostettu 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 vastauksena sosiaalisessa mediassa julkaisemaani ilmoitukseen. 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. Lisäksi poistin aineistostani kaikki kaksoiskappaleet, joita oli eri lähteistä saamieni viestien joukossa. Koska tietojenkalasteluviestejä lähetetään usein suurille vastaanottajajoukoille, on luonnollista, että eri tahoiltakin saaduissa viesteissä on runsaasti päällekkäisyyksiä.

Lopullinen tietojenkalasteluviesti-aineistoni 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 tarkasteluun (Tuomi & Sarajärvi 2018: 104–105). Luin tietojenkalasteluviestejä tarkastellen niiden rakennetta, sanastoa, tyyliä, tunnelmaa ja sisältöä. Tyyli voi olla asiallinen tai esimerkiksi tuttavallinen. Sisältö taas kattaa viestin aiheen ja sen, mitä sanotaan. Viestin tyyli ja sisältö synnyttävät tietynlaisen tunnelman, joka voi olla esimerkiksi uhkaava. Viestien välillä oli monia yhteisiä piirteitä, joita niputtamalla kategorioin löydöksiäni. Tarkastelin viestejä verraten niiden kieltä sekä suomen yleiskielen normeihin että sellaisiin luonnollisiin normeihin, joita vapaamuotoisempikin suomen kieli noudattaa. Erittelin ja analysoin tietojenkalasteluviesteistä sitten suomen yleiskielen normien 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* ja *vaikuttamisen ja vakuuttamisen keinot*. Normeista poikkeavat piirteet jaoin löydösten perusteella viideksi alakategoriaksi: 1) oikeinkirjoituskonventioista poikkeaminen, 2) huomioita lauserakenteista ja puhuttelusta, 3) omituiset ja virheelliset sanavalinnat, 4) tyylinvaihto ja asiaankuulumaton sisältö sekä 5) sisällölliset ristiriidat ja muut huomiot. Vaikuttamisen ja vakuuttamisen keinot jaoin viiteen alakategoriaan: 1) auktoriteettiin vetoaminen, 2) seuraus ja houkutus, 3) hoputtaminen, 4) muunlainen painostava tunnelma ja 5) tulevan yhteydenoton valmistelu.

Vertasin löydöksiäni keskenään sekä määrällisin että laadullisin keinoin. Tarkastelin löydöksiä yhtäältä suhteessa siihen, mitä yleiskielen ja virkakielen nor-

meista ja konventioista on aiemmin kirjoitettu (mm. Hiidenmaa 2000, 2005; Lauerma 2012; Tiililä 2015), ja toisaalta siihen, 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. Aidot viestit olivat itse keräämiäni viestejä minun ja läheisteni sähköpostilaatikosta ja verkkopankista. 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 vastausohjeet. Tehtävänä oli kuvailla, mikä viesteissä herätti epäilyn tai toisaalta vakuutti sen aitoudesta. Vastaajina oli sekä lähipiirini henkilöitä että heidän kauttaan saavutettuja ihmisiä. Vastaajien syntymävuodet ja koulutustaustat vaihtelivat suuresti.

Tietojenkalasteluviestien piirteistä

Seuraavaksi esittelen yhden esimerkin tietojenkalasteluviestistä käymällä läpi sen kielellisiä piirteitä ja vaikuttamisen keinoja, myös Gillin (2013: 413–415) mallia hyödyntäen. Tietokonevälitteiseen viestintään liittyy muita medioita enemmän epävarmuutta, esimerkiksi viestien tarkoitusperistä, mahdollisesta rikollisesta toiminnasta ja haittaohjelmien lataamisesta. Gillin (mas. 413) mukaan hänen tutkimiensa nigerialaiskirjeiden 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 samalla rakenteella kirjoitetut lukuisat viestit. Myös spontaanius vahvistaa vilpittömyyden vaikutelmaa: kun viestin lähettäjä esittää joutuneensa yllättävään tilanteeseen, hänen uskotaan reagoivan suunnittelemattomasti ja näin ollen rehellisesti. Edelleen huijausviestien lähettäjä voi vaikuttaa rehelliseltä, jos hän esimerkiksi paljastaa itsestään tai yrityksestään jotakin arkaluontoista. Vakuuttavuus ja sopivuus tarkoittavat Gillin mukaan sitä, miten asiat muotoillaan viestissä ja miten sopiva vaikkapa viestintäkanava on suhteessa väitettyyn lähettäjään. Sitoutuminen liittyy vuorovaikutukseen, jossa lähettäjäkeskeisyyden sijaan keskitytään vastaanottajaan niin, että syntyy vuorovaikutuksellinen ja sitouttava suhde. (Mas. 413–415.)

Käyn seuraavaksi läpi Nordean nimissä lähetetyn tietojenkalasteluviestin läpi rivi riviltä. Kalasteluviestiä lähetettiin ainakin alkuvuodesta 2019. Se on kirjoitettu sujuvalla 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)

1 Hyvä asiakas
2 Nordea:n asiakkaana on tärkeää olla tietoinen palveluitamme ja tuotteitamme koskevista muutoksista. Haluamme tarjota asiakkaillemme mahdollisimman turvallisen virtuaalisen ympäristön.
3 Tarkastus osoittaa, että useista sähköpostiviesteistä huolimatta

käytät edelleen vanhentuneella tekniikalla varustettua korttia.
4 Hae uutta korttia
5 Sinulla on mahdollisuus hakea uutta korttia ilmaiseksi 25.7. asti. Tämän päivämäärän jälkeen veloitamme jokaisesta uudesta kortista 19,99.
6
7 Hae uutta korttia klikkaamalla tästä.
8
9 Ehkäise petoksia
10 Koska olemme viime aikoina altistuneet korttipetoksille, olemme päättäneet kehittää uuden kortin ennaltaehkäisevässä tarkoituksessa.
11 Uusi kortti täyttää tiukemmat turvallisuusvaatimukset ja antaa sinulle mahdollisuuden käyttää uusia ominaisuuksia.
12 Oletamme näin ollen, että olet tietoinen tästä asiasta.
13
14 Ystävällisin terveisin
15 Nordea

Viestin väitetty lähettäjä on pankki, joka on auktoriteettiasemassa viestin vastaanottajaan eli 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. 7), joka veisi tietojenkalastelusivulle, on peitetty suomenkielisen virkkeen alle.

Viesti alkaa kohteliaalla – joskin tietojenkalasteluviesteille tyypillisellä kohdistamattomalla – tervehdyksellä. Ensimmäisessä virkkeessä (r. 2) on viestin ainoa oikeinkirjoitusvirhe eli kaksoispisteellä taivutettu *Nordea:n*. Kyseisellä kirjoitustavalla voi olla myös käytännöllinen peruste. Kaksoispisteen edelle voidaan vaihtaa helposti toisen yrityksen nimi, jos viestipohjaa halutaan käyttää uudestaan. Virke 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. 2) 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. 3) 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, rivillä 5, luodaan tietojenkalastelulle tyypillinen kiireen tuntu. 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. 7).

Linkin jälkeen viesti perustelee vielä uuden kortin käyttöönottoa. Lähettäjä paljastaa, että pankki on altistunut viime aikoina petoksille (r. 10). 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 petoksista tai kortin uusista ominaisuuksistakaan ei kerrota enempää (r. 11). Viestin viimeinen virke (r. 12) 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?

Astevaihteluvirheitä, viestien kierrättämistä ja suurpiirteisyyttä

Yllä kuvattu Nordean nimissä lähetetty kalasteluviesti on muihin aineistoni viesteihin verrattuna yksi taitavimmin tehdyistä. Se on kielellisesti taitava, 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 tietojenkalasteluviestissä oli vähintään yksi poikkeama oikeinkirjoitussäännöistä tai kielioppikonventioista. Yleisiä olivat astevaihteluun ja persoonan merkitsemiseen liittyvät kömmähdykset, yhdyssanavirheet sekä isoihin alkukirjaimiin ja välimerkkeihin liittyvät virheet. Osa virheistä 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 2–4 on yhtenevä rakenne, vaikka sanavalinnat eroavat toisistaan jonkin verran. Virkerakenne on samankaltainen, verbien rinnastaminen ontuu samalla tavalla (*on hyväksyttävä ja päivittää*), omistusliite puuttuu *(yhteys)tiedot*-sanasta, ja jokaisessa on sama virheellisesti yhteen kirjoitettu *ajantasalle*.

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

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

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

Viestiaineiston kierrättäminen selittää luultavasti myös sen, miksi joissakin viesteissä tyyli vaihtelee huomatta-

vasti. Useassa aineistoni viestissä kömpelö tai sekava kieli muuttui sujuvaksi yleiskieleksi kesken viestin tai jopa kesken virkkeen. Alla oleva esimerkki 5 havainnollistaa kyseistä ilmiötä. Edellä mainittujen ongelmien lisäksi viestin alkuosassa on astevaihteluvirhe ja virkkeiden välistä puuttuu piste (*tästä Prosessi*). Esimerkin jälkiosa taas on tyypillistä, virheetöntä virkakieltä, joka löytyy tismalleen samanlaisena Säästöpankin henkilötietojen käyttöä ja tietosuojaa käsittelevältä verkkosivulta (Säästöpankki 2019).

(5) 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). Kun viestiä ei ole suunnattu tietylle henkilölle, on kalastelijoilla mahdollisuus lähettää sama viesti suurille vastaanottajajoukoille. Analyysini vahvistaa huomiot viestien yksilöimättömyydestä ja lähettäjää koskevien tietojen puutteellisuudesta. Myös sanavalinnat kiinnittävät huomiota. Jotkut sanat 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 vastaanot-

tajan toimivan nopeasti ennen kuin tämä 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 6 ja 7.

(6) Jos vastausta ei vastaanoteta *48 tunnin kuluessa*, käyttöoikeutesi keskeytetään automaattisesti

(7) 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, minkä seurauksena tietokone toimi hitaasti.

Taulukko 1.
Vastaajien päätelmät viestien aitoudesta.

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

Toisessa osatutkimuksessani tarkastelin vastaanottajien päätelmiä heille lähetettyjen viestien vilpillisyydestä ja vilpittömyydestä. Keskeisin tulos oli, että kyselyyn vastanneet ihmiset eivät kiinnittäneet huomiota niinkään kielellisiin ongelmiin, vaan perustelivat päätelmiään viestien tunnelmalla ja sisällöllä. Kielivirheistä mainitsi jokaisen viestin kohdalla korkeintaan neljäsosa vastaajista. Pääsääntöisesti huijausviestit tunnistettiin. Taulukosta 1 näkyy, miten vastaajien päätelmät jakautuivat kunkin viestin kohdalla.

Yksi vapaaehtoisille lähetetyistä viesteistä oli esimerkissä 1 esitelty Nordean nimissä lähetetty tietojenkalasteluviesti. Vastaajien huomion herätti erityisesti viestin kieli ja painostava sävy. Osa vastaajista kuvaili kielen matkivan virkakieltä siinä täysin onnistumatta (esimerkit 8 ja 9). Vastaajat eivät kuitenkaan osanneet eritellä sitä, mikä kielenkäytössä ei toiminut.

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

(9) 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.

Painostus linkin painamiseen kielii kalasteluviestistä

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 oli peräisin 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 tunnelman 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. taulukkoa 1).

Huolimatta siitä, että jokainen aineistoni kalasteluviesti poikkesi vähintään kerran suomen yleiskielen kielioppi- tai oikeinkirjoituskonventioista, 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. *Mikrobitti* 22.1.2021; *Ilta-Sanomat* 1.2.2021).

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.

Annaleena Haapasalo
etunimi.sukunimi@tuni.fi

Kirjoittaja on Tampereen yliopiston jatko-opiskelija kielten tohtoriohjelmassa.

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. Hoboken, N.J.: Wiley-Interscience cop.

Cialdini, Robert B. 2013: *Influence. Pearson new international edition.* Harlow: Pearson Education Limited.

Fincher, Michele – Hadnagy, Christopher 2015: *Phishing dark waters. The offensive and defensive sides of malicious e-mails*. Indiana: John Wiley & Sons, Inc.

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

Haapanen, Minna 2006: Mitä tarkoittaa phishing? – *Kielikello* 3/2006. https://www.kielikello.fi/-/mita-tarkoittaa-phishing- (16.4.2019).

Haapasalo, Annaleena 2019: *Tietojenkalasteluviestit kielentutkimuksen kohteena. Klikkaa tästä! Vilpittömästi, Nordea.* Suomen kielen pro gradu -tutkielma. Tampereen yliopisto. http://urn.fi/URN:NBN:fi:tuni-201911095841.

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.

—— 2005: Näkökulmia yleiskieleen. *Kielikello 4/2005*. 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.

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

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

Junni, Annukka 2020: *Rikos, rangaistus ja kääntäjä jossain siellä välissä? Forensisen kääntäjän toimijuus rikostutkinnassa*. Englannin kääntämisen pro gradu -tutkielma. Helsingin yliopisto. http://urn.fi/URN:NBN:fi:hulib-202004211882.

Kielitoimiston ohjepankki: *Kirjeen lopetus*. http://www.kielitoimistonohjepankki.fi/ohje/147 (9.12.2021).

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.

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

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. Hoboken, N.J.: Wiley-Interscience cop.

Nlebedum, Chisom Joseph 2017: *Dear valued customer. A forensic-linguistic*

analysis of scam texts. Maisterintutkielma. University of Lagos. https://www.academia.edu/37276641/Dear_Valued_Customer_A_Forensic_Linguistic_Analysis_of_Scam_Texts (20.3.2021).

Ozkaya, Erdal 2018: *Learn social engineering.* Birmingham & Mumbai: Packt Publishing.

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

Rentola, Roosa 2017: *Forensinen lingvistiikka. Kielentutkimuksen hyödyntäminen esitutkinnassa ja tuomioistuimessa.* Opinnäytetyö. Poliisiammattikorkeakoulu. https://urn.fi/URN:NBN:fi:amk-2017060312222.

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.* Los Angeles, CA: Silver Lake Publishing.

Säästöpankki 2019: *Henkilötietojen käyttö ja tietosuoja.* https://www.saastopankki.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).

—— 2015: Mitä on asiallinen, selkeä ja ymmärrettävä virkakieli? *Kielikello* 3/2015. https://www.kielikello.fi/-/mita-on-asiallinen-selkea-ja-ymmarrettava-virkakieli- (3.10.2019).

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

Traficom 2020: *Tietoturvan vuosi 2019.* Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_tietoturvan-vuosi_2019_WEB_aukeamittain.pdf (1.3.2022).

Tuomi, Jouni – Sarajärvi, Anneli 2018: *Laadullinen tutkimus ja sisällönanalyysi.* 3. laitos. Helsinki: 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.