Arttu Perämäki

Tutkimus kalasteluhuijauksiin

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

1.9.2023

Tiivistelmä

Tekijä:	Arttu Perämäki
Otsikko:	Tutkimus kalasteluhuijauksiin
Sivumäärä:	50 sivua
Aika:	1.9.2023

Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Ohjelmistotuotanto
Ohjaajat:	Janne Salonen

Insinöörityön tarkoituksena on syventyä internetissä tapahtuviin huijauksiin. Työssä perehdytään kalastelu huijauksiin ja käydään läpi mitä niillä yritetään saavuttaa, miten sellaiset toteutetaan sekä miten sellaisilta voi suojautua.

Työn aikana rakennetaan oma kalastelu sivusto hyödyntäen useita eri työkaluja/tekniikoita ja käydään läpi miten huijaus-/kalastelusivuston voi tunnistaa.

Yhteiskunnan digitalisoituessa, myös rikollisuus on digitalisoitunut. Digitaaliset rikokset eivät välttämättä ole yhtä tuttuja ja tunnistettavia kuin reaalimaailmassa tapahtuvat. Näiden rikosten uhriksi joutuneet eivät välttämättä edes tiedä, mitä heidän tiedoillaan voitaisiin tehdä ja miten sitä voidaan väärinkäyttää.Lisäksi ”digirikollisuus kehittyy nopeasti ja toimijat kehittävät uusia tapoja hyödyntää jatkuvasti kehittyvää teknologiaa rikollisiin tarkoituksiin

Avainsanat: Kalastelu, Huijaukset, Sähköposti, Tekstiviesti

Abstract

Author:	Arttu Perämäki
Title:	A Study on Phishing Scams
Number of Pages:	50 pages
Date:	1 September 2023
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communications Technology
Professional Major:	Software Engineering
Supervisors:	Janne Salonen

This thesis dives deep into the world on internet scams. This is an investigation into the many different types of phishing scams. The overall goal is to learn as much as possible about them by going through the process of a full on phishing campaign.

During this thesis we are going to go through the process of building a phishing website, distributing it with email and trying to figure out what are the key indicators of a phishing scam.

In our modern world where almost everything is digitalized, so is crime. However the public may not be as familiar with digital crime as it's real world counterpart and scams might be more difficult to distinguish from legitimate things.

Keywords: Phishing, Scams, SMS, Email

Contents

Lyhenteet ja termit

Kalastelu:

- Huijaustyyppi, jonka tarkoitus on levittää huijausta mahdollisimman suurelle uhri kunnalle (esim. massasähköpostit, tekstiviestit yms.)

Kohdennettu kalastelu:

- Kalasteluhuijaus, joka on kohdennettu yhteen tai useaan tiettyyn yksilöön (esim. yrityksen talousosasto)

Whaling:

- Kalasteluhuijaus joka kohdistuu yritysten johtajiin tai muihin korkea-arvoisiin henkilöihin

Smishing:

- Kalastelu tekstiviesti muodossa

Seo Poisoning/Search Engine Optimisation Poisoning;

- huijaussivuston optimointi sellaisella tavalla, että se esiintyy hakukoneiden hakutuloksissa aitojen sivujen ohella ensimmäisten tulosten joukossa

Eettinen Hakkerointi:

- Laillinen ja luvallinen toiminta, jossa asiantuntija testaa ja kehittää tietojärjestelmien turvallisuutta ’hakkeroimalla’ ne

Optimointi:

- Järjestelmän tai ohjelmiston toiminnan parantamista tai tehostamista

Punainen lippu:

- Viittaa tilanteeseen, jossa ilmenee varoittavia merkkejä

Social Engineering:

- Uhrin manipulointia, tarkoituksena on uskotella uhrille, että hänen tarvitsee suostua huijarin haluamiin ehtoihin tai esim. ostaa joku palvelu

SEToolkit:

- Social Engineering Toolkit, Henkilön manipulointiin tarkoitettu työkalu

URL-Osoite:

- Uniform Resource Locator on verkkosivun osoite verkossa

HTTPS:

- Hypertext Transfer Protocol Secure on turvallinen versio HTTP-protokollasta, jota käytetään tiedon siirtämiseen netissä.

Google Translate:

- Googlen kielenkääntö palvelu

Brute Force:

- Hyökkäys jossa hyökkääjä käyttää automatisoitua ohjelmaa, joka kokeilee annettuja kirjautumistietoja usealla verkkosivulla nopeassa tahdissa.

Arkaluontoinen tieto:

- Henkilökohtaista tietoa esimerkiksi käyttäjätunnuksia, salasanoja, pankkitunnus, syntymäaika ja muita henkilötietoja tai yksityisiä dokumentteja tai kuvia.

Ai:

- Tekoäly

ML:

- Machine learning, suomeksi koneoppi

ChatGPT:

- Ilmainen internetissä oleva tekoäly työkalu

API:

- Application Programming Interface, ohjelmointirajapinta joka mahdollistaa eri ohjelmistojen toimivan yhdessä

Datasetti:

- Koneoppimismallin kouluttamista varten kerätty tiedostokansio

HTML:

- Hyper Text Markup Language on ohjelmointi kieli, jota käytetään verkkosivujen rakentamiseen

Skripti:

- Ohjelmakoodia

Ip-osoite:

- Internet Protokolla osoite, identifioi laitteen paikallisverkossa/internetissä

1 Johdanto

Yhteiskuntamme digitalisoituminen on johtanut useisiin positiivisiin kehityksiin, jotka helpottavat arkipäivän elämää. Laskut voi maksaa mobiililaitteella, etätyöskentely poistaa pitkät työmatkat, ostokset voi tehdä verkkossa, ja läheisiin on helppo pitää yhteyttä videopuheluiden, sekä viestien avulla. Vaikka digitalisoituminen vaikuttaa kaikin puolin positiiviselta, valitettavasti myös yhteiskuntamme varjopuoli on siirtynyt digitaaliseen maailmaan. Internetissä tapahtuvat huijaukset ovat kehittyneet nopeasti, mikä on huolestuttavaa. Vaikka Koronapandemia on tehnyt yhteiskunnastamme entistä digitaalisemman, ihmisten tietoisuus verkkorikollisuuden eri muodoista ei ole levinnyt samaa tahtia(9).

Tässä Insinöörityössä tarkastellaan erilaisia internetissä tapahtuvia huijauksia, pääpaino on kalasteluhuijauksissa. Työssä käydään läpi miten tälläiset huijaukset etenevät.

1.1 Huijauksista yleisesti

Huijauksien tavoitteena on yleisesti taloudellisen hyödyn saavuttaminen. Hyöty voi olla joko saada uhri maksamaan suoraan vaikka lahjakorttien muodossa tai pyrkiä saavuttamaan taloudellinen hyöty tietoja varastamalla ja edelleenmyymällä tai kiristämällä (12).

Tiedot voivat koostua pankkitunnuksista, merkkipäivistä, salasanoista, sähköpostiosoitteista tai muista henkilökohtaisista tiedoista. Varastetut tiedot eivät rajoitu vain edellä mainittuihin vaan voivat olla mitä vain tietoa mistä huijarit voivat hyötyä. Esimerkiksi videopelien käyttäjätiedot ja pelin sisäiset PIN-koodit voivat olla kalasteluhuijauksen kohteena. Monissa huijauksissa uhri ei edes huomaa tulleensa huijatuksi, eikä siksi koe tarvetta vaihtaa salasanaa tai tehdä muitakaan toimenpiteitä.

Viimevuosina Crypto huijaukset (13)ovat olleet todella suuressa nousussa, ja huijausten tekijät ovat olleet valtamediassa tunnettuja Some vaikuttajia (14). Siltikin vaikka huijausten tekijät ovat suuria julkisuuden henkilöitä, heidän rikokset usein unohtuvat ja niiden uhrit eivät saa heille kuuluvaa oikeutta. Uusia huijaustapoja kehitetään jatkuvasti ja myöskään lainsäädäntö ei pysy aina niiden perässä.

1.2 Miksi tämä aihe

Valitsin aiheekseni kalasteluhuijaukset, sillä koin niiden olevan helpoin ja yleisin huijaus. Vuonna 2022 kalasteluhuijausten määrä nousi 47.2% edellisiin vuosiin verrattuna. (15) Nettihuijaukset ovat todella mielenkiintoisia ja olen tutkinut niitä vapaa-ajallani hyvin syvällisesti. Aiemmin kuvittelin että pääosa nettihuijauksista on niin helppo tunnistaa ettei kukaan ota niitä todesta.

Asenteeni kuitenkin muuttui, kun työskentelin erään elektroniikkaliikkeen IT-tuessa, jossa työnkuvaani kuului avustaa asiakkaita heidän useiden tietoteknisten ongelmien kanssa.

Huomasin, että minulle itsestään selvät asiat saattoivat olla asiakkailleni hyvinkin vieraita. Suuri osa, etenkin vanhemmista asiakkaista eivät osanneet tunnistaa huijauksia oikeistaan ollenkaan.

Huomasin myös miten helposti asiakkaat luovuttivat henkilökohtaisia tietojansa minulle, sekä puhelimitse että kasvotusten. Tämä oli yllättävää, sillä en itse suostuisi luovuttamaan syntymäaikaa tai muita henkilökohtaisia tietojani tietämättä mitä niillä oikeasti tehdään. Olin päivittäin sellaisessa tilanteessa, missä minulla oli täysin vapaa pääsy asiakkaiden tileihin ja tietoihin.

Asiakkaiden luottamusta olisi ollut helppo väärinkäyttää ja ymmärsin miksi niin monet joutuvat erilaisten huijausten uhreiksi.

Koen että asiakkaani eivät täysin ymmärtäneet miten paljon he luovuttivat itsestään minulle ja miten arvokkaita heidän henkilötiedot ovat. Tietokoneet ja mobiililaitteet ovat usein täynnä henkilökohtaisia tietoa ja sitä ei tulisi luovuttaa kenellekään.

Toivoisin, että jokainen nettiä käyttävä olisi skeptinen ja tietoinen yleisimmistä huijauksista ja osaisi välttää niitä. Laitteita ja ohjelmistoja myyvien yritysten tulisi mielestäni valistaa asiakkaitaan netissä tapahtuvista huijauksista. Oman kokemukseni mukaan vaikuttaa siltä, että asiakkaat pelotellaan ostamaan jokin tietoturva. Samalla asiakkaale luvataan, että tietoturvaohjelmisto pelastaa heidät kaikilta mahdollisilta vaaroilta ja tämä taas voi johtaa harhaluuloihin ja liialliseen luottoon tietoturvaohjelmistoa kohtaan. Yrityksessä missä itse työskentelin, tämä oli hyvin yleistä ja asiakkaille myytiin heikosti toimiva virustorjunta ohjelmisto lupauksella, että se suojelee asiakasta kaikelta mahdolliselta. Tosiassa pelkkä virustorjunta ohjelmisto ei ole riittävä ja tämä loi asiakkaille suuria harjaluuloja. Asiakkaiden valistaminen tietoturvasta ja huijauksilta suojautumisesta jäi siis minun ja muiden It-tuessa työskentelevien vastuuksi vaikka se ei kuulunut työkuvaamme.

1.3 Insinöörityön tavoite

Insinöörityön tavoitteena mennä syvemmälle erilaisiin kalasteluhuijauksiin ja selvittää mitä niillä tavoitellaan. Huijaukset ovat yleistyneet suuresti (15) ja koen, että yhteiskuntaa ei ole tiedottu tarpeeksi netissä tapahtuvista huijauksista. Koen, että suuri osa internetin käyttäjistä ei ymmärrä miten arvokkaita heidän henkilökohtaiset tiedot ovat (16). Nettihuijarit nähdään edelleen pääosin harmittomina nörtteinä jotka istuvat tietokoneellaan, eivätkä heistä täten ole juurikaan oikeaa harmia. Mielestäni tämä on hyvin

vanhanaikainen ja vaarallinen ajattelutapa, koska internetissä tapahtuvat rikokset ovat yhtä vaarallisia kuin reaalimaailmassa tapahtuvat. Esimerkiksi pankkeihin kohdistuvalla palvelunestohyökkäyksellä voi olla jopa yhteiskunnallista merkitystä.

Insinöörityössä on tarkoitus rakentaa kalastelusivusto ja samalla dokumentoida miten tällainen kalastelu kampanja etenisi. Sivustoja ei ole tarkoitettu testattavaksi mitenkään ja ne eivät liiku kotiverkkoa pidemmälle. Koen että paras tapa oppia jokin asia on tehdä se itse. Koen että paras tapa opastaa jossakin asiassa on purkaa se pieniin osiin ja käydä ne yksitellen läpi. Tässä työssä on siis tarkoitus käydä koko kalasteluhuijauksen elinkaari läpi ja selittää sen jokainen osa erikseen.

Työn tarkoitus on opastaa miten kalasteluhuijauksen tunnistaa ja miten niiltä voi välttyä.

Työssä käydään läpi mahdollisuuksia huijausten tunnistus ohjelmistoista. Esimerkiksi tekoälymallien kouluttaminen huijaussivustojen ja viestien tunnistamiseen helppottaisi normaalikäyttäjän arkea suuresti.

2 Millaisia kalasteluhuijaukset ovat

Kalastelu hyökkäyksiä on monenlaisia (10)

1. Yleinen kalastelu

   Huijari hankkii jostain mahdollisimman laajan listan sähköposteja ja käyttää automatisoitua ohjelmaa, joka lähettää huijaus sähköpostin jokaiselle listalla olevalle. Tarkoitus on ns “heittää verkko vesille” ja katsoa millaisen saaliin tällä saa.

2. Kohdennettu kalastelu

   Huijari valitsee uhrikseen jonkin tietyn henkilön ja yrittää kerätä juuri hänen tietojaan. Näissä tilanteissa yleensä kohteena on jonkin yrityksen työntekijät ja kalasteluviestit ovat personalisoituja juuri tätä uhria varten.

3. Whaling

   Hyvin samanlainen kuin Kohdennettu kalastelu, mutta tarkoituksena on hakea ns “isoa saalista”. Nämä isot saaliit ovat usein yritysten korkea-arvoisia työntekijöitä tai muuten varakkaita yksilöitä. Esimerkiksi lähetetään perusteeton lasku yrityksen talousosastolle toimitusjohtajan nimissä juuri ennen kesälomaa ja kerrotaan että laskulla on kiire, muuten joku yrityksen toiminnan kannalta elintärkeä palvelu lakkaa toimimasta.

4. Seo Poisoning

   Eroaa muista kalastelu tavoista huomattavasti. Huijausta ei levitetä sähköpostitse vaan huijaussivu tehdään sellaiseksi, että hakukoneet ehdottavat niitä korkeammalla hakutuloksissa. Ideana tässä on se, että kun uhri etsii jotain tiettyä sivua, hän päätyy vahingossa huijaussivulle.

5. Smishing

   Hyvin samanlainen kuin Yleinen kalastelu, termi viittaa tekstiviesteihin (SMS viesti) sähköpostien sijaan

Huijauksilla voi olla useita tavoitteita, mutta kaksi yleisintä ovat (12):

1. Saada uhri luovuttamaan henkilökohtaista tietoa, kuten salasana tai sähköposti

2. Saada uhri asentamaan jokin vaarattomakski ohjelmistoksi naamioitunut haittaohjelma

Usein kalastelu huijaukset seuraavat samaa kaavaa (21).

1. Houkutellaan uhri huijaussivulle, jonkinlaisella syötillä

2. Uhri avaa sivuston ja kirjautuu tai asentaa sivulla olevan ohjelmiston

3. Huijari hyödyntää saatuja tietoja joko itse tai myymällä ne toiselle huijarille

2.1 Syötti

Kuten oikeassa kalastuksessa, kalasteluhuijaus tarvitsee syötin (7) (8). Yleisessä kalastelussa ja smishingissä syötteinä käytetään useimmiten tekstiviestejä tai sähköposteja, joiden tarkoitus on saada uhri toimimaan heti. Esimerkkejä syöteistä voivat olla sähköpostit otsikoilla 'Uusi viesti LinkedInissä, kirjaudu vastataksesi!', 'Sinut on valittu voittajaksi kilpailussa xx!' tai 'Tilauksesi on hyväksytty, kirjaudu peruuttaaksesi!'

Näille syötti viesteille on yleistä olla todella kiireisiä ja tarkoitus on saada uhrille jonkintasoinen paniikkitila, jotta hän olisi alttiimpi virheille ja huijauksille.

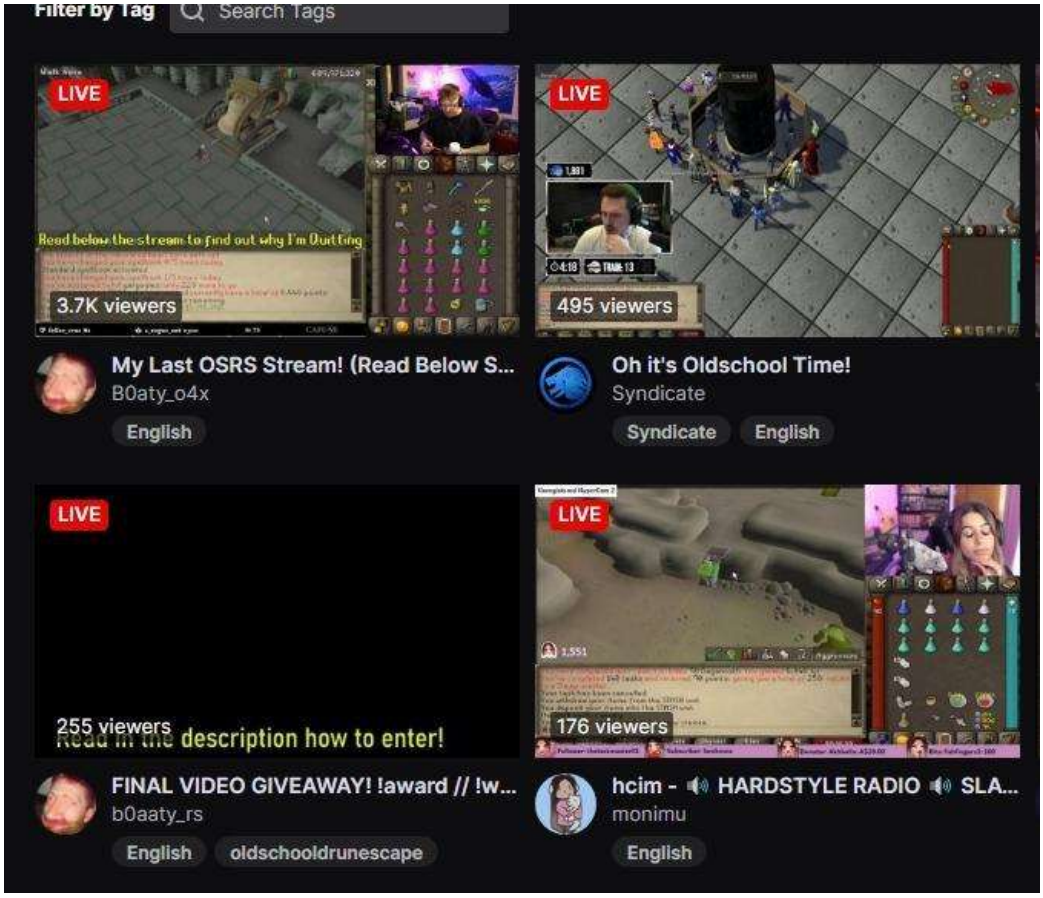
Kuvassa esimerkki Smishing huijauksesta. Huijaus esittää olevansa viesti vero hyvityksestä ja yrittää todennäköisesti urkkia uhrin pankkitietoja.(8)

Syötit eivät kuitenkaan rajoitu pelkästään tekstiviesteihin tai sähköposteihin. Kohdennetussa kalastelussa syötti voi esimerkiksi tulla puheluna, jossa huijari esiintyy yrityksen IT-tukena tai yrityksen pomona (10). Nämä huijaukset ovat vaikeampia tunnistaa, varsinkin jos huijari on saanut jotain yrityksen sisäistä tietoa, jolla hän saa uhrin luottamuksen. Näissä tilanteissa IT-tukena esiintyvä huijari voi saada uhrin asentamaan yritysten laitteille haittaohjelmia, joita huijari voi käyttää myöhemmin tiedon keräämiseen ja mahdolliseen yrityksen kiristämiseen.

Whaling-huijauksissa uhria usein lähestytään uhrille tutunu henkilön nimissä (17). Esimerkiksi uhria voidaan lähestyä työkaverin, pomon tai perheenjäsenen nimissä sähköpostitse tai sosiaalisen median kautta. Tämä tarkoittaa, että uhrin läheisen tili voidaan olla jo kalasteltu aiemmin ja sitä käytetään uhrin luottamuksen voittamiseksi. Vaihtoehtoisesti huijari luo valesähköpostin joka vaikuttaa oikealta. Whaling tarkoittaa yleisesti korkea-arvoisia työntekijöitä tai huomattavan varakkaita yksilöitä. Tämän takia huijarit ovat valmiita käyttämään niihin huomattavasti enemmän aikaa ja resursseja.

SEO Poisoning -huijauksissa huijaussivu optimoidaan niin, että hakukoneet kuten Google ja Bing ehdottavat sitä hakutuloksissaan (18). Tarkoituksena on, että uhri joka etsii jotakin tiettyä ohjelmistoa tai palvelua joutuisi vahingossa tälle huijaus sivulle lataisi haittaohjelman tai luovuttaisi arkaluontoista tietoa itsestään.

Sosiaalisen median maailmassa nämä voivat esiintyä myös huijaus live lähetyksinä, joissa huijari tallentaa tunnetun yhteisön jäsenen livelähetystä. Huijari tekee tilin, joka näyttää oikealta nopeasti katsottuna oikealta, ja laittaa lähetyksen otsikoksi joko ilmoituksen lopettamisesta, arvonnasta tai jostakin muusta huomiota herättävästä asiasta.



Kuvassa on tunnetun Old School Runescape pelin sisällöntuottaja B0atyn huijaus livelähetys. B0atyn oikea käyttäjänimi on “B0aty”, kuvassa näkyvät huijaustilit ovat käyttäjänimillä ”B0aty_o4x” ja ”b0aaty_rs”. Huijaus lähetykset ovat nopeasti katsottuna vaikea erottaa aidosta. Varsinkin uudet pelaajat voivat mennä tämän kanssa helposti sekaisin.

Huijari käyttää vanhaa lähetystä syöttinä, joka ohjaa uhrit pelin foorumi sivulta näyttävälle huijaussivulle. Sivu kalastelee uhrin käyttäjätiedot ja pelin sisäisen pankin pin-koodin. Jotkin pelin sisäiset harvinaiset esineet ovat tuhansien eurojen arvoisia pelin ’mustassa pörssissä’.

2.1.1 Social Engineering

Tämä 'syötti' -prosessi tunnetaan nimellä Social Engineering (19). Social Engineeringin tarkoituksena on huijata uhri luovuttamaan huijarille haluamaansa tietoa. Tämä voi tapahtua monilla eri tavoilla, kuten edellä mainituissa kalasteluhuijauksissa. Huijarit psykologisia temppuja, valheita tai manipulaatiota saadakseen uhrin paljastamaan arkaluontoisia tietoja, kuten salasanoja, luottokorttitietoja tai muita henkilökohtaisia tietoja mitä huijari saattaa haluttakkaan.

Keskutelin asiasta isäni kanssa, ja hänen yrityksensä työntekijät ovat olleet useiden Whaling hyökkäysten kohteena. Sain häneltä erään viestiketjun esimerkiksi ja tätä käytettiin yrityksen sisällä muiden työntekijöiden opastamiseksi. Hujauksen kohteena on Risto niminen henkilö. Viestiketjusta on poistettu oikeat sähköpostiosoitteet, sekä sukunimet ja muut tunnistettavat tiedot.

Tiedotus viesti, jonka Risto lähetti muille yrityksen työntekijöille huijauksesta. Se sisältää ohjeistuksen huijauksen tunnistamiseen ja on täydellinen esimerkki mahdollisista hälytysmerkeistä.

Moro

Kimmo TJn nimissä on tullut muutamille sähköpostia!

Kyseessä on siis jonkun huijarin tekemä sähköpostin spooffaus ja huijari tuntee meidän firman henkilöitä nimeltä. Kimmon tunnusta ei ole korkattu, vaan joku esiintyy Kimmona, ihan peruskamaa siis.

Maili on hyvä esimerkki huijausviestistä ja täyttää ison osan huijauksen tuntomerkeistä:

- Kimmo on mulle tuttu
- Huijarilla on kiire
- Huijari on kokouksessa, jolloin hänelle ei voi soittaa, vain sähköposti
- Maili tulee oudosta tsekkiläisestä osoitteesta, jopa kahdesta 😊
- Huijari ei vastaa mun esittämiin kysymyksiin
- Tekstissä on kielioppivirheitä
- Huijari haluaa taloudellista hyötyä

Lähdin huvikseni hetkeksi tuohon mukaan, alla kirjeenvaihtoa 😉

Turvallista viikkoa kaikille!

Risto

Huijauksen viestiketju:

Huijari:

From: Kimmo TJ
Sent: maanantai 8. kesäkuuta 2020 10.29
To: Risto xxxxxx<risto.Xxxxxx@Firmax.fi>
Subject: Risto

Hei Risto,

Oletko nyt saatavana?

Alkuperäinen ’syöttinä’ toimiva huijausviesti

Risto:

> Datum: 08.06.2020 10:58
> Předmět: RE: Risto
>

Moro!

Pitkästä aikaa, miten menee

Oletko lomilla vai onko sulla jotain mielessä?

Risto

Riston vastaus, huijauri esittää olevansa Ristolle vanha työkaveri.

Huijari:

From: Kimmo TJ
Sent: maanantai 8. kesäkuuta 2020 12.03
To: Risto xxxxxx<risto.Xxxxxx@Firmax.fi>
Subject: RE: Risto

tarvitsen sinua auttamaan minua ostamaan fyysisiä lahjakortteja myymälästä joillekin tietyille asiakkaille. Voitko tehdä sen 15 minuutissa? Kerro minulle, jotta voin lähettää sinulle tarvittavat tiedot lahjakorteista ja tarkan summan.

Minulla on kokous, enkä voi soittaa puheluita, jotta voimme kommunikoida sähköpostitse.

Maksan sinulle takaisin myöhemmin päivällä, mutta tarvitsen lahjakortteja heti.

Kiitos

Huijaus alkaa heti seuraavassa viestissä ja tarkoituksena on vain varastaa rahasumma käyttäen lahjakortteja (20). Viestin oikeinkirjoitus on aika ontuvaa, sekä viesti yrittä olla hyvin ammattimainen, joka korostuu vielä kun niitä vertaa Riston rentoihin vastauksiin. Huijauksessa korostetaan asian kiireellisyyttä, jonka tarkoitus on saada Risto unohtamaan mahdolliset epäilykset. Kyseessä on kuitenkin vanha kaveri, joka tarvitsee nopeasti palvelusta.

Risto:

> Komu: "Kimmo TJ"
> Datum: 08.06.2020 11:06
> Předmět: RE: Risto
>

Hmmm

Saattaisi onnistua

Oletko jossain reissussa kun tuo mailiosoite näyttää vähän oudolta 😮

Risto

Risto ei kuitenkaan usko ja tunnistaa tämän olevan huijaus.

Huijari:

From: Kimmo TJ
Sent: maanantai 8. kesäkuuta 2020 12.10
To: Risto xxxxxx<risto.Xxxxxx@Firmax.fi>
Subject: RE: Risto

Kyllä, olen matkalla.

Hanki minulle iTunes-lahjakortit, joiden nimellisarvo on 100 €.

Tarvitsen yhteensä 7 korttia. Se on 100 € X 7 = 700 €.

Raaputa korttien takaosa paljastaaksesi koodit ja lähetä sitten minulle valokuva kortista täällä sähköpostissani.

Kun olet lähettänyt koodit, älä poistu kaupasta. Minun on vahvistettava koodit ennen kuin voit poistua kaupasta.

Kerro kuinka nopeasti voit tehdä tämän.

Kiitos

Huijauksen tavoite paljastuu olevan lahjakortti huijaus(20).

Risto:

Olen koneen äärellä, joten nou hätä!

Mites noiden takaisinmaksu, milloin ja miten maksat tuon 700 euroa takaisin, tuo on aika iso summa 😲

Risto

Riston vastauksesta on selvää, että hän tunnistaa huijauksen. Hän kuitenkin päättää ’leikkiä’ huijarin kanssa ja selvittää miten huijaus etenee.

Huijari:

From: Kimmo TJ
Sent: maanantai 8. kesäkuuta 2020 12.27
To: Risto xxxxxx<risto.Xxxxxx@Firmax.fi>
Subject: RE: Risto

Palaan 700 euroa myöhemmin tänään. Kuinka haluat minun maksavan sen? Pankkisiirto?

Risto:

> Od: "Risto xxxxxx" <risto.xxxxxx@Firmax.fi>
> Komu: "Kimmo TJ"
> Datum: 08.06.2020 11:30
> Předmět: RE: Risto
>

Hyvä homma!

Mobilepay olisi varmaan nopein, jos laitat sun puhelinnumeron mulle, niin näen että summa tulee oikealta henkilöltä 😊

Risto

Huijari:

From: Kimmo TJ
Sent: maanantai 8. kesäkuuta 2020 12.35
To: Risto xxxxxx<risto.xxxxxx@Firmax.fi>
Subject: RE: Risto

Ok.

Oletko ostanut lahjakortin?

Risto:

> Od: "Risto xxxxxx" <risto.xxxxxx@Firmax.fi>
> Komu: "Kimmo TJ
> Datum: 08.06.2020 11:39
> Předmět: RE: Risto
>

En vielä, kun ruokatunti menossa, mahassa kurnii 😊

Laitatko ensin sen puhelinnumeron, meillä on ohjeistus, että näissä pitää olla tarkkana

Sitten vielä yksi juttu, tuo ensimmäinen maili tuli jostain interia.com osoitteesta, onko se sun työsähköposti?

Kunhan varmistelen

Risto

Huijari:

From: Kimmo TJ
Sent: maanantai 8. kesäkuuta 2020 12.42
To: Risto xxxxxx<risto.Xxxxxx@Firmax.fi>
Subject: RE: Risto

Mihin tarvitset puhelinnumeroa?

Risto:

> Od: "Risto Xxxxxx" <risto.Xxxxxx@Firmax.fi>
> Komu: "Kimmo TJ"
> Datum: 08.06.2020 11:44
> Předmět: RE: Risto
>

Mobilepayta varten

Voisin vaikka soitella muutenkin ja kysellä kuulumiset

Hoidetaan sitten samalla homma kuntoon?

Risto

Huijari:

From: Kimmo TJ <py77@centrum.cz>
Sent: maanantai 8. kesäkuuta 2020 12.49
To: Risto xxxxxx<risto.Xxxxxx@Firmax.fi>
Subject: RE: Risto

Lahjakortti on kuitenkin lähetettävä ensin ennen takaisinmaksua.

Osta lahjakortti ja lähetä ne täällä sähköpostilla

Viestiketju on täydellinen esimerkki erilaisista Social Engineering tekniikoista (19). Kyseinen viestiketju on kieliopillsesti todella ontuvaa, joten se on todennäköisesti tehty netissä olevillä kääntämistyökaluilla.

Näiden manipulointi tekniikkojen ymmärtäminen on hyvin tärkeä osa henkilökohtaista tietoturvaa. Tietoisuus auttaa uhreja olemaan epäileväisiä ja suojaamaan henkilökohtaisia tietojaan. Tämä on erityisen tärkeää nykyaikana, kun internetissä liikkuvat huijaukset ja identiteettivarkaudet ovat yleistyneet.

2.2 Huijaussivu

Huijaussivut ovat tehty matkimalla oikeaa kirjautumis- tai ohjelmiston asennus sivustoa (21). Esimerkiksi LinkedInin oikea kirjautumissivu ja LinkedIn huijaussivu voivat olla täysin identtisiä, eikä niissä vaikuta päälle päin katsottuna olevan mitään eroa. Huijaussivut ovat kylläkin hyvin nopeasti tehtyjä ja usein ainoat toimivat osat ovat vain kirjautumis kentät tai huijaukseen tarvittavat nappulat. Jos uhri kokeilee painaa jotakin nappulaa jolle ei ole ohjelmoitu toimintoja sivu ei reagoi mitenkään. Tämä on punainen lippu ja sivu tulee sulkea saman tien.

Usein huijaussivut antavat uhrin ”kirjautua” palveluun, jonka jälkeen sivu saattaa kysyä jotain lisätietoja: esimerkiksi puhelinnumeroa, kotisosoitetta tai syntymäaikaa. Kun sivu on saanut kaiken haluamansa tiedon, se tallentaa kerätyt tunnukset huijarin tietokantaan ja ohjaa uhrin oikealle sivulle. Lataus sivustoissa haittaohjelma asennetaan koneelle. Haittaohjelmia on monenlaisia, esimerkiksi haittaohjelma voi tallentaa kaikki tietokoneella tehdyt näppäimistön painallukset ja lähettää ne huijarille.

2.3 Kalastelun tavoite

Tavoitteet voivat vaihdella kalastelun tyypistä.

Yleisessä kalastelussa ja Smishingissä tavoitteet ovat usein kerätä uhreista mahdollisimman paljon tietoa myyntiä varten tai päästä heidän pankkitileihin käsiksi ja varastaa rahaa tätä kautta. Tämä ei tietenkään rajoitu edellämainittuihin ja kohteena voi olla useat muut tilit tai tiedot (12).

Kohdennetussa kalastelussa ja Whalingissä taas tarkoituksena voi olla jonkin yrityksen tietokantaan pääsy. Tarkoitus voi olla varastaa yrityksen asiakkaiden arkaluontoisia tietoja ja kiristää yritystä tai asiakasta. Esimerkiksi 2021 uutisoidussa Vastaamon tietovuodossa potilastietoja käytettiin uhrien kiristämiseen. Tiedot uhattiina julkaista nettiin, mikäli lunnaita ei makseta. Vastaamon tietomurtoa ei suoritettu kalasteluviesteillä, mutta se on esimerkki miten arkaluontoista tietoa voidaan käyttää jos se päätyy vääriin käsiin. (2).

3 Miten kalastusivusto tehdään

Ohjelmointi nähdään monimutkaisena ja vaikeana asiana. Moni varmasti kuvittelee, että huijaussivun tekeminen on myös todella vaikeaa tai ehkä jopa mahdotonta ilman siihen soveltuvaa koulutusta. Nämä luulot voivat johtaa siihen, että ei edes vaivauduta ottamaan asiasta selvää kun se on niin vaikeaa.

Todellisuudessa kalastelu sivuston tekeminen on hyvin helppoa. Sivustojen tekemiseen löytyy valmiita työkaluja, jotka ovat ilmaiseksi ladattavissa (4). Työkalut ovat tarkoitettu Eettiseen Hakkerointiin ja niitä ei ole tarkoitus käyttää oikeissa huijauksissa. Mikään ei kuitenkaan estä tätä ja näitä harjoitukseen tarkoitettuja työkaluja voidaan käyttää rikollissiin tarkoituksiin.

Phishing sivustojen rakentamiseen on olemassa useita eri työkaluja. Työkalut toimivat kuitenkin hyvin samanlaisesti ja niiden välillä ei juurikaan ole eroja. Työkalun asentaminen ja sivuston pystyttäminen uuten Linux käyttöjärjestelmään kestää vain muutaman minuutin.

3.1 Sivun rakentaminen

Tässä käydään läpi vaiheet ZPhisher työkalun asentamiseen ja LinkedIn huijaussivun pystyttämiseen upouudella Ubuntu asennuksella. Sama ohjeistus löytyy videomuodossa Youtube videosta ”Phishing attacks are SCARY easy to do!! (let me show you!)” (3).

1. Asenna Git Linuxin-komentorivillä seuraavalla komennolla

2. Asenna Zphisher käyttämällä git clone komentoa

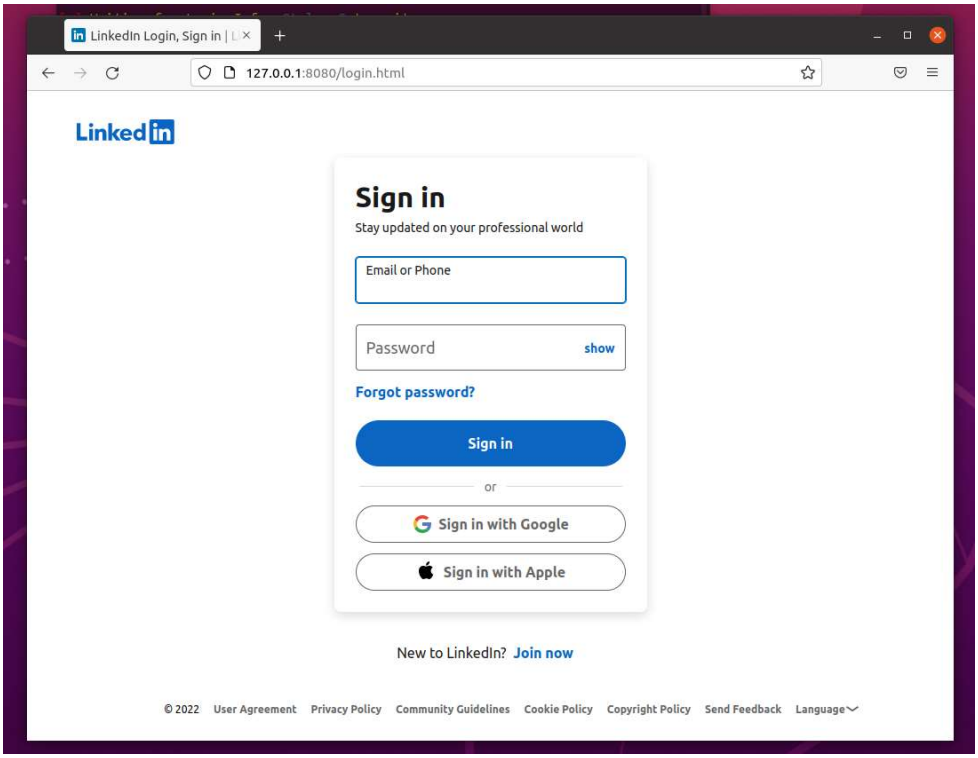
3. Vaihda hakemisto komennolla cd Zphisher

4. Käynnistä Zphisher komennolla bash zphisher.sh

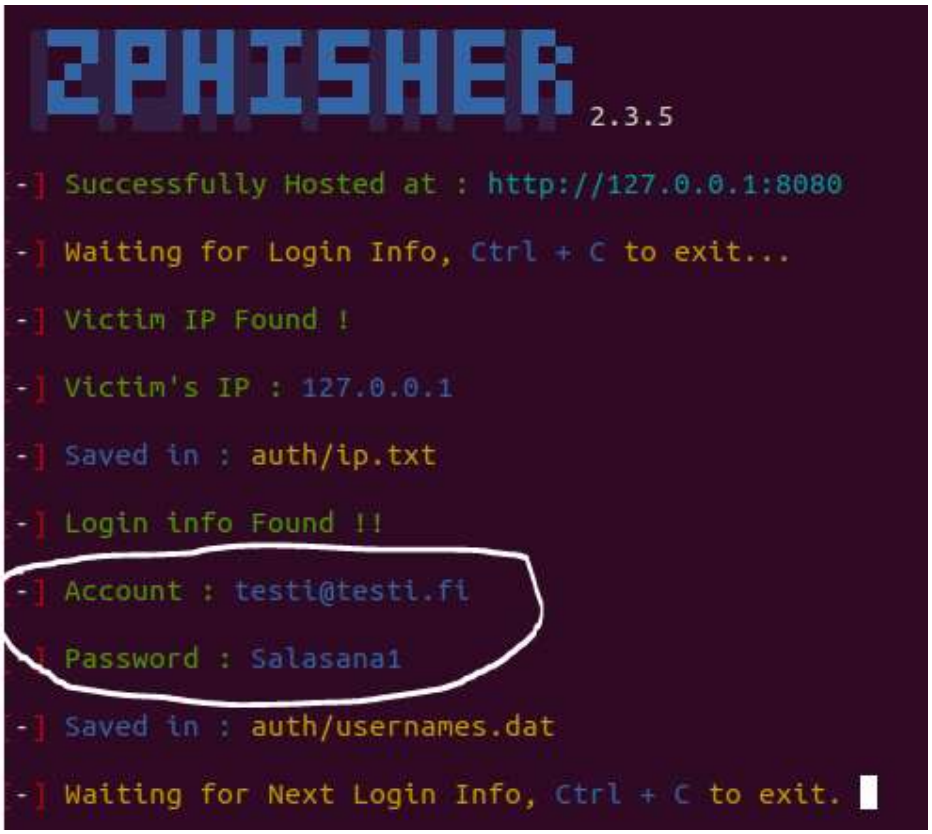
5. Zphisher on asennettu ja voimme valita LinkedInin syöttämällä 14

6. Seuraavassa vaiheessa tulee valita palvelin. Imaisia verkkosivupalvelimia ovat esimerkiksi ngrok, Cloudflared ja LocalXpose. Esimerkissä valitaan localhost.

Kohdassa “Succesfully Hosted at :” näkyy osoite josta huijaussivu on löydettävissä. Osoitteesta löytyy aidon näköinen LinkedIn kirjautumissivu. .



Jos uhri Kirjautuu tälle sivulle, niin verkkosivu ohjaa uhrin oikealla LinkedIn sivulle ja tallentaa kirjautumistiedot Linuxin komentoriviin.



Uhrin näkökulmasta sivu vain päivittyi ja pyytää salasanaa uudestaan. Mikäli uhri on asettanut selaimen muistamaan LinkedIn salasanansa niin hän kirjautuu suoraan sisään ja päällepäin tämä ei näytä poikkeavan normaalista mitenkään.

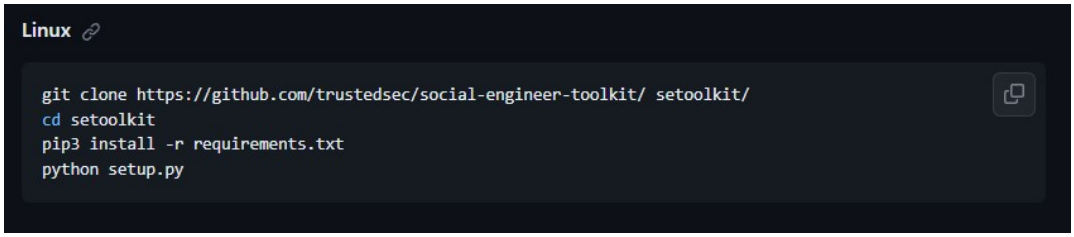
Huijauksen pystyttäminen on olemassa olevilla työkaluilla on huolestuttavan helppoa.

Vastaavanlaisia työkaluja on lukuisia ja ne kaikki toimivat hyvin samalla tavalla.

3.2 Huijauksen levittäminen

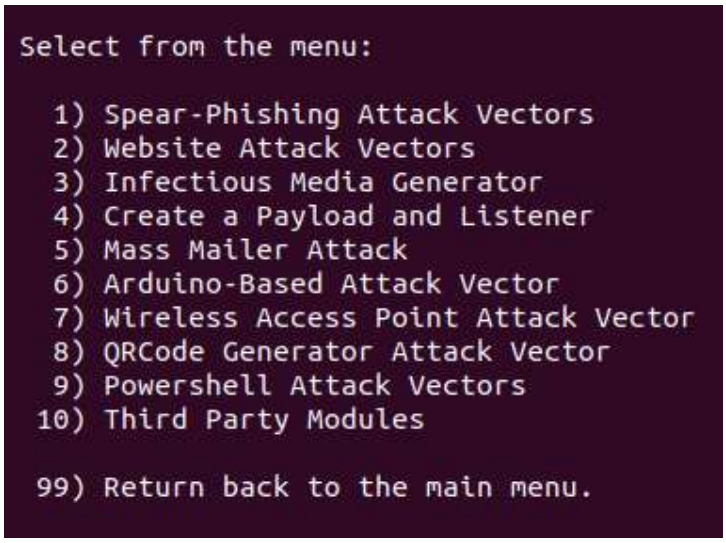
Tämä tapahtuu sähköpostin muodossa ja työkalulla SEToolkit. Vaihtoehtoisesti viestin voi lähettää normaalina sähköpostina, mutta SEToolkit automatisoi viestien lähettämisen ja voi lähettää useaan osoitteeseen viestin kerralla.

SEToolkitin asennus on hyvin samanlainen kuin Zphisherin. Linux asennukseen tarvitsee asentaa Python, mutta muuten prosessi on sama.

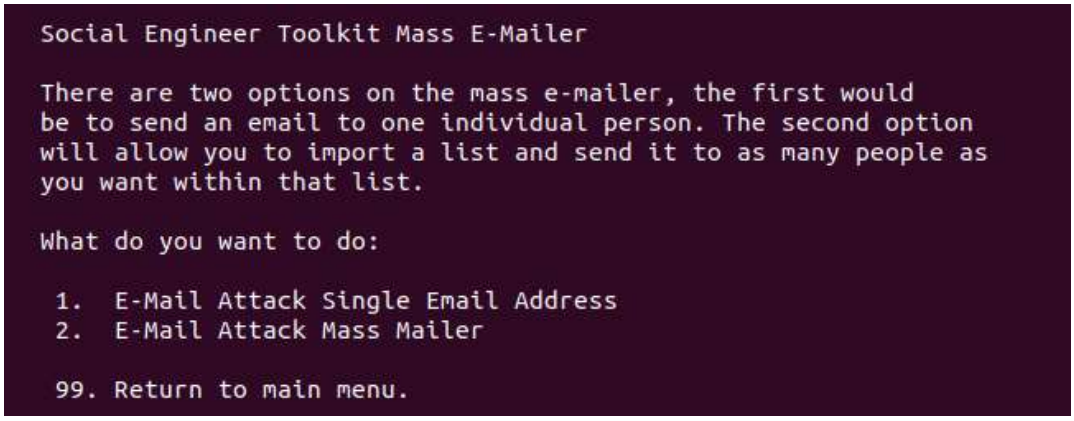


Kun SEToolkit on asennettu, tarvitsee selvittää uhrien sähköpostit. Listan sähköposteja voi vaikka löytää vanhoista tietovuodoista tai ostaa internetin ”mustasta pörssistä”. Esimerkiksi Facebookin 2021 tietovuodossa julkaistiin 533 miljoonan käyttäjän tiedot. (5).

Kun uhrien sähköpostit ovat selvillä ne voidaan syöttää SEToolkittiin. SEToolkitissä on useita vaihtoehtoja, tässä työssä valitaan Mass Mailer attack.



Seuraavaksi täytyy valita joko vaihtoehto: 1 Kohdennettu kalastelu tai vaihtoehto: 2 Yleinen kalastelu



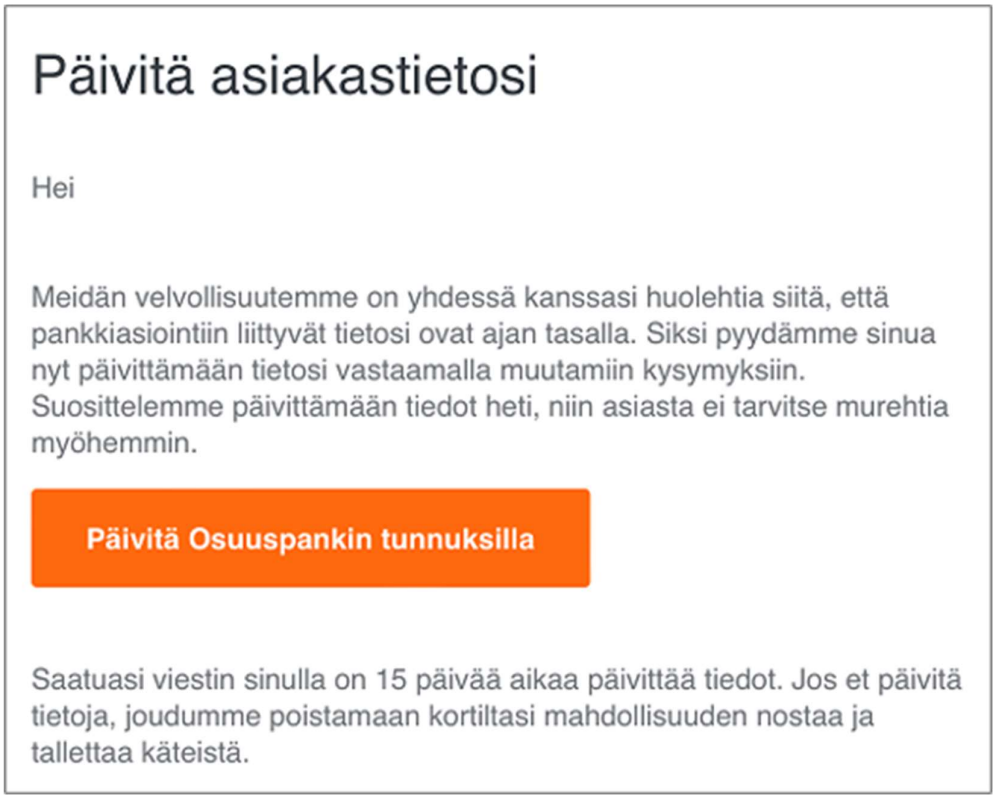
Seuraavaksi sovellus pyytää uhrin sähköpostia, Kohdennetussa hyökkäyksessä uhrin sähköposti kirjoitetaan sovellukseen, kun taas yleisessä kalastelussa sovellus lukee tekstitiedostosta sähköpostiosoitteita ja lähettää jokaiseen osoitteeseen viestin, kunnes tekstitiedosto on käyty läpi.

Tämän jälkeen ohjelmaan täytyy kirjoittaa huijaussähköposti joka lähetetään uhreille ja kirjautua siihen sähköpostiin, mistä viestit lähtevät tai valita serveri.

```
set:phishing> Send email to: arttu.peramaki@gmail.com

 1. Use a gmail Account for your email attack.
 2. Use your own server or open relay
```

Ohjelmassa on valmiita huijausviestipohjia, mutta vaihtoehtoisesti ohjelmaan voi kirjoittaa oman viestin. Tämä on suositeltavaa varsinkin jos kyseessä on kohdennettu kalastelu.



Esimerkki huijausviestin tekstisisällöstä. (7)

3.3 Edistyneemmät huijaussivut

Vaikkakin Zphisher ja muut työkalut ovat nopeita tapoja tehdä ja julkaista huijaussivustoja ne rajoittuvat vain suosituimpiin verkkosivuihin. Jos esimerkiksi haluttaisiin tehdä huijaussivu Postin nimissä se tulisi ohjelmoida käsin, sillä Zphisher sekä muut työkalut eivät sisällä Postin etusivulle valmista pohjaa.

Sivun kopiominen vie huomattavasti enemmän aikaa kuin edellämainituilla työkaluilla rakentaminen. Yksinkertaisten sivujen kopionti on tehtävissä työkaluilla kuten SaveWeb2Zip, joka tallentaa sivun Zip tiedostoon. Se ei kuitenkaan toimi monimutkaisempien sivujen kanssa, esimerkiksi postin sivua ei tällä tavalla voi kopioida.

Valmiilla työkaluilla ei myöskään voinut tehdä haittaohjelman asennus sivustoja. Tällaiset sivut tulisi huijarin ohjelmoida itse tai palkata joku ohjelmoimaan se. Toki tällaiset huijaukset vaativat myös haittaohjelman ohjelmoimisen ja ovat lähtökohtaisesti edistyneempiä ja vaativampia kuin perus käyttäjätietojen keräys sivustot.

3.4 Kerätyn tiedon väärinkäyttäminen

Kalastelu sivustojen tarkoitus on kerätä tietoa uhreista. Tätä tietoa voidaan käyttää usealla eri tavalla (1) (16).

Esimerkiksi SEO Poisoning huijauksen avulla voidaan kerätä suuri lista sähköposteja, jotka voidaa joko hyödyntää tulevassa yleisessä kalasteluhyökkäyksessä tai myydä eteenpäin mainostajille tai toisille huijareille.

Kohdistetut hyökkäykset ja Whaling hyökkäykset taas ovat usein paljon vaarallisempia. Niiden uhrina voi olla vaikka Tasavallan Presidentti ja tarkoituksena on saada asennettua hänen tietokoneelleen jokin haittaohjelma jolla huijarilla olisi pääsy koko maan arkaluontoisimpiin tiedostoihin. Tietystikkin tällaisen hyökkäyksen uhrina voi olla kuka tahansa, mutta mahdollinen vahinko on silti suuri.

Kalastelulla kerättyjä sähköposti + salasana kombinaatiota voidaan myös käyttää Brute Force hyökkäyksissä (22). Näissä hyökkäyksissä automatisoitu ohjelma kokeilee annettua sähköposti + salasana kombinaatiota usealle eri sivulle salaman nopeudella ja kirjaa ylös millä sivulle nämä käyttäjän tiedot toimivat.

Pahimmassa tapauksessa huijarit voivat käyttää keräämiään tietoja luottokorttien avaamisessa ja identiteettivarkauksissa (24).

Kerättyä tietoa voi siis väärinkäyttää usealla eri tavalla ja suurimmassa osassa tapauksista motiivi on rahallinen. Tästä syystä omasta yksityisyydestä täytyy pitää hyvin kiinni.

4 Kalastelulta suojautuminen

Kalasteluhuijauksilta suojautuminen vaatii tarkkuutta (23). Viimeaikoina huijauksia on tullut puheluiden muodoissa, tekstiviesteillä, sekä sähköpostitse ja on tärkeä olla valppaana huijausten varalta.

4.1 Kalastelu huijauksen tunnistaminen

Kalastelusivustoista pyritään tekemään mahdollisimman uskottavia, joten niiden tunnistaminen oikeista sivuista on hyvin haasteellista (21). Sivustot eivät kuitenkaan aina ole täydellisiä ja tietynlaiset virheet ovat hyvin tyypillisiä kalastelusivustoille (7).

Jos tietokone tai mobiililaite on asetettu kirjautumaan automaattisesti sivuille sisään, uuden kirjautumisen vaatiminen on yksi punainen lippu.

4.2 Virheet huijaussivussa

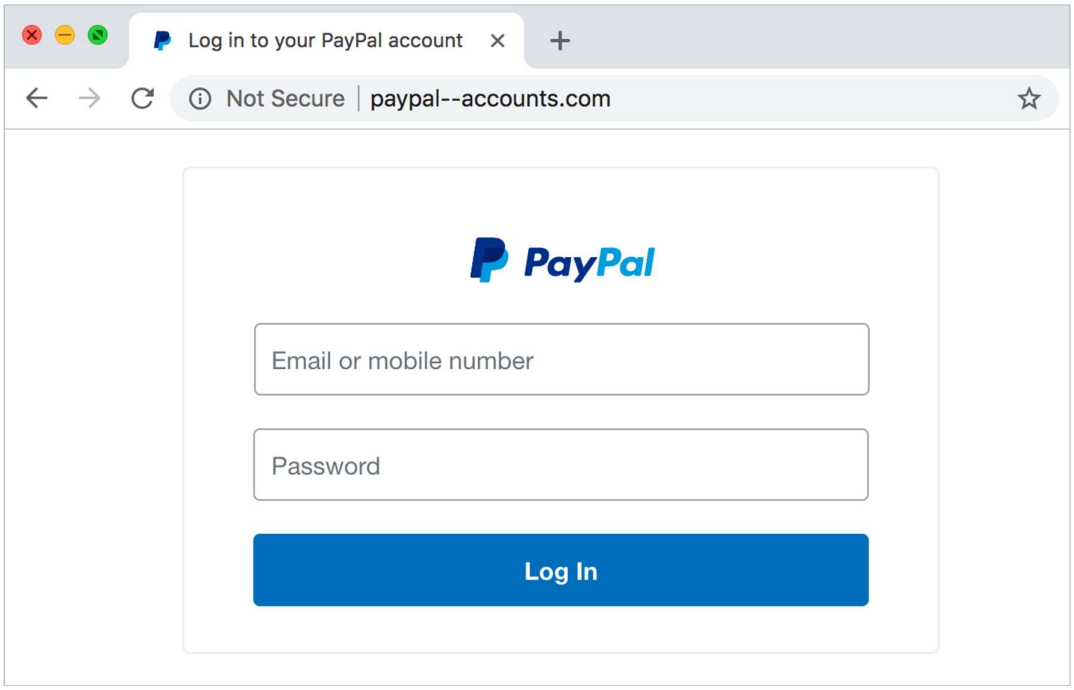
Huijaussivustot ovat tyypillisesti hyvin suppeita toiminnoiltaan. Tyypillistä huijaussivuille on se, että vain huijaukseen liittyvät asiat toimivat. Tämä tarkoittaa, että ainoat nappulat jotka reagoivat käyttäjän komentoihin ovat kirjautumis ja/tai asennus nappulat. Hyvin usein huijarit ovat kopioineet sivun ulkoasun täysin, mutta toiminnallisesti se on hyvin vajaa. Jos sivulla olevat linkit eivät reagoi minkään napin painallukseen, sivu ei todennäköisesti ole aito (21).

Toinen tyypillinen asia näissä sivuissa on se, että ne eivät tarkista kirjautumistietoja mitenkään. Näihin sivuihin voi siis ”kirjautua” täysin keksityillä tunnuksilla ja sivu etenee niin kuin mitään ei olisi tapahtunut.

Huijaussivustojen ulkoasussa saattaa myös olla virheitä. Usein kalastelusivustot pyrkivät matkimaan aitojen sivustojen ulkoasua, mutta jotkin hienovaraiset erot voivat paljastaa huijauksen. Yksityiskohdat kuten fontit, kuvat ja yleinen asettelu saattavat erottaa sivun aidosta. Jos sivu vaikuttaa epäammattimaiselta tai

eroaa jotenkin muuten viime kerrasta, se on suurella todennäköysyydellä huijaus.

Huijaussivuilla on yleensä virheellinen URL-osoite. Aitojen sivustojen URL-osoitteet ovat usein hyvin selkeitä, sekä ne käyttävät HTTPS-yhteyksiä. Jos sivun URL-osoite on epäselvä tai se ei ala ”https://” tulisi sivu sulkea samantien.



Paypalin kirjautumissivua esittävä huijaussivu. Huijauksen tunnistaa virheellisestä URL-osoitteesta. Kuten kuvasta näkyy osoitteen alusta puuttuu ”https://” sekä url osoitteessa on ylimääräisiä merkkejä. Oikea Paypalin url-osoite olisi paypal.com.

4.3 Virheet syötissä

Huijausviesteissä hyvin usein on monia punaisia lippuja (7). Aidot yritykset eivät pyydä asiakkaitaan kirjautumaan, vahvistamaan salasanojaan tai luovuttamaan muita henkiläkohtaisia tietojaan sähköpostitse. Aidot yritykset harvemmin lähettävät viestejä, jotka pelottelevat tai kiirehtivät asiakasta toimimaan nopeasti. Tällaiset hoputtavat viestit ovat jo itsessään punainen lippu ja ne kannattaa käydä läpi hyvin tarkkaan. (11)

Huijausviesteissä on myös hyvin usein kielivirheitä. Osa huijausviesteistä voi olla käännetty esimerkiksi Google Translatella ja niiden kielioppi saattaa olla hyvin ”tönkköä”.

Lähettäjän osoitteeseen tulee myös kiinnittää huomiota ja on hyvä tarkistaa aikaisempia viestejä samalta lähettäjältä ja katsoa ovatko osoitteet samat. Yleensä yrityksillä on oma sähköpostitunnus, joten jos sähköposti päätty @gmail.com tai johonkin muuhun yleiseen ilmaiseen sähköpostin päätteeseen viesti on todennäköisesti huijaus.

Turvallinen tapa varmistaa, että onko kyseessä huijaus on olla yhteydessä yritykseen josta viesti tuli. Tämä kannattaa tehdä aikaisemmilla kontakti tiedoilla, kuten puhelinnumerolla tai muulla vastaavalla tavalla. Esimerkiksi yrityksen asiakaspalveluun soittamalla saa suurella todennäköisyydellä selville, onko kyseessä aito viesti tai huijaus.

Yritysmaailmassa täytyy miettiä, että oliko tällaisesta asiasta aikaisemmin puhetta. Jos yhtäkkiä sähköpostiin ilmestyy latauslinkki, ilman että tulevista asennuksesta tai päivityksistä oli ollut mitään puhetta etukäteen, sen tulisi herättää epäilystä.

4.4 Yleisiä turvatoimenpiteitä

Yleiset turvallisuus toimenpiteet pätevät tällaistakin huijausten ehkäisemisessä (21) (23).

Helppoja tapoja turvata laite on pitää ne päivitetteynä uusimpaan versioon ja käyttää tietoturvaohjelmistoja. Useissa tietoturvaohjelmistoissa on selain lisäyksiä, jotka tunnistavat ja varoittavat huijaussivuista. Ne myös estävät epäilyttävien ohjelmistojen lataamista ja asentamista.

Hyvä tapa on käyttää useita eri salasanoja eri verkkosivuille. Tämä tarkoittaa, että jos uhrin Facebook tilin tiedot kalastellaan tällöin uhri on vain menettänyt yhden sähköposti + salasana kombinaation. Tällöin Facebook tilin salasanan vaihtaminen riittää suojaaman muut tilit tältä iskulta.

Jos taas uhri käyttää samaa sähköposti + salasana kombinaatiota usealla sivulla, hänen kaikki tilit ovat vaarassa ja hyökkäyksen aiheuttama potentiaalinen riski on huomattavasti suurempi.

Yleisesti on hyvä olla skeptinen. Vältä klikkaamista linkkejä epäilyttävissä viesteissä. Tai vältä linkkien klikkaamista ylipäätään, mikäli et tiedä 100% mistä se on peräisin. Samoin myös mikäli sähköpostiviestiin on liitettynä jotakin tiedostoja, näiden liitteiden avaamisen kanssa tulisi olla hyvin skeptinen. Haittaohjelmat voidaan naamioida harmittomiksi pdf tiedostoiksi.

Sivulla 11 olevassa viestissä selitätään huijausten useat tuntomerkit ja nyrkkisäännöt huijausten tunnistamiseksi.

4.5 Aidon viestin tunnistaminen

Ensimmäisenä kannattaa miettiä, onko asia liian hyvä ollakseen totta.

S-Ryhmän artikkelissa ”Varo S-Ryhmän tuoterkkien nimissä lähetetään huijausviestejä” (11) kerottaan, että S-Ryhmä ei koskaan vaadi asiakkaiden henkilötietotoja tekstiviesteillä tai sosiaalisessa mediassa. Artikkelissa sanotaan myös, että S-Ryhmän mahdolliset arvonnat suoritetaan vain sähköpostitse ja sellaisten asiakkaiden kanssa, ketkä ovat antaneet S-Ryhmälle markkinointiluvan.

Nämä S-Ryhmän toimenpiteet ja neuvot pätevät muihinkin yrityksiin. GDPR lakisäädösten mukaan yritykset eivät saa käyttää asiakkaiden henkilökohtaisia tietoja mainostamiseen, mikäli asiakkaat eivät ole sitä erikseen hyväksyneet. Jos kieltäytymisestä huolimatta tälläisiä arvontaviestejä tulee, ne ovat suurella todennäköisyydellä huijauksia.

5 Ohjelmistojen käyttäminen huijausten tunnistamisessa

5.1 Käytössä olevat huijausten tunnistusmenetelmät

Huijasten tunnnistamista varten on tehty useita ohjelmistoja, jotka käyttävät erilaisia tekniikoita viestin aitouden päättelyyn. Sähköpostien tunnistamiseen on käytetty erilaisia toimintoja ja ominaisuuksia(9):

a. Sähköpostin runkoon littyvät ominasuudet: Sähköpostin rungossa on ominaisuuksia, joita tunnistusohjelma voi hyötykäyttää. Rungossa on binäärisiä piirteirä, kuten sen muoto, tietynlaiset lauseet tai linkit sekä sivun HTML koodi.

b. Sähköpostin aiheeseen liittyvät ominaisuudet: Sähköpostin aiheessa olevista ominaisuuksista ohjelmisto voi päätellä viestin

aitouden. Yleisesti termit kuten ”tarkista”, ”voitto” tai ”maksu” herättävät ohjelmston huomion.

c. URL-pohjaiset ominaisuudet: Nämä ominaisuudet tarkistavat käyttääkö viestiin linkittetty URL-osoite Ip-osoitetta verkkotunnuksen sijaan.

d. Skriptipohjaiset ominaisuudet: Tässä käydään JavaScript koodi läpi ja katsotaan onko siellä pop-up ikkunakoodia, klikkaustapahtumia tai muuta hämärää joka ei ole tyypillistä.

Nämä tunnistus tekniikat ovat pääasiallisesti käytössä sähköpostipalveluiden roskapostin tunnistuksessa. Huolettavan suuri osa huijausviesteistä pääsee silti tämän tunnistuksen läpi ja se ei ehkä olekkaan kaikista tehokkain tapa tunnistamiseen.

5.2 Tekoälymallit

Viimeaikoina tekoäly on noussut suureen suosioon maailmalla. Ensimmäisiä suuria peruskuluttajan käytössä olevia tekoälymalleja oli ChatGPT. Tätä ennen on ollut useita julkisesti käytössä olevia tekoälymalleja, mutta mikään niistä ei ole noussut yhtä suureen suosioon kuin ChatGPT(25).

Tekoälymallit voidaan kouluttaa tunnistamaan melkein mitä vain. Sähköpostien tunnistaminen ja niiden sisällön lukeminen on hyvin koulutetulle tekoälymallille helppoa. Tekoälymallin kouluttaminen taas ei ole kovinkaan helppoa.

Tekoälymallin kouluttaminen alusta asti on hyvin pitkäkestoinen prosessi, sitä varten täytyy kerätä todella suuri datasetti aitoja ja huijaussähköposteja. Tämän jälkeen tekoälyä täytyy kouluttaa ja sen todenmukaisuutta täytyy tarkistaa jokaisen koulutuksen jälkeen.

5.2.1 ChatGPT

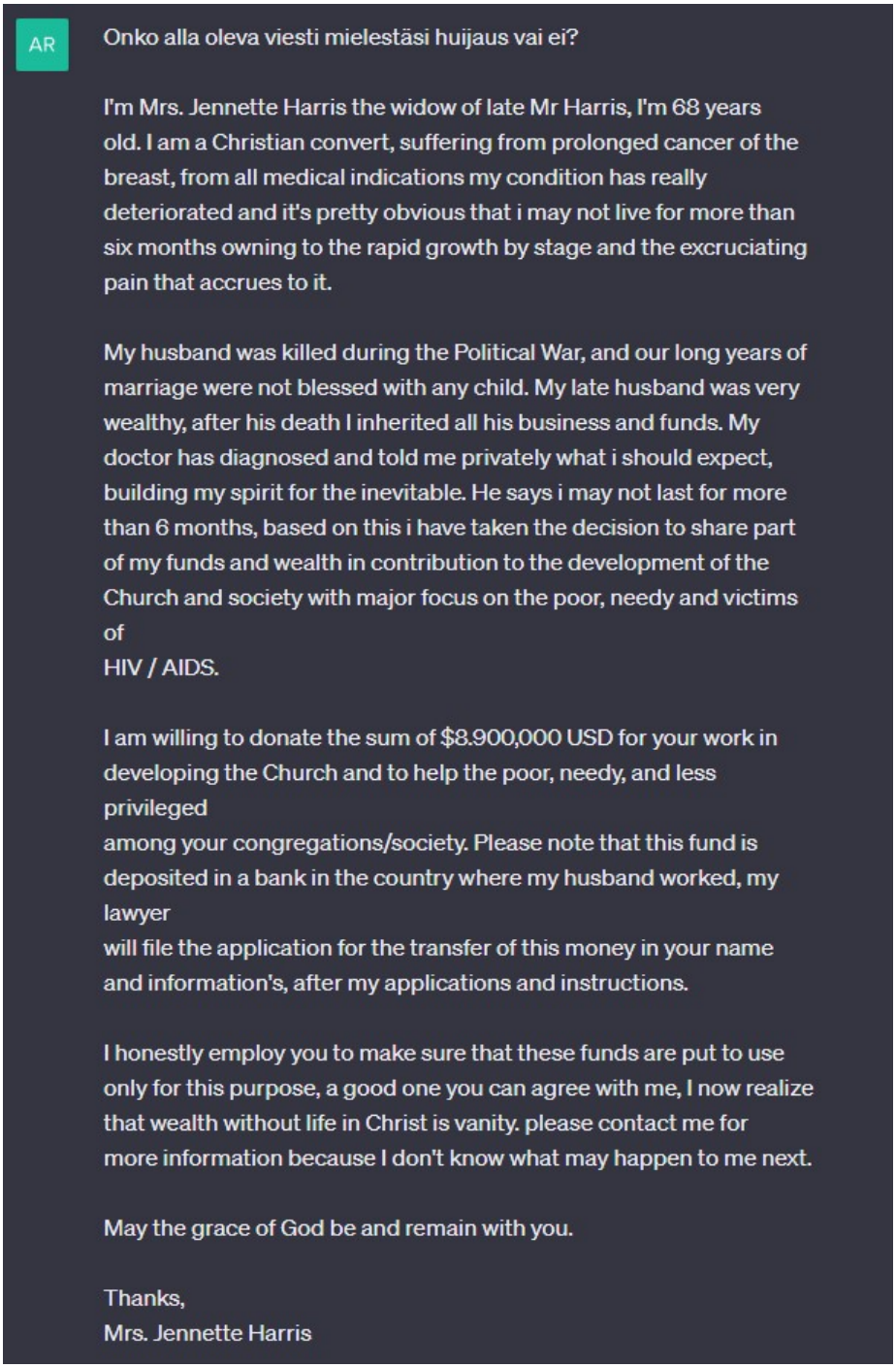
Olemassa olevia tekoälymalleja voidaan hyödyntää ja tässä tilanteessa voimme kokeilla miten ChatGPT:tä voitaisiin hyödyntää huijausten tunnistuksessa.

ChatGPT on oman määritelmänsä mukaan OpenAi:n kehittämä tekoälypohjainen keskusteluagentti. ChatGPT on syväoppimismalli, jonka kouluttamiseen on tarvitti suuria määriä erilaista tekstidataa. Lopputuloksena ChatGPT osaa vastata ”ihmismäisesti” sille lähetettyihin viesteihin (ChatGPT).

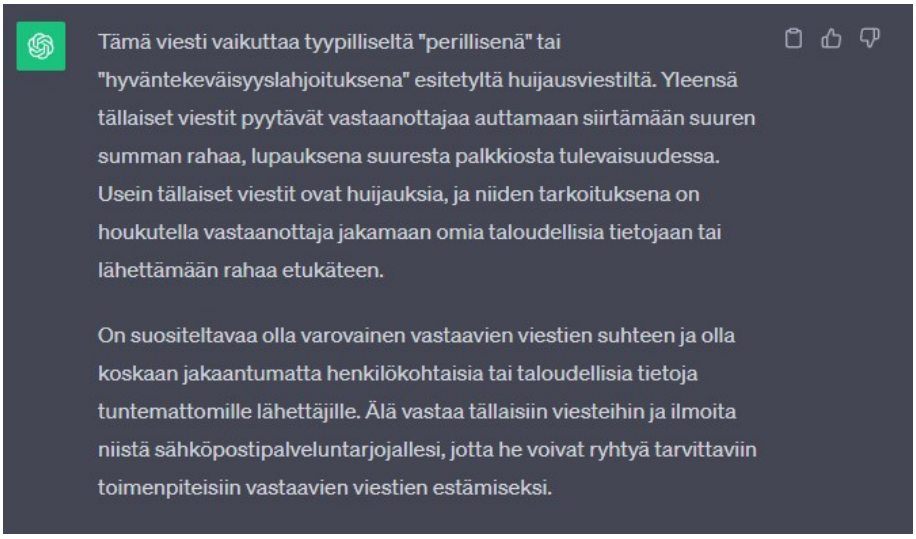
ChatGPT tunnistaa tehokkaasti kielihirveet ja osaa ehdottaa niihin mahdollisia korjauksia. ChatGPT toimii tehokkaiten englanniksi, mutta suomenkielinen versio ei ole ihan yhtä tarkka kieliopin suhteen.

Esimerkiksi ChatGPT:tä voitaisiin käyttää valmiina mallina vaikkakin sähköpostien tunnistamiseen. ChatGPT:lle on olemmassa valmis API, joka mahdollistaa ChatGPT:n yhdistämisen muihin ohjelmistoihin.

Esimerkiksi Google Chrome selaimeen voitaisiin tehdä sovellus, joka käyttäjän halutessa kopio tekstin sähköpostiviestistä ja lähettää sen ChatGPT:lle oikoluettavaksi. Tätä voidaan kokeilla lähettämällä ChatGPT:lle huijausviesti ja pyytämällä tätä kertomaan mielipiteensä.



Kalastusviestin tarkistus ChatGPT:llä (8)



ChatGPT:n vastauksesta ilmenee, että viesti on mitätodennäköisemmin huijaus. ChatGPT:tä voitaisiin siis käyttää valmiina tekoälymallina huijausten tunnistamiseen, mutta se ei välttämättä ole kaikista tehokkain tähän tarkoitukseen.

5.3 Mallin kouluttaminen

Koneoppimismallin kouluttamiseen on useita erilaisia vaihtoehtoja. Syväoppimismalleissa voidaan käyttää erilaisia algoritmeja kuten Random Forest, Decision Trees, Logistic Regression ja Support Vector Machine (8).

Näillä menetelmillä voidaan kouluttaa malleja, jotka osaavat tunnistaa kalasteluviestit suurella tarkkuudella. Mallit ovat huomattavasti tarkempia kuin aikaisemmin mainitut roskaposti filtterien ominasuudet, sillä malli analysoi koko viestin ja vertailee sitä koulutusmateriaalissa olleisiin aitoihin, sekä huijausviesteihin. Mallit siis käyvät koko viestin läpi, sen sijaan että ne tarkistaisivat vain muutaman yleisen punaisen lipun kuten avainsanat viestin aiheessa tai pop-up skriptit.

6 Yhteenveto

6.1 Alkuperäinen tavoite

Insinöörityön alkuperäinen tavoite oli rakentaa kalastelusivusto, ja siinä samalla oppia miten tämänlaiset huijaukset toimivat. Alkuperäinen tavoite oli rakentaa täysin identtinen verkkosivusto, joka näyttäisi LinkedInin kirjautumissivulta. Aluksi tarkoitus oli kokeilla kopioida sivun HTML tiedosto, sekä css tiedosto ja katsoa saisiko sen toimimaan niinkin yksinkertaisella tavalla. Olin täysin varautunut ohjelmoimaan sivun alusta alkaen itse, mikäli tämä kopiointi ei olisi toiminutkaan. Ennen ohjelmoinnin aloittamista, päätin kuitenkin tutustuttaa itseni syvällisemmin tällaisiin kalasteluhuijauksiin ja sivustojen tekemiseen.

Pian aiheeseen syventymisen jälkeen löysin nämä valmiit työkalut, sekä useita Youtube videoita joissa käytiin läpi miten huijaussivusto pystytetään. Hetken asiaan perehdyttyäni, päädyin ”Blackeye” nimiseen työkaluun. Löysin Black Eyen alunperin GitHubista. Muutama viikko työn aloittamisen jälkeen Blackeye työkalu oli kuitenkin poistunut eikä sitä enään löytynyt mistään, joten siirryin käyttämään Zphisheriä. Nämä työkalut nopeuttivat sivun rakentamista huomattavasti ja tavoitteeni muuttui sivun rakentamisesta, enemmän tutkimus luonteiseksi.

6.2 Uusi Tavoite

Valmiit työkalut nopeuttivat sivun perustamista huomattavasti ja alkuperäinen tavoite sivun ohjelmoinnista, muuttui huijausten tutkimukseksi. Nämä työkalut säästävät huomattavasti aikaa, joka olisi käytetty yhden huijaussivun ohjelmoimiseen. Yhden sivun ohjelmoimiseen olisi voinut mennä useita päiviä, mutta nämä työkalut tekivät tämän työn muutamassa minuutissa.

Tämä tarkoitti, että tutkimukselle vapautui huomattavasti enemmän aikaa. Valitettavasti tämä tarkoittaa myös sitä, että huijareilla ei kulu kovinkaan paljoa aikaa sivun perustamiseen.

Tutkiessani eri työkaluja löysin useita videoita Youtubesta, joissa opastettiin työkalujen käyttöä. Hyvin suuressa osassa näistä videoista oli linkitettynä jokin työkalu, mutta usein tämä linkki vei tyhjään Github Repositoryyn. Vaikuttaisi siltä, että Github ei halua tällaisia työkaluja heidän sivuilleen ja niitä poistetaan nopeaa tahtia.

6.3 Loppupohdinta

Vaikka maailman digitalisoituminen tuo paljon hyvää, sen mukanaan tuomaa pahaa ei pidä unohtaa. Valittavaa on se että rikollisuus ja huijaukset seuraavat yhteiskuntaa myös digitaaliseen maailmaan ja niitä on opittava välttämään myös uudessa digitaalisessa ympäristössä.

Tekoälyn kehittyessä huijausten tunnistamisesta tulee entistä helpompaa ja tämä taas turvaa internetin käyttöä ja minimoi käyttäjien omia virheitä.

Internetissä tulee siltikin olla aina valppaana ja kriittisenä aisioiden suhteen. Vanha sanonta pitää siis paikkansa, jos jokin on liian hyvä ollakseen totta se todennäköisisti ei ole.

Lähteet

1 Vastaamo data breach, Wikipedia (Luettu 5.11): https://en.wikipedia.org/wiki/Vastaamo_data_breach#:~:text=The%20company's%20security%20practices%20were,to%20exist%20until%20March%202019.

2 Oikeuden paperit paljastavat: Näin Vastaamon tietomurto tapahtui – salainen kauppasumma paljastui, MTV Uutiset: https://www.mtvuutiset.fi/artikkeli/oikeuden-paperit-paljastavat-nain-vastaamon-tietomurto-tapahtui-salainen-kauppasumma-paljastui/8055050

3 Phishing attacks are SCARY easy to do!! (let me show you!), NetworkChuck: https://www.youtube.com/watch?v=u9dBGWVwMMA

4 Top 3 Phising Tools for Ethical Hacking, Hailbytes: https://hailbytes.com/top-3-phishing-tools-for-ethical-hacking/

5 Meta fined $276 million over Facebook data leak involving more than 533 million users, TheVerge: https://www.theverge.com/2022/11/28/23481786/meta-fine-facebook-data-leak-ireland-dpc-gdpr

6 Saitko verottajalta tämän viestin hyvityksestä?, Länsiväylä: https://www.lansivayla.fi/paikalliset/4653155

7 Mistä tunnistaa huijausviestin, Op: https://www.op.fi/turvallinen-asiointi/mista-tunnistaa-huijausviestin

8 Some excellent Examples of Scam Emails: https://www.conejovalleyguide.com/welcome/some-excellent-examples-of-scam-emails.html

9 Phisihing Email Detection Using Natural Language Procesing Techniques: A Literature Survey: https://www.sciencedirect.com/science/article/pii/S1877050921011741

10 What are the different types of phishing, TrendMicro: https://www.trendmicro.com/en_za/what-is/phishing/types-of-phishing.html

11 S-Ryhmän tuotemerkkien nimissä lähetetään huijausviestejä, S-Ryhmä: https://www.s-kanava.fi/asiakaspalvelu/huijausviestit/

12 What is the goal behind phishing emails?, Graphus: https://www.graphus.ai/blog/what-is-the-goal-behind-phishing-emails/

13 FTX founder Sam Bankman-Fried is guilty of fraud, TheVerge: https://www.theverge.com/23894366/ftx-sam-bankman-fried-trial-updates-news

14 Investigating Logan Paul's Biggest Scam, Coffeezilla: https://www.youtube.com/watch?v=386p68_IDHA

15 2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year: https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year

16 Value of Data, Hewlet Packard Enterprise: https://www.hpe.com/us/en/what-is/value-of-data.html#:~:text=The%20value%20of%20data%20refers,efficiency%2C%20and%20new%20revenue%20streams.

17 How does a whaling phishing attack work? Mimecast.com: https://www.mimecast.com/content/whaling-phishing-attack/#:~:text=A%20whaling%20attack%20is%20a,transfer%20to%20a%20fraudulent%20account.

18 How Seo Poisoning Works, Check Point: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/what-is-seo-poisoning/#:~:text=SEO%20poisoning%20is%20a%20set,trust%20and%20visit%20the%20website.

19 What is "Social Engineering"?, Enisa: https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

20 Why Do Scammers Want Gift Cards?, Aura: https://www.aura.com/learn/why-do-scammers-want-gift-cards

21 What Are Scam Websites and How To Avoid Scam Websites, kaspersky: https://www.kaspersky.com/resource-center/preemptive-safety/scam-websites

22 Brute Force Attack, kaspersky: https://www.kaspersky.com/resource-center/definitions/brute-force-attack

23 Tips to Protect Yourself From Phishing Scams, Mass.gov: https://www.mass.gov/news/tips-to-protect-yourself-from-phishing-scams#:~:text=Avoid%20phishing%20scams%3A&text=Add%20spam%20filters%20to%20your,message%20you%20received%20is%20legitimate.

24 Identity Crimes, CIMIP: https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm#:~:text=This%20type%20of%20theft%20involves,possibly%20steal%20the%20user's%20identity.

25 ChatGPT sets record for fastest-growing user base – analyst note, Reuters: https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/