HUIJAUSVIESTIT JA NIIDEN VÄLTTÄMINEN

Lappeenrannan–Lahden teknillinen yliopisto LUT

Tietotekniikan kandidaatintyö

2022

Akseli Aula

Tarkastaja: TkT Jouni Ikonen

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUT Teknis-luonnontieteellinen

Tietotekniikka

Akseli Aula

Huijausviestit ja Niiden Välttäminen

Tietotekniikan kandidaatintyö

37 sivua, 7 kuvaa, 5 taulukkoa ja 1 liite

Tarkastaja: TkT Jouni Ikonen

Avainsanat: Huijausviestit, suunnittelutiede, opettavainen peli, tietoturva

Nykyajan teknologian- ja verkkojen jatkuvan kehityksen myötä verkkorikollisuus kukoistaa ja erilaisten huijausten kohtaaminen verkossa on yleistä. Myös huijauskeinot kehittyvät jatkuvasti, eikä tavanomaiset käyttäjät kykene aina tunnistamaan erilaisia huijauksia. Tähän ratkaisuna toimii tietoturvatietoisuuden lisääminen, jonka tarkoitus on muun muassa opastaa käyttäjiä tunnistamaan ja välttämään verkossa piileviä uhkia.

Yksi tämän työn tavoitteista on luoda katsaus huijausviestien tutkimukseen, ja siten selvittää erilaisia teksti- ja sähköpostiviestien välityksellä liikkuvia huijaustyylejä ja niiden piirteitä. Työn lopullisena tavoitteena on tietoturvatietoisuuden lisääminen opettavaisen pelin merkeissä.

Lopputuloksena työssä rakennettiin verkkosovellus suunnittelutieteen tutkimusmenetelmää soveltaen. Verkkosovelluksessa yhdistyy niin huijausviestisyötteiden keruu kuin itse opettavainen peli. Pelin toteutuksessa hyödynnettiin tietovisa- tyylistä lähestymistapaa, jossa käyttäjän tehtävä on tunnistaa arvotut viestisyötteet huijauksiksi tai luotettaviksi.

Valmis sovellus julkaistiin verkkoon, joka mahdollisti huijausviestisyötteiden keräyksen ja pelin laajemman testauksen. Pelin soveltuvuutta osaksi tietoturvakoulutusta arvioitiin kyselyllä, jonka perusteella yli 80 % kokivat pelin opettavaiseksi.

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

School of Engineering Science

Software Engineering

Akseli Aula

Scam Messages and Avoiding Them

Bachelor's thesis

2022

37 pages, 7 figures, 5 tables and 1 appendix

Examiner: Associate professor Jouni Ikonen

Keywords: Scam messages, design science, educational game, information security

As technology and networks continue to evolve in today's world, cybercrime is booming, and online scams are everywhere. The scams are also constantly evolving and ordinary users are not always able to identify different types of scams. One possible solution to this problem is improving information security awareness, which aims to educate users to recognize and avoid different online threats among other things.

One of the objectives of this bachelor's thesis is to provide an overview of the research regarding scam messages and thus to identify different types and characteristics of different scam text- and email messages. The main objective, however, is to raise information security awareness through an educational game.

As a final result, a web application was built applying a design science research methodology. The web application combines both the collection of scam messages and the educational game itself. The game was implemented using a quiz-style approach, where the user's task is to identify if a drawn message is scam or trustworthy.

The finished application was published online, which made possible to collect scam messages and to test and evaluate the game. The suitability of the game as a part of information security training was assessed through a survey, which indicated that more than 80 % found the game educational.

Sisällysluettelo

Tiivistelmä

Abstract

1 Johdanto ... 5
1.1 Työn tavoitteet ja rajaukset ... 5
1.2 Käytettävät tutkimusmenetelmät ... 6
1.3 Työn rakenne ... 7
2 Katsaus huijausviestien tutkimukseen ... 8
2.1 Tiedonhaku ... 9
2.2 Hakutulosten seulonta ja luokittelu ... 10
2.3 Tietojen keruu ja yhteenveto ... 12
3 Tunnistetut huijausviestityylit ja niiden välttäminen ... 14
3.1 Menetelmät huijauksien tukena ... 14
3.2 Tietojenkalastelu ... 15
3.3 Petokset ... 16
3.4 Liitetiedostot ... 17
3.5 Muut huijausviestit ... 18
3.6 Keinoja huijauksien välttämiseksi ... 19
4 Verkkosovelluksen suunnittelu, toteutus ja arviointi ... 20
4.1 Tavoitteet ja vaatimukset ... 20
4.1.1 Opettavainen peli ... 20
4.1.2 Viestisyötteiden keruu ... 22
4.2 Sovelluksen tekninen toteutus ja kehitys ... 23
4.3 Verkkopelin arviointi ... 27
5 Johtopäätökset ja yhteenveto ... 29
5.1 Johtopäätökset ... 29
5.2 Yhteenveto ... 30
Lähteet ... 32

1 Johdanto

Tänä päivänä älylaitteista on tullut arkipäivää ja lähes jokaisella on käytössään jopa useita eri älylaitteita. Joissain yhteyksissä niistä on tullut jopa välttämättömiä, elämää helpottavia laitteita, joita ilman on lähes mahdotonta tulla toimeen. Niin pankkiasiat, ostokset kuin työtkin voidaan hoitaa internetin välityksellä, eikä läsnäoloa vaativat käynnit ole enää välttämättömiä. Älylaitteet, niiden teknologia ja käyttökohteet kehittyvät jatkuvasti. Tämä avaa luonnollisesti mahdollisuuksia myös verkossa toimivalle rikollisuudelle. Verkossa tapahtuvasta rikollisuudesta suurimman osan muodostavat omaisuusrikokset, joihin kuuluvat niin petokset, kiristysrikokset kuin maksuvälinepetokset (Valtioneuvosto, 2017). Edellä mainittujen omaisuusrikosten hyökkäysvektorina toimii usein huijausviestit sähköpostin tai tekstiviestien välityksellä. Tietojenkalasteluviestit ovat yksi esimerkki huijausviesteistä. Badran, El-Sawdan ja Hajjehin (2007) tutkimuksessa todetaan, että tietojenkalasteluviestit ovat huijauksia, joissa käyttäjä vastaanottaa viestin näennäisesti luotettavalta taholta, esimerkiksi pankilta, joka kehottaa kirjautumaan sisään viestin linkin kautta. Todellisuudessa kuitenkin viestin lähettäjä ja sivusto on tarkkaan luotuja kopioita, ja kokematon käyttäjä joutuu huijausviestin uhriksi tietämättään.

Verkkorikollisuus on kannattavaa, sillä mahdollisia uhreja voidaan aina löytää lisää. Osittain sen olemassaolo viestii ihmisten riittämättömästä tietoturvatietoisuuden tasosta. National Institute of Standards and Technology (NIST) määrittää, että tietoturvatietoisuus on ihmisten kykyä tunnistaa tietoteknisiä uhkakuvia, ja välttää niitä (Wilson *et al.*, 1998). Tietoturvatietoisuuden tasoon voidaan vaikuttaa koulutuksella joka on tämän kandidaatintyön lopullinen tavoite.

1.1 Työn tavoitteet ja rajaukset

Tämän kandidaatintyön päätavoitteena on luoda verkkosovellus, jossa yhdistyvät niin huijausviestien keräys kuin tietoturvakoulutuksena toimiva opettavainen peli. Pelin tavoitteena on auttaa sen käyttäjiä tunnistamaan erilaisia huijausviestejä. Lisäksi työssä tutustutaan erilaisiin huijausviesteihin ja tunnistetaan niille ominaisia piirteitä.

Peli on suunnattu pääasiassa tavanomaisille älylaitteiden käyttäjille, jolloin myös huijausviestien tutkimuksessa hyödynnetään tätä näkökulmaa. Europan unionin verkko- ja tietoturvaviraston (ENISA, 2010) artikkelin mukaan tavanomaiseksi käyttäjäksi luetaan eri ikäiset henkilöt, jotka käyttävät tietoteknisiä laitteita töiden ulkopuolella. Ryhmään kuuluvien henkilöiden tekninen tietämys vaihtelee, eli siihen voi kuulua sekä aloittelevia että kokeneita älylaitteiden käyttäjiä.

Työssä pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

1. Millaisten huijausviestien avulla ihmisiä pyritään huijaamaan?
2. Miten voidaan tunnistaa erilaisia huijausviestejä?
3. Kuinka huijausviestien tunnistamiseen keskittyvä peli tulisi toteuttaa?
    3.1. Miten pelissä käytettävät huijausviestit tulisi kerätä?

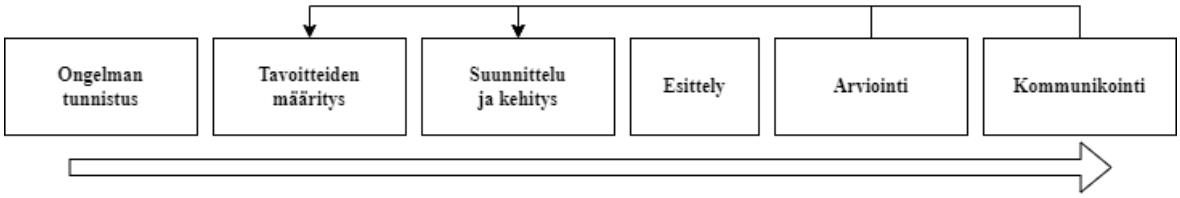
Koska tämä työ keskittyy tavanomaisia käyttäjiä koskeviin huijausviesteihin, työn tutkimusalueen ulkopuolelle jäävät muun muassa erilaiset yrityksiin kohdistuvat huijausviestit, kuten toimitusjohtajahuijaukset. Lisäksi työn luonteen vuoksi tarkastellaan ainoastaan huijauksien viestejä, eikä esimerkiksi liitetiedostojen tai linkkien sisältöä.

1.2 Käytettävät tutkimusmenetelmät

Työn tutkimuskysymyksiin tullaan vastaamaan systemaattisen kirjallisuuskatsauksen, sekä suunnittelutieteen tutkimusmenetelmää hyödyntäen. Systemaattisen kirjallisuuskatsauksen avulla pyritään muodostamaan yleiskuva huijausviestien tutkimuksesta ja vastaamaan tutkimuskysymyksiin yksi ja kaksi. Kyseisen menetelmän tulokset ovat oleellisessa roolissa myös suunnittelutieteen avulla luotavan pelin suunnittelu- ja toteutusvaiheissa. Suunnittelutieteen menetelmää hyödynnetään kolmanteen tutkimuskysymykseen vastaamiseen.

Suunnittelutiede on tietojärjestelmätutkimuksissa käytettävien laadullisten ja määrällisten tutkimusmenetelmien yhdistelmä (Kaplan & Duchon, 1988). Sen tavoitteena on luoda hyödyllisiä artefakteja ratkaisemaan tähän mennessä ratkaisemattomia ongelmia, tai niin sanottuja hankalasti ratkaistavia ongelmia. Luodut artefaktit voivat olla esimerkiksi ohjelmistoratkaisuja tai matemaattista logiikkaa. (Hevner *et al.*, 2004.) Kuvassa 1 esitellään Peffers *et*

al. (2006) luoma tietojärjestelmien tutkimukseen sopivan suunnittelutieteellisen tutkimuksen prosessikuvaus.



Kuva 1. Suunnittelutieteen prosessikuvaus (Peffers et al., 2006)

Suunnittelutieteen tutkimukselle voi olla useita eri lähtökohtia. Tässä työssä lähtökohtana on ongelmakeskeinen lähestyminen, joten muut vaihtoehdot sivuutetaan. Tutkimus siis alkaa ongelman tunnistusvaiheesta, jossa ratkaisulle määritellään tavoitteet ja motivaatio. Seuraavaksi määritellään tutkimuksessa syntyvän artefaktin, eli ratkaisun tavoitteet. Suunnittelu ja kehitysvaiheessa luodaan artefakti, joka esitellään ja arvioidaan myöhemmissä vaiheissa. Suunnittelu- ja kehitysvaiheissa hyödynnetään systemaattisen kirjallisuuskatsauksen tuloksia erilaisista huijausmenetelmistä ja niiden välttämiskeinoista. Esittelyvaiheeseen kuuluu sopivan asiayhteyden määritys ja artefaktin käyttöönotto. Arviointivaiheessa artefaktin tehokkuutta arvioidaan. Tätä vaihetta seuraa kommunikointivaihe, jossa tulokset julkaistaan.

Prosessin vaiheista voidaan siirtyä edelliseen nuolten osoittamalla tavalla, jolloin tutkimusprosessin aikana ratkaisu tai niin kutsuttu tietopankki voi kehittyä parempaan suuntaan esimerkiksi arvioinnin tai uuden tiedon johdosta. Lähtökohtaisesti tietopankki voi kehittyä erityisesti artefaktin avulla kerättyjen huijausviestisyötteiden perusteella, mikäli syötteistä voidaan päätellä uusia havaintoja.

1.3 Työn rakenne

Johdannon jälkeen toisessa luvussa suoritetaan katsaus huijausviestien tutkimukseen systemaattisen kirjallisuuskatsauksen avulla. Kolmannessa luvussa käsitellään systemaattisen kirjallisuuskatsauksen avulla eroteltuja huijaustyylejä, niiden piirteitä ja lisäksi esitellään ohjeita huijauksien välttämiseksi. Sen jälkeisessä luvussa kuvaillaan verkkopelin suunnittelu, toteutus ja arviointi suunnittelutieteen menetelmiä hyödyntäen. Viimeisessä kappaleessa keskustellaan työn tuloksista ja päätetään työ yhteenvetoon.

2 Katsaus huijausviestien tutkimukseen

Tässä luvussa suoritetaan systemaattinen kirjallisuuskatsaus huijausviestien tutkimukseen. Kappaleen alussa esitellään käytettävä tutkimusmenetelmä, sen pääpiirteet ja katsauksen tavoitteet. Seuraavissa alaluvuissa käydään systemaattisen kirjallisuuskatsauksen toteutus läpi vaiheittain. Viimeinen alaluku sisältää yhteenvedon kerätyistä tuloksista muun muassa kuplakaavion muodossa.

Tutkimusten ja raporttien määrä kasvaa tutkimusalueen ollessa laaja. Tällöin on syytä karsia turhia hakutuloksia. Petersen *et al.* (2008) esittelemän menetelmäkuvauksen mukaan systemaattisen kirjallisuuskatsauksen tavoitteena on luoda yhteenveto tutkimusalaa koskevista hakutuloksista rajaamalla ja lajittelemalla niitä. Usein yhteenveto tapahtuu erilaisten visuaalisten karttojen avulla. Kuvassa 2 esitellään alkuperin Bailey *et al.* (2007) suunnitteleman ohjelmistotuotannon alalle sopivan systemaattisen kirjallisuuskatsauksen päävaiheet.

Kuva 2. Systemaattisen kirjallisuuskatsauksen päävaiheet (Petersen et al., 2008)

Systemaattisen kirjallisuuskatsauksen ensimmäisessä vaiheessa määritellään tutkimuskysymykset, joihin sen avulla pyritään vastaamaan. Tässä tapauksessa kyseistä tutkimusmenetelmää käytetään vastaamaan jo määriteltyihin tutkimuskysymyksiin yksi ja kaksi. Muut vaiheet ja niiden kulku esitellään seuraavissa alaluvuissa.

Tarkoituksena on löytää tieteellisiä julkaisuita, joissa käsitellään huijausviestejä. Julkaisut voivat käsitellä huijausviestejä eri näkökulmista, ja ne voivat olla esim. tutkimuksia, joissa luokitellaan eri huijausviestejä tai rakennetaan järjestelmä niiden tunnistamiseksi. Tavoitteena on kuitenkin se, että julkaisusta ilmenee käsiteltävät huijausviestityypit, sekä mahdollisesti niille ominaisia piirteitä. Tarvittaessa hakutulosten julkaisukanavia voidaan arvioida Julkaisufoorumin avulla.

Tietojen avulla pyritään luomaan yleiskuva viestien välityksellä toimivista huijauksista, sekä niiden piirteistä. Yleiskuvasta voidaan havainnoida esimerkiksi, mitkä huijausviestityypit ovat eniten tutkittuja. Tutkimuskysymyksiin yksi ja kaksi vastaamisen lisäksi tämän

tutkimusmenetelmän tavoite on luoda tieteellinen pohja suunnittelutieteen menetelmiä käyttäen rakennettavalle verkkosovellukselle.

2.1 Tiedonhaku

Ennen varsinaista tiedonhakua määriteltiin mistä haetaan, ja miten haetaan. Tätä varten suoritettiin niin kutsuttuja pilottihakuja, joiden avulla voitiin määrittää mitkä hakusanat tuottavat haluttuja tuloksia. Tiedonhakuun päätettiin käyttää IEEE, ACM ja Google Scholar tietokantoja. Pilottihauissa tietoja haettiin erilaisten strukturoitujen hakujen avulla. Hauissa käytettiin erilaisia termien yhdistelmiä, kuten ”Cybercrime” AND ”email” tai ”Scam message” AND ”types”. Koska huijausviesteihin kuuluvat niin sähköpostiviestit kuin tekstiviestitkin, huomioitiin se myös hakutermeissä yleispätevän ”messages” lisäksi.

Ensimmäinen hakutermi ”cybercrime” AND ”email” tuotti aivan liikaa hakutuloksia (36600), ja ensisilmäyksellä lähes kaikki vaikuttivat tutkimuksen kannalta hyödyttömiltä. Muokkaamalla hakua muotoon ”cybercrime” AND ”email” AND ”scam” hakutulokset vaikuttivat lupaavammilta ja tulokset tippuivat 4680 osumaan.

Yhdeksi testihauksi valittiin tietojenkalastelua koskeva ”phishing message” AND ”types”, sillä sen ajateltiin tuottavan paljon yleispätevää materiaalia, koska tietojenkalastelun alle voidaan luokitella useita eri huijausmuotoja. Nopeasti Google Scholarin hakutuloksista voitiin päätellä, ettei tulokset vastanneet odotuksia. Myöskään haku ”scam message” AND ”types” ei tuottanut lisäarvoa muiden hakujen rinnalle.

Haku ”Fraud message” AND ”types” tuotti valitettavan paljon epäolennaisia tuloksia liittyen esim. maksukorttipetoksiin. Pikaisen silmäilyn perusteella joukosta löytyi kuitenkin myös useita relevantteja tutkimuksia.

Muut testihaut voitiin todeta sopiviksi tutkimuskysymysten kannalta. Muiden hakujen osalta myös hakutulosten määrät vaikuttivat sopivilta läpikäytäviksi, lukuun ottamatta hakuja ”Scam emails” ja ”Cybercrime” AND ”email” AND ”scam”, jotka tuottivat 750 ja 4680 Google Scholar hakutulosta. Näiden osalta haussa keskityttiin vuoden 2019 jälkeen julkaistuihin artikkeleihin, jolloin hakutulokset tippuivat 279 ja 1860 tulokseen. Jälkimmäisen haun

osalta tuloksia oli edelleen liikaa, joten näistä päätettiin huomioida ensimmäiset 200 seuraavassa vaiheessa.

Testihakujen perusteella lopulliseen tiedonhakuun valikoituneet hakutermit, sekä tulosten määrät tietokannoittain ovat esiteltynä taulukossa 1.

Taulukko 1. Hakutermit, sekä tietokantojen tulokset

Hakutermi	Google Scholar	ACM	IEEE
”cybercrime” AND ”email” AND ”scam”	4680	321	49
”Fraud message” AND ”types”	90	3	22
”Scam email” AND ”types”	345	8	12
”Scam SMS” AND ”types”	14	3	3
”Scam message” AND ”characteristics”	67	1	0
”Scam emails”	279	11	1

2.2 Hakutulosten seulonta ja luokittelu

Tulosten seulontavaiheessa hakutulokset seulottiin läpi tietokannoittain, tarkoituksena valita joukosta tutkimuskysymysten kannalta oleelliset julkaisut. Seulontaa varten tuli luoda valintakriteerit, joiden perusteella julkaisu otetaan – tai ei oteta mukaan tutkimukseen. Muodostetut kriteerit ovat esitelty seuraavassa taulukossa 2.

Taulukko 2. Valintakriteerit

Hyväksytään	Hylätään
Julkaisussa käsitellään useita huijausviestejä	Kandidaatintyön tasoinen julkaisu
Englannin- tai suomenkielinen	Maksullinen / muuten saamattomissa
	Käsittelee ainoastaan yhtä huijausviestityyppiä

Itse hakutulosten seulonta suoritettiin kahdessa vaiheessa. Ensiksi hakutuloksia tarkasteltiin otsikkotasolla, ja sopivat julkaisut lisättiin Excel laskentataulukkoon. Tuloksista karsittiin muun muassa tulokset, jotka keskittyivät ainoastaan yhteen huijausviestityyliin tai olivat muuten sopimattomia. Ensimmäisen seulonnan läpäisi yhteensä 89 uniikkia artikkelia.

Seuraavassa seulonnassa Excel taulukkoon lisätyt julkaisut seulottiin jälleen. Tällä kertaa julkaisuja tarkasteltiin muun muassa tiivistelmän osuvuuden tai julkaisun saatavuuden

näkökulmasta. Tarkemman seulan jälkeen noin puolet artikkeleista karsiutui pois. Suuri osa karsituista artikkeleista olivat maksumuurin takana, toinen osa taas osoittautui muuten sopimattomiksi. Toisen seulonnan jälkeen jäljelle jäi 37 artikkelia, jotka etenivät luokitteluvaiheeseen.

Tulosten luokitteluvaiheessa noudatettiin Petersen *et al.* (2008) määrittelemää kaksivaiheista luokittelumenetelmää. Ensiksi luokittelu tapahtui erottelemalla tutkimusten tiivistelmistä avainsanoja ja asiayhteyksiä. Mikäli artikkelin tiivistelmä oli riittämätön avainsanojen erotteluun, käytettiin apuna myös johdantoa tai johtopäätöksiä. Seuraavaksi avainsanojen avulla pyrittiin muodostamaan kokonaisuus, josta ilmeni karkeasti tutkimuksissa käsiteltävät aihepiirit. Luokitteluvaiheen aikana julkaisujen joukosta karsiintui 6 tutkimusta, sillä tarkemmin tutkiessa artikkelien sisältö ei vastannut haettua. Lopulta tutkimukseen hyväksyttiin 31 artikkelia.

Luokitteluvaiheessa jokaisesta artikkelista poimittiin seuraavat tiedot: artikkelissa käsiteltävä(t) huijaustyyli(t), käsitelty hyökkäysvektori ja tutkimustyyppi. Tutkimustyypin määrittelyssä käytettiin Wieringa *et al.* (2006) määrittelemiä tutkimustyyppejä, jotka on esitelty taulukossa 3.

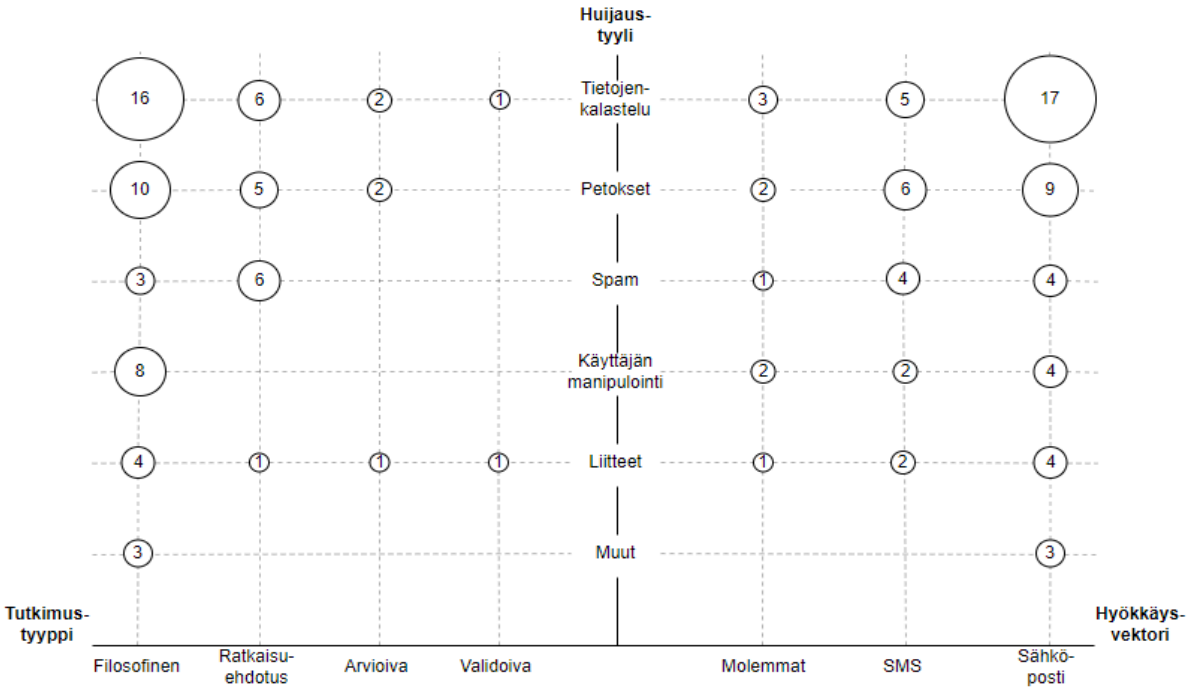
Taulukko 3. Wieringa et al. (2006) määrittelemät tutkimustyypit

Tutkimustyyppi	**Ominaisuudet**
Arvioiva tutkimus	Julkaisussa arvioidaan jo olemassa olevaa ratkaisua johonkin käytännön ongelmaan, tai toteutetaan ja kuvaillaan ratkaisu itse.
Ratkaisuehdotus	Julkaisussa määritellään ratkaisu ja sen tarve perustellaan. Ratkaisu on kokonaan uusi, tai merkittävä parannus aiempaan ratkaisuun.
Validoiva tutkimus	Tutkii ratkaisuehdotusta, jota ei ole toteutettu käytännössä. Mahdollisina tutkimusmenetelminä esimerkiksi kokeet, simulaatiot tai matemaattiset analyysit.
Filosofinen tutkimus	Määrittelee uuden näkökulman, esimerkiksi teoreettisen viitekehyksen merkeissä.
Mielipidejulkaisu	Julkaisijan omaan mielipiteeseen perustuva julkaisu.
Kokemusjulkaisu	Julkaisijan kokemukseen perustuva tutkimus. Esimerkiksi kokemuksia työkalujen/menetelmien käytöstä.

2.3 Tietojen keruu ja yhteenveto

Valituista tutkimuksista (31) kerättiin tietoja luokittelukategorioiden mukaisesti. Kaikista artikkelista 18 oli filosofisia, 9 ratkaisuehdotuksia, 3 arvioivia ja 1 validoiva. Huijaustyylien poiminnassa pyrittiin keräämään ainoastaan huijaustyylin päälaji, eli esimerkiksi arpajaishuijauksen tapauksessa artikkeli luokiteltiin petoksia käsitteleväksi. Mikäli artikkelissa mainittiin esimerkiksi spam tai käyttäjän manipulointi, määriteltiin ne huijaustyyleiksi muiden rinnalle. Voidaan kuitenkin todeta, ettei kumpikaan mainituista ole suoranaisesti huijausmenetelmiä. Hyökkäysvektoreihin jako oli melko suoraviivaista. Mikäli artikkelissa käsiteltiin huijauksia sähköpostin, sekä tekstiviestien näkökulmasta, määriteltiin hyökkäysvektoriksi ”molemmat”. Muuten hyökkäysvektoriksi määräytyi joko SMS tai sähköposti.

Kerättyjen tietojen avulla luotiin kuplakaavio, jonka tarkoituksena on havainnoida, kuinka poimitut huijaustyylit esiintyvät julkaisuissa. Huijaustyylit esitetään kuvan y-akselissa. Kuplakaavion x-akseli puolestaan koostuu kahdesta eri luokittelutyylistä. Koska artikkeleissa käsiteltiin useita huijaustyylejä, ei osumien määrät vastaa tutkimusten määrää (31). Vasemmalla puolella käsitellään tutkimustyyppejä. Vasemman puolen tarkoituksena on havainnoida sitä, miten erilaiset huijaukset ilmenevät kussakin tutkimustyypissä. Oikealla puolella taas käsitellään eri hyökkäysvektoreita. Oikean puolen tarkoituksena on havainnoida, mitkä huijaustyylit ovat ominaisia eri hyökkäysvektoreille. Kuplakaavio on esitelty kuvassa 3.



Kuva 3. Kuplakaavio systemaattisen kirjallisuuskatsauksen tuloksista

Kaavion vasenta puolta tarkastellessa, voidaan todeta filosofisen tutkimustyypin olleen suosituin tutkimusnäkökulma. Se oli myös ainoa tutkimustyyli, joka kattoi kaikki poimitut huijaustyylit. Tutkimustyypeissä tietojenkalastelu oli eniten käsitelty huijaustyyli. Seuraavaksi eniten käsiteltiin petoksia. Muita huijaustyylejä käsiteltiin ainoastaan kolmessa artikkelissa. Validoiva tutkimus oli vähiten käytetty tutkimustyyppi.

Oikealla puolella huomataan sähköpostin olevan suosituin hyökkäysvektori. Myös tässä yhteydessä tietojenkalastelu oli suosituin huijaustyyli, toisena jälleen petokset. Hyökkäysvektorin näkökulmasta lähes kaikkia huijaustyylejä ilmaantuu molemmissa hyökkäysvektoreissa. Ainoan poikkeaman luo muut huijaukset, joita käsiteltiin ainoastaan sähköpostin yhteydessä.

3 Tunnistetut huijausviestityylit ja niiden välttäminen

Tässä luvussa esitellään tarkemmin systemaattisen kirjallisuuskatsauksen tuloksia. Tarkastelu suoritetaan alaluvuissa alkaen menetelmistä, jotka toimivat huijausviestien tukena ja siitä siirtyen huijausviestejä kuvaileviin alalukuihin. Viimeisessä luvussa esitellään keinoja, joiden avulla voidaan välttää joutumista huijauksien uhriksi. Välttämismenetelmistä useimmat ovat yleispäteviä.

Huijausviestityylejä käsittelevissä alaluvuissa pyritään kuvailemaan tutkimuksissa esiteltyjä havaintoja, piirteitä ja johtopäätöksiä liittyen huijausviesteihin. Tunnistamiseen liittyvissä piirteissä erilaisiin algoritmeihin, tai muihin automaattisiin luokittelumenetelmiin pohjautuvat ratkaisut sivuutetaan. Sen sijaan keskitytään poimimaan piirteitä, joita ihminen voi havaita vastaanottaessaan viestin. Käsiteltävät havainnot puolestaan voivat sisältää niin eri huijaustyyleille ominaisia alalajeja tai niiden vertailua käytettävän kielen tai ajanjakson näkökulmasta.

3.1 Menetelmät huijauksien tukena

Artikkeleista poimitulla termillä *spam* tarkoitetaan mitä tahansa merkityksettömiä viestejä, joita vastaanottaja ei odota vastaanottavansa (Markova *et al.*, 2019), usein spammista käytetään nimitystä roskaposti. Artikkelissa Chrobok (2010) määritteli roskapostille kolme kategoriaa: mainokset, petokset ja haitalliset. Duo et al. (2021) sen sijaan määrittelee roskapostiksi luotettavat viestit, joiden tarkoitus on myydä tuotteita ja palveluita. Siten roskapostiviestit eivät suoranaisesti ole huijausmuoto, vaan keino tavoittaa suuria määriä mahdollisia huijauksien uhreja. Lähes kaikki seuraavissa alaluvuissa käsiteltävät kohdistamattomat massahuijaukset voidaan luokitella tähän kategoriaan.

Käyttäjän manipulointi on menetelmä, jossa huijari käyttää sosiaalisia menetelmiä kuten suostuttelua ohjatakseen uhrin käyttäytymistä haluttuun suuntaan. Useimmat huijausviestit perustuvat käyttäjän manipulaatioon erilaisine menetelmineen. Eri huijaustyypeissä käytettävät manipuloimislähestymistavat ja tyyli vaihtelevat, esim. romanssihuijauksissa huijari esittää helposti lähestyttävää rakastajaa, kun taas tietojenkalastelussa voidaan esittää

kiireistä, jonkin arvostetun tahon edustajaa (Chaganti et al., 2021). Newman (2006) kuvailee artikkelissaan manipuloijaa itsevarmaksi henkilöksi, joka omaa hyvät sosiaaliset taidot ja kyvyn valehdella, esittää muita ja vastata nopeasti haastaviinkin kysymyksiin.

Florian Hiß (2015) ”Fraud and Fairy Tales: Storytelling and Linguistic Indexicals in Scam E-mails” artikkelissa analysoidaan huijausviestejä kielitieteellisestä näkökulmasta. Edelliseen lisättynä yhtenä manipulaation keinona mainitaan tahalliset kielioppivirheet, joiden avulla huijari voi luoda kuvan heikosta sosiaalisesta statuksesta ja siten vaikuttaa lukijan tunteisiin. Kirjoitusvirheet eivät kuitenkaan täysin päde suomenkielisiin huijausviesteihin, jotka ovat täynnä kirjoitusvirheitä, sillä ne ovat usein peräisin huonosta käännöksestä.

3.2 Tietojenkalastelu

Tietojenkalastelu (engl. *phishing*) on vilpillinen menetelmä, jonka tavoitteena on vastaanottajien huijaaminen erilaisten tietojen saamiseksi. Stabekin, Wattersin ja Laytonin (2010) artikkelin mukaan näihin tietoihin voi kuulua niin käyttäjätunnusten, pankkikorttien tunnuslukujen tai muiden henkilökohtaisten ja arkaluontoisten tietojen keräys.

Huijaustyyli pohjautuu lukijan harhautukseen (Almoqbil *et al.*, 2021). Se käyttää hyväksi ihmisten heikkouksia, kuten luottamusta ja uteliaisuutta, joka muodostetaan houkuttelevan kommunikaation avulla (Corradini, 2020). Edellä mainittujen lisäksi, viestit voivat sisältää houkuttelevia tarjouksia tai huolestuttavia aiheita, jotka vaativat vastaanottajalta pikaista huomiota ja luovat kiireen tunteen (Corradini, 2020, s. 16; Kerremans et al., 2005; Truchero Visa, 2021).

Duo et al. (2021) tutkimuksessa sähköpostitse suoritettavalle tietojenkalastelulle määriteltiin kolme suosituinta alalajia: lahjakorttihuijaukset, yleiset tietojenkalasteluyritykset, sekä toivomattomat massaviestit. Lisäksi itse tietojenkalastelulla on useita variaatioita, kuten kohdennettu tietojenkalastelu (engl. *spearphishing*), jonka kohteena on jokin tietty henkilö, yritys tai organisaatio. Kohdennettua tietojenkalastelua varten hyökkääjien tulee tehdä taustatöitä esimerkiksi työyhteisöstä tai yrityskumppaneista, jotta voidaan luoda uskottava tietojenkalasteluviesti (Caputo *et al.*, 2014).

Tietojenkalasteluviestin tunnistus voi olla hankalaa, sillä viesti näyttää usein tulevan luotettavalta taholta (Chrobok, 2010; Ahsan Pritom *et al.*, 2020; Arshad *et al.*, 2021) ja vaikuttaa ammattimaiselta. Tyypillisesti viestit sisältävät linkin tietojenkalastelusivustolle (Markova et al. 2019; Kerremans *et al.*, 2005). Linkkien todellinen osoite voi olla piilotettu tai naamioitu esim. lyhennetyillä linkeillä (Broadhurst ja Trivedi, 2019). SMS-tietojenkalastelua (engl. smishing) käsittelevässä tutkimuksessa Mishra ja Soni (2019) totesivat haitallisten-linkkien lisäksi mahdolliseksi sisällöksi myös puhelinnumerot ja sähköpostiosoitteet joihin kehotetaan olemaan yhteydessä.

Ennen tietojenkalasteluviestit olivat helppo tunnistaa niiden kirjoitusvirheiden tai sekavan kirjoitustyylin perusteella (Corradini, 2020 s. 50). Tänä päivänä viestien tunnistus on hankalampaa, sillä viestit ovat tarkasti rakennettuja ja ne vetoavat vastaanottajiin tehokkaasti käyttäjän manipulaation keinoin (Kerremans et al., 2005).

3.3 Petokset

Petoshuijauksissa huijarin tavoitteena on taloudellinen hyöty. Badawi (2021) jakaa tutkimuksessaan huijauksien lähestymistavat neljään eri kategoriaan: toisena henkilönä esiintyminen, harhautus ja kiristys; investoinnit ja nopeat voitot; yllättävät tulot tai voitot; väärennetyt palvelut. Edellä mainittuihin kategorioihin mahtuu huijauksia moneen eri lähtöön, ja kirjoitushetkellä esimerkiksi COVID-19 aiheiset huijausviestit liittyen työttömyyteen tai parannuskeinoihin ovat olleet suosittuja (Chaganti *et al.*, 2021). Muita artikkeleissa mainittuja petoshuijauksia ovat esimerkiksi erilaiset osake-, mainos-, pyramidi-, arpajais-, rikastu nopeasti-, romanssi-, 419-petokset, sekä muut etukäteismaksuun perustuvat huijaukset (Airoldi ja Malin, 2004; Sabillon *et al.*, 2016).

Fischer, Lea ja Evans (2009) artikkelissa ”The psychology of scams” kuvaillaan erilaisia petoshuijauksia, ja niiden piirteitä. Petoshuijauksissa tyypillisiä elementtejä voivat olla muun muassa suuret voittosummat, sympatian ja kiireen tunteen luovat tarinat, turhat lupaukset tai erilaiset määräajat. Yleisesti viesteissä annetaan kuva, että vastaanottaja on valikoitu henkilökohtaisesti ja estetään muille puhuminen ilmoittamalla, että viesti on luottamuksellinen. Lähettäjänä esiintyy usein joku korkea-arvoinen henkilö, tai jopa vastaanottajan läheinen.

Duo et al. (2021) artikkelin mukaan eri kielillä suositaan eri petoshuijaustyylejä, ja viestien lähestymistavat vaihtelevat. Myös petoshuijaukset rakennetaan huolella, erilaisia käyttäjän manipuloinnin menetelmiä käyttäen. Viestien sisällössä voidaan hyödyntää jopa eri alueiden aksentteja (Qabalin *et al.*, 2021) tai tervehtiä vastaanottajaa nimellä (Ribaux ja Souvignet, 2020). Usein niissä voi kuitenkin esiintyä myös kirjoitus- ja muita huolimattomuusvirheitä (Razaq *et al.*, 2021) esimerkiksi käännösten seurauksena.

Yksi tyypillisimmistä petoshuijauksista ovat nigerialaiskirjeet, toiselta nimeltään 419 huijaukset. Huijaustyypin juuret ulottuvat vuosikymmenten taakse, jolloin huijausta toteutettiin kirjeiden välityksellä. Kuitenkin ajan ja teknologian kehityksen myötä myös tämä huijaus on siirtynyt sähköpostin ja viestien välityksellä toimivaksi, toteaa Isacenkova *et al.* (2013) nigerialaiskirjeitä käsittelevässä tutkimuksessa. Nigerialaiskirjeiden ja myös petoksille tyypillinen perusidea on tarjota lukijalle huomattavia summia rahaa pientä palvelusta vastaan (Dyrud, 2005). Palveluksella tarkoitetaan usein pientä rahallista korvausta, joka on naamioitu esimerkiksi rahojen siirtokuluiksi (Hartikainen, 2006). Dyrudin (2005) artikkelin mukaan huijaus jatkuu uhrin maksaessa ensimmäisen summan, jonka jälkeen uhrilta pyydetään jälleen rahaa erilaisiin kuluihin. Huijaus päättyy, kun uhri kieltäytyy maksamasta.

3.4 Liitetiedostot

Huijausviesteissä liitteinä voi olla monenlaisia tiedostoja. Haittaohjelmia sisältäviä sähköposteja käsittelevän tutkimuksen (Broadhurst ja Trivedi 2019) koeotoksesta todettiin lunnastroijalaiset ja kiristyshaittaohjelmat suosituiksi liitetiedostoiksi. Edellä mainitut haittaohjelmatyypit toistuivat myös muissa aihetta käsittelevissä tutkimuksissa: Pritom et al. 2020; Jakobsson, 2016.

Broadhurst ja Trivedin koeotoksen perusteella haitallisten liitetiedostojen formaatit vaihtelivat laajasti esim. kuvatiedostojen, pakattujen kansioiden tai pdf-tiedostojen välillä. Myös Word tai Excel – tiedostoja käytetään haittaohjelmien levittämiseen, sillä niiden sisään voidaan piilottaa erilaisia makroja. Perinteisten liitteiden ohella haittaohjelmien jakeluun voidaan käyttää erilaisia palveluita, kuten Dropbox tai Google Drive, joista uhri ohjataan lataamaan tiedostot (Fagerland, 2017).

Käyttäjän manipulaatio on oleellisessa roolissa myös liitetiedostoja sisältävien huijausviestien sisällössä. Luomalla kiireen ja pelon tunteen huijari voi rohkaista uhria lataamaan ja suorittamaan liitetiedostot.

3.5 Muut huijausviestit

Muihin huijausviestityyppeihin kuuluvat artikkeleista poimitut pretexting, sekä kiristysviestit ja flubot-haittaohjelma. Corradini (2020) mukaan pretexting on käyttäjän manipulointia hyödyntävä menetelmä, jossa huijari pyrkii saavuttamaan uhrin luottamuksen erilaisten teennäisten skenaarioiden avulla. Skenaarioissa huijari voi tiedustella uhrilta tietoja uskottavan tapauksen avulla esimerkiksi vakuutusyhtiön tai virkavallan nimissä.

Kyberturvallisuuskeskuksen (2021) mukaan viime aikoina liikkeellä on ollut tekstiviestitse leviävä mobiilihaittaohjelma Flubot. Kyseisen haittaohjelman leviämisessä käytettävät tekstiviestit voivat sisältää esimerkiksi ilmoituksen tulevasta vastaajaviestistä, sekä linkin, jonka takaa vastaajaviesti löytyy. Linkin avatessa erityisesti Android käyttäjät ovat vaarassa, sillä näytölle avautuu ilmoitus, joka pyytää käyttäjältä lupaa asentuakseen. Asennettuaan ohjelman huijari voi varastaa puhelimesta tietoja, sekä käyttää sitä huijausviestien levittämiseen. Kyseisen haittaohjelman leviämiseen käytettävissä viesteissä on tyypillisesti paljon virheitä ja erikoismerkkejä.

Kiristysviestien tavoitteena on maksun tai uhrin tietojen huijaaminen. Duo *et al.* (2020) mukaan kiristysviestit perustuvat uhrin pelotteluun tai uhkailuun. Viestit voivat liittyä esimerkiksi tappamiseen, kidnappaukseen, mustamaalaukseen tai velkoihin. Kiristysviesteistä erityisesti pornokiristysviestit ovat suosittuja huijareiden keskuudessa (Kyberturvallisuuskeskus, 2019). Tässä huijauksessa vastaanottajalle väitetään, että huijari on salakuvannut uhria tämän vieraillessa aikuisviihdesivustolla ja uhkaa julkaista materiaalit, jos lunnaita ei makseta. Todellisuudessa materiaalia ei ole, vaan huijari pyrkii vetoamaan uhrin tunteisiin luomalla häpeän tunteen. Paquet-Clouston *et al.* (2019) tutkimustulosten mukaan huijarit eivät myöskään seuraa, mikäli huijaus on onnistunut. Lunnaiden maksuun käytetään pääsääntöisesti virtuaalivaluuttoja, kuten Bitcoinia (Sophos, 2022). Kyberturvallisuuskeskuksen (2019) mukaan viestien uskottavuutta pyritään lisäämään erilaisten liitetiedostojen avulla, tai mainitsemalla uhrin aiemmin käyttämiä salasanoja.

3.6 Keinoja huijauksien välttämiseksi

Tutkimuksissa mainitut keinot huijauksien välttämiseksi olivat pääsääntöisesti yleispäteviä, lukuun ottamatta liitetiedostoja koskevia välttämismenetelmiä. Eniten mainittu välttämiskeino oli tietoturvakoulutuksen lisääminen, jota käsiteltiin Truchero Visan 2021, Pritom et al. 2020 ja Badawin 2021 tekemissä artikkeleissa. Tietoturvakoulutuksen lisäksi Sabillon et al. (2016) mainitsi artikkelissaan tietoturvatietoisuus harjoitukset, ja Jakobsson (2016, s. 30) erilaiset tietoturvaan liittyvät verkkopelit ja harjoitusviestit. Koulutukseen liittyen Chaganti et al. (2021) suositteli ajankohtaisten huijausten aktiivista tiedottamista, jotta tietoisuus huijauksista leviäisi.

Newman (2006) suositteli artikkelissaan viestien lähettäjän tarkastusta välttääkseen huijaukset. Lisäksi Newman painotti skeptisyyttä odottamattomia viestejä kohtaan, sekä tarkkaavaisuutta henkilötietojen, tai muiden tärkeiden tietojen luovuttamisen yhteydessä. Pritom et al., (2020) puolestaan suositteli tarkistamaan myös liitteet ja linkit, sekä käyttäjän manipuloinnin piirteitä viestistä.

Mishra ja Soni (2019) sekä Ribaux ja Souvignet (2020) suosittelivat tutkimuksissaan välttämään sähköpostien linkkien painamisen, ja sen sijaan siirtymällä osoitteeseen suoraan URL-osoitteen tai kirjainmerkin avulla. Linkkien osalta on hyvä muistaa myös se, että usein linkin todellinen määränpää selviää viemällä hiiren linkin päälle. Mikäli linkin takana on lyhennetty URL-osoite, voidaan sen lopullinen määränpää selvittää eri verkkosivustojen kuten wheregoes.com avulla.

Myös liitetiedostoja sisältävien viestien yhteydessä suositeltiin skeptisyyttä. Newmanin (2006) mukaan lähettäjän motiiveja tulisi epäillä, mikäli liitetiedostot tulevat yllättäen, vaikka viesti tulisi näennäisesti luotetusta osoitteesta. Myös ”kollegalta” yllättäen tullut liitetiedosto voi sisältää haittaohjelmia (Jakobsson, 2016, s. 116) tai piilotettuja makroja, jonka vuoksi niiden suoritusta ei tulisi sallia teksti- tai taulukkoeditorin sitä pyytäessä.

4 Verkkosovelluksen suunnittelu, toteutus ja arviointi

Tässä luvussa esitellään huijausviestien tunnistamiseen keskittyvän verkkosovelluksen tavoitteet, kehitystyö ja lopulta luodun sovelluksen arviointi. Vaiheet suoritettiin johdantokappaleessa esitellyn suunnittelutieteen tutkimusmenetelmää mukaillen. Tutkimusmenetelmän vaiheet suoritettiin yhdessä iteraatiossa, aikarajoitteiden ja kandidaatintyön suppeahkon laajuuden vuoksi.

4.1 Tavoitteet ja vaatimukset

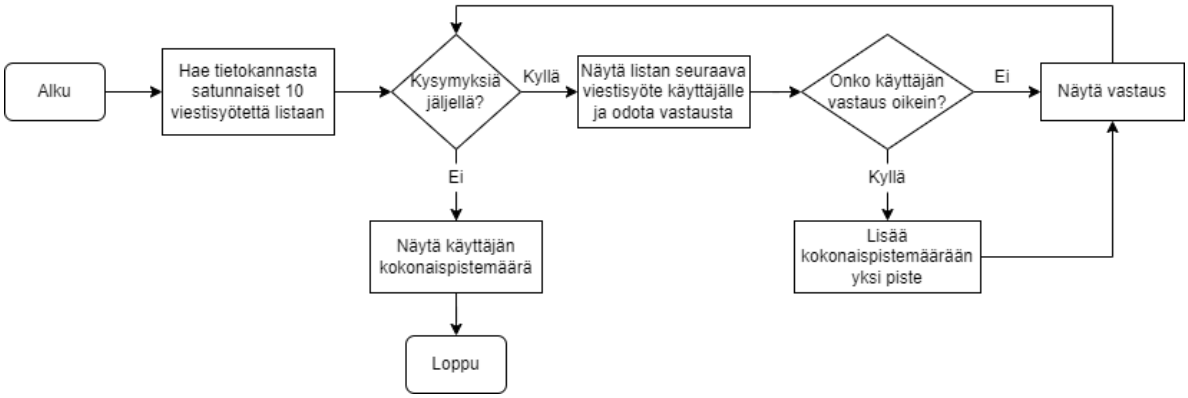
Yksinkertaisuudessaan kehitettävä artefakti on verkkosovellus, jossa yhdistyy huijausviestisyötteiden keruu, sekä huijausviestien tunnistamiseen keskittyvä peli. Sovellus on tarkoitus julkaista verkkoon hyödyntäen tarjolla olevia ilmaisia palveluntarjonta-alustoja. Koska työssä käsiteltäviin huijausviesteihin sisältyy sähköpostiviestien lisäksi myös tekstiviestit, tulee julkaistavan verkkosivun skaalautua eri näyttökokojen mukaan, jolloin viestisyötteiden lisääminen voidaan suorittaa kätevästi suoraan mobiililaitteilla. Muut huijausviestisyötteiden keruuseen ja opettavaiseen peliin liittyvät tekniset tavoitteet sekä pelin idea esitellään tarkemmin seuraavissa alaluvuissa.

4.1.1 Opettavainen peli

Huijausviestien tunnistamiseen keskittyvä peli toteutetaan tietovisana. Tietovisa-tyyppiset pelit ovat hyviä tapoja testata tietämystä, jonka vuoksi ne ovat hyödyllisiä ja toimivia ratkaisuja osana koulutusta (Sherry ja Pacheco, 2010). Lisäksi kyseinen pelimuoto voi auttaa käyttäjiä tunnistamaan omat heikkoudet ja vahvuudet, sekä kohottamaan itsevarmuutta välittömän palautteen avulla (Perrault, 2018).

Toteutettavan pelin alussa käyttäjälle arvotaan 10 kuvan sarja, joka haetaan satunnaisesti tietokannasta. Sarjaan voi kuulua huijausviestien lisäksi kuvia luotettavista viesteistä. Pelaajalle näytetään arvotut kuvat vaiheittain yksi kerrallaan. Aina kuitenkaan pelkkä kuva ei riitä

määrittelemään viestiä huijaukseksi tai luotettavaksi, jonka vuoksi tarvittaessa niiden yhteydessä voidaan esittää pieni taustatarina havainnoimaan tilannetta tarkemmin. Kunkin kuvan kohdalla käyttäjällä on vaihtoehto merkitä kuva huijaukseksi tai luotettavaksi nappia painamalla. Valinnan tehtyään pelaajalle ilmoitetaan oikea vastaus, sekä piirteet mistä kuvan olisi voinut tunnistaa huijaukseksi tai luotettavaksi. Tässä vaiheessa aiempi kuva on edelleen näkyvillä, joka mahdollistaa tarkastelun myös uudesta näkökulmasta vastaustekstin perusteella. Mikäli vastaus on oikein, pelaajan pisteisiin lisätään yksi piste. Aiemmin mainitut vaiheet toistetaan, kunnes 10 kuvan sarja on käyty läpi. Viimeisen kuvan jälkeen käyttäjälle näytetään kokonaispistemäärä. Pelin kulku on kuvailtu kuvassa 4 kulkukaavion muodossa.



Kuva 4. Pelin kulkukaavio

Toteutuksessa sovelletaan osittain Kumaraguru et al. (2010) tutkimuksessa käyttämiä verkkoturvallisuuskoulutuksen suunnitteluperiaatteita. Tähän työhön valikoituneet suunnitteluperiaatteet on esitelty taulukossa neljä.

Taulukko 4. Hyödynnettävät verkkoturvallisuuskoulutuksen suunnitteluperiaatteet (Kumaraguru *et al.*, 2010)

Suunnitteluperiaate	**Selitys**
Tekemällä oppiminen	Oppiminen on tehokkaampaa, kun siihen yhdistyy käyttäjän omat kokemukset ja välitön palaute
Välitön palaute	Välitön palaute mahdollistaa reagoimisen niin vääriin kuin oikeisiin vastauksiin heti. Voi myös lisätä käyttäjän itsevarmuutta.
Samanaikaisuus	Tässä yhteydessä samanaikaisuudella tarkoitetaan sitä, että esimerkiksi tietovisan oikea vastaus sekä itse kysymys (viestin kuva) on esillä samanaikaisesti vastauksen jälkeen. Auttaa käyttäjää hahmottamaan

	ja yhdistämään vastauksen piirteet itse kysymykseen.
Personaalisuus	Muodollisen esitystavan sijaan vapaamuotoisempi esitystapa voi lisätä oppimista.

Lisäksi pelin toteutuksessa hyödynnetään aiemmin PHISHY-tietojenkalastelun tunnistamispelissä (Cj *et al.*, 2018) hyödynnettyjä ominaisuuksia kuten rajatonta vastausaikaa, ja sitä, ettei kysymyksiä voida ohittaa. Edellä mainitut ominaisuudet lisäävät peliin oikean elämän tuntua, sillä myöskään oikeassa elämässä viestien yhteyteen ei liity aikarajoitteita ja harvoin saapuneita viestejäkään voidaan täysin sivuuttaa. Rajaton vastausaika voi myös kannustaa havainnoimaan viestiä tarkemmin ja mahdollistaa koko viestin lukemisen, mikäli tarve vaatii.

4.1.2 Viestisyötteiden keruu

Peliä varten tarvitaan viestisyötteitä, jotka koostuvat pääasiassa näyttökaappauksesta, jossa ilmenee viestin lähettäjä, sisältö ja tarvittaessa myös viestin otsikko. Tätä varten verkkosovellukseen tulee kehittää lomake, jonka avulla huijausviestisyötteitä voidaan kerätä. Näyttökuvan lisäksi käyttäjällä tulee olla mahdollisuus lisätä lisätietoja tai esimerkiksi kyseiselle huijaukselle ominaisia piirteitä lomakkeen yhteyteen. Kuitenkin, koska kaikki käyttäjät eivät ole kykeneväisiä tai halukkaita määrittelemään lisätietoja, voidaan ne jättää täyttämättä. Lopulta, ennen syötteen lähettämistä käyttäjältä tulee kysyä lupa syötteen käyttämiseksi osana opettavaista peliä.

Jotta voidaan välttää epäasialliset syötteet ja estää niiden päätyminen peliin, tulee ne tarkistaa järjestelmänvalvojan toimesta. Tarkastuksen yhteydessä voidaan lisätä puuttuvia piirteitä tai lisätietoja. Lisäksi on hyvä tarkistaa, ettei kuvissa ole esimerkiksi lähettäjien henkilökohtaisia tietoja tai muuta arkaluontoista näkyvissä. Tarkastuksen jälkeen syötteet voidaan vapauttaa osaksi pelissä käytettäviä kuvia.

Ensisijaisena tavoitteena on kerätä huijausviestisyötteet verkkosivun lomakkeen kautta. Jotta varmistetaan riittävä aika viestisyötteiden keruulle, tulee verkkosovellus pyrkiä julkaisemaan käyttäjien saataville mahdollisimman pian lomakkeen valmistuttua. Syötteitä varten

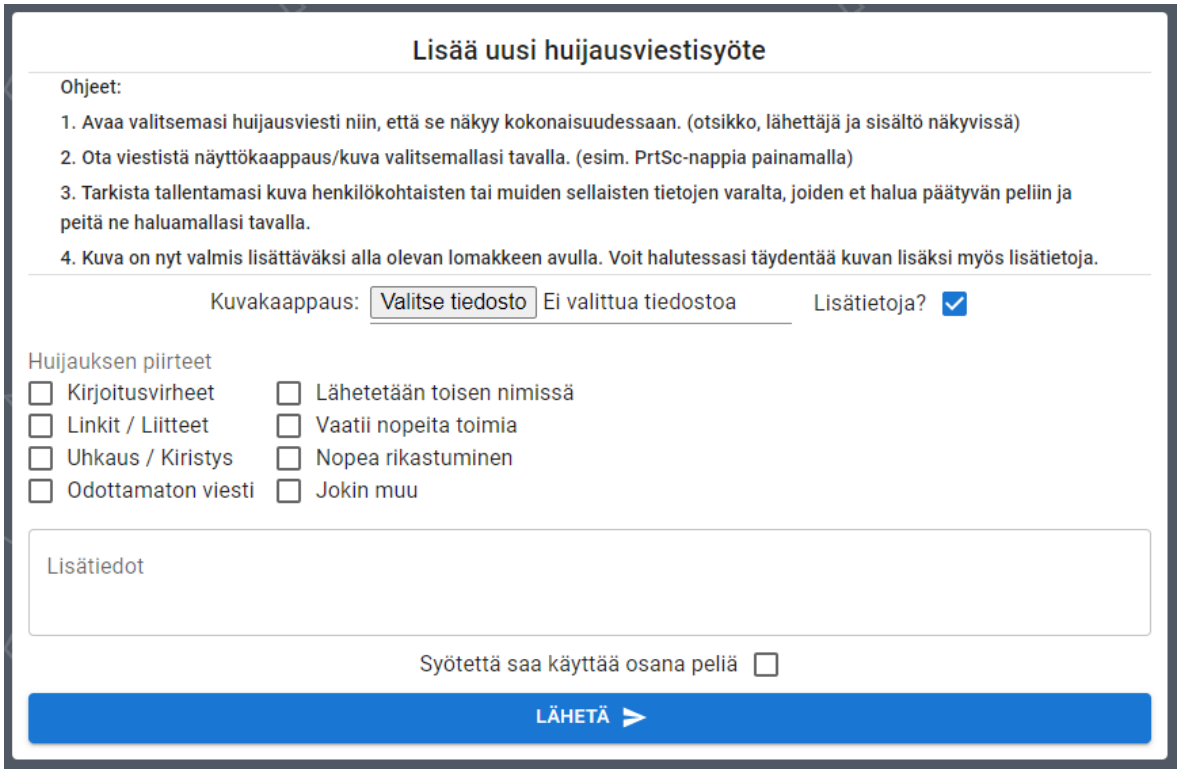
voidaan hyödyntää esimerkiksi yliopistopiirejä, läheisiä, sekä myös omista sähköposteista tai tekstiviesteistä löytyviä huijauksia. Mikäli huijausviestisyötteitä ei kerry tarpeeksi, voidaan hyödyntää internetistä löytyviä huijaustietokantoja kuten ScamWarners tai Scamdex.

Koska pelissä hyödynnetään huijausviestien lisäksi myös luotettavia viestejä, tulee sovelluksessa huomioida myös näiden keruu. Luotettavien viestien osalta viestisyötteiden lisääminen tietokantaan tapahtuu järjestelmänvalvojan yksinoikeudella. Syötteiksi tullaan valitsemaan erilaisia viestejä omista sähköposteista tai tekstiviesteistä. Myös näiden kohdalla tulee kiinnittää erityistä huomiota viestien sisältöön niin, etteivät ne sisällä henkilötietoja, tilausnumeroita tai muuta sopimatonta sisältöä, joiden joutuessa vääriin käsiin voi aiheutua harmia asianosaisille.

4.2 Sovelluksen tekninen toteutus ja kehitys

Verkkosovelluksen kehitys suoritettiin moderneja JavaScript verkkokehityskehyksiä hyödyntäen full-stack toteutuksena. Full-stack sovellukset koostuvat front-end sekä back-end puolista. Front-end puoli hallitsee pääosin sovelluksen ulkoasua, kun taas back-end puolella hoidetaan muun muassa tietokannan toiminta ja API-kutsuihin reagointi. Tämän sovelluksen back-end puoli kehitettiin Node.js ja Express kehityskehysten avulla. Viestisyötteiden ja järjestelmänvalvojan tunnusten tallennukseen ja osana back-end puolta hyödynnettiin MongoDb tietokantaa. MongoDb on niin sanottu NoSQL tietokanta, jossa tiedot tallennetaan dokumentteina perinteisten relaatioiden sijaan ja ovat siten helppokäyttöisempiä ja joustavia (MongoDb). Front-end puoli kehitettiin React kirjaston avulla luomalla eri tarkoituksiin soveltuvia komponentteja ja yhdistelemällä niitä. Lisäksi käyttöliittymän osalta käytössä oli Material UI komponenttikirjasto, jonka avulla huolehdittiin johdonmukaisen ja skaalautuvan ulkoasun toteutumisesta.

Huijausviestien keruuta varten kehitetty keruulomake haluttiin tehdä mahdollisimman yksinkertaiseksi, jolloin parhaimmillaan syötteen lähetys onnistuu helposti lisäämällä kuvan, hyväksymällä ehdot ja painamalla lähetä-nappia. Lisätietojen keruuta varten lomakkeeseen lisättiin ruutu, jota napsauttamalla näiden tietojen syöttäminen onnistuu kohtuu vaivatta. Syötteiden keruulomake on nähtävillä seuraavassa kuvassa.



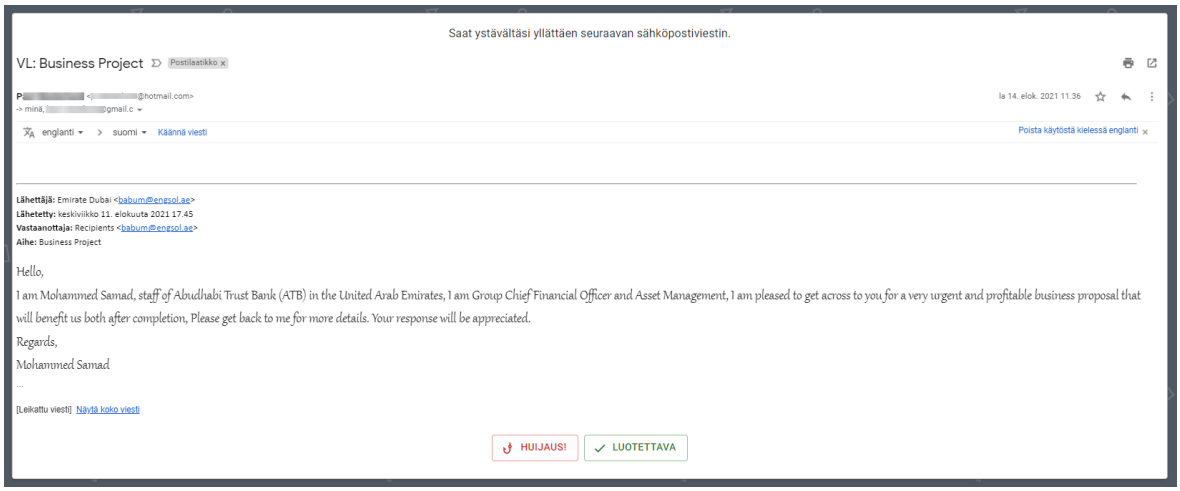
Kuva 5. Huijausviestisyötteiden keruulomake

Verkkosovelluksen ensimmäisen julkaisun jälkeen lomakkeeseen lisättiin yksinkertaiset ohjeet syötteiden lisäämiseksi, sillä puutteellisten ohjeiden myötä osa syötetyistä tiedostoista olivat väärässä muodossa. Samanaikaisesti myös lähdekoodin puolelle lisättiin syötteiden tarkastukset.

Kuvassa 5 näkyvää lähetä-nappia painamalla viestisyöte ohjautuu tietokantaan järjestelmänvalvojan nähtäville. Kaikki lomakkeen kautta lähetetyt viestit siirtyvät ensin niin kutsuttuun odotustilaan ennen siirtoa pelissä käytettävien kuvien joukkoon. Odotustilassa olevat viestit tarkistetaan, niille lisätään mahdollisesti puuttuvat huijauksen piirteet, vastausteksti, sekä tarvittaessa myös taustatarina. Mikäli viesti ei sovellu käytettäväksi osana peliä se voidaan poistaa tietokannasta.

Yllä mainitut viestisyötteiden tarkastukset ja muokkaamiset tapahtuu vain järjestelmänvalvojalle luodussa hallintapaneelissa. Odotustilassa olevien viestien lisäksi hallintapaneelissa voidaan listata kaikki tietokannan viestisyötteet, ja täydentää myös niitä tarvittaessa. Yhtenä hallintapaneelin tärkeimmistä ominaisuuksista on lomake, jonka avulla voidaan lisätä luotettavia viestisyötteitä tietokantaan ja osaksi peliä.

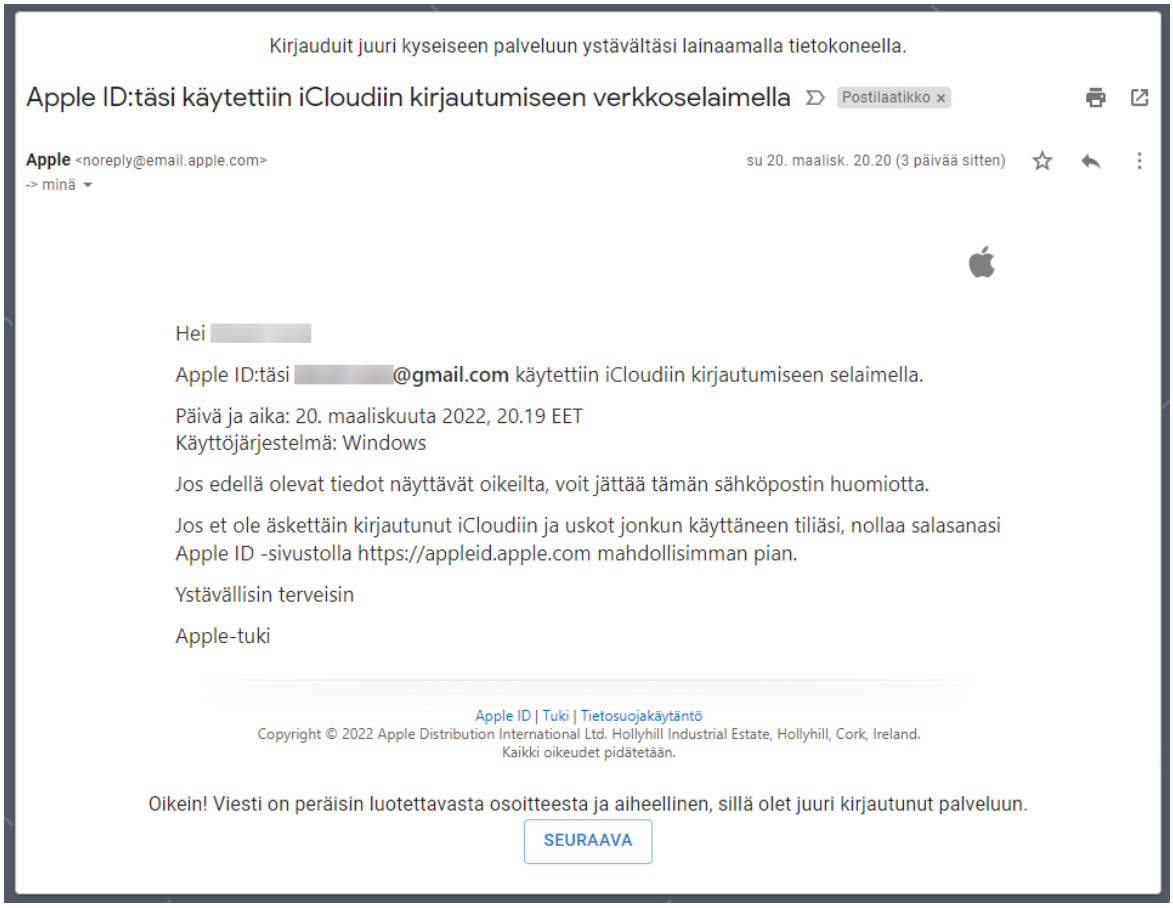
Itse pelin kehitys oli melko suoraviivaista, eikä lopputulos eronnut juurikaan suunnitelmasta. Vaikka sovelluksen kehityksessä huomioitiin skaalautuvuus eri näyttökokoihin, kehitettiin itse peli kuitenkin lähtökohtaisesti työpöytäversiossa käytettäväksi vaihtelevien kuvakokojen vuoksi. Kuvassa 6 esitetään esimerkki pelin vaiheesta, jossa käyttäjä määrittelee viestin huijaukseksi tai luotettavaksi. Määritys tapahtuu painamalla kuvan alareunassa näkyviä nappuloita. Painalluksen jälkeen nappuloiden yläpuolelle ilmestyy teksti, jossa käyttäjälle ilmoitetaan oikea vastaus, tietokannan kuvalle ominaisen tekstin muodossa.



Kuva 6. Esimerkki pelissä esiintyvästä huijauksesta

Kuvassa on tavanomainen pelissä näytettävä huijausviestisyöte, joka on varustettu pienellä taustatarinalla, jonka avulla pohjustetaan viestiä edeltävä tilanne. Lisäksi kuvassa esiintyvät henkilökohtaiset tiedot on sensuroitu. Kuitenkin tavanomaisesta huijauksesta poiketen myös viestin uudelleenlähettäjä ja vastaanottajat on sensuroitu, sillä kuten taustatarinasta ilmenee, on lähettäjä vastaanottajan ystävä.

Seuraavassa kuvassa 7 esitetään esimerkki pelin vaiheesta, jossa huijauksen tilalla näytetään luotettava viestisyöte. Kuvassa vastausnappuloiden tilalla on seuraava- nappula, jota napsauttamalla käyttäjä siirtyy pelissä seuraavaan vaiheeseen. Mikäli kyseessä oli tietokannasta arvottujen syötteiden viimeinen huijaus, siirtyy käyttäjä loppuruutuun, jossa ilmoitetaan lopulliset pisteet. Muussa tapauksessa käyttäjä siirtyy seuraavan huijauksen tunnistusvaiheeseen.



Kuva 7. Esimerkki pelissä esiintyvästä luotettavasta viestistä

Kuten kuvasta näkyy, käyttäjä on vastannut kysymykseen oikein ja näkyvillä on tulos, sekä viestille ominainen vastausteksti. Kullekin syötteelle on luotu omat vastaustekstit, jotka näytetään käyttäjän vastattua kysymykseen. Riippumatta käyttäjän vastauksen oikeellisuudesta, pysyy vastausteksti aina samana.

Verkkosovelluksen julkaisuun hyödynnettiin Tieteen ja Tietotekniikan keskuksen tarjoamaa konttiteknologiaan perustuvaa rahti palvelua, joka mahdollisti niin tietokannan kuin itse lähdekoodin pyörittämisen. Julkaisu suoritettiin suunnitelman mukaisesti heti viestienkeräysominaisuuden valmistuttua. Vielä tässä vaiheessa peliominaisuus pidettiin pois käytöstä, sillä sen avaaminen edellytti riittävästi viestisyötteitä ja järjestelmänvalvojan toimia.

Myöhemmin syötteidenkeruun ja jatkokehityksen seurauksena peliosio voitiin avata käyttäjien saataville. Julkaisuvaiheessa huijausviestisyötteitä oli kertynyt lähes sata, joista suurin osa koostui sähköpostihuijauksista. Järjestelmänvalvojan lisäämiä luotettavia viestisyötteitä puolestaan oli kertynyt noin parikymmentä. Valtaosa viestisyötteistä kerättiin lähipiiriin kuuluvien ystävien, sekä omista sähköposteista ja tekstiviesteistä.

4.3 Verkkopelin arviointi

Yksi suunnittelutieteen tutkimusmenetelmään kuuluvista vaiheista on arviointi. Arvioinnin tarkoituksena on tarkkailla ja mitata kuinka tuotettu artefakti soveltuu ongelman ratkaisuksi (Peffers *et al.*, 2006). Tyypillisesti suunnittelutieteen tutkimus toteutetaan useissa iteraatioissa. Iteraatioiden aikana ratkaisun sen hetkistä riittävyyttä arvioidaan, jolloin seuraavassa iteraatiossa ratkaisua voidaan kehittää arvioinnin pohjalta yhä paremmaksi. Tässä työssä kandidaatintyön asettamien aikarajoitteiden takia arviointi suoritettiin ainoastaan ratkaisun valmistuttua.

Verkkopelin, eli suunnittelutieteen avulla luodun artefaktin varsinainen arviointi suoritettiin kyselyn avulla. Kyselyn tarkoituksena oli arvioida pelin tilaa ja selvittää, mikäli huijausviestien tunnistukseen kehitetty peli oli koulutusmenetelmänä toimiva. Tässä yhteydessä pelin tilan arvioinnilla tarkoitettiin muun muassa yleisen vaikeustason kartoitusta. Täytettävä kyselylomake koostui kuudesta kysymyksestä, joista viiteen oli vastattava. Pakolliset kysymykset vastausvaihtoehtoineen on esitelty taulukossa 5. Viimeinen kysymys oli valinnainen ja vapaamuotoinen palaute peliin liittyen.

Taulukko 5. Pelin palautekyselyn pakolliset kysymykset ja niiden vastausvaihtoehdot

Kysymys	**Vastausvaihtoehdot**
1. Pelissä saadut pisteet?	0–10
2. Pelin vaikeustaso?	1 (Erittäin helppoa) – 5 (Erittäin vaikeaa)
3. Olivatko vastaustekstit tarpeeksi informatiivisia?	Kyllä / Ei
4. Olivatko kuvien yläpuolella näkyvät pienet taustoittavat tekstit tarpeellisia?	Kyllä / En kiinnittänyt huomiota / Ei
5. Oliko peli opettavainen?	Kyllä / Ei

Kysely suoritettiin anonyymisti, eikä yksittäisiä vastauksia voitu yhdistää vastaajiin. Vastaajille jaettiin kyselylomake, joka sisälsi kysymysten lisäksi linkin verkkopeliin. Ennen kysymyksiin vastaamista käyttäjät pelasivat verkkopelin läpi vähintään kerran, jonka jälkeen kysely suoritettiin.

Kyselyyn osallistuneet vastaajat tulivat pääosin lähi- tai yliopistopiireistä, jonka vuoksi kyselyyn vastanneiden määrä jäi melko pieneksi. Vastauksia saatiin 37 kappaletta. Kyselylomakkeen yhteenveto on esitelty liitteessä yksi kysymyksittäin. Vastauksia tarkastelemalla

voitiin tehdä havaintoja, mutta niitä ei kuitenkaan voida pitää erityisen luotettavina otoskoon ollessa ainoastaan 37.

Vaikeustaso

Kyselyssä pelin vaikeustasoa kartoittavien kysymysten yksi ja kaksi mukaan pelin nykyinen vaikeustaso on tasoa erittäin helppo – helppo. Kysymysten tuloksissa on huomattavissa selkeää korrelaatiota. Yli 80 % vastaajista on saanut pelissä yli 8 oikein ja samoin yli 70 % vastaajista on määritellyt vaikeustason numeroasteikolla tasolle 1–2 (erittäin helppo – helppo).

Vastaustekstit ja taustatarinat

Vastauksista valtaosan mielestä pelissä näytetyt vastaustekstit olivat tarpeeksi informatiivisia. Ainoastaan yksi vastaus oli eri mieltä. Taustatarinoiden osalta vastauksissa oli enemmän hajontaa. Noin 60 % vastanneista olivat sitä mieltä, että taustatarinat olivat tarpeellisia. Lähes kaikki muut vastasivat, etteivät kiinnittäneet huomiota kuvien yläpuoleisiin taustatarinoihin. Vain yhden vastauksen mukaan taustatarinat olivat turhia.

Opettavaisuus

Vastauskyselyn viimeiseen pakolliseen kysymykseen saatiin ainoastaan 28 vastausta, sillä kysymys täydennettiin joukkoon muiden kysymysten jälkeen. Kysymykseen vastanneista yli 80 % (23kpl) kokivat pelin opettavaisena, jonka vuoksi luotu artefakti voidaan määritellä onnistuneeksi.

Vapaa palaute

Vapaan palautteen muodossa (13kpl) saatiin kerättyä paljon niin yleisiä kommentteja kuin sovelluksen jatkokehityksen kannalta arvokasta tietoa. Ainakin muutaman vapaan palautteen perusteella peliin kaivattaisiin enemmän luotettavia viestisyötteitä, haastavia huijausviestejä, ja vähemmän samankaltaisia syötteitä. Myös taustatarinoiden ja vastaustekstien sijaintia tai tekstin muotoa voitaisiin korostaa näkyvämmäksi. Lisäksi lopetusnäkymään kaivattiin lisää opettavaista sisältöä, tai esimerkiksi mahdollisuutta tarkastella omia vastauksia.

5 Johtopäätökset ja yhteenveto

Seuraavissa alaluvuissa suoritetaan johtopäätökset ja yhteenveto. Johtopäätöksissä pohditaan ja vertaillaan muun muassa työn keskeisiä tuloksia ja niiden merkitsevyyttä. Yhteenveto alaluvussa käydään läpi tutkimuksen kulku, tulokset ja lopulta päätetään työ mahdollisiin jatkotutkimusmahdollisuuksiin.

5.1 Johtopäätökset

Systemaattisen kirjallisuuskatsauksen lopputuloksena muodostetussa kuplakaaviossa (kuva 3) valtaosan tutkimuksissa käsitellyistä huijaustyyleistä muodosti tietojenkalastelu. Kuitenkin verkkosovelluksen avulla kerätyistä viestisyötteistä suurimman osan muodosti erilaiset petosviestit tai muu roskaposti, ja pienemmän osuuden tietojenkalasteluviestit. Eroavaisuuden voisi selittää se, ettei huijausviestien lajittelu omiin tyyleihinsä ole helppoa. Useimmat viestit voivat sisältää piirteitä monista tyyleistä, esimerkiksi tietojenkalasteluviesti voi sisältää petosviesteille ominaisia piirteitä kuten tarinatyylistä kerrontaa, tai liitetiedostoja. Voidaan ajatella tietojenkalastelun olevan melko yleispätevä huijausluokka.

Kuplakaavion ja kerättyjen huijausviestien suhteen oli kuitenkin myös yhtäläisyyksiä. Kuplakaaviossa hyökkäysvektorien tapauksessa sähköpostin välityksellä toimivia huijauksia käsiteltiin valtaosassa tutkimuksista, tekstiviestitse tapahtuvia huijauksia puolestaan käsiteltiin vähemmän. Sama ilmiö oli havaittavissa myös peliin kerätyistä huijausviestisyötteistä, jossa sähköpostihuijauksia oli lähes nelinkertainen määrä tekstiviestihuijauksiin verrattaessa.

Verkkosovelluksen huijausviestisyötteitä tarkasteltaessa viesteistä voitiin määrittää kaksi ääripäätä: useimmat viesteistä voitiin todeta oitis ilmiselviksi huijauksiksi, kun taas pieni osa viesteistä olivat selkeästi ammattimaisempia ja tunnistaminen vaati jo hieman laajempaa tarkastelua. Tähän vaikuttaa varmasti se, että kerätyt huijausviestit koostuivat lähinnä yleispätevistä massahuijauksista, eli roskapostista. Joukossa ei ollut juurikaan kohdennettuja ja siten huolellisemmin rakennettuja huijauksia, joita käytetään usein yrityksiä koskevissa huijausviesteissä. Yrityksiä koskevat huijausviestit rajattiin jo työn alussa pois tutkimusalasta, sillä niiden kerääminen voisi olla selkeästi työläämpää.

Pelin arviointimenetelmänä käytettiin kyselyä, jonka tavoitteena oli kerätä tietoa sen soveltuvuudesta osana tietoturvakoulutusta. Kyselyn pienen otoskoon vuoksi tuloksia ei voida pitää merkittävinä, mutta niitä voidaan pitää tärkeinä pelin jatkokehityksen ja yleisen arvioinnin kannalta. Koska kyselyyn vastanneet henkilöt voidaan pääosin määritellä diginatiiveiksi, tulee huomioida se, että tulokset voivat poiketa suuntaan tai toiseen arvioidessa peliä eri käyttäjäkunnalla, esimerkiksi lapsilla tai vanhuksilla. Lisäksi opettavaisuutta arvioidessa yksi kysely voi olla riittämätön ja sen sijaan sen arviointi voisi vaatia kyselyitä ennen- ja jälkeen pelin.

5.2 Yhteenveto

Tutkimuksen tavoitteena oli rakentaa opettavainen verkkopeli, jossa käyttäjien tavoitteena on erottaa huijausviestit luotettavista viesteistä ja siten toimia tietoturvakoulutuksena lisäten käyttäjien tietoturvallisuustietämystä. Opettavainen peli ja siihen liittyvä verkkosivu toteutettiin suunnittelutieteen menetelmää soveltaen. Ennen verkkosovelluksen suunnittelua ja kehitystä tuli kuitenkin selvittää taustatietoja siitä, millaisten huijausviestien avulla tavanomaisia älylaitteiden käyttäjiä yritetään huijata. Taustatiedot selvitettiin systemaattisen kirjallisuuskatsauksen avulla.

Systemaattisen kirjallisuuskatsauksen avulla saatiin selvitettyä huijausviestien alaa, erilaisia huijaustyylejä, viesteille ominaisia piirteitä, sekä ohjeita huijausviestien uhriksi joutumisen välttämiseksi. Katsauksen perusteella voitiin todeta huijauksien kirjon olevan laaja. Tietojen myötä saatiin myös vastaukset tutkimuskysymyksiin yksi ja kaksi, joiden tarkoituksena oli pohjustaa tietopankkia, jota hyödynnettiin verkkopelin suunnittelussa ja kehityksessä.

Kolmanteen tutkimuskysymykseen vastaamiseksi kehitetty verkkosovellus suunniteltiin ja toteutettiin suunnittelutieteen tutkimusmenetelmää soveltaen. Systemaattisen kirjallisuuskatsauksen muodostaneen tietopankin lisäksi suunnittelu- ja kehitysvaiheissa hyödynnettiin aiemmissa tutkimuksissa opettavaiselle pelille toimiviksi todettuja ominaisuuksia. Lopulta valmis ohjelmistoartefakti julkaistiin verkkoon, ja sen toimintaa arvioitiin.

Työn lopputuloksena kehitetty ohjelmistoartefakti avaa useita vaihtoehtoja jatkotutkimukselle. Artefaktina toimivaa verkkosovellusta voitaisiin jatkokehittää lisäämällä toteutukseen esimerkiksi lokitiedot, joiden avulla voitaisiin kerätä dataa pelikerroista. Kerättyjen tietojen

avulla voitaisiin luoda laajempi kokonaiskuva käyttäjien huijausviestien tunnistustaidoista, ja siitä millaiset huijaukset tuottavat eniten vaikeuksia tai ovat helppoja tunnistaa. Yhden jatkotutkimusvaihtoehdon avaa toki myös pelin tehokkuuden mittavampi uudelleenarviointi opetusmenetelmänä. Lisäksi itse verkkosivu tarjoaa kehitysmahdollisuuksia eri kielivaihtoehtojen, uusien vaikeustasojen tai sivuston yhteyteen rakennettavan tietopankin merkeissä.

Lähteet

Ahsan Pritom, M.M. *et al.* (2020) ‘Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses’, *2020 IEEE International Conference on Intelligence and Security Informatics (ISI). 2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Arlington, VA, USA: IEEE, pp. 1–6. doi:10.1109/ISI49825.2020.9280539.

Airoldi, E. ja Malin, B. (2004) *Scam-Slam: An Architecture for Learning the Criminal Relations Behind Scam Spam*. Carnegie Mellon University.

Almoqbil, A. *et al.* (2021) ‘Modeling Deception: A Case Study of Email Phishing’, *Proceedings from the Document Academy*, 8(2). doi:10.35492/docam/8/2/8.

Arshad, A. *et al.* (2021) ‘A Systematic Literature Review on Phishing and Anti-Phishing Techniques’. doi:10.48550/ARXIV.2104.01255.

Badawi, E.M.H. (2021) ‘Towards Algorithmic Identification of Online Scams’. doi:10.20381/RUOR-27236.

Badra, M., El-Sawda, S. ja Hajjeh, I. (2007) ‘Phishing Attacks and Solutions’, *Proceedings of the 3rd International Conference on Mobile Multimedia Communications*. Brussels, BEL: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (MobiMedia ’07).

Bailey, J. *et al.* (2007) ‘Evidence relating to object-oriented software design: A survey’, *First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007). First International Symposium on Empirical Software Engineering and Measurement*, Madrid, Spain: IEEE, pp. 482–484. doi:10.1109/ESEM.2007.58.

Broadhurst, R. ja Trivedi, H. (2019) ‘Malware in Spam Email: Trends in the 2016 Australian Spam Intelligence Data’, *SSRN Electronic Journal* [Preprint]. doi:10.2139/ssrn.3413442.

Caputo, D.D. *et al.* (2014) ‘Going Spear Phishing: Exploring Embedded Training and Awareness’, *IEEE Security & Privacy*, 12(1), pp. 28–38. doi:10.1109/MSP.2013.106.

Chaganti, R. *et al.* (2021) ‘Recent trends in Social Engineering Scams and Case study of Gift Card Scam’. doi:10.48550/ARXIV.2110.06487.

Chrobok, N. (2010) *General Delivery - Receiver Driven Email Delivery*. University of Otago. Saatavissa: http://hdl.handle.net/10523/397.

Cj, G. *et al.* (2018) ‘PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness’, *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts. CHI PLAY ’18: The annual symposium on Computer-Human Interaction in Play*, Melbourne VIC Australia: ACM, pp. 169–181. doi:10.1145/3270316.3273042.

Corradini, I. (2020) *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology*. Cham: Springer International Publishing (Studies in Systems, Decision and Control). doi:10.1007/978-3-030-43999-6.

Duo, P. *et al.* (2020) 'A Multilingual Comparison of Email Scams', USENIX Association.

Duo, P. *et al.* (2021) 'Comparing Scam Emails and Email User Education at Universities', USENIX Association.

Dyrud, M.A. (2005) 'I brought you a good news: An analysis of Nigerian 419 letters', *Proceedings of the 2005 Association for Business Communication Annual Convention*, pp. 20–25.

ENISA (2010) *The new users' guide: How to raise information security awareness (EN)*. Saatavissa: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide [Viitattu: 1 helmikuu 2022].

Fagerland, V. (2017) *Automatic Analysis of Scam Emails*. Norwegian University of Science and Technology.

Fischer, P., Lea, S. ja Evans, K. (2009) 'The psychology of scams: Provoking and committing errors of judgement', *Research for the Office of Fair Trading* [Preprint].

Hartikainen, E. (2006) 'The Nigerian Scam: easy money on the Internet, but for whom', *Unpublished paper presented at Michicagoan Conference and blogged online at http://www. antropologi. info/blog/anthropology*.

Hevner, A.R. *et al.* (2004) 'Design Science in Information Systems Research', *MIS Q.*, 28(1), pp. 75–105.

Hiß, F. (2015) 'Fraud and Fairy Tales: Storytelling and Linguistic Indexicals in Scam E-mails', *International Journal of Literary Linguistics*, 4(1). doi:10.15462/ijll.v4i1.26.

Isacenkova, J. *et al.* (2013) 'Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations', *2013 IEEE Security and Privacy Workshops*. *2013 IEEE CS Security and Privacy Workshops (SPW2013)*, San Francisco, CA: IEEE, pp. 143–150. doi:10.1109/SPW.2013.15.

Jakobsson, M. (ed.) (2016) *Understanding Social Engineering Based Scams*. New York, NY: Springer New York. doi:10.1007/978-1-4939-6457-4.

Kaplan, B. ja Duchon, D. (1988) 'Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study', *MIS Q.*, 12(4), pp. 571–586.

Kerremans, K. *et al.* (2005) 'Towards Ontology-based E-mail Fraud Detection', *2005 Purtuguese Conference on Artificial Intelligence*. *2005 Purtuguese Conference on Artificial Intelligence*, Covilha, Portugal: IEEE, pp. 106–111. doi:10.1109/EPIA.2005.341275.

Kumaraguru, P. *et al.* (2010) 'Teaching Johnny not to fall for phish', *ACM Transactions on Internet Technology*, 10(2), pp. 1–31. doi:10.1145/1754393.1754396.

Kyberturvallisuuskeskus (2019) *Pornokiristyksiä runsaasti liikkeellä – älä usko huijarien väitteitä*. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/pornokiristyksia-runsaasti-liikkeella-ala-usko-huijarien-vaitteita [Viitattu: 6 helmikuuta 2022].

Kyberturvallisuuskeskus (2021) *Julkaisimme vakavan varoituksen tekstiviestitse levitettävästä haittaohjelmasta*. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/julkaisimme-vakavan-varoituksen-tekstiviestitse-levitettavasta-haittaohjelmasta [Viitattu: 6 helmikuuta 2022].

Markova, E. *et al.* (2019) 'Classification of malicious emails', *2019 IEEE 15th International Scientific Conference on Informatics*. *2019 IEEE 15th International Scientific Conference on Informatics*, Poprad, Slovakia: IEEE, pp. 000279–000284. doi:10.1109/Informatics47936.2019.9119329.

Mishra, S. ja Soni, D. (2019) 'SMS Phishing and Mitigation Approaches', *2019 Twelfth International Conference on Contemporary Computing (IC3)*. *2019 Twelfth International Conference on Contemporary Computing (IC3)*, Noida, India: IEEE, pp. 1–5. doi:10.1109/IC3.2019.8844920.

MongoDb *What is NoSQL?*, *MongoDb*. Saatavissa: https://www.mongodb.com/nosql-explained [Viitattu: 17 maaliskuuta 2022].

Newman, R.C. (2006) 'Cybercrime, Identity Theft, and Fraud: Practicing Safe Internet - Network Security Threats and Vulnerabilities', *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*. New York, NY, USA: Association for Computing Machinery (InfoSecCD '06), pp. 68–78. doi:10.1145/1231047.1231064.

Paquet-Clouston, M. *et al.* (2019) 'Spams Meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem', *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*. New York, NY, USA: Association for Computing Machinery (AFT '19), pp. 76–88. doi:10.1145/3318041.3355466.

Peffers, K. *et al.* (2006) 'The Design Science Research Process: A Model for Producing and Presenting Information Systems Research', *In: 1st International Conference on Design Science in Information Systems and Technology (DESRIST*, pp. 83–106.

Perrault, E.K. (2018) 'Using an Interactive Online Quiz to Recalibrate College Students' Attitudes and Behavioral Intentions About Phishing', *Journal of Educational Computing Research*, 55(8), pp. 1154–1167. doi:10.1177/0735633117699232.

Petersen, K. *et al.* (2008) 'Systematic Mapping Studies in Software Engineering', *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering*. Swindon, GBR: BCS Learning & Development Ltd. (EASE'08), pp. 68–77.

Qabalin, M. *et al.* (2021) 'Credit Cards Theft Using Social Engineering over WhatsApp: A Survey Study', *2021 22nd International Arab Conference on Information Technology (ACIT)*. *2021 22nd International Arab Conference on Information Technology (ACIT)*, Muscat, Oman: IEEE, pp. 1–7. doi:10.1109/ACIT53391.2021.9677454.

Razaq, L. *et al.* (2021) '"We Even Borrowed Money From Our Neighbor": Understanding Mobile-Based Frauds Through Victims' Experiences', *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW1). doi:10.1145/3449115.

Ribaux, O. ja Souvignet, T.R. (2020) '"Hello are you available?" Dealing with online frauds and the role of forensic science', *Forensic Science International: Digital Investigation*, 33, p. 300978. doi:10.1016/j.fsidi.2020.300978.

Sabillon, R. *et al.* (2016) 'Cybercrime and Cybercriminals: A Comprehensive Study', *International Journal of Computer Networks and Communications Security*, 4, pp. 165-176.

Sherry, J.L. ja Pacheco, A. (2010) 'Matching computer game genres to educational outcomes', *Teaching and Learning with Technology*. Routledge, pp. 234–246.

Sophos (2022) *Following the money in a massive "sextortion" spam scheme*. Saatavissa: https://news.sophos.com/en-us/2020/04/22/following-the-sextortion-money/ [Viitattu: 6 helmikuuta 2022].

Stabek, A., Watters, P. ja Layton, R. (2010) 'The Seven Scam Types: Mapping the Terrain of Cybercrime', *2010 Second Cybercrime and Trustworthy Computing Workshop*. *2010 Second Cybercrime and Trustworthy Computing Workshop (CTC)*, Ballarat, Australia: IEEE, pp. 41–51. doi:10.1109/CTC.2010.14.

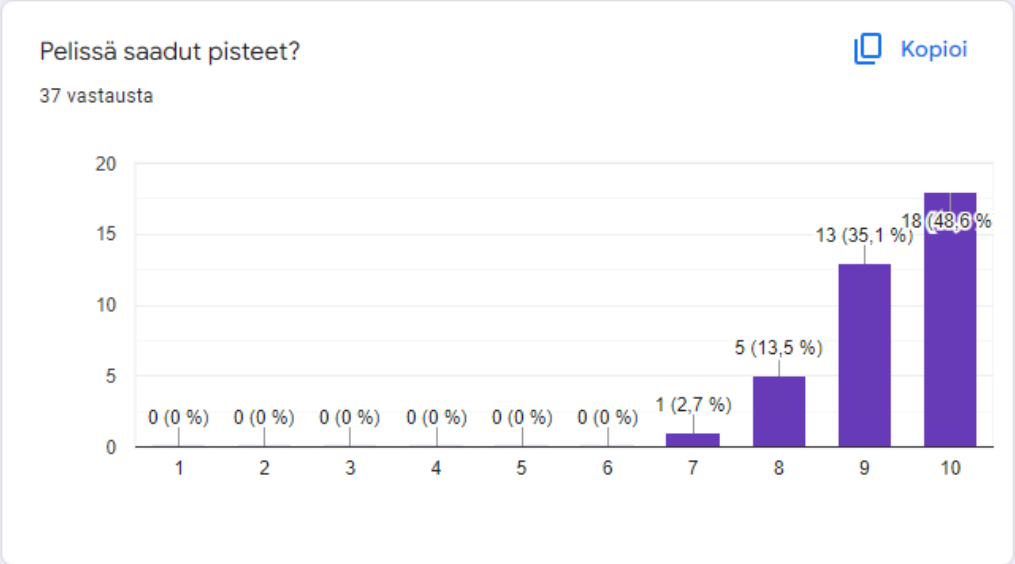
Truchero Visa, R. (2021) *Efficient smishing detector using Machine Learning techniques*. Universitat de Lleida. Saatavissa: http://hdl.handle.net/10459.1/71731.

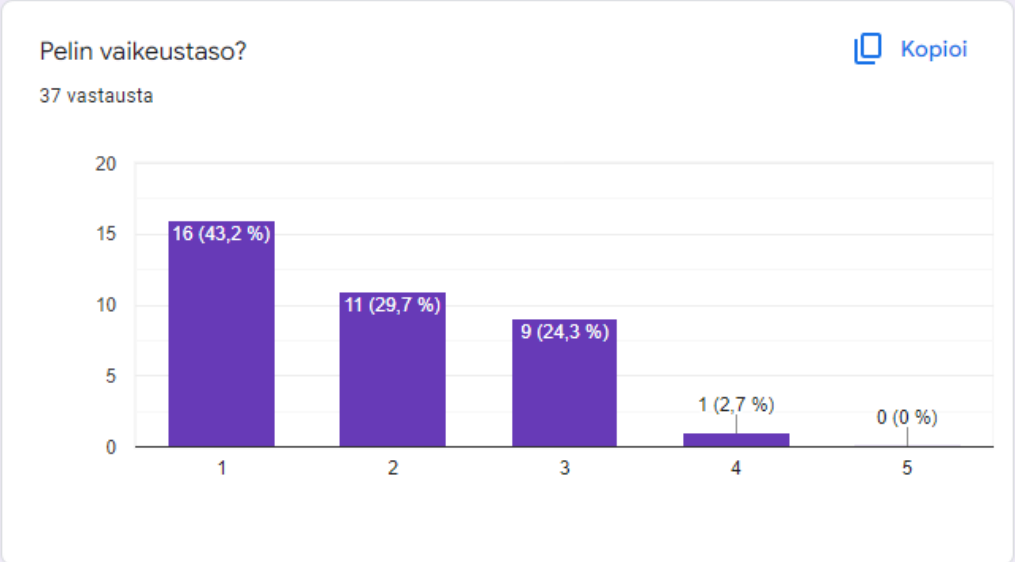
Valtioneuvosto (2017) 'Tietoverkkorikollisuuden torjuntaa koskeva selvitys'. Saatavissa: http://urn.fi/URN:ISBN:978-952-324-136-7 [Accessed: 1 helmikuuta 2022].

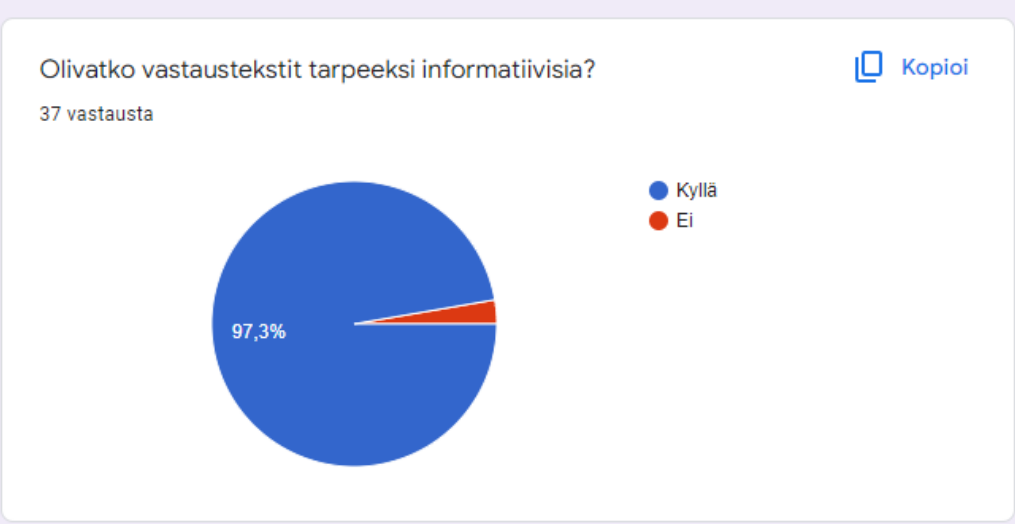
Wieringa, R. *et al.* (2006) 'Requirements engineering paper classification and evaluation criteria: a proposal and a discussion', *Requirements Engineering*, 11(1), pp. 102–107. doi:10.1007/s00766-005-0021-6.

Wilson, M. *et al.* (1998) *Information technology security training requirements :: a role- and performance-based model*. 0 edn. NIST SP 800-16. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST SP 800-16. doi:10.6028/NIST.SP.800-16.

Liite 1. Palautekyselyn tulokset kysymyksittäin (1–5)



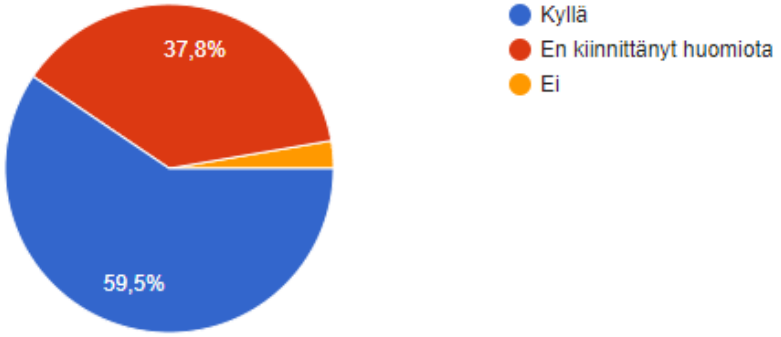




Olivatko kuvien yläpuolella näkyvät pienet taustoittavat tekstit tarpeellisia?

Kopioi

37 vastausta



Oliko peli opettavainen?

Kopioi

28 vastausta