UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Kaspar Jüristo

How to Conduct Email Phishing Experiments

Master's Thesis (30 ECTS)

Supervisor(s):
Sten Mäses
Olaf M. Maennel
Raimundas Matulevičius

Tartu 2018

How to Conduct Email Phishing Experiments

Abstract:

Phishing attacks are on the rise and more sophisticated than ever before inflicting major financial damage on businesses. Simulated phishing attacks are of growing interest in academia, however, the studies are mainly focusing on the specific angles of the phenomenon, e.g. ethical considerations; and not on the implementation itself. Author was not able to find consolidated guidelines that would walk through the whole process of conducting email phishing experiments. The aim of this study is to explore how to conduct simulated phishing experiments and to create consolidated guidelines that companies could easily implement on the example of Company X[1]. The research questions postulated for this study are: What should companies consider when conducting phishing experiments? What is the correlation between the phishing email difficulty level and the click through rate? How people react to simulated email phishing experiments? Both quantitative and qualitative research methods were applied to find answers to the research questions. Firstly, based on the existing studies, guidelines on how to conduct phishing experiments in companies were created. Secondly, phishing experiment (Experiment I) was designed and conducted among 53 participants applying a crossover research design. The employees were randomly divided into two groups (Group K) and (Group L); and they were sent in two distinct time periods two emails which corresponded to the different difficulty levels (Type X and Type Y). During the first campaign Group K was sent Type X email and Group L was sent Type Y email and during the second campaign it was vice versa. Type X email messages were designed to be targeted, grammatically correct and with relevant content. Type Y email messages were designed to be general and with visible grammar mistakes. Additionally, a spear phishing experiment (Experiment II) was conducted among two participants applying a single-subject quasi-experimental research design. The third type of emails (Type Z) that were sent out during the spear phishing experiment were personalized and relevant based on the pre-conducted research about the two targets. Thirdly, qualitative interviews were designed and conducted with the employees who participated in the simulated phishing experiments to investigate how they react to such experiments and to improve the guidelines based on their feedback. This research confirmed that the proposed guidelines are sufficient for conducting phishing experiments in a company setting. The results of this research show that 23% of the employees clicked on the link embedded to the more complex (Type X) phishing email and 11% of the employees clicked on the link embedded to the simpler (Type Y) email. Furthermore, Type Y emails were reported as phishing emails more frequently (22,6%), whereas Type X, emails were reported less (18,9%). The spear phishing experiment was successful, and the participants did not recognize the deceptiveness of the simulated phishing emails. This research shows that the phishing success rate is higher when the content is targeted and relevant. The employee awareness level about reporting phishing was low and the main stimuli for clicking on phishing links was curiosity. The findings of this study imply that people react positively to phishing experiments if these are conducted in a manner that it does not pose psychological damage or distress for the participants.

Keywords:

Phishing, experiments, social engineering, feedback method, security behaviour, security awareness.

CERCS: P170, Computer science, numerical analysis, systems, control

[1] Author impersonated real company name by encoding „Company X“

Kuidas viia läbi õngitsuskirja eksperimenti

Lühikokkuvõte:

Õngitsusrünnete hulk on aasta-aastalt kasvanud ja ründed on muutunud keerumkamaks kui kunagi varem, põhjustades ettevõtetele rahalist kahju. Akadeemilistes ringkondades on kasvanud huvi simuleeritud õngitsusrünnete vastu, kuid uuringud keskenduvad peamiselt spetsiifilistele aspektidele, nagu näiteks eetilised kaalutlused, ja mitte õngitsuseksperimendi läbiviimisele. Autor ei leidnud olemasolevate teadustööde hulgast konsolideeritud juhised, mis kirjeldaksid, kuidas viia läbi õngituskirjade eksperimenti. Käesoleva lõputöö eesmärgiks on uurida, kuidas viia läbi simuleeritud õngituskirjade eksperimenti ja luua konsolideeritud juhiseid, mida ettevõtted saaksid lihtsalt rakendada ettevõtte X[2] näitel. Lõputöö uurimisküsimused on järgnevad: Mida peaksid ettevõtted arvestama õngitsuseksperimendi läbiviimsel? Mis seos on õngitsuskirja raskusastme ja klikkimise sageduse vahel? Kuidas inimesed reageerivad simuleeritud õngitsuseksperimentidele? Antud uurimistöös kasutati nii kvantitatiivseid kui ka kvalitatiivseid meetodeid. Esiteks sai loodud konsolideeritud juhised simuleeritud õngitsuseksperimentide läbiviimiseks, mis baseeruvad eelevatel uurimustöödel. Teiseks viidi läbi õngitsuseksperiment (Eksperiment I) 53 osaleja hulgas, kasutades ristuva uuringu disaini. Töötajad jaotati juhuslikult kaheks grupiks: (Grupp K) ja (Grupp L). Neile saadeti erinevatel kuupäevadel kaks e-kirja erinevate raskusastemega: (Tüüp X) ja (Tüüp Y). Esimeses kampaanias saadeti Grupile K keerulisem kiri (Tüüp X) ja Grupile L lihtsam kiri (Tüüpi Y) ja teise kampaania ajal oli see vastupidi. Raskemad (Tüüp X) e-kirjad olid sihitud, grammatiliselt korrektsed ja relevantse sisuga. Kergemad e-kirjad (Tüüp Y) olid üldisemad ja nähtavate grammatikavigadega. Suunatud õngitsuseksperiment (Eksperiment II) viidi läbi kahe osaleja hulgas, kasutades üksikosaleja kvaasi-eksperimentaalset uurimustöö disaini. Tüüp Z e-kirjad, mis saadeti välja suunatud õngitsuseksperimendi ajal, olid personaalsed ja relevantse sisuga ning baseerusid kahe osaleja taustauuringutel. Kolmandaks kavandati ja viidi läbi kvalitatiivsed intervjuud osalejatega, kes osalesid simuleeritud õngitsusrünnetes, et uurida, kuidas nad sellistele eksperimentidele reageerivad ja parandada lähtuvalt nende tagasisidest õngituskirjade eksperimendi juhiseid. Antud uurimistöö kinnitas, et väljatöötatud juhised on piisavad, et viia läbi õngituskirjade eksperimenti ettevõttetes. Uurimistöö tulemused näitasid, et 23% töötajatest klikkisid raskemini äratuntavale e-kirjale (Tüüp X) ja 11% lihtsamini ära tuntavale e-kirjale (Tüüp Y). Lisaks raporteeriti lihtsamini ära tuntavat kirja sagedamini (22,6%) kui raskemini ära tuntavat kirja (18.9%). Suunatud õngitsuseksperiment osutus edukas ja osalejad ei saanud aru simuleeritud pettusest. Käesolev lõputöö näitab, et õngitsusrünnede edukus on suurem, kui e-kirja sisu on sihitud ja relevantne. Töötajate raporteerimise teadlikkuse tase oli madal ja üks peamisi klikkimise põhjused oli uudishimu. Selle uuringu tulemused viitavad sellele, et inimesed reageerivad simuleeritud õngitsusrünnetele positiivselt, kui need viiakse läbi viisil, mis ei tekita osalejatele psühholoogilist kahju või stressi.

Võtmesõnad:

Õngitsuskiri, eksperiment, tehnosotsiaalne sahkerdamine, tagasiside, turvakäitimine, turvateadlikus

CERCS: P170, Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

[2] Autor asendas päris ettevõtte nime Ettevõtte X-ga

List of Acronyms and Definitions

AOL	American Online
APWG	Anti-Phishing Working Group
UK	United Kingdom
PC	Personal Computer
CEO	Chief Executive Officer
US	United States
FBI	Federal Bureau of Investigation
NATO	North Atlantic Treaty Organization
CIO	Chief Information Officer
URL	Uniform Resource Locator
SaaS	Software as a Service
IT	Information Technology
SET	Social Engineering Toolkit
SCORM	Sharable Content Object Reference Model
LMS	Learning Management System
Bcc	Blind Carbon Copy
DNS	Domain Name System
SMTP	Simple Mail Transfer Protocol
CERT	Computer Emergency Response Team
CTO	Chief Technology Officer
IP	Internet Protocol
SSL	Secure Sockets Layer
FQDN	Fully Qualified Domain Name
MX	Mail Exchanger Record
SPF	Sender Policy Framework
GUI	Graphical User Interface
HTML	Hypertext Markup Language
UID	Unique Identifier
CTR	Click Through Rate
GDPR	General Data Protection Regulation
PII	Personally Identifiable Information

Table of Contents

1 Introduction

1.1 General Background and Motivation

Phishing as such is not a new concept, Symantec notes that the first instances of phishing attack they witnessed occurred in the 1990s and was targeted to America Online (AOL) [1]. The main damage associated with phishing is the cost that companies or individuals pay to deal with the phishing attacks. The average cost of phishing attacks is very high, and it has increased tremendously over the past decade. For example according to the Ponemon Institute [2], a US business with ten thousand employees spends an average around $3.77 million in one year to handle phishing attacks. Independent research company Vanson Bourne concluded from their study conducted in 2015 that 84% of organizations had experienced a spear-phishing attack, which successfully penetrated their organization. They outline that an average financial impact of a successful spear-phishing attack is around $1.6 million and the victims experienced a drop of 15% in their stock prices. [3]

APWG (Anti-Phishing Working Group) report concluded that in 2016 there were around 10% more phishing attacks comparing to the year before [4]. Similarly, IMB X-force report outlines that more than half of emails that people receive are spam and the number of emails containing malicious attachments has increased drastically over the past years [5]. This very well exemplifies that phishing is of growing concern and it cannot be overlooked by companies.

The effectiveness of technical security has increased over time and attacking computer systems using technical attack vectors is not that easy anymore and as a result, attackers have started to incorporate social means to their attack vectors [6]. The latter attacks are also known as social engineering attacks. Social engineering attacks use messages from purported legitimate sources to trick people into disclosing sensitive information [7]. As explained by Ericsson [8], social engineering aims to deceive a victim and make the victim to perform an action, which is beneficial for the attacker. For example, the attacker wishes that the victim clicks on a malicious link or opens an attachment; which, in return, enables the attacker to install malware to the victim's computer or get access to passwords. The Oxford English Dictionary [9] defines phishing as: "The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers."

1.2 Problem Statement and Contribution of author

It is author's experience of helping to conduct phishing experiments that has driven interest towards this research topic. The existing literature and reports on email phishing experiments highlight the importance of testing and measuring cyber security awareness and many studies have been conducted regarding that. Less attention is given to the framework and guidelines of the email phishing experiment itself, in particularly, how to conduct email phishing experiments.

The information about email phishing experiments is scattered between the research papers and author has not been able to find consolidated guidelines that would walk through the whole process of conducting email phishing experiments in a simple easy-to-implement way. During the past decade, however, many companies have started to run simulated phishing campaigns in their organizations to investigate how security-savvy their employees are, but there are no standardised instructions. The aim of this study, therefore, is to develop consolidated easy-to-implement guidelines for companies on how to conduct phishing experiments and to describe in-depth the process, including legal, technical and ethical aspects

that organizations should consider. These guidelines are then tested in a company setting. The selected company wished to remain anonymous and is, therefore, referred to as Company X.

This research seeks to address the following research questions:

- What should companies consider when conducting phishing experiments?
- What is the correlation between the phishing email difficulty level and the click through rate?
- How people react to simulated email phishing experiments?

To answer the research questions, this thesis aims to do the following:

- Describe different types of phishing, the factors of success and the purpose of phishing.
- Discuss and display all the necessary details pertaining to legal, ethical, psychological and technical considerations prior conducting phishing experiments.
- Create consolidated guidelines for companies on how to conduct phishing experiments.
- Test the created guidelines by conducting a phishing experiment (Experiment I) in Company X implementing a crossover experimental research design. In addition, conduct one spear phishing experiment (Experiment II) implementing a single-subject quasi-experimental research design.
- Measure what is a correlation between the phishing email difficulty level and the click through rate.
- Conduct qualitative interviews to explore how employees react to phishing experiments and how to improve the guidelines.
- Give recommendations to Company X on how to improve the process of conducting phishing experiments.

1.3 Outline of the Thesis

The aim of this thesis is to create and test guidelines for conducting phishing experiments. This thesis is composed of seven chapters, which are organized as follows.

- Chapter 1. Introduction – general overview and introduction to the theses.
- Chapter 2. Related Work - outlines the previous research that has addressed phishing experiments and defines the concept of phishing.
- Chapter 3. Creating Phishing Experiment Guidelines – outlines the process of conducting phishing experiments.
- Chapter 4. Methodology - describes the underlying methodology and research design process.
- Chapter 5. Implementation of an Email Phishing Experiment – describes the implementation of the phishing experiment and the results.
- Chapter 6. Implementation of an Email Spear Phishing Experiment – describers the implementation of the spear phishing experiment and the results.
- Chapter 7. Discussion and Conclusion – provides proposals for improvement, ideas for future research and discussions on main results, limitations.

1.4 Acknowledgments

I would like to thank the Company that agreed to participate in this research, in particularly, the CIO and the IT Helpdesk, who helped to conduct the phishing experiments. Additionally, Tallinn Technology University for allowing to use its infrastructure and my supervisors for their advice and recommendations.

2 Related Work

This chapter analyses the existing literature on phishing; what has been researched before and what have been the main results. Furthermore, the concept of phishing is scrutinized, and the key factors of successful phishing outlined.

2.1 Existing Similar Studies Review

Different studies have been conducted regarding phishing. In this chapter some of the relevant similar studies in related field of research are summarized, including the purpose of these studies and main conclusions.

Jakobsson and Myers [10] were one of the first ones to comprehensively study phishing and they built a framework for studying the attack and its countermeasures. Their study focuses on describing how phishing works and what should be the defence mechanisms, but it is not deep diving into the process of phishing nor providing guidelines for conducting phishing experiments.

In order to understand what is phishing and how it is used C. Hadnagy and M. Fincher [11] in their book describe phishing and spear phishing, underline the psychological reasons (*reciprocity, obligation, concession, scarcity, authority, consistency & commitment, liking* and *social proof*) why phishing works. They establish a framework of categorisation based on the email difficulty levels (*level 1-4*). Wright and Marett [12] focus on experiential and dispositional factors that increase the likelihood of detecting phishing. They found that experiential factors (e.g., computer self-efficacy, web experience and security knowledge) significantly influenced the success of deception. Both studies highlight the importance of email difficulty levels and provide insights how to develop phishing email content based on the experiment participants' security awareness.

Finn and Jakobsson [13] describe ethical aspects of phishing and concluded that when ethical aspects are not considered as important or even neglected, phishing simulation participants may get a sense of victimization or irritation. Several other studies exist, which have found ways how to solve the ethical issues and measure users who are vulnerable for phishing attacks without causing them any distress [14][15]. Likewise, El-Din [16] focuses on describing ethics committees' researchers' and professional bodies' perspective on ethical views about deceptive phishing research. She outlines that the use of deception in phishing research can be safe if done correctly. Both studies are focusing on one angle of phishing experiments, i.e. ethical principles and outlining important aspects of conducting ethical research, and not deep diving into the process of conducting phishing campaigns.

Deanna D. Caputo [17] and his colleagues highlight the need to collect qualitative feedback from the participants after the spear phishing experiment, e.g. conduct interviews with the participants to gain a better understanding of how people behave in phishing experiments. In addition, their results indicate that experiment reports and tailored framing do not necessarily suffice to reduce click rates of simulated phishing experiments and, therefore, have little impact on participants' future behaviour.

Two studies bring out key points on how to avoid legal issues when conducting phishing experiments[11][18]. The main legal risks that the researchers are exposed to are violations of a provider's terms of use, intellectual property rights and copyright infringement. It is crucial to understand legal aspects not to intentionally violate laws.

Kumaraguru [19] and his colleagues highlight that phishing assessment and training effects might be lost somewhere between 28 days and conclude that regular simulated phishing assessments are needed to educate participants. Sheng and his colleagues [20] developed

PhishGuru, which is an anti-phishing training solution enabling organizations to train their employees. Participants are periodically sent out training emails in the form of simulated phishing emails and when employee falls for the simulated phishing attack, PhishGuru provides a short training to avoid falling for attacks in the future. Similarly, to Kumaraguru and his colleagues, PhishGuru studies emphasise that practise of sending security notices is not sufficient and follow up trainings with participants should be conducted to teach people how to avoid phishing attacks.

In his research, Kaspar Prei [21] concluded that phishing assessment is an efficient way to measure personnel cyber security awareness level. The strength of his work is that he describes well how to conduct email phishing experiments; however, he does not investigate spear phishing emails and does not develop easy-to-implement guidelines that companies could use to conduct phishing experiments.

Table 1. summarizes the objectives and findings of the above mentioned and other selected studies in the related field of research. The table exemplifies that the focus of the studies has been mainly on behavioural and ethical aspects of phishing, outlining the main reasons why phishing works and how to prevent it, what are the vectors of success and consequences of phishing attacks.

Table 1. Summary of Phishing Studies

Study	Objective	Relevant findings
Designing and Conducting Phishing Experiments [13]	To describe what are the procedural aspects to consider, while conducting phishing experiments.	Outlining ethical and technical details associated with conducting phishing experiments is important as it enables the development and testing of hypotheses and countermeasures.
Ethics and Phishing Experiments [22]	To examine the ethical questions related to phishing experiments in the real-world settings and to explore if the experiments can be conducted ethically if there is an opt-out option for participants and they are debriefed afterwards.	Phishing experiments include deception and contravene informed consent requirements; however, these can be conducted ethically if risks are minimized and the confidentiality and the privacy of participants is protected.
Legal Risks For Phishing Researchers [18]	To describe the legal risks that researchers may be exposed to.	The main risks are violations of a provider's terms of use, intellectual property rights and copyright infringement.
Measuring Personnel Cyber Security Awareness Level Through Phishing Assessment [21]	To suggest an efficient way to measure personnel cyber security awareness level.	An efficient to measure personnel cyber security awareness level was found to be phishing assessment.

Study	Objective	Relevant findings
Teaching Johnny Not to Fall for Phish [20]	To determine whether simulated phishing emails help individuals to detect real phishing attacks.	Authors developed a methodology called PhishGuru, which was approved to be effective in educating individuals about phishing attacks.
Phishing Dark Waters [11]	To describe phishing and why it works and how to better defend against it.	The success of social engineering is based on the conscious guiding of target's choices in other words influencing them. Authors developed a „Principles of Influence" framework to better describe it. There is no one-stop solution to defend against phishing attacks, but with good planning companies can take steps to mitigate the risks.
Using Phishing Experiments and Scenario-Based Surveys to Understand Security Behaviours in Practice [8]	To investigate if there is a correlation between adding personal information about the target to an attack and the successfulness of the attack.	The research results indicate that if information about the target is included into the attack, it is more likely that the attack will be successful.
Baiting the hook: factors impacting susceptibility to phishing attacks [23]	To outline the main factors that influence susceptibility to phishing attacks.	Firstly, in terms of demographic characteristics of individuals and their ability to detect a phishing attack, gender and the years of PC usage have a statistically significant impact. Secondly, in terms of time-related factors, pop-up-based attacks have a higher success rate. Thirdly, psychological anchoring effect has an impact as well.
To Deceive or Not to Deceive! Ethical Questions in Phishing Research [16]	The study discusses the need for deception, the possible consequences of deceptive activities and describes legal restrictions of conducting phishing studies in the context of the UK.	The outcome of the study is a roadmap for researchers to consider ethical and legal aspects prior conducting a research.

2.2 Defining Phishing

This paragraph gives an overview of different types of phishing, firstly, based on the technique and, secondly, based on the attack type. Further on, it is described what is the main difference between the techniques and how to recognize these in practise.

2.2.1 Definition of Phishing

Phishing can be explained as an activity, which involves sending emails from seemingly reputable sources with the purpose to obtain personal information or influence email receivers. This practise combines both social engineering and technical skills. It varies in its form, for example it could be an attachment within the email that loads malicious software into the computer or it could be a link to an illicit website. The website can trick the receiver into downloading malware or to disclose personal information. [16][11] Different types of phishing techniques can be identified. In the following spear phishing, whaling and clone phishing are further described.

Spear Phishing

Spear phishing is a targeted form of phishing. This means that attackers take some time to study the target and gather information about them to create personal and relevant messages. Therefore, it is very difficult to discover and protect against spear phishing [11].

Whaling

Whaling is the more advanced form of phishing and is targeted to executive level employees. The content is crafted to target an upper manager such as a CEO or some supervisor who has access to critical data and accounts. For example, the whaling email or website may come in the form of a false order, a legal complaint or a fake message from authorities. [24]

Clone Phishing

Clone phishing is a type of phishing attack by which the target is sent a cloned email replicating a legitimate and previously delivered email. The email address is spoofed to appear as authentic and attachment or a link from a legitimate email is replaced with a malicious version. For example, quite often the new email is said to be an updated version of the original email. This technique may also be used to gain access to another machine by exploiting the social trust referring to the connection between the parties receiving the original email. [25]

Furthermore, phishing emails can be divided based on the phishing attack type. In the following different forms of phishing pertaining to credential stealing, action-based emails and exploitative emails are described.

Credential stealing

The most usual form of phishing involves the sending of a deceptive email to a target, which at some point redirects the target to a malicious website, which looks legitimate. Since the website looks legitimate, victims are willing to enter their credentials (e.g., usernames and passwords), and depending on a person maybe even financial information. [23]

Action

Action-based phishing emails are widely targeted to businesses. Business email compromise scam is primarily a social engineering attack in which attackers send an email pretending to be a company official and it is normally sent to an emplyee responsible for comapny funds

urging the employee to wire money or leak other critical data. The email may be sent from a domain similar to that of the company's domain, or from an actual account which has been taken over. The US Federal Bureau of Investigation (FBI) highlighted that the loss of such attacks is estimated to be more than 3.1 billion us as of June 2016. [5]

Exploit

Opening attached malware or clicking on a malicious link can infect computer. Attached malware can be, for example, a malicious PowerShell script or an Excel file with malicious macros. PowerShell and macros are default features of Windows and Microsoft Office, which can provide remote access and malware downloads without the use of malicious tools or vulnerabilities [26]. A malicious link could leverage browser exploits to install malware or spyware on the victim's system. Such exploits are used by attackers to compromise network security. [27]

2.2.2 Why Phishing Works

Phishing attacks have evolved over time and while most of the earliest phishing emails were easily recognizable containing obvious mistakes and bad grammar, phishers have become more sophisticated and imitate enquiries from trusted sources [28]. To mitigate the risks of phishing and protect businesses, organizations and individuals against phishing attacks, it is important to understand the factors that affect susceptibility to phishing schemes, which helps to develop effective countermeasures [29].

The success of social engineering is based on the conscious guiding of target's choices in other words influencing them. To better describe why phishing works, author of this thesis uses the „Principles of Influence" framework being described by C. Hadnagy and M. Fincher that consists of eight principles *reciprocity, obligation, concession, scarcity, authority, consistency & commitment, liking* and *social proof*. See Figure 1. It is important to emphasise that these principles most often work together in different interactions

Figure 1. Principles of Influence [11]

The principle of reciprocity is based on a belief that people should return gifts (something that the receiver values). For example, if the target is offered a refund they feel that in return they must give something back (personal information). [11][30]

The principle of obligation creates influence through customs and manners by appealing to something about their identity. For example, fraudsters pretend to be grandkids in trouble and create a sense of obligation to help. [11]

The principle of concession is when a person yields. For example, fraudsters imply that power has been granted to the target. The reason why it works is that concession places the target in a difficult situation. The principle of consistency and commitment goes hand in hand with the principle of concession. After a person has complied with a request, they are likely to continue to do so. [11][30]

The principle of scarcity is created upon the lack of resources or making something to look very valuable and difficult to get. The principle of authority on the other hand is created upon a tendency of people to obey authorities and that people comply with orders coming from authorities or in an authoritative manner, for example, emails seemingly coming from a tax inspectorate. [11][31][30]

The principle of liking works by creating genuine similarities with the target and being amiable and easy to relate to. The principle of social proof is an extremely valuable principle of influence by emphasising on social nature by giving illusions that everyone is contributing by sending money. [11][30]

3 Creating Phishing Experiments Guidelines

The purpose of this chapter is to outline what companies must consider when conducting phishing experiments. This chapter describes all the steps of a phishing experiment; including ethical and legal considerations, choosing a platform, developing content, informing employees, launching the campaign and analysing results. The content for this chapter was developed over the course of the year 2017. The guidelines have been implemented and tested in Company X.

3.1 Before Launching Email Phishing Campaign

3.1.1 Purpose of Phishing Campaigns

The first question to start with is "Why?" Although the question is straightforward, how the company answers, can really shape and change the face of a phishing program. In this chapter four different reasons that author find relevant for a company to begin with are outlined.

The first reason is related to a security awareness with an aim to measure and increase the awareness within the company. Kaspar Prei [21] found that an efficient way to measure personnel cyber security awareness level is to conduct a phishing assessment. It was concluded in "Teaching Johnny Not to Fall for Phish" [20] research that using simulated phishing assessments is an effective tool to educate individuals about phishing attacks.

The second reason is related to experiencing a phishing attack within the company after which a company prioritizes awareness trainings and assessments. Phishing attacks against companies have increased tremendously in the past years [26][5]. Additionally, successful phishing attacks can make companies to lose a lot of money [32][2]. Therefore, it is of growing concern and reason among companies to conduct simulated phishing campaigns.

The third reason is related to the need to comply with regulations. For example, company policy, the board or contract negotiations can dictate the need for testing the organization. This is quite often a case with government regulations that require the company to run phishing assessments and report the results. [11]

The fourth reason is that phishing simulations are conducted as part of a penetration test. It is becoming a common practise for companies to include phishing vectors in the penetration test. There are several ways how this can be done. For example, the phish leads to a shell as it is loaded with executable files or attachments, which contain a code that allows the penetration test to connect to the corporate network. [33]

Choosing a reason to begin with a simulated phishing campaign affects the way the program is structured, which phish and vendor to use, but also the expected outcome and results. After that has been established and the company has a clear understanding why they want to run a phishing program. The next step is to understand ethical, legal and psychological aspects of phishing.

3.1.2 Ethical Considerations

Some ethics committees have a belief that is not ethical to deceive people on research purposes and that learning from experiments should not override participants' welfare because it may pose psychological damage or distress for the participants [34]. On the other hand, M.H. Boynton and colleagues [35] found in their research that necessary use of deception in research, when it is paired with correct experimenter training, conveys limited psychological harm to participants. Therefore, ethical considerations should not be neglected and taken into consideration when designing a phishing experiment.

Employees are seeing more malicious emails flooding their inboxes. According to the IBM's X-Force researchers also illustrated on Figure 2. more than half of all emails are spam and number of emails containing malicious attachments have increased tremendously. [5] Still some organizations are not conducting phishing experiments because these are unethical. This raises a challenge, how to conduct simulated phishing experiments in an ethical manner? Similarly, El-Din raises a question "Can we deceive users, if our goal is to better understand how they are deceived by attackers?" To answer his question, he elaborates that deception is a relatively new method in security related research and, therefore, it provokes ethical debate. However, it has been widely used in psychological research and the use of deception in phishing research, if done correctly, can be safe [16]

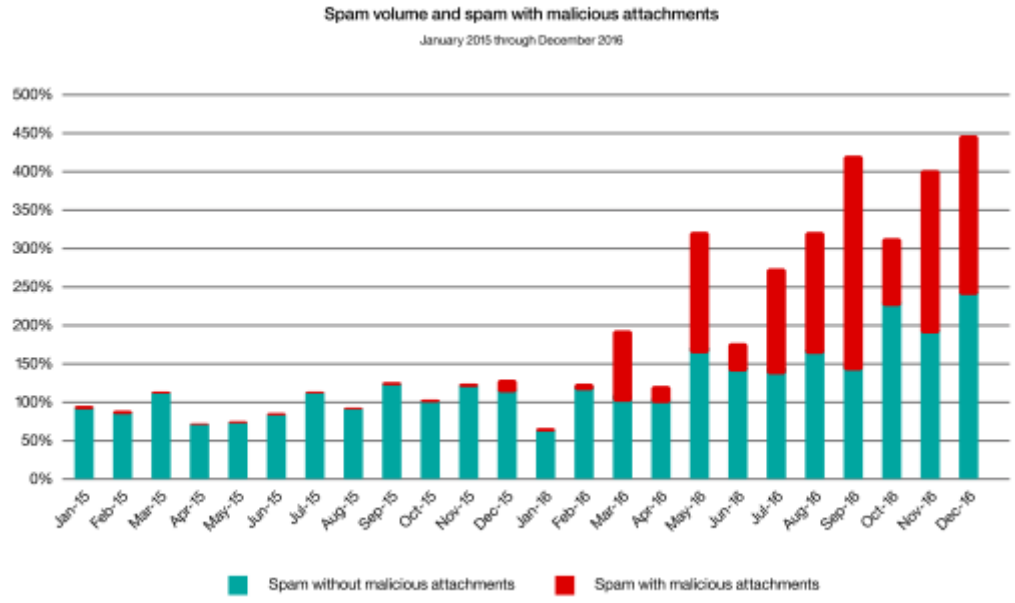


Figure 2. Spam Volume and Spam with Malicious Attachments – January 2015 Through December 2016 [5]

Phishing assessment should be conducted in a manner that it does not pose psychological damage or distress for the participants. Individuals' behaviour is unpredictable, and people react differently to phishing emails based on their personal traits, experience, environment, behavioural characteristics and, therefore; there is no unanimous response to a single email. [16][36] For example, participants are sent a phishing email requesting to pay off a debt to a debt collector. One participant can decide to call an attorney based on previous experience or existing fines. Another participant may just ignore this, because he or she is certain that there are no fines.

An ethical phishing assessment does not attack participant or try to offend them in any matter. [31] For example, an ethical phishing email cannot contain a sentence "We have naked pictures of you, click here to delete". Similarly, to protect participants' privacy, their passwords must not be saved when gathering credentials on phishing sites. It is of great importance, also because about half of people reuse the same password for different online accounts. [31][37][38] Saving participants' passwords, therefore, may pose a threat to their wellbeing.

The purpose of a phishing campaign is to provide employees with simulated environment where they can learn.[21] Employee should not feel stupid after the experiment. Employees

usually trust companies that they work for. This trust, however, cannot be established overnight, but there is a possibility to brake it with unethical activities. Therefore, employees should be notified beforehand about the phishing campaign. Notifying employees will make them feel like part of the team. This can be done via sending an email to all employees and describing the purpose of the phishing program. The process should be also explained, and clear instructions given to the employees about what they should do when receiving a phishing email.

Another thing to consider would be the impact of phishing campaigns and trainings on the employee behaviour regarding opening the legitimate emails. For example, because of phishing campaign and trainings, an employee might be too scared to open an email form an unknown sender, which may be a legitimate query from a potential customer. Therefore, it should be well thought out how to educate employees to recognize phishing emails without causing any unwanted actions regarding legitimate emails.

To summarize, when conducting a phishing campaign, it should adhere to ethical principles and not pose any threat to participants' wellbeing. The email content should not be offensive, privacy of all participants must be protected. Furthermore, employees should be informed beforehand about the awareness campaign and explained the process how to report phishing emails.

3.1.3 Legal Considerations

Phishing studies of users who participate in the experiments without informed consent can expose researchers to legal risks. The main legal issues that phishing assessments may convey are violations of a provider's terms of use, intellectual property rights and copyright infringement.[18]

Soghoian [18] highlights that due to the complexity of laws, the possibility that the research activities may have legal implications is extremely high. Researchers should work closely with respective legal teams within their organization and when needed reach out for expert help. Therefore, it is crucial to understand the legal issues because researchers may intentionally violate laws [39]. For example, a badly designed phishing experiment may lead to a circumstance where participants ask the researcher to be prosecuted [14]. The following chapter highlights some of the legal risks: data protection and privacy, collecting data, trademark and copyright, terms of service; and how to mitigate these with contractual agreements.

Data Protection and Privacy

El-Din [16] advices to comply with Human Rights Act 1998, Article 8 pertaining to the right to respect for private and family life, home, and correspondence. This includes also being mindful that the act must be balanced against the wider public interest and wellbeing. For example, El-Din describes how for their phishing experiments they used a new 'Pay As You Go' SIM card dedicated only for the experiments. It was kept secured in a locked room and after the study all data was deleted, and the SIM physically destroyed.

This example illustrates a compliant process making sure that data is protected and accessible only for relevant people and that after the campaigns all data will be deleted permanently. Likewise, all the reports should be kept secured and encrypted.

Collecting Data from a Phishing Website

According to Article 6 of the Council of Europe Cyber Convention, creating a simulated phishing website without the purpose to collect users' data, especially their credentials, is

allowed [40]. Given that the website is public, other users may unintentionally visit the website and contact authorities without knowing that the website is created for phishing assessment purposes.

In his research Kaspar Prei interviewed NATO Cooperative Cyber Defence Centre of Excellence Legal department researcher Tomáš Minárik, who emphasises that if users' credentials are collected, this is most likely done without their consent, and personal data protection rules are therefore violated. To mitigate this risk, employers should add to the employee contracts that they might be subject to security assessments, including phishing. This may still be a problem if CIO-s (or other people in charge of conducting the experiments), are collecting personal email passwords as this is not in scope of the company security testing. [21] Another option would be not to collect password data in the first place because user name is sufficient enough to conclude that the user is likely willing to give out credentials.

Trademark and Copyright

The aim of phishing assessments is to gain accurate understanding, how users are behaving when facing phishing emails and therefore the same impersonating techniques that hackers are using need to be used by CIO-s and researches. For example, if a phishing website is pretending to be a well-known company's website, there should be used a similar URL, logo, branding, names etc. This, however, may lead to infringement on a trademark and copyright rights.

Hadnagy and Fincher [11] define that "Trademarks are the words, images, phrases, and symbols used by companies to indicate that their products or services belong to them." They further elaborate that there are some requirements that a plaintiff must establish before a court will decide that someone has infringed on a trademark or used it in an unauthorised manner: [11]

- The plaintiff must prove that there is a valid trademark;
- The plaintiff must demonstrate that the same or a similar trademark was used by the defendant in relation to commercial activities without the plaintiff's consent.
- The plaintiff must demonstrate that such use of the trademark is likely to cause confusion.

They conclude that it is safer not to use trademarks for phishing purposes and not to use any real logos in phishing email simulations to advertise a product. Laws that govern the trademarks, however, differ by country and local legislation should be carefully checked to avoid any violations.

However, some SaaS anti-phishing solution providers, e.g. PhishSim [41] offer to use templates of simulated websites, which raises a question, how this is legally possible? KnowBe4 [42], which provides the claimed to be the world's largest security awareness training and simulated phishing platform, brings out on their website that trademarks could be displayed in simulated phishing emails if these are not used in a way that it confuses customers into believing that the services and/or goods originate with or are related to the company whose logo is featured. Additional way to mitigate the potential risks of confusion would be to launch an instructional video and or/a corrective landing page after the simulated attack, where customers are advised to be aware of phishing. Nevertheless, in the KnowBe4 website it is also clearly stated that they are not a law firm and therefore not authorised to provide such interpretations, but rather this is based on their experience.

In conclusion, it is safer not to use trademarks for phishing purposes. However, if there is still a need to do that, legal advice should be sought to avoid any legal consequences.

Terms of Service

As part of the phishing assessments there might be a need to gather large amount of user data from websites, such as Facebook, LinkedIn, using automated means. Websites may restrict using the bots to gather information. For example, in the terms and conditions of Facebook the following is stated:"You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission"[43]. Therefore, automated means of data collection are not always allowed, and before automated information gathering respective website's Terms and Conditions should be reviewed and when applicable permission asked from the website owners.

Agreement to Conduct Phishing Campaigns

Given all the possible legal and ethical risks outlined in the above chapters, approvals must be obtained from the board prior the phishing assessments and an agreement signed to ensure data is protected and processed in accordance with all regulations. Companies have different internal policies that outline contractual needs and what should be included to the contract when sensitive data is being handled. Based on author experience, statement of confidentiality and clear roles and responsibilities between different parties should be the minimal two clauses that the agreement consists of. One example of what should be included to the contract can be found in the chapter "Signing a Contract" on page 38.

Corporate policy, the board, and contract negotiations can also influence and dictate how the phishing assessment should to be conducted. In such cases it is good to determine a baseline, but compliance should not affect the testing to the lengths that results are affected. [11]

3.1.4 Choosing Phishing Email Difficulty Level

Different Difficulty Levels of Phishing

The common way to categorize phishing emails is that based on the difficulty level, i.e. the complexity of email content, which is further described below. Additionally, author will give an overview of categorization based on the goals of attackers and the attack type

C. Hadnagy and M. Fincher [11] have broken down phishing emails into four categories based on the difficulty level of emails. The table below summarizes the different level phishes (Table 2).

Table 2. Summarized the different level phishes

Indicator	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Greeting and Closing	Impersonal	Impersonal	Personal	Personal
Grammar	Misspellings	Some misspellings	Overall good grammar	No grammar mistakes
Messaging	Easy message, appeals on sense of greed, fear, or curiosity.	More complex, but basic, appeals on sense of greed, fear, or curiosity.	Complex message, appeals on fear or curiosity. Branding is used.	Simple and to the point. Branding is used.
Links	Email body contains links	Email body contains links	Email body contains links	Email body contains links
Sender	Unknown	Unknown	Appears legitimate	Appears legitimate
Example	Email indicating that "you have inherited millions",	Email containing "results of some test".	Branded email to "sign up for some deal".	Attached "recruitment plans" for review sent to relevant people.

A level one phishing is the easiest to detect for most average users. The main identifying characteristics are impersonal greeting, bad grammar and spelling mistakes, unlikely cause (e.g. you have inherited a million), appeals to feelings of greed, fear or curiosity, bad links (embedded phishing URL) in the email body and unknown sender. These emails seem silly, but in some cases work because of fear and greed. [11]

A level two phish is more complex and sophisticated and therefore harder to detect. The identifying characteristics are impersonal greeting, some bad grammar, messaging is more complex but rather basic, appeals to feelings of greed, fear and curiosity, bad links in body and unknown sender. Although there are many similarities with level one phishing, the main difference is the theme. The content is more personal and corporate and builds curiosity among targets by asking them, for example, to review some test results. [11]

A level three phish is about as complex and difficult to detect. Some of the indicators are personalized greeting, spelled properly, generally good grammar, complex message, bad links in body, sometimes a bad origin email addresses, but sender seems legitimate, in many cases branding. These emails seem real and the attackers are not appealing on fear but on curiosity. [11]

A level four phish is very advanced, personal. The emails have no grammar mistakes and are targeted, so that the message seems relevant to victims and something they are expecting to receive, open and read. [11]

Authors also highlight that when choosing the level for simulated phishing campaigns, one should start with the simpler phish and then based on the employee readiness move further with more difficult levels.

Choosing the Email Content Difficulty Level

Choosing the appropriate level for phishing assessments depends on, firstly, whether there have been any previous assessments conducted in the company and, secondly, at what level these have been carried out.

As outlined by Fincher and Hadnagy [11] in case there have been no phishing assessments conducted in the company, then starting from simpler phishing (level 1) makes more sense. The reason being is that if more participants will recognise phishing email and report about it, they do not feel stupid and this helps to adopt the program more easily. When starting with a more difficult phishing campaign, it is likely that less participants will recognise the phishing email and they may feel stupid and that can cause negative emotions about the program [11]. In practise, however, simpler phishing campaigns (level 1) are used less, because criminals are nowadays using more advanced phishing emails. Therefore, to prepare employees to recognize real life phishing emails, the starting point should be to conduct more difficult phishing campaigns (level 2 or level 3). [11]

In case there have been previously conducted phishing assessments in the company, earlier campaign results must be considered, and employee security awareness taken into consideration. For example, if a level 1 phishing has been previously already carried out in the company and awareness trainings have been held, it does not make sense to repeat the level 1 phishing campaign as there would be less learning for the participants.

Choosing Participants and Group Size

Conducting a phishing assessment among all employees maximises the validity of findings. However, regarding large companies it is not always realistic due to limited resources. For example, the assessment will impact the workload of the IT department as they are the point of contact for most queries. Different calculators exist to determine the ideal sample size, which would be representative of the target population with the desired confidence level. The latter is expressed as a percentage of times that different samples would produce the result. Likewise, quite often the sample is targeted, i.e. phishing emails are sent to different departments like Executive Management, Finance, Human resources etc. This enables to decrease the sample size and develop targeted phishing email content for more difficult (level 3 and 4) phishing emails. [27] In terms of validity of the results, it is also important to exclude people who are on holidays during the campaign period. When people are out of office, they do not click on the link not because they recognized a suspicious email, but simply because they are most probably not reading it in the first place and that affects the results.

3.1.5 Platform for Experiments

Three main types of technical solutions exist to perform a phishing assessment: open-source platform, commercial software, SaaS solutions. In this chapter the main features of the selected software solutions and what are the main advantages and disadvantages are described. Table 3. gives a summary of these solutions and outlines the main features.

The overview of technical solutions is based on the framework developed by Fincher and Hadnagy [11], who conducted an Internet research about the existing software solutions. Additionally, they contacted five top commercial tool service providers and two open-source project leads to carry out interviews with them to validate the findings about the outlined software features.

The limitation to their findings is that this comparison is from 2015, which means it is three years old. This is a long time in the software life cycle and it is likely that the software solutions have developed over time. Author used his developed framework about relevant features and software solutions, however, checked one by one if there have been any changes in the functionalities of selected software solutions comparing to that outlined in the initial table and improved the table accordingly. For example, WOMBAT acquired ThreatSim in 2015, which resulted in changes regarding some functionalities.

Additionally, author made improvements to the table by adding three new solutions providers (PhishSim, Gophish, Lucy), which were mentioned in the InfoSec Institute review [44] "Top 9 Free Phishing Simulators". The reviews were done using the publicly available official manuals and webpages for Rapid7 [45], ThreatSim [46], PhishMe [47], PhishLine [48], SET [33], Phishing Frenzy[49], Gophish [50], PhishSim [41], and Lucy [51].

Two additional features were added to complement the table: whether the software is free or commercial and whether it is on-premise or not. It was necessary to add the feature about cost as companies are operating based on the available budget. In terms of on-premise software versus SaaS (cloud-based software), since personally identifiable information is handled during the experiment, it may pose restrictions on the choice of software based on internal company policies and/or external regulations.

Table 3. Phishing software comparison chart

Software name	Rapid7 Meta-Sploit Pro	ThreatSim (WOMBAT)	PhishMe (Cofense)	PhishLine	SET	Phishing Frenzy	Gophish	PhishSim	Lucy
Free or commercial	COMM	COMM	COMM*	COMM	FREE	FREE	FREE	FREE	COMM
On-premises?	Y	N (SaaS)	N (SaaS)	Y*	Y (O-S)	Y (O-S)	Y (O-S)	N (SaaS)	Y*
Feature									
Allow for scheduled start times for campaigns?	Y	Y	Y	Y	N	N	Y	Y	Y
Allow for scheduled times to stop for campaigns?	Y	Y	Y	Y	N	N	Y	Y	Y
Allow for the use of logos from vendors to simulate phishing emails?	Y	Y	Y**	Y	Y	Y	Y	Y	Y**
Allow for export of all your data?	Y	Y	Y	Y	Y	Y	Y	Y	Y
Handle incident response or reporting?	N	Y	Y	Y	N	N	N	Y*	Y
If yes dose it have stats for who reported/clicked, reported/noclick?	N/A	Y	Y	Y	N/A	N/A	N/A	Y	Y
Allow for SMSing test?	N	Y	Y	Y	Y	N	N	N	Y
Allow for USB/media creation tests?	Y	Y	Y	Y	Y	N	N	Y#	Y
Allow for spoofing of e-mail addresses?	N	Y	Y	Y	Y	Y	Y	N	Y
Multistaged authentication?	N/A	N/A	Y	Y	N/A	N/A	N/A	N	Y
Use Amazon Web Servers for load balancing?	N/A	N/A	Y	N	N/A	Y*	N/A	Y	N/A
Have segregated instances for each customer?	Y	Y	Y#	Y	N/A	N	N	N	N
Allow for importing from XLS, CSV?	Y	Y	Y	Y	N	Y	Y	Y	Y
Has live tech support?	Y	Y	Y	Y	N	N	N	Y	Y
Ability to run multiple simultaneous campaigns?	N	Y	Y	Y	N	Y	N	Y	Y
Limitation on numbers of e-mails sent in one campaign?	N	N	N	N	N	N	N	N	N
Y = Yes, the feature exists in this tool. N = No, the feature does not exist in this tool. N/A = Not applicable; this feature doesn't apply at all to this tool. *, ** or # A footnote in the chart gives more information about that particular answer feature. O-S = Open Source SaaS = Software as a service COMM = Commercial			*Phishme free with limited feature SaaS ** Only w/permission #Upon request	*Possible On-premises and SaaS		* Depense on your setup		*Requres Outlook plugin installation #Requres commeral licence	*Also possible SaaS **stated that this is illegal and your respons-ibility

Open-Source Solutions

Regarding open-source software, three solutions were analysed: Phishing Frenzy, Social-Engineering Toolkit (SET) and Gophish. The strength of these solutions is that all of them are on GitHub (environment for open-source software developers) and have been updated in 2018, which means that some bugs have been fixed recently. The main benefit of open-source software is that its free to use. The downsize, however, is that it is more difficult to get timely support.

Commercial Software

Regarding commercial software, five solutions were analysed: Rapid7 Metasploit, ThreatSim, PhishMe, PhishLine and Lucy. The main benefit of commercial software is live technical support, which helps to troubleshoot possible issues and educate users if they need help in using the software. Additionally, some commercial software tools, e.g. Lucy, provide full service meaning they execute the whole phishing campaign for the company (campaign as a service). The cost is 1800$ per campaign. [52]. The downsize, however, is the cost of commercial software solutions.

SaaS solutions

Gartner [53] defines Software as a service (SaaS) as "Software that is owned, delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics." SaaS customers do not need to install any software or acquire new hardware, they only need a computer with a web browser connected to the Internet. Regarding SaaS, three solutions were analysed: ThreatSim, PhishMe, PhishLine.

The benefit of SaaS solutions is that the user can start using the functionalities immediately and that no configuration is needed. Some of the existing SaaS solutions, e.g. ThreatSim, are also free to use. The downsize is that since during the phishing assessment sensitive data is being processed, many companies have concerns over data protection and security of SaaS solutions. In some cases, it can be prohibited by regulators to use SaaS for processing sensitive data based on the classification of data and the company's field of activity.

In conclusion, each of the solution type has its pros and cons. Prior choosing the most appropriate solution, companies should first define their available budget for phishing assessments, in-house technical capabilities, time and people resources. They should also consider the internal and external data protection policies to determine whether it is allowed to use SaaS for processing sensitive data and based on the set criteria look for the appropriate solution. For example, if the company has limited budget and is not allowed to use SaaS for processing sensitive data but on the other hand has in-house IT-department to manage the phishing campaigns; open source solution would be most appropriate.

3.1.6 Informing Employees

Learning Website for Phishing

The purpose of the learning website is to educate participants about phishing and how to recognise phishing emails. Acquisti [20] and his colleagues have developed an interactive game called "Anti-Phishing Phil" that teaches users to avoid falling for phishing attacks.

They conducted a research to evaluate the impact of the game on user's awareness and concluded that after playing the game users were able to more accurately and quickly distinguish phishing websites from legitimate websites and that they retain knowledge learned from the game.

Developing websites for anti-phishing user education is widely used. Many solution providers, e.g. PhishMe, ThreatSim and some other commercial anti-phishing solution providers offer ready-made interactive learning websites as part of their anti-phishing solution.

Security Awareness Company [54] offers a similar free interactive training solution called Phishing ILM, which is in SCORM (Sharable Content Object Reference Model) format. The solution does not work in a typical browser and LMS (Learning Management System) application is needed for online learning delivery. Certain limitations exist with regard to altering some aspects of Phishing ILM, so before using it, the users should familiarize themselves with the licensing conditions. [55]

One way to use Phishing IML is to run it on Moodle software (it was also tested by author), which enables to track whether users have completed the training. [56] The first step is to install Moodle [57] and the second step to import SCROM container to Moodle [58] Phishing LMS provides information about phishing, phishing indicators, lessons from Craigslist Scam and gives multiple examples and recommendations how to recognize phishing emails (see Figure 3.)

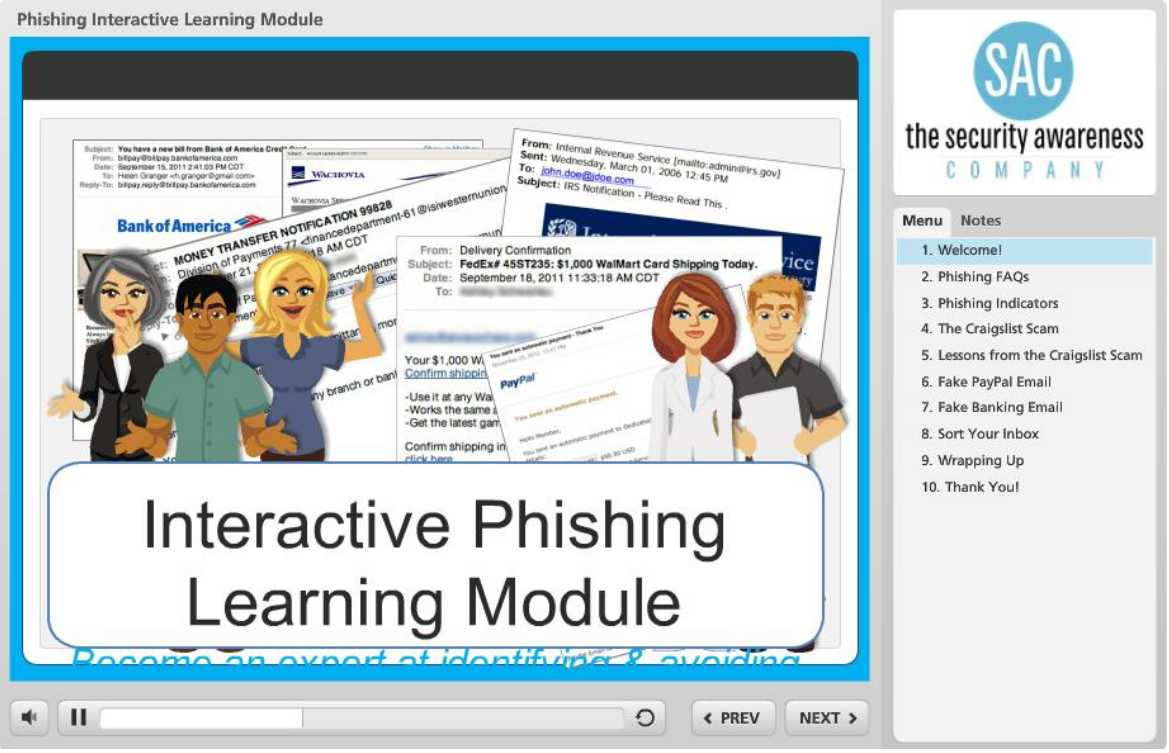


Figure 3. SAC Phishing interactive learning module.

Using an interactive learning environment is a practical way to ensure that participants have spent time on the website and passed different exercises. In contrast, using a regular learning website does not allow to evaluate if users have read through the content or merely clicked on the link [17].

Informing Participants Prior the Campaign

As it was discussed before, because of the legal, ethical and psychological considerations all employees must be informed about the simulated phishing assessments. This is also emphasised by Caputo and colleagues [17]. Resnik and Finn [22] argue that if participants are not aware that they are enrolled in a research study, this could add to their anger and frustration. In contrast, briefing the participants is believed to have a long-lasting positive impact if the briefing is structured in a way that the subject learns how to avoid falling for real phishing attacks [13].

The notification email serves the following purposes:

- Describe what is phishing and the possible consequences of phishing to the company.
- The role of the employee.
- Describe the phishing prevention program and introduce the learning website.
- Provide an overview of the internal process about reporting phishing emails.

It is important to let the employees know that the phishing experiment will not result in any negative consequences if they fall for the simulated phishing attack. One example of the notification email following the four outlined principles can be found in San José State University webpage [59] in English.

In some studies participants are not briefed about the simulated phishing assessments, for example Kaspar Prei did not send out a notification email prior to the campaign [21]. One could argue that sending the notification email may impact the research results because people are more alert to receive a simulated phishing email. Therefore, author decided to investigate in the qualitative research part of this study, whether the users remembered receiving the notification email.

Informing Participants After the Experiment

Similarly, the participants should be provided with additional information concerning their participation in the phishing assessment after the experiments are concluded [22] A notification email should be sent to all phishing campaign participants without revealing their identity to other participants, i.e. they should be in Bcc (blind carbon copy).

The notification email serves the following purposes:

- Information about the simulated phishing email:
    - Letting the employees know the email address from where the phishing email was sent and that they were not infected with malware.
    - Letting them know that passwords were not collected, in case their credentials were asked.
    - Attaching a screenshot of the actual phishing email.
- Description of phishing:
    - How to recognise phishing emails, including a link to the learning website.
    - The role of employees, e.g. in reporting suspicious emails.
    - The possible consequences of not reporting suspicious emails.

Informing employees is crucial not only due to ethical, psychological and legal reasons, but it also helps to educate employees about phishing, how to recognise phishing emails and what to do when receiving a suspicious email. To maximise the impact and learning form the simulated phishing campaigns, the emails should consist of recognisable characteristics that are typical to real phishing emails. Sending out flawlessly written emails does not help

the employees to learn to detect phishing emails. Furthermore, employees should be introduced to learning websites and/or provide them with tools for independent learning.

Another option is to debrief participants about the phishing assessment not after the assessment has been concluded for all participants but immediately after they have clicked on the link. The limitation to this approach is that participants may inform their colleagues, which affects the results. [21]

3.1.7 Creating Phishing Content

Phishing Email

The next step would be to put together email content. Many simulated phishing solutions come with the email and landing page templates, such as Phishing Frenzy [60], PhishSim [41] and Gophish [50]. For illustrative purposes, author tested the PhishSim solution. Screenshot of Facebook phishing template preview generated with the help of PhisSim can be seen Figure 4. Some solution providers, such as Lucy [51], offer customizable phishing templates or a possibility to create templates from the scratch.

Phishing emails have different topics, such as resetting a password to induce users to click on the phishing links [61]. However, one should bear in mind what is the selected difficulty level of the email content and based on that choose a relevant topic. For example, if the aim is to send out level 3 phishing emails, the content should be relevant and reflect the real-life situation. When creating a content for the phishing email, it is important to be conscious that it is a phishing email and that there must be recognizable mistakes depending on the chosen difficulty level. The mistakes help to educate employees regarding recognizing certain characteristics that they should pay attention to when receiving suspicious emails. Even though for the writer the mistakes may seem obvious, in reality this is not the case [11].

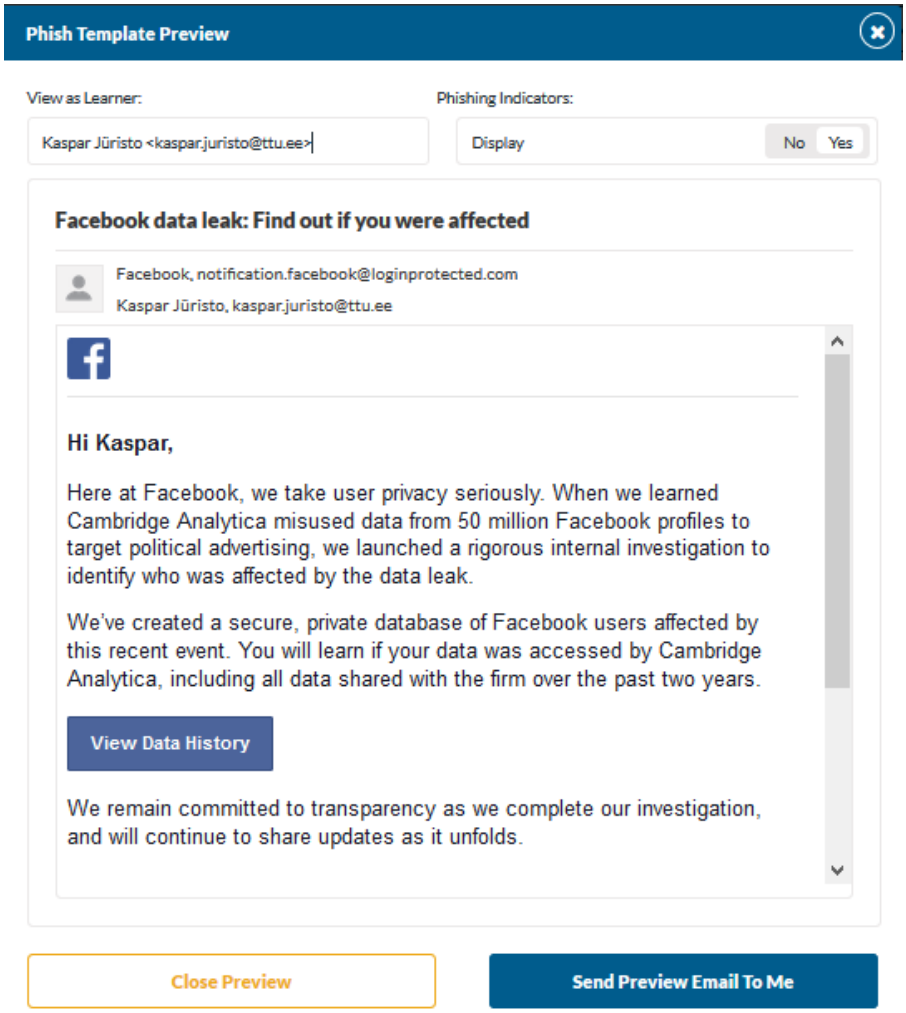


Figure 4. PhishSim screenshot of email template review

Spear Phishing Email

Spear phishing is a high priority security concern to businesses and it continues to grow as a problem [3], [4]. Therefore, more spear phishing assessments should be conducted also among employees. A Cisco report [62] highlights that spear phishing attacks are much more successful in terms of the open rate, click through rate and monetary value (see Figure 5.)

Example of a Typical Campaign	Mass Phishing Attack (Single Campaign)	Spearphishing Attack (Single Campaign)
(A) Total Messages Sent in Campaign	1,000,000	1,000
(B) Block Rate	99%	99%
(C) Open Rate	3%	70%
(D) Click Through Rate	5%	50%
(E) Conversion Rate	50%	50%
Victims	**8**	**2**
Value per Victim	$2,000	$80,000
Total Value from Campaign	**$16,000**	**$160,000**
Total Cost for Campaign	$2,000	$10,000
Total Profit from Campaign	**$14,000**	**$150,000**

Figure 5. Economic comparison between Mass Phishing and Spear Phishing [62]

The main difference between the phishing email and spear phishing email content is that since the spear phishing email is more targeted, additional time should be allocated to gather personal information about the targets to create relevant messages. Information can be gathered from different pages, e.g., Profile engine[63] and Google. Same email templates could be utilized for spear phishing as for phishing experiments.

Sending out simulated phishing emails to all targets at once is less time-consuming for the company comparing to sending out spear phishing emails one by one. However, as discussed before the loss from the spear phishing attacks is higher and employees should be educated to recognize both types of emails. Therefore, both phishing and simulated phishing campaigns should be conducted for better employee education.

Creating Landing Page

In general, landing pages can be divided into four categories: credential catering, exploit, page not found and instant notification about phishing simulation. In the below the four different approaches are described:

- Credential catering. The phishing email link leads to a website that harvests credentials. To copy the exact company login page HTTrack, which is a website copy tool, can be used [64]. Another option is to use pre-built website templates [41]. ThreatSim is also offering multiple landing pages, which are very similar to real pages with only URL path being different.
- Exploit. The phish leads to a shell as it is loaded with executable files or attachments, which contain a code that allows the penetration test to connect to the corporate network.
- Page not found. The destination of the phishing link is a 404 Error Page, and the employee is not instantly alerted that he or she is part of the phishing experiment.

- Instant notification about the phishing simulation When clicking on a phishing link it directs to the learning website and employees are notified about the campaign immediately, which is likely to decrease anxiety and distress. The limitation of this approach is that some employees may spread a word about the simulated phishing attack and that, in return, affects the results. [21]

Testing Technical Setup

End-to-end verification must be done before the phishing campaign to make sure and double check that all the components, including DNS configuration, email servers, phishing platform and target SMTP spam filter or target computer antivirus protection software are fully functioning. It is also important to click on the links embedded in the test email to verify that a unique click is registered in the phishing platform. In case the phishing email contains attachments then these need to be tested with the company's antivirus protection software.

3.2 During Email Phishing Campaign

The simulated phishing campaign day should go smoothly if all preparations are done correctly. On the campaign day relevant stakeholders should be informed about the campaign being launched. In terms of internal partners, IT helpdesk should be reminded about the campaign and in terms of external partners, administrative bodies, e.g. national CERT, should also be notified. This is needed, because in case employees would turn directly to CERT, they would be prepared and not start an official investigation process. It is recommended to inform CERT before the phishing campaign day, especially when contacting them for the first time.

After the internal and external parties have been briefed the next step is to launch the email phishing campaign. During the campaign, the wellbeing of participants should be considered, and all their queries answered. The campaign will be concluded by sending an informative email to participants.

3.3 After Launching Phishing Campaign

3.3.1 Analysing Results

Analysing the phishing campaign results enables the company to assess the security awareness of employees and helps to understand how vulnerable they are to phishing attacks. This gives the baseline for employee education and for future assessments. The following statistics should be considered relevant to draw conclusions: [11][17][65]

- The number of participants who clicked on the link embedded to a phishing email. This number illustrates the vulnerability of the company to attacks, giving insights into how many people may put the company at risk and how many employees should be further educated.
- The number of people who reported the suspicious emails. This is an important statistic, because deleting an email is not helping to solve the problem. Employees should act and report the emails as soon as they receive these to respective departments to prevent future attacks.

It is important to gather statistics about how many people "caught" the phishing email and reported it, these people can be divided into four categories. Firstly, how many people clicked on the phishing link and did not report it. Secondly, the number of people who clicked on the link but also reported it. Thirdly, how many people did not click and did not

report and lastly, number of people who did not click and did report about the suspicious email. [11]

The highest risk to the company comes from the people who clicked on the phishing link but did not report. These employees need the most training and help. People who clicked on the phishing link and still reported can be considered as a positive outcome. Although these people clicked on the phishing link, they realized the risk and ended up taking a positive step to report it. People who neither clicked nor reported the email are not imposing a substantial risk to the company but they should be educated that reporting is a needed step and should not be overlooked. People who did not click on the phishing link and reported it are behaving in a manner that a company wants them to behave. They did not fall for the phishing email and furthermore they reported it to save others. [11]

Such categorisation gives guidelines how to further educate employees and what should be the focus of training. For example, if majority of people did not click on the phishing link but they also did not report it, the focus should be on educating people why reporting is of great importance and how it helps to prevent future attacks.

3.3.2 Interviewing Participants

In addition to statistical reports, which merely give an overview of the situation, many researchers have interviewed the participants after the phishing assessments to better understand the motives behind people's behaviour [21][17][19]. Interviews allow to investigate why people took the specific actions during the phishing campaign and this gives valuable insights to detect the shortcomings within the awareness programs and to better design future campaigns. For more structured interviewing three groups of people based on their behaviour could be distinguished[17]:

- All-clickers. These are people who click links regardless of previous awareness trainings;
- Non-clickers. These are people who do not click links at all;
- The rest. These are people who do not exhibit consistent clicking behaviour.

Interview investigation, including developing the interview guide and dividing participants into groups, is discussed in more detail on Chapter 4.3 Interview Investigation (Qualitative research).

3.4 New Proposed Consolidated Guidelines for Email Phishing Experiment

Author has created the guidelines for phishing experiments based on the existing studies and literature. The guidelines consist of three parts: Pre-launching phishing campaign; Launching Phishing campaign and Post- Launching Phishing campaign. To visualize the different steps author created a diagram in Unified Modeling Language (UML) format, which can be found in Appendix A – New Proposed Consolidated Guideline for Email Phishing Experiment and a one-pager to summarize all the relevant steps, which can be found in Appendix J – One-Pager Checklist. The circles illustrate the different phases of the phishing campaign from the beginning to the end. Additional information and things to consider are brought out with keywords in the squares connected to the circles with dotted lines to supplement the steps. This diagram is supporting Chapters 3, 4, 5 and 6.

4 Methodology

The aim of this research is to explore how to conduct simulated phishing experiments and to create consolidated guidelines that companies could implement. For that purpose, one quantitative and one qualitative study were conducted to test and improve the composed guidelines, which were put together based on the existing literature and author's experience. This chapter gives an overview of the main concepts, research designs, sample size and some reflections on reliability and validity.

4.1.1 Definition of Concepts

Phishing Campaign. In the light of this research, the phishing campaign is defined sending out an email or several emails to get participants to click on a link that is embedded to the email, to register his or her public IP, browser agent, date and time. Each link is unique and links back to participants, which means that people who click on the link can be recognized.

Phishing Experiment (Assesment). In the light of this research, the phishing experiment refers to one or several assessment campaigns conducted among the same target group in distinct time periods using different emails with the purpose to investigate behavioural patterns of the selected targets. One experiment can consist of several campaigns.

4.2 Phishing Experiments (Quantitative research)

4.2.1 Experimental Research Design

Experimental research has been defined as a group of techniques where the researcher establishes different conditions for the experiment subjects and it maximises the information that can be obtained on the cause-effect relationship.[66] It is important to distinguish between the random selection and the random assignment of participants to further define the type of the research design. The random selection is the process of randomly choosing participants to the experiment, e.g. everyone has an equal chance to be selected. The random assignment means that every participant has an equal chance of being assigned into different experimental groups. Experimental research designs have one characteristic in common, namely, that participants are assigned randomly to treatment conditions. When it is not possible to randomly assign people to groups, it results in the quasi-experimental study.[67] Concerning this research the sample (employees of Company X) was predetermined, however, participants were randomly assigned to groups, which means that the study can be defined as an experimental study.

Different experimental research designs exist, for example Post-test, Only Design, Pretest-Post-Test Only Design, Solomon Four Group Design, Factorial Design, Randomized Block Design and Crossover Design. For the purposes of this study, author decided to use Crossover Design as it enables to measure whether there is a correlation between the email difficulty level and the click rate. Subjects of this design receive all the same exposures (phishing emails) that are being investigated over time and are randomly assigned to different orders of the exposures. The groups compared have an equal distribution of characteristics and the subjects that are exposed to different conditions have a high level of similarity. In other words, the groups are rather similar in terms of participants and they are exposed to the different conditions (email difficulty levels) over time (see Figure 6).

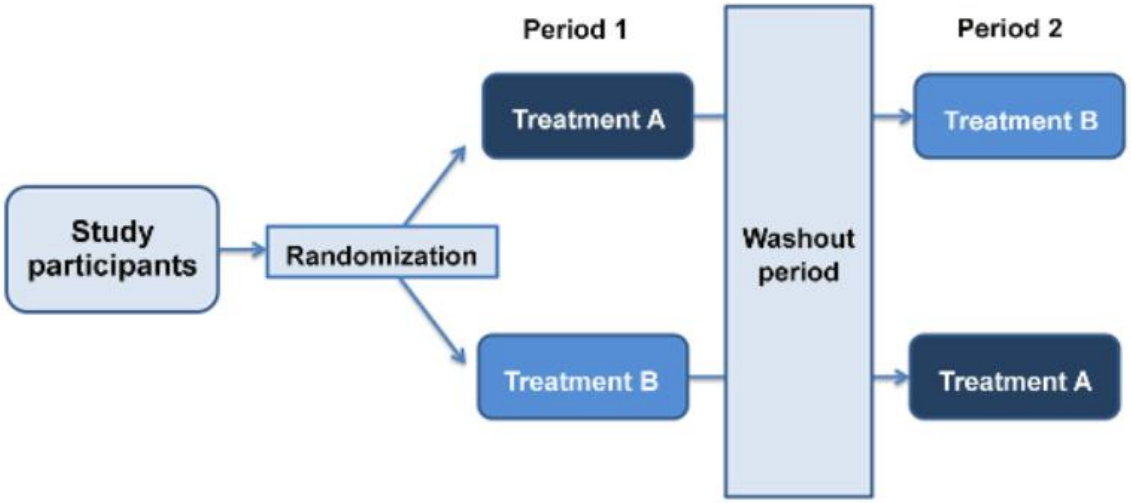


Figure 6. Illustration of The Design and Analysis of a Crossover Trial [68]

The concern, however, over this design has been that the response to the second condition may be influenced by their experience with the first exposure.[66] In terms of phishing experiments Finn and Jakobsson [31] argue that choosing two distinct types of emails gives more statistical significance, under the assumption that each campaign is independent, i.e. that the participants do not become smarter because of the previous experiment. They believe that this assumption is fair because users are exposed to numerous phishing attacks during their normal Internet use and is likely to be already affected by the unknown number of phishing attacks they already encountered.

To conduct the additional spear phishing experiment, author utilized single-subject quasi-experimental research design, i.e. subjects were not randomly selected, and data was collected on each subject/participant and individually analysed. For this purpose, A-B design was implemented. In this design, baseline measures were obtained (information about the targets) and then the experiment was conducted (spear phishing emails) to measure if there was an effect after the experiment. The criticism on this design is that its results may be subjects to numerous competing explanations.[67]

Regarding experimental standards, internal and external validity should be considered. Internal validity is the degree to which measured differences are a result of the manipulation. When changes, that can be directly attributed to the effects of the exposure, occur; the study has internal validity. External validity refers to the degree to which the experiment results can be generalized and are applicable to other groups and settings, meaning that the setting, intervention and measures should be thoroughly described. Replication helps to establish reliability of previous findings and define the generality under different conditions.[67] Both internal and external validity are considered when conducting the experiments.

4.2.2 Sample size and research period

Prior to deciding a sample size, a target population (e.g. all employees) needs to be identified and then a group size that would be representative enough can be determined [69]. The higher the sample, the more generalizable are the results. Small sample size limits measuring the effect of the research and may lead to biased results. [61] Regarding this study the target population is more than 250 people (all employees of Company X) and the sample size 53 people. The sample size was pre-determined by the Company X, therefore; one could argue that this could decrease the validity of the results. The experiments were conducted between June 2017 and September 2017. The first campaign took place in the end of June, the second

campaign in the beginning of September and the spear phishing experiment in the middle of June 2017.

4.3 Interview Investigation (Qualitative research)

4.3.1 Qualitative Interview

The chosen qualitative interview method helps us to set goals how to interpret the general orientation how we should conduct the research [70] and is best suited to answer the research question: "How people react to simulated email phishing experiments?" Therefore, this qualitative interview research is concerned with words and interpretations of the social world and how people interpret the experiment. As explained by Hennik and his colleagues [71], the objective of qualitative research is to acquire understanding of underlying reasons, beliefs and motivations of a subject matter.

The present research is an analysis of a single company, Company X. Each company has its own culture and established systems, shaping the way people react to different situations. The design chosen for this research is a case study, which is concerned with "the complexity and particular nature of the case in question"[70]. The criticism of a case study is that findings deriving from it cannot be generalized [70]. The results cannot be generalised to the entire company, but it gives some confidence that this phishing process can provide more insights on how to conduct phishing experiments, in the context of the Company X, which is why case study design is chosen.

4.3.2 Interview Investigation

Kvale [72] highlights seven stages of a qualitative interview; thematizing, designing, interviewing, transcribing, analysing, verifying and reporting. The steps were considered in planning the design of this study. Firstly, a pre-knowledge of the subject was obtained by considering the existing literature and developing theoretical understanding on how to conduct and design phishing experiments. Secondly the quantitative analysis of reports of the phishing experiment gave background information about the behaviour of interviewees, e.g. whether they clicked on the phishing emails, did they report back to the IT helpdesk that they received a suspicious email or not and how their conduct differed from the average behaviour of the studied group.

To stimulate a flow of conversation and get better understanding of how people react to phishing experiments, author decided not to completely structure the interview and thus a semi-structured interview was chosen. Such an approach means that the interviewer has a series of questions in form of an interview guide, but the interviewer may choose the sequence of questions and ask further questions in response to the statements of the interviewees [70]. Based on the gathered knowledge, a preliminary research guide was developed.

The questions chosen for this interview investigation are based on [72]: firstly, "introducing questions", to start a conversation and make people think about the experiment, secondly "probing questions" to acquire deeper knowledge on what they think of the phishing campaign, thirdly "specifying questions" to acquire knowledge about their behaviour about different phishing campaigns, fourthly "direct questions" to understand what is central to them. Some questions are also taken from the research guide developed by Caputo and his collages "Going Spear Phishing: Exploring Embedded Training and Awareness" [17].

The overall criticism of the semi-structured interview method has been that the interview statements can be ambiguous and contradictory and that the findings may not be intersubjectively reproducible.[72]

4.3.3 The Process of Selecting Interviewees

The interviewees are selected amongst the group who participated in the experiments. In total 54 people participated in the two experiments. One person participated in both experiments. The selection of interviewees for the research was purposive, i.e. the sampling was made in a strategic way as proposed by Bryman [70]. In terms of finding interviewees for the research, it was necessary to define and distinguish separate groups of people who participated on Experiment I and Experiment II. In terms of deciding how to divide interviews into groups, the methodology of Caputo and his Colleagues was used [17]. Namely, people were divided into groups based on whether they had clicked on the phishing links or not. For more details, see Chapter 3.3.2. The primary goal of such a division is to evaluate how those people who clicked on the email differ from those who did not. Also, to evaluate if participating in Experiment I affected participants' behaviour during Experiment II.

Table 4. summarizes the distinct groups. People who clicked on the phishing email, which was designed to be more easily recognizable (Group A); people who clicked on the phishing email, which was designed to be more difficult to recognize (Group B); people who clicked on both emails (Group C) and people who did not click on neither of the emails (Group D). The last group consists of two participants of Experiment II, who clicked on the spear phishing email links.

Table 4. Interview group description

	Experiment I	Experiment II
Group A	Clicked on the phishing link (Type Y email)	
Group B	Clicked on the phishing link (Type X email)	
Group C	Clicked on both phishing links (Type X and Type Y email)	
Group D	Did not click on the phishing links	
Group E		Clicked on the spear-phishing email link

Given that interviews are a qualitative part of the research and the focus is on gaining in-depth knowledge of the phishing experiment from the perspective of participants and not to make statistical generalizations, it was decided to select two interviewees from each of the group and focus on a few subjects, which makes possible to spend more time on the analysis and work out consistent and recurrent patterns [72]. Therefore, it was decided to interview ten people. However, out of the 53 people, who participated in Experiment I, only one employee clicked on both emails (Group C), which meant that it was not possible to choose two representatives from that group. In addition, only one person agreed to be interviewed from Group A and one person from Group B. In total seven interviewees were therefore conducted.

Regarding Groups A, B, C, D (Experiment I participants); the five interviewees were randomly selected, meaning that all the email addresses were numbered, and random number generation application (random.org) was used. Regrading Group E (Experiment II participants), it was not possible to randomly select the interviews as only two employees participated in the spear phishing experiment. Prior emailing the interviewees a written consent

was obtained via email from the CTO of Company confirming that these people can be contacted to conduct this research. After obtaining the consent, the seven selected employees were contacted via email and suitable times were agreed for interviews.

4.3.4 Interview Process

The interviews were conducted from December 2017 to March 2018. The interviews were carried out in different minimal noise environments, e.g. meeting rooms to guarantee privacy and avoid disturbances. Prior the interview, author introduced himself and outlined the objectives of this research along with explaining the concept `phishing experiment`. Interviewees were encouraged not to restrict themselves to answering strictly to the interview questions, but to consider different angles of the subject matter and elaborate on the topic as much as possible. To create a natural flow of discussion reflecting upon the interviewees' distinct experience and viewpoints, the order of asking the questions was not pre-determined. The interviews lasted between 40 minutes and one hour and these were conducted in Estonian. After the interviews content analysis was performed to identify major themes and topics that exhibited a viewpoint or opinion relevant to the research question.

4.3.5 Ethical Issues

Kvale [72], outlines ethical questions that one should consider prior conducting an interview, such as: what is the benefit of the study, how to obtain consent from interviewees, how to protect their confidentiality and how will the researcher affect the study. These questions were taken into consideration while designing the research questions and the process, meaning an introduction email was written explaining the benefits of this research to potential interviewees and explaining them that the interview is fully confidential, and interpretations are anonymous and that their personal data will not be stored. The questions are being asked without trying to influence the way people answer to the questions but let them have natural flow of conversations and their own interpretations and maintain critical perspective on the obtained knowledge. Prior the interviews, all the participants were asked if the interview can be recorded and after the analysis all the recordings were deleted.

4.3.6 Reflections on Reliability and Validity

The two things to consider in terms of evaluating if the research is scientific are reliability and validity. To make a research valid, the choices made throughout the process should be explained and transparent. Reliability is concerned with the consistency of the findings; in other words, whether the results of the research can be repeated [70][72]. Therefore, the process, gathered data and interpretations on the results should be well exemplified and transparent for the readers to follow. These principles were followed throughout this research.

5 Implementation of an Email Phishing Experiment

As part of the first experiment, two phishing campaigns were conducted in the selected company, which is called Company X to protect the anonymity of the company. The first campaign was conducted in June 2017 and the second one in September 2017. This chapter gives an overview of what to consider prior the campaigns, how to choose a platform, technical set up, how to create phishing email content and gives an overview of the experiment results.

5.1 Before Launching Email Phishing Campaign

5.1.1 Legal Considerations

Signing a Contract

It was discussed in Chapter 3.1.3 that due to the complexity of laws, the possibility that the research activities may have legal implications is extremely high. It should be consulted with legal advisors on how to conduct the assessment compliantly and what contracts should be in place. In most of the cases if phishing experiments are conducted contracts are signed with the service provider as sensitive data is being handled. This triggers a need to sign a contract with the board member of the Company, particularly if the experiments are conducted by a third party. The contract may vary by company, but it should outline the responsibilities and obligations of both parties, consisting the following information, which was also included to the contract signed for this case study:

- Campaign timeframe, including dates.
- Target group size and selection. The company will provide the email addresses of employees chosen for the assessment. Concerning this experiment, 53 employees were selected by the company to participate in this experiment.
- Phishing email difficulty level. The appropriate difficulty level of phishing emails based on the categorization by C. Hadnagy and M. Fincher, who categorized these into level 1, 2, 3 and 4 attacks [11]. The level should be chosen based on employee security awareness.
- Data Protection. What type of sensitive information and PII (personally identifiable information) is collected and how data is protected. Concerning this experiment, the information that was collected and stored was unique trackable link to identify the employee, IP address and browser type.
- Ethical guidelines for conducting the experiments, namely that the email content should not be offensive and cause any distress to participants. Examples: “We have naked pictures of you”, “You have won a lottery”, “Your aunt got into an accident”, etc.
- Defining roles and responsibilities. The company is responsible for registering incidents regarding the phishing experiments and forwarding this information to the appropriate roles within the company as set in the company policy. Concerning this research, the responsible point of contact for such incidents was the IT Helpdesk.
- Notifying participants. The responsibility of the Company is to send out an informative email on the same day after the phishing experiment has been concluded. The purpose is, firstly, to inform the participants that they were included into the testing sample and if they clicked on the email their computers were not affected. Secondly, to give further instructions and guidelines on how to recognize phishing emails in the future.

- An agreement that after the experiment a report describing the process of phishing experiment, the main results and suggestions for improvement will be sent to the Company.

In addition to the above-mentioned terms and conditions, the Company should notify the employees also prior the phishing experiment, because of the legal, ethical and psychological considerations. Regarding this case study the company had sent out the notification prior signing this agreement, which meant it was not relevant to add this to the agreement.

Establishing the agreement and outlining the main responsibilities, obligations and the process itself will also give a framework to thoroughly think through the necessary steps, level of engagement with the Company and handling of sensitive data to ensure all the relevant steps are taken to successfully conduct the phishing experiment.

5.1.2 Choosing Phishing Email Difficulty Level

It was discussed in the Chapter 3.1.4 that choosing the appropriate email difficulty level for phishing assessments depends on employee security awareness and whether any assessments have been previously conducted in the company. This chapter gives an overview of the current situation in Company X, how the appropriate email difficulty level was chosen and how participants were divided into groups.

Current Situation of Company X

Company X is selected as a target company for the purposes of this study. It can be categorised, in the Estonian context, as a large enterprise with more than 250 full time employees based in Estonia. It is mainly an ICT and online service company with a large customer base and revenue of more than one billion euros.

This chapter aims to analyse the previously conducted phishing assessments in Company X. Obtaining background information helps to design appropriate phishing campaigns to meet the company needs considering employee security awareness. There is no need to evaluate uneducated employees with the most difficult simulated attacks or vice versa, conduct repeatedly the same level assessments.

Analysis of previously conducted phishing assessment I

During May 2016, a level 3 phishing attack simulation was conducted in Company X. The used domain and the content on the landing website were similar to those of Company X website. The employees were lured to a website under the control of testers impersonating an internal and trusted person, who was also inviting the employees to fill in a web form with user credentials.

Phishing email was sent to 63 employees, of whom 3 were out of office based on their automatic email replies. Around 51% of all email recipients fell for the phishing attack, meaning that clicked on email link, which illustrates the vulnerability of the company to phishing attacks.

Around 36% of all email recipients entered their user credentials into the phishing form. Hijacking usernames and passwords provides direct access to company's confidential data like trade secrets, know-how and personal data.

Observations made within Company X during the session revealed that none of the phishing mail recipients noticed the fake domain name, none of them found collecting passwords suspicious and none of them informed the IT Helpdesk.

Similarly, to the theft of credentials, registering a lookalike domain name gives the possibility to start active email communication with at least one internal employee to solicit more confidential information.

Security Awareness Training

After the phishing assessment employees were asked to participate in a mandatory awareness training. The training gave an overview of phishing, the purpose of phishing emails, described the criminals behind the phishing attacks and their goals and how to recognise phishing emails.

Analysis of Previously Conducted Phishing Assessment II

During October 2016, a level 2 phishing attack simulation was conducted in Company X. For the second simulation, testers impersonated a fictive debt collection company and forwarded a claim notice with a link to file, which lured the employees to execute a "malicious" macro script mimicking. This kind of attack software could lead to data theft, remote controlling of the computer or blackmailing after encrypting all user data with ransomware.

Phishing email was sent to 63 employees, of whom 4 were out of office based on their automatic email replies. The results were that 16% of all recipients opened the email and clicked on the link and 13 employees reported the suspicious email.

Impact of the Security Awareness Training

The results of the two experiments imply that awareness testing and subsequent training had an impact on the employee behaviour. Regarding the first simulated phishing email, 36% of participants inserted their credentials to simulated phishing site, whereas regarding the second simulated email, which took place after the training, only 16% fell for it. One must also consider that the phishing attacks were with different purpose and level, which does not allow to draw final conclusions without further testing.

Choosing the Email Content Difficulty Level in Company X

As previous assessments and security training had been conducted in Company X, author together with the CTO of Company X decided to choose more advanced content for the purposes of the experiment (level 2 and level 3 phishing emails). It was decided to implement crossover research design, divide participants randomly into Group K and Group L and to send out two distinct types of emails (Type X and Type Y) with the purpose to gain more statistical significance as discussed in the Chapter 4.2.1. Table 5. summarizes what type of email was sent to each group and when.

Table 5. Summary of experiments, target groups and email types

	Experiment I (Phishing)	
	Campaign I (29.06.2017)	Campaign II (06.09.2017)
Group K	Type X (level 3)	Type Y^2 (level 2)
Group L	Type Y^1 (level 2)	Type X (level 3)

After Campaign I emails were sent out at 8:30 in the morning on the campaign day, one of the participants forwarded the simulated phishing email to 150 other employees at 14:30 the

same day. Therefore, an additional phishing email content (Type Y^2), which is corresponding to the same difficulty level, was put together for Campaign II. This is a limitation to this research findings and may affect the results.

Choosing Participants and Group Size

As it was discussed in Chapter 4.2.2. conducting a phishing assessment among all employees maximises the validity of findings, however, regarding this experiment the sample size (53 people) was pre-decided by the company. The participants were chosen from different departments and those people who were out of office during the campaign period were excluded from the sample.

5.1.3 Informing Employees

Learning Website for Phishing

There was no need to develop an additional learning platform as Company X already had internal learning website, where employees can find more information about phishing and how to recognize phishing emails. Company X learning solution followed the same principles discussed in chapter Learning Website for Phishing on page 25.

Informing Employees Prior the Experiment

All participants were briefed two months before the experiments. The notification email described what is phishing, what can be consequences of phishing and what is the role of employees in this. It described the phishing prevention program and provided an overview what to do and to whom to report when receiving a suspicious email. The email also included the link to the learning website. The email was structured in a way that the participants could learn how to avoid falling for phishing attacks and it aimed to build positive impact.

5.1.4 Choosing a Platform and Technical set up

As it was discussed in the Chapter 3.1.5 different technical solutions exist to perform a phishing assessment: open-source platform, commercial software, SaaS solutions. This chapter gives an overview of how it was determined what platform to use for Company X and describes step by step how to technically set up the campaigns.

Application Platform

Before choosing a platform, it is important to define the requirements for the platform. Regarding the phishing experiments, the requirements were:

- Open-source
- Easy to use
    - Graphical user interface
    - Installation guides
    - Tutorial videos or documentation
- Campaign management
    - Ability to develop multiple campaigns with different parameters
    - Ability to view detailed campaign statistics
    - Automatic unique target page generation and click registration

Based on the established requirements, Phishing Frenzy [49] was chosen to be the platform for both phishing assessments. It consists of traditional application components like Apache, MySQL, PHP5, Ruby, Ruby's gems, Redis and Sidekiq. The installation was done using the

guidelines provided in the official installation instruction, “Ubuntu Server 16.04.2 LTS x64”, which is published at their website. As a variation from the official instruction, author used Sendmail for sending our emails, because sending emails in the background queue was not properly working and unknown error message appeared. To ensure the administrators web interface access was limited to specific IP. In addition to ensure secure authentication, confidentiality, and integrity SSL was enforced [73].

When configuring Phishing Frenzy SMTP server to be 127.0.0.1, it uses locally installed SendMail. It is possible to configure Phishing Frenzy in a way that it will send out two emails in every 10 seconds, whereas other emails are on hold in the SendMail queue. Sendmail was configured according to the guidelines [74] published in Internet.

Server Platform

VMware ESXi was chosen to be the hypervisor platform because this was already in place in Tallinn Technological University Institute of Computer Science resources. Installing application on top of the virtualized environment gives an advantage of creating snapshots. Snapshots give opportunity to revert machine back to desirable state [75]. This guarantees that it will always run the same way, regardless of previously conducted assessments. It can be especially handy for phishing experiment conductor, who needs to ensure the same verified state in the phishing platform. In this research after collecting logs and reports from the first assessment, the server was reverted to the same state it was before the first assessment.

Landing Website

When using Phishing Frenzy, Phishing sites are being hosted in Apache’s web server. After creating a new campaign, the field "FQDN" can be found under Email Settings and when the campaign is activated it triggers the creation of a new VirtualHost to run the website. VirtualHost configuration can be modified at /etc/apache2/sites-enabled/:id.conf. When the campaign has been deactivated, VirtualHost will be removed and phishing website will no longer be accessible. This means that with the same FQDN it is not possible to simultaneously run more than one campaign [60].

Buying a Domain

Domain names are used in Internet for unique identity [76]. Firstly, it should be determined if the company would like to spoof an email address or send it out using a valid existing email account. Although for spoofing, it is not a pre-requirement to own a domain it mitigates the risk of getting detected by spam filters [77]. Buying a domain name is not obligatory, but it is very much recommended in order to conduct successful phishing campaigns [77].

On the other hand, domain names are not only used for managing emails but also for creating valid URL links, which then can be embedded to the phishing emails. Spoofing emails can be easily detected. In case of spoofing, there is a mismatch between the link text and the displayed link address when hovering the mouse over it. In the same situation if you use a legitimate URL then it will not raise suspicions about the origin of the email.

Concerning this research, DNS was configured to have MX, TXT and A records to point to application server public IP. Firstly, “MX record is a type of resource record in the DNS that specifies a mail server responsible for accepting email messages on behalf of a recipient’s domain, and a preference value used to prioritize mail delivery if multiple mail servers are available. The set of MX records of a domain name specifies how email should be routed

with the Simple Mail Transfer Protocol (SMTP) [77]". Secondary, TXT value can be used for Sender Policy Framework (SPF), which is an open standard to prevent falsifying the email address of the sender. This technical method validates which mail server is used to send mail from the domain [78]. SPF requirements are the following:

“(1) the domain owner publishes this information in an SPF record in the domain's DNS zone, and when someone else's mail server receives a message claiming to come from that domain, then (2) the receiving server can check whether the message complies with the domain's stated policy. If, for example, the message comes from an unknown server, it can be considered a fake.”[78]

Values used to configure DNS are described in

Appendix B - Example of Required DNS values. In addition, three domain names where purchased for two phishing campaigns to create senders, manage email logs, and track link clicks.

5.1.5 Creating Phishing Content

It was discussed in the Chapter 3.1.2 that phishing assessments conducted in an ethical manner must not attack participants or offend them in any way. The key for establishing that is developing an email content that is not offensive and does not pose any threat to participants well-being. Topics such as "security training", "somebody has shared a video with you" and "an unpaid invoice" were therefore chosen.

This chapter illustrates how to create a campaign in Phishing Frenzy. The first step is to configure email settings; write the subject, from whom the email is being sent and add the phishing URL path. As seen on Figure 7. Phishing Frenzy Campaign Email Settings, configuration can be done using GUI (graphical user interface).

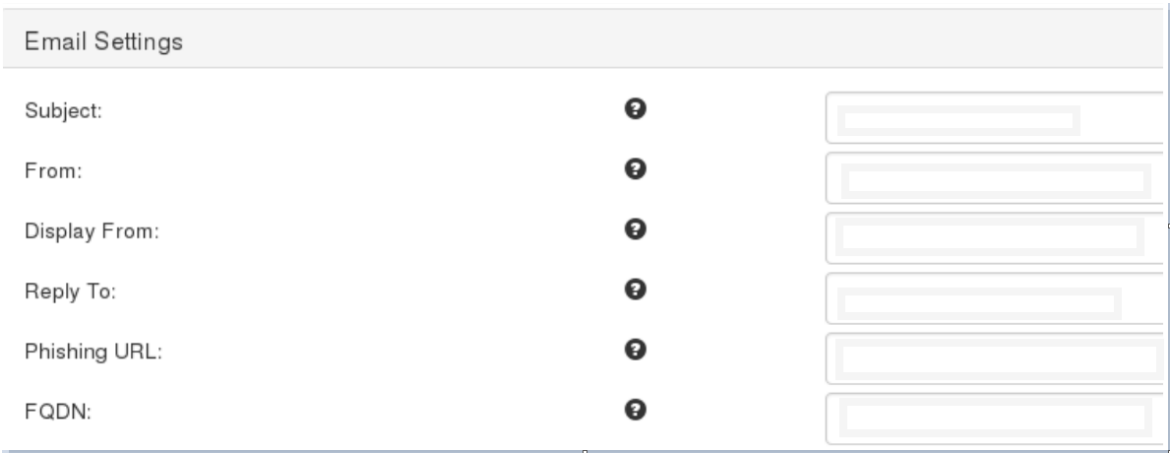


Figure 7. Phishing Frenzy Campaign Email Settings

To design an email, firstly, campaign settings should be opened and, secondly, clicked on the option Add attachment. From the drop-down menu four options can be selected: Email; Website File, Image attachment, and File Attachment. From previous list it email should be chosen and then edit the created .html.erb file with HTML design view.

In this experiment, HTML design was used to generate an email to invite employees to sign up for a GDPR training (Type X email), which corresponds to level 3. The screenshot of the Type X email, HTML code and translation from Estonian to English can be found in Appendix C - Experiment I Campaign I and II Type X Email Content. The configuration of the unique trackable link on the example of Type X emails is the following: "<a href="<%= @url %>"> http://gdprcompliance.ee/koolitused/ajaplaan-2017.
"

The Type X phishing, which corresponds to level 3, should be complex and difficult to detect with generally good grammar. These emails seem real and are appealing on curiosity. Type X email followed the below characteristics:

- Sender seems legitimate;
- Appears as a regular informative email with relevant content;
- When clicking on the phishing link it redirected to the legitimate website without the clicker most likely not noticing it first visited Phishing Frenzy landing page;

- If the participant would have clicked on the sender, he or she would have seen that it was not spoofed;
- Generally good grammar;
- Sender email domain and link domain were the same;
- In case the participant hovered the mouse over URL, he or she would have seen a correct domain name;
- Exploit of sense of curiosity, obligation, authority and social proof.

There are some giveaways that show this email is a phishing attack. Firstly, employees should have thought if they have visited before such a website, secondly, was this training communicated by their managers and lastly, when hovering over the URL link they would have seen it ending with http://gdprcompliance.ee/?uid=XXXXXX

An email informing about successful subscription for a service and an unpaid invoice (Type Y^1 email) was used only for the first campaign. The screenshot of Type Y^1 email, HTML code and translation from Estonian to English can be found in Appendix D - Experiment I Campaign I Type Y1 Email Content.

The Type Y^1 phishing email, which corresponds to level 2, should be rather basic with some spelling mistakes and impersonal greeting. The emails are appealing to feelings of greed, fear and curiosity. Type Y^1 email followed the below characteristics:

- Impersonal greeting;
- When clicking on the link, the landing website redirected to "page not found" website;
- If the participant would have clicked on the sender, he or she would have seen that it was not spoofed;
- Some grammar mistakes;
- Sender email domain and link domain were the same;
- In case the participant hovered the mouse over URL, he or she would have seen a correct domain name;
- Exploit of sense of curiosity, greed, fear, authority, obligation and scarcity;

The giveaways for this email are that the subject of the email does not correspond to the body text. When hovering over the URL the ending seems suspicious http://kaunidpildid.eu/?uid=XXXXXX. The participants should also think whether they have ever heard of Kaunidpildid, visited their website or ordered anything from this company.

An email informing that someone has shared a video with the email recipient (Type Y^2 email), which corresponds to level 2, was created for the second campaign. The screenshot of the Type Y^2 email, HTML code and translation from Estonian to English can be found in Appendix E - Experiment I Campaign II Type Y2 Email Content.

Type Y^2 email followed the same characteristic as Type Y^1 phishing email and should be recognized as a phishing email as the subject of the email does not match with the body text. Although not visible at first sight, when hovering over the URL link, it looks suspicious http://salavideo.eu/?uid=XXXXXX-. Likewise, the users should think if they have ever heard of such a service provider like Salavideo and whether they have ever visited their website or used their services.

The key distinguisher between the two emails was the level of complexity and the relevance. Level 2 email was less relevant as it was offering a service (in one case inviting to watch a video and in second case informing about an unpaid invoice), which when landing to the

work inbox should seem bizarre. On the other hand, level 3 email informed about an upcoming GDPR training and asked the employees to sign up for it, which given the relevance of the topic among employees, seems more legitimate.

Landing Website

To design a website on Phishing Frenzy the first step would be to open campaign settings and then to choose the option Edit Email. The next step would be to click on Add Attachment and from drop-down menu choose Website File. Then when clicking on index.php the HTML editor will appear.

Figure 8. illustrates how the website landing page created for Type X emails looks like. The full HTML code can be found in Appendix F - Experiment I Type X, Type Y^1 Type Y^2 Link Landing Page HTML Code.

Figure 8. Type X, Type Y^1 Type Y^2 Landing Website Screenshot

After clicking on the phishing link, it redirected the user to the legitimate purposefully chosen website. However, the clicker most likely did not notice that the link at first directed to Phishing Frenzy landing page. Redirect was configured in Apache GDPR VirtualHost config file. VirtualHost configuration can be modified at /etc/apache2/sites-enabled/:id.conf and the .conf file was created by Phishing Frenzy when campaign was activated. After modifying VirtalHost file apache service needs to be restarted to apply the new configuration.[79] The giveaway regarding the phishing link should have been that, firstly, the URL changed from http://gdprcompliance.ee/?uid=XXXXXX to other domain. Secondly the landing website was not related to GDPR albeit the topic of the email was related to GDPR training.

When employees clicked on the link embedded to Type Y^1 or Type Y^2 email, they saw a page not found information as seen in Figure 8, and this time they were not redirected to an authentic website. Participants should have, therefore, questioned the legitimacy of the link because it does not often happen that the website is not found. The landing pages did not purposefully direct to the legitimate landing page because author wanted to measure how many employees would report an email with a suspicious link.

When users visited the phishing campaign landing pages their falling for the phishing was registered using a unique trackable link. This link enabled to identify the employee, IP address and browser type.

Sending Out a Test Email

End-to-end verification must be done before the phishing experiment, to make sure and double check that all the components, including DNS configuration, email servers, phishing platform and target SMTP spam filter or target computer antivirus protection software are fully functioning. It is also important to click on the links embedded in the test email to verify that a unique click is registered in the phishing platform. Concerning this research,

no attachments were sent together with the email and therefore there were no issues with the target's Antivirus protection software.

5.2 During Email Phishing Campaigns I and II

5.2.1 Informing internal and external parties

On the campaign day relevant stakeholders were informed about the phishing campaign being launched. In terms of internal partners, IT helpdesk was informed. In terms of external partners, the Estonian national CERT was notified letting them know that simulated email phishing experiment is being conducted in the Company X and forwarding them also the emails used for testing purposes. In Estonia, although it is not legally regulated to notify CERT, it has been a common practise and it is important because if the information regarding the phishing experiment leaks out of the company, e.g. an employee forwards the suspicious email directly to CERT, then CERT is aware that it is part of the company's internal testing and will not initiate an investigation. It is recommended to inform CERT before the actual phishing campaign day and then during the campaign day to send a reminder.

5.2.2 Launching Campaigns

From the initial 72 targets, after excluding the employees, who were on holidays 53 targets were left. Regarding both campaigns, phishing emails were sent out in the morning and the campaign was concluded by sending out debriefing emails to all participants at 16:30. After sending out the emails, author verified from the email logs that emails were received by Company X email server. During the campaign day IT Helpdesk was asked to be alert and to reply to any email queries or phone calls coming from the participants and to provide them with necessary information, considering the wellbeing of employees.

5.2.3 Inform Employees After the Campaign

All participants were sent a debriefing email after the campaigns had concluded due to ethical, psychological and legal considerations. This was done on the same day that the campaign took place. A notification email was sent to all phishing campaign participants without any disclosure to their identity or the identity of other participants.

Following the guidelines described in the Chapter 3.1.6, the debriefing email contained information about the phishing campaign, including a copy of the phishing email, to disclose as much information as possible and to be transparent. Participants were informed that their computers were not infected with malware and that their passwords were not collected. The email also described how to recognize phishing emails, including a link to the learning website of Company X. In the email, it was once more stressed why reporting of suspicious emails is important, how it helps to prevent future attacks and the possible consequences of negligence to the company.

5.3 After Launching Phishing Campaign

5.3.1 Results

The aim of this chapter is to answer to the research question: What is a correlation between the phishing email difficulty level and the click through rate? Therefore, the below analysis seeks to find out are there differences between falling for Type X phishing email comparing to Type Y email. Additionally, participants' ability to detect phishing emails based on their gender is scrutinized. The link clicks were counted using UID system provided by Phishing Frenzy. Every participant had a random UID tagged to the email address which allowed to

track his or her actions. Statistics about how many people reported was gathered by the IT Helpdesk.

In total 53 employees participated in the experiment. Out of all respondents, 20 were men and 33 women (see Figure 9). Participants were randomly divided into two groups. Group K ended up having 13 women and 12 men and Group L ended up having 20 women and 7 men.

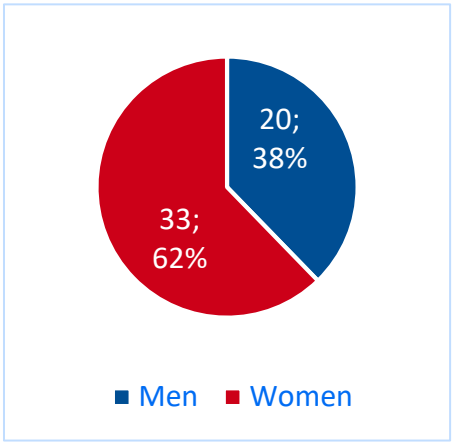


Figure 9. Participants by Gender

Figure 10. illustrates that there is a different click through rate (CTR) regarding Type X and Type Y emails; 22,6% comparing to that of 11,3%, which elucidates that when the email content is more complex (higher-level phishing) people are more likely to click on it. In terms of reporting, although the difference is not that striking; simpler emails (Type Y) were reported as phishing more frequently (22,6%), whereas more complex emails (Type Y) were reported less (18,9%). Therefore, one could conclude that when the phishing email is more recognizable, people are also more likely to report it.

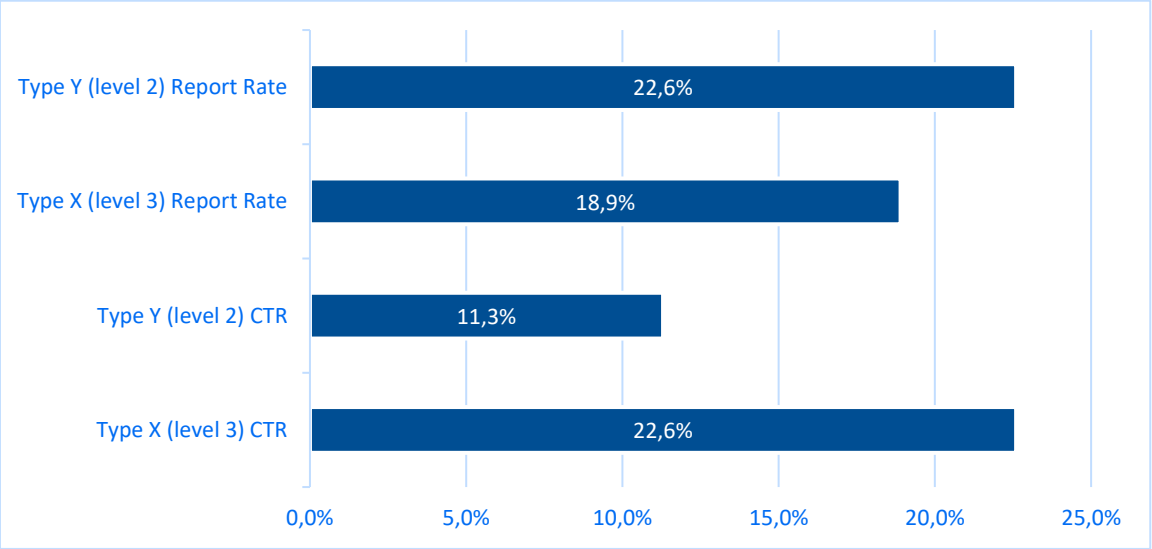


Figure 10. Click Through Rate (CTR) and Report Rate

Comparing to the results of earlier phishing campaigns conducted in Company X, level 2 phishing email click through rate had dropped (11,3% in 2017 comparing to 16% in 2016).

Likewise, level 3 phishing email click through rate had decreased (22,6% in 2017 comparing to 51% in 2016). Therefore, one could imply that the awareness testing and subsequent training in 2016 had an impact on the employee security awareness.

Iuga and colleagues [23] concluded from their study that in terms of demographic characteristics gender has a statistically significant impact for individuals' ability to detect a phishing attack. Regarding this study, in total 11 women clicked on the phishing email comparing to 9 men, however, given that more women than men participated in the study this can affect the results and no conclusions can be drawn. However, if to compare how men and women acted within their gender group, some interesting patterns can be detected. Figure 11. illustrates that the click trough rate for women is not that much affected by the email difficulty level. This is rather opposite for men. Only 5% of all men clicked on the simpler email (Type Y), whereas 30% of all men clicked on the more difficult email (Type X). Regarding women, 15,2% of all women clicked on the simpler email and 18,2% on the higher-level phishing email. Therefore, one could imply that phishing email difficulty level plays less role for women. Nevertheless, since the sample size was rather small further research should be done to validate the results.

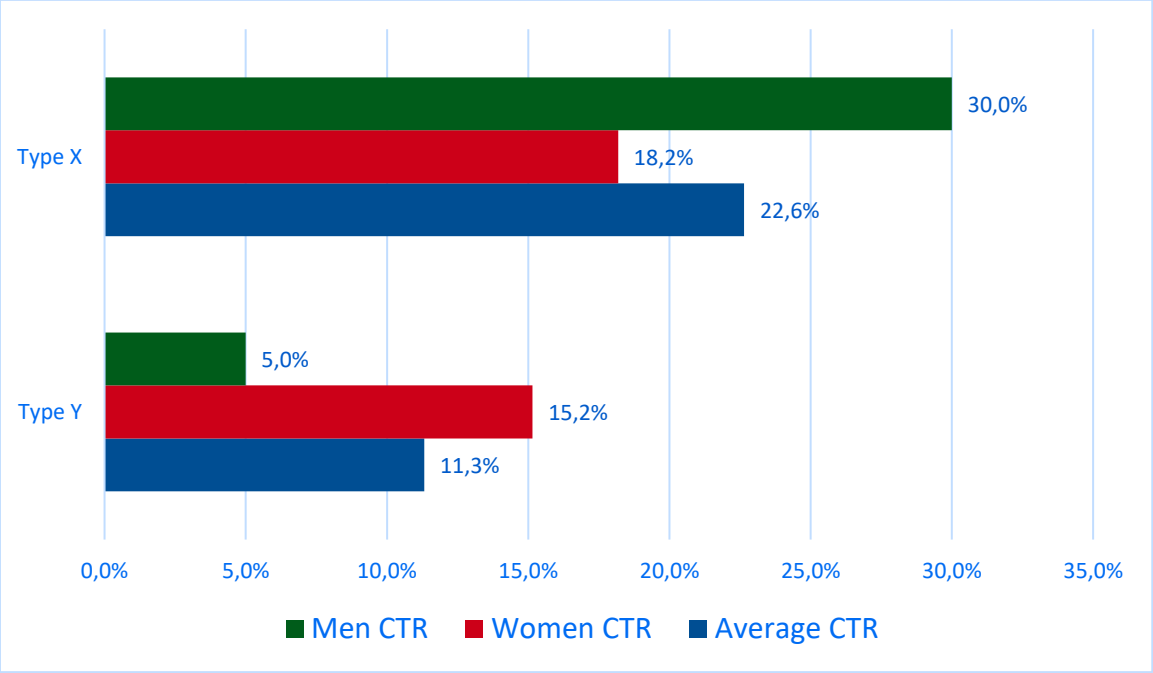


Figure 11. Men CTR, Female CTR and Average CTR

As discussed in 3.1.3. it is also important to gather statistics about how many people "caught" the phishing email and reported it. Figure 12 illustrates the current situation in Company X regarding reporting. The data captures the results pertaining to 106 emails, which were sent out in total, to give an overall picture. Only 18,9% of all phishing emails were "caught" and reported (action that the company would expect).

More than half (64,2%) of all emails were not clicked but also not reported, which illustrates that although people detect phishing emails quite well, they do not report these. This implies that employees should be educated why reporting is important and how it helps to detect future attacks. Almost 2% of all emails were clicked and reported. This behaviour is still a positive outcome; albeit there were people who clicked on the phishing emails they realized that something was suspicious and ended up taking a positive action and reported the email.

Lastly, the highest risk to the company comes from people who click on the email but do not report. Regarding this research, 15,1% of phishing emails were clicked and not reported. This illustrates that there are still people who need training and help to detect phishing emails and that the company is still vulnerable to phishing attacks.

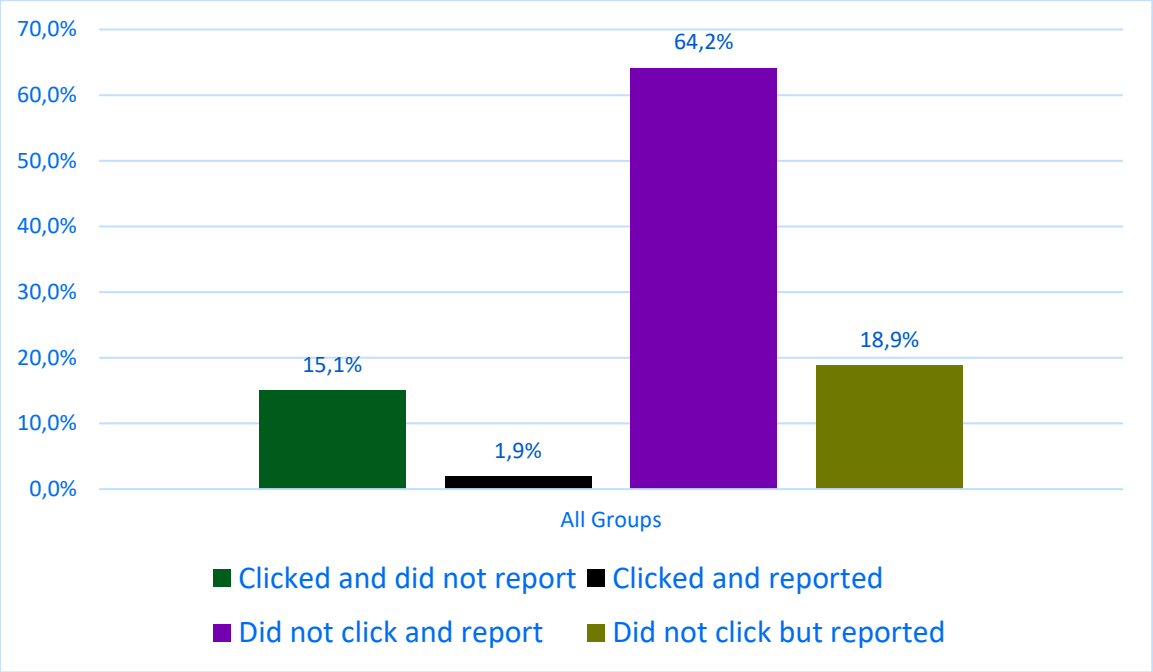


Figure 12. Reporting Behaviour of Participants (All Campaigns)

In terms of participants actions regarding the two different types of email, Figure 13. implies that regardless of the difficulty level more than half of people did not click on and report neither the Type X (60,4%) nor Type Y (67,9%) emails and there is not much difference in this behavior. Likewise, the number of people who clicked on the phishing email and reported it to be suspicious does not differ. Also, the email difficulty level does not significantly affect the percentage of people who did not click on the phishing email but reported. However, there is distinguishable difference between participants' action regarding reporting the email after clicking on it. Namely, 20,8% of participants who clicked on the more difficult email (Type X) did not report it, whereas 9,4% of participants who clicked on the simpler email (Type X) did not report it. Therefore, one could imply that after people clicked on the more difficult email, they might have not realized it was a phishing email. More detailed table consisting of all the results can be found in Appendix G – Experiment I Result Analyse Table.

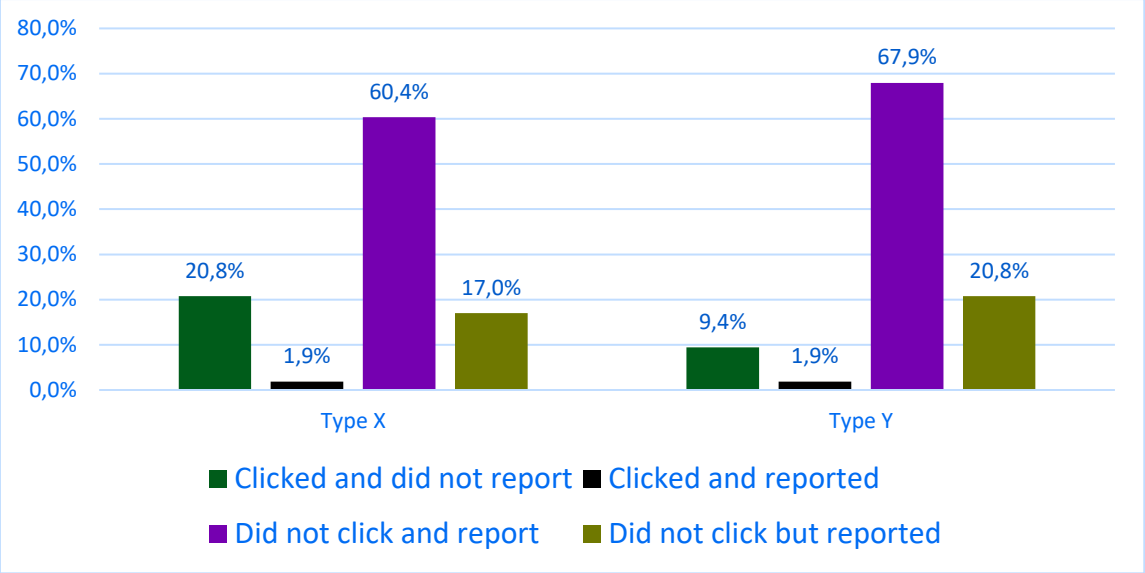


Figure 13. Actions Taken with Type X and Type Y Emails

Comparing to the reporting behaviour during the second wave of the campaigns conducted in 2016, the overall situation is rather similar and in average around 20% of people reported the suspicious emails.

The reason for concern regarding these findings is that majority of employees did not report suspicious emails and that the results have not improved since the phishing campaigns and a training held in 2016. This shows that training effect does not last very long and recurrent trainings are needed to refresh their memory. As it was discussed in Chapter 3.1.2, it can be also that people react differently to phishing emails based on their personal traits, experience, behavioural characteristics etc. Therefore, it would be interesting to investigate why some employees report phishing emails while others do not and what are the characteristics preventing them to take a certain action.

5.3.2 Interviewing Participants

As it was discussed in Chapter 3.3.2, interviews allow to probe into participant behaviour and investigate how people react to simulated email phishing experiments, which is one of the research questions. For more structured interviewing, five people based on their behaviour were distinguished for interviewing. Firstly, a participant who clicked on the phishing email, which was designed to be more easily recognizable. Secondly, a participant who clicked on the phishing email, which was designed to be more difficult to recognize. Thirdly, a participant who clicked on both emails. Fourthly, two participants who did not click on neither of the emails. Overview of groups can be found in Table 4.

Analysis of the Interviews

Three out of five interviewees stated it was their first experience with such a simulated campaign and two respondents said they had previously participated in similar campaigns. All interviews agreed that the conducted campaigns where ethical and one of the respondents added that employees must be notified about the campaign and its purpose beforehand. This was also highlighted by Finn and Jakobson [13] in their study. Another respondent added that such campaigns help to better recognize phishing attacks in the future. It was also elaborated that the content of the emails should not be offensive in any way, e.g. threatening someone's life, family or friends, asking to send money, saying there has been an accident.

This very well resonates with what Finn and Jakobsson [13] were emphasising. One participant also mentioned that he or she would not like if the campaign results would be publicly shared and everyone would know that this person failed. This illustrates that distress from failure can be one of the negative consequences as discussed by many authors [16][36]. Employees should be encouraged and asserted that phishing campaigns are for learning purposes only and they are not evaluated based on their failure, which should alleviate stress and help them to see the benefits of such campaigns.

All the interviews were positive towards the simulated phishing campaigns, recognized that such campaigns help them to prepare for real life phishing attacks and agreed that the campaigns should be organized regularly. One respondent elaborated that the campaigns should take place in every six months to sharpen memory. Two respondents added that learning through experience is the best way to learn. Half of the respondents also emphasised that the campaigns are beneficial to increase the security awareness within the company. This correlates very well with what M.H. Boynton [35] was also saying that when phishing campaigns are conducted in an ethical manner and paired with training phishing campaigns can evoke positive emotions and people do not feel that they were deceived.

Four interviewees out of five discussed that it is relatively easy for them to recognize phishing emails. It was added that main giveaways regarding phishing emails are bad grammar, unknown sender, requests to send money, something is needed urgently etc. The interviewee who said that it is not easy for him or her to recognize phishing emails elaborated that phishing campaigns have become very sophisticated and more difficult to recognize. Interesting here is that the person who clicked on the link also said that for him or her it is easy to recognise phishing emails, which contradicts to the behaviour.

Only one interviewee remembered clearly receiving the briefing email and stated it somewhat helped him or her to recognize the simulated phishing email. Other respondents said that either they did not remember receiving the notification email or the notification email had no impact. This confirms that people do not necessarily remember receiving the notification email and it has limited impact on the campaign results. On the other hand, if participants do not recall receiving the email, yet they were all positive towards the assessment, it contradicts to what Resnik and Finn [22] argued that if participants are not aware of being enrolled to the program it may result in frustration.

All the respondents said that they recognized the phishing email that was designed to be more difficult pertaining to GDPR training (level 3), because it came from outside of the company, which is not a regular practise, and this seemed bizarre. Although one interviewee recognized it was a suspicious email he or she still clicked on the phishing email out of curiosity. In terms of Type Y email, which was designed to be more easily recognizable as phishing, the main reason why participants did not click on it was that they had never heard of the service provider, it came from an unknown sender, it was not related to work, there was a sense of urgency and recognizable grammar mistakes. Once again, a person, who clicked on it, said he or she did it out of curiosity. This illustrates that curiosity was the main driver to influence participant's actions. This is an interesting finding because it is not related to conscious steering of people by hackers in the form of social pressure described by C. Hadnagy and M. Fincher [11]. The stimuli for the interviewees was curiosity albeit they recognized that the email is suspicious and should have been aware of the possible threat to the company. It can also be that the two people who clicked on the phishing email were embarrassed to admit that they fall for phishing attack and claimed they did it out of curiosity.

All the interviewees said that the Type X email was more difficult to recognize as the content was less personal and more relevant. Regarding reporting, one interviewee stated that he or she reported both emails and two employees stated that they reported only one of the emails. The stimuli for reporting was that it was stipulated by internal processes. The main reason for not reporting the suspicious email was not finding time to report it or forgetting to do it. Four out of five interviewees were aware that suspicious emails should be reported to IT Helpdesk and one person admitted that he or she is not quite sure what actions should be taken when encountering suspicious emails. In terms of how the email should be forwarded to the IT Helpdesk, two people were aware it should be sent as an attachment, however one of those two people did not know how to do it in practise. One interviewee said he or she would take the PC to the IT Helpdesk and others said they would just forward the email. Therefore, although it is quite clear for the interviewees to whom they should report about phishing, not all of them are aware of the process or do not feel the urgency to do it.

In terms of how to improve the simulated phishing campaign process, opinions differed. One person thought there should be an informative email sent to employees, another person thought it is not necessary (it was sent, but the person who brought it out did not remember it). It was also added that it should be included to the brief what is the purpose of the campaign. Three people emphasised that debriefing is crucial and receiving feedback how to act when receiving suspicious emails is very important to them. One person elaborated that all employees who failed the assessment should be signed to a security training. It was also mentioned by two other interviewees that a short training should be organized right after the campaigns. Anonymity and data protection were also considered vital for such campaigns. In terms of how to improve the simulated phishing campaigns, the main recommendation was to send out more personalized emails. Overall, it also seems that level 2 and level 3 emails were perceived to be too recognizable by some interviewees and they recommended to use more complex emails for the assessment.

The findings imply that people react positively to phishing experiments, if these are done properly, and consider it as a learning experience. It confirms that necessary use of deception in research, when it is paired with training, conveys limited psychological harm to participants. On the other hand, they are concerned about their privacy and want the assessments to be anonymous.

6 Implementation of an Email Spear Phishing Experiment

As part of this research, author attended Cyber Security Summer School 2017 (Social Engineering Capture the Flag Summer School) which was held in Estonia on July 10th to July 14th, 2017. During the Summer School two spear phishing experiments were conducted in company X. The experiments were part of the assignments which were given out to the Summer School teams, including the team author was part of. This chapter gives a description of the spear phishing experiments in Company X during the Summer School, describes the technical requirements, underlines how data was collected and provides the analysis of the results.

6.1 Introduction to the Cyber Security Summer School 2017

The focus of the Cyber Security Summer School in 2017 was social engineering. The Summer School included experts from different fields, e.g. computer science, law, criminology, forensics and psychology and consisted of 14 presentations and team assignments supported by 9 mentors from different universities. The main purpose of the Summer School was to explain how and why social engineering works and give instructions on how to prevent and find evidence for social engineering attacks. In addition to increase security awareness and knowledge of the participants. [80]

"Cyber Security Summer School 2017 is organized by Information Technology Foundation for Education (Estonia), Tallinn University of Technology (Estonia), Ravensburg-Weingarten University of Applied Sciences (Germany), the University of Adelaide (Australia), the University of Tartu (Estonia). The Summer School is supported by Estonian Ministry of Education and Research, Estonian Internet Foundation, and Baltic-American Freedom Foundation." [80]

6.2 Before Launching Email Spear Phishing Campaign

6.2.1 Signing a Contract with the Company and Informing Employees

Before the Summer School, the organizers were looking for companies who were willing to cooperate and participate in the experiments as targets. Company X was considered as one of the suitable candidates and author was asked to negotiate with Company X to agree on terms and conditions for their participation in the experiments during the Summer School.

Signing a Contract

As it was described in Chapter 3.1.3, in most of the cases if phishing experiments are conducted contracts must be signed. Likewise, an agreement was signed with Company X prior the Summer School outlining the responsibilities and obligations of both parties, including the following information. Contract concluded two parts: background information about the Summer School assignments and overall terms and conditions.

Background Information about the Summer School assignments:

- During the Summer School, participants will search for publicly available information about the Company and its employees (Open Source Intelligence);
- During the Summer School participants are given an assignment to find specific information about the Company or its employees. Examples of specific information include web browser version, display resolution. Specific information that the participants will be asked to search for, must be aligned with and confirmed by the company.

- Participants can use emailing or phone calls to the Company employees to acquire necessary information, however, identity theft or threats of any kind are not prohibited. The methods of collecting data must be aligned with and confirmed by the Company.

Overall Terms and Conditions:

- Dates of Summer School (phishing experiments).
- Target group size.
- What type of sensitive information and PII (personally identifiable information) is collected. Concerning this experiment, the information that was collected and stored was unique trackable link to identify the employee, IP address and browser type.
- A statement of the ethical conduct of the experiment, namely that the email content should not be not offensive and not even otherwise causing strong emotions. Examples: "We have naked pictures of you", "Winning the lottery", "Someone breaking into the target's home", "Some worrying news about his/her relatives etc."
- A statement that the company is responsible for registering incidents regarding the phishing experiments and forwarding this information to the appropriate roles within the company as set in the company policy. Concerning this research, the responsible point of contact for such incidents was the IT Helpdesk.
- The responsibility of the Company is to send out an informative email on the same day after the phishing experiment was conducted. The purpose is, firstly, to inform the participants that they were included into the testing sample and if they clicked on the email their computers were not affected. Secondly, to give further instructions and guidelines on how to recognize phishing emails in the future.
- An agreement, that after the experiment a report describing the process of phishing experiment, the main outcomes and suggestions for improvement will be sent to the Company.

Due to legal, ethical and psychological considerations, notification emails should be sent out to employees to inform them about the experiment prior the experiment and this should also be stated in the agreement, but as mentioned also in Chapter 5.1.1, the Company had already informed employees before the first experiment.

6.2.2 Informing Internal and External Parties

The Estonian national CERT was notified prior the phishing experiments during the Summer School letting them know that simulated email and phone phishing experiments are being conducted in the Company X. They were also sent the copies of the emails for their awareness.

The employees were notified about the planned experiments before the first phishing experiment was conducted by author and, therefore, Company X decided that further notification emails were not necessary given that the Summer School took place in approximately two weeks after the first campaign.

6.2.3 Choosing Targets

At the beginning of the summer school one company was drawn from the list of previously selected potential target companies and the randomly chosen company was Company X. All the experiments were conducted in teams and author was part of the team of six people. The spear phishing assignment that was given to the team consisted of a task to design two spear phishing emails. The first task was to lead the target to click on a link (provided by the

organizing team of the summer school) embedded to the email (Target A). The second task was to lead the target to click on a link directing to a simulated website and enable JavaScript in case it was disabled (Target B). The following steps were agreed within the team to do this assignment:

1. Collecting background information about Company X.
    - Using Open Source Intelligence Gathering sufficient amount of information about the company, potential targets and topics relevant to them with the purpose to put together an email that would lead the targets to click on the link embedded to the email.
2. Selecting the two targets for the experiment and spear phishing email content.
    a. Sharing gathered information within the team and selecting the two "easiest" targets based on the publicly available gathered information.
3. Creating the content for the phishing email and sending it to the selected targets.
    a. Creating simulated email accounts, putting together email body and sending it out.

Spear Phishing Target A

"The success of spear phishing depends upon three things: The apparent source must appear to be a known and trusted individual; there is information within the message that supports its validity, and the request the individual makes seems to have a logical basis." [81]

The first step was to gather information about Company X. To successfully complete the task the following sources were used:

- Company X website
- Search engines: Google, Duck Go Search
- Profile engines: Profile engine[63]
- Social media platforms: LinkedIn, Facebook

Author started gathering information from the company website. A choice was made to select the target from the PR team for three reasons. Firstly, given that the time was limited to execute the experiment, it seemed reasonable to select someone who is likely to be responsive to external enquiries. Secondly, due to the nature of their job, the PR specialists are used to communicating with people outside of the office and given that due to ethical considerations we had to create a fake person, it seemed also plausible to choose someone from the PR team. Thirdly, this person's contacts were publicly available.

That being decided, author started to gather information about the person and Company X using Facebook, LinkedIn, Profile engine [63]. It appeared that one local news site cooperates quite frequently with Company X and publishes stories about the company, which seemed like a potential connection that would seem valid and relevant to the target.

The second step was to present the Target A and spear phishing email content to the team. The idea was to send out an email to the PR specialist, using reference to the news site to whom Company X cooperates and claiming to be a new employee of the news site and asking for an additional comment to an already published news story. For that it would be necessary to create the fake email account and to think of a realistic email content that would also explain why the email was not coming from the news site email domain; e.g. that the employee just started and his or her account has not been set up yet, but that he or she would need additional information to reply to readers' comments regarding the specific news story.

Into the email there would be embedded a link leading to the "news story" that was the link provided by the summer school organizers. The team members agreed to author's proposal.

Spear Phishing Target B

Since the target company was the same, the first step (collecting background information) was already completed and the subsequent step was to choose the second target (Target B). The criteria for selection was similar; the target had to be responsive and used to getting emails from external contacts. In addition to that on the Company X website there was a call for action for new partners to contact Company X for potential cooperation. The contact form led to the email address of the New Services Manager and therefore the second plausible target that author came up with was the New Services Manager

The second step was to validate the choice of Target B and create spear phishing email content within the team. The idea, proposed by author, was to contact the Services Manager (Target B) with an intent to establish cooperation between the simulated company and Company X. After the discussion within the team it was decided to proceed with this proposal.

It was decided to send out an email to the target by creating a simulated company and introducing the sender as a startup owner who is selling smart earrings and is interested in potential cooperation with Company X. To establish trust, one of the team members developed a website and registered the domain name and therefore the simulated company name was visible in the email address.

The aim of the task was to get the target to, firstly, click on a spear phishing email link embedded to the email, which directed to the website and, secondly, enable JavaScript (in case JavaScript was disabled) to see the content of the page. JavaScript allows website creators to run any code which they like, while user is visiting the website [82]. If the visitors' browser settings do not allow JavaScript the person will not see any content and a pop-up message will appear describing that JavaScript must be enabled to see content.

6.3 Executing Spear Phishing Experiment and informing employees

After the initial preparations were done, the next step was to create an actual spear phishing emails and to send these out to Target A. The team created a fake email account in Gmail and devised a name that would not exist in publicly available search engines, including Google Search, Facebook, LinkedIn and Profile engine [63]. The email content remained the same that was already described in paragraph 6.2.3. Due to privacy concerns the exact wording of the email content is not disclosed as it would unveil the Company X and the news website. The phishing link provided by the organizers was made invisible by hiding it in the hyperlink, which looked like the URL from the news website. The actual link was visible only when manually hovering mouse over the link. As it was reported by the summer school organizers, Target A clicked on the link and therefore fell for the simulated phishing attack

Regarding the second spear phishing email the content was prepared as described in 6.2.3. and then sent out to Target B. The exact wording of the email content is not described as it would unveil Company X. As it was reported by the summer school organizers, Target B had clicked on the email and JavaScript had been enabled to see the content. After the experiment, Company X informed the employees that they had been included to the spear phishing testing as it was agreed in the contract.

6.4 After Launching Email Spear Phishing Campaign

6.4.1 Results

Both spear phishing attacks were successful, meaning that Target A clicked on the link and Target B visited the website and had enabled or enabled manually default JavaScript to see the content. In terms of reporting, none of the targets had contacted the IT Helpdesk to report suspicious emails or visiting a suspicious website.

The findings are similar to Cisco's [83] report results and confirm that spear phishing attacks are more successful comparing to mass phishing attacks. There are many reasons that simulated spear phishing assessments should be more widely conducted among employees. For example, the average monetary value from spear phishing attacks is 80 000 USD comparing to that of 2000 USD from mass phishing attacks, which means it results in much higher financial loss for the company. Given all the publicly available data and that it is not that difficult for attackers to design targeted emails, it is likely that the amount of spear phishing emails is to increase even more.

6.4.2 Interviewing Participants

Both interviewees said that they had been participating in phishing campaigns before. One of the interviewees was not positive about the ethical conduct of the experiment. The reason being that he or she was allegedly contacted by a journalist with whom he or she is in close work relationship. This participant also highlighted that someone should have notified him or her about the campaign (this was done but the person did not remember it). This is also what Resnik and Finn [22] argued that if participants are not notified this could cause negative emotions. In contrast, phishing experiment participants did not have that strong feelings towards notification email, which means that when the content is more personal; people have also stronger emotions. The second interviewee said that the simulated phishing campaigns are needed to educate employees, but the emails should not be too personal or offensive. This interviewee added that debriefing emails should be sent instantly after the spear phishing campaign, in particularly, if the employee falls for simulated phishing attack.

Both interviewees feel positive about the campaigns and agreed that spear phishing campaigns are needed to mitigate security risks for the company and to educate employees. This correlates with what M.H. Boynton [35] and colleagues found in their research that necessary use of deception in research, when it is paired with correct training, conveys limited psychological harm to participants.

One of the interviewees elaborated that the briefing emails should be more structured and descriptive giving real-life examples of threats to the company and it should be sent out from higher level otherwise it may disappear in the pile of emails. Finn and Jakobsson [13] also argued that briefing should be done in a structured way so that the subject learns how to avoid falling for real phishing attacks and this helps to build long-term positive relationships. Both interviewees admitted that for them it is not easy to detect spear phishing emails.

Regarding informative emails, one of the interviewees said he or she remembered receiving the briefing, but since it was sent couple of months before the actual campaign, it did not have any impact on the results. The other participant said he or she does not recall receiving the email after the campaign albeit this would be needed. None of the interviewees instantly recognized the phishing email and clicked on it as it seemed relevant and acted both on the "principle of obligation" [11], which creates influence through manners by appealing to identity. One of them, however, after clicking on the link searched the company from Internet and then realized it was a phoney email.

None of the interviewees reported the suspicious email, one because he or she did not recognize it was phishing and the other because he or she did not think it would matter. Both interviewees are aware of the process how suspicious emails should be reported, but one of them admitted that sending it as an attachment is too complicated.

In terms of how to improve the process, one of the interviewees suggested that employees should receive instant feedback about falling for the simulated phishing attack and the email could be more advanced, e.g. asking to enter credentials. The other interviewee elaborated that the simulated phishing emails should be more "shocking" and not too ethical to leave a memorable experience for participants. In addition, he or she added that trainings are needed, and employees should be walked through the process of reporting suspicious emails.

Spear phishing emails seem to cause more anxiety and stronger emotions among participants, which is expected, given that these emails are targeted and touch them personally. On the other hand, employees do feel the assessment campaigns are needed to avoid falling for real life attacks and given the rise of spear phishing attacks preparing employees is needed. Therefore, it should be very well thought through what the possible psychological and ethical consequences of targeted emails are. Likewise, how the privacy and wellbeing of participants can be best accomplished so that it would not breach any privacy regulations.

7 Discussion and Conclusions

The aim of this study was to develop consolidated easy-to-implement guidelines for companies on how to conduct phishing experiments and describe in-depth the process, including legal, technical and ethical aspects, that organizations should consider. The study sought to find out what should companies consider when conducting phishing experiments, what is the correlation between the phishing email difficulty level and the click through rate and how people react to simulated email phishing experiments.

7.1 Improvement Proposals

The main shortcomings regarding Company X that the findings revealed are insufficient training and low employee engagement in reporting. The phishing campaigns revealed that the company is vulnerable to phishing attacks and therefore further trainings are needed. It was brought out by many interviewees themselves that at least after the campaigns short trainings should be organized.

80% of the phishing emails were not reported. Interviewees were not sure how to do it and some of them admitted it seemed too complicated for them, which is likely to decrease their motivation to report. This problem should be mitigated, and reporting should be made easier for users.

One solution would be to use Outlook Phishing button, which sends the suspicious email directly to the appropriate email address as an attachment and deletes the suspicious email from the employee's computer. There are multiple companies who provide such an Outlook add-in, for example Lucy [84]. Likewise, PhishReporter offers free Outlook add-in [24] available from GitHub. "This simple, yet efficient, Outlook Add-In adds a button to your Outlook Home Ribbon that allows users to simply select/highlight a phishing email and it will forward it to the appropriate mailbox/email address as an attachment for further analysis. Once the user has verified that they want to send this Phishing email, then the Outlook Add-In removes it from their inbox and places it in their "trash" folder[85]"

Employees seem not to properly understand why reporting is needed and how it helps to detect future attacks, which once again highlights the need for a training. Additionally, an incentives program could be designed so that employees would get used to reporting suspicious emails. Further management engagement might also improve reporting behaviour and get through the message on the security risk coming from phishing attacks.

7.2 Future Work

More research should be done to more thoroughly analyse the legal aspects and whether GDPR will have any impact on the process of conducting phishing campaigns and how to maximise the certainty that the personal data is protected.

One interesting finding from this study was that employees claimed they clicked on the links out of curiosity, albeit recognising it was a phishing email. Therefore, it could be further scrutinized, what triggers people to click on the links embedded to suspicious emails even though they recognize the content to be fishy.

It could be also tested whether sending the notification email prior the campaigns affects the results or there is no statistical significance. Furthermore, credential harvesting could be tested to measure how many participants are willing to give out their credentials.

Employee motivation to report phishing emails should be scrutinized and, in particularly, what triggers some employees to report suspicious emails and why still so many employees are negligent towards reporting.

Additionally, it should be investigated what impact the phishing experiments and trainings have on making employees overtly cautious not to open even legitimate emails, which may hamper company productivity. For example, because of phishing campaign and trainings, an employee might be too scared to open an email form an unknown sender, which may be a legitimate query from a potential customer.

7.3 Limitations

This research has limitations that can be addressed in replications of this study. The main limitation of this study is that two hours before the first campaign was to conclude, one employee forwarded Type Y^1 emails to some other employees, which can affect the validity of the results, albeit the content was renewed for the second campaign. This study is based on one company and the results cannot be generalised. For widespread validity, the study must be replicated at other companies.

7.4 Conclusions

Making embedded security assessments effective in a corporate environment is difficult. Changing employees' security behaviour is challenging and effective security assessments must consider not only ethical and legal principles but also preferred notification method, employee reaction to phishing and reporting behaviour. This research confirmed that proposed guidelines are sufficient for conducting phishing experiments in a company setting. Summary of the guidelines can be found Appendix A and J.

The companies must consider that phishing assessment are conducted in a manner that it does not pose psychological damage or distress for the participants. The content should not be offensive nor attack the participants in any matter and their privacy must be protected. Employees should feel good about the campaigns and, therefore, structured briefing and debriefing are necessary so that the participants learn how to avoid falling for real phishing attacks and feel positive about the campaign. The briefing should come from the management to ensure maximum impact and employee awareness. The campaigns should be paired with educational trainings.

The main legal issues that phishing assessments may convey are violations of a provider's terms of use, intellectual property rights and copyright infringement along with data protection. It is crucial to understand legal aspects prior conducting the campaign not to violate any laws; the risks can be mitigated with contractual agreements.

Prior conducting phishing assessments companies should consider that employees are likely to communicate with each other and share information about the suspicious email. This affects the reliability of results when trying to assess the security awareness of employees. To mitigate this risk, one of the solutions would be not to send out the phishing email on the same day to all employees, but to divide people into groups and send out the email in distinct time periods. If it is not possible to test all employees, prioritization should be made based on job roles. People whose contacts are publicly available or who process a lot of external emails (e.g. employees working within public relation or marketing department) are seeing more malicious emails flooding their inboxes and they should be prioritized for internal assessments.

When choosing the level for simulated phishing campaigns, the company should start with the simpler phishing and then based on the employee readiness move further with more difficult phishing emails. When starting with a more difficult phishing campaign, it is likely that less participants will recognise the phishing email and they may feel unwise and that can cause negative emotions about the program; therefore, level 2 or level 3 phishing emails would be an appropriate baseline.

Three main types of technical solutions exist to perform a phishing assessment: open-source platform, commercial software, SaaS solutions. Prior choosing the most appropriate solution, companies should first define their available budget for phishing assessments, in-house technical capabilities, time and people resources. They should also consider the internal and external data protection policies to determine whether it is allowed to use SaaS for processing critical data and based on the set criteria look for the appropriate solution.

Before launching the phishing campaign relevant stakeholders should be informed about the campaign, e.g. national CERT and IT Helpdesk. During the campaign, the wellbeing of participants should be considered, and all their queries answered. After the campaign, results should be analysed to assess the security awareness of employees and to understand how vulnerable the company is to phishing attacks. This gives the baseline for employee education and for future assessments.

The experiment conducted in Company X revealed that the click through rate for more complex (higher-level phishing) emails was 21% and for simpler emails 11% percent. In terms of demographic findings, phishing email difficulty level influenced the behaviour of women less, as the click trough rate for women was not that much affected by the email difficulty level, whereas this was rather opposite for the men. Given the small sample size further research should be done to validate the results.

The findings of interviews imply that people react positively to phishing experiments, if these are done properly, and consider it as a learning experience; which confirms that necessary use of deception in research, when it is paired with training, conveys limited psychological harm to participants. Such phishing campaigns are perceived necessary to detect and fight against real phishing attacks.

Phishing experiments under real life condition provide valuable knowledge to develop countermeasures and prevent individuals from being duped by phishing emails. Although the experiments involve deception, they can be conducted ethically if risks are minimized, confidentiality and privacy are protected, potential participants and subjects are appropriately briefed before the experiments and debriefed after their participation ends.

8 References

[1] Zulfikar Ramzan, “A Brief History of Phishing,” *Symantec Official Blog*, 2007. [Online]. Available: https://www.symantec.com/connect/blogs/brief-history-phishing-part-i. [Accessed: 04-Mar-2018].

[2] “The Cost of Phishing & Value of Employee Training The Cost of Phishing and Value of Employee Training,” *Ponemon Inst.*, 2015.

[3] Cloudmark Security Blog, “Survey Reveals Spear Phishing as a Top Security Concern to Enterprises,” 2016. [Online]. Available: https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/. [Accessed: 22-Mar-2018].

[4] G. Aaron and R. Rasmussen, “Global Phishing Survey: Trends and Domain Name Use in 2016,” 2015.

[5] M. Alvarez *et al.*, “IBM X-Force Threat Intelligence Index 2017 The Year of the Mega Breach,” in *https://www.ibm.com/security/data-breach/threat-intelligence-index.html*, 2017, no. March, pp. 1–30.

[6] Techtarget, “What is social engineering? SearchSecurity.” [Online]. Available: https://searchsecurity.techtarget.com/definition/social-engineering. [Accessed: 08-Apr-2018].

[7] R. Dhamija, J. D. Tygar, and M. Hearst, “Why phishing works,” *Proc. SIGCHI Conf. Hum. Factors Comput. Syst. - CHI ’06*, no. November 2005, p. 581, 2006.

[8] W. Rocha Flores, H. Holm, G. Svensson, and G. Ericsson, “Using Phishing Experiments and Scenario-Based Surveys to Understand Security Behaviours in Practice,” *Inf. Manag. Comput. Secur.*, vol. 22, no. 4, pp. 393–406, 2014.

[9] “Oxford Dictionaries.” [Online]. Available: https://en.oxforddictionaries.com/. [Accessed: 03-Dec-2017].

[10] M. Jakobsson and S. Myers, *Phishing and countermeasures : understanding the increasing problem of electronic identity theft*. Wiley-Interscience, 2007.

[11] C. Hadnagy and M. Fincher, *Phishing Dark Waters: The of Fensive and Defensive Sides of Malicious Emails*. John Wiley & Sons, 2015.

[12] R. T. Wright and K. Marett, “The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived,” *J. Manag. Inf. Syst.*, vol. 27, no. 1, pp. 273–303, 2010.

[13] P. Finn and M. Jakobsson, “Designing and conducting phishing experiments,” *IEEE Technol. Soc. Mag. Spec. Issue Usability Secur.*, pp. 1–21, 2007.

[14] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” *Commun. ACM*, vol. 50, no. 10, pp. 94–100, Oct. 2007.

[15] M. Jakobsson and J. Ratkiewicz, “Designing ethical phishing experiments: A study of (ROT13) rOnl query features,” in *Proceedings of the 15th international conference on World Wide Web - WWW ’06*, 2006, p. 513.

[16] R. Salah El-Din, “To Deceive or Not to Deceive! Ethical Questions in Phishing Research,” no. In Proceedings of the British Computing Society, human–computer interaction 2012 Workshops, 2012.

[17] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, “Going spear phishing: Exploring embedded training and awareness,” *IEEE Secur. Priv.*, vol. 12, no. 1, pp. 28–38, 2014.

[18] C. Soghoian, “Legal risks for phishing researchers,” *eCrime Res. Summit, eCrime 2008*, 2008.

[19] P. Kumaraguru *et al.*, “School of Phish: A Real-World Evaluation of Anti-Phishing Training,” *SOUPS ’09 Proc. 5th Symp. Usable Priv. Secur.*, vol. 3, no. Mountain View, California, 2009.

[20] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, “Teaching Johnny Not to Fall for Phish,” *ACM Trans. Internet Technol. ACM Ref. Format ACM Trans. Intern. Tech*, vol. 10, no. 7, pp. 1–31, 2010.

[21] K. Prei, “Measuring Personnel Cyber Security Awareness Level Through Phishing Assessment,” 2017.

[22] D. B. Resnik and B. R. Peter Finn, “Ethics and Phishing Experiments,” *Sci. Eng. Ethics*, 2017.

[23] C. Iuga, J. R. C. Nurse, and A. Erola, “Baiting the hook: factors impacting susceptibility to phishing attacks,” *Human-centric Comput. Inf. Sci.*, vol. 6, no. 1, 2016.

[24] P. Gil, “Whaling and Spear Phishing Are Usually Malicious Scam,” *Lifewire*, 2018. [Online]. Available: https://www.lifewire.com/what-is-whaling-2483605.

[25] F. Y. Rashid, “Types of phishing attacks and how to identify them,” *CSO*, 2017. [Online]. Available: https://www.csoonline.com/article/3234716/phishing/types-of-phishing-attacks-and-how-to-identify-them.html.

[26] Symantec, “Internet Security Threat Report - ISTR,” *Symantec [Online]*, vol. 22, no. April, p. 77, 2017.

[27] W. J. Papanikolas, “Conducting an Email Phishing Campaign,” in *WMISACA/Lansing IIA Joint Seminar*, 2016.

[28] Symantec, “SPEAR-PHISHING SCAMMERS SHARPEN THEIR ATTACKS WITH CLEVER NEW TACTICS,” 2015.

[29] E. Buchanan, J. Aycock, S. Dexter, D. Dittrich, and E. Hvizdak, “Computer Science Security Research and Human Subjects: Emerging Considerations for Research Ethics Boards,” *J. Empir. Res. Hum. Res. Ethics*, vol. 6, no. 2, pp. 71–83, 2011.

[30] Dr. Robert Cialdini, *Influence: The Psychology of Persuasion*. HarperCollins Publishers Ltd., 2007.

[31] P. Finn and M. Jakobsson, “Designing Ethical Phishing Experiments,” in *IEEE Technology and Society Magazine*, 2007, vol. 26, no. 1, pp. 46–58.

[32] A. C. M. Leung and I. Bose, “Association for Information Systems AIS Electronic Library (AISeL) Indirect Financial Loss of Phishing to Global Market INDIRECT FINANCIAL LOSS OF PHISHING TO GLOBAL MARKET,” 2008.

[33] Devid Kennedy, “SET User Manual.” [Online]. Available: https://github.com/trustedsec/social-engineer-toolkit/blob/master/readme/User_Manual.pdf. [Accessed: 25-Mar-2018].

[34] N. Athanassoulis and J. Wilson, “When is deception in research ethical?,” *Clin.*

Ethics, vol. 4, no. 1, pp. 44–49, 2009.

[35] M. H. Boynton, D. B. Portnoy, and B. T. Johnson, "Exploring the ethics and psychological impact of deception in psychological research.," *IRB*, vol. 35, no. 2, pp. 7–13, 2013.

[36] G. Mazzanti, "The combination of electro-thermal stress, load cycling and thermal transients and its effects on the life of high voltage ac cables," *IEEE Trans. Dielectr. Electr. Insul.*, vol. 16, no. 4, pp. 1168–1179, 2009.

[37] E. Hayashi and J. I. Hong, "A Diary Study of Password Usage in Daily Life," in *CyLab*, 2010, pp. 2627–2630.

[38] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The Tangled Web of Password Reuse," in *Network and Distributed System Security (NDSS) Symposium*, 2004, pp. 1–15.

[39] D. C. Sicker, P. Ohm, and D. Grunwald, "Legal issues surrounding monitoring during network research," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement - IMC '07*, 2007, pp. 141–148.

[40] Council of Europe, "Convention on Cybercrime (ETS No. 185), Budapest, 23.XI.2001." [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. [Accessed: 27-Mar-2018].

[41] SecurityIQ, "PhishSim User's Manual," 2018. [Online]. Available: http://resources.infosecinstitute.com/securityiq-awareed-and-phishsim-users-manual-pt-5-phishsim-phishing-simulator/. [Accessed: 24-Mar-2018].

[42] "KnowBe4 - Trademark Issues." [Online]. Available: https://www.knowbe4.com/fud. [Accessed: 30-Mar-2018].

[43] "Facebook - Terms of Service." [Online]. Available: https://www.facebook.com/terms.php. [Accessed: 25-Mar-2018].

[44] InfoSec Institute, "Top 9 Free Phishing Simulators," 2016. [Online]. Available: http://resources.infosecinstitute.com/top-9-free-phishing-simulators/. [Accessed: 24-Mar-2018].

[45] Rapid7, "Rapid7 Metasploit PRO manual," 2018. [Online]. Available: https://metasploit.help.rapid7.com/docs/social-engineering. [Accessed: 25-Mar-2018].

[46] "ThreatSIM manual." [Online]. Available: https://info.wombatsecurity.com/hubfs/Wombat_FeatureOverview_Reporting_August2017.pdf?t=1521833425043. [Accessed: 25-Mar-2018].

[47] "Cofense webpage." [Online]. Available: https://cofense.com/. [Accessed: 25-Mar-2018].

[48] "PhishLine - Phihsing." [Online]. Available: https://www.phishline.com/solutions/phishing/. [Accessed: 25-Mar-2018].

[49] "Phishing Frenzy," *https://www.phishingfrenzy.com/*. [Online]. Available: https://www.phishingfrenzy.com/. [Accessed: 03-Dec-2017].

[50] Gophish, "Gophish User Guide," 2018. [Online]. Available: https://gophish.gitbooks.io/user-guide/content/documentation/campaigns.html?q=. [Accessed: 24-Mar-2018].

[51] Lucy, “Lucy Manual v. 2.01,” 2018. [Online]. Available: https://www.lucysecurity.com/PS/doc/dokuwiki/doku.php?do=search&id=. [Accessed: 24-Mar-2018].

[52] “Pricing - Lucy Phishing, Social Hacking and Security Awareness.” [Online]. Available: https://www.lucysecurity.com/en/pricing/. [Accessed: 24-Mar-2018].

[53] “Gartner Research.” [Online]. Available: https://www.gartner.com/it-glossary/software-as-a-service-saas/. [Accessed: 24-Mar-2018].

[54] “Phishing ILM - Security Awareness Company.” [Online]. Available: https://free.thesecurityawarenesscompany.com/downloads/phishing-ilm/. [Accessed: 25-Mar-2018].

[55] “Licensing Rules - SAC.” [Online]. Available: https://free.thesecurityawarenesscompany.com/licensing-rules/. [Accessed: 25-Mar-2018].

[56] “Features - Moodle.” [Online]. Available: https://docs.moodle.org/34/en/Features. [Accessed: 25-Mar-2018].

[57] “Download - Moodle.” [Online]. Available: https://download.moodle.org/releases/latest/. [Accessed: 25-Mar-2018].

[58] “SCORM - Moodle.” [Online]. Available: https://docs.moodle.org/26/en/SCORM_settings#Adding_a_SCORM_package. [Accessed: 25-Mar-2018].

[59] “Information Technology Divison,” *San José State University*. .

[60] “Phishing Frenzy -Getting Started.” [Online]. Available: https://www.phishingfrenzy.com/resources/getting_started.

[61] H. Siadati, S. Palka, A. Siegel, and D. Mccoy, “Measuring the Effectiveness of Embedded Phishing Exercises,” in *10th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 17*, {USENIX} Association, 2017.

[62] Cisco, “Email Attacks: This Time It’s Personal,” 2011.

[63] “Profileengine.” [Online]. Available: https://profileengine.com/peoplesearch.

[64] Xavier Roche, “HTTrack Website Copier.” [Online]. Available: https://www.httrack.com/html/index.html. [Accessed: 31-Mar-2018].

[65] R. C. Dodge, C. Carver, and A. J. Ferguson, “Phishing for user security awareness,” *Comput. Secur.*, vol. 26, no. 1, pp. 73–80, Feb. 2007.

[66] A. M. Dean, “Experimental Design: Overview,” in *International Encyclopedia of the Social & Behavioral Sciences*, Elsevier, 2001, pp. 5090–5096.

[67] C. M. C. and C. A. Mertler, “Quantitative Research Methods,” in *Introduction to Educational Research*, SAGE Publications Inc, 2016, pp. 108–140.

[68] T. Li, T. Yu, B. S. Hawkins, K. Dickersin, and L. Manzoli, “Design, Analysis, and Reporting of Crossover Trials for Inclusion in a Meta-Analysis,” 2015.

[69] R. C. Dodge and A. J. Ferguson, “Using Phishing for User Email Security Awareness,” in *Security and Privacy in Dynamic Environments*, Boston: Kluwer Academic Publishers, 2006, pp. 454–459.

[70] Alan Bryman, *Social Research Methods*, Fourth Edi. Oxford University Press Inc,

2012.

[71] A. B. Monique Hennink, Inge Hutter, *Qualitative Research Methods*. SAGE Publications, 2010.

[72] K. Steinar, *An Introduction to Qualitative Research Interviewing*. London: SAGE Publications, 1996.

[73] "How SSL Provides Authentication, Confidentiality, and Integrity," *IBM® IBM Knowledge Center*, 2017. [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.0.1/com.ibm.mq.csqzas.doc/sy10670_.htm. [Accessed: 03-Dec-2017].

[74] "Configuring Sendmail on Ubuntu 14.04." [Online]. Available: https://www.abeautifulsite.net/configuring-sendmail-on-ubuntu-1404.

[75] "Understanding VM snapshots in ESXi / ESX," *WMware*, 2015. [Online]. Available: https://kb.vmware.com/s/article/1015180. [Accessed: 03-Dec-2017].

[76] P. Mockapetris, "Domain System Changes and Observations," *IETF Working Group*, 1986. [Online]. Available: https://tools.ietf.org/html/rfc973. [Accessed: 03-Dec-2017].

[77] "Phishing Frenzy - Methodology." [Online]. Available: https://www.phishingfrenzy.com/resources/methodology. [Accessed: 03-Dec-2017].

[78] "Sender Policy Framework." [Online]. Available: http://www.openspf.org/Introduction. [Accessed: 03-Dec-2017].

[79] "Stopping and Restarting Apache HTTP Server," *apache.org*. [Online]. Available: https://httpd.apache.org/docs/2.4/stopping.html.

[80] "Cyber Security Summer School 2017." [Online]. Available: http://www.studyitin.ee/c3s2017.

[81] "Search Security - spear phishing." [Online]. Available: http://searchsecurity.techtarget.com/definition/spear-phishing.

[82] "Heimdalsecurity - Javascript malware explained." [Online]. Available: https://heimdalsecurity.com/blog/javascript-malware-explained/.

[83] Cisco, "Cisco 2011 Annual Security Report," 2011.

[84] "Configuration and Usage of the Lucy Phishing Button for Outlook." [Online]. Available: https://www.lucysecurity.com/en/configuration-usage-phishing-button-outlook-video/. [Accessed: 01-Apr-2018].

[85] "PhishReporter-Outlook-Add-In - GitHub." [Online]. Available: https://github.com/braxtone/PhishReporter-Outlook-Add-In. [Accessed: 01-Apr-2018].

Appendix A – New Proposed Consolidated Guideline for Email Phishing Experiment

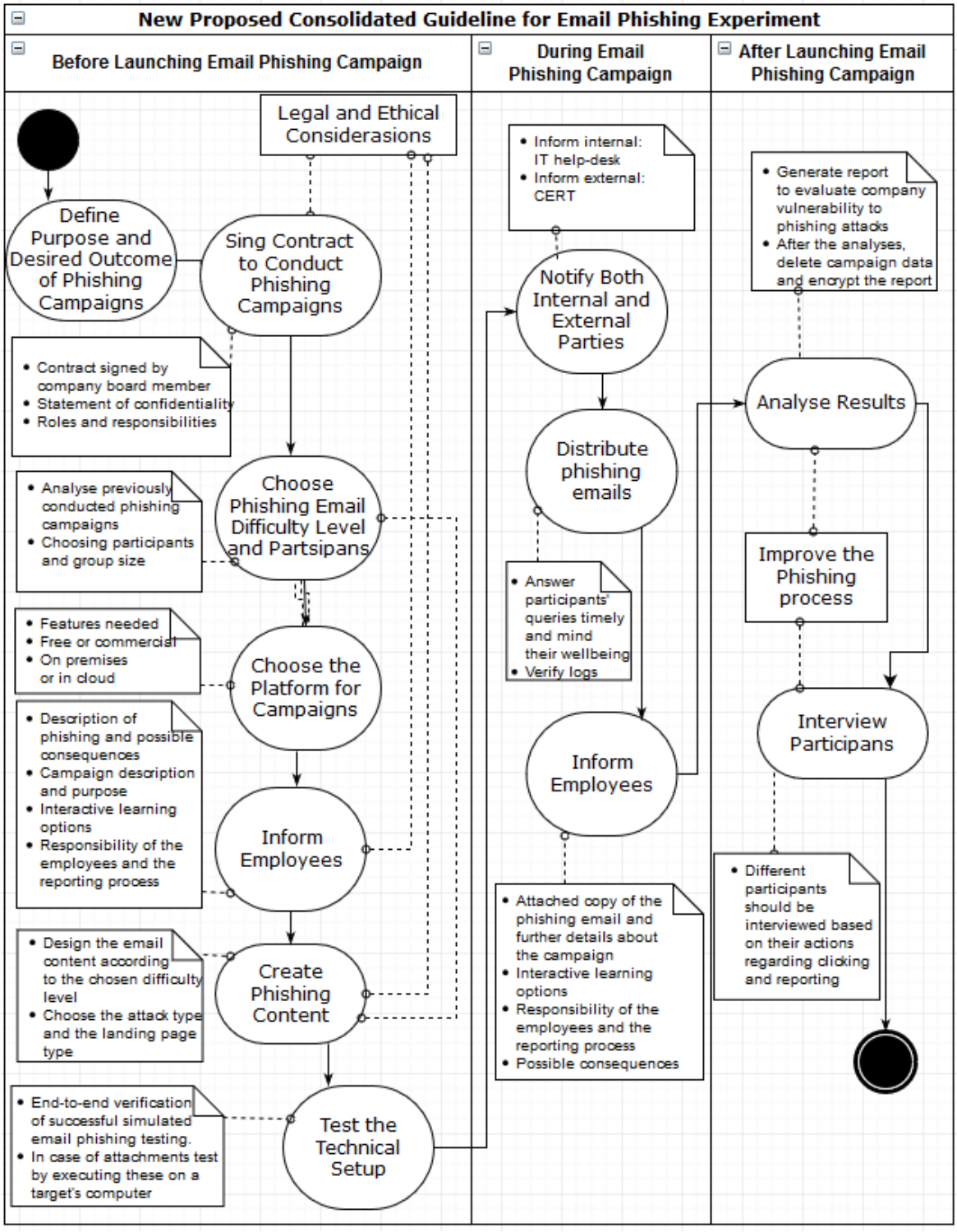


Figure 14. New Proposed Consolidated Guideline for Email Phishing experiment

Appendix B - Example of Required DNS values

Table 6. DNS Configuration

MX records		
Priority	MX record value	
10	mail.example.com	
Other records		
Record	Type	Value
example.com	A	x.x.x.x (IP of redirected web server)
mail.example.com	A	x.x.x.x (IP of mail server)
mail.example.com	txt	v=spf1 a mx include:mail.example.com ~all

Appendix C - Experiment I Campaign I and II Type X Email Content

Subject: GDPR infotundide ajaplaan
Date: Thu, 29 Jun 2017 11:09:43 +0300
From: GDPR Compliance <info@gdprcompliance.ee>
Reply-To: info@gdprcompliance.ee

Tere

Seoses üleeuroopalise GDPR rakendamisega on kõikidel kriitilise infrastruktuuri ettevõtete töötajatel kohustus läbida vastav koolitus.
Palun kõigil tutvuda ajaplaaniga:
http://gdprcompliance.ee/koolitused/ajaplaan-2017
Esimene infotund toimub juba juulikuus.

Lugupidamisega,
info@gdprcompliance.ee

Figure 15. Type X Email Content

Translation from Estonian to English:

Hello,

In the context of the implementation of pan-European GDPR, all employees of critical infrastructure enterprises are required to complete the corresponding training.

Please get acquainted with timetable: http://gdprcompliance.ee/koolitused/ajaplaan-2017

First timeslots will be in July.

Best regards,

info@gdprcompliance.ee

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" style="-webkit-text-size-ad-
just:none;">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title></title>
<body>
Tere<br /><br />
Seoses üleeuroopalise GDPR rakendamisega on kõikidel kriitilise infrastruktuuri
ettevõtete töötajatel kohustus läbida vastav koolitus.<br />
Palun kõigil tutvuda ajaplaaniga: <a href="<%= @url %>">http://gdprcompli-
ance.ee/koolitused/ajaplaan-2017</a>.<br />
Esimene infotund toimub juba septembris.
<br /><br />
Lugupidamisega,<br />
info@gdprcompliance.ee<br />
</body>
</html>
```

Figure 16. Type X Email HTML Full Code

Appendix D - Experiment I Campaign I Type Y[1] Email Content

Subject: Teie tellimus on valmis
Date: Thu, 29 Jun 2017 11:02:15 +0300
From: Kaunid Pildid <info@kaunidpildid.eu>
Reply-To: info@kaunidpildid.eu

Hea Klient,

Palju õnne! Olete registeeritud oma kasutaja. Registeerumise kulusid tasuda enne 04.07.2017.
Tellimus näete aadress kaunidpildid.eu
Kui saite selle kirja kogemata, siis palun külastage leht kaunidpildid.eu ja tühistage tellimus.

Lugupidamisega,
Kaunidpildid
info@kaunidpildid.eu

Figure 17. Type Y[1] Email Content

Translation from Estonian to English:

Dear Client,

Congratulations! You are registered with your user. Registration fee must be paid before July 4, 2017

You will see an order at kaudnidpildid.eu

If you accidentally received this message, please visit kaudnidpildid.eu and cancel the order

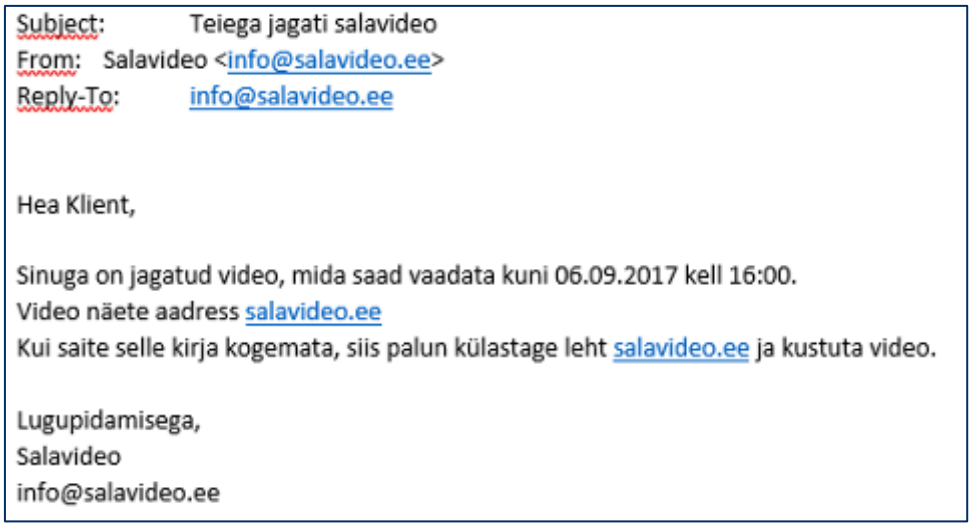
Sincerely,

Kaunidpildid

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" style="-webkit-text-size-ad-
just:none;">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title></title>
<body>
Hea Klient, <br /><br />
Palju õnne! Olete registeeritud oma kasutaja. Registeerumise kulusid tasuda enne
04.07.2017.<br />
Tellimus näete aadress <a href="<%= @url %>">kaunidpildid.eu</a><br />
Kui saite selle kirja kogemata, siis palun külastage leht <a href="<%= @url
%>">kaunidpildid.eu</a> ja tühistage tellimus.<br />
<br /><br />
Lugupidamisega,<br />
Kaunidpildid<br />
info@kaunidpildid.eu<br />
</body>
</html>
```

Figure 18. Type Y[1] Email HTML Full Code

Appendix E - Experiment I Campaign II Type Y² Email Content



Subject: Teiega jagati salavideo
From: Salavideo <info@salavideo.ee>
Reply-To: info@salavideo.ee

Hea Klient,

Sinuga on jagatud video, mida saad vaadata kuni 06.09.2017 kell 16:00.
Video näete aadress salavideo.ee
Kui saite selle kirja kogemata, siis palun külastage leht salavideo.ee ja kustuta video.

Lugupidamisega,
Salavideo
info@salavideo.ee

Figure 19. Email of Type Y² email in experiment I

Translation from Estonian to English:

Dear Client,

Video has been shared with you, you can see it until 06.09.2017 16:00

Video can be seen on address salavideo.ee

If you got this letter by accident, then please visit webpage salavideo.ee and delete the video.

Best regards,

Salavideo

info@salavideo.ee

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" style="-webkit-text-size-ad-
just:none;">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title></title>
<body>
Hea Klient, <br /><br />
Sinuga on jagatud video, mida saad vaadata kuni 06.09.2017 kell 16:00.<br />
Video näete aadress <a href="<%= @url %>">salavideo.ee</a><br />
Kui saite selle kirja kogemata, siis palun külastage leht <a href="<%= @url
%>">salavideo.ee</a> ja kustuta video.<br />
<br /><br />
Lugupidamisega,<br />
Salavideo<br />
info@salavideo.ee<br />
</body>
</html>
```

Figure 20. Type Y² email HTML Full Code

Appendix F - Experiment I Type X, Type Y[1] Type Y[2] Link Landing Page HTML Code

```
<!DOCTYPE html PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>404 Not Found</title>
</head>
<body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
</body></html>
</html>
```

Appendix G – Experiment I Result Analyse Table

Table 7. Experiment I Result Analysis Table

Experiment I (Phishing)												
	Campaign I (29.06.2017)											
	Type X (level 3)						Type Y (level 2)					
	Group K male		Group K female		Group K		Group L male		Group L female		Group L	
Emails sent	12	100%	14	100%	26	100%	7	100%	20	100%	27	100%
Number Clicked	3	25,0%	0	0,0%	3	11,5%	1	14,3%	4	20,0%	5	18,5%
Number Reported	5	41,7%	2	14,3%	7	26,9%	0	0,0%	5	25,0%	5	18,5%
Click / No Report	2	16,7%	0	0,0%	2	7,7%	1	14,3%	3	15,0%	4	14,8%
Click / Report	1	8,3%	0	0,0%	1	3,8%	0	0,0%	1	5,0%	1	3,7%
No Click / No Report	5	41,7%	12	85,7%	17	65,4%	6	85,7%	12	60,0%	18	66,7%
No Click / Report	4	33,3%	2	14,3%	6	23,1%	0	0,0%	4	20,0%	4	14,8%
	Campaign II (06.09.2017)											
	Type X (level 3)						Type Y (level 2)					
	Group L male		Group L female		Group L		Group K male		Group K female		Group K	
Emails sent	7	100%	20	100%	27	100%	12	100%	14	100%	26	100%
Number Clicked	3	42,9%	6	30,0%	9	33,3%	0	0,0%	1	7,1%	1	3,8%
Number Reported	0	0,0%	3	15,0%	3	11,1%	5	41,7%	2	14,3%	7	26,9%
Click / No Report	3	42,9%	6	30,0%	9	33,3%	0	0,0%	1	7,1%	1	3,8%
Click / Report	0	0,0%	0	0,0%	0	0,0%	0	0,0%	0	0,0%	0	0,0%
No Click / No Report	4	57,1%	11	55,0%	15	55,6%	7	58,3%	11	78,6%	18	69,2%
No Click / Report	0	0,0%	3	15,0%	3	11,1%	5	41,7%	2	14,3%	7	26,9%
	Campaign I and II											
	Type X (level 3)						Type Y (level 2)					
Emails sent	53	100%					53	100%				
Number Clicked	12	22,6%					6	11,3%				
Number Reported	10	18,9%					12	22,6%				
Click / No Report	11	20,8%					5	9,4%				
Click / Report	1	1,9%					1	1,9%				
No Click / No Report	32	60,4%					36	67,9%				
No Click / Report	9	17,0%					11	20,8%				

Appendix H - Questions Related to Phishing

General questions:

2. Have you been targeted by similar phishing campaigns before? If "Yes", Was this campaign any different form the one you have participated in? Please elaborate? *Kas te olete varem ka kokku puutunud õngituskirjade kampaaniaga, kas siis praeguses või eelnevas töökohas? Kas see kampaania oli erinev? Palun põhjendage!*
3. Do you think that conducting phishing campaigns among employees is ethical? Could you please elaborate? *Kas te tunnete, et õngitsuskampaania läbiviimine on eetiline ja millisel juhul ebaeetiline? (Kas töötaja tundeid riivatakse testi tehes, s.t. kas ta tunneb ennast katsealusena)*
4. Do you think that it is necessary to conduct phishing campaigns among employees? Could you please elaborate? *Kas teie arvates on õngitsuskampaania läbiviimine ettevõtte töötajate seas vajalik? Miks on vajalik? Põhjendage!*
5. In your opinion, how could the process of phishing campaigns, that are sent to employees, be improved? *Kuidas võiks teie arvates õngitsuskampaania protsessi paremaks muuta?*

Campaign-related questions:

6. In general, is it easy for you to recognise a phishing email? Please elaborate. *Kui lihtne on teie meelest ära tunda sellised kirju?*
7. Do you remember receiving the communication that informed you about the upcoming phishing campaign in advance? If they say "Yes": Did receiving such an announcement email helped you to recognize that the email sent to you was a phishing email? *Kas te mäletate, et saite teavituskirja õngitsuskampaania kohta? (Jah/Ei) Kui jah: Kas teavituskirja saamine aitas teil aru saada, et õngitsuskampaania käigus tulnud kiri oli test? (Jah/Ei)?*
8. Did you recognize that the email sent to you in June was a phishing email? What made you to have that conclusion? If they say "Yes", but still clicked on the email: What made you to click on the email even though you recognised it was a phishing email? *Kas te saite juunis saadetud kirja puhul aru, et tegemist on õngitsuskirjaga? Jah/Ei. Mis teid sellele järeldusele viis?* (Kui sai aru, et on õngitsuskiri, aga ikkagi klikkis, siis peaks küsima juurde: Miks te ikkagi kirjal klikkasite, kuigi saite aru, et on õngitsuskiri?)
9. Did you recognize that the email sent to you in September was a phishing email? What made you to have that conclusion? If they say "Yes", but still clicked on the email: What made you to click on the email even though you recognised it was a phishing email? *Kas te saite septembris saadetud kirja puhul aru, et tegemist on õngitsuskirjaga? Jah/Ei. Mis teid sellele järeldusele viis?* (Kui sai aru, et on õngitsuskiri, aga ikkagi klikkis, siis peaks küsima juurde: Miks te ikkagi kirjal klikkisite, kuigi saite aru, et on õngitsuskiri?)
10. How would you compare the two phishing campaigns? In your opinion where there any differences? *Kuidas te võrdleksite kahte väljasaadetud kirja? Kas teie arvates*

oli neis suuri erinevusi? (kas oli ära tuntav, et üks on kerge ja teine raske) Mis need olid?

11. Did you report the phishing email? Why did you take that decision? *Kas te raporteerisite õngitsuskirjast? Miks te nii tegite? Kuidas te reageerisite ja miks?*
12. Are you aware whom you should contact when you see a phishing email? *Kas te olete teadlik mis käitumist teilt oodatakse.*
13. How should you forward such an email? *Kuidas tuleks kahtlane kiri edastada?*
14. Do you think that participating in such experiments helps you to better recognize similar phishing emails in the future? *Kas te arvate, et eksperimendis osalemine aitab teil tulevikus taolisi kirju ära tunda? Miks?*
15. What could be better done in a phishing email experiment? *Mida saaks paremini teha õngituskirjade testis?*

Appendix I - Questions Related to Spear Phishing

General questions:

1. Have you been targeted by similar spear phishing campaigns before? If "Yes", Was this campaign any different form the one you have participated in? Please elaborate? *Kas te olete varem ka kokku puutunud suunitletud õngituskirjade kampaaniaga, kas siis praeguses või eelnevas töökohas? Kas see kampaania oli erinev? Palun põhjendage!*
2. Do you think that conducting spear phishing campaigns among employees is ethical? Could you please elaborate? *Kas te tunnete, et suunitletud õngitsuskampaania läbiviimine on eetiline ja millisel juhul ebaeetiline? (Kas töötaja tundeid riivatakse testi tehes, s.t. kas ta tunneb ennast katsealusena)*
3. Do you think that it is necessary to conduct spear phishing campaigns among employees? Could you please elaborate? *Kas teie arvates on suunitletud õngitsuskampaania läbiviimine ettevõtte töötajate seas vajalik? Miks on vajalik? Põhjendage!*
4. In your opinion, how could the process of spear phishing campaigns, that are sent to employees, be improved? *Kuidas võiks teie arvates suunitletud õngitsuskampaania protsessi paremaks muuta?*

Experiment-related questions:

1. In general, is it easy for you to recognise a spear phishing email? Please elaborate. *Kui lihtne on teie meelest ära tunda sellised suunitletud kirju?*
2. Do you remember receiving the communication that informed you about the upcoming spear phishing campaign in advance? If they say "Yes": Did receiving such an announcement email helped you to recognize that the email sent to you was a phishing email? *Kas te mäletate, et saite teavituskirja suunitletud õngitsuskampaania kohta? (Jah/Ei) Kui jah: Kas teavituskirja saamine aitas teil aru saada, et õngitsuskampaania käigus tulnud kiri oli test? (Jah/Ei)?*
3. Did you recognize that the email sent to you in July was a spear phishing email? What made you to have that conclusion? If they say "Yes", but still clicked on the email: What made you to click on the email even though you recognised it was a phishing email? *Kas te saite juunis saadetud kirja puhul aru, et tegemist on suunitletud õngitsuskirjaga? Jah/Ei. Mis teid sellele järeldusele viis?* (Kui sai aru, et on õngitsuskiri, aga ikkagi klikkis, siis peaks küsima juurde: Miks te ikkagi kirjal klikkasite, kuigi saite aru, et on õngitsuskiri?)
4. Did you report the spear phishing email? Why did you take that decision? *Kas te raporteerisite suunitletud õngitsuskirjast? Miks te nii tegite? Kuidas te reageerisite ja miks?*
5. Are you aware who you should contact when you see a phishing email? *Kas te olete teadlik mis käitumist teilt oodatakse.*
6. How should you forward such an email? *Kuidas tuleks kahtlane kiri edastada?*

7. Do you think that participating in such experiments helps you to better recognize similar spear phishing emails in the future? *Kas te arvate, et eksperimendis osalemine aitab teil tulevikus taolisi kirju ära tunda? Miks?*
8. What could be better done in a spear phishing email experiment? *Mida saaks paremini teha suunitletud õngituskirjade testis?*

Appendix J – One-Pager Checklist

Before launching the email phishing campaign

1. Define the purpose and desired outcome of the phishing campaign. This affects the way the program is structured. Insource or outsource the capabilities.
2. Sign a contract. It must be signed by a legal representative of the company. Consider ethical and legal aspects, e.g. processing of data. The contract should outline the following:
    a. Statement of confidentiality and roles and responsibilities
3. Choose the phishing email difficulty level and participants
    a. Analyse previously conducted phishing campaigns
    b. Select participants and define the target group size
4. Choose the platform for campaigns, by deciding the following:
    a. Features needed
    b. Free or commercial
    c. On premises or in cloud
5. Inform employees. Consider ethical and legal aspects so that employees would not feel deceived. The briefing email should include:
    a. Description of phishing and possible consequences
    b. Campaign description and purpose
    c. Interactive learning options
    d. Responsibility of the employees and the reporting process
6. Create phishing content. Consider the chosen phishing email difficulty level. Understand ethical and legal aspects of phishing content, e.g. violations of a provider's terms of use, intellectual property rights and copyright infringement.
    a. Design the email content according to the chosen difficulty level
    b. Choose the attack type and the landing page type
7. Test the technical setup
    a. End-to-end verification of successful simulated email phishing testing
    b. In case of attachments test by executing these on a target's computer

During the email phishing campaign

1. Notify both internal and external parties
    a. Inform internal IT Helpdesk
    b. Inform external CERT
2. Distribute phishing emails
    a. Answer participants' queries timely and mind their wellbeing
    b. Verify logs
3. Inform participants after the campaign. The debriefing email should include:
    a. Attached copy of the phishing email and further details about the campaign
    b. Interactive learning options
    c. Responsibility of the employees and the reporting process
    d. Possible consequences

After launching the email phishing campaign

1. Analyse results
    a. Generate report to evaluate company vulnerability to phishing attacks
    b. After the analyses, delete campaign data and encrypt the report
2. Interview participants to ask feedback for improving the process. Different participants should be interviewed based on their actions regarding clicking and reporting.

I. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Kaspar Jüristo**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

How to Conduct Email Phishing Experiments,

supervised by Sten Mäses, Olaf M. Maennel, Raimundas Matulevičius.

2. I am aware of the fact that author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **16.05.2018**