

TALLINN UNIVERSITY OF TECHNOLOGY  
School of Information Technology  
Department of Software Science  
TUT Centre for Digital Forensics and Cyber Security

MEASURING PERSONNEL CYBER SECURITY  
AWARENESS LEVEL THROUGH PHISHING  
ASSESSMENT

Masters's thesis  
ITC70LT

Author: Kaspr Prei  
Student code:143903IVCM  
Supervisors: Olaf Manuel Maennel,  
Bernhards Blumbergs

Tallinn 2017

## Declaration

I hereby declare that I am the sole author of this thesis. The work is original and has not been submitted for any degree or diploma at any other University. I further declare that the material obtained from other sources has been duly acknowledged in the thesis.

.....

(signature)

[January 2, 2017]

## List of Acronyms and Abbreviations

2FA	Two-Factor Authentication
API	Application Program Interface
APWG	Anti-Phishing Working Group
CERT EE	Computer Emergency Response Team Estonia
CIO	Chief Information Officer
CTR	Click Through Rate
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication Reporting and Conformance
DNS	Domain Name Server
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ISP	Internet Service Provider
IT	Information Technology
MX Record	Mail Exchanger Record
NDA	Non-disclosure Agreement
PHP	Hypertext Preprocessor
POST	An HTTP command used to send text to a Web server for processing
PTR Record	Pointer Record
OTP	One Time Password
SaaS	Software as a Service
SMTP	Simple Mail Transfer Protocol
SPF	Sender Framework Policy
SSL	Secure Sockets Layer
UID	User Identification
URL	Uniform Resource Identifier

## **Abstract**

The thesis focuses on finding the best method to measure personnel cyber security awareness level. To accomplish this goal, first, good metric for the purpose is found. Secondly, analyses of anti-phishing tools were conducted. It concluded that, as security tools are not providing enough protection, the employee frequently needs to make decisions about authentic or unauthentic requests and it is important for organizations to identify employees vulnerable to social-engineering attacks. In addition for finding best methodology, demonstration of how to set up the measurement programme is done. Steps which will be shown are getting the right approvals, ethical, legal, and technical considerations.

Using Phishing Frenzy, two phishing assessments were conducted. In the thesis, results of the campaigns are conveyed and analyses about assessments result, users and CIOs feedback, personnel learning curve, and correlation between cyber hygiene test and phishing assessments are completed. According to analyzes, phishing assessment is found as the best way to measure personnel cyber security awareness level.

## Annotatsioon

Käesolev lõputöö keskendub asutuse töötajate küberturbe teadlikkuse mõõtmiseks sobivaima meetodi leidmisele. Selle nimel leiti esiteks sobiv mõõdik, seejärel viidi läbi kalastusrünnete kaitsmiseks mõeldud rakenduste analüüs. Analüüsi järelduseks on see, et vastavad rakendused ei paku piisavat kaitset ning töötajad on tihtipeale sunnitud ise tuvastama autentse või mitteautentse päringu ning seetõttu on asutuste jaoks oluline tuvastada töötajad, kes on manipulatsiooni rünnete suhtes haavatavad. Lisaks parima viisi leidmisele, toob käesolev lõputöö välja kuidas vastavat meetodit rakendada. Sel puhul demonstreeritakse vajalike loa saamiste, eetiliste, õiguslike ja tehniliste nüansside sammud.

Kasutades Phishing Frenzy tarkvara, viiakse läbi kaks küberturbe teadlikkuse mõõtmiseks mõeldud kalastusründe testi. Lõpustöös on kahe vastava testi tulemused ning nende tulemuste, kasutajate ja infoturbejuhtide tagasiside, kasutajate õppimistulemuste ning küberhügieeni ja kalastusründe testi võrdluse analüüs välja toodud. Käesolev lõputöö leiab, et parim viis töötajate küberturbe teadlikkuse mõõtmiseks on kalastusründe testi läbiiviimine.

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>11</b>
1.1	Problem statement and contribution of the thesis . . . . .	12
1.2	Detecting and measuring personnel vulnerable to social engineering attacks	12
1.3	Overview of related work . . . . .	15
1.4	Outline of the Thesis . . . . .	17
1.5	Acknowledgments . . . . .	17
<b>2</b>	<b>Effectiveness of anti-phishing tools</b>	<b>18</b>
2.1	Taking down the phishing websites . . . . .	18
2.2	Email scanning . . . . .	20
2.3	Client based anti-phishing tools . . . . .	25
2.3.1	E-mail client based mitigation . . . . .	25
2.3.2	Browser based mitigation . . . . .	26
2.3.3	Anti-phishing toolbars . . . . .	28
2.3.4	Password management . . . . .	28
2.4	Authentication . . . . .	29
2.5	Statistical curve from past to nowadays . . . . .	31
<b>3</b>	<b>Measuring personnel cyber security awareness level</b>	<b>32</b>
3.1	Questions about knowledge or something else? . . . . .	32
3.2	Decision-making factors . . . . .	33
3.2.1	Hunger . . . . .	33
3.2.2	Lack of sleep . . . . .	34
3.2.3	Stress . . . . .	34
3.2.4	External factors . . . . .	34
3.3	Personality factors . . . . .	34
3.4	Following the rules . . . . .	35
<b>4</b>	<b>Preparing for phishing assessment</b>	<b>37</b>
4.1	Categorization of phishing e-mails . . . . .	37
4.1.1	Level one phish . . . . .	37
4.1.2	Level two phish . . . . .	38
4.1.3	Level three phish . . . . .	38
4.1.4	Level four phish, or spear-phishing . . . . .	39
4.2	Choosing e-mail difficulty for assessments . . . . .	39

4.3	Approvals for assessment . . . . .	40
4.4	Ethical considerations . . . . .	43
4.5	Legal considerations . . . . .	44
4.5.1	Using IT systems . . . . .	44
4.5.2	Trademark and copyright . . . . .	45
4.5.3	Collecting phishing data . . . . .	46
4.5.4	Terms of Conditions . . . . .	47
4.6	Choosing technical solution . . . . .	47
4.6.1	SaaS solution . . . . .	48
4.6.2	Open-source server . . . . .	48
4.6.3	Commercial server . . . . .	49
4.6.4	Custom made . . . . .	50
<b>5</b>	<b>Conducting phishing assessment</b>	<b>51</b>
5.1	Technical set up . . . . .	51
5.1.1	Send e-mails . . . . .	51
5.1.2	Landing website . . . . .	52
5.2	Assessment 1 . . . . .	53
5.2.1	Phishing e-mail . . . . .	53
5.2.2	Landing web page . . . . .	55
5.2.3	Result . . . . .	56
5.3	Assessment 2 . . . . .	57
5.3.1	Phishing e-mail . . . . .	57
5.3.2	Landing web page . . . . .	59
5.3.3	Result . . . . .	60
5.4	Reaction by participants . . . . .	61
5.5	Learning curve . . . . .	61
5.6	Compare phishing assessments and cyber hygiene test . . . . .	62
5.7	Additional benefits . . . . .	63
5.8	Future work . . . . .	63
<b>6</b>	<b>Conclusion</b>	<b>65</b>
	<b>References</b>	<b>67</b>
	<b>Appendix 1 - Bulk e-mail sending pricelist</b>	<b>82</b>
	<b>Appendix 2 - Postfix configuration file</b>	<b>83</b>

Appendix 3 - Email during preparation phase	85
Appendix 4 - Email design for assessment one	86
Appendix 5 - HTML code of assessment one landing page	87
Appendix 6 - Email design for assessment two	90



# List of Figures

- 1 Phishing site uptimes (hh:mm) . . . . . 18
- 2 Phishing victims over the first 72 hours . . . . . 19
- 3 Spammer tricks Q3 2015 . . . . . 23
- 4 A phishing trampoline – embedding redirects in PDF documents . . . . . 24
- 5 Who will eventually click [1] . . . . . 24
- 6 Outlook warning [2] . . . . . 25
- 7 Google Chrome warning about potential phishing website [3] . . . . . 26
- 8 Attacking two-factor authentication [4] . . . . . 30
- 9 Percentage reported [5] . . . . . 36
- 10 RSA phishing e-mail [6] . . . . . 39
- 11 Choosing web attack method in SET [7] . . . . . 49
- 12 Campaign 1 Email Settings . . . . . 53
- 13 Email of assessment one . . . . . 54
- 14 Landing page of assessment one . . . . . 56
- 15 Email of assessment two . . . . . 58
- 16 Screenshot in landing web page during assessment two . . . . . 59
- 17 Assessment 2: clicks in minutes . . . . . 60
- 18 Bulk e-mail sending pricelist [8] . . . . . 82
- 19 Email during testing period . . . . . 85

## List of Tables

1	Browsers' phishing websites URL blocking ratio . . . . .	27
2	Phishing attack trend report . . . . .	31
3	Campaign 1 summary . . . . .	57
4	Campaign 2 summary . . . . .	60
5	Cyber hygiene and phishing assessments comparison matrix . . . . .	62

# 1 Introduction

IT systems consist of technology, human and processes. Technological parts are logged, scanned, monitored and pen-tested; processes are audited, but because regular employees are not seen as the persons who can raise the level of resistance against cyber attacks, human testing is often either forgotten or given low priority to. It has led to a situation where human being is frequently referred to as the weakest link in cyber security and therefore social engineering attacks are so successful and frequently used. Kevin Mitnick: *"the only thing that's changed in regards to vulnerability are technical issues, but with social engineering, it's all remained the same. So, it depends how vigilant the owners and the operators of the computer systems and the network are"* [9]. SANS Institute, that claims itself to be the most trusted and by far the largest source for information security training in the world[10], has written *"The complacent user is extremely common in all phases of our workplace and as a result now becomes "THE WEAKEST LINK* [11]." Anti-Phishing Working Group states: *"We strongly encourage that businesses educate their employees about the dangers of these scams and implement technologies that intercept the incoming e-mails* [12]." Many other publications have the same understanding – the uneducated user is seen as the weakest link [13, 14].

Social engineering is using various techniques like manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefit to the attacker [9]. According to different reports, social engineering, specifically phishing, is still highly-used attack vector by cyber criminals [15, 16, 17, 18]. Phishing is a form of fraud in which the attacker tries to acquire information such as login credentials or account information by masquerading as a reputable entity or person in e-mail, IM or other communication channels [19]. According to Verizon's 2013 Data Breach Investigation Report, phishing was associated with over 95% of incidents assigned to state sponsored actors, and for two years in a row, more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing [15].

In order to reduce the success of phishing, which is one of the most wide-spread social engineering attacks, various anti-phishing tools are used: two-factor authentication, spam filters, e-mail client configuration, certificates and security toolbars. However, the question is, whether anti-phishing tools are enough to fight against social engineering attacks or it is vital to identify the users who are vulnerable to social engineering attacks [20, 21, 22]. In addition, it is vital to find the most appropriate methodology to identify vulnerable users.

## **1.1 Problem statement and contribution of the thesis**

This thesis aims to demonstrate why and how one needs to measure personnel cyber security awareness level. Most of the papers completed on this topic are approximately 5-10 years old. In other cases, information is scattered between different papers and blog articles. This means there are no recent papers available which would walk through the whole process needed for the best measurement program.

This thesis will do the following:

- Identify the necessity to measure personnel cyber security awareness level
- Analyse how anti-phishing tools perform
- Find the best way to measure cyber security awareness level
- Explain how phishing assessments are prepared
- Conduct two phishing assessments
- Analyze the results of assessments

The main contribution of the thesis is suggesting a way to measure personnel awareness level, and show how to prepare for the program. In addition to analyzing previous work, two phishing assessments are conducted, results and analyses of assessments are delivered, and finally, additional benefits of using recommended methodology are highlighted.

## **1.2 Detecting and measuring personnel vulnerable to social engineering attacks**

In order to detect and measure vulnerable users, cyber security awareness level metrics will be used. SANS Institute has provided summary of suitable metrics, based on Andrew Jaquith's book "Security Metrics: Replacing Fear, Uncertainty, and Doubt[23]": cyber security awareness has to be measured in a consistent way; value needs to be displayed as either number or percentage; metrics have to be easy and cheap; and they have to be relevant, an example of an irrelevant metric is a top ten list of countries that host spam. Although the United States is the frontrunner in this category, the fact in itself does not help the security specialists, because blocking every e-mail coming from the US is clearly not a viable solution. It is important to have a metrics which we can do something about[24].

To measure the impact of security awareness program, SANS Institute offers four options [25]: Metric Matrix; Human Risk Survey; Human Metrics: Measuring Behavior; and Effective Phishing of Employees.

First option is Metric Matrix, an example Excel file of which is available for download at <https://www.securingthehuman.org/media/resources/planning/Stage05-01-MetricsMatrix.zip>. Named “Measure the Impact of Your Security Awareness Program”, it consists 13 metrics. The list of metrics is comprehensive, but one needs to ask: if the organization is implementing the Metric Matrix, is it following key standpoints of security metrics? As pointed out, measurements need to be conducted in a consistent way; taking into consideration that value value needs to be expressed either a number or percentage; metric has to be easy and cheap; and it has to be relevant. The problem with the listed metrics is that many organizations do not have the resources required for running the Matrix. The goal is to achieve maximum results while using as little resources as possible. In addition, some metric options do not meet the requirements for good metrics provided by "Security Metrics: Replacing Fear, Uncertainty, and Doubt". For example, metrics like "Number of employees who has a secure desk environment"; "Number of employees posting sensitive organizational information on social networking sites"; "Number of employees who are properly following data destruction processes;" "Number of employees who left their devices unsecured in their cars in the organization’s parking lot"; and "Number of employees who understand, follow and enforce your policies for restricted or protected access to facilities" are subjective, and not necessarily easy or cheap to measure. For these reasons, it is possible to state that Metric Matrix is not the best way to measure personnel cyber security awareness level.

The second metric is Human Risk Survey [26]. SANS Institute describes Human Risk Survey as following: *“This twenty-five question survey will help you determine the human risk in your organization. Each question and its respective answers have different levels of risk associated with them. Depending on how your employees respond, you can add up the answers and determine a quantitative value of your human risk [27]”*. The survey is a good way to understand how well personnel knows the security policies, standards, procedures and how they think they would act while working with information assets. Nevertheless, the problem with the survey is that it tests only personnel knowledge, not how they actually act. A publication named “Why Phishing Works [28]” conducted a research project in which twenty-two participants were involved in the phishing assessment where they had to identify spoofed and real websites. Although the main reason why people are victims of phishing attack was their lack of knowledge, there appeared to be other reasons behind the failures: visual deception

and bounded attention. In addition, other research studies bring out the importance to understand that question is not only about education, it can be tiredness, hunger, stress, personality factors and attack timing [29, 30, 31, 32, 33].

Third possible metric is Effective Phishing of Employees. SANS Institute claims the following: "One of the most effective ways to address phishing attacks is to train and measure employees through phishing assessments [25]." Also, as phishing plays major role in social engineering attacks, to spot and to mitigate social engineering attacks, maybe it is good idea to focus on users who are vulnerable to phishing [34, 35, 36]? Some of the reasons, to use phishing as metric are as follows:

- As described in chapter "Measuring personnel cyber security awareness level", phishing is a frequently used social engineering attack vector and social engineering is directly manipulating users with low cyber security awareness level;
- It allows to recreate the very same attacks that the cyber criminals are launching [37];
- It provides a vast range of aspects that make phishing a successful attack vector, such as information available on the Internet, psychological principles, influencing options and available tools [38];
- It provides an excellent way to measure changes in behavior [39];
  - ◊ Measures personnel with high risk to be victim of phishing attack;
  - ◊ Simple, low-cost and easy to repeat;
  - ◊ Quantifiable measurements;
  - ◊ Actionable;

Thus, it seems to be a near-to perfect solution to measure personnel awareness level through using a widespread attack vector, which mostly includes more than one aspect of social engineering attacks? However, if this is true, then why is phishing assessment not widely used? Possible reasons for this could be ethical; legal; technical; difficulty of getting the necessary approvals; and organizations may be afraid of losing vital cooperation between security personnel and regular employees. The question is: how to overcome these obstacles, and are the solutions in fact worth countering the risk?

Fourth metric: "Human Metrics: Measuring Behavior [37]," has three other topics in addition to the phishing assessment: Are People Updating Devices; Desktop Physical Security; and Rogue Wi-Fi Access Points. As two topics can be solved by central

management and Desktop Physical Security is not a good metric, then compared to Effective Phishing of Employees "Human Metrics: Measuring Behavior" is not providing additional benefit for measuring personnel awareness level.

### 1.3 Overview of related work

In order to fight against phishing attacks, organizations rely on various defence layers. Firstly, there are companies who support access to phishing websites - ISPs and website hosting companies. There are no comprehensive research papers about how successful they are at neutralizing attacks before they start, but according to APWG's Global Phishing Report [40] and Cyveillance's chart [1], it can be concluded that this layer needs to be improved. Second layer has to do with the effectiveness of spam filters. Overall, spam filters are performing well by successfully blocking on average 90% of spam [1], but 10% of malicious e-mails still manages to pass spam filters. Several papers are describing why it is happening and which techniques are used by spammers [41, 42, 43]. Third level is constituted of client-based mitigation tools. It can be done by applying secure configuration on e-mail client [44]; browser; or using password managers. Although browsers are using active indicators and splash screens, users are still ignoring them by proceeding to a phishing website [45, 46]. Fourth layer is multi-factor authentication. While it is a recommended way to protect your accounts [47], it is still not as widely used as needed.

Although anti-phishing mitigation tools are widely used, phishing still remains to be one of the most common attack vectors. To mitigate the threat that stems from it, it is necessary to provide adequate education to the personnel. The term 'awareness' can have different meanings, hereby a definition by NIST is provided: "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security [48]". Some others suggest that the primary purpose of security awareness is to change the behavior [49]. In this thesis, awareness is perceived as something that is not only about knowledge, but also about how employees would act during real phishing attack in their real-life environment. There are several reasons for people sometimes acting in erroneous ways, despite having been educated enough to spot phishing attack. For instance, decision-making can be influenced by hunger [50, 51], lack of sleep [30], working under stress [52, 53], or external factors like hot or cold weather [54]. In addition, personality "Big Five" traits [32] will contribute to differences, whereas some people just do not follow the rules [5].

When one starts to conduct phishing assessment, many things can go wrong. If ethical aspects are underestimated or neglected, participants who are part of the phishing

simulation may get a sense of victimization or anger [55]. As one of the key elements in information security is trust between employees and security specialists, such a situation has to be avoided. Also, participants have previously requested phishing researchers to be prosecuted or fired [56]. Several studies have been published about possibilities to solve the ethical issues while still having options to measure users who are vulnerable to phishing attacks [55, 56]. In addition, two phishing assessments were conducted in the highly religious country of Qatar [57].

The perspectives assumed by the law and the researchers often tend to differ, hence, in the recent decades, governments have sued a significant number of computer scientists [58, 59, 60, 61]. The legal problems related to phishing assessment may, for instance, be related to the illegal use of IT systems [62, 63]; trademark and copyright questions [33, 64]; collecting phishing data; or with Terms and Conditions. Two publications bring out key points on how to avoid prosecution [33, 65].

In order to have a possibility to conduct a phishing assessment and to measure personnel awareness level, a well-functioning technical environment is needed. There are commercial [66, 67] and open-source [68, 69, 70] tools available. When choosing a solution regarding the phishing server, there is number of topics which need to be considered. It is important to start with setting the scale and purpose of your campaign. The following aspects need to be considered: the amount of e-mails to be sent; the number of simultaneous campaigns that will be run; location of the phishing server; organization's security policy about handling confidential information; the level of competency of your organization's IT team. "Phishing Dark Waters: The offensive and defensive sides of malicious emails" [33] gives an overview about some of the products, their pros and cons.

In addition to technical, legal and ethical issues, security personnel carrying out the test, needs to get an approval for the assessment. Most widely used and community websites point out to have an approval from management [71, 72], but it is not enough even in case the phishing server and e-mails are used only internally.

Phishing one's own colleagues is often the recommended way to measure and to educate employees [25, 34, 35, 36], but there are no analyses about comparing the results of phishing assessment and quizzes.

Most of published phishing assessments have been carried out almost ten years ago [73, 56, 74, 5, 75, 76]. As ten years is a long time in the field of cyber security, it is important to repeat similar assessments. In addition, most of the phishing assessment related papers are describing only minor parts, as opposed to the assessment as a whole, and relevant pieces are scattered around different publications. The following



thesis aims to display all the necessary details in one thesis.

## **1.4 Outline of the Thesis**

This thesis is organized into five chapters. Chapter 1 gives an introduction to the thesis. Problem statement and previous work on related topics are also discussed. Chapter 2 analyzes anti-phishing tools. Chapter 3 looks into human weakness and asks why despite adequately educated personnel, phishing attack is still an effective attack vector. Next, chapter 4 demonstrates necessary steps in preparation for the phishing assessment. chapter 5 describes two assessments conducted for the thesis, analyzes the results, and explains some of the additional advantage of phishing assessments. Finally, chapter 6 concludes the thesis.

## **1.5 Acknowledgments**

I would like to thank all the four organizations that were involved in research for this thesis. These include the organization that allowed to use its infrastructure; one of the Estonian ministries that impersonated their domain; and two companies and their CIOs together with whom phishing assessments were carried out.

## 2 Effectiveness of anti-phishing tools

This chapter will give an overview of existing anti-phishing tools and their effectiveness. Such techniques include taking down the phishing websites, e-mail scanning, client device tools, authentication. In addition, this chapter will analyse the statistic curve regarding these techniques from past to nowadays.

### 2.1 Taking down the phishing websites

In order to block access to phishing websites, ISPs are blacklisting IP addresses and domain names, and website hosting companies are deleting the websites. As seen on Figure 1, the average lifespan of a phishing website has remained relatively stable from 2012 to 2014 - between 24 hours and 30 hours. To give more detail, the average uptime for phishing attacks in second half of 2014 was 29 hours and 51 minutes [40]. Method how uptime duration was counted was following: *"The system used to track the uptimes automatically monitored the phishing sites, and monitoring began as soon as the system became aware of a phish via feeds or honeypots. Each phish was checked several times per hour to confirm its availability, and was not declared "down" until it had stayed down for at least one hour [40]."*

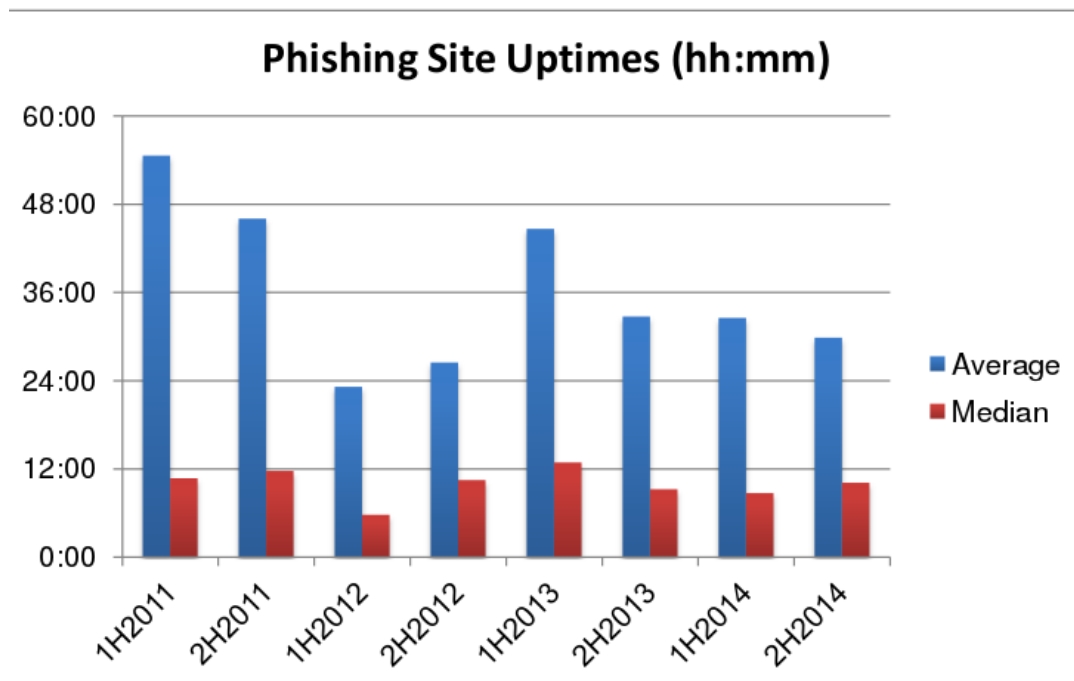


Figure 1. Phishing site uptimes (hh:mm)

[40]

In order to understand whether taking down the websites is effective, one could, for instance, draw one report *The Cost of Phishing*, published by Cyveillance. According to report, 12 hours after the attack is the peak-time in terms of the amount of victims, while after 24 hours, the amount of phished victims is going down: *"Duration is a key factor in the overall cost of a phishing attack, and most costs are incurred in the first 24 hours. Thus, speed of detection and takedown are key [1]."* Figure 2 visualizes the graph about phishing victims over the first 72 hours. Addition, Verizon reports that nearly 50% of phished users will open e-mail and click on phishing links within the first hour [15].



Figure 2. Phishing victims over the first 72 hours [1]

If one considers that most of the users will be victims of phishing attack within first 24 hours, whereas identifying and taking down the website usually takes more than one day, it is clear that techniques used at the moment to block phishing websites are not efficient enough to effectively fight against phishing.

Lesson to security minded organization is that, at the moment they cannot rely on ISPs and website hosting companies blacklisting methods. If organization is interested in mitigating phishing attacks, they have to use techniques that help them to tell the difference. For example, many companies pay security firms to look for potential phish-

ing websites in the market: "Security companies usually carry out Internet search, chat room monitoring, or domain name registration checks to see if anyone newly registers a website or owns a website with similar domain name. They compare the visual similarity of those newly found websites with their customers' websites, and if they find one website they ask the ISP to shut down the website or notify all customers to watch out for it [21]".

## 2.2 Email scanning

Second option to mitigate phishing attacks can be executed by the organization's itself: filtering malicious e-mails. Anti-spam filter has proved to work efficiently and is recommended mitigation component [21], but one needs to critically ask: how successful are the filters, and to what extent can we rely on them? Spam-filtering and spammer tricks are separate topic, and this thesis hereby gives a brief overview of it. Techniques used by spammers to bypass the filter are as follows:

- Use of botnets. TechTarget: "A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet [77]."
- Hiding text. There are numerous ways to trick a spam filter not to recognize bad words, or to show good words to spam filter and in same time not to human eye.
  - ◊ Take a suspicious word like Viagra and space it out - V I A G R A [43];
  - ◊ Splitting words with HTML comments. For example, the HTML:  
Fr<!-- 63 -->ee mor<!-- adf -->tgage fin<!-- sdf -->anci<!-- e -->ng  
would be rendered as: Free mortgage financing [42];
  - ◊ Word salad. IT News Africa: "Spam filters evaluate the words in an e-mail message and group them into 'good' and 'bad' words – bad ones being the ones typically found in spam e-mails. The term 'word salad' refers to the spammer's trick, whereby extra 'good' words are added to an e-mail message (those typically not associated with spam). The spam filter will pick up more good words than bad words, and decide that the message is 'good' [41]." To hide 'good' words from e-mail which are not associated with the message, spammers are using HTML font tags to have same color code both for text and background [42];

- ◇ Dyslexia. *"A popular optical illusion demonstrates that as long as the first and last letters of a word are in the correct place, the remaining letters can be used randomly and the word can still be recognized [42]."* Some examples are:
  - "FWREE HRBAL VGRAIA SAMPULS"
  - "Nekad scoohlgurl photos!!" [42];
- ◇ Encoding. Some spammers encode their message text, hoping that the anti-spam filter is not smart enough to decode messages before filtering them. In addition to encoding the message text itself, some spammers use HTML entity encodings to hide each individual character of their message. For example, the HTML encoding `&#70;&#82;&#69;&#69;` would be rendered as FREE in an HTML-enabled e-mail client [42];
- ◇ Securelist: *"In Q1 2015 spammers exploited another technique, deliberately distorting spammer site addresses by writing them separately or adding extra characters. At the same time the message text always contained the name of a second-level domain where the spammer site is hosted, as well as instructions about how to use it with the domain zone: for example, "remove all the extra characters, and copy to the address bar" or "enter in the address bar without spaces". In fact, the addressee of the e-mail is encouraged to create the address of spam site of his own and enter it in the address bar [78]";*
- Obscuring URLs. This means getting the IP address of the web site, then converting it to a single decimal number using the following formula:  $(X3 * 256^3) + (X2 * 256^2) + (X1 * 256) + X0$ , where IP address is X3.X2.X1.X0 [43];
- Valid DNS records.
  - ◇ Phishing Frenzy: *"MX record is a type of resource record in the DNS that specifies a mail server responsible for accepting e-mail 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 e-mail should be routed with the Simple Mail Transfer Protocol (SMTP) [79]";*
  - ◇ The Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery. SPF validates which mail server is used to send mail from the domain. Technology needs two sides to cooperate with each other [80];

1. Owner of the domain specifies allowed mail server which can send e-mails on behalf of their domain.
  2. Receiving server can check is the received message sent from valid mail servers;
- ◇ is designed to detect e-mail spoofing by providing mechanism that incoming e-mail is coming from a domain which is authorized by their administrator. Authorization is done by checking public key in DNS [81];
  - ◇ DMARC is the next step to prevent domain from spoofing emails - "*Implementing DMARC (Domain-based Message Authentication Reporting and Conformance) is the best way to defend your customers, your brand, and your employees from phishing and spoofing attacks* [82]." A DMARC policy enables sender to point out to receiver what to do if DKIM and/or SPF authentication fails [83]. In addition, DMARC gives an option to receive aggregate and forensic reports. Aggregate report gives overall visibility into the health of domain's email program by helping to identify authentication issues [84]. Forensic report is generated almost immediately if DMARC authentication failure is detected. In the forensic reports, "To" and "From" email addresses, IP address of sender, subject line, message header and any URLs in the email are included [85].
- Using third party SMTP servers
    - ◇ For small scale spamming, it is possible to use SMTP servers provided by free webmail service providers - for example Gmail, Yahoo, Yandex and AOL. When using free e-mail service providers, spammers are taking into consideration rate limits provided by companies. As the rate limits are constantly changing and it also depends on users' reputation, there is no one answer how many e-mails per minute/hour/day spammers can send, but it will vary around 100 e-mail per hour and 200-500 e-mails per day [86].  
Simple trick how spammer can slowly send e-mails by not exceeding rate limits, is to install SMTP server, like Postfix, and set rate limits. Technique is simple and it can be used only for small-scale attacks;
    - ◇ Using SMTP service providers. For example sending 1 000 000 unique e-mails will cost 200\$ [8]. Example price list can be found in Appendix 1;
    - ◇ Using open relays. Indiana University's Knowledge Base: "*A computer that functions as an open mail relay can pass along e-mail from anywhere to*

anywhere else, including messages that are neither from nor destined for its own users. Open relays occurs because of misconfiguration or because some mail servers allow it by default" [87];

- According to Kaspersky Spam Report, in third quarter in 2015, a new way was identified to distribute phishing e-mails and bypass spam filters : "*The text of the phishing e-mail and the fake link were included in a PDF document attached to the e-mail. After clicking the link, a standard phishing page opened and the user was asked to enter his personal information.*" However, detailed text in the message body provided genuine links to official bank resources [88]. Real-world example how the following technique was used can be found on Figure 3 and Figure 4.

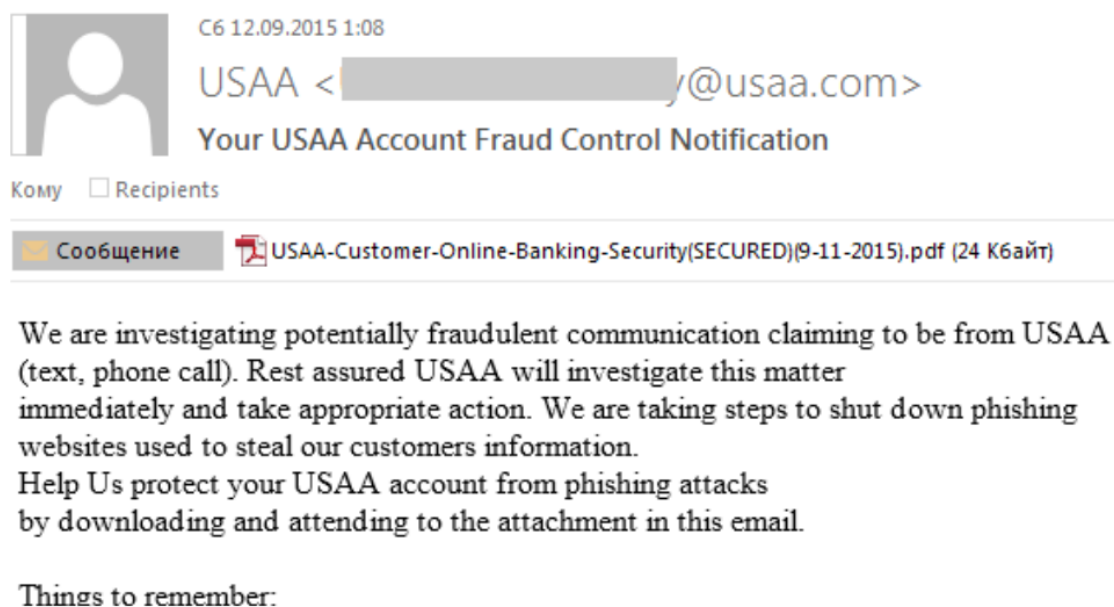


Figure 3. Spammer tricks Q3 2015  
[88]

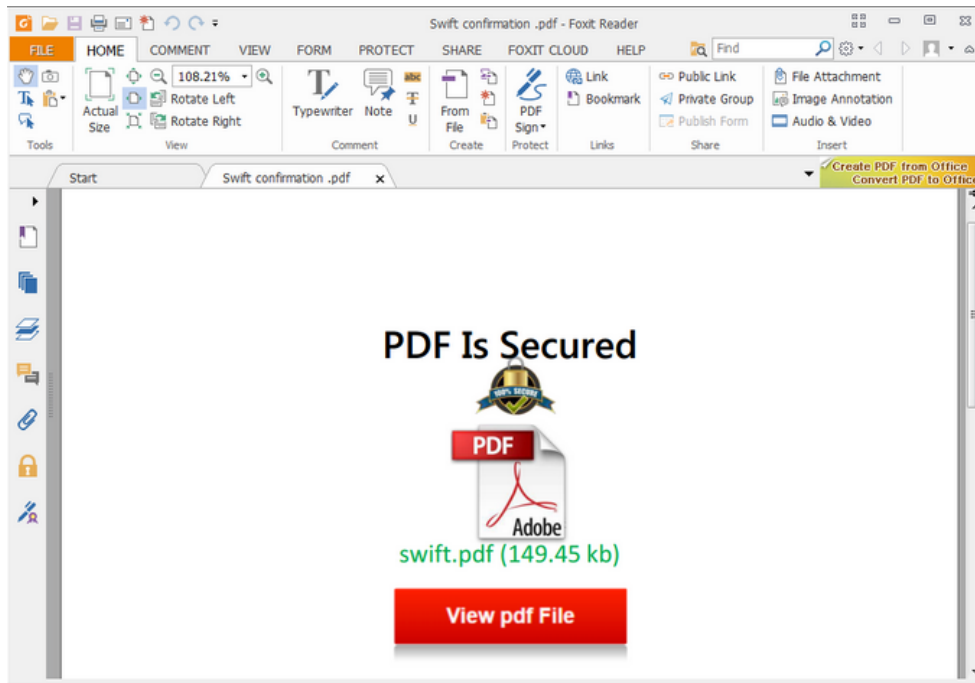


Figure 4. A phishing trampoline – embedding redirects in PDF documents [89]

Previously some of the spammer tricks to bypass the filters were mentioned, but how well do these work? To swiftly illustrate their effectiveness, one suggest to take a look at the following, summarized by Cyveillance on Figure 5.

<b>Spam emails sent</b>	<b>5,000,000</b>
<b>Percent filtered by spam filters</b>	<b>90%</b>
<b>Percent of people who get the email that will eventually open the email</b>	<b>50%</b>
<b>Percentage of those who will read the email and click on the link to the attack web page</b>	<b>10%</b>
<b>Of those who clicked on the link, percent that fall for the attack</b>	<b>10%</b>
<b>Total number of people successfully phished</b>	<b>2,500</b>

Figure 5. Who will eventually click [1]



Verizon concluded in its 2015 Data Breach Report [15], that 23 percent of recipients of phishing e-mails open them. To make matters worse, 11 percent not only open the mails, but also click on the malicious attachments [90].

Although the statistical numbers provided by Cyveillance and Verizon differ to some extent, it is certain that anti-spam protection is a must-have and has proved to help, but extra steps are needed to mitigate phishing attacks.

### 2.3 Client based anti-phishing tools

Phishing usually starts either from e-mail, chat room, social media or messengers. If phishing e-mail has passed all the previous technical countermeasures, last option is to use client based anti-phishing tools. Alert about potential phishing attack can be showed and mitigated by e-mail client, web browser or by anti-phishing toolbars.

#### 2.3.1 E-mail client based mitigation

Some e-mail clients, like Microsoft Outlook, have a built-in phishing protection feature. Positive side is that it can easily be activated [44] and as seen on Figure 6, it is using active notification - one cannot open the link unless one does not read the notification and choose react accordingly. Negative side is that employees or administrators can just turn it off or on, but cannot configure sensitivity of the setting [44].

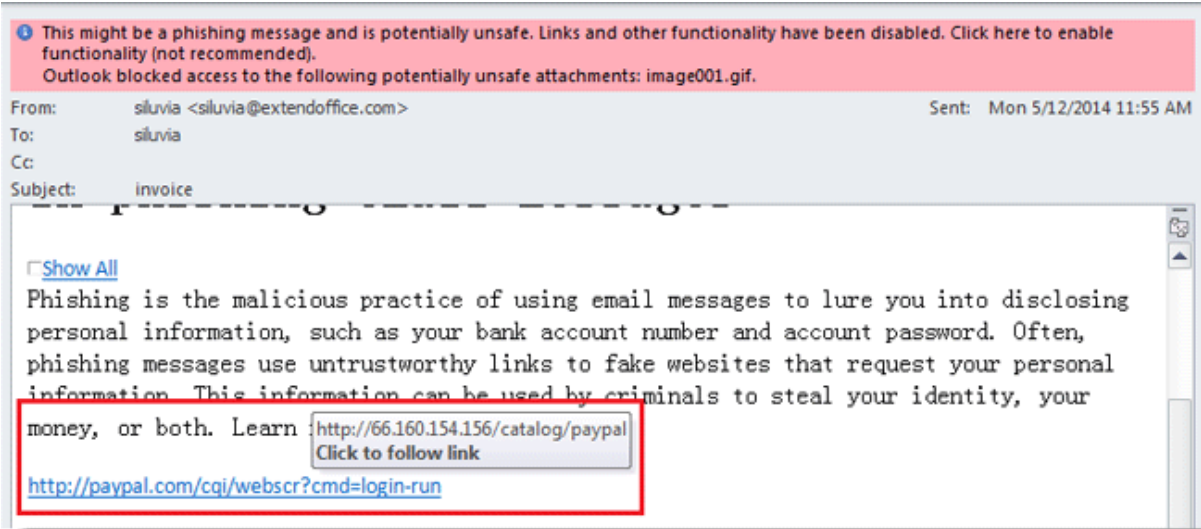


Figure 6. Outlook warning [2]

### 2.3.2 Browser based mitigation

To mitigate a phishing attack, browsers are using blacklists. According to J. Hong's research, the best-known anti-phishing blacklists are operated by Google, Microsoft, and PhishTank, each containing URLs manually verified as phish. Google's is integrated with Firefox and Chrome and Microsoft's is integrated with Internet Explorer [91]. If a potential phishing website is detected, a splash screen, like on Figure 7, will appear.



Figure 7. Google Chrome warning about potential phishing website [3]

MozillaZine, which provides Mozilla product documentation written by the user community, confirms it by stating the following in their knowledge base: "*Mozilla applications offer some protection against such websites since Firefox 2.0 (malware protection since 3.0) and SeaMonkey 2.18. If the feature is enabled, a list of domains which have been reported as being malicious is downloaded in regular intervals. The address (URL) of each website the user is about to visit is compared against these lists and a warning issued before the content of that website is actually loaded. In this way, the user has the opportunity to cancel the loading process before any potential harm is done.*" [92]

Although browser based mitigation can sometimes be useful, there are some concerns:

- It takes time to blacklist a malicious site, and as mentioned in chapter "Taking down phishing website", phishing makes most of the damage inside first 24 hours
- Browser accuracy. To measure browsers' accuracy, AV-Comparatives e.V. made a test with five browsers using their default settings. The purpose of this test

was to evaluate anti-phishing protection provided by web browsers on December 2012. In total, 294 active phishing URLs were used for this test [93]. Results of the test with used browsers and their versions can be found on Table 1.

Table 1. Browsers' phishing websites URL blocking ratio

	<b>Browser</b>	<b>Version</b>	<b>Blocking ratio</b>
	Apple Safari	5.1.7.7534.57.2	65.6%
[93]	Google Chrome	23.0.1271.97	72.4%
	Microsoft Internet Explorer	9.0.9112.16421 / 9.0.12	82.0%
	Mozilla Firefox	17.0.1	54.8%
	Opera	12.11.1661	94.2%

- How do employees react to warnings? Warning messages are not 100% accurate and if an organization chooses to trust the warnings, a considerable extra burden will affect IT team managing the access lists. Another approach is that the organization chooses to trust their personnel and is convinced that they will act as needed.

Various studies have focused on determining the effectiveness of browser warnings. Most studies conclude that internet users mostly ignore browser warnings for a variety of reasons. Study with 60 participants in a lab environment found that 21% of the participants clicked through an active warning message whereas 90% of the participants clicked through passive warnings [46]. As described in "The state of phishing attack": *"Passive indicator warns against potential dangers without interrupting the user's task. In contrast, active indicators force users to notice the warnings by interrupting them"* [91].

Various studies have looked into reasons behind users' ignorance of browser warning messages. Most common reasons are following: user's inability to understand the message due to its esoteric nature [94]; trust in 'protective technologies' like anti-virus software; and depending on operating system and browser, confusion between different types of warning messages [95]. Also, users get used of frequent warning messages, and slowly start to ignore them [96, 45].

Sharma gives a good overview regarding displaying warning messages and users' reaction to that: *"In a study focused on improving Google Chromes SSL warning effectiveness, Felt incorporated Mozilla Firefox SSL warning design in the Chrome browser [97]. This study was based on the results from a previous study [98] where it was found that Google Chrome SSL warning was ignored by over 70% of the*

users who encountered them. In comparison, Firefox SSL warning was ignored by just 33% of the users who encountered them. On redesigning the Chrome warning to a 'Mock Firefox' design, the CTR was seen to go down to 56%, which is still a very high number of users ignoring the SSL warning" [45].

Addition to browser warning studies, Akhawe and Felt [98] found in their that about 9% of Firefox users and 18% of Chrome users ignore the phishing warning to proceed to the spoof website and could potentially disclose confidential information [45]. "Interface design elements for anti-phishing systems" concludes that future work focusing on warning and interface design is essential [99].

### 2.3.3 Anti-phishing toolbars

A study that analyses 23 anti-phishing tools using techniques, such as password management, heuristic, whitelists, blacklists, user ratings, SPF, Open Phishing Database, spell checking, SSL verification and steganography concludes that although the tools studied here help the users to avoid becoming victims of phishing to some extent, there is a need for much more effective methods to successfully and comprehensively protect the users against phishing [22].

Similar studies have previously been conducted in 2006 and 2007 where the message has been the same: anti-phishing toolbars are deficient against phishing attacks [100, 20] and as the human is the weakest [11, 101] link in information security, better user education is needed [102, 101, 103].

### 2.3.4 Password management

S.Purkait writes in his literature review: "*Most users have multiple passwords protecting their accounts over the Internet. In order to avoid the headache of remembering and managing a long list of different unrelated passwords, most users simply use the same password for multiple accounts. A phisher can effectively steal users' passwords for high-security servers, such as an online banking web site by setting up a malicious server or breaking into a low-security server, such as a high-school alumni web site*" [101]. In order to avoid such a incidents, password managers could be used. From the past ten years, there have been several studies on how password management can mitigate phishing attacks.

- Web Wallet. To submit sensitive information, research paper "Web Wallet: Preventing Phishing Attacks by Revealing User Intentions" suggests to use their browser sidebar. Web Wallet detects if current and intended site does not match.

Detection is based by security questions which cannot be missed by user. During the study, Web Wallet decreased spoofed rate from 63% to 7% [104].

- AntiPhish. "*A browser extension that aims to protect inexperienced users against spoofed web site-based phishing attacks. AntiPhish keeps track of the sensitive information of a user and generates warnings whenever sensitive information is typed into a form on a web site that is considered untrusted* [105]." They way how AntiPhish makes difference between legitimate and illegitimate websites, is that it stores mapping between the legitimate website and user credentials [105].
- Passpet is a tool that uses multiple techniques to mitigate phishing attack. It uses site labels to identify legitimate sites and password strengthening functionality to defend against dictionary attacks. In addition, it is using hashed master password to store different user credentials [106].
- Password manager LastPass, which is stating in their webpage: "*LastPass simplifies your online life by remembering your passwords for you. With LastPass to manage your logins, it's easy to have a strong, unique password for every online account and improve your online security* [107]." Although LastPass is a recommended tool for password management, there is still important downside - it is possible to protect password's manager's vault only by password and the data is located in the cloud. In the security notice by LastPass, they announced that hackers got into their network and data breach occurred [108]. Hackers most probably got users' e-mail addresses, password hints, and a representation of passwords. Officially they got nothing more than authentication data, whereas passwords were salted, hashed and stretched, and only ever stored in that scrambled, irreversible form [109].

In conclusion, not only technical mitigation solutions are enough. In client-based solutions, eventually employees need to take the decision whether to ignore the warning and proceed to website or not to visit it. In order for the employee to act as expected by organizations', employees need to be aware of the phishing attacks, be able to identify them, and know how to act.

## 2.4 Authentication

Two-factor and multi-channel authentication. Usually in web services, users are authenticated by username and password, if hacker gets the credentials, account is compromised. To make it more difficult to hack an account, two-factor authentication is

recommended. In two-factor authentication process, user should prove “something a person knows”, “something a person has” or "something you are". Here, "something a person knows" is a password, "something a person has" is a hardware token, and "something you are" is based on physical attribute [110].

According to article "An empirical study of the effect of perceived risk upon intention to use online applications", main problem for two-factor authentication(2FA) is added complexity. Most users do not adopt security processes which are too difficult or time consuming, and organization does not want to stress their employees [111]. In addition, research paper "On the (In)Security of Mobile Two-Factor Authentication" concluded that poorly implemented 2FA scheme offers various ways to bypass secondary authentication token and hackers can intercept the One-Time Password (OTP) transmission or steal private key material for OTP [112].

Figure 8 is a real life example how attackers are trying to get the authentication keys.

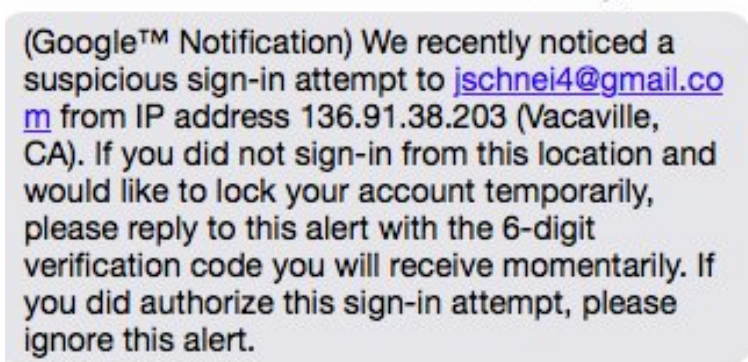


Figure 8. Attacking two-factor authentication [4]

Even though there are weaknesses on 2FA, it is a recommended way to protect customers' credentials. Apple: "*Because your password alone is no longer enough to access your account, two-factor authentication dramatically improves the security of your Apple ID and all the personal information you store with Apple* [113]." According to statista.com [114], we have around 2.1 billion smartphone users in the world [114] and apps like Google Authenticator and Authy are one of the possible solutions. Although for customers, mentioned apps are for free, and there are manuals for web developers available [115], two-factor authentication is still not very widely used. According to APWG survey [40], 54% of all the phishing attacks impersonated Apple, PayPal, and Taobao.com [40]. Apple and Paypal have two-factor authentication enabled, as Taobao.com has no English web site, it is not possible to know their authentication options. But as Apple and Paypal already have free two-factor authentication enabled

and they are still the most impersonated companies, it is clear, that for protecting big masses, this is not enough to mitigate phishing attacks.

## 2.5 Statistical curve from past to nowadays

Important figures to understand whether anti-phishing tools are working or not, is to analyze statistics from past to nowadays. Number of phishing attacks, number of phishing websites and cost of phishing attack will be discussed.

RSA showed that between 2010-2013 the number of phishing attacks increased from 100,000 to 400,000 [16]. Table 2 is a summary of APWG reports, where increasing trend of phishing attacks can be seen[116].

Table 2. Phishing attack trend report

	<b>Topic</b>	<b>Year</b>	<b>Value</b>
	Number of unique phishing reports received	2015	1,423,000
	Number of unique phishing sites received	2015	788,000
[116]	Number of unique phishing reports received	2013	448,000
	Number of unique phishing sites received	2013	512,000
	Number of unique phishing reports received	2008	335,000
	Number of unique phishing sites received	2008	278,000

### 3 Measuring personnel cyber security awareness level

Chapter 1 proved that social-engineering has a major part in cyber security attacks and as phishing plays important role in social-engineering attacks, it may be good idea to measure resistance against social-engineering attacks through phishing assessment. Chapter 2 shows that relying on technical solutions is not enough, and because of that, it is important to identify vulnerable users.

Chapter 1 analyzed four options to measure personnel vulnerability to social-engineering attacks: Metric Matrix, Human Risk Survey, Human Metrics: Measuring Behavior and Effective Phishing of Employees [25]. the analysis suggest that Effective Phishing of Employees is the model most suitable to reach the aim of the thesis. The following chapter analyzes the difference between education and awareness, and the reason why persons with outstanding technical skills can be victims of a phishing attack.

#### 3.1 Questions about knowledge or something else?

Regarding phishing, the cat and mouse game between security companies and hackers has been going on for 20 years. According to Internet records, the first time that the term “phishing” was used and recorded was on January 2, 1996 when America Online (AOL) was phished. The incident was mentioned in a Usenet newsgroup called alt.online-service.america-online [117]. Starting from the first phishing campaigns, technical solutions regarding attacks and defense have been in constant change, but what has not changed is the idea behind phish and ways how end-user can detect it. Kevin Mitnick: *"the only thing that's changed in regards to vulnerability are technical issues, but with social engineering, it's all remained the same. So, it depends how vigilant the owners and the operators of the computer systems and the network are [9]."*

As the way how the end-user can detect malicious e-mail has not changed, and as human is frequently stated as the weakest link, it could be a good idea to mitigate phishing attacks by raising personnel cyber security awareness level [118]. National Security Agency states that: *"all the past two year high-profile incidents you've read about in the Washington Post and New York Times, all of these attacks were conducted using simple methods, including spear phishing schemes or USB drive delivery, not through zero days [119]."* In addition, researchers at the Friedrich-Alexander University sent out 1700 emails and Facebook messages to their students where even though they claimed to be technically savvy, 56% of e-mail recipients and about 40% of Facebook users clicked the phishing link [120].

However, first one may need to ask: what has instructors and information specialist



done wrong, so that human is still referred to as the weakest link? Report by the University of Oxford's Global Cyber Security Capability Centre [121] shows that simply lecturing people about the risks of not changing their passwords is not enough. Many people know that there are risks, but are still not doing enough to prevent them [122]. In addition, *"there is a basic lack of understanding in industry as to what security awareness actually is. There is a major difference between security awareness programs and security training. Training is about providing a set body of knowledge and typically tests for short-term comprehension. Watching the standard "awareness" video is an example of such training. The primary purpose of security awareness is to change behavior [49]."*

Various publications are pointing out that only theoretical education is not enough, in addition to identifying the phishing attack, people need to know how to respond. Thesis "Fighting phishing at the user interface" shows that, users fail to consistently check the browser's security indicators, because maintaining security is not the user's primary goal [20]. One way to solve the problem is to show pop-up warnings which cannot be missed. However, it has also been found that pop-up confirmations, used indiscriminately, become less effective over time: the more often they appear, the less often users heed them [123]. In addition, bounded attention is one of the most common reasons why people are victims of phishing attack [28]. Next chapters analyze in more detail that why the employees who know how to identify a phishing attack and how to act after that, can still be victims of phishing attacks.

## **3.2 Decision-making factors**

Even if an employee has a high cyber security awareness level and is willing to cooperate with the IT department, sometimes it is still not enough to avoid successful phishing attack. Hunger, stress, lack of sleep and attack timing are some of the reasons why employee makes wrong decisions and becomes victim of a phishing attack. The interviews with area specialists have revealed that even if one knows how to detect the attack, one can still be victim of phishing attack.

### **3.2.1 Hunger**

Study proves that empty stomach influences human and animals decision making - the more hungrier they are, the more riskier decisions they make [51]. Same conclusion is found by other studies [50]. Hadnagy comments in his book: *"This makes sense from a survival perspective, because deep down, hunger is a threat and when survival*

*mechanisms are hardwired, we respond to hunger by starting to make riskier decisions [33]."*

### **3.2.2 Lack of sleep**

Riskier decisions are also likely to be made already when a person is suffering from only as little as one night's of lack of sleep. Reason behind this is that, we are tired, we overestimate our ability of taking right decisions [30]. Casinos have used the same concept for a long time, by not having too many clocks in the room, no windows, a lot of light and cheap alcohol, all these factors facilitate casino visitors' bad decisions that overestimate their chances of winning [33].

### **3.2.3 Stress**

Several studies demonstrate a strong connection between stress level and decision-making. Research by Keinan and Giora (1987) shows that people under stress do not consider all the possible solutions and may make irrational decisions. This sort of behavior is called singular evaluation approach. It mostly means that people take the first solution without comparing it with other solutions [124]. Another problem is that people under stress do not ask right questions and rely on familiar patterns [125]. In addition, employees under stress are more easily distracted, thus, the probability of making harmful mistakes is bigger [52, 53].

### **3.2.4 External factors**

Researchers have found that external factors, like light and temperature, are some of the factors that can impact our feelings about the situation. For example, a paper by Kang reveals that a brief warm or cold feeling results in different decisions in the trust game [54]. Same findings were summarized by Williams and Bargh [126]. In addition, studies show that extreme heat is associated with anger and it is changing decision-making [127, 128].

## **3.3 Personality factors**

Arkansas and Louisiana universities studied the "Big-Five" personality traits and their connections to becoming victim of a phishing attack. The five personality domains are: Openness, Extraversion, Agreeableness, Neuroticism and Conscientiousness [32].

- Openness: the person tends to be transparent and free, values cooperative management, decision-making rather than a central authority [129];
- Extraversion: the person has energy, positive emotions, sociability and seeks the company of others [130];
- Neuroticism is characterized as anxiety, fear, moodiness, worry, envy, frustration, jealousy, and a tendency of loneliness [129];
- Agreeableness is characterized as being kind, sympathetic, cooperative, warm and considerate [129];
- Conscientiousness: the person tends to be neat and systematic, careful and thorough [129];

Research shows that the people who are agreeable and inclined towards extraversion, are possessing a high rate of security risk. Conscientious people are more mature and are good at following the rules and standards [131]. Several phishing assessments have shown that young users and women are more vulnerable [132, 133]. Young users are known to be agreeable [134], whereas women tend to be more agreeable than male, which explains why younger employees [75] and women are more likely to become victims of phishing attack [135].

### 3.4 Following the rules

It can be often the case that if an employee spots a threat, he/she does not report it. In order to mitigate the attack, it is important to report it - usually to IT helpdesk or to Chief Information Officer. Although reporting malicious e-mails is usually employees' duty, many of them are still not doing it.

Within the organization, the incident handling procedure can include the following: Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity [136]. The same logic is followed by SANS Institute's Incident Handler's Handbook: Incident handling procedure is Preparation, Identification; Containment, Eradication, Recovery and Lessons Learned [137]. From the point of view of human vulnerability, Preparation and Detection can be solved and measured by conducting quizzes or lab tests - it is a question of education. Using phishing assessments, it is possible to go even more further by measuring who will help to mitigate attack in phase 3 (Containment) by identifying the ones who will report.

The importance of employees who tend to report possible attacks is emphasized by Hadnagy who recommends to use various statistics: Number of people who reported the phish; Number of people who clicked and did not report; Number of people who clicked and did report; Number of people who did click and did not report; and Number of people who did not click and did report [33]. Article by Ronald C. Dodge and Curtis A. Carver shows the difference by Figure 9 about the users who will report the attack - 52% of freshmen got phished and only 8% of students reported about the phishing e-mail. But from seniors, 18% of students failed and 69% made a report [5].

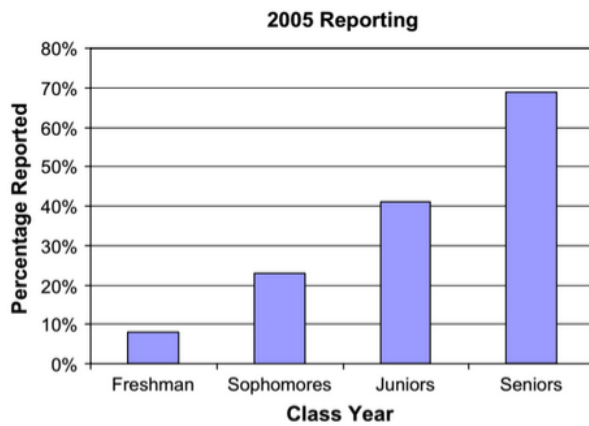


Figure 9. Percentage reported [5]

## 4 Preparing for phishing assessment

As we have aware that anti-phishing tools are not providing enough protection and persons with high technical skills can be victims of phishing attacks, it is vital to measure personnel cyber security awareness level through a phishing assessment. Studies show that due to privacy, security and ethical issues [57], there is a shortage of research concerning penetration tests to examine people's susceptibility to phishing, plus assessments need to be conducted in care [121]. The following chapter focuses on these details and shows how to overcome these problems, as well as to be prepared for a phishing assessment.

### 4.1 Categorization of phishing e-mails

Phishing Dark Waters: "Even if you get nothing else from this book, please pay attention to this section, as it is the crux of our program". Christopher Hadnagy and Michele Fincher have analyzed real phishing e-mails and according to the difficulty of identifying phishing e-mail, they categorized them to level 1, 2, 3, or 4 attacks [33]. The appropriate level needs to be chosen according to organization's purpose and personnel training - there is no need to test uneducated employees with the most difficult e-mails, or to conduct simplest assessment every quarter for many years.

#### 4.1.1 Level one phish

Level one is the simplest to recognize. The list of indicators to identify phishing e-mails is the following [33]:

- Impersonal greeting and closing;
- Misspelling/poor grammar;
- Simple message/unlikely pretext(for example "you've inherited millions");
- Exploit of sense of greed, fear, or curiosity;
- Bad links in body;
- Bad or unknown sender;

For example, the content of level one can be: "Please pay the invoice inside 48 hours, otherwise fine will be applied", or "You have won money, please contact us for the transfer."

Level one phish mostly works because of the fear of potential loss and greed outweighing the logic [33].

#### **4.1.2 Level two phish**

Level two phish is similar to level one, but it is slightly harder to detect. Mostly it has the following characteristic [33]:

- Impersonal greeting and closing;
- Bad links in body;
- Good spelling with some bad grammar;
- Message more complex but still primitive;
- Exploit of sense of greed, fear, or curiosity;
- Bad or unknown sender;

Content of level two phish could be: "The result of your exams are available, please click login and view the results" or "This automated response has been delivered today to inform you that someone just ran background-scan on you. [33]"

The main reason why similar attacks are more successful is that one is interested to click the link or open the attachment.

#### **4.1.3 Level three phish**

Difficult to catch, and is close to spear-phishing attack. Indicators for level three phish are the following [33]:

- Personalized greeting and closing;
- Spelled properly;
- Generally good grammar;
- Complex message that appeals to sense of fear or curiosity;
- Bad links in body;
- Sometimes a bad origin e-mail address, but sender can appear legitimate;
- Branding;

The most important is that it looks and feels like a real e-mail. Even professionals cannot always catch the level three phish [33].

#### 4.1.4 Level four phish, or spear-phishing

The most difficult phish to detect, advanced, personal, and successful. Level four phishes like RSA hack in 2011 [6], Sony [138], and shut down of Ukraine power plant [139], are frequently the key element for major breaches.

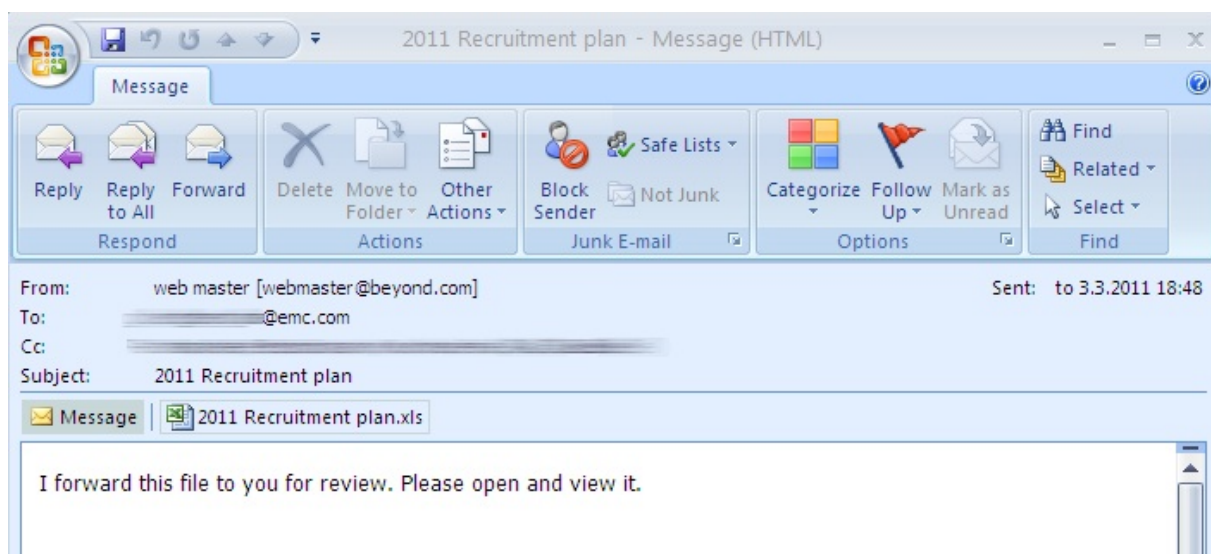


Figure 10. RSA phishing e-mail [6]

As seen on Figure 10, RSA spear-phishing e-mail looks really simple, but the reason why it is so difficult to detect it, lies in the message. Employees are working to receive, open and work with e-mails which can be categorized as level four phish. Phishing Dark Waters: "In many cases, the spear phish is more about the open-source intelligence portion of the attack than the e-mail portion [33]."

## 4.2 Choosing e-mail difficulty for assessments

To meet the aim of this thesis, two assessments with different difficulty levels were conducted. Purpose of the first test was to be as simple as possible - both to employees and to organizations by not any mimicking well-known company and by having clear hints suggesting that it is of potential phishing e-mail. Similar approach can be used if researchers or CIOs do not get the approval to mimic desired company, but still see the phishing assessment as is vital to measure personnel cyber security awareness level. First assessment can be categorized as level 1 phish.

The purpose of the second assessment is to make the decision-making more difficult for employees and planners. In the campaign conducted in the framework of this thesis, the impersonated organization was one of the Estonian ministries. Several options to mimic the Ministry were used:

- Correct domain name consists of almost 20 letters, for the assessment, only one letter was added in the middle of the name;
- In the e-mail that which was sent to participants, a link was visualized that appeared to lead to the Ministry's document handling system;
- The e-mail was sent out from an e-mail address using a similar name to someone who worked for the Ministry a few years ago;
- The e-mail signature was authentic.

After a successful first assessment, second organization was added to the campaign. As the level of difficulty of second e-mail was higher, it was difficult to find a compromise between the organizations for choosing category of the campaign. One of the differences between the organizations was the age of the employees. As according to previous research, personnel close to retirement period is more likely victim of phishing attack, organization who had older employees wanted to have an easier campaign. CIO's opinion was, that it is not rational to send the e-mail if it is already known that a high percentage of employees would be fail the phishing assessment. Eventually, the text was modified to be not as official as a real one could be, and an additional element (fast reaction) from level 1 phish was added. Having a higher rate of victims during assessment has a positive side - by showing potential threats to organization's board members, it can be used as one of the key elements for the following year's budget or personnel planning.

In order to impersonate well-known and high-level organizations, it is important to understand that this kind of assessment gives similar results to a real world attack and in order to conduct the campaign, corresponding approvals are needed.

### **4.3 Approvals for assessment**

In 2015, a phishing assessment was conducted in Estonia by an organization's CIOs, where web server service provider, CERT EE and the impersonated company got an alarm about a phishing attack. Soon after the alarm, it was clear that an uncoordinated phishing assessment was being carried out. In order not to have the same scenario where



management, cooperation partners, employees and other entities tied with assessment are angry about the test, approval from different entities needs to be obtained.

Even though it is well-known to organizations' board members that phishing is dangerous, and needs to be tested, sometimes conducting a test in real-life environment is still not possible. During the research for this thesis, two main reasons why it cannot be done were detected.

1. It is unethical.
2. A company has worked many years to guarantee that personnel trusts IT systems. As employees do not understand how easy it is to send impersonated e-mails, they would doubt the effectiveness of the IT department and their systems.

Thus, in order to conduct a phishing assessment and to avoid organizational problems, following issues needs to be considered:

- During the human metrics presentation by SANS Institute Training Director Lance Spitzner, one of the most common questions was: "how to get management approval for human assessment?" According to Spitzner, the first step is getting senior leadership's support for human assessments, mainly demonstrating their value. It can be achieved by showing them statistical numbers and damage done through phishing attacks. Addition, one could conduct a pilot test for a limited number of employees. As on average, 30%-60% will fail the test in non-trained environment, it should get the management's attention. After one has the management's support, depending on the organization, one may need to get additional approvals from other groups, like Human Resources and Legal [140];
- The employees need to be educated as to how to spot and how to act if a phishing attack has occurred. If CIO test's personnel awareness level without educating them, people are likely to be unhappy about the test and vital cooperation between information officers and employees could suffer;
- One should sign an NDA contract with the company whose personnel will be assessed;
- One needs to get an approval from the impersonated company. In the previously mentioned test in 2015, it was not done. As a result, the impersonated company's helpdesk got many phone calls which were escalated to higher level, and some participants even visited the impersonated company. To show different options how the approval part can be played out, two phishing assessments were done for the thesis. The first one did not impersonate any company, whereas the second

impersonated one of the ministries in Estonia with permission to use similar domain name, their logo in the e-mail and to impersonate a real person. Getting approval from high-level organizations takes time - for instance, regarding the second assessment, it took one and half months (with good connections) to get the approval;

- While setting up the phishing assessment, one needs to add your contact information to test e-mails and website, as described in Appendix 3;
- One should get an approval from the owner of the infrastructure and organizations dealing with cyber incidents. As all the entities, like infrastructure owner, assessed organizations, impersonated Ministry, CA where domains were registered, who were involved with two phishing assessment campaigns were Estonian entities, CERT EE and the branch dealing with infrastructure cyber incidents were informed.

Message to the entities dealing with incidents described the attack with following bullet points:

- ◊ Information about the date, who is conducting the test and which organizations' employees will be tested;
  - ◊ Goal of the assessment - to measure personnel awareness level, to measure if the training has been good enough to mitigate social-engineering attacks, and to measure which employees are following organization's cyber security policy;
  - ◊ Description of the assessment - from which address the e-mails are sent out, original message of the e-mail, screenshot of the landing page, and IP of assessment server;
  - ◊ Technical description;
  - ◊ Information about approvals which have already been received;
- One needs to secure the phishing server and DNS. If one's landing web page is working on HTTP, only port 80 needs to be left open. The phishing web server needs to be accessed only via HTTPS and SSH and these ports need to be available only from internal network. If one has approval to use similar domain name to the one that the well-known company has, one needs to secure it by restricting e-mail sending from certain IP addresses. It can be solved by using SPF and/or DKIM records.

## 4.4 Ethical considerations

Some of the organizations are not conducting phishing assessment because they are considered to be unethical, but as phishing assessment is the most recommended way to measure personnel awareness level, it is important understand the sensitive issue, and to find a workaround. Ph.D. thesis by Mariam Khalid AL-Hamar has stated: "*There were also major difficulties in getting authority from organisations for holding a penetration test for phishing for ethical, security and privacy reasons. Even when authority was granted, the collaborating organisation still required full control over the test to ensure its privacy. However, giving the authority to do such a test was a significant concession on the part of the organisation* [141]."

The phishing assessment has to be accurate and measurable [23], plus ethical. An ethical experiment does not expose participants to any risk and does not imply them being offended. As it is important to have accurate test results, the assessment needs to be as close to real attack as possible. In order not to put participants at risk after revealing the password, Jakobsson and Ratkiewicz did not save the passwords to fake eBay website [73].

A Culture of Trust Threatens Security and Privacy in Qatar conducted two phishing assessments. During the tests, they solved three ethical problems [57].

- One test asked private information from company employees. Due to the confidentiality, IT team used an e-mail address unknown to either the employees or the researchers;
- To avoid problems from e-mail service provider, only 150 e-mails were sent out;
- All participants were identified that all of them were over 12 years old;

Another experiment, where students were tested ended with harsh feedback from students, and some of the students complained that the phishing assessment was unethical, illegal, inappropriate, unprofessional and useless. Some participants even wanted the researchers to be fired and prosecuted. The reason why there was such harsh feedback is that the researchers sent e-mails on behalf of other students whose names were gathered from social media networks [56].

In the research done by West Point Academy, no ethical issues were identified, even though the assessment was carried out three weeks before the start of the busiest period for the students. Timing was intentionally selected because, before the exam period, students are specially interested in opening e-mails about their grades and exam notifications [142].

During the two assessment campaigns conducted for the thesis, ethical issues were solved by not sending offensive e-mails and by using immediate feedback about phishing attack on the landing page, landing pages are brought up in Figure 14 and Figure 16. In addition to solving ethical issues, having an immediate response on the landing page, has extra benefit with good training material which is the reason why this approach is often referred as "embedded training [143, 91]." When designing the landing page with immediate response, one needs to keep in mind that it has to be simple and instantly understandable. According to an article by Caputo, employees have to understand the feedback page within 20 seconds [144].

## 4.5 Legal considerations

With regards to phishing assessments, researchers and organizations' CIOs need to understand possible legal issues. Researchers may need to intentionally violate a number of laws, by following the norms in their scientific community [145]. A badly designed research project may lead to a situation where participants want the researcher to be prosecuted [56]. Some researchers have been sued by the U.S. government, for example Michael Lynn in 2005 by presenting a flaw in Cisco's router at the BlackHat security conference [60]; Dimitri Skylarov who was arrested minutes after his presentation about Adobe's e-book encryption software [59]; in 1996, cryptographer Phil Zimmerman was investigated for three years for spreading his Pretty Good Privacy(PGP) tool beyond American borders [61]; and in 1993 professor Dan Bernstein had to argue with the U.S. for six years to publish encryption source code [58].

When conducting a phishing assessment, mistakes can be with regard to harvesting confidential information, data protection, intellectual property, impersonated companies' Terms and Conditions, and using IT systems.

### 4.5.1 Using IT systems

When setting up IT systems for the purpose of research, the main principle is that they cannot be intrusive, and disturb work of IT systems. For example, port scanning is acceptable by itself, because it is not intrusive.

In 2003, Avi Mizrahi, had port scanned the Mossad website, and was accused by the Israeli authorities of the offense of attempting unauthorized access to computer material. About eight months later, he was acquitted of all charges. Verdict Of the Hon. Abrahan N. Tennenbaum: "*In regard to the Internet, legislation should be interpreted in a way that helps Internet to continue its progress for the benefit of the public and not in a*

*way it limits, interferes with, and impedes such progress. According to this principle, security examinations of a website are a positive action in principle, and, in principle should encouraged; we should therefore avoid discouraging such acts, even though they may seem contemptuous with regards to website owners [62]."*

In addition, according to the Council of Europe Cyber Convention's Article 6, creating a phishing website without the aim to collect users' data, especially their credentials, and using them illegally, is acceptable [63]. However, as the rest of the Internet users do not know that the phishing server set up by researchers or CIOs is not a real phishing website, they might still contact the authorities.

#### **4.5.2 Trademark and copyright**

In order to have accurate assessment results, the same impersonating techniques that hackers are using, need to be used by CIOs and researchers. For example, a similar URL, use of logo, color scheme, right names, and signatures can be used. As one part of the phishing is pretending to be well-known company, assessment organizers may run across the situation where trademark and copyright elements needs be used.

Trademarks are images, words, symbols that are indicating company's identity. In U.S. federal law the Lanham Act, 15 U.S.C. §§ 1111 - 1129 governs trademarks. Although trademark law has developed in the course of many years, it is sometimes difficult to establish whether or not law is violated, the decisions are rather made case-by-case bases [146]. In addition, the U.S. is called "a nation of oblivious copyright infringers [147]."

In order not to violate law, it is important to know, are there any legally binding reasons why we should ask permission from impersonated organizations to make phishing assessment? Before the assessments, two questions were asked from Legal department researcher Tomáš Minárik at NATO Cooperative Cyber Defence Centre of Excellence.

1. If I am doing phishing assessment in country X (where all the IT systems, myself, the company who would like to test their employees are situated), and I am impersonating organisation (for example Tax and Customs Board) from the same country, do I really need Tax and Customs Board's permission? Question arises if hackers have previously impersonated Tax and Customs Board and their attacks have been successful. Security Officer is concerned about the issue and he really needs to conduct a phishing assessment, but Tax and Customs Board does not allow it.

*Answer: It depends on the country X's domestic laws, which may be different from country to country, but I would expect that most countries consider it an offence to pretend to be an official without a sufficient reason. I don't think that security testing is a*

*sufficient reason by itself, because you have enough time to ask for a permission from an official. Depending on the wording of the law in a particular country, you might be able to pretend to be an official from a non-existent state body, or from a non-existent company, as long as the name and logo do not remind an existing state body or company too much.*

2. Same scenario at the international level. Let assume I am doing a test in Estonia and I want to impersonate Facebook. Hereby, the test does not violate Facebook terms and conditions.

Answer: *You need a consent from the company whose logo you are using, as long as there is a "likelihood of confusion on the part of the public. And, any time when you are trying to impersonate Facebook (or another company) without its consent, you are creating exactly that confusion [64]."*

As researchers and CIOs need to measure their personnel awareness level, they need solutions. For the thesis, according to ethical and legal considerations, approval to impersonate one of the ministries in Estonia was received. But if you do not have a permission, Hadnagy recommends to consider the following basic requirements [33]:

- The plaintiff has to prove that valid mark was used;
- The plaintiff must show the defendant used the same or a similar mark in commerce in connection with sale or advertising of goods or services without plaintiff's consent;
- The plaintiff must prove that defendant's use of the mark is probably to cause confusion;

Some phishing server and SaaS service providers are offering built-in templates which are mimicking well-known companies. For the thesis, the question about possible legal problems was asked from two service providers. Unfortunately neither of them provided an answer as to how they solve this problem.

Proceeding "Designing Ethical Phishing Experiments: A study of (ROT13) rOnl query features" is an example of how researchers can publish their work. They do not show the impersonated company name by encoding "eBay" with ROT13, which equals to "r0nl" [73].

### **4.5.3 Collecting phishing data**

If an employee clicks the malicious link, it does not automatically mean that he or she would be phished - after visiting the link, the employee may spot the malicious web

site, close the browser's window, and report to CIO. According to Jakobsson, 70% of phishing web page visitors gave out the credentials[73].

According to NATO CCD COE Legal department researcher, if users' credentials are collected in any way, personal data protection rules are most probably violated. The reason is that data is collected without their consent. This problem can be avoided by having the users agree beforehand in their work contract with their company that they might be subjected to security testing, including phishing. However, if CIOs are collecting data that are not connected to their work, such as their personal e-mail passwords, this might still be a problem.

#### 4.5.4 Terms of Conditions

One part of phishing assessment can be information gathering. Under most of companies' Terms and Conditions, there is restriction about using the bots to gather information. As stated by Facebook: "*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 [148].*" Or eBay: "*In connection with using or accessing the Services you will not: use any robot, spider, scraper, or other automated means to access our Services for any purpose [149].*" On the other another hand, most of big companies' are offering Application Programming Interface(API), where queries can be made in a friendly way. In addition, search engines, like Google, can be combined with API results.

## 4.6 Choosing technical solution

To perform a phishing assessment, four types of technical solutions can be used: ready to use SaaS solutions, open-source platform, commercial tools, or a solution created by the organization's IT team. Choosing the right technical solution can provide material for a separate research paper on its own. Considering the purpose of the thesis, which is to show the reasons and provide guidelines for conducting a phishing assessment and measure personnel awareness level, detailed analysis about choosing the best tool is out of its scope.

The overview of technical solutions is based on the analysis by Christopher Hadnagy, Internet search about newest solutions and based on interviews. Hagnagy contacted five top commercial tool service providers and two open-source project leads. He asked three questions [33]:

1. How would you describe the tool?

2. What are the top pros of your tool?
3. What are the top cons of your tool?

Additionally, he answers to the following questions:

1. What level of knowledge is needed to use the tool?
2. What is overall security of customer info?
3. Are there any challenges using this tool ?
4. What is availability of tech support?

#### 4.6.1 SaaS solution

Salesforce: "*Software as a service (or SaaS) is a way of delivering applications over the Internet—as a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management* [150]." SaaS customers do not need to install special software or hardware, only a computer with a web browser, connected to the Internet is needed. For this thesis, four SaaS solutions were analyzed - ThreadSim, PhishMe, PhishGuru, and PhishLine

The main purpose of the SaaS solution is to have an easy set up and running the campaign as easily as possible. Although there are slight differences between the solutions, they all serve the main purpose, which is conducting a phishing assessment.

Since phishing assessment deals with sensitive information, many companies do not want to use it or it is prohibited by internal regulations. Due to the fact that assessments that are performed for this thesis, are holding public organization data, it was not possible to use SaaS solution, and thus, in-depth analyzes about the most suitable solution was not provided.

#### 4.6.2 Open-source server

Two open-source solutions were analyzed: Phishing Frenzy and Social-Engineering Toolkit (SET).

TrustedSec: "*The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community* [151]." SET is a tool which in addition to sending phish-



ing e-mails, can be used to make pentesting to IT systems, example of different web attack vectors can be seen on Figure 11. It gives a possibility to craft custom messages, choose an attack type, and add payloads. Since preparation for the attack requires research and using it with a large-scale assessment takes lot of time, it is more suitable for spear-phishing assessments [33].

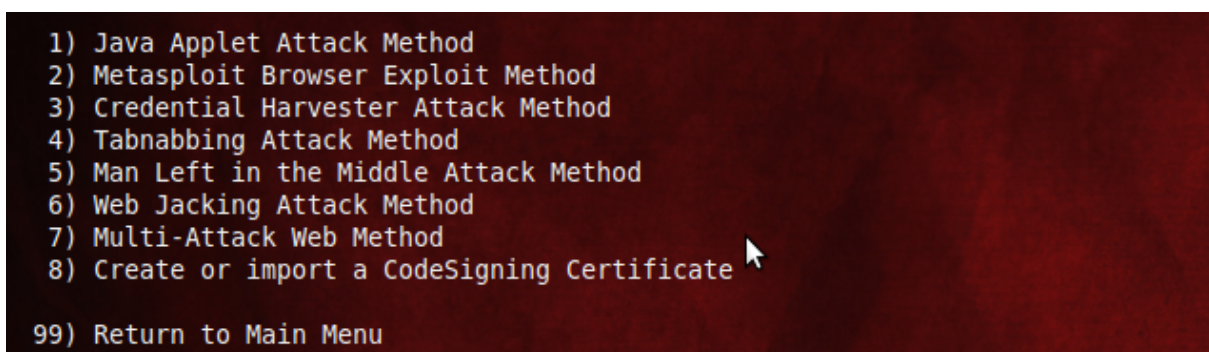


Figure 11. Choosing web attack method in SET [7]

Second open-source solution is Phishing Frenzy: "*Phishing Frenzy is an Open Source Ruby on Rails application that is leveraged by penetration testers to manage e-mail phishing campaigns* [152]." It is only meant for conducting phishing assessments, and since it has a graphical user interface, Phishing Frenzy is suitable for IT personnel with moderate technical skills. Phishing Dark Waters: "*Besides the difficulty of setting up e-mails, Phishing Frenzy is very easy to use and understand* [33]."

#### 4.6.3 Commercial server

Rapid7 MetaSploit Pro is an addition to user testing, a pen-testing to IT system, it covers exploitation, credentials, and web-app testing. As MetaSploit Pro has a GUI, and browsing around the environment is intuitive, no high-level specialist is needed to carry out phishing campaigns [33]. Like Phishing Frenzy, it is a self-hosted server, which means security of the data largely depends on customer setup.

Another commercial server LUCY describes their product as follows: "*To find the weakest security link in your organization, you need to think like a hacker. Thanks to LUCY, you can now measure and improve awareness towards phishing, SMiShing, BadUSB, malware and drive-by attacks by launching your own realistic security campaigns. LUCY can emulate cyberattacks in your own network or in the cloud through four main modules* [67]." the main modules are Traditional Phishing/SMiShing Attack, Malware Attack, Malware Protection Test, and Training.

#### 4.6.4 Custom made

Cova, Kruegek, and Vigna published a research paper in 2008, where a large collection of phishing kits was analyzed. Their conclusion is that many kits contain backdoors that transmit phishing campaign data to third parties [153]. If CIOs are cautious and want to avoid the possible backdoors, custom made option can be used.

One option is to have a unique link for all the employees, so that if an employee clicks the malicious link in the e-mail, the database gives a match suggesting who did it. For example Phishing Frenzy is using following technique: *"PF leverages tags within the phishing sites to track user clicks and other important analytics. Each PHP phishing page is deployed with a tag that will invoke when the page is loaded. The code that is run will make an HTTP POST request back to the Phishing Frenzy application. The Phishing Frenzy application has an API that is listening for these POST requests when the appropriate paramaters are sent. Parameters such as UID, browser, IP, username, password, etc. are sent back to the server where they are then correlated to the appropriate campaign and stored within the database for reporting [154]."*

With small-scale assessments, more expedient solutions can be used. For example, all the employees get the identical link, and web server access logs, can be viewed. Example of Apache access log [155]:

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200  
2326
```

As the purpose of the thesis is to measure cyber security awareness level through phishing assessment, open-source tool Phishing Frenzy provides all the needed features and will be used for both phishing campaigns. Additional features offered by commercial tools, like IT systems' pen-testing, are not needed in case of such research.

## 5 Conducting phishing assessment

Two phishing assessment campaigns were carried out in Estonian public organizations. The first one was conducted in January 2016 and the second one in April 2016. This chapter provides a description to researchers and CIOs interested in conducting similar phishing assessment, analyses the results, shows the learning curve, compares the results of the cyber hygiene test and the phishing assessments, and suggests ideas for future research.

### 5.1 Technical set up

Phishing Frenzy was chosen to be the platform for both assessments. It consists of traditional web server components like Apache; MySQL and PHP5, plus Ruby and Ruby's gems; Redis and Sidekiq. Step-by-step manual can be easily followed, but attention to the end of manual is needed, where there is the following notification: "*Update the Application Site URL within Global Settings menu to the appropriate FQDN with the HTTPS address with SSL enabled*" [156]. In practice, it means that, if the phishing web server needs to be accessible to administrators from `https://192.168.0.1`, it has to be inserted in Application Site URL field, whereas it is not the IP address or domain name which will be shown to assessment participants.

In addition to Ubuntu and Kali installation manuals, there is the Docker manual. As stated on Docker's website: "*Docker containers wrap up a piece of software in a complete filesystem that contains everything it needs to run: code, runtime, system tools, system libraries – anything you can install on a server. This guarantees that it will always run the same, regardless of the environment it is running in*" [157]. It can be especially handy for researchers or human vulnerability testers, who are frequently making assessments for different organizations. If using Docker, they do not need to set up the environment from scratch every time.

#### 5.1.1 Send e-mails

Phishing Frenzy is using rails' library named Action Mailer [158] to send e-mails within the application. In addition to Action Mailer, Sidekiq is used for background processing. As the server was set up for the thesis only, some parts were set up for temporary solutions. For example Sidekiq did not start automatically after reboot, it was started by moving under Phishing Frenzy folder and entering command:

```
$ rmsudo bundle exec sidekiq -C config/sidekiq.xml
```

If the phishing server is made to work for a longer period, the Sidekiq process can be daemonized [159].

In order to gain better control and flexibility over sending out e-mails, local Postfix SMTP server was installed. It is not a needed step if one is using Phishing Frenzy, but for some reasons mail queue management did not work and sometimes unknown error messages appeared. If one is using mail server just for sending out e-mails, the setup is easy to follow [160].

After Postfix installation, few changes in Postfix configuration file had to be done [161, 162, 163]

```
$ vim /etc/postfix/main.cfg
```

```
mynetworks = 127.0.0.0/8,[::1]/128
smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
smtpd_recipient_restrictions = permit_mynetworks
smtp_destination_concurrency_limit = 2
smtp_destination_rate_delay = 10s
```

Configuration change makes difference on two points. Firstly, if one chooses in Phishing Frenzy SMTP server to be 127.0.0.1, it will use locally installed Postfix. Secondly, queue management is solved by last two lines - two e-mails are sent out every 10 seconds, whereas the the rest is placed to the Postfix queue. Full Postfix configuration file can be found in Appendix 2.

As e-mails are only sent out and not received, no PTR records were applied.

### 5.1.2 Landing website

Phishing Frenzy is using Apache's web server to host phishing sites. If one creates a new campaign, one finds the field "FQDN" under E-Mail Settings, if a campaign is made active, a new VirtualHost is created to run the website. VirtualHost settings can be modified at /etc/apache2/sites-enabled/:id.conf. After the campaign has been marked as inactive, VirtualHost is removed and phishing website ceases to be accessible. It also means that one cannot simultaneously run more than one campaign with same FQDN [154].

## 5.2 Assessment 1

Purpose of the assessment 1 was to not impersonate well-known company, not to put attention to e-mail design, and landing web page gave immediate response about phishing assessment. Assessment started on Wednesday before lunch and finished on Friday at 16:00, in total 52 hours. It is easy to carry out similar test because of simple technical set-up, less legal and ethical issues. Immediate response on landing page guarantees that phished employees will not try to contact with impersonated company and CIOs.

### 5.2.1 Phishing e-mail

Email was intentionally made as easy as possible - no well-known company was mimicked, simple e-mail design was used and when hovering mouse over the only URL, instead of the domain name, IP address appeared.

The first step is to configure E-mail Settings, and set the Subject, from which user is e-mail sent out, sender Name, and phishing URL. Phishing URL and FQDN are the same IP addresses in assessment 1. As seen on Figure 12, configuration can be done by GUI.

Email Settings		
Subject:	?	Kiire, toode ostukorvis!!
From:	?	epood@[redacted].eu
Display From:	?	E-pood
Reply To:	?	email@phishingfrenzy.local
Phishing URL:	?	http://[redacted]/index.php
FQDN:	?	[redacted]

Figure 12. Campaign 1 Email Settings

To design an e-mail for campaign browse under campaign settings and click "Add attachment". From the drop-down menu four options can be selected - E-mail; Web-site File, Image attachment, and File Attachment. Choose E-mail and click to created .html.erb file. HTML design view will open, with the assessment 1, HTML code is simple. Full code is described in Appendix 4, but the main part is the following

Tere , <br>

Teie poolt valitud aastalõpu reisipakkumine on ostukorvis ning aegub  
homme õhtul , palun kinnitage pakkumine meie e-poes <a href="<%=\_@url  
\_%">www.domainname.eu</a>

<br>

Aitäh ,<br>

Company Name<br>

Translated text from Estonian to English: "*End of year's sales offer is still in the basket and expires tomorrow evening, please approve the offer in our e-shop.*"

As the purpose of first assessment was to be as simple as possible, it can be categorized as level one phish, having the following characteristics [33]:

- Impersonal greeting;
- Easy message;
- Exploit of sense of greed, fear, or curiosity;
- Bad links in body;
- Unknown sender;

Figure 13 is screenshot of the e-mail which arrived to participants' inbox.

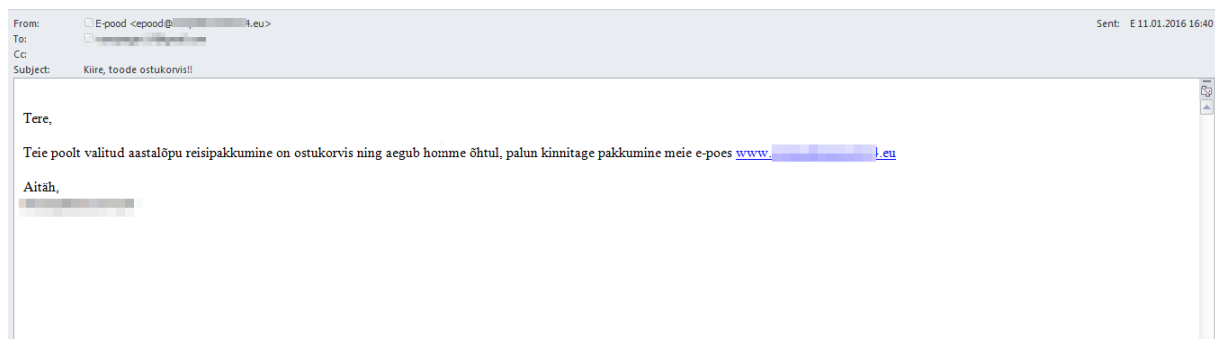


Figure 13. Email of assessment one

There are several key points based on which the employee should question the authenticity of the e-mail.

- Simple design;
- Think carefully, have you visited the website;

- Subject name translated from Estonian - "*Hurry, product is in basket.*"
- If participants hovered the mouse over URL, they would see IP address ending with: `index.php?uid=xxxxxxxx`

### 5.2.2 Landing web page

To design a web page, move under Campaign settings and Edit Email. Click Add Attachment and from drop-down menu choose Website File. Next, click to created `index.php` and the HTML editor will appear. In assessment 1, landing page is not copied from any well-known company and it consists only one PHP file including message that it was a test, to participants who fell for phishing assessment as well as the key points with screenshot suggesting points to consider before clicking the link.

Structure of HTML code for the landing page is the following (the full code can be found in Appendix 5):

```
<h1> SUBJECT</h1>
<hr>
<br>
<p><strong> Message that he/she has failed the phishing assessment :
</strong></p>
<ol>
<li> Description of what the employee should consider when reading the e-

</li>
</ol>
```

To show custom picture in landing page, jpg file was copied to campaign folder:

```
$ sudo cp /home/user/pic.jpg /var/www/phishing-frenzy/public/deployed/
campaigns/22/
```

In order for the employees to access to landing page, an A record was configured in DNS zone file:

```
domainname.eu. IN A IP_address
```

Figure 14 is a screenshot of the landing page, which was seen by employees who clicked the link.

## SEE OLI TEST

---

Sa langesid e-posti testründe ohvriks. Teeseldes küberkurjategijat, saatis infoturbejuht kõikidele töötajatele samasuguse kirja, kus link, millele Sa Outlookis vajutasid, oli osa testist. Sinu arvutiga on kõik hästi, kuigi, kui see oleks olnud tegelik rünne, võinuks Sinu arvuti nakatuda viirusega. Paar olulist punkti mida meeles pidada:

1. Linkide ja manuste avamine võib olla ohtlik. Kui kiri on kummaline või kahtlustäratav, saada see infoturbejuhile.
2. Petukiri soovitab reageerida kiiresti.
3. Petukirjas ei ole mainitud Sinu nime.
4. Petukirja saatjaks võib kuvada keda iganes.
5. Aseta hiire nool Outlookis olevale lingile nii, et Sa **linki ei vajuta**. Kui e-kirjas olev silmaga nähtav link ei ühti lingiga, mis tuleb nähtavale kui hiire nool lingi peale asetada, on suure tõenäosusega tegemist petukirjaga.

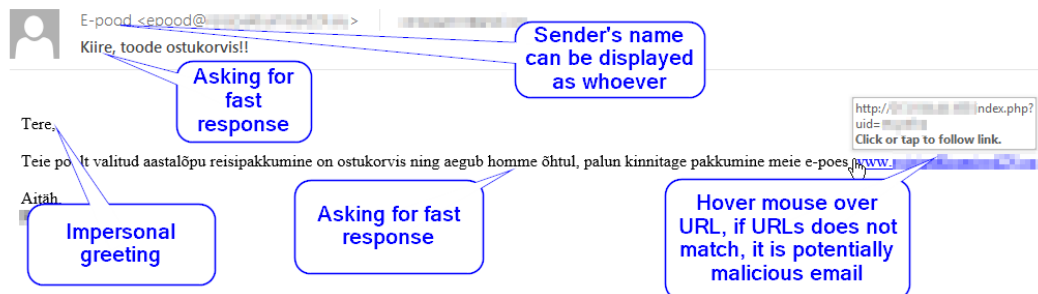


Figure 14. Landing page of assessment one

Translation from Estonian to English:

### IT WAS A TEST

You are a victim of a phishing assessment. CIO impersonated a hacker and sent the same e-mail to all the employees, whereas the hyperlink which you clicked was part of the test. Everything is fine with your computer, but had it been be real attack, your computer could be infected with a virus. A few things to remember:

1. Clicking the links and opening the attachments can be dangerous. If the letter is suspicious, please send it to the CIO;
2. Malicious e-mails often recommend to react fast;
3. Impersonal greeting and closing;
4. Any name can be displayed as that of the sender;
5. Hover the mouse over the link and if the appeared domain name is different from the one you see in the e-mail, it can potentially be malicious e-mail;

### 5.2.3 Result

Clicks of the participants are counted in following way: Phishing Frenzy uses a similar system UID system where every target imported into a phishing campaign will have a random UID tagged to that e-mail address. This UID value is then used when sending



the e-mails to generate a unique phishing URL for each target that can be traced back to a specific e-mail address [164].

Table 3 shows results of first campaign.

Table 3. Campaign 1 summary

Emails Sent	215
Emails Clicked	24
Victims %	11.2%
Reported	<10

Persons who did not click were mostly passive - only a few notified IT or CIO. Possible reasons for this are that as purpose of the campaign 1 was to show test as simplistic as possible without directly mimicking well-known company, it may look like regular spam or most of the employees just do not care about possible cyber attacks. Nonetheless, some of the employees searched information about the company on the Internet, and when Google did not provide any viable answer about the company, a report was sent to IT. 22 out of 24 victims clicked the phishing link within the first 24 hours after the assessment was started.

## 5.3 Assessment 2

The purpose of the second assessment was to make it more difficult to spot the phish. In order to achieve the goal, one of the Estonian ministries was impersonated, and URL in the e-mail looked almost authentic. With the second campaign, an additional organization joined in and around 250 employees were tested. Assessment started on Tuesday before lunch and finished on Friday at 16:00 - in total 78 hours.

### 5.3.1 Phishing e-mail

To impersonate a well-known organization, almost identical domain name was used. Domain name of the ministry consist of around 20 letters, one letter was added in the middle of the name.

To send a phishing e-mail in Phishing Frenzy, two steps need to be taken - configuring Email Settings in GUI and designing an e-mail. Compared to the previous assessment, Email Settings Subject, From, Display From, Phishing URL, and FQDN were changed in a way that they impersonated the Ministry domain and one of the Ministry's employees.

The e-mail that arrived to participants is Figure 15:

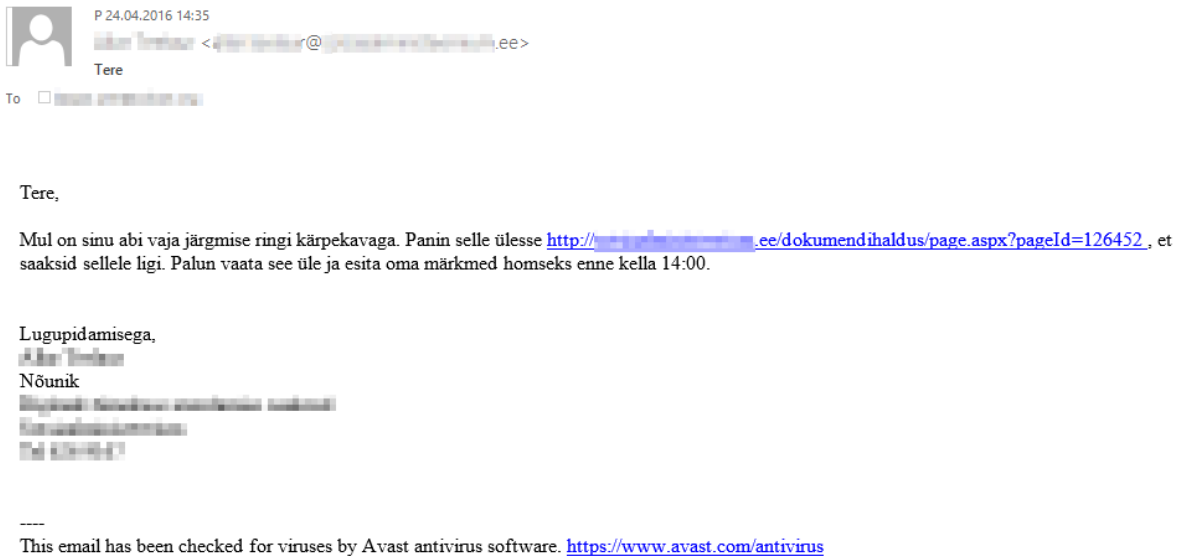


Figure 15. Email of assessment two

Translation from Estonian to English: *I need your help with the upcoming plan for the budget cut. I uploaded it to <http://domain.dokumendihaldus/page.aspx?pageId=126452>. Please review it and give your feedback by tomorrow at 14:00 at the latest.* Additionally, authentic signature of the Ministry and message about successful antivirus scanning were added.

The E-mail was designed in HTML, full part can be found in Appendix 6, but the translated two sentences in HTML code are the following:

Tere , <br>

<br>

Mul on sinu abi vaja järgmise ringi kärpekavaga. Panin selle ülesse

<a href="<%=□@url□%>"> http://domain/dokumendi haldus/page.aspx? pageId=126452

</a> , et saaksid sellele ligi.

Palun vaata see üle ja esita oma märkmed homseks enne kella 14:00.

<br>

There are several elements based on which the employees should question the authenticity of the e-mail and identify it as a phishing attack.

- Ministry is sending e-mails by using a few letters acronym of its full name;
- Full name of the domain is not correct;

- If the participant hovered the mouse over URL, he would see a different domain;
- The recipient should think carefully if it is his/her task to provide desired feedback;
- Phishing e-mails often exploit human benevolence and the will to act fast;

### 5.3.2 Landing web page

As the landing page for assessments one and two used immediate feedback for participants who fell to phishing attack, similar techniques were used to set up landing web page in both cases.

Difference of the landing page compared to assessment one was that, in the second case, it used a screenshot of the second assessment with an explanation of how the participant could recognize the phishing letter. Landing webpage for assessment two is seen on Figure 16.

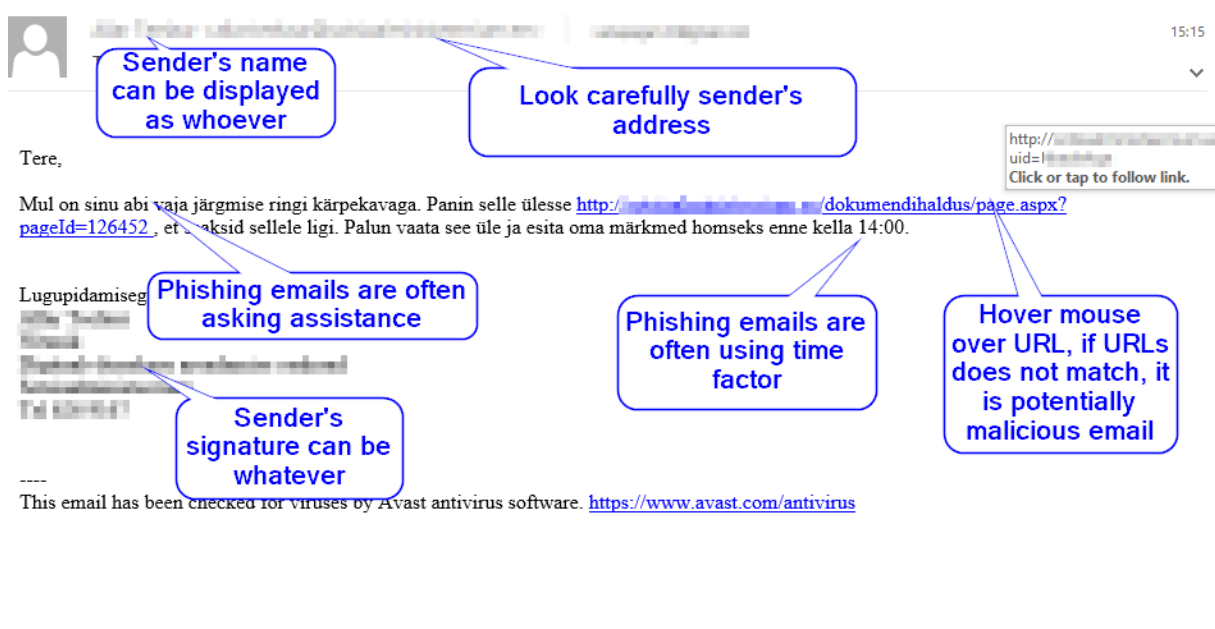


Figure 16. Screenshot in landing web page during assessment two

Translated content in blue bubbles from Estonian to English is as follow: *Any sender name can be displayed; malicious e-mail often emphasizes the kindness of others; look closely at the sender domain; hover mouse over URL, if links do not match, there is a high possibility of it being a malicious e-mail; sender signature can be from whoever*

### 5.3.3 Result

In case of the more difficult assessment, number of victims doubled. The amount of employees who notified about possible phishing attack was remarkable - 114 notifications came through e-mail, phone calls, and by visiting IT helpdesk or CIO. Results of assessment two is seen on Table 4.

Table 4. Campaign 2 summary

Emails Sent	251
Emails Clicked	50
Victims %	20%
Reported	114

For the second assessment, another organization joined the campaign. If analyzing only the employees who took part in both assessments, 212 e-mails were sent. Of these persons, 42 (19,5%) clicked the link.

In Figure 17, campaign activity was divided into blocks of 15 minutes, and within these blocks, the number of clicks was counted. As the beginning of attack is the most active period, CIOs need to think how they can react immediately to isolate the victim's computer and block access to the phishing web site.

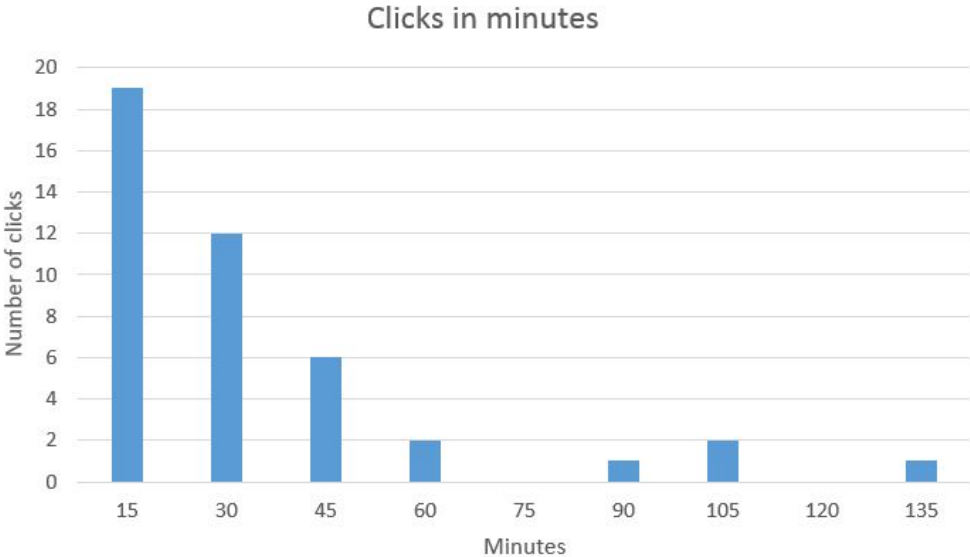


Figure 17. Assessment 2: clicks in minutes

## 5.4 Reaction by participants

In the case of both assessments, the landing web page gave an immediate response about the phishing assessment. Because of using this technique, employees did not need to worry about real threat. It can be considered to be one of the most important nuances that allowed participants to understand the need for similar tests, which is also proved by the fact that no complaints were issued. Participants feedback about their reaction if they received the e-mail:

- "hurry" and "tomorrow" is usually not asked;
- Email header contained "Received: from kasparubuntu.localdomain (IP address);
- Information about Avast antivirus scanner on the e-mail footer was not seen;
- Unceremonious writing style is often used, it did not give a hint;
- Content was well chosen, appropriate and caught attention;
- Impersonated organization will send e-mails by using short version of the Ministry's domain;
- Persons name, role, and telephone number did not match;
- Participants are not connected to the topic.

## 5.5 Learning curve

According to other researchers, having immediate response on landing page, is recommended way to educate the personnel: "*Based on the exercise, it can be concluded that a simulated phishing attack together with embedded training can contribute towards cultivating users' phishing resistance as this approach reduces the user's risk of becoming a victim to any future phishing attack [165].*"

First assessment was failed by 24 participants, only 6 of these 24 persons failed also in the second assessment. It suggests that 75% of the employees who were victims of assessment 1, learned the lessons and did not make the same mistake after 3 months when the second iteration was conducted. Participants who clicked the link and therefore were informed about the phishing assessment, most probably informed some of the colleagues about the test, which means that the real learning percentage number is most probably slightly lower.

If analyzing when these six participants clicked the link, then half of them did it within the first 15 minutes, which could mean that some persons frequently click the links without thinking about possible threats. The remaining three persons who failed in both assessments, made the clicks on next day.

### 5.6 Compare phishing assessments and cyber hygiene test

A significant part that research papers with similar content often fall short of, is the analysis of links between the phishing assessments and cyber hygiene test. The organization that involved 215 participants had conducted a cyber hygiene test one and half year before the phishing assessment. The test was set-up in a web server and all the employees had to finish the quiz. 20 questions were asked, potential answers were offered, one or more answers could be marked as correct. Topics covered in the hygiene test were following: what is a cyber attack; what type of attacks are used; how to mitigate attacks; which information is exploited; information security; physical security; cryptography; social engineering; phishing; use of smart devices; using passwords; using Internet at work and home; and data protection. If a participant answered 17 questions of 20 correctly, the test was considered as passed. Total result - 15% of participants failed the test.

Around 200 persons in total were participants in both phishing assessments and cyber hygiene test. Table 5 is organized as following: Cyber hygiene score (maximum 20 points); and mark "-" if failed in phishing assessment 1 or 2.

Table 5. Cyber hygiene and phishing assessments comparison matrix

Cyber hygiene	Assessment 1	Assessment 2
9,25		-
11,75		-
12,75	-	
14,5		-
16	-	
16,5		-
N/A		-
N/A	-	
19	-	-
19	-	-
19	-	-
19	-	-
19,33	-	-
20	-	-

In total, around 30 participants failed the cyber hygiene test, the reason why only 6 are presented in Table 5 is either that, the rest passed both phishing assessments, or they are not working for the organization anymore. 15 participants did not complete the hygiene test, 2 of them failed in one of the assessments. Both phishing assessments were failed by 6 participants. The most interesting observation is that all of these 6 participants got a score of more than 95% from cyber hygiene test. Hence, further research on the topic is recommended. All the rest who are not marked in Table 5 are the employees who failed either the cyber hygiene test or assessment one or two.

## **5.7 Additional benefits**

Although the goal of the assessments was to measure personnel cyber security awareness level, IT systems and processes were also tested. Thanks to the assessment, one of the companies' spam filter set-up got vital feedback, and alert about simple e-mail spoofing option was notified. In addition, in the course of a phishing assessment, it is possible to test how well IT processes are working - one is provided with information on the amount of people likely to notify CIOs or IT helpdesk, and how fast and in which way notifications were provided. Depending on the goal of the assessment, different scenarios can be used.

## **5.8 Future work**

The most important goal of the phishing assessment in a real working environment is to make the phishing attack look as realistic as possible. In order to conduct attacks that are even more realistic, an elevated version of assessment can be conducted. Research papers, which would use some of these techniques, for example spoofing well-known domain in large-scale assessment, are not publicly available. Possibilities to elevate complexity of assessment and understand more about success of phishing attacks:

1. Conduct assessments on different times, and also during busy working period. Hunger and stress can make the difference of test results.
2. Do not give immediate response. In this case, learning curve may be not so effective, but CIOs will have better overview about their vulnerable users. In order to make such a assessment, two things need to be considered:
  - One needs to assess even more carefully the phishing e-mail - one does not want to stress the employees about misinformation, and one does not want them to spend hours working with the content withing e-mail.

- One has to copy the original web page and make it look like the authentic web page.
3. The idea of phishing is to get information from the victim, just the click by itself does not mean that someone has been phished. Thus, one could measure how many participants are willing to give out confidential information. According to proceeding "Designing ethical phishing experiments: a study of (rot13) ronl query features", if a phishing website is well set-up, 70% on participants who click the link, would give out their password [73].
  4. To make the assessment even more difficult, one could try a level four phish, in other words spear-phishing. To play a worst-case scenario, one should try to find approval from an organization where spoofing is easy, and send out spoofed e-mails.
  5. In addition to possibly using level three of spear-phishing e-mails, a bigger data set is needed for comparing cyber hygiene test and phishing assessment correlation.



## 6 Conclusion

This thesis highlighted the importance of personnel cyber security awareness and provided a description of a way to measure personnel cyber security awareness level.

It appears that employees often click malicious links and open attachments partly because they trust organization's IT systems. Internet service providers, website hosting companies, spam filters, client device, and authentication mechanisms will block most of the attacks, but not all of them. The possible reasons are either a slow blacklisting, automatic detection tools that are not good enough or the fact that the employee who is operating behind client device does not act as needed.

As none of the anti-phishing tools constitute a silver bullet against phishing attack and the statistical curve does not show a downward trend, it is clear that trusting barely on technological solutions is not enough. Regarding information security, human is frequently seen as the weakest link, hence, organizations need to find vulnerable users and improve personnel cyber security awareness level.

Giving lectures about cyber threats and measuring their knowledge by quizzes is not enough. It is important to know how employees would act if a real phishing attack occurred - this can be achieved by measuring personnel cyber security awareness level. Decision-making factors like hunger, working under stress, sleeplessness, work conditions, the fact that some employees do not follow the rules, personality factors; and well chosen e-mail content can be listed among the most important aspects of why only theoretical education is not enough. To measure personnel vulnerable against phishing attack, phishing assessment in real working environment is recommended.

When conducting assessment many things can go wrong - for instance, it can even happen that researchers or CIOs who are conducting campaigns are demanded to be prosecuted or fired. In order to avoid it, all legal and ethical aspects need to be carefully considered, whereas all necessary approvals need to be signed.

When choosing phishing servers, a different option like SaaS, open-source, commercial, or custom made solutions can be used. One should make the choice according to data classification, organization's regulation, number of assessments, number of participants, and organization's in-house technical capability - best solution varies.

For this thesis, two assessments were conducted. Purpose of the first one was to be as easy as possible for participants, as well as for persons organizing the campaign. The E-mail looked like it was sent from unknown company that did not impersonate any well-known organization, and content of the e-mail could be easily spotted as phish. In total, 215 e-mails were sent and 11% of the recipients clicked the link. After participants

clicked the link, immediate response telling about the phishing assessment was shown, along with instructions on how the participants could have identified it as a phish, and on how to act. After the campaign finished, an e-mail was sent to all the employees, where one of the points was a reminder that CIOs and IT helpdesk need to be notified when potentially malicious e-mail is received.

Second assessment was launched three months after the first one, and it involved impersonating one of the ministries in Estonia. 20% of the 251 employees clicked the link. The number of reports made by employees was remarkable - 114, which is 46% of the total amount of participants. In addition, 75% of the employees who were victims in the first assessment, had learned from their mistakes and were not victims of second assessment.

When comparing cyber hygiene test results from more than one year before to those of the phishing assessments, no correlation was found. In fact, all the 6 participants who failed both phishing assessments, got a score of more than 95% in the cyber hygiene test.

Finally, the primary purpose of the phishing assessments was to measure personnel cyber security awareness level. Also, the research highlighted that if the measurement is done by using the phishing assessment, extra benefits for testing organization's e-mail server occur. The vital hint about the spam filter and the simple way to spoof their domain were noted.

## References

- [1] Cyveillance, “The cost of phishing: Understanding the true cost dynamics behind phishing attacks,” <http://info.cyveillance.com/rs/cyveillanceinc/images/CYV-WP-CostofPhishing.pdf>, May 2015, last accessed: 03 March 2016.
- [2] ExtendOffice, “How to get phishing warning in receiving email messages in Outlook?” <https://www.extendoffice.com/documents/outlook/1670-outlook-phishing-warning.html>, last accessed: 07 July 2016.
- [3] Jade Carter, <http://www.jadecarter.info/warning-facebook-suspected-phishing-site/2010/07>, July 2010, last accessed: 07 July 2016.
- [4] A. MacCaw, “Be warned, there’s a nasty Google 2-factor auth attack going around,” <https://twitter.com/maccaw/status/739232334541524992/photo/1>, June 2016, last accessed: 18 September 2016.
- [5] R. C. Dodge, C. Carver, and A. J. Ferguson, “Phishing for user security awareness,” *Computers & Security*, vol. 26, no. 1, pp. 73–80, 2007.
- [6] K. Zetter, “Researchers uncover RSA phishing attack, hiding in plain sight,” <http://www.wired.com/2011/08/how-rsa-got-hacked/>, August 2011, last accessed: 17 april 2016.
- [7] Mirovola, “How to hack passwords with SET,” <http://hacktheblog-mirovola.blogspot.com/2011/09/credential-harvesting-attack-social.html>, September 2011, last accessed: 17 april 2016.
- [8] Massmailservers.net, “SMTP hosting,” <http://www.massmailservers.net/services/bulk-smtp>, last accessed: 12 July 2016.
- [9] CNN, “A convicted hacker debunks some myths,” <http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cna/>, October 2005, last accessed: 04 February 2016.
- [10] SANS Institute, <https://www.sans.org/>, last accessed: 04 February 2016.
- [11] SANS institute, “The weakest link...this is not a game,” <https://www.sans.org/reading-room/whitepapers/basics/weakest-linkthis-game-440>, last accessed: 04 February 2016.

- [12] APWG, “Phishing activity trends report: 1st- 3rd quarter’s 2015s,” [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1-q3\\_2015.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf), December 2015, last accessed: 24 February 2016.
- [13] F. H. Katz, “The effect of a university information security survey on instructing methods in information security,” in *Proc of the Annual Conference on Information Security Curriculum Development*, 2005, pp. 43–48.
- [14] F. A. Aloul, “The need for effective information security awareness,” *Journal of Advances in Information Technology*, vol. 3, no. 3, pp. 176–183, 2012.
- [15] Verizon, “Quantify the impact of a data breach with new data from the 2015 DBIR,” [http://www.verizonenterprise.com/resources/reports/rp\\_data-breach-investigation-report\\_2015\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf), 2015, last accessed: 04 July 2016.
- [16] EMC, “2014 cybercrime roundup,” <https://www.emc.com/collateral/fraud-report/h13929-rsa-fraud-report-jan-2015.pdf>, 2015, last accessed: 04 February 2016.
- [17] Symantec, “Symantec intelligence report, June 2015,” [https://www.symantec.com/content/en/us/enterprise/other\\_resources/intelligence-report-06-2015-en-us.pdf](https://www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-06-2015-en-us.pdf), 2015, last accessed: 04 February 2016.
- [18] Europol, “Internet organised crime threat assessment,” [https://www.europol.europa.eu/sites/default/files/publications/europol\\_iocta\\_web\\_2016.pdf](https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2016.pdf), September 2016, last accessed: 29 Sept 2016.
- [19] Techtarget, “The social engineering framework,” <http://www.social-engineer.org/framework/psychological-principles/>, last accessed: 04 February 2016.
- [20] M. Wu, R. C. Miller, and S. L. Garfinkel, “Do security toolbars actually prevent phishing attacks?” in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006, pp. 601–610.
- [21] I. Bose and A. C. M. Leung, “Unveiling the mask of phishing: Threats, preventive measures, and responsibilities,” *Communications of the Association for Information Systems*, vol. 19, no. 1, p. 24, 2007.
- [22] B. Kurian and B. Sangeetha Sangam, “A study on browser-based anti-phishing tools,” 2014.

- [23] A. Jaquith, “Security metrics: Replacing fear,” *Uncertainty, and Doubt*, 2007.
- [24] SANS Institute, “Security awareness metrics - part 2,” <https://securingthehuman.sans.org/blog/2010/10/05/metrics-2>, last accessed: 04 February 2016.
- [25] “Resources: Measuring results,” <https://www.securingthehuman.org/resources/metrics>, last accessed: 04 February 2016.
- [26] SANS Institute, “The human risk survey,” <https://files.sans.org/summit/secaware14/PDFs/The%20Human%20Risk%20Survey%20-%20Hayden.pdf>, last accessed: 04 February 2016.
- [27] SANS institute, “Security awareness metrics - measuring human risk,” <https://securingthehuman.sans.org/blog/2012/08/21/security-awareness-metrics-measuring-human-risk>, last accessed: 04 February 2016.
- [28] R. Dhamija, J. D. Tygar, and M. Hearst, “Why phishing works,” in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006, pp. 581–590.
- [29] Social-Engineer, “Phishing definition,” <http://searchsecurity.techtarget.com/definition/phishing>, last accessed: 04 February 2016.
- [30] V. Venkatraman, S. A. Huettel, L. Y. Chuah, J. W. Payne, and M. W. Chee, “Sleep deprivation biases the neural mechanisms underlying economic preferences,” *The Journal of Neuroscience*, vol. 31, no. 10, pp. 3712–3718, 2011.
- [31] Phys.org, “Hunger affects decision making and perception risk,” <http://phys.org/news/2013-06-hunger-affects-decision-perception.html>, last accessed: 04 February 2016.
- [32] S. D. Gosling, P. J. Rentfrow, and W. B. Swann, “A very brief measure of the big-five personality domains,” *Journal of Research in personality*, vol. 37, no. 6, pp. 504–528, 2003.
- [33] C. Hadnagy and M. Fincher, *Phishing Dark Waters: The offensive and defensive sides of malicious emails*. John Wiley & Sons, 2015.
- [34] M. Hasan, N. Prajapati, and S. Vohara, “Case study on social engineering techniques for persuasion,” *arXiv preprint arXiv:1006.3848*, 2010.

- [35] T. Mataracioglu, “Analysis of Social Engineering Attacks in Turkey,” *Journal of National Research Institute of Electronics and Cryptology (UEKAE)*, vol. 2, no. 4, 2010.
- [36] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2011.
- [37] SANS Institute, “Human metrics: Measuring behavior,” <https://securingthehuman.sans.org/media/resources/presentations/STH-Presentation-HumanMetrics.pdf>, last accessed: 04 February 2016.
- [38] Social-engineer.org, “The social engineering framework,” <http://www.social-engineer.org/framework/general-discussion/>, last accessed: 04 February 2016.
- [39] SANS Institute, “Building an effective phishing program,” <https://securingthehuman.sans.org/media/resources/presentations/STH-Presentation-PhishingYourEmployees.pdf>, last accessed: 04 February 2016.
- [40] APWG, “Global phishing survey: Trends and domain name use in 2H2014,” [http://www.antiphishing.org/download/document/245/APWG\\_Global\\_Phishing\\_Report\\_2H\\_2014.pdf](http://www.antiphishing.org/download/document/245/APWG_Global_Phishing_Report_2H_2014.pdf), May 2015, last accessed: 19 april 2016.
- [41] I. N. Africa, “10 tricks used by spammers to get into your inbox,” <http://www.itnewsafrika.com/2009/11/10-tricks-used-by-spammers-to-get-into-your-inbox/>, last accessed: 14 March 2016.
- [42] P. Software, “Common spammer tricks: white paper,” [http://www.process.com/psc/fileadmin/user\\_upload/whitepapers/pmas/common\\_spammer\\_tricks.pdf](http://www.process.com/psc/fileadmin/user_upload/whitepapers/pmas/common_spammer_tricks.pdf), last accessed: 10 March 2016.
- [43] J. Graham-Cumming, “Tricks of the spammer’s trade,” [http://www.windowsecurity.com/uplarticle/anti-spam/Spammer\\_tricks.pdf](http://www.windowsecurity.com/uplarticle/anti-spam/Spammer_tricks.pdf), March 2004, last accessed: 10 March 2016.
- [44] Office.com, “Enable or disable links and functionality in phishing email messages,” <https://support.office.com/en-us/article/Enable-or-disable-links-and-functionality-in-phishing-email-messages-f157f978-c8ed-410b-a9e3-a1>, last accessed: 29 April 2016.

- [45] S. Sharma, “Using contextual information to improve phishing warning effectiveness,” Ph.D. dissertation, Arizona State University, 2015.
- [46] S. Egelman, L. F. Cranor, and J. Hong, “You’ve been warned: an empirical study of the effectiveness of web browser phishing warnings,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2008, pp. 1065–1074.
- [47] M. Mannan and P. C. van Oorschot, “Using a personal device to strengthen password authentication from an untrusted computer,” in *Financial Cryptography and Data Security*. Springer, 2007, pp. 88–103.
- [48] M. Wilson and J. Hash, “Building an information technology security awareness and training program,” *NIST Special publication*, vol. 800, p. 50, 2003.
- [49] S. M. Ira Winkler, “7 reasons for security awareness failure,” <http://www.csoonline.com/article/2133697/metrics-budgets/7-reasons-for-security-awareness-failure.html>, July 2013, last accessed: 28 March 2016.
- [50] M. Symmonds, J. J. Emmanuel, M. E. Drew, R. L. Batterham, and R. J. Dolan, “Metabolic state alters economic decision making under risk in humans,” *PloS one*, vol. 5, no. 6, p. e11090, 2010.
- [51] Neurosciences, “Hunger affects decision making and perception of risk,” <https://www.mpg.de/7422218/hunger-behaviour>, June 2013, last accessed: 03 april 2016.
- [52] D. M. Christina Hamlett, “How stress affects your work performance,” <http://smallbusiness.chron.com/stress-affects-work-performance-18040.html>, last accessed: 20 april 2016.
- [53] U. of Cambridge, “Effects of work-related stress,” <http://www.admin.cam.ac.uk/offices/hr/policy/stress/effects.html>, November 2011, last accessed: 20 april 2016.
- [54] Y. Kang, L. E. Williams, M. S. Clark, J. R. Gray, and J. A. Bargh, “Physical temperature effects on trust behavior: the role of insula,” *Social Cognitive and Affective Neuroscience*, p. nsq077, 2010.
- [55] M. Jakobsson and P. Finn, “Designing and conducting phishing experiments,” *IEEE Technology and Society Magazine, Special Issue on Usability and Security*, 2007.

- [56] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007.
- [57] M. Al-Hamar, R. Dawson, and L. Guan, “A culture of trust threatens security and privacy in Qatar,” in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*. IEEE, 2010, pp. 991–995.
- [58] U. S. C. O. APPEALS, “ U.S. Court of Appeals for the Ninth Circuit: Bernstein v USDOJ ,” [https://epic.org/crypto/export\\_controls/bernstein\\_decision\\_9\\_cir.html](https://epic.org/crypto/export_controls/bernstein_decision_9_cir.html), September 1996, last accessed: 27 april 2016.
- [59] J. Markoff, “Record panel threatens researcher with lawsuit,” <http://www.nytimes.com/2001/04/24/technology/24MUSI.html>, August 2005, last accessed: 27 april 2016.
- [60] J. Granick, “An insider’s view of ‘Ciscogate’ ,” <http://archive.wired.com/science/discoveries/news/2005/08/68435?currentPage=all>, August 2005, last accessed: 27 april 2016.
- [61] J. Markoff, “ Data-Secrecy export case dropped by U.S. ,” <http://www.nytimes.com/1996/01/12/business/data-secrecy-export-case-dropped-by-us.html>, January 1996, last accessed: 27 april 2016.
- [62] J. M. Court, “Verdict Of the Hon. Abraham N. Tennenbaum ,” [http://www.law.co.il/media/computer-law/mizrachi\\_en.pdf](http://www.law.co.il/media/computer-law/mizrachi_en.pdf), February 2004, last accessed: 27 april 2016.
- [63] C. of Europe, “ETS 185 – Cybercrime (Convention), 23.XI.2001 ,” <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>, November 2001, last accessed: 27 april 2016.
- [64] U. S. C. O. APPEALS, “ Article 5(1)(b) of directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trade marks ,” <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008L0095>, October 2008, last accessed: 27 april 2016.
- [65] C. Soghoian, “Legal risks for phishing researchers,” in *eCrime Researchers Summit, 2008*. IEEE, 2008, pp. 1–11.
- [66] PhishMe, <http://phishme.com/>, last accessed: 04 February 2016.



- [67] LUCY, “What is LUCY? ,” <http://phishing-server.com/>, last accessed: 23 april 2016.
- [68] Sptoolkit, <https://github.com/sptoolkit/sptoolkit/>, last accessed: 04 February 2016.
- [69] TrustedSec, “Social-engineering toolkit,” <https://www.trustedsec.com/social-engineer-toolkit/>, last accessed: 04 February 2016.
- [70] Phishing Frenzy, <https://www.phishingfrenzy.com/>, last accessed: 04 February 2016.
- [71] SANS Institute, “Getting support and approval for phishing assessments,” <https://securingthehuman.sans.org/blog/2014/03/12/getting-support-and-approval-for-phishing-assessments>, last accessed: 04 February 2016.
- [72] KnowBe4, “How to get the ok to phish your own employee,” <https://blog.knowbe4.com/how-to-get-the-ok-to-phish-your-own-employees>, last accessed: 04 February 2016.
- [73] 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*. ACM, 2006, pp. 513–522.
- [74] M. L. Hale, R. F. Gamble, and P. Gamble, “CyberPhishing: A game-based platform for phishing awareness testing,” in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. IEEE, 2015, pp. 5260–5269.
- [75] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham, “School of phish: a real-world evaluation of anti-phishing training,” in *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, 2009, p. 3.
- [76] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, “Teaching johnny not to fall for phish,” *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, p. 7, 2010.
- [77] Techtarget.com, “Botnet (zombie army) ,” <http://searchsecurity.techtarget.com/definition/botnet>, February 2012.

- [78] N. D. Tatyana Shcherbakova, Maria Vergelis, “Spam: features of the quarter,” <https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/>, May 2015, last accessed: 24 March 2016.
- [79] P. Frenzy, “Methodology,” <https://www.phishingfrenzy.com/resources/methodology>, last accessed: 21 april 2016.
- [80] J. Mehnle, “Sender policy framework,” <http://www.openspf.org/Introduction>, April 2010, last accessed: 21 april 2016.
- [81] T. Hansen, “DKIM Service Overview,” <https://tools.ietf.org/html/rfc5585>, July 2009, last accessed: 21 april 2016.
- [82] A. Gorrell, “Build your DMARC record in 15 minutes,” <https://blog.returnpath.com/build-your-dmarc-record-in-15-minutes-v2/>, February 2016, last accessed: 18 October 2016.
- [83] dmarc.org, “Frequently asked questions,” <https://dmarc.org/wiki/FAQ>, February 2016, last accessed: 18 October 2016.
- [84] A. Gorrell, “How to read your first DMARC reports (part 1),” <https://blog.returnpath.com/how-to-read-your-first-dmarc-reports-part-1/>, February 2016, last accessed: 18 October 2016.
- [85] “How to Read Your First DMARC Reports (Part 2),” <https://blog.returnpath.com/how-to-read-your-first-dmarc-reports-part-2/>, March 2016, last accessed: 18 October 2016.
- [86] D. S. Development, “Send email rate limit for webmail providers - Gmail, Yahoo! Mail, Hotmail, AOL, Lycos Mail,” <http://www.emailaddressmanager.com/tips/email-address-limit.html>, last accessed: 14 March 2016.
- [87] I. U. U. I. T. Services, “In Unix, what is an open mail relay?” <http://web.archive.org/web/20070617083024/kb.iu.edu/data/aivh.html>, last accessed: 14 March 2016.
- [88] Kaspersky, “Spam and phising in Q3 2015,” [https://securelist.com/files/2015/11/Q3-2015\\_Spam-report\\_final\\_EN.pdf](https://securelist.com/files/2015/11/Q3-2015_Spam-report_final_EN.pdf), last accessed: 14 March 2016.

- [89] D. Bestuzhev, “A phishing trampoline – embedding redirects in PDF documents,” <https://securelist.com/blog/phishing/71963/a-phishing-trampoline-embedding-redirects-in-pdf-documents/>, August 2015, last accessed: 04 July 2016.
- [90] Forbes, “Simulated phishing attacks yield 37 percent return on investment,” <http://www.forbes.com/sites/lisabrownlee/2015/10/07/security-simulated-phishing-attacks-yield-37-percent-return-on-investment/#13d0c8c42642>, October 2015, last accessed: 10 March 2016.
- [91] J. Hong, “The state of phishing attacks,” *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, 2012.
- [92] MozillaZine, “Safe browsing,” [http://kb.mozillazine.org/Safe\\_browsing](http://kb.mozillazine.org/Safe_browsing), last accessed: 14 March 2016.
- [93] AV-Comparatives, “Anti-phishing protection of popular web browsers,” [http://www.av-comparatives.org/images/docs/avc\\_phi\\_browser\\_201212\\_en.pdf](http://www.av-comparatives.org/images/docs/avc_phi_browser_201212_en.pdf), december 2012, last accessed: 18 March 2016.
- [94] A. Vance, B. B. Anderson, C. B. Kirwan, and D. Eargle, “Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG),” *Journal of the Association for Information Systems*, vol. 15, no. 10, p. 679, 2014.
- [95] H. Almuhammedi, A. P. Felt, R. W. Reeder, and S. Consolvo, “Your reputation precedes you: History, reputation, and the chrome malware warning.” in *SOUPS*, 2014, pp. 113–128.
- [96] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, “Your attention please: designing security-decision UIs to make genuine risks harder to ignore,” in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 6.
- [97] A. P. Felt, R. W. Reeder, H. Almuhammedi, and S. Consolvo, “Experimenting at scale with Google Chrome’s SSL warning,” in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2667–2670.
- [98] D. Akhawe and A. P. Felt, “Alice in warningland: A large-scale field study of browser security warning effectiveness.” in *Usenix security*, 2013, pp. 257–272.

- [99] Y. Chen, F. M. Zahedi, and A. Abbasi, “Interface design elements for anti-phishing systems,” in *Service-oriented perspectives in design science research*. Springer, 2011, pp. 253–265.
- [100] L. F. Cranor, S. Egelman, J. I. Hong, and Y. Zhang, “Phinding phish: An evaluation of anti-phishing toolbars.” in *NDSS*, 2007.
- [101] S. Purkait, “Phishing counter measures and their effectiveness-literature review,” *Information Management & Computer Security*, vol. 20, no. 5, pp. 382–420, 2012.
- [102] N. A. G. Arachchilage and S. Love, “A game design framework for avoiding phishing attacks,” *Computers in Human Behavior*, vol. 29, no. 3, pp. 706–714, 2013.
- [103] A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, “PhishAri: Automatic realtime phishing detection on Twitter,” in *eCrime Researchers Summit (eCrime), 2012*. IEEE, 2012, pp. 1–12.
- [104] M. Wu, R. C. Miller, and G. Little, “Web Wallet: preventing phishing attacks by revealing user intentions,” in *Proceedings of the second symposium on Usable privacy and security*. ACM, 2006, pp. 102–113.
- [105] E. Kirda and C. Kruegel, “Protecting users against phishing attacks with antiphish,” in *Computer Software and Applications Conference, 2005. COMPSAC 2005. 29th Annual International*, vol. 1. IEEE, 2005, pp. 517–524.
- [106] K.-P. Yee and K. Sitaker, “Passpet: Convenient password management and phishing protection,” in *Proceedings of the second symposium on Usable privacy and security*. ACM, 2006, pp. 32–43.
- [107] LastPass, <https://lastpass.com>, last accessed: 22 March 2016.
- [108] J. Siegrist, “Lastpass security notice,” <https://blog.lastpass.com/2015/06/lastpass-security-notice.html/>, June 2015, last accessed: 22 March 2016.
- [109] Sophos, “Bad news! LastPass breached. Good news! You should be OK...,” <https://nakedsecurity.sophos.com/2015/06/16/bad-news-lastpass-breached-good-news-you-should-be-ok/>, last accessed: 22 March 2016.
- [110] S. Harris, *CISSP all-in-one exam guide*. McGraw-Hill, Inc., 2013.

- [111] H.-P. Lu, C.-L. Hsu, and H.-Y. Hsu, “An empirical study of the effect of perceived risk upon intention to use online applications,” *Information Management & Computer Security*, vol. 13, no. 2, pp. 106–120, 2005.
- [112] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, “On the (in) security of mobile two-factor authentication,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 365–383.
- [113] Apple, “Two-factor authentication for Apple ID,” <https://support.apple.com/en-us/HT204915>, March 2016, last accessed: 17 april 2016.
- [114] Statista, “Number of smartphone users worldwide from 2014 to 2019 (in millions),” <http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>, 2016, last accessed: 19 april 2016.
- [115] J. Franusic, “Add two-factor authentication to your website with Google Authenticator and Twilio SMS ,” <https://www.twilio.com/blog/2013/04/add-two-factor-authentication-to-your-website-with-google-authenticator-and-twilio-sms.html>, April 2013, last accessed: 19 april 2016.
- [116] APWG, “APWG phishing attack trends reports,” <http://www.antiphishing.org/resources/apwg-reports/>, last accessed: 19 april 2016.
- [117] phishing.org, “History of phishing,” <http://www.phishing.org/history-of-phishing/>, last accessed: 28 March 2016.
- [118] C. Dawson, “Education is still the key to stopping phishing attacks,” <https://blog.fortinet.com/post/education-is-still-the-key-to-stopping-phishing-attacks>, November 2015, last accessed: 28 March 2016.
- [119] J. S. Davis, “Poor cyber hygiene - not zero days - to blame for high-profile intrusions, says NSA,” <http://www.scmagazine.com/poor-cyber-hygiene--not-zero-days--to-blame-for-high-profile-intrusions-says-nsa/article/523259/>, September 2016, last accessed: 07 October 2016.
- [120] FAU, “One in two users click on links from unknown senders,” <https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/>, August 2016, last accessed: 07 October 2016.

- [121] M. Bada, A. Sasse, and J. R. Nurse, “Cyber Security Awareness Campaigns: Why do they fail to change behaviour?” *Report*). *Global Cyber Security Centre*, 2014.
- [122] D. Bradbury, “Why cybersecurity awareness is failing,” <http://www.sector.ca/blog/why-cybersecurity-awareness-is-failing-classiclecturedoesnothelp>, April 2014, last accessed: 28 March 2016.
- [123] D. A. Norman, “Design rules based on analyses of human error,” *Communications of the ACM*, vol. 26, no. 4, pp. 254–258, 1983.
- [124] G. Keinan, “Decision making under stress: scanning of alternatives under controllable and uncontrollable threats.” *Journal of personality and social psychology*, vol. 52, no. 3, p. 639, 1987.
- [125] A. Tversky and D. Kahneman, “Judgment under uncertainty: Heuristics and biases,” *science*, vol. 185, no. 4157, pp. 1124–1131, 1974.
- [126] L. E. Williams and J. A. Bargh, “Experiencing physical warmth promotes interpersonal warmth,” *Science*, vol. 322, no. 5901, pp. 606–607, 2008.
- [127] C. A. Anderson, “Temperature and aggression: ubiquitous effects of heat on occurrence of human violence,” *Psychological bulletin*, vol. 106, no. 1, p. 74, 1989.
- [128] A. Cheema and V. M. Patrick, “Influence of warm versus cool temperatures on consumer choice: A resource depletion account,” *Journal of Marketing Research*, vol. 49, no. 6, pp. 984–995, 2012.
- [129] E. R. Thompson, “Development and validation of an international english big-five mini-markers,” *Personality and Individual Differences*, vol. 45, no. 6, pp. 542–548, 2008.
- [130] J.-L. B. Ginka Toegel, “How to become a better leader,” <http://sloanreview.mit.edu/article/how-to-become-a-better-leader/>, March 2012, last accessed: 03 april 2016.
- [131] I. B. Weiner and R. L. Greene, *Handbook of personality assessment*. John Wiley & Sons, 2011.
- [132] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, “Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 373–382.

- [133] A. Darwish, A. Zarka, and F. Aloul, "Towards understanding phishing victims' profile," in *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on*. IEEE, 2012, pp. 1–5.
- [134] S. Srivastava, O. P. John, S. D. Gosling, and J. Potter, "Development of personality in early and middle adulthood: set like plaster or persistent change?" *Journal of personality and social psychology*, vol. 84, no. 5, p. 1041, 2003.
- [135] P. Costa Jr, A. Terracciano, and R. R. McCrae, "Gender differences in personality traits across cultures: robust and surprising findings." *Journal of personality and social psychology*, vol. 81, no. 2, p. 322, 2001.
- [136] T. Grance *et al.*, "Computer security incident handling guide (NIST special publication 800-61). Gaithersburg, MD: Computer Security Division," *Information Technology Laboratory, National Institute of Standards and Technology*, 2004.
- [137] P. Kral, "The incident handlers handbook," 2011.
- [138] D. Bisson, "Sony hackers used phishing emails to breach company networks," <http://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/>, April 2015, last accessed: 17 april 2016.
- [139] Fireeye, "Cyber attacks on the Ukrainian grid: What should you know," <https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf>, 2016, last accessed: 17 april 2016.
- [140] L. Spitzner, "Getting support and approval for phishing assessments," <https://securingthehuman.sans.org/blog/2014/03/12/getting-support-and-approval-for-phishing-assessments>, May 2014, last accessed: 05 april 2016.
- [141] M. K. Al-Hamar, "Reducing the risk of e-mail phishing in the state of qatar through an effective awareness framework," Ph.D. dissertation, © Mariam Khalid Al-Hamar, 2010.
- [142] A. J. Ferguson, "Fostering e-mail security awareness: The West Point carronade," *Educase Quarterly*, vol. 28, no. 1, pp. 54–57, 2005.
- [143] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Protecting people from phishing: the design and evaluation of an embedded training

email system,” in *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2007, pp. 905–914.

- [144] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, “Going spear phishing: Exploring embedded training and awareness,” *Security & Privacy, IEEE*, vol. 12, no. 1, pp. 28–38, 2014.
- [145] 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*. ACM, 2007, pp. 141–148.
- [146] U. S. C. O. APPEALS, “ United States Court of Appeals for the Federal Circuit: 02 - 1243 ,” [https://e-foia.uspto.gov/Foia/RetrievePdf?system=FCA&flNm=02-1243\\_1](https://e-foia.uspto.gov/Foia/RetrievePdf?system=FCA&flNm=02-1243_1), January 2003, last accessed: 27 april 2016.
- [147] J. Tehranian, “Infringement nation: Copyright reform and the law/norm gap,” *Utah Law Review*, vol. 2007, p. 537, 2007.
- [148] Facebook.com, “Statement of rights and responsibilities,” <https://www.facebook.com/terms.php>, January 2015, last accessed: 27 december 2016.
- [149] eBay.com, “eBay User Agreement,” <http://pages.ebay.com/help/policies/user-agreement.html>, last accessed: 27 december 2016.
- [150] Salesforce, “SaaS: Software as a Service,” <https://www.salesforce.com/saas/>, last accessed: 23 april 2016.
- [151] TrustedSec, “The Social-Engineer Toolkit (SET) ,” <https://www.trustedsec.com/social-engineer-toolkit/>, last accessed: 23 april 2016.
- [152] P. Frenzy, “About,” <https://www.phishingfrenzy.com/about>, last accessed: 23 april 2016.
- [153] M. Cova, C. Kruegel, and G. Vigna, “There is no free phish: An analysis of" free" and live phishing kits.” *WOOT*, vol. 8, pp. 1–8, 2008.
- [154] “Getting started,” [https://www.phishingfrenzy.com/resources/getting\\_started](https://www.phishingfrenzy.com/resources/getting_started), last accessed: 07 april 2016.
- [155] Apache, “Log files,” <https://httpd.apache.org/docs/2.4/logs.html>, last accessed: 23 april 2016.



- [156] “Installing Phishing Frenzy on Ubuntu Linux,” [https://www.phishingfrenzy.com/resources/install\\_ubuntu\\_linux](https://www.phishingfrenzy.com/resources/install_ubuntu_linux), last accessed: 07 april 2016.
- [157] “What is Docker,” <https://www.docker.com/what-docker>, last accessed: 07 april 2016.
- [158] “Action Mailer basics,” [http://guides.rubyonrails.org/action\\_mailer\\_basics.html](http://guides.rubyonrails.org/action_mailer_basics.html), last accessed: 07 april 2016.
- [159] “Init script for Sidekiq with Rbenv,” <http://cdyer.co.uk/blog/init-script-for-sidekiq-with-rbenv>, last accessed: 07 april 2016.
- [160] “Configure Postfix to Send Mail using an external SMTP server,” <https://www.linode.com/docs/email/postfix/postfix-smtp-debian7>, last accessed: 07 april 2016.
- [161] J. Rivera, “Configuration of mail server to relay emails,” <http://askubuntu.com/questions/24575/configuration-of-mail-server-to-relay-emails>, February 2011, last accessed: 05 april 2016.
- [162] “SMTP don’t work when try to send mail from mail client,” <http://serverfault.com/questions/612159/smtp-dont-work-when-try-to-send-mail-from-mail-clinet>, July 2015, last accessed: 05 april 2016.
- [163] “Postfix rate limiting – Politeness goes a long way,” <http://steam.io/2013/04/01/postfix-rate-limiting/>, April 2013, last accessed: 07 april 2016.
- [164] Zeknox, “Thotcon 0x5 Phishing Frenzy,” <https://www.pentestgeek.com/presentations/thotcon-phishing-frenzy/>, May 2014, last accessed: 12 april 2016.
- [165] K. Jansson and R. von Solms, “Phishing for phishing awareness,” *Behaviour & Information Technology*, vol. 32, no. 6, pp. 584–593, 2013.

# Appendix 1 - Bulk e-mail sending pricelist







## Your Application, Our SMTP

Unlike typical email marketing services, our high volume BULK SMTP service lets you send emails from your own software/script/application server, email client or a combination of different sources. For distributions of several thousand to greater than **1,000,000 messages per month**, our high volume BULK SMTP services are highly scalable and competitively priced.

## Becoming a Client

In accordance with our **Zero Spam** Tolerance Policy, MMS's bulk email hosting is a tightly regulated service. Clients are expected to responsibly manage ISP abuse reports and follow **CAN-SPAM** guidelines. In addition, MMS researches potential clients and performs extensive due diligence to prevent abuse.

## SMTP Pricing

	Sends Emails per month	Monthly Price	Order Now
Plan 1	100000	\$50	 Buy now
Plan 2	300000	\$100	 Buy now
Plan 3	500000	\$150	 Buy now
Plan 4	1000000	\$200	 Buy now
Plan 5	3000000	\$300	 Buy now
Plan 6	Unlimited	\$500	 Buy now

- 1. One Dedicated IP (*free ip replacement if become blacklist*).

Figure 18. Bulk e-mail sending pricelist [8]

## Appendix 2 - Postfix configuration file

Postfix configuration file `/etc/postfix/main.cf`

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version
```

```
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
```

```
#myorigin = /etc/mailname
```

```
smtpd_banner = myhostnameESMTPmail_name (Ubuntu)
biff = no
```

```
# appending .domain is the MUA's job.
append_dot_mydomain = no
```

```
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
```

```
readme_directory = no
```

```
# TLS parameters
```

```
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
```

```
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

```
# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.
```

```
mynetworks = 127.0.0.0/8 [::1]/128
```

```
#smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
smtpd_recipient_restrictions = permit_mynetworks
```

```
smtp_destination_concurrency_limit = 2
```

```
smtp_destination_rate_delay = 10s
```

```
myorigin = /etc/mailname
```

```
mydestination = $myhostname, localhost.$mydomain, localhost
relayhost =
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

## Appendix 3 - Email during preparation phase

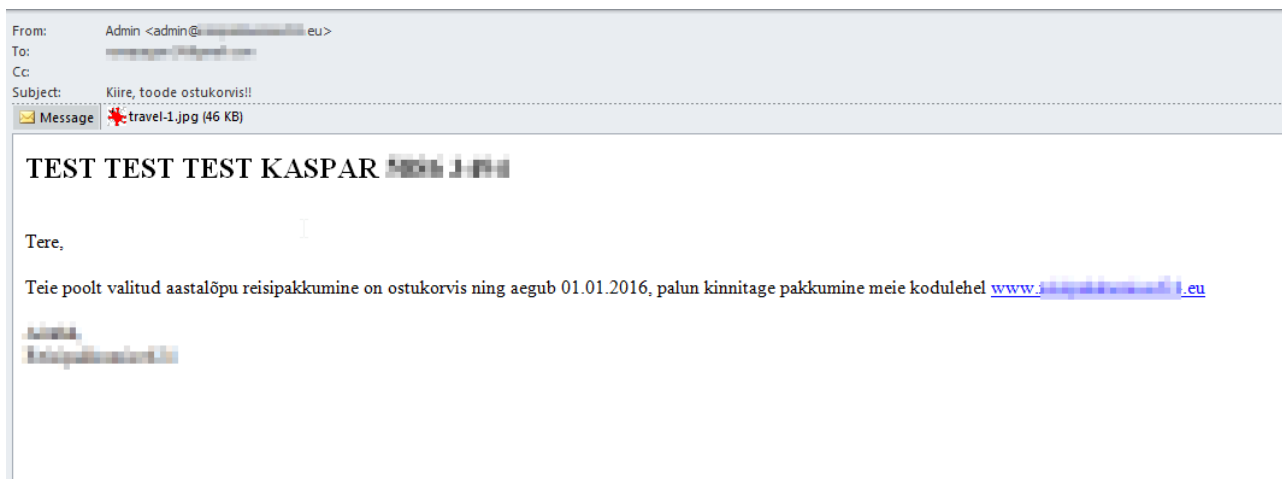


Figure 19. Email during testing period

S

Preparation e-mails in campaign 1

## Appendix 4 - Email design for assessment one

```
<html>  
<head>  
</head>
```

```
<body>
```

```
<br>
```

```
Tere, <br>
```

```
<br>
```

```
Teie poolt valitud aastalõpu reisipakkumine on ostukorvis ning aegub  
homme õhtul, palun kinnitage pakkumine meie e-poes <a href="<%= @url  
<%= ">www.domain.eu</a>
```

```
<br>
```

```
<br>
```

```
Aitäh, <br>
```

```
Company Name<br>
```

```
<br>
```

```
<br>
```

```
<br>
```

```
</body>
```

```
</html>
```

## Appendix 5 - HTML code of assessment one landing page

```
user@kasparubuntu:/var/www/phishing-frenzy/public/deployed/campaigns/22
$ cat index.php
```

```
<?php
// Turn off all error reporting
error_reporting(0);

if (isset($_GET['uid'])) {
    $uid = $_GET['uid'];
} else {
    header('404 Not Found', true, 404);
    echo "404 Page Not Found";
    exit();
}

function get_ip() {
    if (function_exists('apache_request_headers')) {
        $headers = apache_request_headers();
    } else {
        $headers = $_SERVER;
    }
    if (array_key_exists('X-Forwarded-For', $headers) &&
        filter_var($headers['X-Forwarded-For'], FILTER_VALIDATE_IP, FILTER_FLAG_IPV4)) {
        $the_ip = $headers['X-Forwarded-For'];
    } elseif (array_key_exists('HTTP_X_FORWARDED_FOR', $headers) &&
        filter_var($headers['HTTP_X_FORWARDED_FOR'], FILTER_VALIDATE_IP,
            FILTER_FLAG_IPV4)) {
        $the_ip = $headers['HTTP_X_FORWARDED_FOR'];
    } else {
        $the_ip = filter_var($_SERVER['REMOTE_ADDR'], FILTER_VALIDATE_IP,
            FILTER_FLAG_IPV4);
    }
    return $the_ip;
}
```

```

}

$password = $_POST['PasswordForm'];
$username = $_POST['UsernameForm'];

if ($password != '') {
    $creds = 'user:' . $username . ' password:' . $password;
}

$ip = get_ip();
$browser = $_SERVER['HTTP_USER_AGENT'];
$host = $_SERVER['HTTP_HOST'];
$url = "https://IP_address" . '/reports/results/';
$data = array('uid' => $uid, 'browser_info' => $browser, 'ip_address'
    => $ip, 'extra' => $creds);

// use key 'http' even if you send the request to https://...
$options = array(
    'http' => array(
        'header' => 'Content-type: application/x-www-form-urlencoded',
        'method' => 'POST',
        'content' => http_build_query($data),
    ),
);
$context = stream_context_create($options);
$result = file_get_contents($url, false, $context);
?>
<html>
<head>
<meta charset="UTF-8">
</head>

<br>
<h1> SEE OLI TEST</h1>

```



<hr>

<br>

<p><strong> Sa langesid e-posti teistründe ohvriks. Teeseldes küberkurjategijat, saatis infoturbejuht kõikidele töötajatele samasuguse kirja, kus link, millele Sa Outlookis vajutasid, oli osa testist. Sinu arvutiga on kõik hästi, kuigi, kui see oleks olnud tegelik rünne, võinuks Sinu arvuti nakatuda viirusega. Paar olulist punkti mida meeles pidada:</strong></p>

<ol>

<li> Linkide ja manuste avamine võib olla ohtlik. Kui kiri on kummaline või kahtlustäratav, saada see infoturbejuhile.</li>

<li> Petukiri soovib reageerida kiiresti.</li>

<li> Petukirjas ei ole mainitud Sinu nime.</li>

<li> Petukirja saatjaks võib kuvada keda iganes. </li>

<li> Aseta hiire nool Outlookis olevale lingile nii, et Sa <b>linki ei vajuta</b>. Kui e-kirjas olev silmaga nähtav link (www.rdomain.eu) ei ühti lingiga, mis tuleb nähtavale kui hiire nool lingi peale asetada (http://IP\_address/index.php?uid=xxxxxx), on tegemist petukirjaga.

<br><br>



</li>

</ol>

</body>

</html>

## Appendix 6 - Email design for assessment two

```
<html>
<head>
</head>
<body>
<br>
Tere , <br>
<br>
Mul on sinu abi vaja järgmise ringi kärpekavaga. Panin selle ülesse
  <a href="<%=□@url□%"> http://domain.ee/dokumendihaldus/
  page.aspx?pageId=126452
</a> , et saaksid sellele ligi.
Palun vaata see üle ja esita oma märkmed homseks enne kella 14:00.
<br>
<br>
<br>
Lugupidamisega ,<br>
Name<br>
Nõunik<br>
Department<br>
Ministry<br>
Telephone
<br>
<br>
<br>


---


<br>
This e-mail has been checked for viruses by Avast antivirus software.
<a href>https://www.avast.com/antivirus</a>

</body>
</html>
```