UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Lejla Islami

Assessing generational differences in susceptibility to Social Engineering attacks. A comparison between Millennial and Baby Boomer generations.

Master's Thesis (30 ECTS)

Supervisor(s): Olaf Manuel Maennel, PhD
Raimundas Matulevicius, PhD

Tartu 2018

Assessing generational differences in susceptibility to Social Engineering attacks. A comparison between Millennial and Baby Boomer generations.

Abstract:

In the age of digital society Social Engineering attacks are very successful and unfortunately users still cannot protect themselves against these threats. Social Engineering is a very complex problem, which makes it difficult to differentiate among vulnerable users. These attacks not only target young users or employees, they select massively, regardless of the users' age. Due to the rapid growth of technology and its misuse, everyone is affected by these attacks, everyone is vulnerable to them (Purkait, 2012; Aggarwal et al., 2012). Users are considered the "weakest link" of security (Mohebzada et al., 2012; Mitnick and Simon, 2011) and as such, protecting confidential information should be the ultimate goal of all people. However, despite the fact that a number of different strategies exists to educate or train endusers to avoid these attacks, they still do, phishing still succeeds (Dhamija et al., 2006). This is mainly because the existing security awareness trainings, theoretical courses, or frameworks are expected to be equally effective for all users regardless of their age, but experience has shown that this is not true (Alseadoon, 2014). In order for these security trainings to be effective, it is essential that they are composed based on the Social Engineering security weaknesses attributed differently to different generations. Identifying unique characteristics (demographic and personality) of generations, determinants of their vulnerability is what this work aims to do. Then frameworks crafted based on that information (addressing these weaknesses) would be of use and worth implementing. Therefore, taking into consideration the complexity of this problem, this study suggests that there is a need to research it from a broader perspective, adding the "generation" element into the study focus to find out if there is indeed any difference in susceptibility among generational cohorts. In order to do so, this research will adapt both qualitative and quantitative methods towards reaching its objectives. Collected-data of users' performance in a phishing assessment are analyzed and psychological translation of results is provided. Thus, the first research question seeks to address what factors determinate endusers vulnerability to Social Engineering, and results from quantitative data (statistical analysis) show that generation is an important element to differentiate potential victims of Social Engineering, whilst computer-efficacy or educational level do not play any noteworthy role in predicting endusers' likelihood of falling for these threats. In consistency with the above elements and previous studies, also gender is shown no potentiality in predicting susceptibility (Parsons et al., 2013). The second research question deems to explain what makes generations differ in susceptibility and this study's findings propose that generation Y personality traits such as consciousness, extraversion and agreeableness are key influencers of their shown vulnerability. Finally, along with establishing strong foundations for future research in studying generations susceptibility to Social Engineering, this thesis employ these findings in proposing a framework aiming to lessen millennial likelihood to Social Engineering victimization. The originality of this study lies on its overall approach: starting with an exhaustive literature review towards identifying factors impacting generations' susceptibility level, then statistically measuring their vulnerability, to finish with a solution proposal crafted to suit the observed generational security weaknesses.

Keywords:

Social Engineering attacks, Phishing susceptibility, Millennial, Security awareness, Generational cohort, Baby Boomer.

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

Põlvkondade erisuste hindamine sotsiaalse manipuleerimisrünnetega (Social Engineering attacks). Y-põlvkonna (millennial) ja beebibuumi ajastul sündinud põlvkonna võrdlus.

Lühikokkuvõte:

Digitaalse ühiskonna ajastul on sotsiaalse manipuleerimise ründed (social engineering attacks)väga edukad ja kahjuks kasutajad ei suuda ennast selliste rünnakute vastu kaitsta. Sotsiaalne manipuleerimine (social engineering) on keeruline probleem, mistõttu on väga raske eristada kõige kaitsetumaid kasutajaid. Sellised ründed ei ole suunatud ainult noorte ja töötajate vastu, vaid on laiaulatuslikud sõltumata vanusest. Tehnoloogia kiire kasvu ja selle ebasihipärase kasutamise tõttu on kõik selliste rünnakute poolt mõjutatud, kõik on haavatavad (Purkait, 2012; Aggarwal et al., 2012). Kasutajaid peetakse turvalisuse "nõrgimaks lüliks" (Mohebzada et al., 2012; Mitnick and Simon, 2011), ja seega konfidentsiaalse info kaitsmine peaks olema kõikide inimeste eesmärk. Hoolimata sellest, et on olemas erinevaid lahendusi kasutajate koolitamiseks selliste rünnakute vältimiseks, andmepüük on jätkuvalt edukas (Dhamija et al., 2006). See on eelkõige seetõttu, et küberteadlikkuse koolitused, teoreetilised kursused või raamistikud eeldatakse olevat võrdselt efektiivsed kõikidele kasutajatele vaatamata nende vanusest, kuigi kogemus näitab et see ei ole tõsi (Alseadoon, 2014). Selleks, et koolitused saaksid olla efektiivsed, on oluline et need on koostatud lähtudes sotsiaalse manipuleerimise turvanõrkustest, mis on erinevatel vanusegruppidel erinevad. Käesoleva töö eesmärgiks on põlvkondade unikaalsete tunnuste (demograafilised ja isikulised) ja nende haavatavuste faktorite määratlemine. Sellealusel on loodud raamistik, mis on võimalik rakendada ja mis addresseerib neid nõrkusi. Arvesse võttes probleemi keerikust, käesolev uurimistöö näitab, et on vaja läbi viia edasisi uurimusi laiemast perspektiivist lähtuvalt lisades "põlvkondade" elemendi uurimiseesmärkidesse, et kas on erinevusi haavatuse riskide osas läbi põlvkondade. Käesolev uurimistöö kasutab nii kvalitatiivseid kui kvantitatiivseid meetodeid eesmärkide saavutamiseks. Andmekogumise rünnaku efektiivsuse hindamisel analüüsitakse kasutajate käitumist ning antakse sellele psühholoogiline tõlgendus. Esimene uurimisküsimus keskendub sotsiaalne manipulatsiooni haavatavuse faktorite määratlemisele ja kvantitatiivsed andmed (statistiline analüüs) näitab, et põlvkond on oluline element potentsiaalsete sotsiaalse manipulatsiooni ohvrite eristamisel, kusjuures arvutikasutusoskus ja haridustase ei määra olulist rolli hindamaks kasutajate tõenäosust langeda selliste rünnakute ohvriks. Eelpool toodud faktorite ja ka eelnevate uuringute alusel, ei ole ka sugu määrav faktor haavatuvuse ennustamisel (Parsons et al., 2013). Teine uurimisküsimus püüab selgitada, mis põhjustab põlvkondade haavatuvuse erinevused ning uuringu tulemusel näitavad, et Y-põlvkonna isikuomadused, sh teadvus, ektravertsus, ja meeldivus on põhifaktorid mis mõjutavad haavatavust. Viimasena, lisaks tugeva aluse loomisel edaspidiseks põlvkondade haavatavuse uurimisel, pakub käesolev töö välja raamistiku, milles on eeltoodud leiud arvesse võetud ja mille eesmärk on vähendada Y-põlvkonna haavatuse vähendamine sotsiaalse manipuleerimise rünnakutele. Käesoleva magistritöö unikaalsus seisneb üldises lähenemisviisis: alates ulatusliku kirjanduse ülevaatega "põlvkondade" haavatavuse faktorite määratlemisega, statistilise analüüsiga

haavatavuste hindamiseks ja lõpetades lahenduse väljapakkumisega, mis aitab lahendada "põlvkondade" turvalisuse haavatavuse probleemi.

Võtmesõnad:

sotsiaalse manipuleerimise ründed, andmepüügi haavatavused, küberteadlikkus, põlvkondade kohort, y-põlvkond, beebibuumi ajastul sündinud põlvkond

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

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Motivation

In the digital age, technology has an unavoidable presence in the lives of people, they can now carry all of their everyday activities online: go shopping online, work online, vote online, in other words, all users now have another "residency" online. While involved in such online services they often forget or pay little attention to the security threats behind these activities. Users do not give equal attention to security, some lack doing it and become “easy prey” or favorite targets for the attackers. Their lack of attention towards these attacks is known as vulnerability or susceptibility, which is attributed differently to victims. Some authors claim that the current generation (a precise definition of what a generation is, is given by (Borges et al., 2006)) is extremely vulnerable to these attacks, (Alseadoon, 2014) although other studies have found their parents (older users) possess higher susceptibility rates to Social Engineering attacks. Therefore, it is essential to specify groups more vulnerable to these attacks.

In order to find out if there is any significant difference in the likelihood of falling victim to Social Engineering among generations, firstly it is necessary to identify factors which impact cohorts' vulnerability. Only then, it is possible to propose methods to reduce susceptibility of different groups to Social Engineering attacks, tailored specifically to their unique Social Engineering security weaknesses.

There are many works addressing reasons why users fall for Social Engineering attacks. For instance, some studies list lack of technology related knowledge at the top, while some others argue users' education as the most important factor. Thus, to mitigate their susceptibility to Social Engineering attacks as undoubtedly the most successful security attacks nowadays, this study seeks to first identify and understand these determinant factors on deeper grounds and then address them to determine the most appropriate defense strategy.

Social Engineering hereinafter SE, is considered to be "the act of manipulating a person to accomplish goals that may or may not be in the "target’s” best interest" (Hadnagy, 2010, p.32). From identity theft to financial losses, the damages that Social Engineering attacks bring both on individual and organizational scale are enormous. Phishing is the most commonly used form of Social Engineering attacks, there are around 150 million phishing emails sent every day stated in a study by Get Cyber Safe (2013).

Taking into consideration the dimensions of this problem it has been studied by previous works as well, where most researches focused on specific personality or demographic factors determining certain individual’s susceptibility to Social Engineering attacks and leaving the generational element fairly unaddressed. Furthermore, the literature has been studying users' phishing detection behavior and no attention (to the best of this thesis’ knowledge) has been given to generations, in terms of comparison of their vulnerability to Social Engineering attacks. What if there is indeed difference?

This thesis aims to properly address this question by assessing generations' real performance on Social Engineering attacks (particularly in phishing assessment). Moreover, a detailed focus to this problem is given in the following sections.

1.2 Research problem

Users exposing important credentials to attackers, is one of the biggest issues of security of today and many researchers believe that vigilance and education are the only ways to protect against Social Engineering as such (Aggarwal et al., 2012; Kumaraguru et al., 2007; Allen, 2006), since technology has demonstrated that it cannot do a lot in regards (Mitnick and Simon, 2011). **However, no matter how much SE education frameworks are composed or how many SE security trainings are implemented, this problem has still remained unsolved, people still fall for SE attacks, they are still considered the easiest potential victims of the security chain** (Purkait, 2012; Long, 2013). Therefore, the main reason why Social Engineering attacks are more successful than other security attacks, is because they target directly the human element since it is easier to manipulate people than technology (Mitnick, 2011). Mitnick and Simon explain that "cracking the human firewall is often easy, requires no investment beyond the cost of a phone call, and involves minimal risk" (2011, p. 4). In regards, previous works have lacked to cover all the reasons behind users' susceptibility, factors that influence their actual behavior when presented with actual Social Engineering attacks. Moreover, literature has a gap in identifying groups more vulnerable to Social Engineering attacks and understand each generation's SE security weaknesses.

This work will seek to find and propose the most adequate way to educate this "vulnerability link" not to be the easiest pray of these attacks via patching their SE security weaknesses.

For a proper approach towards the outlined problem, this thesis attempts to solve the following issues:

- Firstly, it identifies factors impacting generational groups' victimization to SE attacks.
- Then it assesses the differences in generational susceptibility via analyzing collected data from real-life performance on phishing assessment.
- Translation of statistical analysis findings to personality differences across the two generational groups is the next carried out step.
- Finally, it presents the most efficient SE security training program to fit the security requirements of specific generations.

1.3 Research questions

a. Is there any significant generational difference in susceptibility to Social Engineering attacks?

This research claims to assess the response of this question by quantitatively examining data collected from real phishing attack assessment. Statistical analysis is used to reveal any potential distinction in vulnerability among generational groups, along with providing a clear panorama of their actual likelihood of victimization. Nowadays, many organizations complain of the current generation, or young people of today born between 1982 and 2002 (Howe and Strauss, 2009), claiming that they are extremely vulnerable to SE threats (due to their distinct personality traits and heedless behavior) and that could put every organization into great security risks making organizations more and more unwilling to hire them. Is there indeed such a contrast in SE vulnerability among them or is it all overhyped?

b. What factors impact generational groups susceptibility to SE?

Demographic factors are proven to indicate users tendency to respond to Social Engineering risks with many researchers suggesting women to be more susceptible than men (Janet et al., 2008) or others have found age group 18-25 more likely to become victims of these attacks. Besides age and gender, users scoring higher in computer-efficacy are inclined to defend from phishing (Parrish et al., 2009). On the other side, also Big Five model's personality traits are claimed to be important factors to differentiate among groups, thus understanding their impact on generations' possibility to SE victimization is trivial. Literature has shown that different cohorts share unique characteristics and attitudes (Sessa et al., 2007; Wey Smola and Sutton, 2002), even talking about security. Thus, these qualities affect their actual behavior (Coomes and DeBard, 2004) and at the same time are key to explain users' tendency of becoming victims of phishing attacks (Parrish et al., 2009). This thesis will dig deeper into understanding each of these factors' correlation with vulnerability to SE threats, in terms of determining their role in predicting the more susceptible groups. For instance, would a phishing attack affect equally one teenager who shows an over-sharing attitude on SNS, and a Baby Boomer who does not share the same weakness? Does Social Engineering have the same success rate in groups scoring differently on agreeableness trait?

c. How to craft the best solution to reduce cohorts vulnerability to Social Engineering threats?

The final contribution of the author to complete this research as a whole, is to propose the most proper strategy to mitigate generational groups' found susceptibility based on their specific SE security needs and requirements. After identifying the generational cohort most vulnerable to these risks and listing its SE unique security weaknesses, it is meaningful to explore the most appropriate defense meeting all the covered issues throughout this research. The solution is thought to be planned matching the necessary behavior skills to the targeted audience based on their SE needs and weaknesses. Thus, the thesis aims to design a solution based on the CIA triad principles via balancing both attackers' and targets' motivation (note that end users are not motivated to protect themselves from Social Engineering). The originality and the value of the solution is tied to its main objective: train the enduser through motivation.

1.4 Significance of the study and contribution

Considering it an essential starting point in deploying the most adequate solution to mitigate users vulnerability, **this thesis proposes a new way to differentiate potential victims of Social Engineering attacks based on generational cohorts**.

This work strongly assumes that the existing frameworks fail to educate users against Social Engineering due to their generalized attribution or the wrong "tailoring" they give to all endusers, pretending equal effectiveness regardless of their security differences. Therefore, this thesis claims that via understanding and explaining how generational cohorts differ in perceiving Social Engineering risks (in terms of unique factors which make them fall for these attacks), it is easier to build up better mitigation methods or education frameworks to help lessen their susceptibility**.**

Thus, the next contribution of the author is emphasizing the importance of crafting unique SE mitigation strategies for every generational cohort (and not only) attempting to patch specific security weaknesses each group owns.

Then, this thesis' effort in comparing different generational groups' actual vulnerability to social engineering attacks to find out if there is any noteworthy difference they share, is considered its main contribution.

To achieve these goals, a great focus is given to identification of generations' factors influencing their likelihood to become potential victims. Hence, the first task is to **identify** and **analyze** different generations' specific personality attributes that play an important role in determining their degree of susceptibility with a systematic literature review performed. The second task is statistical analysis of the collected dataset from real phishing assessments. At the end as a full-packet, a defense strategy approaching findings is proposed.

Briefly, the specific contribution is to:

- explain the importance of measuring generational differences in vulnerability to Social Engineering attacks.
- explore the best way to measure generations' actual susceptibility.
- identify factors influencing cohort-groups' possibility to fall victims to SE attacks.
- measure susceptibility via statistical analysis of the phishing collected-dataset.
- explain found susceptibility difference across groups.
- propose solutions to reduce the generational gap in vulnerability level.
- propose future directions complying with this work's findings and implications.

Moreover, the ability to identify groups more vulnerable to Social Engineering attacks should benefit the literature considerably in pursuing further research in mitigating these attacks and reducing the damages they bring. On the other side, this work can also be a big assistance to organizations as well since knowing your employees' weaknesses and vulnerability level is translated to risk assessment done to them. To this thesis best of knowledge no previous study has empirically examined the difference in susceptibility to Social Engineering attacks across these two specific generations.

1.5 Thesis Outline

The thesis is composed of 7 chapters.

- Chapter 1- Introduction- This chapter introduces the general background, its motivation, the research focus and research questions.
- Chapter 2- Definitions - This chapter explains further the core concepts of this thesis and gives an overview how the literature has defined them.
- Chapter 3 - Related Work- It performs an exhaustive literature review via analyzing the different approaches taken by previous works on the same topic.
- Chapter 4 - Methodology- It explains the theoretical framework and the research methodology used in this study.
- Chapter 5 - Implementation - This chapter focuses on carrying out a statistical analysis of the phishing assessment dataset and results are presented.
- Chapter 6 - Proposed Solution - It explains the found susceptibility differences among generations and outlines a solution proposal based on findings.
- Chapter 7 - Conclusion - At the end, this chapter concludes the research via a detailed presentation of results and discusses implications for future research to address.

2 Defining Terms

This chapter is mostly used to explain keywords crucial for this paper and discover how literature has defined them. Analyzing terms such as Social Engineering or security vulnerability in the context of this thesis is key before proceeding further. It also explains the core focuses of this thesis, the current generation (the millennial generation) and their parents (the Baby Boomer generation), seeking to gather more background knowledge on these subjects. Moreover, in this section abbreviations used throughout the thesis are explained.

2.1 Acronyms and Abbreviations

SE	Social Engineering
NIST	National Institute of Standards and Technology
BYOD	Bring your own device
SNS	Social Networking Sites
NDA	Non-disclosure Agreement
CSE	Computer Self-Efficacy
WWW	World Wide Web
ENISA	European Union Agency for Network and Information Security
SAE	Security Awareness Education
BB	Baby Boomer
Gen Yer	Generation Y member
Gen Xer	Generation X member
TUT	Tallinn University of Technology

2.2 Core Concepts

Security awareness is one of the core terms of this work and a specific definition of it is essential in order to clarify possible misconceptions. Unfortunately, literature still lacks a precise definition of this term (Hänsch and Benenson, 2014) thus, researchers have come up with their own definitions implementing different approaches. Having said that, Hänsch and Benenson (2014) have carried out a deep systematic study in getting the definition of the term. They propose 3 different aspects of it to be defined: security awareness as perception, as protection and as behavior. Paying particular attention to all three categories, they emphasize the fact that users should know that danger exist and also how

to protect themselves against it. Similar to other papers, Shaw et al., differentiate between awareness programs and trainings (2009). They define security awareness as a combination of "perception, comprehension and projection" (2009, p.1). Amankwa et al., state that information security awareness is "any endeavor to focus employees' attention on information security in order to ensure that all employees understand their roles and responsibilities in protecting the information that is in their possession by using print or electronic media" (2014, p.3). However, there are other works that propose that security awareness aims to change behavior towards Social Engineering threats (Winkler and Manke, 2017).

Actually, there is no "right" or "wrong" security awareness (Hänsch and Benenson, 2014), but in this paper Social Engineering awareness is defined **as a combination of knowledge and attitude towards Social Engineering threats. To put it simply, it is the actual behavior users present towards real Social Engineering attacks.**

Social Engineering is the most crucial term to be defined as the main focus of this thesis. It is interesting to know that even users that almost do not have any relation to technology at all understand that Social Engineering is a problem and as such, it should be solved. A simple search on Wikipedia precisely highlights it being "psychological manipulation of people into performing actions or divulging confidential information". One of the creators of the http://www.social-engineer.org, Hadnagy deeply explains all the consecutive phases of Social Engineering attacks and the idea of persuasion behinds it (2010). Furthermore, Allsopp states that Social Engineering is "obtaining of confidential or privileged information by manipulating legitimate sources" (2010, p.51). Regarding the way how Social Engineering attacks are carried out, the traditional template is described in detail by Snyder (2015), explaining all phases from information gathering to persuasion.

There is an enormous number of definitions for Social Engineering, but the one to best fit this paper's perspective is **"the act of manipulating a person to accomplish goals that may or may not be in the "target's" best interest"** (Hadnagy, 2010, p.32).

In light of this thesis' aim, **phishing** is the next term that should be aptly defined. Actually, there are many disagreements among authors while categorizing phishing**,** as many of them do not consider it a form of Social Engineering attack (Snyder, 2015). However, definitions given to this term are very similar, even by quoting Wikipedia: "phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in electronic communication"(Wikipedia, 2017) one can get the idea behind it. In the context of this thesis it is described as: **a method used by cybercriminals to steal mostly login-credentials or other relevant information by camouflaging emails to look legal for mainly financial fraud or identity theft** (Alghamdi, 2017). Phishing attacks mostly deploy tricking techniques (sophisticating day by day) and different mediums (mainly emails or social networking sites) to make users give up personal information. Phishing attacks are not solely damaging end users by making them phish out log-in information or install malware on their computers (Hong, 2012), but can also ruin an organizations' reputation together with tremendous monetary losses. As far as users lack the proper security behavior in regards, phishing will continue being a step ahead of the current attempts to protect endusers against it.

Susceptibility to Social Engineering attacks is the likelihood that a person will respond to and become victim of a real Social Engineering attack. Others have also proposed similar definitions, defining it as "the inability of users to suspect a phishing email" (Alseadoon, 2014, p.67). A different aspect is defined by Parrish et al., though, in context

of phishing it is the time to respond to such attack or the time calculated that a person will interact with the attacker (the hook) (2009). **It is the state of being inclined to respond to a SE attack.**

Millennials are actually called people of the current generation or the first generation of the new millennium. Born and raised in the times of digital technology and social media, they are the first "always connected" generation (Palfrey and Gasser, 2011; Prensy, 2001). Many different categorizations exist regarding this generation's starting period, but in this study's scope it is from or after 1982 to the early 2000s (Howe and Strauss, 2009). Actually, there are also different points of view regarding this generation's endpoint, as there are researches that argue that millennials are still being born (Donnison, 2007). However, it is noticed that most of the studies use the span of 18-25 years to categorize them. Literature has called them by different nicknames: the Net Generation (Braber, 2016; Becker, 2015), digital natives (Stringfellow Otey, 2013; Palfrey and Gasser, 2011), Generation Y (Hurst and Good, 2009), Nexters (Ng et al., 2010) or Nexus Generation. All these labels are coined due to them being highly technology or internet-competent and the fact that they have a strong multitasking and BOYD attitude in their workplace. It is claimed they trust the virtual world like no previous generation, and moreover lack attention of their working organization's cyber security policies. It is also argued that users of age 18-25 are more susceptible to phishing attacks than older age-groups (Pattinson et al., 2012; Sheng et al., 2010). On the other hand, many researchers claim that this generation's members are more aware of phishing attacks due to being computer-savvy users. A detailed overview of the Millennial generation's unique qualities related to SE security awareness compared to the particular traits of the previous generation is presented in the following chapter.

On the other side are the **Baby Bommers**, the other studied subject of this thesis. People of this generation are born between 1946-1964 (Kumar and Lim, 2008). According to Borges et al., they have higher self-reliance than millennials (2006). Current literature has called them immigrants of the digital world (Jiang et al., 2016). In comparison to digital natives (current generation members) who have grown up with computers and the Internet, they "learned how to use email and social engineering late in life" (Palfrey and Gasser, 2011, p.4). Millennial, Baby Boomer, digital natives and digital immigrants or other alike terms are used interchangeably throughout this study.

2.3 Studied Subjects

As stated in the introduction as well, this study extends its concentration on two particular generational groups: Millennials and Baby Boomers. Actually, selecting solely these two generations to focus on, is not purposeless. The main motivation behind this choice, is due to the conflicting notions: digital natives v. digital immigrants. Comparing one cohort that has grown up with the internet being always there with a cohort group which learned to use the internet later on life (Palfrey and Gasser, 2011) and understanding this difference in respect to falling for Social Engineering attacks is trivial.

Secondly, this thesis is focused only on these two specific groups as they cover most of the today's workforce. Moreover, in the nearest future the boomers will retire and millennials will take over the workforce by making up the biggest percentage in the workforce (80% by end of 2020). Thus, it is a must to find out their susceptibility in comparison to the previous generations in the workforce, then organizations will know what to expect and

what to consider while crafting security policies. Here it is also safe to mention the organizations' recent unwillingness to hire employees of Generation Y due to the claims that they are much more likely to fall for these attacks. To aid the understanding of organizations' reluctance, it is crucial to seek out the real truth, their degree of vulnerability to falling for Social Engineering attacks.

Then, having experienced different historical events, they do not differ only on age, but also on personality which has relevant ramifications on their Social Engineering attitude and behavior. For instance, their SE security perception: the millennial generation consider themselves more protective to these threats compared to boomers and vice versa. It is relevant to study their perceptions towards these attacks in general and to identify their actual degree of susceptibility. Furthermore, sharing a strong relationship among them (parent-child) and having lived in two different societies (millennials are the internet kids), it is interesting to find out their SE security weaknesses.

On the other side, there exist many inconsistencies in generations starting dates (Solnet et al., 2012) (many researchers conflict on categorizing cohorts years span). Risking to lead to a possible generational overlap because of this reason, this study left out of its focus the generation in between the Baby Boomer and the Millennial generations (Generation X). As such, this research assumes a more precise differentiation among the targeted cohorts in regards to their vulnerability to Social Engineering.

Finally, the previous literature has claimed that specifically these two cohorts differ the most in terms of security awareness, it is time to solve this dilemma, do they indeed?

2.4 Summary

This chapter has identified and explained the main concepts of this work, defining them in the context of the studied problem. It discusses the central subjects of this thesis: the Boomers and Millennials and specifies the reasons why does it matter to direct the research on these particular generations. Furthermore, the list of abbreviations used throughout the thesis is provided here.

3 Related Work

In this chapter an exhaustive research on the current literature is carried out to help identify the relevant papers conducted on this topic, to help explain the academic context pursued towards writing this thesis. The way it approaches the previous research is via a systematic and exhaustive literature review, considering the research questions to be answered (Armitage and Keeble-Allen, 2008). Hence, many online libraries and other repositories are used as sources to gather previous related works. In order to find studies pertinent to this thesis focus, a combination of keywords such as : social engineering, phishing, vulnerability, susceptibility, millennial and generational cohort is used for the searching phase. Papers are then gathered for a brief abstract reading, to select the ones noteworthy for this thesis. As a matter of fact, this chapter identifies and digests factors proposed by current literature determining users' degree of vulnerability to analyze them later in the next chapter. It seeks to find out to which group the literature has coined the term "easy prey of SE attacks", to digital natives or to their parents? Apart from that, it seeks to understand reasons why standard trainings or awareness increasing materials have limited effect in reducing users' vulnerability.

3.1 Identifying factors impacting users' vulnerability

To defend from Social Engineering attacks organizations assign a considerable budget to protective measures such as technology or employees security trainings. However, due to different reasons they fail to properly protect their assets from these types of attacks. Thus, many researchers have addressed the problem of Social Engineering as an area of particular concern in terms of finding out what makes its attacks so successful.

One of the most explicit approaches to this question is taken by Dhamija et al., trying to understand why phishing works (2006). The answer to this question seems easy though: security is not the main concern of people (Purkait, 2012). Most of the researchers somehow ring the alarms, stressing that "Users are not motivated to learn about security; for most users, security is a secondary task" (Kumaraguru et al., 2010, p.1). Although, this is not that superficial since there are many other reasons behind this heedlessness, weaknesses that social engineers wisely exploit. What particular factors predict users' vulnerability to SE attacks?

Lack of knowledge related to Social Engineering in particular or technology in general is said to be one key factor influencing users' susceptibility. Literature uses the term computer self-efficacy (CSE) meaning in other words, the users' capability to successfully use computers (Compeau and Higgins, 1995). Dhamija et al., in their work explain that people lack the adequate knowledge to understand how operating systems, email or the entire web works and, phishing criminals exploit this weakness to get what they need. Furthermore, many endusers ignore security warnings because they find them technically difficult to understand (2006; Wu et al., 2006), and they risk more falling for phishing attacks. Along these lines, Downs et al., suggest a more detailed understanding of the web as such, could reduce vulnerability (2007). Therefore, technology sophistication decreases individuals' phishing susceptibility (Wright and Marett, 2010) since users' showing high computer knowledge tend to doubt more the authenticity of everything online (Wright et al., 2010).

However, deficiency in knowledge regarding technology is not the only factor influencing users' likelihood to become potential victims of SE attacks, their lack of awareness is another vital element (Aburrous et al., 2010; Wright and Marett, 2010). With Social Engineering attacks evolving day-by-day, users should be aware how to protect against and not simply know that they exist. The wrong decisions people usually make when faced with real phishing attacks are mainly due to their lack of awareness, demonstrating once more the great necessity of efficient phishing awareness trainings to deploy (Aburrous et al., 2010). Although, a contrary approach is assessed by Halevi et al., who disagree to translate users' susceptibility to lack of awareness (2015) since experience have shown that regardless possessing phishing awareness, many users yet fall for phishing attacks in great terms (Alseadoon, 2014).

"Big Five" personality model, made up of traits such as openness, conscientiousness, extraversion, agreeableness and neuroticism (Gosling et al., 2003) are found to be notable predictors of human behavior (Jagatic et al., 2007), and potential determinants of individuals' vulnerability to Social Engineering attacks (Uebelacker and Quiel, 2014; Halevi et al., 2013). Addressing the relation of personality and phishing email response, many studies have proposed neuroticism the trait mostly associated with responding to phishing emails (Halevi et al., 2013; Cho et al., 2016). Furthermore, Cho et al., on their study developed a mathematical model aimed to predict what personality elements are indicators of social engineering vulnerability and found that agreeableness and neuroticism have remarkable effects on decision performance (2016). However, in another work Halevi et al., via real-life spear-phishing attacks conducted in their study targeted conscientiousness the most relevant trait to determine phishing susceptibility (2015). On the other side, Parrish et al., suggest that extraversion in context of phishing could lead to increased vulnerability (2009). Supporting the same findings, Workman explains that extraversion is considerably related to high effective commitment, making users divulge personal information as they want to fit to some particular group (2008). Moreover, people's ability to detect deception is directly influenced by their emotions (Forgas et al., 2008) and characterized by positive emotions, extraverted people may easily fall for phishing while processing emails (Alseadoon et al., 2012). Parrish et al., in their work were focused mainly on trust as one of the main aspect of agreeableness and found it to be the strongest personality characteristic influencing peoples' susceptibility (2009; Modic and Lea, 2012). While users' phish out sensitive information, trust is highly involved (Weirich and Sasse, 2001).

It is known that Social Engineering attacks become even more successful when criminals are armed with enough information about targets beforehand, and social networks are the perfect repositories to provide such information. SNSs are recently converted into dangerous weapons in the hands of social engineers who may take criminal actions towards damaging endusers. In the same line with these studies Vishwanath et al., in their work implemented a research model to explain factors that best predict an individual's possibility to get phished, and apart from technological efficacy and email load, suggest also media habits as a major contributor to Social Engineering susceptibility (2011). With internet being no longer limited to anyone, people often just want to explore the online world but unfortunately happen to expose themselves to phishing (Furnell, 2010), mainly due to the over-sharing attitude on social media. Defining self-disclosure as personal-relevant information exchanged online in this paper's context, it is said to be a very dangerous asset in help of so-called social phishing attacks (Jagatic et al., 2007). As a matter of fact, Halevi et al., did the first work on studying the relationship among

personality, Facebook and phishing and found that people who tend to post more on Facebook are more vulnerable to privacy attacks (2013).

At the end, Mitnick and Simon quote: “as improvements are made in the technological weapons against security breaches, the social engineering approach… will certainly become significantly more frequent and attractive to information thieves” (2011, p. 259). It has passed a long time since then but unfortunately this statement is more accurate than never, Social Engineering attacks continue making the latest news and feasibly increase in the nearest future. This all means that there is still an enormous and rapid work that should be done in order to further study these and other factors influencing users' likelihood to become prey of Social Engineering attacks. In order to hopefully "patch" them in the nearest future it should further the investigations aiming to understand the human aspect of these semantic attacks. At the end of the day, this is not a problem with no solution, it is just a very complex issue. As Schneier quotes: "to target the people problem, not the math problem" (2000), these elements should be addressed and studied in deeper grounds and dimensions.

3.2 Millennials vs. Baby Boomers, who are more vulnerable?

Many researchers (Kumaraguru et al., 2009; Sheng et al., 2010; Workman, 2008; Dhamija et al., 2006; Alseadoon, 2014) agree that demographics explicitly impacts users' perceptions and decisions when dealing with phishing emails. Specifying solely "age" asset of demographics, they claim that it can anticipate users' likelihood to become potential victims. There are other works though, that found that user's demographic in general and age in particular, cannot predict users' vulnerability to phishing attacks (Mohebzada et al., 2012; Long, 2013). Considering these contradictions, it is safe to clarify that different works carry out different approaches to the division of age periods when categorizing groups and thus, may obtain distinct findings (Alseadoon, 2014).

Emphasizing the lack of research studying demographics in context of phishing susceptibility Sheng et al., argue that via knowing groups more susceptible to phishing, it is easier to concentrate into anti-phishing education (2010). This work is the nearest to this thesis's focus, not only in terms of analyzing groups more vulnerable to phishing attacks, but also in studying the psychology behind their great potential to fall for such threats. Moreover, they found that targets of age 18-25 fell mostly for the attack (Sheng et al., 2010).

Being born on the glorious times of Web 2.0, the members of net generation are used to the tremendous amount of information online, as a result they can handle and process it better than any other generation (Parment, 2013). Moreover, it is undoubting that people of current generation are great multi-taskers and tech-savvy and also, it is suggested that these qualities can decrease the possibility of getting phished or social engineered. However, even-though the millennial group possess these unique characteristics in high rates, they still fall for phishing, mainly because they overestimate themselves to be able to evaluate certain cues in phishing emails (Stebila, 2010). This implies that they consider themselves enough computer-efficient to defend against these threats but actually, they are equally likely to get phished as others less technically sophisticated. Alseadoon also, in his PhD dissertation found that young people aged 18-25 are more vulnerable to these attacks as they tend to be more risk-takers (2014). To support the same findings, other authors explain that young people of today yet lack the sufficient security awareness to protect

themselves from internet vulnerabilities (Boyd, 2007; Livingstone et al., 2005). The National Study of Youth and Religion, stated that almost 60% of millennials believe in their own greatness to be able to distinguish what is right or wrong in terms of security (Stein, 2013), overestimating the ability to protect themselves online compared to older users (Miltgen and Peyrat-Guillard, 2014; Jiang et al., 2016). This generation's members have narcissistic perceptions (Bergman et al., 2010) and entitlement attitude (Ng et al., 2010; Bauer, 2009) due to the excessive praise gained by their parents, the Boomers. Other noteworthy studies attain their focus on agreeableness and stated that more agreeable individuals are at a higher rate of security risk and generally, younger people and women present higher values of agreeableness (Darwish et al., 2012).

On the other hand, contrasting the above findings there are studies that have found that older adults lack awareness and knowledge concerning security more compared to younger users (Jiang et al., 2016). Therefore, in their work Jiang et al., analyze differences in SE behavior among 3 generations: the Silent Generation, older Baby Boomers and Millennials. Hence, an interesting fact noticed on their findings is the SE security perceptions the groups have for each-other, such that older adults defined Millennials reckless and more vulnerable to online threats, while Millennials claimed to attribute this weakness to older adults, considering themselves knowledgeable enough not to fall for these threats (Jiang et al., 2016). In context of media over-sharing habits previous studies have showed previous generations' members less likely to post personal information on Facebook compared to digital natives (Christofides et al., 2012) decreasing their scale of vulnerability.

Actually, there exist different approaches taken by researchers to find out user age-groups more likely to become potential victims of Social Engineering attacks and as a result, different findings are presented. Although, the findings are not proportional due to distinct directions purchased and differences in groups' age division. Accordingly, this explains the fact that there is no previous work (to the best of this thesis knowledge) that focuses on studying generational-groups differences in likelihood to fall for SE attacks.

3.3 Methods implemented to measure users' vulnerability

Proportional with users' increase in vulnerability to Social Engineering attacks, have been the proposed attempts to lessen it. Experience has shown that it cannot be reduced what is not calculated, as such the approach should start from measuring end-users' vulnerability to later be able to try to mitigate it. There are different methodologies proposed to measure users' susceptibility to phishing or Social Engineering attacks in general, researchers have suggested many possible ways starting from the real attack scenario assessments to cognitive processing tests. Therefore, Kumaraguru et al. proposed the Cognitive Reflection Test(CRT), as an efficient way to measure users' vulnerability to phishing. They found that people who scored high on the CRT were more likely to fall for phishing emails (2007; Jensen,1998).

On the other side, Kevin Mitnick suggests security assessment as the best way to test employees' susceptibility to Social Engineering attacks (Mitnick and Simon, 2009). Sharing the same proposal, Jakobsson et al., argue that real-life attack assessments not only explain potential extend of victimization but at the same time identify the kind of attacks working the most among end users (2008). Shifting the attention to organizations, Nohlberg also stresses that the best way to measure employees' security awareness is testing them when they do now know they are being tested (2005). However, researchers

emphasize the fact that those assessments should be ethically and legally complying with security policies (Jakobsson and Ratkiewicz, 2006). Moreover, SANS Institute also proposes security awareness survey as the adequate method to measure employees' awareness within an organization (also the best way to identify gaps in regards to security awareness) (SANS Institute, 2017).

Each of these methods have drawbacks, some arise in more accurate results and some lack it, some involve ethical issues or risks of data disclosure. For instance, it is claimed that some methods produce less reliable data and others, can easily put subjects at risk through exposure of sensitive data (Hale et al., 2015). Aiming to reduce endusers vulnerability, many researchers propose education and training to prevent people from falling for this attacks (Jakobsson and Myers, 2006; Downl et al., 2006). Taking into consideration the failure on teaching the individual not to fall for Social Engineering attacks, is seems like "security user education is a myth" (Gorgling, 2006).

3.4 Gaps in literature

As the problem of social engineering is escalating and techniques deployed by attackers sophisticating, it is vital to investigate further this issue of great concern in deeper grounds, to possibly find out why educational programs and standard awareness trainings have not lessen endusers fallings for phishing (even-though they have been trained) (Karakasiliotis et al., 2006; Kumaraguru et al., 2009). In order to compose frameworks or tools aiming to reduce phishing susceptibility one must firstly understand how and why people fall for them (Downs et al., 2007). To do this, the literature yet lacks to further consider potential roles of individual attributes into predicting their vulnerability.

Secondly, there should be a fair balance in studying victims' SE detection and response behavior, in terms of difference in their susceptibility determination. Apart from that, almost all the existing work is focused on the individual to understand why he falls for these attacks, and little attention is given to other elements of study for instance, generational cohorts. In regards this work will purpose a new direction to pursue, claiming a meaningful correlation among generations and vulnerability to Social Engineering.

Should it ever be considered that in lieu of composing more and more standard solutions that lack to fully achieve their goals, to address potential victims differently, perhaps into particular generational-groups. What if trying to tailor mitigation strategies to different audiences (generational groups) respectively in line of their needs and weaknesses in terms of vulnerability to SE attacks? Would this change anything?

3.5 Summary

This chapter has analyzed previous approaches taken to identify the main factors explaining users' likelihood of falling for Social Engineering attacks and at the same time have examined the proposed methods deemed to measure users' scale of vulnerability. All this done in purpose to possibly understand the extent of the gap in the literature and what is lacking in terms of directions to pursue in the future to properly address these issues. To finally find out who are more susceptible and what qualities makes them behave that way, to later be able to close this gap.

4 Conceptual Framework

This chapter presents the theoretical framework of the thesis and gives further insight to the importance of the research problem studied in this paper. Hereby, it explains the research methodology of data collection. The main research question and the reflective hypothesis are synthesized here. The factors identified by the previous studies are categorized and will be analyzed and digested to justify findings.

4.1 Research question and hypothesis

- RQ : Are generational cohorts equally vulnerable to Social Engineering attacks?

In order to deepen the focus on millennial generation, in this chapter the research question is slightly modulated to be: Is there any significant difference in susceptibility to Social Engineering attacks among the current generation and their parents' generation? To assess the response of this question, a holistic approach is taken combining an exhaustive literature review with analysis of quantitative data obtained from real-life phishing experiment conducted.

- H1: There is a notable difference in susceptibility to Social Engineering attacks among generation Y and Baby Boomers.

This study hypothesizes that indeed there is distinction in susceptibility among generational cohorts, specifically millennials may be more vulnerable and possess a greater likelihood of becoming potential victims of SE. To shed light to this problem of particular concern, this study will combine generations security weakness indicators supported by analysis of their real performance in phishing assessment. To reveal insights into how differently generations get Social Engineered, throughout this study generations are studied as groups rather than individuals, assuming them representatives of each whole generation (Fisher, 2015).

4.2 Obtained dataset justification

When trying to carry out a Social Engineering attack experiment or a phishing assessment in particular, there are a lot of constraints involved, be them ethical, legal, security or privacy related. Keeping in mind these considerations discussed below and the opportunity to get a proper dataset of sufficient quality for this study's research questions, the author does not conduct its own experiment and in lieu of, decides to use dataset from previously conducted phishing assessment.

4.2.1 Ethical Considerations

Even-though phishing experiments are considered one of the best ways to measure users' and employees' vulnerability to Social Engineering threats, there are also cases in which organizations avoid conducting them. Major contributors to this reluctance are ethical issues evolved. Social Engineering is strongly correlated with ethical considerations due to manipulation and deception techniques used. Moreover, these concerns are more present when running real-life phishing assessments since they have direct impact on participants.

Thus, they can damage them financially but most frightening is the psychological cost they leave to victims (Alseadoon, 2014; Aburrus et al., 2010). Experience has shown that most of the participants react really harsh to the assessment since they feel violated, mainly when they are not previously notified about the attack (Kumaraguru et al., 2009). "Some of the employees called the experiment unethical, inappropriate, illegal and unprofessional"(Aburrus et al., 2010, pg.251). The cases requiring researchers to be prosecuted are numerous, for instance in cases when participants' personal information from social-media is used.

Having a good dataset on hand (with respect to this thesis research questions), this work does not consider it necessary repeating the same study. However, before obtaining the dataset this study ensured that the sample group was not asked to provide any secret account information and also ensured to destroy the raw data at the end of this study. Anyway, to further the understanding of how to conduct ethical SE assessments, it is important to read the Jakobsson and Finn (2007) work, emphasizing three ethical principles to take into account: the respect for persons, beneficence, and justice, in terms of rights and the well-being of users (Jakobsson and Finn, 2007).

4.2.2 Legal Considerations

Apart from ethical constraints, while conducting an experiment researchers often have to assess legal considerations as well. There have been cases unintentionally resulted in law infringements and consequently, many researchers were being sued or prosecuted. Hence, everyone should be especially careful with risks of data breaches, data leakages or identity thefts. Unintentional leads to sensitive personal data harvesting or confidential information disclosure can occur, be this on individual or organizational scale. Data protection laws and regulations, protecting actors' privacy or security rights on internet should be strongly taken into account. On the other hand, companies' Terms and Conditions should be strictly respected and followed in cases where organizations are subjects of the experiment. Taking into account all these risks and having the opportunity to rely on others' data, this study avoids carrying out such risky experiments.

4.2.3 Getting Approvals

Besides ethical and legal considerations, getting the needed approvals on time is another serious element many authors have to ensure before conducting such studies. Hereby, one needs to get the appropriate approvals from the entities evolved in the assessment before setting-up such assessment. For instance, in this case it was aimed to conduct the experiment in a big organization and in a high school thus, getting the needed approvals would had not been an easy task, taking into account the fact that young teenagers and Baby Boomer employees would have been the experiments' feasible targets. On one side stand companies, which work for years to ensure employees' trust and on the other side stand the school's representatives or teenagers' parents who would not have been easily convinced to expose students to risks of this nature. Adding here the fact that getting the right approvals takes a lot of time, this study considered it be the case.

4.2.4 Significant sampling

Along these lines, the most important factor that should be taken into account while planning to conduct an experiment is the sampling. Getting a considerable sample to carry out the phishing attack is often difficult due to many limitations, and this leads to fail attaining statistically meaningful sample size and results as well. In this case, obtaining a truly representative sample of target users was difficult, nearly impossible. Apart from that, ensuring a homogeneous representative of the studied generations from the available dataset, is the main reason why this study does not involve conducting any form of Social Engineering attack assessment.

4.3 Methodology used

In this research a combination of data-collection techniques is used, a mix of quantitative and qualitative methods. Taking into account this research problem of particular concern, the methodology chosen aims to solve out the research questions (Gable, 1994). By combining these two complimenting methods, it is studied the interactive relationship between groups' security weaknesses and their actual susceptibility, to provide detailed insights into how and why generations get Social Engineered.

4.3.1 Qualitative method

In the first phase, the literature review is conducted to identify factors impacting users' possibility to fall for SE attacks, making up the qualitative data used in this study. The theoretical model carried out aims to investigate and digest the level of influence these factors have on groups' susceptibility. Their impact is tested and evaluated combining related works' findings with phishing email experiment's results. This work was reluctant in choosing other methods for the data collection (survey or questionnaire) due to high chances of outcomes overestimation, since users still limit the understanding of phishing (Jakobsson and Finn, 2007). As such, this research methodology assumes that each factor extracted from the literature review plays an important role in explaining users' vulnerability to Social Engineering attacks. The approach assessed does not assign every factor to a single generation, in a one-to-one relationship (Fisher, 2015) rather distributes them on each generation, based on their degree of appliance and level of presence. The generation showing higher occurrence of elements strongly related to victimization, is determined the most likely to fall for Social Engineering attacks, and hence, the most vulnerable. The detailed analysis is carried out in the next chapter. This thesis validates findings and assumptions analyzing the obtained dataset.

4.3.2 Quantitative method

Quantitative methodology is proven to be able to support findings, that is the main reason this study preferred to integrate it in the chosen methodology. On the other side, both literature and experience has shown that one of the best methods to gather data related to participants' behavior and their potential to fall for these attacks is via real-life phishing assessments. In distinct from other forms of attacks, phishing experiments have the benefit of being able to measure real performance results. In this way, the gathered data from the experiment provide a panoramic view of users' deployed decisions when faced with real-life phishing emails and hence, their degree of vulnerability.

The quantitative dataset taken from a phishing assessment is analyzed using appropriate tools, and details are given in the next chapter.

4.3.3 Experimental variables

- Dependent variables:
  - Susceptibility
- Independent variables:
  - Computer self-efficiency,
  - Generation,
  - Personality traits,
  - Education,
  - Gender,
  - Age

The identified qualities assumed to be primary indicators of groups' degree of vulnerability, make up the independent variables of the thesis statistical analysis. To better comprehend the relationship between independent variables with the dependent one, a detailed statistical analysis is carried out and findings are presented in the next chapter. Studied by previous works as well, all these elements are thought to play a significant impact on determining peoples' susceptibility and this study will seek to quantitatively validate assumptions in the next chapter.

4.4 Summary

This chapter has presented an overview of the research methodology, what approach is used in the thesis and how it is implemented. The justifications of obtained dataset is provided and hypothesis is stated. Hence, it has also revealed techniques used towards collection of both qualitative and quantitative data for analysis. The ethical and legal considerations are presented. Therefore, the evaluation framework that lays out the research questions is done on the next chapter.

5 Quantitative Analysis

This chapter describes the implementation of the conceptual framework presented in the previous chapter and its empirical evaluation. It also analyzes phishing assessment obtained dataset and report findings. Here are also outlined factors influencing phishing susceptibility dissimilarity among generations. The groups' found differences in the degree of vulnerability are explained using generations' unique characteristics synthesized from the literature review.

5.1 Descriptive statistics

In order to answer the main research question listed on chapter 1(**Is there any significant generational difference in susceptibility to Social Engineering attacks?**), the simulated phishing assessment dataset is analyzed. Despite its many constraints (mainly legal and ethical), phishing experiment is considered the best method to measure users' vulnerability since it can demonstrate users' actual likelihood of victimization (Jones, 2016). Along with assessing endusers' susceptibility, it can outline relevance to real world behavior users show when faced with any SE attacks.

5.1.1 Experimental Email

Simulated phishing experiment is used to measure users' actual susceptibility to SE attacks, as the most genuine way to assess their actual phishing management behavior. Adding particular value to this research, the collected-dataset is received from another researcher (Swapan Purkait). The type of phishing email sent to participants is a click email, aiming to direct participants to disclose sensitive information (specifically, their Gmail account login credentials) into a spoofed site.

Regarding the determination when one becomes victim of phishing, according to different studies and authors there are many definitions of "falling for the phish". Thus, a precise explanation of its meaning, is given by Sheng et al., (2010) however, in this thesis context falling for phish or getting social engineered, are considered cases when participants clicked on the provided link and submitted their personal information.

5.1.2 Experimental Subjects

A total of 430 people participated in the assessment but in order to draw more significant conclusions, the population considered for this study is focused on two particular generational cohorts : (the Millennial and the Baby Boomer generation). Thus, for this study only the data pertaining to these two specific groups is analyzed, the remaining data is deleted. The final sample size for this research is 337 (N=337). The sample is chosen to represent both groups, consisting of 337 participants of different background (age, education, gender, occupation). The targets selected for the assignment are part of the same university campus in India. As a matter of fact, the participants are considerably representative of this thesis's studied population. Thus, participants varies in elements like:

- **Generation:** Actually, 293 participants of the assessment are millennials (86.9%) and the other 44(N=44) or 13.1% of the sample pertain to the Baby Boomer generation.
- **Age:** The same age categorization of groups that is outlined on chapter 2 is used, practically millennials (17-35), and Baby Boomers (50-62). The mean of age for the millennial cohort is 27.3 years old and 54.6 years for Baby Boomers. There is a highest number of 25 years old participants (n=35) from millennials and a highest number of 51 years old participants (n=10) from Baby Boomers.
- **Gender:** All the participants of the sample are Indians comprised of 229 male (68.0%) and 108 (32.0%) female. There are 95(32.4%) female and 198 (67.6%) male from the millennials. On the other hand, there are 31(70.5%) males and 13(29.5%) females from the BB group. Data coding is used for the sake of this experiment data analysis. For instance, regarding participants' gender, male is coded 1 and female is coded 2. Data coding is also used to present other elements of the dataset as well, such as education and computer self-efficacy (shown below). The age and gender distribution of the sample are presented in the tables below.
- **Computer efficacy:** 168 users (49.9%) have technical background and 169(50.1%) have non-technical background. In this thesis technical background is translated as computer self-efficacy. Coding is also used here, where being technical competent is given a 1, and not competent a 2.
- **Education:** Concerning education, codes 1-4 are used representing the level of education the users have, Bachelor(1), Masers(2), PhD(3) and Professional(4). Out of the studied sample: 151 participants have bachelor degree, 124 masters, 40 PhD and 22 professional education.

5.1.3 Demographic distribution

After excluding the data not pertaining to either of the focused groups (Millennial and Baby Boomer), the answers of 337 responders are kept and analyzed. Details of the descriptive characteristics are given in the tables below.

Table 1. Age distribution of subjects

Age	Frequency	Proportion
(17-35)	293	86.9
(50-65)	44	13.1
Total	337	100.0

Table 2. Gender distribution of sample

Gender	Code	Frequency	Proportion
Male	1	229	68.0
Female	2	108	32.0
Total		337	100.0

Table 3. Computer efficacy of participants

Computer efficacy	Code	Frequency	Proportion
Tech-savvy	1	168	49.9
Non-tech-savvy	2	169	50.1
Total		337	100.0

Table 4. Education distribution of participants

Education	Code	Frequency	Proportion
Bachelor	1	151	44.8
Master	2	124	36.8
PhD	3	40	11.9
Professional	4	22	6.5
Total		337	100.0

5.2 Analysis of results

5.2.1 Susceptibility rates

Lord Kelvin quotes: “To measure is to know”, in the same reasoning this study aims to know each generation's degree of vulnerability by measuring their actual performance when faced with the phishing attack. Analysis of data collected from the phishing assignment generates the effects' of several independent variables (see section 4.3.3) on the single dependent variable (phishing susceptibility). Having said that, the received

dataset is initially entered into a Microsoft Excel file to statistically analyze it. The figure below presents participants' actual victimization on the phishing assessment.

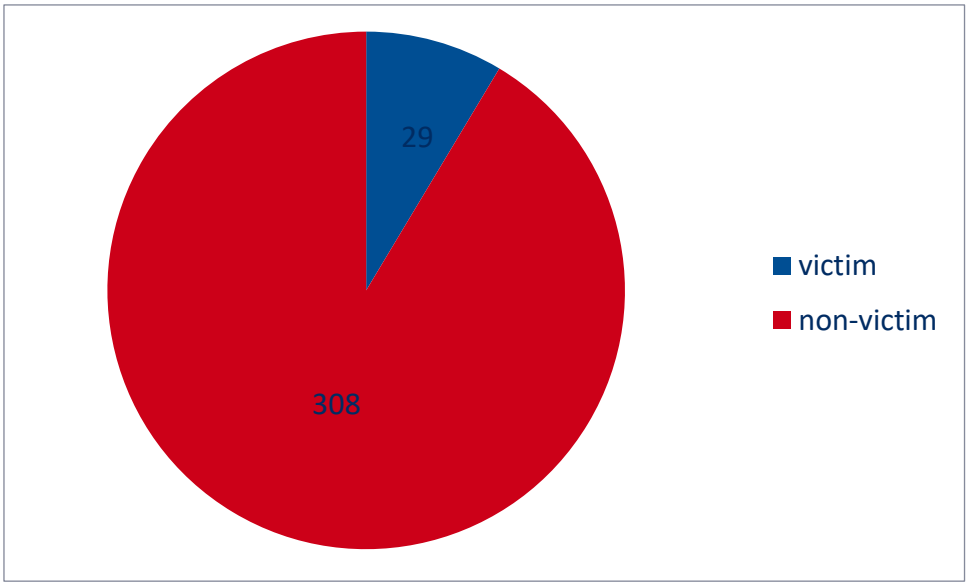

Figure 1. Participants victimization rates

In order to indicate falling for the phish, data coding is reused. A value of (2) is given to "falling" victim of the experiment and a value of (1), to non-victim. Presented also in the table below solely 29 participants or (8.6%), responded to the email and gave up their login credentials and 308 (91.4%) of them did not. It is safe to mention that it is surprising the number of participants who got phished. Hence, the assessment's results show a considerable value of victimization from the overall targeted sample, and the generation who mostly fell for the attack is the millennial generation. Moreover, on generational scale out of 293 millennial participants', 29 responded to the email, this percentage (8.6%) is higher than Baby Boomers, whose number of victimization occurrence is surprisingly 0.

Table 5. Generations extend of victimization

Group	Total	Victim	Non-Victim
Millennial	293	29	264
Baby Boomer	44	0	44
Total	337	29	308

As a matter of fact, the calculated percentage of victimization of the whole sample (8.6%) is considered acceptable and in normal range for victims who fall for phishing incidents (Knight, 2004). This high victimization rates among millennials shows that they are comfortable divulging their login credentials via email. This hypothesize a lack of concern

from their part in authenticating phishing emails or in SE security in general. However, possible factors impacting these results are discussed in the sections below.

5.2.2 Supporting the stated hypothesis

This thesis' aim to answer the first research question (see Chapter 1), is attained by quantitatively measuring the targeted cohorts' actual vulnerability on phishing performance. Thus, independent sample t-test is performed in order to analyze the null and alternative hypothesis. T-test is used to test whether there is any significant distinction between means of two groups (DeCoster and Claypool, 2004). The null hypothesis (see H0 and H1 in Chapter 4: That is no statically significant difference among the two studied generational cohorts) is actually rejected by the analyzed data which, supports the alternative hypothesis. Having set alpha α=.05, results from the unpaired sample t-test show a significant contrast of subjects actual performance on the phishing attack (probability $p < \alpha$). Independent sample t-test arise in a t-Stat (two-tail) value of 5.663 with 292 degrees of freedom, explaining the existing difference on phishing susceptibility among them. To summarize, these results fit also the results of the Chi-squared test (see section 5.2.3), rejecting the null hypothesis (the approach of hypothesis disproving is attained). Further details on t-test are provided on the table below.

Table 6. Unpaired samples t-Test results

t-Stat(two-tail)	t Crit(two-tail)	Prob p(2-tail)	α=.05	Df
5.663	1.968	p=0.000000035	0.05	292

5.2.3 Groups and falling for phish

Another way to answer the first research question is by executing the Chi-Squared test to assess any difference among the two studied-generations leading to acceptance or rejection of the null hypothesis (Zibran, 2007). Chi-Squared test is used to measure the probability of association of independent groups (Maxwell, 1971). Results show a significant distinction on susceptibility among millennials and baby boomers, with millennials being more vulnerable (p=0.02). Thus, there is enough evidence (t-test and chi-squared test) to conclude an undeniable contrast among these two studied generational cohorts on performance on phishing assessment. Slightly differing on age categorization, other researchers (Sheng et al., 2010; Kumaraguru et al., 2009) have also found younger users of age 18-25 to be more vulnerable to these types of threats.

On the other hand, both males and females are considered equally vulnerable to SE attacks, with not enough evidence proving the opposite (p=0.4). Moreover, no difference was also shown among technical efficient group and the non-technical efficient one (p=0.3), having set the target ($p<0.05$). Also, groups alternated in educational level, demonstrated non-statistically significant difference on susceptibility from the Chi-squared test results (p=0.08).

5.2.4 Estimating variables impact on susceptibility

In order to find out the main reasons users fall for Social Engineering attacks, the impact of several variables on susceptibility is analyzed. Thus, having susceptibility to phishing attack the only dependent variable of the study, linear regression is performed to test the impact of a number of potential predictors on this variable. Linear regression is used to measure the strength of each of the predictors on the one variable of interest (susceptibility) (Montgomery et al., 2012). Hence, regression coefficient is calculated to show the type of relationship among variables. For this study, the significance of a relation is obtained in a probability value lower than ($p< 0.05$) (DeCoster, 2006). Any p-value (indicating the strength of relationships) greater that this significance level demonstrates lack of evidence to prove variables' notable influence on vulnerability to SE threats.

Therefore, linear regression is applied many times independently among pairs of the dependent variable with the independent ones and results are shown below.

Table 7. Linear regression output

Susceptibility predictors	(p-value)	Regression coefficient(Beta)
Age	p=0.29	β=-0.002
Gender	p=0.47	β =0.023
Generation	p=0.02	β =-0.098
Education	p=0.86	β =0.002
Technology efficacy	p=0.34	β =0.029

As shown also from the table above, the analysis of variance (ANOVA) is performed on finding out the strength of the relationship among pairs.

Age

Participants' age is found to not predict their susceptibility to Social Engineering attacks $F(1\text{-}335)=1.103$, $p=0.29$, with a negative insignificant relationship between these two variables ($\beta=-0.002$). These results are consistent with results of other studies (Kumaraguru et al., 2007; Dhamija et al., 2006). However, there exist also studies that claim that age do have an important impact on users' performance on phishing attacks (Sheng et al., 2010; Kumaraguru et al., 2009).

Education

A positive non-significant correlation is also found between users' education and their fall for the attack $F(1\text{-}335)=0.0278$, $p=0.86$. In support to results of this study, (Dhamija et al., 2006; Sheng et al., 2007) concluded that educational level does not play any significant role on users' vulnerability.

Gender

Linear regression results do not show any significant impact of gender on users' shown degree of vulnerability, $F(1\text{-}335)=0.502$, $p=0.47$ with the Chi-Squared test also showing

no difference among males and females in the rates they fell for the phishing assessment. In support to these findings, Kumaraguru et al, also found no distinction in phishing performance among 2 genders (2007). Other researchers however, have found females to be more vulnerable to such attacks (Jagatic et al., 2007; Sheng et al., 2010; Alseadoon 2014).

Technology-efficacy

Furthermore, technology efficacy is spotted unimportant in predicting susceptibility $F(1-337)=0.908$, $p=0.34$, supporting the findings of the other researchers (Vishwanath et al., 2011). However Dhamija et al., found lack of knowledge regarding technology in general to be one of the main reasons why people get phished (Dhamija et al., 2006). Sheng et al, found that for each unit of users' increase in knowledge concerning technology, they fall for 3.6% fewer phish, categorizing self-rated knowledge regarding technology a relevant asset in reducing users' likelihood of becoming potential victims of any type of SE attack(2010).

Generation

As it is assumed, generation is observed to explicitly predict users' susceptibility to SE, resulting in having the highest impact of all factors $F(1-335)=4.805$, $p=.029$. This means that when this item increases, the likelihood of users responding to phishing emails decreases ($\beta=-0.098$). This variable is proposed and studied by this thesis for the first time and statistical results highlight that it should be a new essential field of study for other researchers as well. Additionally, these results demonstrate higher chances for intruders to exploit millennials comfort zone in regards to Social Engineering.

This analysis is focused understanding 5 correlations in total and surprisingly only one of them is classified as noteworthy and the remaining 4 are considered statistically unacceptable. Generational element is found to be significant at $p<.05$, being the only supported factor to have a worthy of attention correlation with vulnerability.

5.2.5 Multiple regression and Multicollinearity

Multi-collinearity tests if there exists any relationship among independent variables that could influence the regression analysis outcomes and hinder the overall output interpretation. Hence it is notable to be performed in this study to deepen the understanding of the findings. The multi-collinearity test is done when there are more than one potential predictors on the model that could have a significant relationship among each-other (Hair et al., 1998) and interfere the results. This study assumes that the relationship between age and generation makes it difficult to distinguish each of these variables' effect. Thus, variable inflation factors (VIF) (used to calculate the inflection of the independent variables' variances (Lin, 2008)) are measured and results interpretation is given below.

Table 8. Multicollinearity test results

Independent variables	VIF value
Age	9.296
Gender	1.019
Technology	1.060
Education	1.385
Generation	8.336

In order to understand the variable inflation factor values presented in the table below, the threshold 10 (VIF > 10) is set to indicate the presence of collinearity among independent variables (Belsley et al., 2005). Comparing the computed VIF values, it is assumed to exist a correlation among age and generation explanatory variables. Though, assumptions cannot be concluded since the VIF values are below the threshold and further investigation controlling for age effect is necessary. Therefore, recalculating the VIF values omitting the variable showing the highest VIF factor (the age factor) changes the results of the analysis and collinearity is avoided. Nevertheless, this approach is claimed to obscure the statistical model and getting a large enough sample size to cover geographic representation of the targets is suggested as the most proper solution to circumvent collinearity occurrence within the model.

Table 9. Multicollinearity test

Remained factors	VIF values
Gender	1.003255
Technology	1.058756
Education	1.100619
Generation	1.158866

The justification of using multiple regression apart from linear regression, is not only to investigate multicollinearity presence in the model, but also because linear regression could only measure a single predicting variable with the predicted one, being unable to test many-to-one relationships. Moreover, this is done in order to at the end solely the variables resulting in significant relationships are kept and exclude the others from the final model. Multiple regression is suitable for analyzing multiple independent variables impact on a single dependent variable. Thus, multiple regression is performed and results are shown in the table below.

Table 10. Multiple Regression output

Predictors	Std err	p-value	β coefficient	Statist signific
Age	0.004	0.008	0.012	Yes
Gender	0.032	0.294	0.034	No
Education	0.020	0.676	-0.008	No
Tech-efficacy	0.031	0.734	0.010	No
Generation	0.129	0.001	-0.422	Yes
Significant at **p<.005				

Again, in the same line with linear regression, results from multiple regression show generation factor to have the strongest impact on susceptibility (p-value <.005). Consisting in a negative relationship (β=-0.422), as generation variable increases, vulnerability level of users actually decreases. The coefficients (Beta values) for the rest of the independent variables are listed in the table above.

An explanation of the younger generation's shown vulnerability can be attributed to their lack of awareness on SE risks. Therefore, the Millennials' high tendency to respond to Social Engineering attacks is described and related to their personality traits, distinguishing them from previous generations.

5.4 Summary

This chapter has analyzed collected-dataset from phishing assessment and findings are presented. It has explained how outcomes of the analysis enabled answers to the research questions. The results from the phishing experiment have showed that young people of today fell victim of the assessment at higher rates than their parents and as such, are assumed to be more susceptible to Social Engineering threats. This section has also outlined factors influencing users' response to these attacks.

6 Understanding gens shown susceptibility

This chapter explains generations found vulnerability to SE, reasons that interpret their shown high degree of susceptibility and the psychology behind it. Having said that, this section aims to answer the third research question of this study and at the same time to psychologically explain the quantitative findings from the phishing assignment dataset analysis. In light to this aim, certain personality traits are highlighted as having major contribution to generations' likelihood of victimization. At the end of the chapter, a defense strategy to combat Social Engineering threats is proposed.

6.1 Potential victims psychological profile

In order to explain cohort groups shown susceptibility to phishing experiment this study seeks to understand how are personality traits and generational differences in regards to phishing related. Generational groups unique personality characteristics are a reflection of different political and social changes lived by each cohort group thus, generations are proven to differ in personality traits (Barrick et al., 2001; Macky et al., 2008). As such, shaped by certain personality traits sensitive to these attacks, different cohorts perceive security risks differently (Ng et al., 2012). Peoples' personality is nothing more than their likelihood to behave in certain ways, and its traits (Big Five traits) are shown to have a determinant impact on users feasibility to responding to Social Engineering attacks (Uebelacker and Quiel, 2014; Halevi et al., 2013) .

The Chi-squared test and regression analysis show a significant correlation between millennials and falling for the phish (See 5.2.3). Hence, it is worth finding out what personality qualities make this cohort more susceptible to phishing, compared to their Baby Boomer parents.

Many researchers target **conscientiousness**, the most relevant personality trait to determine phishing susceptibility (Halevi et al., 2015), due to its link to continuance commitment (Erdheim et al., 2006; Workman, 2008). Therefore, a significant difference is found between generations on conscientiousness trait with young people of today (millennials) found to be more conscientious than the other generations on the workforce (Generation X and Baby Boomers) (Roberts et al., 2006), clarifying millennials bad performance on the conducted assessment. On the other side, both effective and normative commitment are suggested to relate to **extraversion** as such, (Erdheim et al., 2006), increasing the likelihood of millennials falling for SE attacks (Workman, 2008; Parrish et al., 2009; Alseadoon et al., 2012). Correspondingly, an increase of extraversion, conscientiousness and emotional stability is found to characterize younger generations (age 20 to 40), all being personality elements explicitly increasing susceptibility to security risks and to SE attacks (Roberts et al., 2006). Thus, many other researchers (Andre et al., 2010; Gentile et al., 2010; Scollon and Diener, 2006; Smits et al., 2011) emphasized the fact that younger cohort groups are more vulnerable to phishing as they score higher on extraversion compared to older generations.

Showing a generational increase on self-esteem, over-confidence and entitlement, many studies found Generation Y to possess higher levels of narcissistic personality traits (Steward and Bernhardt, 2010; Twenge et al., 2008; Twenge and Foster, 2010; Bourke and Mechler, 2010) than older generations, who show lower narcissism scores (Foster et al.,

2003). Narcissism in particular is found to have a strong relationship with extraversion, explaining this paper's found generational difference in vulnerability to phishing attack.

Moreover, one other domain of Big Five personality traits that happen to increase peoples' susceptibility to SE is high **agreeableness** rates (Parrish et al., 2009; Modic and Lea, 2012). Darwish et al., claim an increased level of agreeableness among younger people and woman (2012), potentially explaining results of the statistical analysis in this work (specifically, millennials shown high victimization rates on the assignment). In the same consistency other studies found young users to be more vulnerable to phishing attacks as possessing higher levels of agreeableness, which is strongly correlated to the likelihood of falling victims of security attacks (Srivastava et al., 2003).

6.2 Awareness and training against SE

This section reveals insight towards designing the most effective strategy to reduce young people of today susceptibility to Social Engineering threats. It specifies objectives to achieve, needs and weaknesses to comply with, policies and procedures that have to be met. It covers all the phases of a continual awareness training from design, development and implementation to explore at the end the best evaluation practices to measure its effectiveness. It describes the combination of the current solutions on place to establish the best program to include in every high-school curricula.

6.2.1 The best defense against Social Engineering

It is already clear that there are no great solutions decreasing end-users vulnerability to Social Engineering, regardless of existing numerous proposals having different effectiveness rates. In this case it is worthless to propose any new equally effective solution. Moreover, there is "no need to reinvent the wheel if there are vehicles already in place (Desman, 2001, pg. xv)." How about exploiting all these taken efforts by combining them, taking the best of each to comply with specific requirements and specific target group? This leads to the idea of expansion of the already proposed solutions via necessities recognition and meeting objectives.

Special awareness campaigns, training sessions or education are examples of several applied methods that have been the most effective ones in mitigating vulnerability to Social Engineering attacks. Trying to find out the best possible solution that works reducing likelihood to fall for SE attacks, recall the educational security conferences and their approach. Excellent events with detailed covering of most important security issues, a lot of text material which is tough to understand and many security threats to became aware of. Then every participant walks through the conference door accompanied by the positive feedback and the brain filled with important theory needed to be remembered. Taken by the everyday's routine, the great lessons picked up at the conference hall are already gone. The core theoretical security concepts are forgotten, none is bothered changing passwords, doubting a friendly behavior or even paying attention to malicious or unapproved content spread on SNS. At this point everybody realizes that this is not the best approach to follow. Education is the highest level of any learning phases which starts with awareness, than training. Thus, it is worth implementing it only when the first two phases are fully and effectively covered.

Millennials are critically not aware of Social Engineering threats because no one has put sufficient efforts to show them, so every program of this profile should start addressing awareness at the very grounds. It is crucial to achieve building SE awareness among the current generation (you cannot make them change attitude unless they want to). However, awareness is simple attention to security thus it is not enough, a more interactive approach should also be included in any effort reducing susceptibility towards SE. Both awareness and training as fundamental learning phases should be tightly incorporated in any Social Engineering defense framework.

In a research conducted to understand Estonians attitude and willingness on the implementation of security awareness and trainings in elementary, secondary and higher education it is emphasized by the researchers that nothing is done at the lower stages of education yet (Lorenz and Kikkas, 2012). Also the results of some interviews conducted with some fellow students of Cyber Security program at TUT, emphasized that education of new generations should start from schools as part of their curricula as soon as possible. They argue that parents do not have neither time nor resources to do it. A very well-crafted security program part of every school can do better in training students to grow up knowledgeable users ready to enter the workforce and able to influence their parents.

Due to all the above covered reasons and millennials' specific security needs, this thesis proposes an effective awareness and training program as the best solution to mitigate vulnerability to Social Engineering, with awareness intended to create SE security consciousness and training to build security skills and behavior.

The thesis also stresses out the necessity of such program to be integrated in every national high-school curricula and to be implemented periodically. It proposes a very productive way to develop training programs or campaigns to raise awareness to Social Engineering threats and to meet each school's goals. The only known defense for SE attacks is an effective security awareness program (Gardner and Thomas, 2014). A template of a SE security awareness training is provided on Appendix A of this thesis.

6.3 Program model and assets

Objectives:

It is essential to recognize the need for such security frameworks to be incorporated to any school program since there is not a single high school (to this thesis best of knowledge) that offers a Social Engineering security program. In light to this objective it is crucial to clear out that there is not either any previous work that have emphasized the necessity for a SE security program nor have composed a training framework for schools to implement. However the main objective of this program is to build security consciousness among students, arriving at the point they posses secure behavior without having to think before applying it. The program will continually remind and teach them the importance of protecting themselves against SE threats. To do so, the program aims to ensure that all students understand the need to include a SE security awareness program in the school curricula via letting them know that everyone is vulnerable to SE attacks. Moreover, it should ensure that they understand and acknowledge their security responsibilities. The program should clearly specify security policies, ensure that the training have a strong awareness approach. So, users must be appropriately focused to meet the program goals, be fully motivated to change the behavior that makes them vulnerable to Social Engineering risks. Thus, the ultimate scope of the awareness training is **making the weakest asset of the security chain (users), the strongest link** via teaching them to play

an essential role in ensuring Social Engineering security via protecting themselves and sharing awareness also to their Baby Boomers parents.

Program profile

The program should be build focusing mainly on two things: meeting students security needs and schools policies and requirements. The model proposed here passes through program design, development, its implementation and evaluation. Such strategy combining practical learning and interaction is fundamental for this on-going training program, being able to build security skills and behavior. In their work Lorenz and Kikkas found out that 71% of Estonians prefer hands-on security trainings instead of theoretical ones (2012). People learn differently based on their generational and educational background, and current generation learns much different than those entering in the workforce 30 years ago (Gardner and Thomas, 2014). There is a big difference between providing material of how to defend against SE to this generation and teaching them practical skills of a security behavior. Passive learning seems not to work among millennials, they would prefer interactive learning instead. Current generation students needs social learning, workshops to make them realize how easy it is to fall for these attacks. Also this thesis proposes classroom training via active learning, as the most efficient type of learning in reaching goals (Gardner and Thomas, 2014). Active learning in this training context is explained here (Prince, 2004). This thesis proposes a awareness and training model to incorporate seminars, conferences, workshops, short security meetings, roundtables, Q&A sessions and other alike facilities in the material delivery.

Program material

The selection of material is another essential element to decide about while crafting the proper awareness training. Therefore, the training material should be carefully selected considering the behavior that school want to convey to students and skills to show when faced with actual Social Engineering threats. Achieving to share awareness to students, ways to deliver the awareness material are enormous: school monthly newsletter, poster campaigns, pens campaigns, monthly security days, security note of the day or other innovative ideas created by the security team while designing the program or when updating it. Another innovative and appealing idea is rewarding students for compliance with school's security policies or continual SE security promotions or acknowledgements via coffee mugs, bookmarks, mouse pad, paper weight. In order to make millennials pay attention to the program and to awareness particularly, the message in the awareness material should also be short and concise, integrate catchy security slogans. Therefore both awareness and training material should be simple, easy to use and easy-to-access. Because it is an on-going process it is crucial not to stick to only one technique, instead mix different delivery techniques up and look to adequate repositories to get the most appropriate material. In reach of this, it should not be a take-on-somewhere framework or any traditional one, it should be composed based on school's culture. The ways to deliver the training should also be new and creative enough to make them participate and learn security skills. A list of topics to be covered by the program is provided in Appendix B of this thesis.

Social Psychology

The crafted program should take into detailed consideration the millennial students psychology, as directly involved in the process of changing attitude and behavior via changing behavioral intentions. Manjak argues, “Employees will not be motivated to change behaviors if they see no reason to change (2006, p. 12)." **This thesis highlights**

the importance to carefully include motivational drivers while designing and implementing the program. The security team responsible to design the awareness training should include an expert of the field of psychology in planning and composing the program. Security rewarding or appraisals for proper security behavior by students are innovative ideas that should not miss in the maintenance of the program. Moreover, the training should be designed to comply with generation Y personality traits vulnerable to Social Engineering attacks. By specifying particular security behaviors intended to convey among school students, social learning in compliance with social psychology is proved to work best for them. However, security is said to be a process (Schneier, 2000) and it should take a lot of continual efforts in achieving to build security consciousness among "nexters". Thus, this is crucial for young people of this generation and employees of tomorrow, to be packed with the needed security behavior (before entering the workforce) required in every organization struggling to create such a culture.

The program security team

In order to build the most appropriate awareness and training strategy for any school to execute, the establishment of a security team is crucial. Behaving as the central authority of this long process, its primary duty is to develop security policies and set standards. The team will have to deal with the general management of the awareness and training program being the main responsible party of the training overall efficacy. Thus, it should ensure the training productivity via keeping track of its success and compliance. Therefore, the security team will specify methods to be used in evaluating the program effectiveness: conduct questionnaires, focus groups, interviews, periodic assessment on students' security awareness etc. These tools are also a way to measure the program's accessibility and material understanding by students, via monitoring their attendance and performance. At the end the team should carry on needed updates on the program based on the conducted periodic reviews.

6.4 Summary

This chapter has pursued to explain the current generation observed susceptibility to Social Engineering and has revealed different methods aimed to lessen their vulnerability. The results found on chapter 5 are validated in this section via tuning the adequate SE defense for schools to integrate in their curricula. The next session gives suggestions and directions for future work to be done through assessing the thesis limitations.

7 Discussions

This chapter focuses on concluding this thesis findings and summarize its core contribution. Reviewing results and implications, it identifies new challenges to extend the mitigation of SE vulnerability in the future and explore the unaddressed aspects of this problem. On the whole, it is still requisite to study deeper the generational factor of SE attack and evaluate any thoughts or findings in regards. On that reason, this research concludes with recommendations.

7.1 Drawing final conclusions

Overall, this thesis proposed to study endusers' vulnerability to Social Engineering in terms of generational cohorts. The statistical analysis showed susceptibility to be significantly affected by generational factor and paradoxically, technology-efficiency was not found to be able to ameliorate users SE threats detection abilities. In the same lines with the current research findings, it was reasonable to conclude that none of the analyzed demographic factors plays any relevant role determining users vulnerability. Moreover, educational level produced insignificant results to expect a furthered education to give better chances of detecting SE threats.

The obtained results enabled this thesis to meet its main objective, highlighting the importance to differentiate victims of Social Engineering frauds on generation-base in future studies. Via analysis of targets' performance on phishing assessment, this research found the current generation of today showing higher likelihood to be deceived by SE attacks. Having the starting date the same as Internet Domain Name System, it was surprising to find out the most internet-savvy generation to be more vulnerable to SE attacks compared to Baby Boomer generation. This implies that just because one is knowledgeable to SE threats, does not become more aware or less vulnerable and vice versa.

In chapter five and six, the author explained reasons contributing to gens' shown susceptibility and claimed to link SE vulnerability to their personality characteristics. Generally speaking, consciousness, agreeableness and extraversion traits were found to show the highest impact on generation Ys' tendency to fall for Social Engineering threats. These particular personality elements are also suggested by previous works to correlate to increased susceptibility to phishing and to enlarge current generation potential to SE victimization. Answering the second research question these personality characteristics can be exploited by intruders to make millennials phish out sensitive information.

Implying the necessity for a defense strategy for any high school to implement, finally this study evaluated the effectiveness of the numerous SE mitigation methods proposed, to come out with a solution meeting the observations driven from the overall research. Rather than changing current generation personality characteristics (proved to correlate to increased vulnerability) the mitigation strategy propose to employ these specific characteristics to build secure behavior and attitude towards SE among high-school students. The third research question was answered crafting the SE security program complying with the millennial generation SE security needs and expectations. The impact of the awareness and training program proposed in chapter 6 is promising since it is planned covering relevant findings of this research.

7.2 Practical limitations

Target groups' tested vulnerability is translated to SE security weaknesses they demonstrate when faced with SE attacks and that should be addressed by every methodology seeking to reduce users susceptibility. Generally speaking, changing weaknesses into adequate SE security skills will definitely confine Millennials from fall for SE attacks at higher rates via lessen their deficiency in SE security awareness.

The first limitation of this research is being a cross-sectional study (see Twenge and Campbell, 2008) as such, it does not expect to have fully assessed and support the stated hypothesis or to have completely answered the research questions. Moreover, the approached hypothesis is just an assumption (since this work is the first to anticipate a substantive difference among the studied generational cohorts) and specific conclusions of the root causes of the detected difference in vulnerability cannot be easily elicited.

The second limitation constitutes in that although both generations were core targets of the study, there was a disproportional generational distribution of participants on the assessment (low number of Baby Boomer participants) which could lead to question the significance of the results.

Another core limitation of this research stays on the fact that the targeted endusers shared the same cultural background and more specifically, the same university campus, lacking to validate the revealed outcomes through covering a wider geographic area. Therefore, the same findings do not expend to other cultures and countries (due to deficiency of research on the same topic), which may result in different generations profiling on Social Engineering susceptibility.

In addition, generational groups in this research were created assigning individuals to a generation according their birth years however, what if the observed vulnerability dissimilarities be confounded by age and to have altered this research's results? For future works, a fleshed-out methodology should be employed, isolating the effect of generation or keeping the age variable constant to derive more specific outcomes.

Furthermore, in order to reveal meaningful conclusions and understand stereotypes occurring across these two generations it is trivial to access a large enough number of victims (confined by many reasons).

These several elements could have resulted in better conclusions if could have been included in this research, thus **a longitudinal research should be undertaken to cover these limitations via taking this thesis as a benchmark to draw better outcomes.**

7.3 Recommendations for future work

Along the findings, the author in this study has also outlined hints to evolve researching to defend against SE and at the same time to avoid digging into wrong directions. Currently, there is a fair gap in related works studying generational differences in personality influencing their susceptibility to SE, since the few studies that exist are mostly focused on generational differences in general (Twenge, 2000) and not on susceptibility to SE specifically hence, this thesis is a crucial foundation on seeking empirical evidence to this approach. Moreover, there is no other research on studying endusers vulnerability to SE on generation-base, this work propose a means of categorizing victims of SE on generational cohorts sharing similar personality characteristics directly correlated to increase SE

vulnerability. For instance, replication of this study could be recommended to continue analyzing the effect of variables which are studied here for the first time.

Hence, this research highlights the importance to continue research:

- personality differences among generations in relation to susceptibility to SE (since it is already proven that generations distinctions in personality traits impact their likelihood to respond to these attacks).
- deeper grounds towards supporting the stated hypothesis, for instance it is worthwhile seek to complement other researches on how to profile SE victims.
- how to determine what is the right balance to propose strategies to mitigate endusers tendency to get social engineered (why not improving the existing ones complying with your needs instead).
- the same topic with data in which age factor can be controlled (noting the interdependence that age-generation elements have on each-other).

Bounded by time constraint, this study missed to evaluate the proposed SE security awareness and training program efficiency thus, it is trivial to evaluate this thesis proposed model effectiveness in reducing vulnerability and furthermore, use this as a benchmark for other proposed training programs. Nevertheless, this work is a promising start to the idea of studying victims to SE attacks categorized on generational cohorts and future approaches should continue exploring how victims of SE attacks differ via enhancing this study's rule of thumb guidelines and listed challenges.

8 References

Aburrous, M., Hossain, M.A., Dahal, K. and Thabtah, F., 2010. Experimental case studies for investigating e-banking phishing techniques and attack strategies. *Cognitive Computation*, *2*(3), pp.242-253.

Aggarwal, A., Rajadesingan, A. and Kumaraguru, P., 2012, October. Phishari: automatic realtime phishing detection on twitter. In *eCrime Researchers Summit (eCrime), 2012* (pp. 1-12). IEEE.

Alghamdi, H., 2017. Can Phishing Education Enable Users To Recognize Phishing Attacks?.

Allen, M., 2006. Social Engineering. *A means to violate a computer system, listopad*.

Allsopp, W., 2010. *Unauthorised Access: Physical Penetration Testing For IT Security Teams*. John Wiley & Sons.

Alseadoon, I.M.A., 2014. *The impact of users' characteristics on their ability to detect phishing emails* (Doctoral dissertation, Queensland University of Technology).

Alseadoon, I., Chan, T., Foo, E. and Gonzales Nieto, J., 2012, January. Who is more susceptible to phishing emails?: A Saudi Arabian study. In *ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012* (pp. 1-11). ACIS.

Amankwa, E., Loock, M. and Kritzinger, E., 2014, December. A conceptual analysis of information security education, information security training and information security awareness definitions. In *Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for* (pp. 248-252). IEEE.

André, M., Lissner, L., Bengtsson, C., Hällström, T., Sundh, V. and Björkelund, C., 2010. Cohort differences in personality in middle-aged women during a 36-year period. Results from the Population Study of Women in Gothenburg. *Scandinavian Journal of Social Medicine*, *38*(5), pp.457-464.

Arachchilage, N.A.G. and Love, S., 2013. A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), pp.706-714.

Armitage, A. and Keeble-Allen, D., 2008, June. Undertaking a structured literature review or structuring a literature review: tales from the field. In *Proceedings of the 7th European Conference on Research Methodology for Business and Management Studies: ECRM2008, Regent's College, London* (p. 35).

Barrick, M.R., Mount, M.K. and Judge, T.A., 2001. Personality and performance at the beginning of the new millennium: What do we know and where do we go next?.*International Journal of Selection and assessment*, *9*(1-2), pp.9-30.

Becker, M.A., 2015. Understanding the Tethered Generation: Next Gens Come to Law School. *Duq. L. Rev.*, *53*, p.9.

Belsley, D.A., Kuh, E. and Welsch, R.E., 2005. *Regression diagnostics: Identifying influential data and sources of collinearity* (Vol. 571). John Wiley & Sons.

Bergman, J.Z., Westerman, J.W. and Daly, J.P., 2010. Narcissism in management education. *Academy of Management Learning & Education*, *9*(1), pp.119-131.

Borges, N.J., Manuel, R.S., Elam, C.L. and Jones, B.J., 2006. Comparing millennial and generation X medical students at one medical school. *Academic Medicine*, *81*(6), pp.571-576.

Bourke, B. and Mechler, H.S., 2010. A new me generation? The increasing self-interest among Millennial college students. *Journal of College and Character*, *11*(2).

Boyd, D., 2007. Why youth (heart) social network sites: The role of networked publics in teenage social life. *MacArthur foundation series on digital learning–Youth, identity, and digital media volume*, pp.119-142.

Braber, S., 2016. *Security and privacy perceptions of millennials (18-24) and non-millennials (36-50) on Facebook* (Bachelor's thesis, University of Twente).

Cho, J.H., Cam, H. and Oltramari, A., 2016, March. Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. In *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2016 IEEE International Multi-Disciplinary Conference on* (pp. 7-13). IEEE.

Christofides, E., Muise, A. and Desmarais, S., 2012. Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science*, *3*(1), pp.48-54.

Compeau, D.R. and Higgins, C.A., 1995. Application of social cognitive theory to training for computer skills. *Information systems research*, *6*(2), pp.118-143.

Coomes, M.D. and DeBard, R., 2004. A generational approach to understanding students. *New Directions for Student Services*, *2004*(106), pp.5-16.

Darwish, A., El Zarka, A. and Aloul, F., 2012, December. Towards understanding phishing victims' profile. In *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on* (pp. 1-5). IEEE.

DeCoster, J., 2006. Testing group differences using t-tests, ANOVA, and nonparametric measures. *Accessed November*, *30*(2010), pp.202006-0.

DeCoster, J. and Claypool, H., 2004. Data analysis in SPSS.

Desman, M.B., 2001. *Building an information security awareness program*. CRC Press.

Dhamija, R., Tygar, J.D. and Hearst, M., 2006, April. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). ACM.

Donnison, S., 2007. Unpacking the millennials: A cautionary tale for teacher education. *Australian Journal of Teacher Education (Online)*, *32*(3), p.1.

Downs, J.S., Holbrook, M. and Cranor, L.F., 2007, October. Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 37-44). ACM.

Downs, J.S., Holbrook, M.B. and Cranor, L.F., 2006, July. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security* (pp. 79-90). ACM.

Erdheim, J., Wang, M. and Zickar, M.J., 2006. Linking the Big Five personality constructs to organizational commitment. *Personality and Individual Differences*, *41*(5), pp.959-970.

Fisher, D.J., 2015. *The Millennial generation as an insider threat: high risk or overhyped?* (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Forgas, J.P. and East, R., 2008. On being happy and gullible: Mood effects on skepticism and the detection of deception. *Journal of Experimental Social Psychology*, *44*(5), pp.1362-1367.

Foster, J.D., Campbell, W.K. and Twenge, J.M., 2003. Individual differences in narcissism: Inflated self-views across the lifespan and around the world. *Journal of Research in Personality*, *37*(6), pp.469-486.

Furnell, S., 2010. Jumping security hurdles. *Computer Fraud & Security*, *2010*(6), pp.10-14.

Gable, G.G., 1994. Integrating case study and survey research methods: an example in information systems. *European journal of information systems*, *3*(2), pp.112-126.

Gardner, B. and Thomas, V., 2014. *Building an information security awareness program: Defending against social engineering and technical threats*. Elsevier.

Gentile, B., Twenge, J.M. and Campbell, W.K., 2010. Birth cohort differences in self-esteem, 1988–2008: A cross-temporal meta-analysis. *Review of General Psychology*, *14*(3), p.261.

Get Cyber Safe, 2013.*Phishing: How many take the bait?* http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx(18/02/2017)

Gorling, S., 2006. The myth of user education.

Gosling, S.D., Rentfrow, P.J. and Swann, W.B., 2003. A very brief measure of the Big-Five personality domains. *Journal of Research in personality*, *37*(6), pp.504-528.

Hadnagy, C., 2010. *Social engineering: The art of human hacking*. John Wiley & Sons.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L., 1998. *Multivariate data analysis* (Vol. 5, No. 3, pp. 207-219). Upper Saddle River, NJ: Prentice hall.

Hale, M.L., Gamble, R.F. and Gamble, P., 2015, January. CyberPhishing: a game-based platform for phishing awareness testing. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on* (pp. 5260-5269). IEEE.

Halevi, T., Memon, N. and Nov, O., 2015. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks.

Halevi, T., Lewis, J. and Memon, N., 2013, May. A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd International Conference on World Wide Web* (pp. 737-744). ACM.

Hänsch, N. and Benenson, Z., 2014, September. Specifying IT security awareness. In *Database and Expert Systems Applications (DEXA), 2014 25th International Workshop on* (pp. 326-330). IEEE.

Hong, J., 2012. The state of phishing attacks. *Communications of the ACM*, *55*(1), pp.74-81.

Howe, N. and Strauss, W., 2009. *Millennials rising: The next great generation*. Vintage.

Hurst, J.L. and Good, L.K., 2009. Generation Y and career choice: The impact of retail career perceptions, expectations and entitlement perceptions. *Career Development International*, *14*(6), pp.570-593.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F., 2007. Social phishing. *Communications of the ACM*, *50*(10), pp.94-100.
Jakobsson, M. and Finn, P., 2007. Designing and conducting phishing experiments. *IEEE Technology and Society Magazine, Special Issue on Usability and Security*.

Jakobsson, M. and Myers, S. eds., 2006. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons.

Jakobsson, M., Johnson, N. and Finn, P., 2008. Why and how to perform fraud experiments. *IEEE Security & Privacy*, *6*(2).

Jakobsson, M. and Ratkiewicz, J., 2006, May. Designing ethical phishing experiments: a study of (ROT13) rOnl query features. In *Proceedings of the 15th international conference on World Wide Web* (pp. 513-522). ACM.

Jensen, A.R., 1998. The g factor: The science of mental ability.

Jiang, M., Tsai, H.Y.S., Cotten, S.R., Rifon, N.J., LaRose, R. and Alhabash, S., 2016. Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, *42*(9), pp.621-634.

Jones, H., 2016. *What makes people click: assessing individual differences in susceptibility to email fraud* (Doctoral dissertation, Lancaster University).

Karakasiliotis, A., Furnell, S.M. and Papadaki, M., 2006. Assessing end-user awareness of social engineering and phishing.

Knight, W., 2004. Goin'phishing?. *Infosecurity Today*, *1*(4), pp.36-38.

Kruger, H.A. and Kearney, W.D., 2006. A prototype for assessing information security awareness. *computers & security*, *25*(4), pp.289-296.

Kumar, A. and Lim, H., 2008. Age differences in mobile service perceptions: comparison of Generation Y and baby boomers. *Journal of services marketing*, *22*(7), pp.568-577.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F. and Hong, J., 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, *10*(2), p.7.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A. and Pham, T., 2009, July. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (p. 3). ACM.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L.F. and Hong, J., 2007, October. Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 70-81). ACM.

Lin, F.J., 2008. Solving multicollinearity in the process of fitting regression model using the nested estimate procedure. *Quality & Quantity*, *42*(3), pp.417-426.

Livingstone, S., Bober, M. and Helsper, E., 2005. Internet literacy among children and young people: Findings from the UK Children Go Online Project.

Long, R.M., 2013. Using phishing to test social engineering awareness of financial employees.

Lorenz, B. and Kikkas, K., 2012, June. Socially engineered commoners as cyber warriors-Estonian future or present?. In *Cyber Conflict (CYCON), 2012 4th International Conference on* (pp. 1-12). IEEE.

Macky, K., Gardner, D. and Forsyth, S., 2008. Generational differences at work: Introduction and overview. *Journal of Managerial Psychology*, *23*(8), pp.857-861.

Manjak, M., 2006. Social Engineering Your Employees to Information Security. http://www.sans.org/reading_room/whitepapers/engineering/1686.php (13.03.2018)

Maxwell, A.E., 1971. Analysing qualitative data.

Miltgen, C.L. and Peyrat-Guillard, D., 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), pp.103-125.

Mitnick, K., 2011. *Ghost in the wires: My adventures as the world's most wanted hacker*. Hachette UK.

Mitnick, K.D. and Simon, W.L., 2011. *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mitnick, K.D. and Simon, W.L., 2009. *The Art of Intrusion: The real stories behind the exploits of hackers, intruders and deceivers*. John Wiley & Sons.

Modic, D. and Lea, S.E., 2012. How neurotic are scam victims, really? the big five and internet scams.

Mohebzada, J.G., El Zarka, A., BHojani, A.H. and Darwish, A., 2012, March. Phishing in a university community: Two large scale phishing experiments. In *Innovations in Information Technology (IIT), 2012 International Conference on* (pp. 249-254). IEEE.

Montgomery, D.C., Peck, E.A. and Vining, G.G., 2012. *Introduction to linear regression analysis* (Vol. 821). John Wiley & Sons.

Ng, E.S., Schweitzer, L. and Lyons, S.T., 2010. New generation, great expectations: A field study of the millennial generation. *Journal of Business and Psychology*, *25*(2), pp.281-292.

Ng, E., Lyons, S.T. and Schweitzer, L. eds., 2012. *Managing the new workforce: International perspectives on the millennial generation*. Edward Elgar Publishing.

Nohlberg, M., 2005. Social Engineering Audits Using Anonymous Surveys: Conning the Users in Order to Know if They Can Be Conned. In *4th Security Conference, Las Vegas, USA, March 30–31, 2005*.

Palfrey, J.G. and Gasser, U., 2011. *Born digital: Understanding the first generation of digital natives*.

Parment, A., 2013. Generation Y vs. Baby Boomers: Shopping behavior, buyer involvement and implications for retailing. *Journal of retailing and consumer services*, *20*(2), pp.189-199.

Parrish Jr, J.L., Bailey, J.L. and Courtney, J.F., 2009. A personality based model for determining susceptibility to phishing attacks. *Little Rock: University of Arkansas*.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C., 2013, July. Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In *IFIP International Information Security Conference* (pp. 366-378). Springer, Berlin, Heidelberg.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A. and Butavicius, M., 2012. Why do some people manage phishing e-mails better than others?. *Information Management & Computer Security*, *20*(1), pp.18-28.

Prensky, M., 2001. Digital natives, digital immigrants part 1. *On the horizon*, *9*(5), pp.1-6.

Prince, M., 2004. Does active learning work? A review of the research. *Journal of engineering education*, *93*(3), pp.223-231.

Purkait, S., 2012. Phishing counter measures and their effectiveness–literature review. *Information Management & Computer Security*, *20*(5), pp.382-420.

Roberts, B.W., Walton, K.E. and Viechtbauer, W., 2006. Patterns of mean-level change in personality traits across the life course: a meta-analysis of longitudinal studies. *Psychological bulletin*, *132*(1), p.1.

SANS Institute. Employee security awareness survey.

https://www.sans.edu/student-files/awareness/employee-security-awareness-survey.pdf (06.03.2017)

Schneier, Bruce. 2000. Semantic Attacks: The Third Wave of Network Attacks. *Cryptogram Newsletter* http://www.schneier.com/crypto-gram-0010.html (26.02.2017).

Scollon, C.N. and Diener, E., 2006. Love, work, and changes in extraversion and neuroticism over time. *Journal of personality and social psychology*, *91*(6), p.1152.

Sessa, V.I., Kabacoff, R.I., Deal, J. and Brown, H., 2007. Generational differences in leader values and leadership behaviors. *The Psychologist-Manager Journal*, *10*(1), pp.47-74.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.J., 2009. The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), pp.92-100.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J., 2010, April. 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* (pp. 373-382). ACM.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E., 2007, July. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99). ACM.

Snyder, C., 2015. Handling Human Hacking: Creating a Comprehensive Defensive Strategy Against Modern Social Engineering.

Smits, I.A., Dolan, C.V., Vorst, H., Wicherts, J.M. and Timmerman, M.E., 2011. Cohort differences in Big Five personality factors over a period of 25 years. *Journal of personality and social psychology*, *100*(6), p.1124.

Solnet, D., Kralj, A. and Kandampully, J., 2012. Generation Y employees: An examination of work attitude differences. *Journal of Applied Management and Entrepreneurship*, *17*(3), p.36.

Srivastava, S., John, O.P., Gosling, S.D. and Potter, J., 2003. Development of personality in early and middle adulthood: Set like plaster or persistent change?. *Journal of personality and social psychology*, *84*(5), p.1041.

Stebila, D., 2010, November. Reinforcing bad behaviour: the misuse of security indicators on popular websites. In *Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction* (pp. 248-251). ACM.

Stein, J., 2013. Millennials: The me me me generation. *Time magazine*, *20*, pp.1-8.

Stewart, K.D. and Bernhardt, P.C., 2010. Comparing Millennials to Pre-1987 Students and with One Another. *North American Journal of Psychology*, *12*(3).

Twenge, J.M. and Foster, J.D., 2010. Birth cohort increases in narcissistic personality traits among American college students, 1982–2009. *Social Psychological and Personality Science*, *1*(1), pp.99-106.

Twenge, J.M. and Campbell, W.K., 2008. Increases in positive self-views among high school students: Birth-cohort changes in anticipated performance, self-satisfaction, self-liking, and self-competence. *Psychological Science*, *19*(11), pp.1082-1086.

Twenge, J.M., Konrath, S., Foster, J.D., Keith Campbell, W. and Bushman, B.J., 2008. Egos inflating over time: A cross-temporal meta-analysis of the Narcissistic Personality Inventory. *Journal of personality*, *76*(4), pp.875-902.

Twenge, J.M., 2000. The age of anxiety? The birth cohort change in anxiety and neuroticism, 1952–1993. *Journal of personality and social psychology*, *79*(6), p.1007.

Uebelacker, S. and Quiel, S., 2014, July. The social engineering personality framework. In *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on* (pp. 24-30). IEEE.

Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R., 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), pp.576-586.

Weirich, D. and Sasse, M.A., 2001, September. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 137-143). ACM.

Wey Smola, K. and Sutton, C.D., 2002. Generational differences: Revisiting generational work values for the new millennium. *Journal of organizational behavior*, *23*(4), pp.363-382.

Wikipedia. *Phishing* https://en.wikipedia.org/wiki/Phishing. (03.03.2017)

Wikipedia.*Social Engineering(security)* http://en.wikipedia.org/wiki/Social_engineering_(security)/ (20.02.2017)

Winkler, I. and Manke, S., 7. Reasons for Security Awareness Failure. *CSO Security and Risk*. http://www.csoonline.com/article/2133697/metrics-budgets/7-reasons-for-security-awareness-failure.html/ (20.02.2017)

Workman, M., 2008. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the Association for Information Science and Technology*, *59*(4), pp.662-674.

Wright, R.T. and Marett, K., 2010. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), pp.273-303.

Wright, R., Chakraborty, S., Basoglu, A. and Marett, K., 2010. Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation*, *19*(4), pp.391-416.

Wu, M., Miller, R.C. and Garfinkel, S.L., 2006, April. Do security toolbars actually prevent phishing attacks?. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 601-610). ACM.

Zibran, M.F., 2007. Chi-squared test of independence. *Department of Computer Science, University of Calgary, Alberta, Canada*.

Appendix

I. The Social Engineering security awareness and training framework layout for any high school to corporate in its curricula

- **National School Security Policy and procedures**
  - SE security scope
  - Objectives
  - Duties and limitations

- **Program design**

  This phase of the program reveals the first impact to its approach since it outlines the particular objectives the program aims to meet. Such, the overall strategy should be developed complying with the school requirements and students security needs. It ought to clearly identify school's security policies and standards, the communication channels used and needs for such a program to include in the school curricula. In other words it should list out crucial elements of the program before implementing it. Having said that, the program of this nature should be planned on detail, after a long period of time collecting ideas, pointing out expectations and identifying intended goals.

  Via incorporating any existing technique proven to reduce individuals susceptibility, the program should be designed making students understand the necessity to include a SE security training program in their school curricula, along with making them recognize school's IT security policies and their security responsibilities.

- **Program management**

  In order to achieve the aspired goals it is crucial to put particular emphasis on the program management, hence this thesis proposes to settle it on a central authority. Every school should establish a **security awareness team** to carry out the whole on-going program and as such, the program effectiveness responsibility to be mainly concentrated on this asset. Therefore, the team should work on each program's element and instill compliances towards obtaining its objectives. It should manage the bullet points of the strategy: policy enforcement (schools security policy should be practical enough to ensure students acceptance and compliance), successful promotion of the security program and make decisions on how often the program will be implemented (note that it is very taught to achieve security consciousness by running the program once, twice or three times a year). Being part of the school curricula, the program should be persistent, a continual event to implement.

- **Program development**

  Development of the training content via establishing its core scope and the designed strategy is carried out. The selection of the training resources should be addressed keeping in mind students needs and their approach to learning (in achieving to bolster their SE security skills). Being a fundamental asset of any learning theory, awareness material of the program should be chosen to be both low cost and efficient in delivering the Social Engineering security message. The campaigns content should be simple, short and straight to the point. Towards retaining students competence to Social Engineering defense, the security policy development is trivial for this program. Hence, sufficient documents listing goals, limitations and expectations of school should be created. The overall program must be set complying the school's vast array of requirements via outlining students security duties and limitations.

- **Program implementation**

  Once have gone through all the above phases of the training strategy and being equipped with clear-cut goals, implementing the program is the final step in achieving to render the adequate SE fortification. Additionally, beneficial communication channels and training material delivery mediums should be on place while implementing the training (prefer class-based instead of web-based or distance-learning). In the broadest view, such robust training can undoubtedly achieve hardening the millennial students falling for Social Engineering. Delivering the training periodically, continual implementation of lessons learned and feedback, is the best way to reach program's testing and evaluation.

- **Program evaluation**

  Even-though this is a post-implementation step, constructive testing is core to maintain in a on-going security awareness program. It directly addresses the training efficiency via monitoring and evaluation of the program. By selecting effective evaluation methods to carry on (conducted questionnaires, focus groups, interviews, periodic assessment of school's security awareness), it provides opportunities to improve students training for the next implementation. Furthermore, feedback is crucial in any on-going process, as it provides chances to patch management or perform program updates to reach better results on upcoming sessions. Beyond measuring the program's accessibility via periodic reviews worth performing, it safeguards targets from serious endangerment of falling prey of SE attacks. The inclusion of motivational drivers on the very roots of the program leads to the most efficient arsenal towards fighting Social Engineering.

II. List of topics to be included in any high-school SE security awareness and training program

Here are listed some core awareness and training topics to be covered by the program. Note that the list should be modified and updated after each program reimplementation.

- The program's focus ...
- What is Social Engineering ?
- Are we even affected ?
- Why do we need to be aware of SE threats ?
- The weakest link of the security chain ...
- Are we vulnerable towards these attacks ?
- What are the SE weaknesses making us vulnerable ?
- Reasons choosing a specific audience (target group) for the training.
- What are our security responsibilities towards SE ?
- Understanding the necessity of Social Engineering security.
- Explaining the necessity of a SE security awareness and training to corporate in the school curricula.
- Deploying motivation and interest in the program.
- Identify the intended social engineering security awareness attitude to achieve.
- Identify the intended social engineering security training skills to achieve.
- Study real-case scenarios of popular Social Engineering attacks.
- Identify the importance of Question&Answer sessions of the training.
- List the most common SE attack forms and analyze techniques deployed by attackers.
- Policy understanding and compliance.
- PASSWORD security.
- Phishing, the criminals most favorite SE attack.
- Social Engineering on Social Networking sites, what to be careful about ?
- Define effective communication channels for the program.
- The importance to conduct evaluations for the program.
- Adjust the program implementing the lessons learned, students feedback and reviews.

- Review objectives: what were goals the program planned to reach (the objectives specifically are to ensure social engineering security awareness and build security skills in regards) and were they reached ?
- The frequency of program implementation.

III. Students questionnaire to assess their general knowledge and viewpoint on the issue

NOTE: This can be carried out before designing the program in order to address the core points (identify students knowledge, attitude, and perspective in regards to social engineering) to include in the training.

1. What is Social Engineering?

2. What human weaknesses social engineering attacks mostly exploit?

3. Which social engineering attack types you think you are more vulnerable to?

4. List the first protection measures you personally would take to protect against social engineering?

5. What do you think are your security needs and obligations?

6. What personality aspects you find more vulnerable to social engineering attacks?

- commitment
- social proof
- Big 5 personality traits
- reciprocity
- liking
- any other you could specify

7. Do you consider yourself vulnerable to social engineering threats ?

8. What do you think is the weakest link in the security chain ?

9. What do you think are the adequate countermeasures to social engineering ?

10. Are you aware of your school security policies ?

a) yes b)no c)somehow d)our school do not have any

IV. Evaluating the training effectiveness questionnaire

(same approach can be followed using other evaluation methods such as: surveys, interviews, etc, for every post-implementation of the training)

1. From 1-10 score the relevance of the implemented security awareness and training program at your school?

2. What were your expectations of your school social engineering security awareness and training program?

3. List any motivational driver that made you focus more attention to the training?

4. How applicable are your school policies and standards, and which of the following do you find the least applicable?

a) physical security policies b) computer security policies(password policies)

c) person verification policies d) guest acceptance policies

5. Which would be the best way (communication channel) to deliver the school awareness and training material:

- ✓ The school monthly security newspaper
- ✓ Posters campaigns
- ✓ Monthly security days
- ✓ Security tip of the day
- ✓ Catchy slogans on the school webpage
- ✓ SE security workshops
- ✓ Other (your proposal)

6. What are the main elements you find relevant to build social engineering security habits?

7. How do you rate the complexity of the training material delivery and understanding?

very easy complex very complex do not know

8. How do you assess your SE knowledge/awareness/security skills after the deployment of the school training (comparing these before integrating the program in the curricula and now) ?

Limited

Considerable

High

Expert

9. Were the program objectives and your expectations met?

10. What do you think should be improved in the next coming program implementation?

11. Please list any additional comments/ remarks for the program as a whole or for any element of it ?

12. Overall, I think my SE security awareness and behavioral capabilities have improved due to the training. (please, give also your comment)

- Agree
- Disagree
- Neutral
- Do not know
- Not at all

V. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Lejla Islami**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:
   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and
   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

Assessing generational differences in susceptibility to Social Engineering attacks. A comparison between Millennial and Baby Boomer generations.

supervised by Olaf Manuel Maennel und Raimundas Matulevicius

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

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

Tartu, **20.05.2018**