universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„CRM Support for creating IT Security Awareness with Electronic Banking customers“

verfasst von / submitted by

Nino Gelashvili

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Diplom-Ingenieur (Dipl.-Ing.)

Wien, 2017 / Vienna 2017

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 926
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Wirtschaftsinformatik
Betreut von / Supervisor:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

To Mom

who has been my rock and

encouragement throughout my life

Acknowledgement

I would like to thank my supervisor, Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr, who provided a tremendous help in completing this thesis. I am particularly grateful for his valuable and constructive suggestions, his patience and time, as well as support and guidance in moments of the creative standstill.

I would like to express my appreciation to the employees of the Center of Free Pedagogics for their help in the prototype evaluation. I thank them for their support and a positive attitude towards my request, as well as for prompt response and for the time spent.

I thank my family for their moral and emotional support, encouragement and immense help throughout my study. I thank them for giving me the opportunity and support that made this study possible.

Table of Contents

List of Figures

List of Tables

Chapter 1 | Introduction

All modern financial institutions, as well as other companies that interact with sensitive data as part of their work, pay a particularly good attention to information security. They employ highly trained security specialists, invest in the best security technologies on the market and make sure their policies are up to date for the ever-changing IT security threat patterns.

However, with these technologies in place it is possible to end up with false sense of security (Mitnik, Simon 2003). Biggest vulnerability to the integrity of sensitive data is a human factor. Be it intentional or not, human actions might create security breaches that cannot be prevented or recovered by the technology.

IT Security as a whole - is a set of measures and should be perceived as a system. It has different aspects that cannot be under or overrated, every part of these measures is important and disregarding any one of them will cause the collapse of the whole system. To ensure highest level of computer security every contact point of the system with the aggressive environment must be monitored and covered. People working with information must be also considered a part of the security mechanism, a link that needs to be strengthened by education about technology, general operability and newest security measures.

1.1 Motivation

Over the years the Internet became an influential technology for our everyday lives, providing the opportunity to connect people worldwide, conduct businesses globally and enhance operational performance. With progressing development of remote banking services, the volume of monetary and banking transactions conducted over the Internet reached new heights. "Internet banking has the scope to grow through demographic changes and increased access to broadband connections throughout the country." (SOAS 2016, p. 10)

Many countries and their banks are beginning to discourage cash payments which pushes the non-cash payment methods, including online transactions to thrive even

more (CapGemini 2016, p.11). Growing online financial activity is becoming an attractive playground for cyber criminals. Number and sophistication of threats is increasing at such pace, that it becomes immensely difficult to be updated about most recent issues. This is where the knowledge and awareness of customers about current risks gains high importance.

For a long while information security and training programs in security were associated only with technical solutions such as firewalls, access controls, intrusion detection systems and many other software and hardware. While these approaches were perfected from year to year, human element was not considered an issue. Only recently the organizations began the re-evaluations of security measures and focusing on educating and training the employees. Today, implementation of strong security policies, including security-related issues as a part of organizational training strategy and acquiring mechanisms to promote IT security awareness during day-to-day activities has become as natural as setting up a firewall and using anti-malware programs.

Banks have to take proactive approach and make customer education policies a part of their business strategy. Additionally, this approach keeps customers up to date about trending IT security topics, eliminating thus majority of threats that can be caused by human error. On the other hand, such policies create loyal customers.

The purpose of this work is to identify the existing IT security issues that the customers of electronic banking are facing day to day and create a Security Awareness tool for raising and maintaining the high level of IT security awareness among the customers. The relevance of this study is very high for the banking sector of Georgia, given the fact that electronic banking and Customer Relationship Management systems are relatively new implementations; a complete lack customer awareness or low awareness level about IT security issues is still a big concern among the banks.

This thesis proposes a substantial change in methods of educating electronic banking customers about IT security and proper use of the electronic banking system, consequently, avoiding the danger of losing the sensible information. The goal is achieved by creating a two-way (mutual) connection between customer and the online banking system via CRM approach. This unconventional method of teaching ensures an individual approach to the customers, making them part of the big process and

boosting therefore their motivation. It is important to find a creative way of delivering an educational information to a customer in a way that is most acceptable for them and generates genuine interest for the topic. In its turn customer motivation guarantees the full involvement in the process and higher level of productivity and positive outcome. "It is giving the right information to the right people in the right form." (Lacey 2009)

1.2 Problem Definition

Communities and organizations are increasingly dependent on computers and Internet for automating their processes in order to increase efficiency and reduce time and resource consumption. We rely on computers and networks to store, manage and transfer sensitive information, thus creating ideal environment for cyber criminals and hacktivists, who prefer using scattering techniques such as phishing or exploiting avoidable weaknesses.

As the world is becoming more digital, an intuitive and highly secure digital experience is vital for any organization, however the security of that experience depends on how well the organization can manage the threats and other risks. The proactive strategies include updating data governance policies and developing employee training on matters of cyber security (PWC 2017).

While the security technologies become sophisticated and advanced, they will never be impenetrable. Cyber criminals are keeping up with the latest improvements and develop even more elaborate bypass tactics and counteract protection mechanisms. "[..] the importance of protecting our electronic assets has existed for some time, the amount of sensitive and personally identifiable information that is now available and accessible globally calls for increased security measures." (LeClair et al. 2013, p. 71)

In order to build the strong defensive systems, it is important to identify both existing and potential threats.

In developing countries, such as Georgia, customers are just starting to rely majorly on their computers for the daily operations and financial transactions, which poses the need for remote banking services like online banking to be available for everyone.

Since an electronic banking system is relatively new to Georgian customers, physical availability does not guarantee that the services will be widely used.

According to LeClair et al. (2013), the protection of cyber assets, e.g. monetary information, private and sensitive data, requires a collaborative approach of government, academia and industry. In case of Georgia, the government has yet to consider developing up-to-date and refined legal and regulatory measures.

Even though most of the leading banks in Georgia have developed necessary regulations for remote banking services and their electronic banking systems meet the modern safety standards, the problem of delivering information to the users remains unsolved. Although the numbers of online banking users are growing every year, the growth is not nearly fast enough. Due to the lack of an academic component in developing a security system of the Georgian banks, the significant factor against an adoption of this new technology remains the fear of unknown.

The most common eBanking security threats for last five years are extortion of the information via ransomware attacks, adware, malware, keyloggers, phishing, Trojans and viruses (Subsorn, Limwiriyakul 2012). All those threats target mostly the customers' computers, making them a weak link in banking elaborate security system. According to (Howarth 2014) 95% of security incidents that took place in 2014 were caused by human error. "Internet thieves try to extract personal financial data through malware, key-logging devices, point-of-sale skimming of bank data and other forms of high-tech skulduggery. [...] Customers must not be careless with their personal banking details, and banks constantly remind customers to safeguard those details, particularly their PINs." (SOAS 2016, p. 8)

While the bank is able to provide ongoing employee training, alternative ways for customer education like seminars, lectures etc. have a number of shortcomings and are therefore virtually non-existent. Other than being costly and time consuming for both the bank and customers, research shows, that traditional adult education methods lack scalability and efficiency due to the rapidly changing environment of cyber security and constant need of updating the learning material (LeClair et al. 2013).

In order for a bank to stand out from their competition, there arises a need for effective learning platform for training and educating large numbers of adult learners. The

platform that should prove cost efficient, "[...] affordable and flexible strategies which cater to the needs of working employees and adult learners." (LeClair et al. 2013, p. 73)

This thesis work proposes a customer-centric andragogical platform that is incorporated in bank CRM system and targets individual customers via their online banking page and provides appropriate content based on their prior knowledge and level of awareness about Information Security.

1.3 Goal and Objectives of this Work

The main goal of this work is to create and maintain customer awareness level about IT security issues by creating an environment for the customers in which they can receive information about basic security according to their prior knowledge and learning rate.

The objectives for achieving this goal include:

- Study the theoretical aspects of CRM approach to customer learning; based on this study it will be easier to determine whether it is necessary to develop a completely new approach to customer education via CRM or there already exist solutions that can be used and adapted for achieving the set goal.
- Study the current state/situation of customer education methods in Georgia; this objective includes developing a detailed questionnaire, which allows us to collect customer data for further situational analysis;
- Identify security issues as perceived by customers;
- Identify objectively most sensitive areas and common issues; we can identify current most common security issues and address them accordingly when creating an adapted curriculum for the support tool;
- Determine optimal ways for increasing customer awareness level;
- Develop a process-oriented model of the system;
- Implement the support tool;
- Develop or choose the existing methods for approbation of the implemented support tool.

1.4 Structure of the Thesis

This thesis consists of eight chapters making up the two main parts: theoretical part, which provides an introduction to the master thesis and an overview of current state and advancement level of banking sector in Georgia and the eBanking customers. This part also covers the topics of approaches towards the customers' education and existing IT security issues; practical part outlines the development process of a support tool and its further testing and evaluation.

Chapter 1 presents the background of this thesis and discusses the problem definition, motivation behind the work and identifies thesis objectives and goals.

Chapter 2 provides an overview of the current situation on the research topic in Georgia. Additionally, this chapter provides an analysis of the target audience by means of an empirical study.

Chapter 3 covers the relevant literature and provides a review and base knowledge for further work.

Chapter 4 describes the process-oriented model of the support tool which is developed as a part of the research.

Chapter 5 provides a technical description of the prototype implementation.

Chapter 6 covers the topic and details of prototype testing and the evaluation results.

Chapter 7 presents discussions and reflection on the overall results obtained. Additionally, it covers the topics and ideas for further work.

Chapter 8 presents conclusion and last remarks.

Chapter 2 | Situational Analysis

This chapter provides an overview about the current situation in Georgia in terms of IT and eBanking technology adoption by the population; it also provides three different viewpoints towards the approaches to the IT security, which should work together for increased effectiveness of the protection of the cyber assets. The second part of the chapter provides a picture and provides a picture of an average customer of a Georgian bank, based on the conducted empirical study.

2.1 Current Situation

Today almost every Georgian bank uses modern electronic payment systems for their distant banking services. A demand for the presence of electronic banking is growing every year and becomes a make or break point when it comes to choosing a bank. In Georgia, electronic commerce is just starting to grow and although it still develops at a slow pace, adoption of new technologies seems to have a steady upward trend. Major Georgian banks are working hard to adopt best practices developed by countries that are much farther ahead in technical development. Peculiarities of using western banks' experience in modern Georgian market require continuous improvement, alongside with building awareness about general banking terminology and more in-depth knowledge about security issues.

According to statistical report for 2016 of National Statistics Office of Georgia[1], by June 2016, the population of Georgia closes to 3.7 million people, that is 2.1 and 1.6 million people in urban and rural areas accordingly. A gap between educational backgrounds brings forward the importance of distinguishing users from urban population and users from rural areas. A difference in education levels creates distinctive patterns of Internet use [research purposes, online transactions, online shopping, exclusively for social media use, etc]. 64.7 percent of Georgian households (avg. 2-3 persons per household) possess a computer [urban - 76, village - 24], 70 percent additionally have Internet and/or mobile Internet access (approx. 56 thousand people) [79 percent of urban population, 57.7 percent of the rural population]. 86

[1] http://geostat.ge/

percent of people use their computer and Internet every day [48 thousand people]. Only 19 percent of the whole population uses the Internet for online shopping, that is 23.8 percent of all urban population and 7.6 percent of all rural population, who have both computer and Internet access. Geostat does not provide any data about use of electronic banking; however, a survey, conducted for the purposes of this study, spread some light on these numbers [299 people]. Although 61 percent of surveyed people use electronic banking and have formed a vague opinion about the technology, a demand for human interactions with a bank representative to answer questions, provide guidance for the transaction processes or validate their initial decision is still high. "This need for validation from bank personnel who are regarded by customers as experts in their field is reinforced by the view that the average person finds banking products to be complex, not only in terms of the specific features of the product but also because of the 'legalese' embedded in the language of the documentation that often accompanies bank products and services." (SOAS 2007, p. 26)

Consequently, the volume of online retail and online transactions in Georgia is lower than one of traditional retail. This is caused, among others, by the low quality of life, low awareness level about electronic commerce in general, as well as the high complexity of banking infrastructure and modern payment mechanisms. Additionally, main problems in the regulation of electronic commerce and electronic banking activities via a global computer network are the following circumstances: indefinite legal status of the computer network and tremendous difficulties in resolving issues of state jurisdiction.

Protection of cyber security assets should be a collaborative task for organizations, end users, and government. With a collective effort, there exist bigger chances of withstanding cyber-attacks and malicious actions (LeClair et al. 2013, p. 71). Regarding Georgia, two of the three links are still to be promoted; while the government is obligated to establish a legal base for these issues, there are no legal obligations for the banks. Thus, the problem of educating end users is completely disregarded. The concept "awareness of the end user about IT safety" has at the moment dim and abstract character.

2.1.1 Government

"Since the restoration of its independence in 1991, Georgia has undergone a substantial political transformation from a constituent republic in a federal socialist state to an independent sovereign democracy" (TBC Bank 2015, p. 50). A legislative and normative base for protection of consumer rights, a popularization of electronic commerce, cyber security, data protection and privacy remain on government agenda since 2010 (Netgazeti, 2010); however, by the year 2016 only data protection directives have been developed.

The association agreement between the European Union and Georgia signed in 2014 requires the government of Georgia to uphold the European standards concerning electronic commerce (Official Journal of the European Union 2014). "Georgia is continuously developing an adequate legal framework required for the proper functioning of a market economy. Several fundamental Georgian civil, criminal, tax, administrative and commercial laws are frequently amended as per the legislative standards of continental Europe. Moreover, as a result of the conclusion of the EU-Georgia Deep and Comprehensive Free Trade Agreement ('DCFTA'), Georgia's laws and enforcement standards will have to be fully harmonized with the EU standards." (TBC Bank 2015, p. 50)

The absence of state regulations on online banking and protection of consumer rights results in low adoption pace of the technology and dissatisfaction of existing consumers, due to fear of unknown and lack of transparency. "Every banking system requires prudential regulation" (SOAS 2007, p. 6), otherwise some banks take unawareness of consumers as an advantage. They advertise an absolute online security guarantee; however, they hold their customers responsible for any financial loss that was caused by e.g. phishing attacks or identity theft (Zaabi, Tubaishat 2015, p. 80).

2.1.2 Banks

An in-depth research about the laws and regulations about electronic banking in Georgia also revealed a distinct lack of information about electronic banking provided by the financial organizations themselves. As part of an examination, we consider both

subjective and objective point of view on completeness of such information. Subjective information on customer perspective was collected via the questionnaire. A most effective way of analyzing whether the information is objectively sufficient proved to be the creation of electronic banking security checklist (Subsorn, Limwiriyakul 2012, p. 262).

Analysis carried out on the base of the checklist revealed the inadequacy of both general and security information in all the major Georgian banks. This fact exposes banks not only to harm of reputation and confidentiality but might also drive away potential customers.

As the subject of the closer examination, for the purposes of this master thesis, we will be considering one of the leading Georgian banks. "TBC Bank offers a wide range of banking products and services to its retail, corporate, SME and micro clients." (TBC Bank 2015, p. 3)

TBC was one of the first banks to develop and implement Customer Relationship Management (CRM) system and address the value of customer centricity in corporate culture by improving customer experience and shortening the decision-making processes. "[T]he Bank completed a full integration of CRM capabilities in all of its business lines, including through remote banking channels enabling the Bank to better customize product offerings to its customers." (TBC Bank 2015, p. 30)

An analysis of internet banking security features of the Bank that was based on the checklist, suggested by Subsorn and Limwiriyakul and adapted for Georgian bank, revealed weakness in delivering internet banking security information to customers, general deficiency of that information and partial lack of transparency on bank security management system and banks site authentication technologies, as well as lack of several security mechanisms and necessary secure customer authentication.

The Bank website does not provide information about compliance with the national privacy principles and privacy law. On closer examination customer can learn that "[...] banking operations in Georgia are required to comply with Georgian banking regulations. In addition to mandatory capital adequacy ratios, the NBG sets lending limits and other economic ratios for banks in Georgia." (TBC Bank 2015, p. 45). However, since laws and regulations for electronic finance and internet banking are still

absent and therefore have not been in force, this fact consequently results in unclear or non-existent implementing regulations. Furthermore, there is no closer information about losses compensation guarantee and bank responsibilities for any losses occurred by phishing or other attacks on electronic banking customer.

A view into more technical features showed that bank does not offer any session management information on their website. Session management information such as cookies, page and session tokens would increase awareness as well as confidentiality to both existing and potential internet banking customers. There is also no information about bank site authentication technologies like employed encryption and digital certificates. Bank currently employs extended validation SSL certificate; however, one can only find this out by manual checking.

The Bank does not declare, whether it provides logging information such as the last log in and activity logs, however existing customers can confirm that logging information is provided on their private online banking page. For a customer authentication, both customer ID, as well as the password, is required. Two-factor authentication such as SMS, token devices or email is not provided. There is no explicit information about password requirements on the website, however, there are recommendations on the creation of secure passwords. The strength of the password is automatically checked when creating or changing the password.

Most Georgian banks provide limited general information guidelines on their website, however, there is a lack of internet banking security information about several current topics, e.g. keyloggers. There is also no information about internet banking security alerts or up-to-date issues.

This checklist analysis provides an overview on existing requirements for curricula that must be developed for an educational program for raising customers' security awareness about issues such as potential risks and threats, which is especially important given the fact that banks do not carry any responsibility for losses occurred by customers and non-authorized users.

2.1.3 Academia

”The biggest threat to a computer system is not a virus, an unpatched hole in a key program, nor a badly installed firewall. In fact, the biggest threat could be you." (Mitnik, Simon 2003)

While banks and other financial organizations are developing strategies to improve customer management and adopt a more customer-centric approach to business in order to eventually boost their sales, IT security and protection of cyber assets is falling back on technical capabilities of each organization. It is without question that elaborate security policies and technological advances have a crucial role in the organization's security chain, the human factor is very often left out and completely neglected. "Many times organizations overlook the human factor, a factor that security depends upon" (Metalidou et al. 2014, p. 425).

LeClair et.al identify three major aspects of security - people, process and technology. All three of these pillars must be considered when evaluating the effectiveness of an organizations security measures, and they must be integrated into the education program designed for the employees and for the customers. The success of a technology is based on a clever design of the system and processes. Moreover, while the technological aspect provides automated safeguards and strategies and actions to be taken to achieve a high level of security, the human error still makes the organization vulnerable to attacks both from outside, and from the inside.

Security is not so much of a product as it is a process. A process which involves technology and people. As Kevin Mitnik puts it, "security is not a technology problem - it's a people and management problem." (Mitnik, Simon 2003, p. 13)

People are easily manipulated into false assumptions and beliefs, especially if those people are ignorant about the subject matter. Humans tend to be careless, curious, gullible and naive which makes them perfect targets for social engineering (Kahraman 2005); social engineering has become one of the major threats to IT security in past several years. Consequently, the need for commitment to educating people involved in everyday life of the organization arises.

Georgian banks maintain a system of controls [based on Basel II/III requirements] that is designed to overlook and monitor operational risk and provide controls for fraud prevention. They maintain the high-quality systems both for physical and cyber security. On the educational part, most of the banks are failing to maintain a high level of IT security awareness amongst their employees and customers. As a solution, employees are provided training and seminars in Information Technology and Cyber Security. However, education of the bank customer has never been a topic. A customer is only ever mentioned in regard to credit risk management, never as a potential security risk.

"[I]nformation security awareness deals with the use of security awareness programs to create and maintain security-positive behaviour as a critical element in an effective information security environment." (Kruger, Kearney 2006, p. 289)

At this moment, there are no effective security training programs targeted at bank customers. The banks only provide limited information about the secure use of eBanking services on their web page in form of a PDF file or a plain text. The security guidelines and policies are only circulating within the organization and are not eligible for open access. An elaborate security policy is only effective if it is accessible and understandable to the target audience, and whereas bank employees might be trained and generally required to understand and comply to these policies a customer might be far from comprehending and accepting the necessary precautions (Furnell et al. 2002).

This circumstance creates the following dilemma: if a customer is savvy enough to search the bank website for security information and guidelines, they can search for more elaborate and in-depth information on the Internet; however if we consider our main target group to be customers who are more or less ignorant about Information Technologies and IT security, it is likely that they will not make an effort of searching the information on purpose.

Furthermore, while there might be various resources about security guidance and valuable security tips that are available within easy reach for the customers, they "do not offer the ability to test one's understanding in practice" (Furnell et al. 2002, p.354).

There are different ways of creating security awareness. This thesis proposes creating an educational program based on banking CRM system which will communicate to the

customers the information about security. It is important to provide learning venues, andragogy, based on the needs of an individual customer. "[I]t is recognized that working adults need a more flexible environment that the traditional education settings won't be able to offer." (LeClair et al. 2013, p. 74)

A flexible learning environment has a larger response and importance amongst working customers. Possibility of training around the clock, at a comfortable, individual pace and targeted content, as well as general design of educational program can have a great influence on the learning outcome; this can provide a meaningful educational experience for a customer, and a high security awareness level for the bank (LeClair et al. 2013, p. 74). By integrating this solution into an existing system and procedures of the bank it will prove to be a cost-effective way of training and educating large numbers of working customers. "It can run with minimal resource requirements, as there is much less need for a centralised training facility." (Furnell et al. 2002)

Online learning will promote the educational opportunities in cyber security and enable learners (customers) to "apply their daily use of technology into meaningful educational activities." (LeClair et al. 2013, p.74)

2.2 Empirical study

This chapter is dedicated to providing a closer look at an average e-Banking customer of any Georgian bank. The chapter covers topics of data collection technique, the reasoning behind the questions and the descriptive analysis of collected customer data. Based on the preliminary analysis results we can point out most common concerns and knowledge about security issues amongst the customers and address them later at development stage of the support tool. Data analysis is conducted with IBM SPSS Statistics, which provides a clear overview of data and offers a variety of analysis options.

2.2.1 Preparation

Data can be interpreted in many different ways depending on existing initial interests and set goal questions, therefore it is vital to determine exactly what information do we

need for this study. Difficulty in data interpretation might be caused by the abstract nature of collected responses, meaning that seemingly same results might paint radically different pictures when coming from respondents with drastically different backgrounds, be it social or economic. In many cases, the studied situation can only be successfully reflected if we add a general assumption of social-economical norms of people's background (Atteslander, Cromm 2003).

Without considering these norms the survey results may give scattered and inaccurate depiction. For this reason, the previous chapter provides a short study of the economic and social situation in Georgia, which will provide the needed background information for understanding and 'interpretation' data in further chapters.

Because the main goal for this study is educating and raising customer awareness about IT security issues in electronic banking in Georgia, the main objective of conducting the empirical study is to collect information about e-Banking users' customs, motivations behind their actions and their demands. For this purpose, it is essential to identify the right questions to be answered by the collected data. Variables, analysis methods, and visualizations must be then selected accordingly.

If we operate under the assumption that a general awareness level of a customer is lower than average, then the following questions must be answered:

- Is the awareness level low because of the lack of information provided?
- Is it low because of the lack of interest to learn amongst the customers?
- Is the system too complicated for customers, thus causing the information to get lost without reaching the customer?
- Is the message delivery method wrong?
- What kind of change, if any, are the customers envisioning?

Questions can be answered by evaluating data collected via questionnaire. Data analysis helps assess the customers' perspective of the situation, which will be translated into deriving appropriate techniques and methods of message delivery to the customers by the educational tool, which in its turn will have increased effectiveness when adapted to fit the abilities of an individual customer.

2.2.2 The Conducted Survey

In this chapter, the processes behind the development and design of the questionnaire are explained. Additionally, the chapter looks closer into some peculiarities of delivery methods of the questionnaire to participants and identifying the target population by geographic area.

2.2.2.1 The Questionnaire

The main objective was to create a questionnaire which would help collect all the essential data, but at the same time would not be overcomplicated and would not drive the potential respondents away. The questionnaire consists of 37 questions altogether. It includes several types of questions to ensure that every important data is collected and nothing is missed. The types of questions are following:

Demographic questions: this type of questions is the key part of any survey, they include parameters like age, income group, occupation, social status, etc. These questions are used to identify characteristics of a respondent, they provide background information about the person and provide better insights into the target group we are currently studying.

Dichotomous questions: generally, these are fixed Yes or No questions. They are designed to help "screen" survey participants or assign them to categories, which is useful when determining customers who will be most relevant to the study.

Multiple choice questions: there are two sub-types for these questions - a single-answer multiple choice question and multiple-answer multiple choice question. In this case, respondents are provided with several answers to the given question and are asked for single or multiple answers.

Matrix questions: are used when several questions in a row have the same answer option. The answers can be of dichotomous, ranked or scaled type.

Likert scales[2]: The answers to these questions are given in form of a ranged scale that goes from one extreme attitude to another.

[2] https://www.surveymonkey.com/mp/likert-scale

Open-ended question[3]: It is an empty field, such as "other" option for a multiple-choice question or "remarks/comments" at the end of the survey, which can be filled by survey participants their own words, adding more detailed descriptions or explanations (Burgess, 2001).

The latter type of questions was provided to collect additional information that might have been missing on the questionnaire, however, during the actual survey process, these fields remained empty.

Structurally, the questionnaire is divided into three nominal categories:

Demographic data: it handles the age group, education, occupation, social status, income group and two yes or no questions - whether the respondent has a computer and whether they have access to the Internet.

E-Banking experience: this section starts off with filter yes or no questions, which redirect respondents to the specific sections of the survey according to their answer. The category is dedicated to collect existing e-Banking customer experience on the one hand and analyze the reasons behind not using electronic banking by the respondents on the other.

Behavioral data: this section includes just five questions to paint a picture about customers habits with regards to basic security measures such as logout, password changes, password sharing, antivirus use and handling cache and cookies.

The questionnaire is constructed in the way that is inviting and not overwhelming, thus the limited number of questions. The heading provides short information about the aim of the survey and brief explanation of the study along with the assurance that the data will be fully confidential and will be handled with delicacy. In order to keep respondent engaged in the survey the questions are short and easy to understand (Burgess, 2001). Answers to the question are never divided between pages, for the respondent not to miss any of available answers.

[3] https://www.questionpro.com/article/survey-question-answer-type.html

2.2.2.2 Data Collection

Before launching the questionnaires into public, a pilot survey was conducted amongst a small number of respondents. Since the surveying took place without an interviewer (as self-administered questionnaires), this step was crucial in determining the efficiency of the questionnaire design, wording of questions, length and other characteristics. After pilot survey respondents' feedback, the questionnaire was adjusted and sent off and delivered to the target groups.

Because the survey was conducted in Georgia, the questionnaire was translated into Georgian and Russian to engage more respondents to participate. Given the demographic particularity of Georgia, the questionnaire was distributed both as an online survey and as a printed version.

Questionnaires were filled out in several cities in Georgia in the period from March 2017 to May 2017 by people of different backgrounds. It is highly important to sample the data from all over the country, and not to concentrate just on the capital. The results are drastically different between the city and rural population, and even from city to city, they may have significant variations. Because of the difference in education, social and economic background, people living outside the capital area tend to have decidedly less experience both with technological advances in e-Commerce and IT Security, as well as more common concepts such as opening and managing an account in the bank. A number of people declined to take part in the survey with reasoning, that they do not have an account in the bank and they do not see the point of spending their time on this questionnaire. However, some of them changed their mind when the cause of the survey was explained to them. They made up 28 percent of the survey participants as respondents who do not have an account in the bank.

Out of 299 questionnaires that were handed back in, only 36 were filled out online. Online survey general statistics showed that about 180 more participants have started the survey and have never finished it, meaning that only roughly 17 percent were able to finish a 12-15 minute survey.

This fact also underlines the importance of a right approach to a Georgian customer and the need of developing individually customized message delivery method to engage the customer in the learning process. None of the online questionnaires were filled by the

people who live in cities and villages outside of Tbilisi, which is mainly explained by the limited of experience in using the computer for browsing the Internet.

2.2.2.3 Data Transformation and Processing

After the questionnaires were filled out, data from paper-based surveys had to be extracted into electronic form to be analyzed further. In this case, I entered all the data manually into an Excel spreadsheet, which was later transformed it into an SPSS file for more convenience.

SPSS software provides the possibility of coding variables by assigning numeric codes to them. This feature is very helpful, especially when working with the nominal (categorical) variables that cannot be used in the analysis in form of a string.

Assigning codes to value labels is a simple but extensive procedure for a big dataset. Labels can be defined in the Value Label window under Variable View tab.

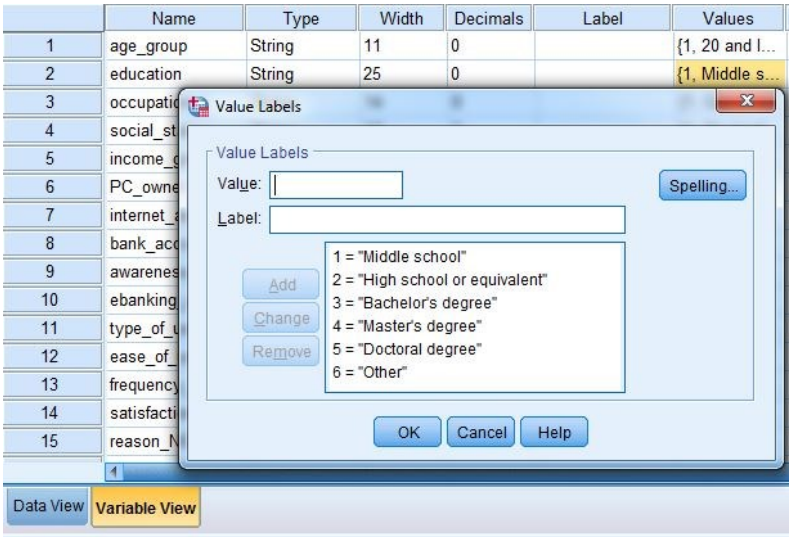
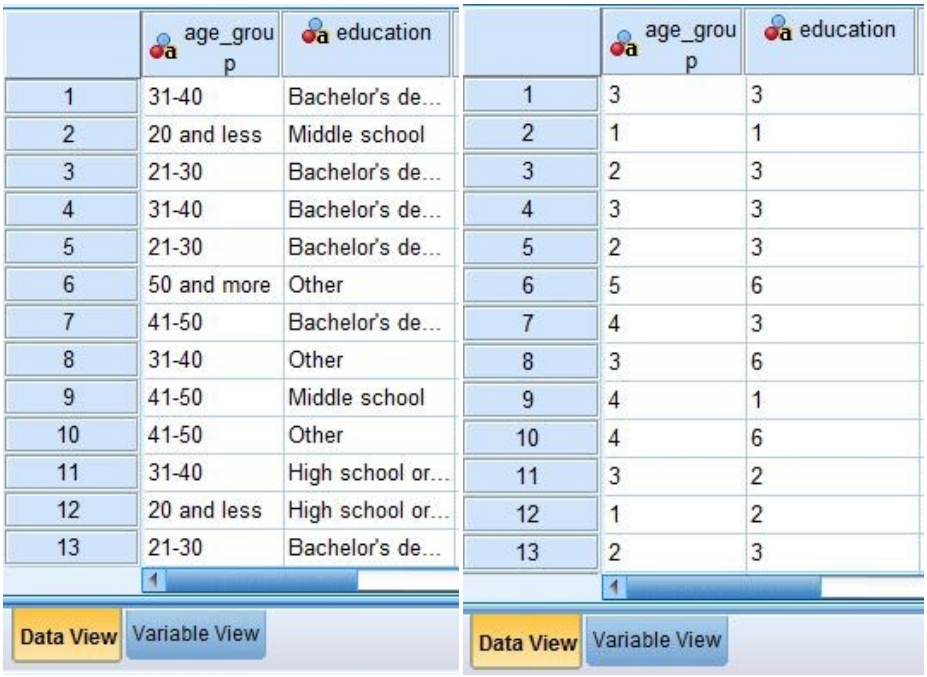


Figure 1: Coding of variables

Coded values still have value labels attached to them and dataset can be viewed both ways, as coded values or as value labels.



	age_group	education
1	31-40	Bachelor's de...
2	20 and less	Middle school
3	21-30	Bachelor's de...
4	31-40	Bachelor's de...
5	21-30	Bachelor's de...
6	50 and more	Other
7	41-50	Bachelor's de...
8	31-40	Other
9	41-50	Middle school
10	41-50	Other
11	31-40	High school or...
12	20 and less	High school or...
13	21-30	Bachelor's de...

Data View Variable View

	age_group	education
1	3	3
2	1	1
3	2	3
4	3	3
5	2	3
6	5	6
7	4	3
8	3	6
9	4	1
10	4	6
11	3	2
12	1	2
13	2	3

Data View Variable View

Figure 2: Value lables and coded variables

In case of multiple choice answers, every answer option gets a separate variable name and coded value. E.g. for question Q1 with three possible answer options separate variable (q1, q2 and q3) is created for each answer option. The values for all of these variables would be 0 and 1, for "not chosen" and "chosen" respectively. Missing variables are automatically counted as "not chosen" and are handled as such. After all, variables are named and coded they are defined as a set, i.e. grouped under one name and can be used for descriptive analysis later on as one variable with multiple answer options (Raab, 2017).

For further manipulations, the dataset is transformed again. The data that was used for descriptive statistical analysis is either disregarded or converted into easy-to-use variables. All changes to the set are conducted to simplify its use in more complicated analysis, without altering data value and meaning. The changes do not affect the outcome of the analysis. An example of this kind of transformation is converting a variable with multiple choice answers into a single option variable, without affecting its value for the set.

Let us take variable T for 'type of used e-Banking services', which has four answer options t1, t2, t3, and t4. A respondent can choose one or more of the answers which include "Electronic banking", "Mobile banking", "Phone bank" and "ATM". For the

descriptive statistics, it is interesting to know what combination of services is the customer keen to use. However, for a more in-depth look at the customer and their behavior with online services we are concentrating on the use of electronic Banking, which means that other options become abundant. In data analysis simplicity is highly valued, abundant data will overcomplicate the process and might even lead to incorrect conclusions.

For purposes of simplifying the dataset, all multiple choice variables including matrix questions and scales were converted to single answer variables, and all irrelevant data was disregarded. Transformation of is straightforward. An additional variable is created which provides a drop-down menu with coded answer options according to the previously created set. If for the question "what types of e-Banking services do you use?" a customer has chosen several answer options including "Electronic banking", the new variable gets the first priority value, or in this case "Electronic banking" automatically.

2.2.3 Evaluation of the Questionnaire Results

This chapter handles the descriptive statistical analysis of the acquired data. Descriptive analysis paints a picture about the current situation in Georgian banks, current needs of an average customer and concerns they are facing most frequently. Results will help us identify what kind of change, if any, is envisioned by the customer.

2.2.3.1 Descriptive analysis

As mentioned above, questions are divided into three sections: demographic questions, questions addressing customer experience and questions addressing customer behavior concerning the secure use of e-Banking. The first section is directed to include information from all respondents. The section about customer experience is divided to address particular groups of customers separately to collect information about both existing customers and their experience as well as potential customers. Behavioral questions are aimed strictly at bank customers who use electronic banking services.

Demographic data

A short overlook on demographic data will help us create a vision of a customer and provide information about their background. By getting to know our customer we understand the motives behind their behavior online.

Age group. The age group distribution amongst 299 respondents is fairly equal, there is no distinguished outlier in the group. This means there exists a possibility to conduct analysis for each age group separately and get demonstrative results just as with the whole dataset.

Highest completed level of education. When we take a look at the educational background of respondents we can see that people with bachelor's degree are prevailing, followed by master's degree holders and high school graduates. The option "other" refers to a technical college certificate or equivalent and is positioned second to last with roughly 7 percent followed by middle school graduates with 2 percent.

Social status. From the 299 respondents, almost 78 percent were employed, the rest is divided among unemployed participants, students, and housewives. The category "Housewife" is a Georgian peculiarity and cannot be left out in this case. Although these persons are technically unemployed, under certain circumstances, e.g. marriage, they choose the status of housewife to be assigned to them, which will spare them from qualifying as unemployed. These circumstances do not affect the financial or legal situation, it is mostly a part of personal characteristics.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Student	16	5.4	5.4	5.4
	Employed	233	77.9	77.9	83.3
	Unemployed	35	11.7	11.7	95.0
	Housewife	15	5.0	5.0	100.0
	Total	299	100.0	100.0	

Table 1: Distribution of answers based on social status

Income. Following bar graph displays the percentage distribution of income groups. The income currency is given in Georgian Lari (GEL). An exchange rate of GEL to EUR for the moment of this study was 1 to 0.35.

Due to continuous political instability and consequently the shortage of foreign investments, amongst many other problems, the Georgian government is failing to develop a stable growth model for the economy, leading to the poor quality of life and lower income in population. Subsistence minimum for July 2017 is 167.2 GEL (for single working male). "Subsistence minimum indicators are calculated based on the minimum food basket defined and established according to the decree N 111/n of 2003 May 8 of the Minister of Georgian Labour, Health and Social Affairs on 'Norms of determining the composition of minimum food basket for subsistence minimum regarding food substance and energy for physiology demand'." (CBW 2016)

It should be also noted that Georgia is on the last place among similar countries with a minimum subsistence rate. Although this indicator has increased in 2015, the living wage in the background of the impairment and inflationary pressure of GEL fails to reflect the actual picture and there is a strong need for its adjustment.

With this information on hand, it is not surprising that roughly 61 percent of respondents fall into the first group, with income that is less than 500 GEL. 23 percent of questioned persons earn more than 500 but less than 1000 GEL. Only 16 percent of respondents have what qualifies in Georgia as luxury-level salary.

According to results of cross-tabulation between age groups and income respondents in the age group from 21 to 30 have highest total income.

		income_group			
		500 and less	between 500 and 1000	1000 and more	Total
age_group	20 and less	24	0	0	24
	21-30	39	32	24	95
	31-40	65	0	0	65
	41-50	38	0	21	59
	50 and more	16	36	4	56
Total		182	68	49	299

Table 2: Cross-tabulation of age groups and income

PC owners and access to Internet. Majority of respondents answered positively to the question about owning a computer and having access to the Internet. With 91 percent of people with at least one computer and 97 percent of respondents with access to Internet, including people with access only to mobile Internet, the survey indicates the growth in number from 64.7 percent for PC owners and 70 percent for people with access to Internet over the time period from June 2016 to May 2017 (normalized numbers). These numbers include respondents who do not possess a computer but have access to mobile Internet.

Customer experience

As was already mentioned previously, the main part of the survey starts off with the filter Yes or No questions, which divide respondents into three main groups: respondents who have an account in the bank and use the electronic Banking services, respondents with account that do not use e-Banking and respondents without bank account and hence non-users.

Asking suggestive questions will help create a clear picture of customer experience with the use of electronic banking services.

How many of the respondents have an account in a bank?

Many of the following questions are dependent on the answers to this question. Later on, these dichotomous answers will be used in combination with other answers as a filter variable, to distinguish different categories of respondents. From 299 survey respondents, 72 percent (215 respondents) have an active account in the bank, the survey participants who do not have and never have had an account make up the rest 28 percent (84 respondents).

How many of the respondents use e-Banking services from their bank?

Answers to this question are also of crucial importance. It is used as main filter variable in combination with previous one and will divide the respondents into two main groups. The questions below will address either only one of the two groups, each of them separately or both combined.

181 of all respondents are e-Banking users, they make up 60.5 percent, whereas 118 of them (35.5 percent) prefer not to use online services of the bank.

How frequently do the customers use e-Banking services?

Answers to this question are filtered to address the only group of people who use e-Banking services. Most of the customers use electronic banking several times a month (36.6 percent), the other major group of users logs on several times a week (28.6 percent). Rest of the customers' answers lay under 10 percent.

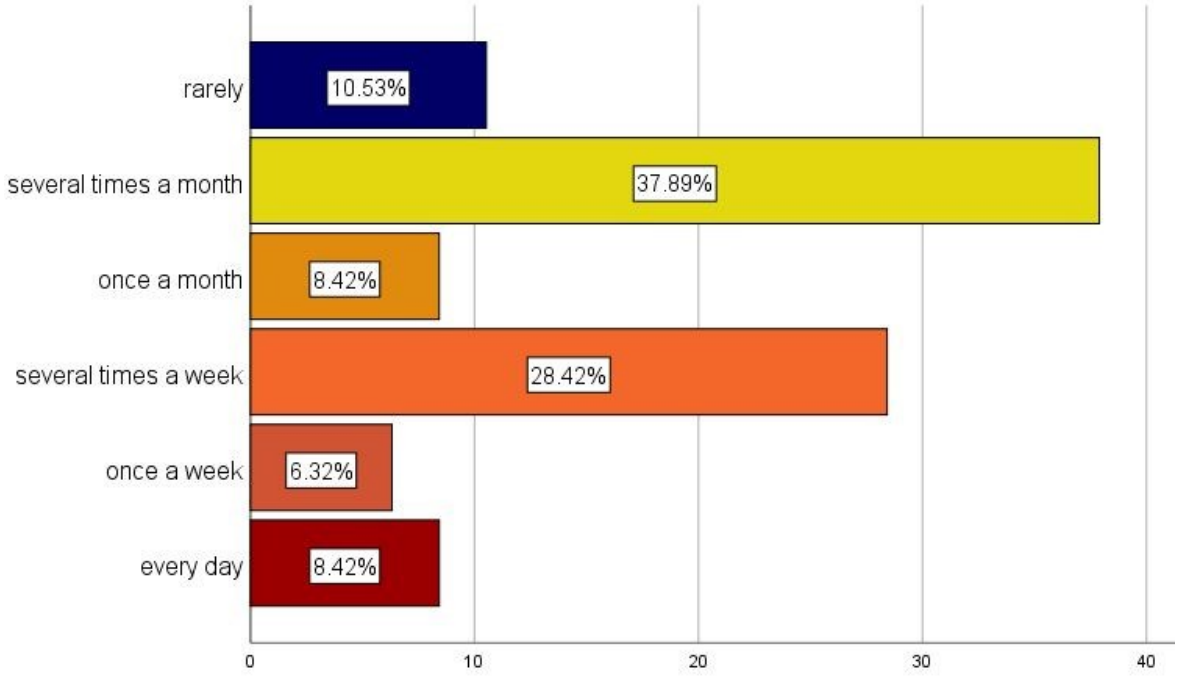


Figure 3: Frequency of eBanking use

What is the reason for not using e-Banking services by respondents with a bank account?

Cross-tabulation results show that 16 percent of people (35 of 215) with the bank account do not use e-Banking for various reasons, in descending order of relevance: "no need of electronic banking" which means they prefer traditional banking, "it seems like a botheration" and "lack of operational knowledge", followed by "possible security threats", "fear of losing money" and "hidden costs". Least concern is no access to the Internet.

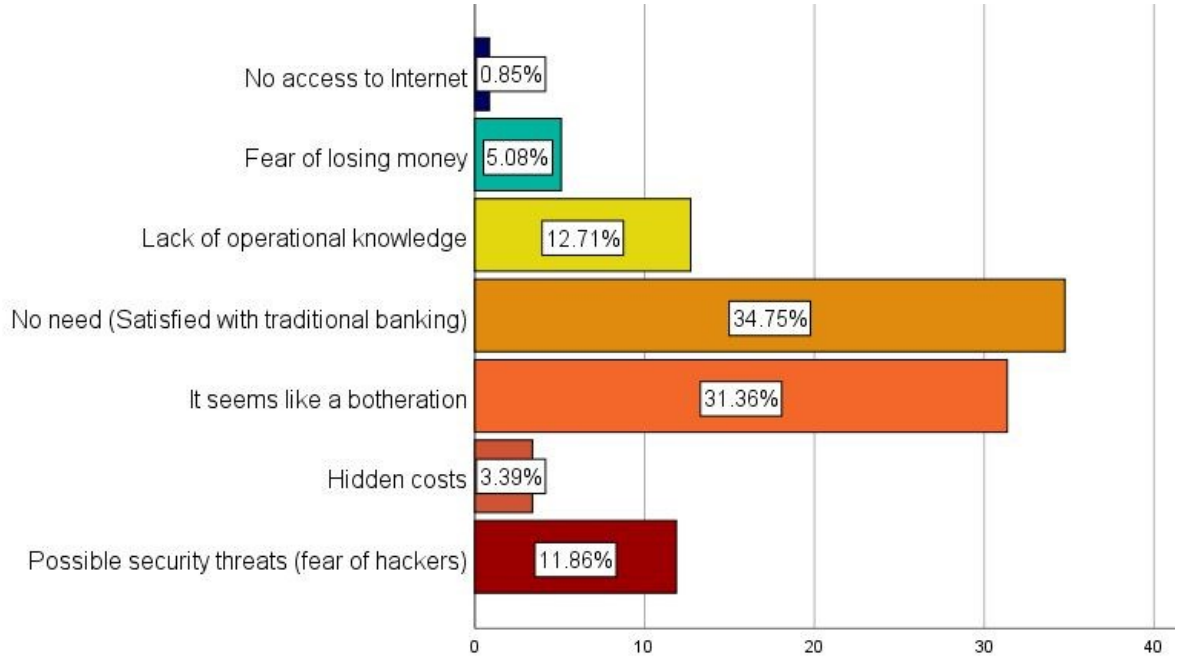


Figure 4: Reasons for not using eBanking: non-users' perspective

Just to see the difference in reasoning between two groups of respondents I filtered out respondents who do not use electronic banking and analyzed just the group of e-Banking users. The results show their presumption on why wouldn't an average customer use the e-Banking services.

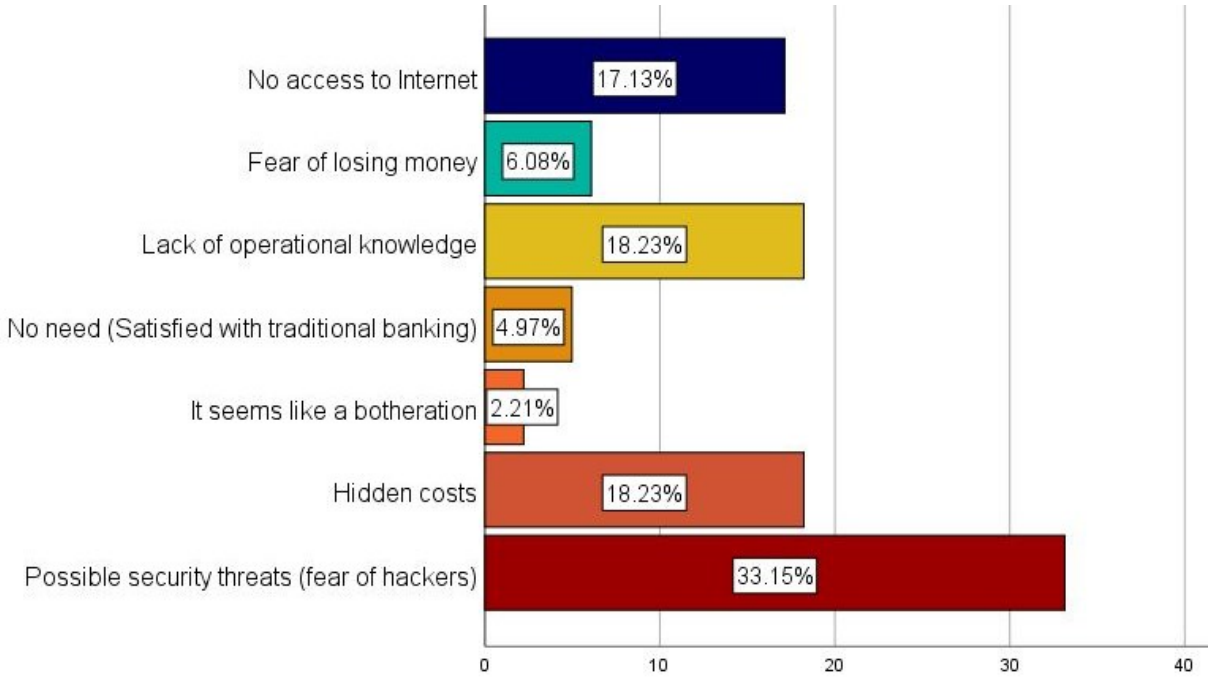


Figure 5: Perceived reasons for not using eBanking: users' perspective

From a perspective of an existing electronic banking customer, who already has some level of awareness about working mechanisms and security, potential problems seem vastly different from the non-user's perception of electronic banking and its processes. Majority of users recognize that security threats, lack of operational knowledge and hidden costs are far more serious and substantial (potential) threats.

In the first case, we have a naïve impression of people with low awareness level that is translated into fear of unknown. In the later - a more conscious and realistic outlook of a person which is somewhat aware of the potentially real problems and pitfalls.

What problems do customers encounter while using e-Banking services?

Following results are shown for the filtered group of electronic banking users, as answering this question requires experience with e-Banking use. The bar graph shows perceived concerns of e-Banking customers as opposed to previous one, which pictured their logical or theoretical speculation.

32.6 percent of customers, a significant majority, see the lack of awareness as their main concern, with security issues and lack of legal regulations following it. In this case, awareness includes operational knowledge, understanding of processes behind the transactions, information about security and safe use of the system. Security issues may arise because of low awareness, therefore it follows information shortage in second place with 24.9 percent. Lack of legal regulations is interconnected with all of the major issues and is also highly concerning to the users. False transactions that happen due to customers' fault or without their knowledge are impossible to claim not just in a technical sense, but they also have no backup by the legal regulations, banks usually refuse to refund the loss (Mannan, Van Oorschot, 2008). 4.4 percent of customers find that forgotten password might be an issue, especially when in a hurry. None of the respondents think the electronic services are time-consuming.

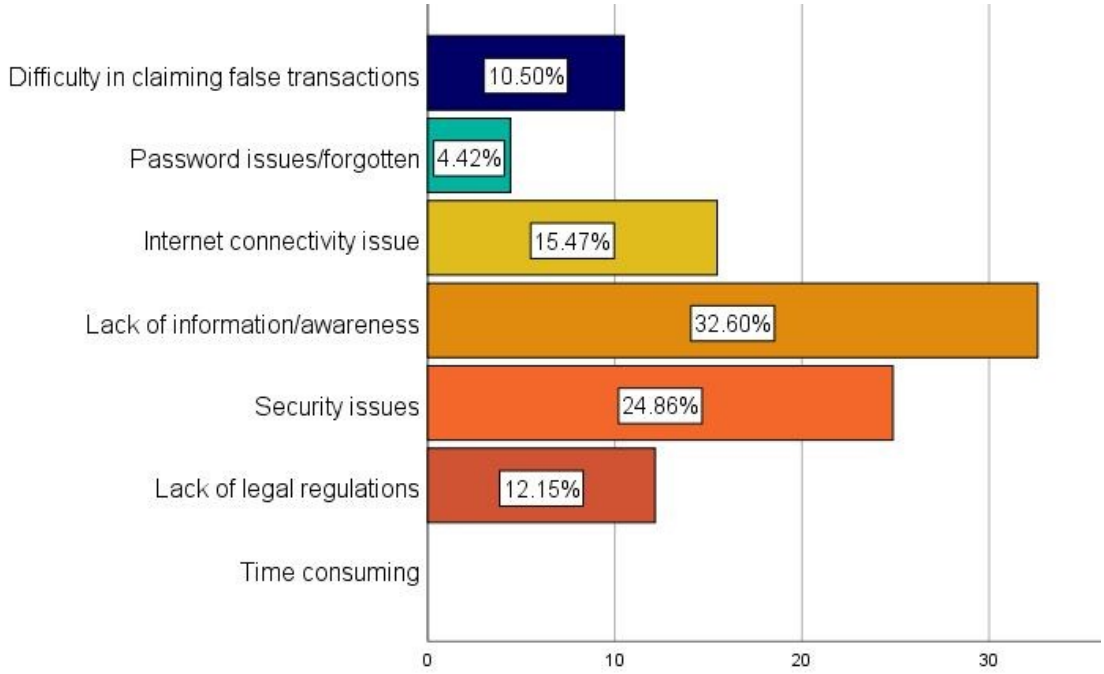


Figure 6: Perceived problems in eBanking use: users' perspective

What is the general level of satisfaction with the e-Banking use?

This question addresses the level of satisfaction with the services of electronic banking amongst users. Roughly 65 percent of them are satisfied, 17 percent even highly satisfied with the experience. 18 percent of users have neutral attitude toward their user experience, however over all it still qualifies as a positive rating, considering that two negative answers "dissatisfied" and "highly dissatisfied" were completely disregarded by all of 181 customers.

How straightforward is the use of services and what do customers see as potential pitfalls?

This question is important for various reasons. Since electronic banking is relatively new technology for a broad audience, perceived ease of use plays a crucial role for understanding customers' abilities understand the technology at hand, to learn how to operate it (Jahangir, Begum 2008). Additionally, studying customers' perceived ease of use and satisfaction level, we can conclude how well is the innovation adapting to an average customer and helps developers ensure that customers will have a positive, flexible and user-friendly banking experience (Ernovianti et.al. 2012). Positive experience and perceived ease of use (also in combination with efficiency, usefulness, and credibility) create a fundamental emphasis on customers' behavioral intentions

(Guriting, Oly Ndubisi 2006). It eliminates the fear of the unknown and boosts perceived usefulness, consequently ensuring a smooth adoption of innovative technology.

From the table 3 below it is easily deduced, that customers in their majority find the use of electronic banking services easy (62.4 percent), roughly 37 percent perceive it as normal and only four percent of all 180 e-Banking users think it is difficult. These circumstances indicate that the adoption of electronic banking in Georgia is successful and will most likely be spreading through the population in coming years.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Easy	113	62.4	62.8	62.8
	Normal	59	32.6	32.8	95.6
	Difficult	8	4.4	4.4	100.0
	Total	180	99.4	100.0	
Missing		1	.6		
Total		181	100.0		

Table 3: Ease of use: user's perspective

Interestingly, cross-tabulation results below showed that all 8 of the respondents (four percent) who find the use of e-Banking services difficult, fall under the same age group (41-50).

		ease_of_use			
		Easy	Normal	Difficult	Total
age_group	20 and less	8	0	0	8
	21-30	60	10	0	70
	31-40	12	9	0	21
	41-50	8	13	8	29
	50 and more	25	27	0	52
Total		113	59	8	180

Table 4: Cross-tabulation ease of use and age group

Are the customers provided with enough information about management of their account and IT security?

With this question, we evaluate the volume, quality, and usefulness of information that is provided to customers by the bank. It is also important to identify the information delivery methods and the efficiency of such. A priori we know that bank provides information via the bank's Website, verbal consulting at the branch and printed brochures provided to customers at the branch as well. Information content consists of general instructions on e-Banking use, security measures and tips, such as tips for creating a strong password, precautions about using mobile banking, information about phishing etc. Analysis showed, that 27 percent of respondents get their information about IT security from the bank's website, about seven percent are consulted personally by the employees at the branch and only about two percent is informed by the printed media. More than half of the respondents (roughly 65 percent) obtain their share of information from the sources outside the bank. Sources can be Internet, press, books, university, and others.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bank website	66	22.1	27.2	27.2
	Brochure	4	1.3	1.6	28.8
	Verbally at the branch	16	5.4	6.6	35.4
	Other non-bank related sources	157	52.5	64.6	100.0
	Total	243	81.3	100.0	
Missing		56	18.7		
Total		299	100.0		

Table 5: Sources of IT security information

This picture does not differ too much, when we apply the same analysis to a selected group of respondents, namely just the e-Banking users. more than 58 percent of customers choose to be informed from the outside sources, whereas 35 percent relies on the website and seven percent prefers the verbal communication. Printed media is excluded from the answers.

Is the provided information useful to customers or is it considered as just a formality coming from the Bank?

We asked the customers whose information source was bank's website, whether they were intentionally searching for the information or they happen to stumble upon it. 29 percent of customers found the information by chance. 71 percent answered that their search was purposeful. These customers were then asked how difficult the search for the information was for them. Only six percent found the desired information easily, more than half of them (51 percent) were relatively neutral to this question with the answer "normal", 43 percent admitted they had a hard time finding the information on the website.

How complete was the information on the website?

35 percent of customers was disappointed with the content of given information and found it to be too general for them. For 61 percent the information was sufficient. Four percent admitted, they did not even read it.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very general	23	34.8	34.8	34.8
	Sufficient	40	60.6	60.6	95.5
	I don't know, I did not read it	3	4.5	4.5	100.0
	Total	66	100.0	100.0	

Table 6: Completeness of information provided on the website: users' perspective

Attitude

The purpose of following questions is to get to know customers' presence on the e-Banking website and their thought process behind their actions. The previous section pointed out aspects of customer experience and was characterizing and picturing the technical side of the e-Banking system, a look through customers' eyes on how straightforward and customer-friendly the system is. In this section, customer attitude is put under examination. This analysis is conducted for a group of respondents that use e-Banking services.

Have you ever received a personal message on your e-Banking page?

For the first question, more than 80 percent of users answered positively with a yes, admitting they have received the messages. 12 percent of users admit they do not know what a private message is and seven percent deny receiving any sort of private message on their page. The latter two subgroups of users together make up 19 percent. Their answers lead to a conclusion that despite the provided instructions of use and level of knowledge the customers are claiming to have, the awareness level of these 19 percent is lower than expected based on the previous analysis. Additional questions partially explain why this is happening**.**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	145	80.1	80.6	80.6
	No	13	7.2	7.2	87.8
	I don't know what that is	22	12.2	12.2	100.0
	Total	180	99.4	100.0	
Missing		1	.6		
Total		181	100.0		

Table 7: Number of users who received a private message from the bank

How informative did you find the content of the personal message?

55 customers out of 145 (38 percent) who had received a message feel that the information in it was too general, 70 of 145 (48.2 percent) think the message was sufficiently informative and the rest 21 percent of users, including 20 out of 145 that received a message and decided not to read it, understandingly answered that they do not know.

Do you usually take provided information into consideration?

After receiving the message and reading it, slightly more than half of the users (54 percent) decide to take the information into consideration and apply that knowledge for further use of service and experience. The rest 46 percent consists of customers who usually disregard the contents of the message for various reasons and the customers who are not sure whether they take something out of the message. The distribution is 35 percent and 11 percent respectively.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	92	50.8	54.4	54.4
	No	59	32.6	34.9	89.3
	I don't know	18	9.9	10.7	100.0
	Total	169	93.4	100.0	
Missing		12	6.6		
Total		181	100.0		

Table 8: Number of users who took the received information into consideration

The above table (table 8) paints a picture about customers' attitude toward responsibility and seriousness required from them for the work with online banking. Following cross-tabulation clarifies the picture even further with numbers. 92 out of 145 people (63 percent) who received a message are taking the information into consideration. 45 out of 145 recipients (31 percent) chose to ignore the contents for various reasons, and eight customers (six percent) disregard the information most likely unwillingly due to lack of experience/awareness.

		considered			
		Yes	No	I don't know	Total
received_PM	Yes	92	45	8	145
	No	0	1	5	6
	I don't know what that is	0	13	5	18
Total		92	59	18	169

Table 9: Cross-tabulation received PM and took info into consideration

What are the reasons for not taking the provided information into consideration?

Majority of customers (40.5 percent) stated they do not have time to read the messages, 30 percent have never noticed the message function on their e-Banking personal page. 22 percent of users are convinced, they know more than the bank message can provide. Seven percent find the messages one-dimensional and are put off by the simplicity and ambiguity of information. One percent finds the messages annoying and the waste of time. None of the customers find the content of these messages too complicated to understand and employ.

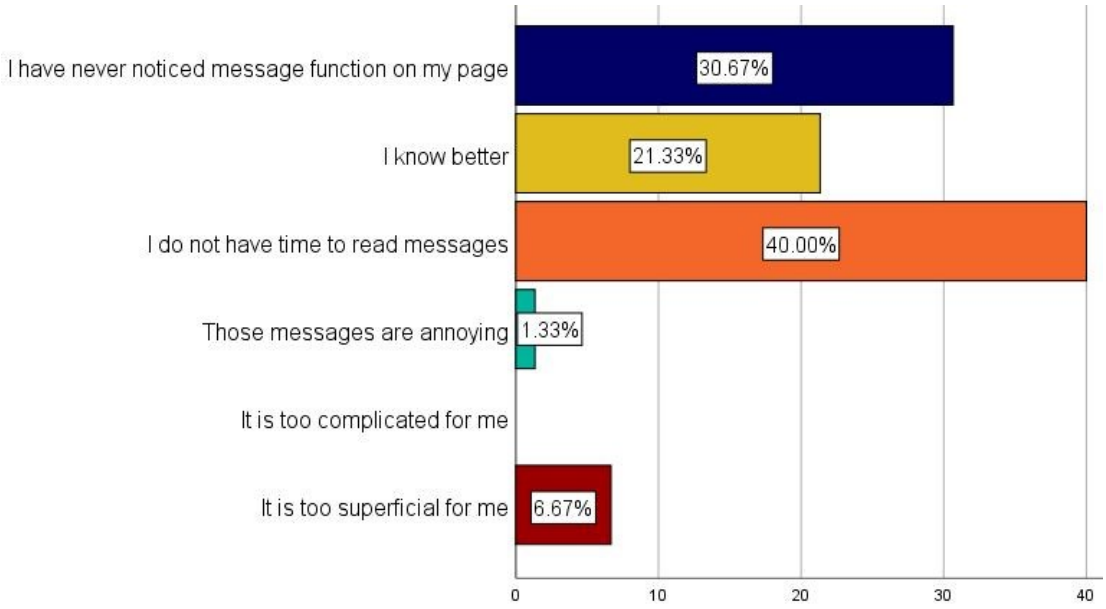


Figure 7: Reasons fot not taking the information in consideration

Do you feel you have sufficient knowledge about IT security?

When asked whether they feel they have enough knowledge about the topics of IT security, 34 percent of customers were not sure if their knowledge level is sufficient enough. 30 percent were definitely sure they have very little familiarity with IT security. A quarter of customers (25 percent) felt they are well aware of the surrounding situation, and they think they have enough knowledge and only 10 percent were convinced they have enough proficiency to stay safe while working online.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	31	10.4	10.5	10.5
	No	90	30.1	30.5	41.0
	Not sure	100	33.4	33.9	74.9
	I think I do	74	24.7	25.1	100.0
	Total	295	98.7	100.0	
Missing		4	1.3		
Total		299	100.0		

Table 10: Sufficient knowledge about IT security Table

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	31	17.1	17.3	17.3
	No	22	12.2	12.3	29.6
	Not sure	65	35.9	36.3	65.9
	I think I do	61	33.7	34.1	100.0
	Total	179	98.9	100.0	
Missing		2	1.1		
Total		181	100.0		

Table 11: Sufficient knowledge about IT security: users' perspective

Considering how difficult it appears to be to gain customers' attention even for a very short time, following questions arise:

For existing customers:

- Will the new source of information be welcome amongst the customers or not?
- Are customers willing to learn if the information source was more interactive, or adjusted to their likening and needs?
- For potential customers (currently not using e-banking services):
- Will they consider joining e-Banking provided that they will get coaching as they go?

The numbers show that roughly 79 percent of current eBanking users would welcome the changes in information delivery methods if it suits them better than the existing one. 21 percent show no interest in change and receiving information on their personal e-Banking page.

Will you consider joining e-Banking, provided you will be guided by the system step by step with useful information on operating and managing your e-Banking account, securing your transactions and using the advantages of electronic banking in general?

This question was understandingly directed towards bank customers who refuse to use eBanking services. More than half of the respondents (roughly 52 percent) gave a strong negative answer, 13 percent were not sure about joining e-Banking. About 30

percent would definitely consider joining if they are provided the information and guidance and six percent were on the verge and answered with "maybe".

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	35	29.7	29.7	29.7
	No	61	51.7	51.7	81.4
	I don't know	15	12.7	12.7	94.1
	Maybe	7	5.9	5.9	100.0
	Total	118	100.0	100.0	

Table 12: Consider joining eBanking: non-users' perspective

Behavior

This section of the questionnaire concentrates solely on customers' habits in regards to e-Banking use. The questions are aimed to address security-related actions of customers. The answers depict the general level of security awareness of each customer. However, it is not possible to fully rely on a questionnaire in order to determine customers' level of awareness. It cannot be guaranteed, that the answers are 100 percent accurate (Kruger, Kearney 2006) and involve a reasonable amount of speculations based on the known background of the customer. The number of questions in a survey is limited and cannot capture all the details, furthermore, there is always a risk of misinterpreting the data and coming to an incorrect conclusion.

Evaluation of survey results provides a stepping stone towards the creation of a prototype tool for raising customer awareness, which will analyze actual behavioral data collected by the CRM system and rely on behavioral patterns to distinguish different groups of customers based on their knowledge level. Questionnaire results provide us with preliminary analysis and indicate the important points of interest that would be addressed in more detail in the future work.

How do you usually end your work with online banking system?

61 percent of e-Banking users end their session with the logout button, 29 percent simply close the browser tab without logging out. Almost six percent leave the e-Banking page open until the system logs them out automatically and three percent of respondents close the browser itself. Two percent gave a vague answer to this question.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	logout	111	61.3	61.3	61.3
	close the tab	52	28.7	28.7	90.1
	leave it open	10	5.5	5.5	95.6
	close the browser	5	2.8	2.8	98.3
	I don't know	3	1.7	1.7	100.0
	Total	181	100.0	100.0	

Table 13: Sign off method: users' perspective

How often do you change the password for your e-Banking account?

An overwhelming 65 percent of customers answered, that they only change the password if the system demands this action, time periods for password change request can differ from bank to bank. In several major Georgian banks password, expiration periods vary from 6 months to two years.

16 percent of electronic banking users change their password once a year, another 12 percent prefer to change it twice a year, every six months. People who change their password every other month make up just six percent of e-Banking users and only two percent prefer to ensure their security by changing their password every 30 days.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	every 30 days	4	2.2	2.2	2.2
	every other month	10	5.5	5.5	7.7
	every 6 months	22	12.2	12.2	19.9
	once a year	28	15.5	15.5	35.4
	whenever system demands	117	64.6	64.6	100.0
	Total	181	100.0	100.0	

Table 14: Frequency of password change: users' perspective

Do you or have you ever disclosed your username and password to your friends or family?

91 percent of all users never share their username and password, whereas the rest (nine percent) do not neglect this security aspect.

Where do you normally use the electronic banking services?

69 percent of e-Banking customers work with electronic banking exclusively from home (personal computer and home secured home network). 23 percent use the services at home and occasionally at work. Almost 8 percent are not limiting their work just by using the secured network, they admit that they use e-Banking anywhere, including public places with open/public Wi-Fi.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	only at home	125	69.1	69.1	69.1
	home and workplace	42	23.2	23.2	92.3
	anywhere, including public places	14	7.7	7.7	100.0
	Total	181	100.0	100.0	

Table 15: Use of unprotected network for work: users' perspective

How often do you clean your browser cache and cookies?

An Internet browser stores a lot of information about its users online activity, including cache, cookies, browsing history, passwords, credentials and other sensitive data from the filled out online forms and more.

Cache and browser history disclose the sites which were visited by users. Cookies pose the risk of revealing the sessions that weren't ended with a log out. Session ID (SID) may store information either locally on the disc or server-side and even in case when user renders the SID itself as invalid by logging out from the website (providing the log out process is correctly implemented by developers), the risk of potential disclosure of leftover sensitive data is still very high[4]. Most of the customers seem to be aware of concepts of cache and cookies, in fact, only 20 percent of them have stated, that they know nothing about the cache. 33 percent of users clean cache every now and then, 27 percent claim they never delete cache and cookies. 17 percent clear browser data every day, assumedly by setting the browser to clear cache after closing. And three percent delete cache immediately after they have done working with e-Banking.

2.3 Summary

The main purpose of this study was to set the base for future work by taking a closer look at an average customer of a Georgian bank in order to get to know their behavior and attitude towards e-Banking use and existing or perceived issues. Without knowing the target audience any further implementation would have been ineffective and vain.

As a starting point, we set an assumption that the overall IT security awareness level amongst the customers was low. The scope of the survey was to check whether this hypothesis was accurate, by investigating the possible reasons for low awareness level amongst existing and potential users of electronic banking.

The study found that our target audience consists predominantly of employed, lower-income customers with a higher education degree, living in urban areas.

A number of people refused to take part in the survey with the reason that they do not have an account in the bank and filling out the questionnaire would be difficult due to

[4] http://resources.infosecinstitute.com/session-hijacking-cheat-sheet/#gref

lack of general terminology or knowledge. When explained the purpose of the survey and offer to assist with filling out several people decided to participate. It is noteworthy that these people were participants from rural areas only. Lack of operational knowledge and bank account itself is explained by financial instability (no steady income) and low level of awareness about managing account and finances; in other words no need and no interest.

When examining the potential issues or threats that customer might encounter when working online, the survey showed that there were two perspectives towards them. Customers who do not use electronic banking services justify their choice by claiming that they see no need in e-Banking, that it would be a botheration for them and that they lack the operational knowledge to manage their account online. We can only speculate that these customers do not have the general knowledge about e-Banking itself and IT security, as we know how useful electronic banking can be and that the risks of using e-Banking can be connected with the loss of money due to online theft, fraud, hacking and similar security threats.

To prove this hypothesis we can take a look at same question answered by e-Banking users. Users' comprehension of possible problems and risks included possible security threat, lack of operational knowledge and fear of losing money. The difference in awareness levels is evident.

Addressing customers' attitude towards existing information about IT security and methods of its delivery to customers showed that majority of participants prefer to seek for this information in sources other than provided by the bank, the reasoning being various for groups of customers from difficulty of finding information on bank website to its insufficiency and lack of informativeness.

The general attitude of customers towards message delivery was neutral; however, a significant number of users tend to ignore provided safety tips and security information, which can indicate to the lack of responsibility or lack of knowledge. In latter case, we end up with a closed circle, which can only be broken by a substantial change in message delivery method and consequently change in customer's understanding and attitude.

This finding suggests designing a method that will be interesting and engaging without creating the feeling that the information it is being forced to the customer; with regards to some customers that might actually be the case.

Initial limitation of this study was that it depended highly on speculations about customer background and its influence on customers' attitude and behavior. Nevertheless, the resulted customer profile is painted from the actual data and its accurate interpretation.

Chapter 3 | Literature Review

This chapter introduces the theoretical basis for the design and creation of Security Awareness tool. It determines the methods of approach to the adult learners in a way that will be effective for raising their awareness about Information Security. Besides the technical background for a successful implementation of the tool into a working CRM system, the chapter also discusses the psychological and andragogical aspects of creating an compelling program.

3.1 Information Security Awareness

The need for a high level of IT security awareness emerged at the very beginning of the bloom and globalization of information technology. Wilson et al. underlined the importance of making employees aware of their responsibilities and role in the security of an organization. The aim of information security awareness programs is to make positive changes towards a more secure behavior and working habits among employees and customers. Security awareness program should deliver information about general security topics, security issues, updates and current security trends to the users.

NIST standard defines security awareness in the following way:

"Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is a recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques." (NIST 800-16, p. 15)

In other words, an organization must make sure to deliver an understanding of IT security and their responsibility in it to their employees and customers. While Wilson et al. define information awareness as not a training, this thesis does use the term training in regard to a customer's security awareness education. According to Schlienger and Teufel (2003) "schooling is one of the core elements to create security awareness."

Shaw et al. in their paper underline the need for creating an e-learning based security awareness program to attract the interest of the users to the subject. They examine the impact of the richness of the media carrying the information to the users on the acceptance level from a user's side, the richest media being face-to-face meeting followed hypermedia, multimedia, and hypertext. (Shaw et al. 2009, p. 94)

Considering that the awareness program proposed in this thesis is aimed at electronic banking users, the choice of message delivery media is limited. Understandably, face-to-face meetings are completely excluded from the list; the shortcomings for this type of education include many points, from definite lack of resources to train large numbers of customers and employees to a nearly impossible task of covering all of the existing customers who might be geographically and timely unavailable.

Hypermedia and other similar mediums cannot be used in combination with an electronic banking. The intention of a security awareness program proposed in this work is to provide information to customers without taking too much of their time and without requiring any effort from them. Education of working adults is proved to be more effective if the learners receive the provided information along with their everyday and routine tasks, without any unnecessary disruptions.

3.1.1 The Human Factor

"Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naïveté, or ignorance come into play." (Mitnik, Simon 2003, p. 12)

No matter how elaborate the organizations' security measures become, maintaining an organizations security environment solely by protecting their networks and implementing advanced technologies is useless against modern attackers. In the current age of information technology, an attacker is not required to be proficient in programming or even being a technophile. A Former hacker, Kevin Mitnik, describes in his book how a completely unrelated person managed to obtain a highly sensitive financial information from a bank just by calling the 800 number - a customer service hotline.

Users are the most important group of people who are responsible for the vulnerability and high risk of a security incident caused by neglecting the security policies and guidelines. By the term 'users' we identify actors who have a relationship with an organization at least in some form; these could be bank employees, external contractors, customers, researchers etc.

According to the NIST 800-50 standard, a security training awareness program is divided into three main parts: education, training, and awareness. Education gives a user the knowledge as to why is information security important to them and their business. Training provides them with practical knowledge and behavior practices to be and stay secure. Awareness indicates if the user has really learned a lesson, keeps the acquired knowledge in mind and uses it in everyday situations.

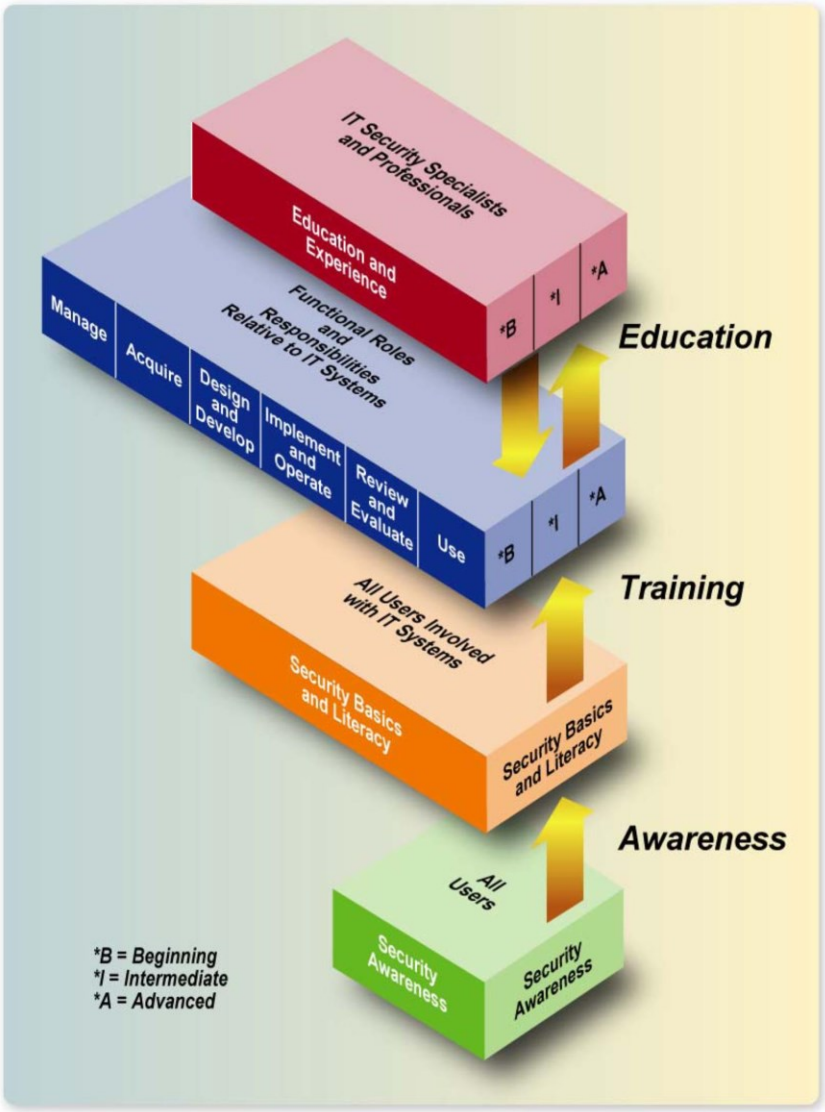


Figure 8: The IT Security Learning Continuum [Source: NIST Special Publication (p. 19)]

Figure 8 shows the requirements of an IT security education for each actor on a corporate hierarchy. Security awareness is a basic level of security knowledge that is expected from all users, especially bank customers.

Based on the research and examples provided by authors, we identify the increasing need for creating an effective Information Security Awareness Program that will cover the education of the bank customers, which is by this time virtually non-existent.

3.1.2 A Need for an Effective Security Awareness Program

A further issue is the correct and thoughtful design of the training process. The safety instructions, that are usually provided to e-banking users in form of a text file, are not able to cover all the possible scenarios and tasks that can occur during e-Banking usage. Instructions are static and can be useless when users face the novel tasks that are not covered by the document. It is difficult for system designers to predict every possible issue scenario, because it depends too much on individual user behavior and interaction that is happening outside of the e-banking system, namely on user's computer. Hertzum et al. describe one of the limitations of this kind of instructions in following. "Users may have different browsers, different versions of the same browser, or their browsers may be set up differently. This defeats thorough instruction because neither the sequence of steps a user will go through nor their exact contents are known to the eBanking system. Relying on instruction in such a situation involves a risk of confusing and frustrating users due to mismatches between the instructions and the actual system behaviour." (Hertzum et al. 2004, p. 61)

3.2 CRM Approaches for Raising Customer Awareness

This subchapter provides a brief introduction to CRM systems as well as the channels used by the system to establish a successful human-computer communication. Additionally, the chapter discusses briefly the eLearning and adult learning philosophies, which will be used as a base knowledge for designing the model.

3.2.1 CRM system - an overview

A CRM system provides a link between front and back office with the customer information sources (e.g e-mail, call centers, mail), feeding organizations functional processes with the resources gained from customer interaction. It can also be defined as a technology for tracking and analyzing customer behavior, not just from a sales point of view, but operational behavior as well. Based on identified behavioral patterns the application provides a better understanding of customer and allows improved communication with individual customer types (Chen, Popovich 2003). It provides an organization with the knowledge about their markets and customers. CRM is a "[...] sophisticated application that mines customer data that has been pulled from all customer touch points, creating a single and comprehensive view of a customer while uncovering profiles of key customers and predicting their purchasing patterns" (Chen, Popovich 2003).

Many organizations including financial organizations like banks are implementing the Customer Relationship Management (CRM) software for their everyday and long-term activities. However, even today, after years since CRM was first introduced to the market, the capability of this software is not used to their fullest extent (Peppard 2000, p. 312). CRM systems have been in use for a while now, and many organizations learned to make a profit by utilizing the system's marketing capabilities, e.g. customer retention, calculating customer lifetime value, tailored transactions. The system entails development of the offers and it can also help make a decision about the information to be provided: what level of information goes to which customer. (Rygielski et. al, 2002)

A CRM system is based on repositories of consistent and reliable customer data (Meltzer) without which it would not be half as useful as the information management tool. "In the traditional process, the marketing goal is to reach more customers and expand the customer base." (Rygielski et. al, 2002) The software is capable of collecting and storing various types of customer data, from their recent activities to the transaction analysis results and predictions of their next purchase. These repositories can potentially become a source of a great many achievements, not just in marketing, but in cyber security as well.

3.2.2 Importance of Security Awareness

As it was already mentioned in previous chapters, easier access and expanding nature of technological advances changed the customer profile, making the behavior of an end user less predictable than before. "This increasing sophistication of the user combined with the need to grant them access to the information that they require means that it is no longer possible to maintain effective information security with physical [controls]" (Thomson, Solms 1998). Today's customers expect and demand more from the organizations they are dealing with and organizations put more effort in strengthening the relationship with their customers. This relationship is majorly based on B2C communication.

Information security awareness amongst employees and customers is a preventive measure against security breaches and other incidents (COBIT 2007). Mitnik and Simon, Abraham et al. and many others explored the most sources of popular security issues in organizations and concluded that most common cause for a security breach is due to social engineering attacks. Social engineering attack is directly connected with the level of awareness and experience of both an employee and a customer. A user is the weakest link in an organization's security chain and if this issue is not addressed, all advances in IT security technology and software and general preventive measures will be useless.

3.2.3 CRM Communication Channels

Currently, CRM systems are offering a variety of communication channels to choose from. A bank can contact their client via postal services, e-mail, phone calls, Fax, Short Message Service (SMS), Multimedia Message Service (MMS), chat, blogs, Social Network, video conference (VC). Depending on the nature of the information to be communicated and the different factors such as communication policy, budget factors, the demographic coverage of targeted audience etc., the organization choose an appropriate method for message delivery.

While these communication channels are a part of CRM system, they are not fully connected with the other CRM features. Without the interconnection of all CRM

features customer communication must be conducted by the bank employees manually. At this stage of CRM development, the systems are not designed to support direct communication and interaction methods with the customers. A growing demand for meeting a customer's individual needs creates a necessity for automation of customer interaction channels. This provides a much-needed flexibility in time and communication methods; on one hand - appealing to busy customers, and on the other - automation of customer interactions eases up the operational load. The automation, clearly, is meant for the communications that do not require personal and immediate assistance. For the features like raising customer awareness level about IT security, the integration of CRM system with communication channels and processes provides a great value. "[...] improving customer interaction can be rapidly tested and operationally deployed, without the risk of disruption to existing systems" (Marlon Bowser).

The measures for raising customers' awareness level about IT security, which are currently used in banks, include guidelines, policies, written and verbal recommendations (Kruger, Kearney 2006, p. 290). In the extremely rare cases, a bank offers an occasionally paid seminars about IT security, however, due to the financial situation of an average Georgian bank customer these seminars are rarely visited, and therefore even rarely offered.

CRM system can potentially provide a great platform for one-to-one communication with the customer (Chen, Popovich 2003). Apart from improving organization's sales CRM applications can allow direct feedback to customers through the system itself, avoiding the routinely ignored call centers and e-mails.

For example, after CRM's analytical data mart collects and analyses customers' behavior and actions with respect of security on the eBanking site, the information is stored again in the "back room" of the CRM system; the proposed application (integrated CRM features and communication channels) can use this information to sent the tailored messages and alerts to the customer, thus informing them about correct and secure behavior or provide security tips and guidelines to protect themselves from cyber criminals. Customers can have a choice how to receive these messages, be it via e-mail, text or intrasystem message.

Adding this feature to the CRM system will leave customers satisfied that they get the individual approach from a bank; it will benefit the bank by easing up the operational load that is currently carried out mostly manually; and most importantly integrating analyzed CRM data with the outbound customer communications will strengthen the security by raising awareness of each customer.

3.3 Approaches for Identifying Customer Demand

Identifying a customers' need and expectation is the main stepping stone for designing an appropriate education system for raising their awareness about the needed topic. For purposes of studying our customers, in addition to the empirical study, conducted earlier, we have to take a glance at the field of psychology and sociology. Understanding a customer has become a whole new chapter of marketing and its importance is growing every year. In this chapter, we discuss the influences on customer behavior and their expectations with regards to eBanking. Additionally, we will discuss the attitude and behavior changing methods, which will help us in achieving our main goal. Finally, based on these methods we will propose the functional and effective message delivery techniques, which should raise customer awareness level and transform their knowledge into positive habits.

3.3.1 Customers' Demand

The key to understanding a customer's demands and expectations lays in understanding analyzing their attitude and behavior. For the purposes of the clarity of the picture, we divided the bank customers into two groups: bank customers who use eBanking services and customers associated with the bank but who do not use online services. We will discuss them separately, since they have distinctive perspectives, hence different expectations and needs. "To be able to define the right cultural measures, you must know the people you want to influence" (Schlienger, Teufel 2003).

The study conducted for this thesis showed that from 299 respondents who agreed to participate in the survey, 118 (35.5 percent) are not using eBanking services.

Considering the fact, that electronic banking has been around in Georgia for several years now, this number is significantly high. The factors affecting customers' decision not to use electronic banking also have been studied and analyzed.

Based on the information learned from the empirical study, banks fail to deliver the information to their own customers about usefulness and benefits that the eBanking can provide to their everyday and routine bank activities. Hence, the majority of customers who do not use eBanking services explain it by their lack of need for online services and a potential botheration these services might cause. Another 12 percent of the non-users are concerned with the security issues and about the same percentage admits that they do not have enough operational knowledge, hence fear to start using the service. Overall, the study identified the lack of information about services, operational use and security measures as the main concerns for the users. It is also worth mentioning again, that more than 200 people refused to participate in the study due to lack of any information about their bank and online services.

According to a number of similar studies conducted worldwide based on Technology Acceptance Model (TAM), Technology Readiness Index (TRI) and various surveys, Georgia is not an exception in slow adoption rates of internet banking. Majority of the customers not willing to use self-service or electronic banking had similar perceptions on the risks associated with the Internet and conducting work online. Top six reasons for not using eBanking according to Gerrard et al. (2006) were following: no perceived need, lack of knowledge about the service, inertia, inaccessibility, lacking human touch and pricing issues.

Respondents often indicated their lack of need in using of internet banking. They insisted, that they were satisfied with traditional services in a financial center or a bank branch. Besides, these customers stated that they did not see any use or benefit in changing their source of banking services and there were also the ones, who falsely assumed, that if they would switch to electronic banking, it would eliminate the traditional methods which would limit the range of financial services and create some new operational issues.

Customers concerned with lack of knowledge about the service stated their unawareness about the functionality of the online services, the requirements for joining

online banking and even fear of new technology and insufficient IT skills for operating the new and mysterious Internet banking services.

As a third reason for not using eBanking was stated customers' inertia for doing research about pros and cons of this technology and about basic operational procedures required for managing the online account. In other words, online banking seemed like a botheration to them.

Inaccessibility, or inability to connect to the internet and online banking services was the fifth factor. Reasons for inaccessibility also varied from respondents who did not own a PC or had an old one that did not support the modern broadband technologies to ones who had no or slow internet connection.

Understandably, lacking human touch was a big concert to customers with lack of experience in Internet technologies. (Gerrard et al. 2006)

Additionally, a great concern both for eBanking users as well as for non-users seem to be the security risks such as hacking, identity theft, losing money due to false transactions and others.

Many other studies and literature support this list of factors affecting the adoption of internet banking. With some insignificant differences, this list stays the same for many different countries worldwide. Studies, however, differentiate the non-users who were likely to join eBanking after some time or under specific circumstances and bank customers who are persuaded not to use eBanking at all.

According to Gerrard et al. (2006), customers whose characteristics included lower levels of education were less likely to become internet banking consumers, as well as customers who had never had any interaction with electronic commerce, meaning customers who have never conducted any payment online.

All these factors can be summarized in one single aspect, namely, lack of awareness. "One of the most important things to do is to respond to the anxieties people feel about the risks associated with internet banking. Security is seen here to be of concern to almost all, in terms of unauthorized use and abuse of accounts, and keeping customers' personal details private " (Gerrard et al. 2006). Informing consumers about benefits of eBanking, about security measures, basic operational requirements and practices would

eliminate most of these reasons and not only attract more customers to the banking self-service, it would also make them more aware and concerned with their own security, benefiting therefore towards the overall security of the bank as well. Raising customer awareness by providing them with updated information about secure use of the banking services and secure behavior in Internet in general would provide consumers with new skills for their everyday use of technology and "[u]ser skill level could be a micro driver for the banks to devise their technological strategies" (Syed Shan e Raza 2011).

Based on Syed Shan e Raza (2011) it is important to address every customer according to their skill or knowledge level. Advanced users should get the information that is more up to their level, whereas less skilled customers will be getting more basic information, thus forming their online behavior and awareness of security from the very core.

Heikki Karjaluoto et al. (2002) suggests the banks conduct their own research and offer training courses explaining computer, Internet and electronic payment systems to willing and interested customers. However, given the facts that organizing this kind of training will cost both banks and customers time and money, they are less likely to be popular. Additionally, there are many other factors affecting customer attraction to eBanking and their attitude towards security. Demographic factors play a significant role in customer behavior and their level of awareness.

Nasri (2011) suggests that such demographic characteristics as customers' occupation and instruction have a significant impact on their willingness to use internet banking. From the empirical study, we also deducted that education, occupation, age and social status pointed out customer's openness toward receiving new information.

3.3.1.1 Psychological Demand

Continuing the topic of the influence of demographic characteristic on a customer's attitude and behavior, the underlined importance of social approval must be mentioned as well. Social approval or disapproval originates in the immediate surroundings or social class of a person (Cohen,1964, pp.39-41). Depending on the customer's personality traits they might be highly or moderately susceptible to the group influence.

A number of experiments proved, that there are no outliers who are capable to completely ignore the general opinion of their social group and persist on their own perception of the subject matter.

Group influence might play a big motivational role if incorporated in the design of educational program correctly. For example, if a customer achieves the highest level of awareness within the set margins, they might eventually become a member of 'expert group' and be awarded of a certain status under the condition that they maintain the high level of awareness for a certain amount of time. Experiments showed, that "persons who are most strongly motivated to retain their membership in a group and therefore depend most upon approval from the group are less likely to accept communications which advocate positions counter to the norms and values of the group" (Cohen, 1964, pp.40-41). That means that the membership of a certain group will motivate a customer to keep up the achieved level of awareness and even give them a stimulus to go further.

On a lower scale, the same effect might be achieved by introducing a reward system. If the educational program is designed to have a game-like learning style, without getting too immature, it must include a reward system for certain achievements. It is important to maintain the balance between a childish game, which will throw off the majority of our target audience, and a rigid and monotonous communication in form of the appearing messages on the screen. The reward system is discussed in more detail in the next chapter.

3.3.2 Delivering the Message to the Customers

This chapter discusses the four approaches to customers' education about IT security. The first section is dedicated to the effects of social psychology on customers' attitude change; second part examines educational methodologies and best practices to create a learning program for working adults.

The approach to raising users security awareness must be adapted in a way that engages users to participate without becoming annoying or overwhelming. For increased productiveness of an educational program, it is necessary to address the field of

psychology both to understand the user as well as to 'manipulate' them towards needed direction and behavior. Since we are concentrating on customers' attitude and are interested in applying positive changes to their behavior, for the theoretical part we need to take a closer look at a specific section of psychology - social psychology. Additionally, if we consider that as a bank is trying to "sell" awareness and secure behavior to their eBanking users, we must take a look at the techniques of internal marketing.

How these methods are translated into an actual functioning program will be discussed in chapter 4 more technically.

Providing information to customers is not limited by the technical side of message delivery process, it also includes the carefully thought through methods of delivery which will appeal to customers and engage them and motivate them to read and pay attention to the information without simply dismissing it as an annoying pop-up. "Regardless of delivery media, all learning requires engagement" (Clark, Mayer 2011). Clark and Mayer make the distinction between customers behavioral and psychological engagement. Behavioral engagement or customers attitude towards learning new material is visible by the actions which they are taking during the process of learning. This includes the type of responses the customers give to certain questions and how they behave in a technical sense, what they are clicking and whether or not they are dismissing the information window without even engaging in the process. The objective of the learning program, proposed in this thesis, is to utilize psychological principles to make the educational platform more effective (Thomson, Solms 1998).

Psychological engagement is defined by the authors (Clark and Mayer) as a cognitive process behind the customers' actions and their ability to process the new information into acquired knowledge or skill.

In their book "Attitude change and social influence" Cohen (1964) explains the techniques of attitude change towards willingness to engage in the learning process. He goes even further with attitude change on a behavioral level, which leads to the adoption of newly acquired information into the conscious and unconscious habits. Considering today's global technological development and increasing number of services that are updated to online services, it is crucial to have sufficient level of

awareness about online security, and even more important - to have that knowledge at the everyday subconscious behavioral (habit) level.

This chapter explores all possible backgrounds for influencing customer engagement level into learning procedures; additionally, it examines the suggestions for a correct approach to teaching working adults for increased the effectiveness of learning program.

3.3.2.1 Attitude and Behavior Change

Social psychology explains the factors that lead a person to behave in a certain way in the specific circumstances or around specific people. It is 'the scientific field that seeks to understand the nature and causes of individual behavior in social situations', as defined by Baron and Byrne (1982). Combining psychology and sociology this scientific study explores the relationship between a person's beliefs, feelings, thoughts and their surroundings, the influences of such psychological factors on our attitude and interaction with people surrounding us.

Forms of social influence

Cohen (1964) identifies several major influence factors which should be taken into consideration when working with a customer.

The credibility of the communicator, or in our case information source, and how a customer perceives them is of a great significance for establishing a connection with a customer. It is as important as the content of delivered information, in some cases even greater. When the information comes from highly dependable and trustworthy sources it creates two initial effects: the information effect and the source effect. In this case recipient of this information, or a customer, tends to agree to the provided information and their desire to argue approaches minimums. And on the contrary, information that has a less credible source will be most likely disregarded and argued, even if the content itself is highly interesting and topical. However, this last case has its own unexpected effect. If the recognition of the less credible source is gone and what's left is just the substance, a customer will regard the information objectively based purely on the content and their general attitude (Cohen, 1964:pp31-34). Consequently, the

importance of highly credible sources tends to lose their value, since it's just an initial component that might be forgotten. The actual information provided to customers must be compelling and highly accurate, interesting and informative since with time it will be the only aspect that matters.

In our case this factor plays in our favor, considering that our source of information for the customers will be the bank they trust, meaning highly credible source. This will guarantee the high level of acceptance, which is important considering the limitation on volumes of provided information. Most importantly, according to Cohen (1964), highly credible sources can even allow high discrepancy of content from customer's own opinion.

Next factor affecting customers attitude and behavior is approval or disapproval. The experiments of Hovland, Janis, and Keley (1953) proved the high importance for a customer to be approved socially. Approval can come from peers, social group or the communicator. In later years number of experiments conducted by Hildum and Brown (1956), Singer (1961) and others, supported the hypothesis that approval and disapproval can induce attitude change. Simple response such as "good" or "right" from the communicator can change customer's attitude towards more "democratic", whereas no response would equal a verbal "mhm" and would not affect the customer in a positive way.

Alongside with approval a reward system, proposed initially by Kelman (1953) as an experiment takes an influential position on customers' attitude. Reward system is based heavily on dissonance theory. Cohen (1964) underlines the importance of creating a greater dissonance in the customer's mind to effectively change their behavior. "Dissonance refers to inconsistencies between a person's beliefs or attitudes and the actual behavior being exhibited. This dissonance causes tension and in order to reduce this tension either a change of behavior or a change of attitude has to take place" (Thomson, Solms 1998). Achieving a great dissonance is possible only in the case where a customer cannot justify the objectionable behavior by a significant incentive. Meaning that an expectation of great a reward must not be the reason for the behavior change, otherwise, this change will not last long after all motivations are gone (Cohen, 1964) (Thomson, Solms 1998). This hypothesis was also proven by several experiments on effects of justification. The less reason a person gets to do something,

the higher chances for an attitude change. The reason, in this case, refers to a reward of some monetary value.

The dissonance theory also explains the paradoxical fact, that a person is more likely to change their attitude towards a subject matter if the inducing agent is disliked and unpleasant for them. Whereas if an attractive and pleasant person is persuading us to change our opinion, the dissonance that is created by such a person's request is very low. Therefore, according to nature of dissonance theory, the impact of the request will less likely change out attitude. This circumstance can justify the design of message, that will be straight and on point, even if it is considered as botheration. According to the theory above, a customer will more likely to comprehend the content of the message if its appearance will seem vexing. This fact doesn't imply that the tool must be designed to annoy customers. Any unwanted message will be perceived as a waste of time and annoyance by a customer, but the actual science behind the message delivery will justifiably turn it around and give positive results.

All of the influence forms discussed above will lead to discrepant behavior, but not necessarily toward an attitude change. Cohen (1964) suggests the minimum needed coercion for an attitude change, relying on the experiments conducted by him and his colleagues. Experiments showed, that "the less the coercion, beyond the minimum necessary to obtain compliance, the greater the dissonance and the greater the consequent attitude change" (Cohen, 1964). Additionally, the satisfaction with the accomplished task increases as the magnitude of coercion decreased.

Methods for the attitude change

Researches show, that there are many methods that can affect changes in person's attitude change. Thomson and Solms (1998) sum up these in three main methods:

- directly changing a person's behavior;
- using a change in behavior to influence a person's attitude;
- changing attitude trough persuasion.

Direct change in a person's behavior includes methods that ignore initial attitude or knowledge of a person on the subject matter. Regardless of their attitude, customer's behavior can be changed by means of, for one, instrumental learning. Instrumental

learning is a combination of operant learning and shaping. In case of operant learning there is always a relationship between a person's response and the consequences. "If a person is correct, then they are praised, and if their behavior is incorrect, then they are reprimanded" (Thomson, Solms 1998).

In the contrary to the first method, changing attitudes through a change in behavior is much more likely to have a higher efficiency and "result in long-term modification of behavior" (Thomson, Solms 1998). This method is based on dissonance theory and attribution techniques. Baron and Byrne (1982) define self-attribution as a person's need for justification of their behavior, they want to know the reason why they should behave in a particular way.

Lastly, a most effective way for lasting attitude change is change through persuasion. This method does not trick customers into changing their mind and views on the subject. Persuasion includes correct exposure, attention, comprehension, acceptance, and retention (Thomson, Solms 1998). Here, we again face the need to know our target audience better, to find the ways of engaging a customer with the information provided, to make them listen to the message. To be able to keep the attention of a customer and not to let them "zone out" the information provided message must be useful and current. The message must be formulated in a way that makes a customer believe that the content of the message is not as different from their beliefs after all. It is also crucial for the information to be comprehensible. If it is overcomplicated or too technical and dull, the customers will not be able to understand it, therefore all interest and engagement will be lost.

At this stage, the choice of message delivery method plays a vital role. Message delivery media must ensure that the customers will have an opportunity to receive the information at their own pace and with timing that is comfortable to them. Which means the message must be visible until a customer decides that they have read and understood it completely.

Retention deals with maintaining achieved progress in attitude change and in accumulated knowledge by the customers. To ensure this, the messages must be recurrent. Repetition is the mother of knowledge - says a Russian proverb.

Additionally, it is possible to evaluate customers' gained knowledge with occasional checkup and quizzes.

In order to achieve success in the customers' attitude change towards a more aware use of eBanking system, the issues and methods discussed above should be integrated into a security awareness program (Thomson, Solms 1998), be it a face-to-face presentation or a remote learning platform.

3.3.2.2 Educational Point of View

During the development of a training program for eBanking customers we are facing not only a dilemma of the psychological approach to an individual customer and the target group as a whole, but we are also faced with the task of finding the right educational approach to learning. Development of an effective training program can only be based on a scientific approach. The literature provides numerous studies that cover the techniques and methodologies of adult education. Recent studies show, that personal approach to adult education is developed by various factors such as a person's personality, social class even gender (Milheim, 2011). According to Millheim, there are several teaching philosophies which influence the design of education program and the learning environment in general. At its core, the adult education philosophy consists of several categories: liberal, behaviorist, progressive, humanistic and radical (Elias, Merriam, 1995).

Each of the mentioned educational approaches has their strong and weak sides. They must be chosen according to the purpose and desired design of a "classroom environment". For the purposes of this thesis, we address the humanistic approach to the education, more precisely - critical humanism.

Humanism "essentially relies on a learner-centered focus in the classroom. It relies on the identification of learner needs, and how to best address them in the classroom" (Milheim 2011, p. 25). Critical-humanism, which will be used in this work, adopts similar elements as humanism. However, instead of being concentrated on learner's willingness and need of self-direction, this approach emphasizes the "importance of the surroundings and environment that are influencing their needs" (Milheim 2011, p. 26).

Environmental influence can include various factors as mentioned above, e.g. class, political or social views or demographic aspects.

Another factor to consider while exploring the theoretical approaches to adult education is the medium for delivering knowledge to learners. Educating customers online provides different challenges in comparison with the face-to-face education. "In an online learning environment, both motivation and learner control must exist in order for learning to take place" (Milheim 2011, p. 26). Amongst many perks of online education are low cost, availability, ability to cover a high number of people simultaneously. Most importantly, it provides an opportunity for the customers to learn at their own pace and in their own time. "To support the humanism approach of learning, the online learning environment will need to be set up in a way that motivates learners and allows opportunities for the learners to set up their own goals and the strategies to achieve them" (LeClair et al. 2013, p. 73). In other words, the task for a critical-humanist educator is to design the teaching process in a way to ensure that the learner will become an "autonomous thinker". This can only be achieved through the "[...] recognition of difference, that is, the factors that influence our thoughts and beliefs, particularly with respect to our viewpoints" (Milheim 2011, p. 27).

Hantea et al. (2006) identifies the need for a comprehensive approach to the education of IT security and presents information security model which underlines the need for integrated cyber security education. In their research about roles of individual employees on information security in an organization, Lee et al. (2010) necessitates the need for every employee regardless of their rank and specialty, to have a required set of IT and cyber security skills. This notion must as well be translated for every customer who has a relationship with an organization. A customer must be required to have high awareness level about IT security, issues, and prevention methods and meet the set requirements. This way they will lose their status as the weakest link in organization's security system and make the system more stable as a whole.

LeClair et al. (2013), based on ideas from Amanda Andress's book, proposes dividing the process of creating cyber security awareness into three main pillars: technology, people, and process.

People element of the domain implies designing the educational platform with the end user in mind (LeClair et al. 2013). Human error is still a very current issue and has been one of the major causes of security breaches in past (Mitnik, Simon 2003). The system should be easy to use and easy to understand, content must be informative but at the same time not overwhelming. The main objective is to deliver information to the customer and this goal can be achieved by drawing the customer and waking their interest. Moreover, the goal of the program is to lead a customer towards a security-aware behavior on the very core level. This can be achieved by finding an individual approach to a customer based on their previous knowledge and experience. "It is through this individual understanding that education leads to social change" (Tisdell, Waylor). Overcomplicated system or content material may have a radically opposite effect. A customer might lose interest right away, get annoyed or even repulsed by the program (LeClair et al. 2013, p. 75); the process element implies integrating cyber security strategies into existing system and procedures in the organization and the technology element takes us back to the need for all actors of organization, be it management, employees or customers, to play their role in the cyber security program (LeClair et al. 2013).

These elements will be taken into consideration in the development of the prototype for raising customers' awareness about IT security.

3.3.2.3 Continuous learning

Getting an education and learning new things is an important aspect of every persons' life. Any individual person has their methods and approaches to learning; depending on their age, mindset interests, and other characteristics, a person accumulates knowledge either with ease and at a set pace or rather slowly and with some degree of struggle. However, regardless of the speed or volumes of gathered knowledge, the traditional learning method has its limits.

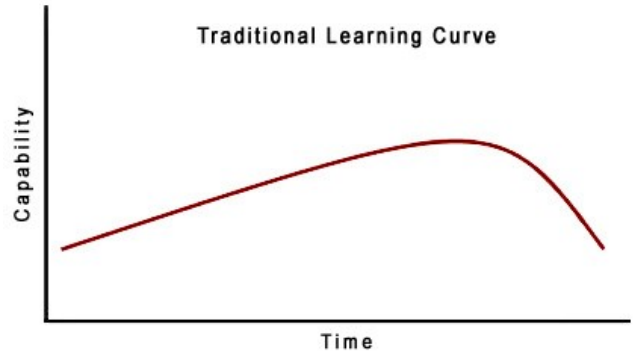


Figure 9: Traditional Learning Curve [Source of original: Hebert 2007]

Figure 9 demonstrates the finite nature of a person's ability to hold on to the acquired knowledge. This means that regardless of how diligent the person was during the learning process, eventually big part of the information will be forgotten.

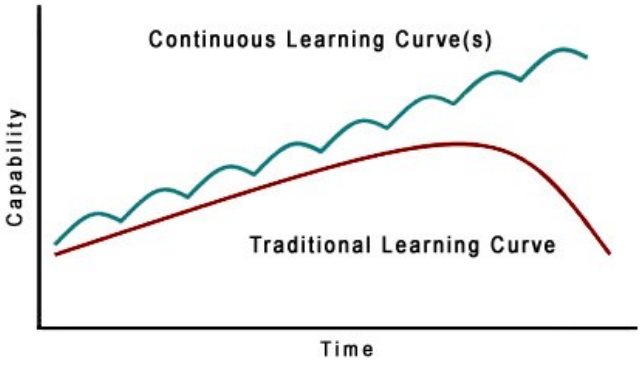


Figure 10: Continuous Learning Curve [Source of original: Herbert 2007]

On the other hand, a continuous learning approach keeps the learner on track throughout their whole life, if needed. Figure 3.3 shows the comparison between the traditional learning curve and continuous (step-like) learning curve. With the nonstop flow of information, a person has no time to forget much of it and is more likely to apply their knowledge in practice. Moreover, providing knowledge in small portions is perceived benevolently and in its turn, this perception promotes a positive attitude towards learning and high level of absorption of the provided material.

Additionally, this approach proves to be relevant and applicable to the teaching about advanced topics, e.g. Information Security, given their tendency of becoming obsolete and requiring a regular update of information.

3.3.2.4 Marketing Approach

When studying the means of providing the customers' with the information about security, it is helpful to consider some of the techniques borrowed from the domain of internal marketing. If we approach the message delivery to a customer as "selling" the information to a consumer, then we can borrow the famous four P's of marketing (Product, Price, Place, and Promotion)and adapt it to face our needs (Schlienger, Teufel 2003).

As a product, we consider the information about IT security. The requirements to the product are informativeness, appeal to the broader audience, simplicity, and usefulness; price in our case would be the time and effort a customer spends to read and comprehend the provided information. In the background price might have an actual monetary value, for example, the real cost of training and seminars on IT security, which the customers can spare if they will have the alternative, affordable source of education; the third P defines a place, or distribution channel, which is an online tool that is integrated into a bank's CRM system; Under promotion we must understand the ways of message delivery (Schlienger, Teufel 2003), which will be discussed in detail in chapter 4.

3.3.2.5 Technical Approach

The means and method of delivering a message to the customers play a deciding role for the level of effectiveness of the educational program. As already mentioned in earlier chapters, without engaging a customer in an interesting learning experience, the whole intention of raising their awareness will fail.

It has been established long ago, that there is a strong relationship between the method of assimilation of an educational material and a person's ability to recollect the acquired knowledge sometime later. If the provided material is in an audio format, a person can remember only about one-quarter of it; If it is a visual media - a person can remember about a third of the amount; with the combination of both of the above - half of the information is taken in by a person. The most successful method, however, is

recognized to be the one that engages the learner to actively participate in the education process.

E-learning tools usually use the active learning methods, which increases the learning success significantly. Active learning implies an interactive communication between an e-learning tool and the learner. The communication can be synchronous, used for supervised online courses, or asynchronous when each learner is becoming the information at a time convenient for them.

To create a successful online learning platform there arises the need for humanizing and online learning environment. This humanized type of communication is considered to be a great influence on learners' satisfaction, hence, motivation and acquisition of knowledge (Clouse, Evans 2003).

Clouse and Evans also distinguish three types of interaction: student-to-content, student-to-instructor, and student-to-student. The first type of interaction is straightforward. Student-to-instructor interaction is the most important, as the instructor takes over the responsibility to stimulate the interest to the material and create motivation for a student to learn. In our case, it is more of an indirect communication style, masked to be in the background of student-to-content interaction as the content wording, form, and appeal to a student.

Educating a customer via an unsupervised computer-mediated communication can be tricky, however, with the correct approach and design it might be highly beneficial and effective. "Interaction with technology can be as deeply relational as face-to-face interactions if sufficient time and messages are exchanged" (Clouse, Evans 2003).

3.3.3 The Role of the SA Tool in the Banking System

Based on the studies and the authors' shared experience, there emerges a necessity of design and implementation a strong IT Security Awareness program. Training customers on the topic of IT security will reduce the exposure to attacks enabled by human errors. Technologies implemented in banking sector today can provide a great platform for creating the SA program.

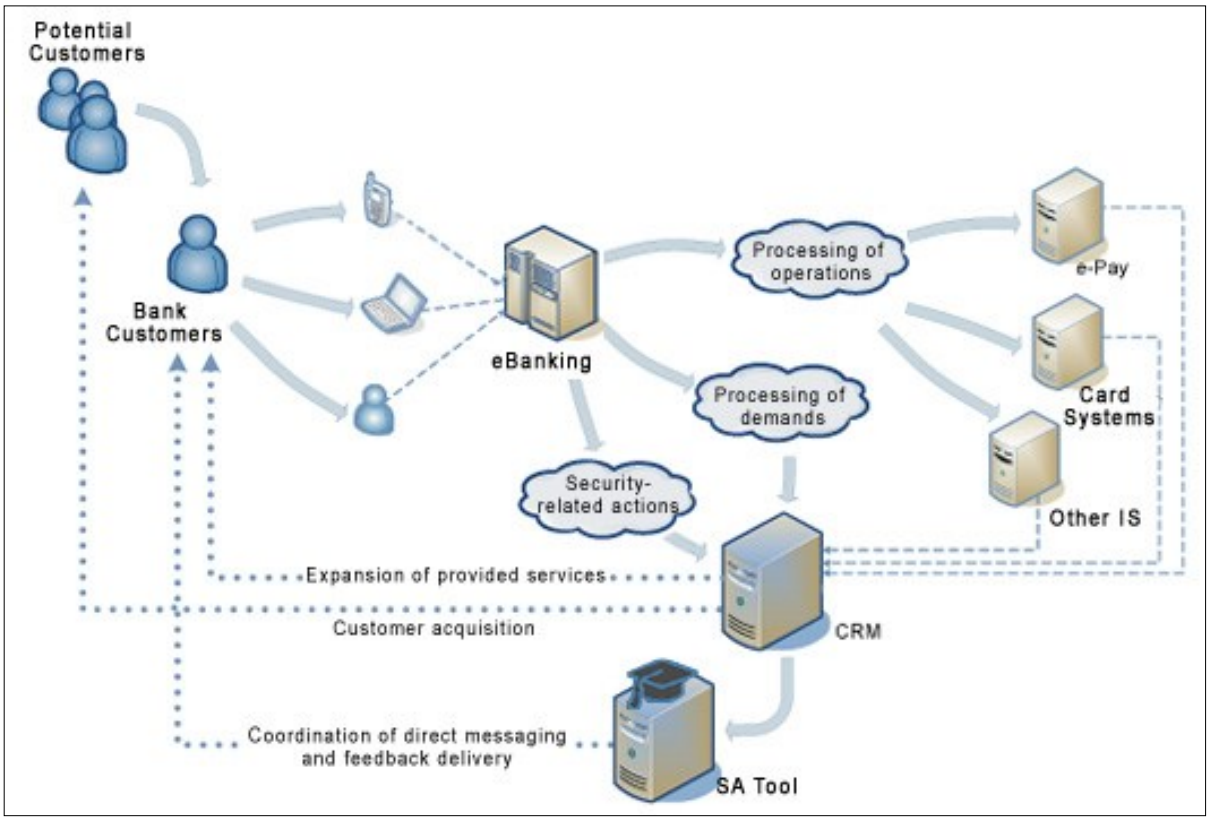


Figure 11: The assigned role of the SA tool in the general system [Source of original: Stepanov, 2008]

Figure 11 demonstrates the proposed place of the SA tool in the interconnection of other information systems. To discuss how the proposed mechanism will work, we must first define some basic concepts of the approach. The tool is intended to provide the IT security information to the customers in an effective way. For that, we need to engage the customer in the process. We intend to provide an individual approach by means of customer segmentation and addressing each group of customers on a different level with different content.

The tool uses the eBanking system as its front-office solution. First, the data from the ABS about the customer's security-related actions and behavior on the eBanking site is transferred to the CRM system; next, according to the specified segmentation parameters, the appropriate message is formed and delivered to the client either by means of an interactive dialog box or in form of an alert. The delivery method is based on the type of the corresponding action the message is about. This process is intended to be automated at large, only requiring the update of the content and twigging the parameters for achieving better effectiveness.

A particularity of processing of an outgoing and incoming flow of the communication with a customer sets the need for a process-oriented approach to the matter.

The interaction of the bank's information systems, in this case, would take place as follows: As a customer logs into their eBanking account, their behavior on the site is documented and analyzed from the security perspective. Hence the process starts in the front-office of the banking system and continues as analysis of the collected data, that is sitting in the ABS, in the CRM system. A customer's actions are registered in The CRM system as events; an event is the core element upon which the work of SA tool is based. The consequent feedback, or in our case the educational information is then communicated to a customer via the communication channels used by CRM.

A well thought through segmentation scheme, implemented in the CRM-system and behavioral data that is stored in the ABS will contribute towards implementing a successful and effective SA program.

3.4 Chapter Conclusion

While the mentioned researches concentrated on the employees and organization managers, the idea of including some of the principles in the training process can be transmitted and fitted to the present objective. The authors highlighted the fact that user profiles have changed over years. With the level of accessibility of modern technologies, we need to consider that our end-user can be of any social or educational level, it can be a CEO of a company or a grad student. Another important concept mentioned in several articles is the need of grouping users by a certain attribute and use different methods to provide appropriate knowledge to each of the user group.

By combining the actual actions and motivational techniques we can alter customers' behavior even in those cases when they do not desire to learn and make any changes. If the motivation (in any form, be it own increased security or bonus points) does not work, other techniques, that work with deeper levels of users' sub-consciousness will do their dedicated work.

Conscious changes will certainly be visible much sooner than the altered behavior of the customers who were unwilling to try. However, a slow result is still a result and will eventually bring us to the set goal.

Chapter 4 | A Process-Oriented Model

The evaluation of an existing security culture in Georgian banks based on customers attitude and behavior revealed that the target culture is not that far from existing one. The main issue is determined to be the lack of awareness program for the customers, whose numbers are slowly but steadily growing. A full change of security culture requires a complete re-engineering of existing measures and policies (Schlienger, Teufel 2003); however, maintaining an existing culture by means of a well thought through and well-designed security awareness program, which will be adjusted to meet the needs of an individual customer, is easily possible.

For designing and modeling of the mentioned awareness program and the prototype, I used the process-oriented approach, which implies modeling the sequence of events and processes.

4.1 Overview

The two main approaches that are commonly used in program modeling are event-oriented and process-oriented. The event-oriented method has advantages in terms of flexibility and computational efficiency, however, it is less suitable for training because it hides the "life cycle" of each process.

Process modeling, on the other hand, can be used to identify structure requirements and services; it can also define processes that are executed on different interconnected platforms. Therefore process-oriented approach provides a necessary tool for highlighting and delivering the benefits of the system architecture. (Schoonderwoerd 2008)

"[P]rocess modeling may be used in strategy definition, organizational change, requirements solicitation, operational optimization, functional specification, user interface flow, work instructions, and enterprise application integration (EAI) flows. Even if two models are meant to represent the same process, if they're produced for different purposes, they are likely to be different." (Schoonderwoerd 2008, p.2)

Adoption of process-centric or process-oriented modeling is a continuous process, which allows avoiding risks of failure and promotes continuous improvement and re-use of the model. With this technique, the main goal is the identification of the strategic processes. (Pavlovič 2009)

All additional or redundant processes can be easily left out and the model will still be sustainable and sound.

4.2 General View of the Support Tool (Prototype)

As it was described in previous chapters, the purpose of the support tool/prototype developed for this thesis is to provide affordable and flexible learning venue to a large group of people who might be geographically separated and have tight time constraints. More specifically, the prototype serves an andragogical purpose (LeClair et.al 2013) and creates a learner-centered learning environment for raising the customer awareness level about IT security issues and any new security threats that might become relevant. The idea is to concentrate on the needs of a learner, or their existing awareness level, and not on the specific curricula that are attributed to a learners age, like in a traditional classroom environment.

The prototype is meant to target the existing customers of a Georgian bank, who are using the electronic banking services.

4.2.1 Segmentation of Customers

In order to ensure that each customer will gate the information according to their prior knowledge it is reasonable to break down the customers into several groups; the segmentation is based on customers' level of IT and Cyber Security awareness. COBIT best practices suggest distinguishing five awareness levels of a customer: recognition, awareness, understanding the need to act, understand full requirements, advanced forward-looking understanding (COBIT 2000).

This model contains and addresses five customer maturity stages accordingly: novice, advanced beginner, competent, proficient and expert. Customer segmentation will

ensure that the right educational material is delivered to right customer, avoiding mix-up and under or overtraining the learners.

The proposed model suggests assigning levels according to customers' progress in the learning process; a priori assumption being that all of the customers are new to the concept of security culture.

Another, more elaborate method of customer segmentation would be the statistical cluster analysis. This method defines different groups according to similarities of attributes of group members. (Schlienger, Teufel 2003)

Cluster analysis requires accurate and detailed customer data, which in this particular case was not provided, hence the use of the first method.

4.3 Components of the Model

The model consists of several elements which combine into the lifecycle-components of the prototype:

Actions

Actions play a deciding role in triggering the delivery of the appropriate educational message to the customers. We distinguish two types of actions for this tool:

Event-based actions - these are the customers' actions on the eBanking site starting with the Login (including the password length and strength choice) and ending with Logout.

Response-based actions - require interaction with a user. Due to the broad nature of the topic of IT and Cyber Security, there are a variety of educational messages to be delivered to the customers. However, there are not enough on-site actions to trigger all the topics of security and evaluate a customer's behavior on a specific topic. Which means we are facing the need to interact with a customer by asking them directly about their behavior in certain situations.

After logging in a customer gets a message window with a question about their behavior or attitude to a certain security aspect. The message window provides the opportunity for a "YES" or "No" answer. At this point, we rely on customer's honest

answer to the question, although it must be mentioned, that every answer, whether it is acceptable (right) or not, provides a follow-up message about the right action for the given situation. Therefore, a customer still gets the information about correct behavior.

Level up

Level acquisition and leveling up is based on the actions. Each level consists of several unaccomplished actions. When a customer gets the message about a specific action, for example, a response-driven action, they are expected to provide an answer that is correct in the provided scenario. If the answer is acceptable, meaning that customer has the right attitude and knowledge, the status of an according to action is set to "accomplished" and that message will no longer be displayed while the customer is on the current level. Respectively, an incorrect answer sets the action to "failed" and the message will be displayed again until it is learned/accomplished.

The event-based actions have the same design, however, unlike the response-based ones, their status might change in both direction. Even if the event action is set to accomplished, if a customer fails to behave correctly on the eBanking site, e.g. closes the browser tab without hitting Logout first, the action will be set to "failed" and the customer will get the appropriate educational message again with their next Login.

Distribution of actions

Since the event-based actions are very basic security requirements, to which all eBanking customers are obliged to comply, they are distributed majorly in the first two (lower) levels. Accomplishments are evaluated and checked off based on actual events. However, as it was already mentioned before, in case of an incorrect action, a customer will get the according alert, regardless of their level.

Level down

In the future, it is possible to set a counter for these fails and set up rules for leveling a customer down in case of non-compliance.

Messages

Since messages are delivered according to the customers' actions, they also are divided into two kinds:

Event-based messages provide a short educational text and option to expand and read further. In an actual system, it is designed to be in form of a system alert; the alert is displayed in the top of the screen during the whole session and is gone after the logout action.

Alerts have three levels of severity: danger, warning, and information. Event-based actions that trigger the alerts are very basic and important security features, therefore they are designed to appear to customers at the first or the second level.

The response-based message provides security tip or a security-themed question and the YES/NO buttons. After submitting their answer (clicking yes/no) message window displays an educational information on the subject. The questions are designed in a way, that all positive answers are viewed by the system as correct, and negatives as incorrect.

There are two delivery methods for messages according to their type. Event-based messages, which do not require any interaction, are displayed in form of HTML alerts on the screen. The color of an alert varies according to the severity or level of importance of the message. Response-based messages are delivered as interactive message windows.

Reward system

Even though the awareness program is necessary to involve customers in security effort and culture, the compliance from the side of an end user is still not guaranteed; a necessity of customers' motivation arises. To boost the motivation of customers, the model should include some incentives for accomplishing the given tasks and leveling up. A suggested boost is a reward system based on points, where a customer collects a certain amount of points for each accomplished action, a point boost at each level up and additional points for keeping a good job at maintaining the high levels for a longer period of time.

The cumulative points might serve as a ranking amongst customers, that will be visible to all customers on their eBanking site. The ranking would potential lift the competitive spirit amongst the customers, motivating them to stay on their best behavior/stay on point.

Additionally, the points might be exchanged for small incentives or tokens, e.g. a promotional product from a bank, a small credit on the mobile account, a month of free premium service etc.

A point/reward system ensures an individual approach to the customer, that means engaging them and making them part of the process, consequently boosting their motivation to participate.

4.4 The Structure of the Support Tool

The model can be viewed as a cycle consisting of three major components: level assessment, training, and level up.

4.4.1 Level assessment

This component includes in itself both level acquisition by a new customer, meaning assigning level to the customer that just logged in to their eBanking account; and assessment of existing level for an ongoing customer at the Login. The customer data is matched with the patterns with pre-assigned levels, from 1 to 5.

Since the proposed support tool is a part of a bank's CRM system, it re-uses the system's database and engines to serve its purpose. Therefore, in an actual system, customer cluster analysis and pattern extraction will be taken over by the CRM system and its data mining engine.

In a program-mockup that is developed for demonstration purposes, each level has several actions assigned to it. These actions have statuses, which are by default set to 'false'. This means that the action is not accomplished by the user yet, therefore the action-bound message is still in the queue to be displayed at the next user login. A customer will not be able to level up until there is at least one not accomplished or failed task in the queue. An action, be it event-based or response-based, is chosen randomly at the start of the program. The chosen action triggers the message to be displayed. This event leads to the next step - training.

4.4.2 Training

At every login to the eBanking account, the engine is prompted to analyze and compare customer's current status (level, checked off actions, event status for the last session). The outcome triggers the corresponding events or actions to be activated and consequently, an appropriate message is displayed to the customer. In cases, if a customer's last session was conducted or has ended abnormally, for example, a customer has forgotten to end their work with a click on the Logout button, the triggered message will relate to that specific action, regardless of the customer's level.

At this point, the design of delivery process and the educational material will play the crucial role in the successful outcome. The important part is to push users forwards and not confuse them, simultaneously not to lose their interest and motivation.

4.4.2.1 Content

A number of sources from the literature review claim that educational messages, which are delivered to customers, should be informative but short; they should not be filled with technical jargon and must ensure that all users will fully understand the content. The content of the message must deliver the necessary information by engaging the customer to read it and trigger interest to learn more. Moreover, it should not allow the reader to 'zone out' while reading, or skip reading altogether. The delivered content is based on the customer's prior knowledge and experience, or on their behavior on the eBanking site during each session.

Raising information security awareness is a dynamic process. The fact that the risks and circumstances change continuously causes the need for constant evaluation of the training program and keeping it up-to-date with newest data on risk profiles. (Kruger, Kearney 2006)

The training course is composed to include educational messages that are thematically divided into five groups. Every level includes one or several messages from each thematic group according to the complexity of a given message. The five group topics are following:

Password management. Every password-related message is grouped under this topic, from creating a strong password to password storing, sharing and reusing issues;

Handling sensitive information. This group contains messages that concern sharing own and foreign sensitive information with the third parties, storing this information on a removable media or within reach of others;

Physical protection. This group unites such topics as leaving one's computer unattended in a public place, using unsecured network or public computers for work etc;

Social engineering - groups the topics about scammers, phishing, oversharing on social media and more.

Actual topics - contain the information about current and actual issues, the latest security breaches, attacks and the means of protection.

4.4.3 Evaluation and Level-up

After checking off every single corresponding action from a current level, a customer achieves a new level. All new level appropriate actions are initially checked as "not accomplished" and the new educational message is chosen randomly to be displayed. After a certain number of logins, the evaluation process takes place. The customer data is matched to the patterns again, if there are no "failed" actions (fail counters are all set to 0), the customer gains additional points.

An additional feature that can be added to the model in the future is the evaluation of gained knowledge and adherence to the covered material by the customer. Besides the existing method of level assessment, where a customer checks off the list of level-appropriate actions, other evaluation methods can be designed and implemented. As an example of an additional method, we could view an occasional IT security quiz or a possibility for a customer to upload their proof of IT security knowledge in form of a certificate or other credentials.

An evaluation will affect the current level of a customer and provide additional motivational points if completed successfully.

4.5 System Design

The delivered content is based on the customer's prior knowledge and experience, or on their behavior on the eBanking site in each session. The tool has a task-centered (need-centered) learning approach, which means identifying a weak spot in the customer's knowledge and addressing that spot more intensively, thus eliminating gaps in customer's IT security knowledge.

4.5.1 Process Model

The following figure (figure 12) represents a process model for the developed tool. This model describes the sequence of the carried-out processes as well as their relative order. (Chopra et al. 2013)

A process start is triggered when a customer logs in to their eBanking account. After a page is fully loaded the tool waits a previously set amount of time, in this case3 seconds, to execute the first action. This gives a customer time to adapt to a new screen without getting instant pop-ups which would dazzle them.

After the waiting time is up, the first requests for checking the customers' data is sent to the database. This action includes checking CRM event log for an abnormal operational behavior of a customer in their previous session. Under the term "abnormal behavior" we imply such actions which contradict the security features and policies of the system. For example, if a customer closed the browser tab or window without signing out; or they let the session to time out, assuming they left their computer unattended for a certain amount of time, which might also lead to security problems.

In case the database/JSON file returns the positive response to the abnormal activity in the previous session. In this case, an alert message corresponding to the abnormal activity is displayed on the customer's screen, addressing the specific issue and drawing their attention to the severity of their actions.

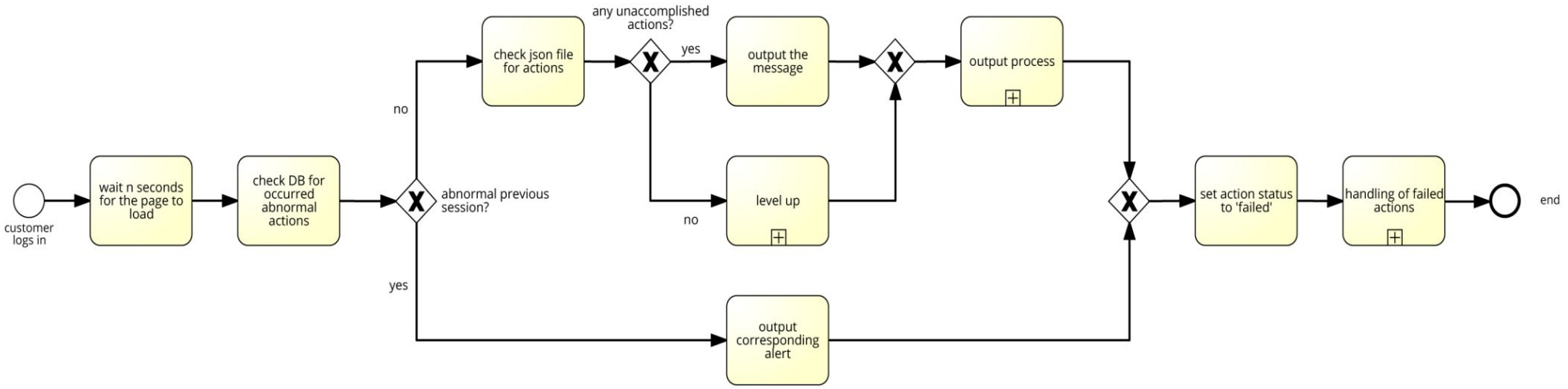


Figure 12: A process model of the support tool

Following the output of an alert message the tool sets a 'fail-counter' for this action to +1 and continues to a sub-process that handles the failed actions. The sub-processes will be discussed further in this chapter.

An alternative process flow is carried out when the event log does not show any dubious actions from a customers' side, a request for a level check is sent to the database (JSON file in our particular case). A customers' current level is checked by evaluating the status of each action/message that is assigned to this level. If the actions/messages are marked as successfully accomplished they are no more in the sequence of being displayed to the customer. Hence, if all of the actions with corresponding messages have this status and there are no more messages to be displayed, a customer is considered to have had finished the level successfully and they are hence promoted to the next level. Leveling up is a sub-process in itself. As is the next activity - message output process.

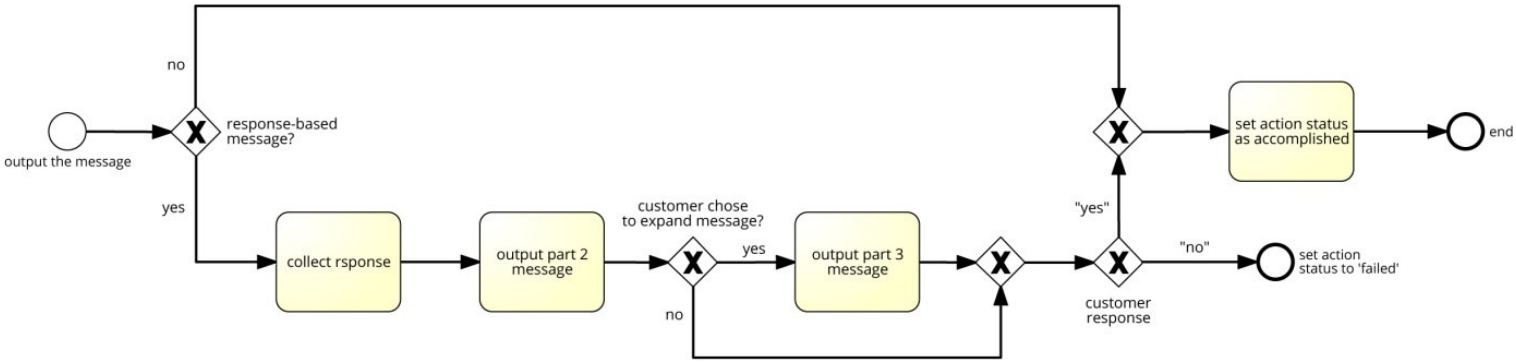


Figure 13: Message output sub-process

A message output sub-process is triggered when the educational message is displayed to the customer. Depending on the type of the displayed message one of two process flows will be activated. If it is a response-based message, after an output the system will wait for the customer's response, after which the second part - the educational message itself is displayed. If a customer chooses to expand the message using the built-in link they will be provided with a full text of the message.

At this point, the tool evaluates the customers' first response. Since a customer's response is an alternative to their actions, it will be further handled as such. If the customer responded to the question/message with a YES, indicating that they know the right behavior for this security related situation, the status of the message will be set to accomplished and the message will not appear to the customer anymore.

In case if the response is negative, it is assumed that a customer has still to be made aware of the right behavior for the set situation, hence the status for this action/message is marked as failed and the process flow continues with the fail handling sub-process.

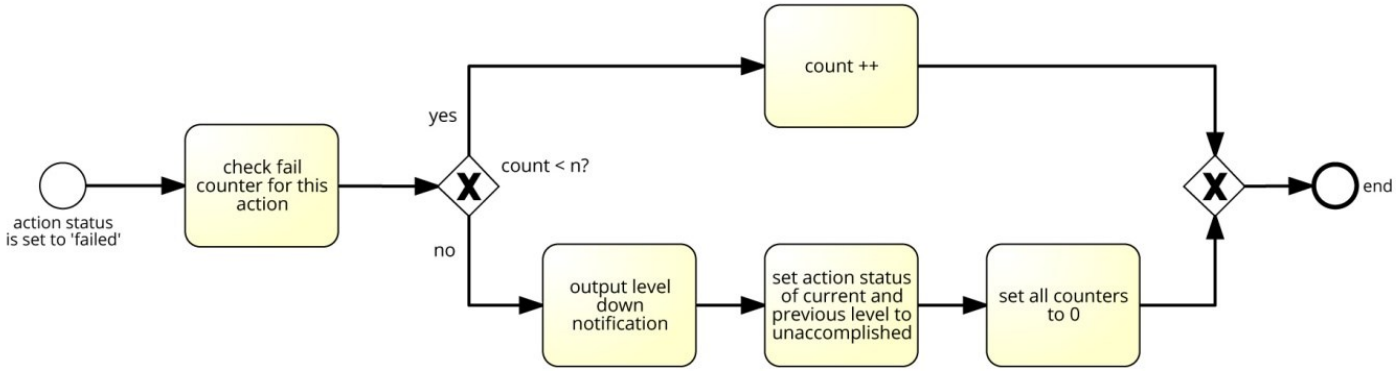


Figure 14: Fail handling sub-process

A sub-process that handles the failed actions is triggered when the status of the action/message is set to "failed". The system checks the fail counter to determine the number of times a customer has not understood the message and/or has not behaved accordingly. If the counter shows the number that is less than η, where η is a predetermined number of allowed fails, the number is increased by one and the process comes to an end. In case when an n number of fails has been achieved, a customer gets a notification that they have been downgraded a level. After delivering the notification the status of the actions for current and previous levels roll back to default, which is neutral or unaccomplished. All counters are then set to 0. This way, at the next login when the system checks the level of the customer and finds, that actions from the previous level are yet to be accomplished, the customer will automatically be assigned to that level.

Modeling the processes in this way allows for standardization of the work to be done. Furthermore, a process model can help identify an operational problem at early stages and it allows us to analyze each process step separately to determine the actual necessity of this step. Each action can be overlooked, modified to be more effective or completely eliminated if it is proved to create a redundancy.

Chapter 5 | Implementation of a Prototype

This chapter describes the technical aspects of the prototype implementation. It creates an overview on the architecture of the support tool, its main components and the interoperability with the actual CRM system. Additionally, the chapter presents a visual storyboard depicting the message delivery component, as a part of the eBanking GUI.

5.1 Main Technical Solutions

The prototype of the support tool is intended for the use in collaboration with a CRM System and electronic banking, therefore it can be implemented in .NET or any other programming language that is compatible with the particular CRM System employed by the bank.

The actual proposed prototype that was developed within the framework of this thesis represents a model of the tool; it was developed in JavaScript on basis of Electron. Electron is a system that enables development of cross-platform desktop applications simply using web-technologies such as HTML, CSS, and JavaScript[5]. The tool uses JSON for exchanging data between a server and a browser; Electron uses Chromium (version 45.0.2454.85) and its multi-processor architecture to display created web pages.

Compared to a regular browser, where the web pages are launched in a closed environment (the so-called sandbox), Electron provides the opportunity to access native resources; it uses Node.js API on the web pages, enabling access and interaction with the operating system at a low level (Habr2016-1) (Habr2016-2).

The user interface is the web page we create. In this case, we are not limited to the system selection of interface elements of our platform and we can create the needed UI elements using web technologies.

For the purposes of clarity, the term "interface" will be used in relation to the Chromium window that imitates a customer's online banking experience.

[5] https://electronjs.org/

5.1.2 Interoperability with the Adjacent Systems

There are several options for an integration of a prototype into the CRM system. The simplest one is the integration on a process-level of inter-system relationships. An alternative could be an implementation of the solutions in SOA-architecture, which allows to manage various integration systems and flexibly configure them. Of course, the use of SOA is a more progressive approach, but in its turn, this approach requires certain requirements for "maturity" and the degree of formalization of the processes that are subject to automation. (Yaroslavceva 2013)

As already mentioned before, the support tool can be implemented as a CRM plug-in to avoid complications with the interoperability of different technologies. Plug-ins are powerful approaches to extending the application; its objective being enhancing the standard features and processes of a CRM System; a plug-in adds a custom touch and adapted business logic into the execution of tasks performed by an end user (Power Objects 2017).

It must be mentioned, that plug-in development requires an understanding of such concepts as a context of the incoming data, exception handling, using impersonation and debugging issues.

5.2 General Description

As a result of the conducted study, a support tool was created. Current prototype serves as a mockup for a future CRM plug-ins that can be incorporated into the system for adding a customer IT security education element to the overall security of the bank. The tool does not have a specifically designed interface since it is merged to work with an existing interface of the eBanking website. This fact makes the tool intuitive and easy to use by default. User interaction is carried out by the interactive message delivery system, that provides the eBanking customers with an information about IT security, general security tips and updates on the topic.

In real life application of the prototype, most of the actions are carried out 'behind the scenes' by the CRM engines and the algorithm of the tool. The latter uses data from

repositories of information, mined and analyzed by the CRM to provide an individual approach to each customer as accurately as possible.

For the demonstrative program-mockup, we use our own repositories with the data that imitates the CRM system events (or messages) that are triggered by customers' actions on the site.

5.3 Program architecture

This chapter creates an overview of the implementation process and its outcome - the prototype itself. It includes the definition of a structured solution which meets the technical and operational requirements set in the previous chapter.

5.3.1 Component diagram

A component diagram, in contrast to the previously presented process model diagram, describes the features of the physical representation of the system. The component diagram allows us to determine the architecture of the system being developed, establishing dependencies between software components, which can be either the source, binary or an executable code.

provides a generic view of the main components of the SA tool. Each component represents a separate function in the main code of the program; except of the eBanking page, which acts as an interface for displaying the results of the work the tool.

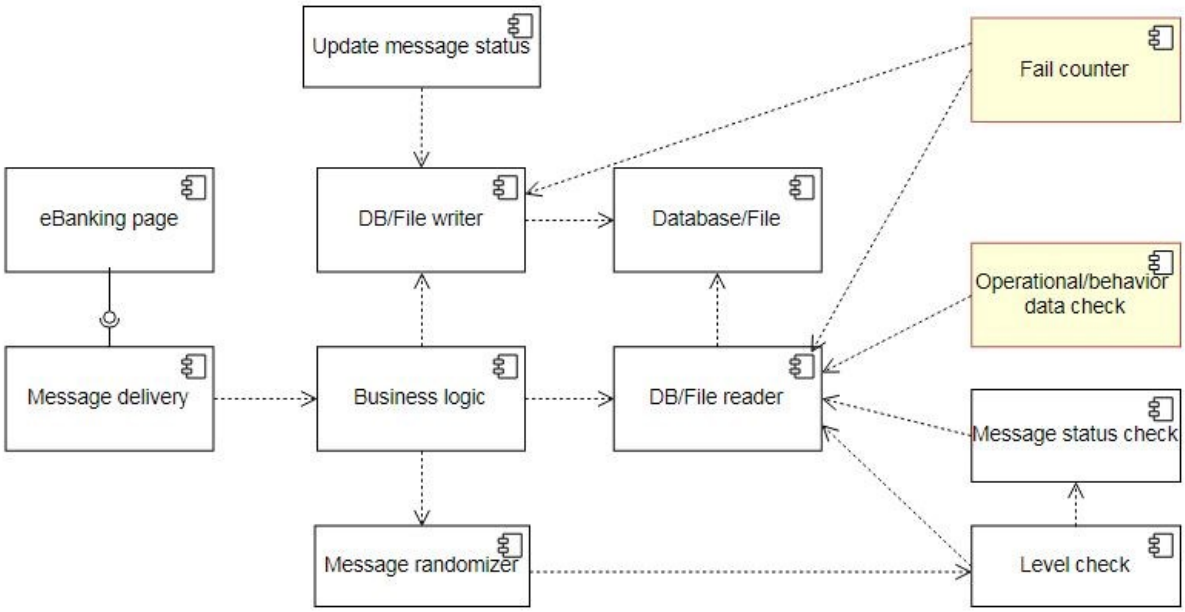


Figure 15: A component diagram for the SA tool

The core processes take place in the business logic module, where all the main decisions are made. This module in its turn uses several other modules to keep the processes running.

Database/file reader consists of the code responsible for retrieving the data from database and repositories for further processing.

For working with the actual CRM system and DB-based data storages it will be using the CRUD operations, which are common for working with the persistent data storages. [GET function]

Database/file writer is similar to the previous module with a distinction, that it is responsible for making alterations and modifying the database tables and the data they contain. [POST and UPDATE function] In our case it is based on JavaScript's writeFile function that is provided with the file path to .json file containing data.

The three other components that use the reader module are level check, status check, and behavioral data check. The first function evaluates a customer's current level using the results of the status check function.

Message randomizer makes sure the messages are displayed in random order; it uses the level check function in order to disregard the messages with corresponding actions that are already marked as accomplished.

Updating the message status occurs through database/file writer function. Both reader and writer functions are connected to the actual database/data repository, which serves as an external component.

The colored components are still in the development phase and are part of the future development work for this project.

5.3.2 Sequence diagram

When the system is implemented it can produce a variety of use cases, depending on the number of parallel or alternative process flows it incorporates.

"Whenever during the realization an interaction between the business actor and a business worker that is automated, this introduces the interaction between the User and a System, which ultimately results in one or more System Use Cases. Similarly, when there is an interaction between two automated business workers, this results in a system-to-system interaction". (Java Exam 2012)

If we take an example of a simple straightforward process, where there are no complications in form of the abnormal user actions or misunderstood message contents (negative response to the message) the first use case would look somewhat as shown in figure 12. The following sequence (or cooperation) diagram represents how the participating actors cooperate with each other to implement the activity; the diagram also shows the interactions between the customer and the different systems.

The tool is intended to run when the CRM system receives a system message about an operation which is triggered when a customer logs in to their eBanking account. System messages, in substance, are web service operations (Power Objects 2017). They are referenced to CRM system events, triggered when certain actions from a user are taken, e.g. creation of a new record, queries etc. In this scenario, we have the trigger - a customer logs in, and the following sequence of activities which occur after the SA tool processes are set off by it.

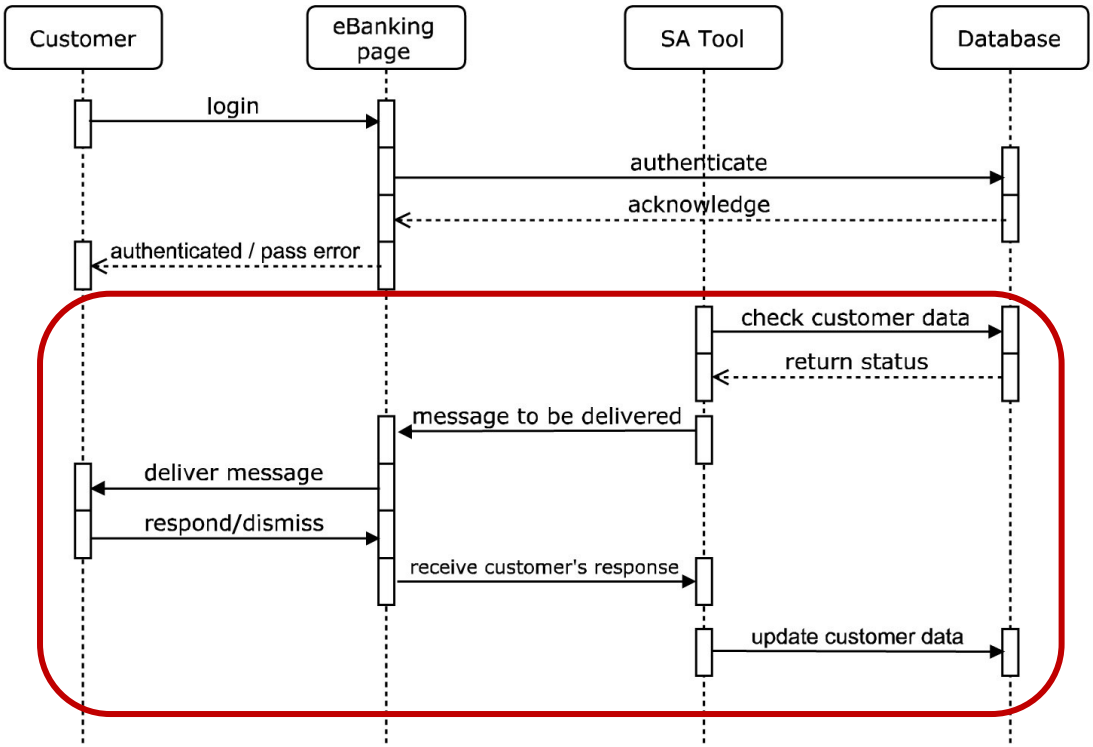


Figure 16: A sequence/cooperation diagram

The interaction happens mostly between the systems; hence the majority of processes are hidden from the customer's view. However, the key is still the interaction between a user and the system. To achieve this communication, we require having a graphical user interface (GUI). In our case the eBanking system GUI, specifically the eBanking web page serves as the intermediary system for the system-user communication.

5.3.3 Visual storyboard

Further chapters will provide the visualization of the users' interaction experience with the prototype. The visual storyboard is based on actual scenarios that have been modeled during the process modeling phase.

5.4 The Prototype

To start the program, we need to click on the folder containing the project with the right mouse button and select Git Bash here from the drop-down menu. This will open a

console window. To run the program, we first need to start electron using the "npm start" command. This will open a browser window - a desktop version of an eBanking login page that a customer will access via their browser.

Figure 17: Console window and commands for starting Electron

5.4.1 Visual storyboard: User Interaction

During an interaction with the system, only a fraction of the SA tool is actually visible to the user; it does not take up too much of customers' time or effort. It might seem to have a low functionality; however, we have to remember that this tool is not meant to provide the lectures on Information Security, but a short information about the topic, in order to make a customer aware of the issue and maybe even wake enough interest to learn more.

During the login process, a customer enters their credentials into appropriate fields. Every n-th login a system sends a note to the customer to remind them of the importance of creating a strong password and other password related tips.

After a successful login, the program waits until the page is fully loaded. The waiting timer can be set to a desired amount of time, in this case, the program starts after 3 seconds when the page is loaded. Based on the customer's level, accomplished actions and behavior analysis from the previous session, they get a message box, which contains appropriate security information.

In case of the response-based message customer gets a choice of two answer buttons: YES and NO. The alerts.json file containing the actions and messages are designed in a way, that by answering YES a customer checks the corresponding action as accomplished. In this case, the program will skip that action at next logins indefinitely, allowing a customer to level up (in case all actions are accomplished).

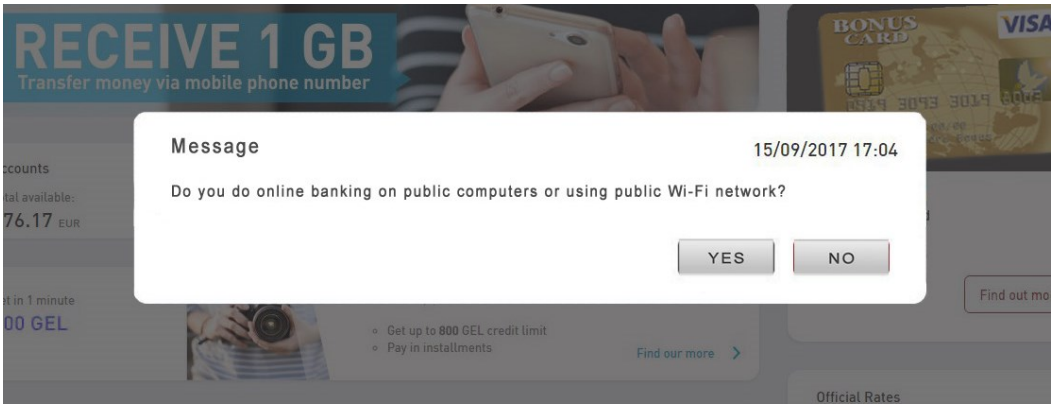


Figure 18: A response-based message example

After submitting their response, a customer gets another message box with an educational message. The box contains the short and on point information and an option expand the window and to read a more elaborate version of it, in case of an awoken interest. The message box can be then dismissed by clicking a single 'Good to know' button.

Figure 19: An example of an educational message

Event-based messages do not require an answer, therefore they only provide the information and can be dismissed by clicking the OK button. In an actual system, the model implies a different approach to delivering the event-driven messages. The messages will be displayed in form of alerts, that cannot be dismissed unless the correct action is taken by the customer. Alerts are color coded according to the severity of the incorrect customer actions and behavior.

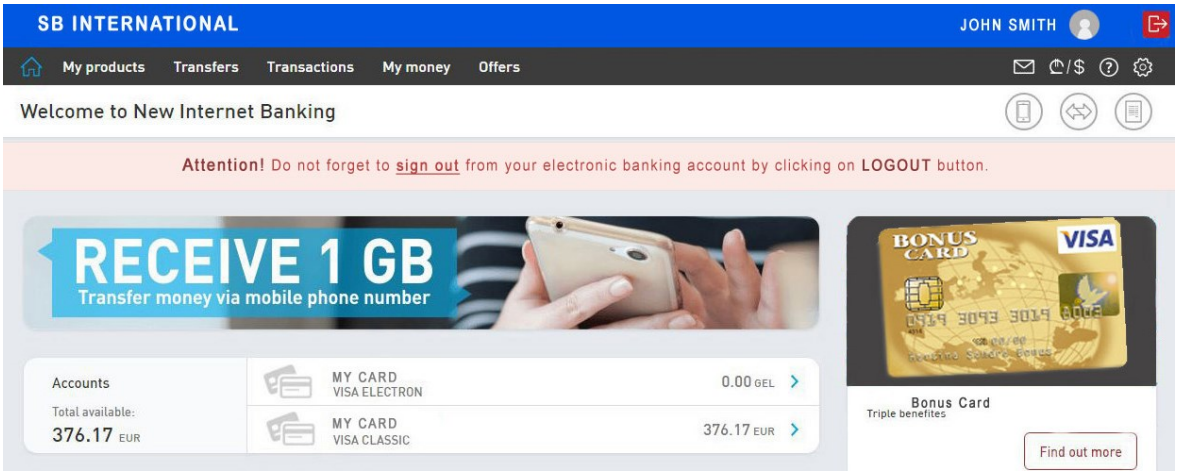


Figure 20: An example of event-based alert display

Let us examine the processes behind the YES and NO buttons. As it was already mentioned, the response buttons carry an additional logical construct in the code of the program. The YES button is assigned a task to change the status of an action from neutral, which is by default set as 'false' to positive; Accordingly, the NO button, when clicked, changes the status to 'failed'. When an action is set to 'failed' the fail counter for this action adds up by one unit. After a pre-determined number of fails to perform the action correctly, the system is alerted to downgrade the customer. Downgrading implies a set of actions from the program code. The statuses of already accomplished actions from a previous level are changed to 'false', which automatically implies that a customer has not finished that level yet. Hence, they level down. The fail counters are set to zero and the level education begins from scratch.

Chapter 6 | Testing and Evaluation

This chapter describes the evaluation process for the prototype. The evaluation includes preparation for the testing, assessment of participants' knowledge prior to the testing, the evaluation process itself and discussion of the results.

Hereby it must be noted, that due to the small number of participants the acquired results do not provide sufficient data for statistical analysis. The goal of this evaluation is to collect the assessment indicators, which help to determine whether the tool provides an influence on users' attitude and change in the level of awareness about information security. With the help of a group of participants, who are representing different age, social and educational groups, this goal was successfully reached.

6.1 Theoretical Description of the Testing Method

The evaluation of the developed prototype is conducted with the objective to check the correspondence between the expected and actual results provided by the program. Evaluation is performed based on testing methods selected to assess a particular aspect of the program -the outcome.

There are several software testing types, which can be roughly grouped into three categories: technical evaluation, functional testing, and user testing. Additionally, one can distinguish three methods of user testing: model-based, expert-based and user-based methods (Dillon 2001).

In this particular case, the aim is to evaluate the efficiency of a developed prototype and for this reason we will address the latter testing method - testing the program on the end user, intending to determine how the program matches its purpose of creating, raising and maintaining awareness about Information Security.

The purpose of this testing process does not target the assessment of the technical or functional aspects of the prototype; furthermore, since the program does not imply an active use from the customer side, such concept as usability testing are also rendered unimportant.

Accordingly, the outcomes-based program evaluation will be employed and discussed in this chapter.

6.1.1 User Tests

For the user testing of a prototype, a sample of users was asked to perform a set of pre-determined tasks that imitated their normal work with the eBanking application. The goal of the evaluation is to collect information about the actual usefulness of the SA tool: is it working, is it teaching; and to reveal the customers' way of thinking and attitude towards the topic and overall acceptance of this technology: are they learning?

Consequently, the identified criteria set for prototype testing are:

- evaluation of the level of accessibility of the provided information (i.e. lucidity, ease of understanding, wording, the volume of delivered information);
- the relevance of addressed topics for the customers;
- helpfulness of the tool and the extent to which it supports the intended users in their task of keeping their private information secure;
- overall effectiveness of the approach towards raising a customer's awareness level.

The testing was performed on site, amongst the employees of an NGO - Center of Free Pedagogics. The organization is responsible for managing several projects such as the Early Intervention Programme for children with developmental delays, the professional education center for people with special needs, a school for children with problems in cognitive development and many more. CFP employs a number of people with different backgrounds and personal characteristics. A scope of employees was selected with an aim to test the effectiveness of the SA tool on users of different awareness levels and backgrounds. The participants cover a wide range of characteristics: different age groups, distinct social and educational backgrounds, contrasting levels of awareness about information technologies and information security. This scope can, therefore, represent the scaled version of the population of Georgia.

Before providing the SA tool for an evaluation, the employees were asked to fill out a questionnaire. After they submitted the answers they were provided with the prototype.

Overall the evaluation process was scheduled to run for one week, with an average time expenditure of 20-30 minutes per day. During that time a test participant had an opportunity to run the program three to six times. Each cycle takes an average 3-5 minutes of a user's time, depending on the type of information/message provided, user's level and the choice whether they want to stick with the short message or expand and read more.

6.1.2 Approach to the User Evaluation

In order to determine the pace with which a person comprehends the proposed educational material, and consequently determines the effectiveness of the program itself, two questionnaires were created. The questionnaires were developed with the objective to address a specific set of users. The first questionnaire, conditionally denoted as a "before" questionnaire, carries a task of revealing the general behavioral habits of the users, as well as determining their real level of knowledge on the topic of Information Security. Additionally, the first questionnaire includes questions that are aimed at identifying the general readiness of the users to accept/adopt a technology, which allows them to learn more about Information Security and simultaneously is a part of the electronic banking system already used by them.

The second questionnaire, sent to the test participants after passing the evaluation process, aims at revealing of the learning progress among the users. This progress can be evaluated by comparing the results of "before" and "after" questionnaires.

After both questionnaires were submitted, an informal interview was conducted with more than half of the evaluation participants. The discussion filled some gaps in assessment of the general attitude of the respondents towards the topic and the tool itself. It also provided a chance to determine the respondents' mindset and their perception of different aspects of security and privacy more accurately.

6.1.3 Questionnaires and Surveys

The first questionnaire consists of two parts. Part one includes single choice questions with several answer options. The questions cover the general topic of eBanking use and some corresponding operational aspects. The questions are intended to reveal the behavioral characteristics and attitude of a user towards the issues of working with electronic banking. The participants are allowed to skip the first part in case if they are not using the electronic banking services.

Part two of the first questionnaire is aimed at identifying the specific knowledge about Information Security amongst the participants. The inquiry includes direct questions about specific notions of Information Security, scenarios of behavior cases, and a survey for the self-evaluation of users' knowledge in this field.

The second questionnaire includes the smaller number of questions and is directed to provide the results for comparison between pre-testing level of users' knowledge and their actual knowledge after an interaction with the prototype. The questionnaire consists mainly of survey type of questions and open questions. Open questions about the IS topics, which reflect the questions from a previous questionnaire, allow us to clearly recognize the user's awareness level about this topic; since they are not provided with answer options, meaning that they cannot rely on a 'lucky guess' approach, users provide their answers based solely on their knowledge.

Next step is the analysis of the collected responses and the identification of progress of user training, hence the effectiveness of the developed program.

6.2 The First Questionnaire Responses

A total of 24 employees participated in the prototype evaluation process. The first questionnaire revealed, that only 10 people from 24 are actually using the eBanking services. The half of non-users decided to skip the first part of the questionnaire with the operational questions and proceed with the knowledge assessment part directly. Therefore, the questions from part one were answered by 17 employees.

6.2.1 Operational part

The questions about the browser choice for doing electronic banking and the used operating system were asked to paint the general picture of a user's working environment and the potential level of vulnerability. For example, it is established, that Windows is by far the easiest OS to exploit; due to its intuitive design, it does not require highly technical skills and knowledge in order to be compromised and manipulated; a number of potentially unsecured sockets increase the hacker's chances.

What browser do you use for online banking?

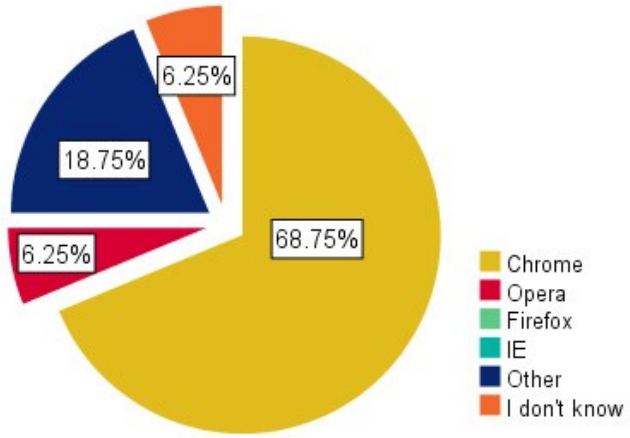


Figure 21: Browser use

68.8 percent use Chrome browser for all of their online browsing, including online banking.

What operating system do you use for online banking?

Not surprisingly, the survey showed that majority of participants use Windows-based OS (93 percent). In Georgia, the choice of Operating System is conditioned by its accessibility both physical and in terms of ease of use. People are usually provided with Windows OS when they are buying the computer and they usually do not inquire further about the security features and characteristics of the OS.

Do you keep your operating system up-to-date?

To the question about updating their OS and its security patches 56 percent admitted, that they do not keep their system up-to-date, 31 percent could not answer the question. Only two people have the automatic system update switched on.

This fact has also been explained by the respondents during a personal conversation by the fact that they a) do not understand the importance of these updates; b) fear that they will have problems with the software license; c) find the update process slow and bothersome.

Do you have the antivirus tools installed on your computers and you keep them updated?

All apart one participant have an installed antivirus software on their computer.

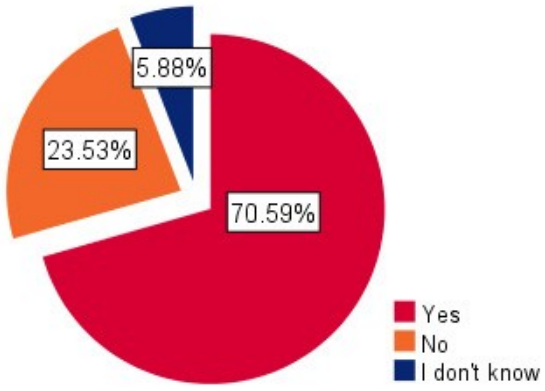


Figure 22: Installed antivirus

12 people (71 percent) of them are keeping the software up-to-date, 4 people (23.5 percent) do not update their antivirus to the latest version. One person could not answer the question.

When buying a computer in Georgia it comes equipped with a standard OS and antivirus configurations with the implication that each user will configure the software and their settings on their own. However, due to the fact that the vast majority of users are not savvy enough and have no sufficient knowledge about the technology, they are fully content with the basic setup and never attempt changing it. This is, certainly not true for all of the users. However, it is a fact for the majority of current respondents.

This fact explains the presence of an antivirus software on all of their computers. Sadly, only three of them stated in the personal conversation that they have installed their antivirus and anti-malware software consciously to protect their information and data from the external damage.

How frequently do you change your online banking password?

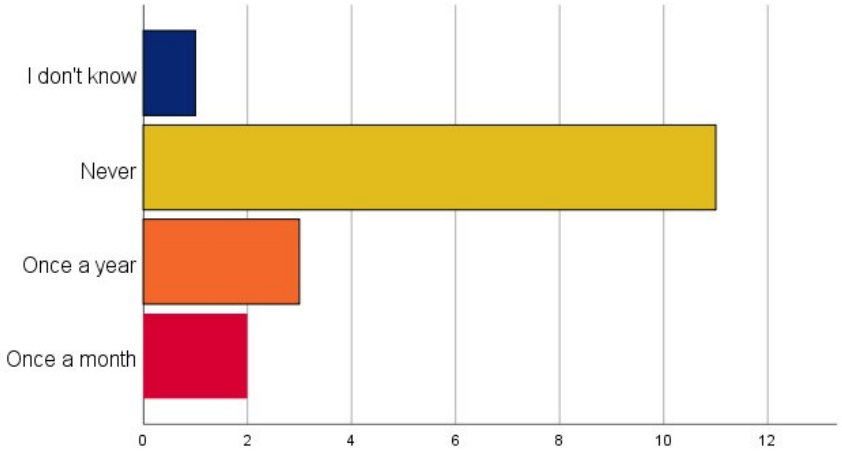


Figure 23: Frequency of password change

Eleven people or 64.7 percent of the participants never change their passwords for their online accounts. Three people (17.6 percent) set a new password once a year and two others (11.8 percent) change it every month. One person could not answer the question (5.9 percent).

How often do you check your bank statements?

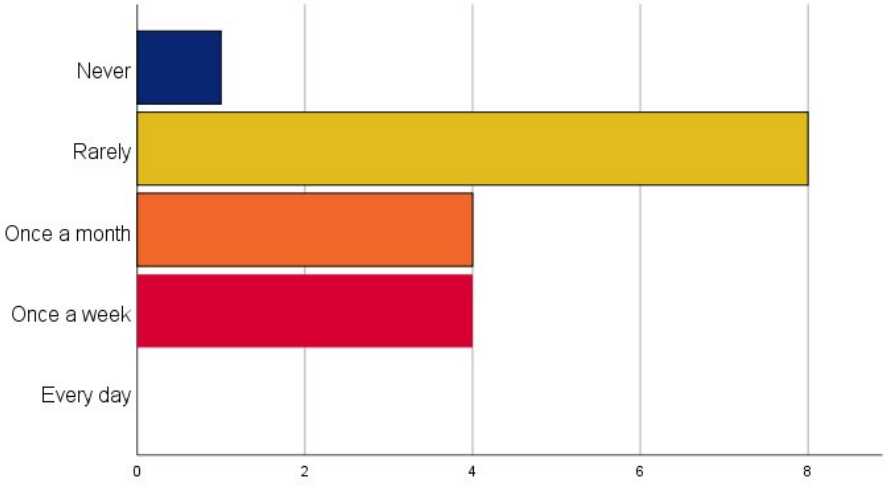


Figure 24: Frequency of account checks

An evenly distributed percentage of participants, namely 23.5 percent, check their bank accounts with the frequency of once a week and once a month. 47 percent admit that they rarely monitor their transactions. One person (6 percent) admitted that they never check their bank statements.

Did you read your banking agreement, privacy and security policies of your bank?

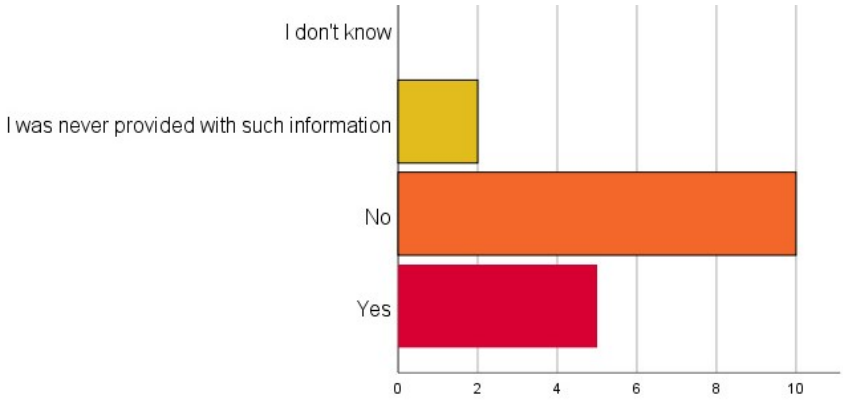


Figure 25: Read banking agreement

The survey participants were also asked, whether or not they have read the banking agreement, privacy and security policies of their bank. Almost 59 percent of them answered that they never read these documents; 11.8 percent claimed they were never provided with such information by the bank. Only 29.4 percent answered that they have read this information.

It is common for Georgian bank customers to disregard the information that is provided to them in a written form unless its importance has been explicitly brought to their attention. It is worth mentioning, that many of the Georgian banks do not provide security policies either on their web page within the user's reach nor with the general documentation that a new customer receives when joining the bank.

Do you use a unique password (i.e., not related to your other passwords) for online banking?

In order to further examine the attitude of eBanking customers towards their own security, they were asked whether or not they use the unique password for their electronic banking account. Almost 53 percent answered this question positively, 41.2

percent admitted to using same passwords for all their online accounts including social networks, emails etc. One participant could not answer the question.

Next question consisted of three parts and was aimed to identify users' actions after they have finished working with their eBanking account.

When you are finished with an online banking session which of the following do you do promptly:

Use logout: 60 percent use logout button to sing out, 20 percent end their session otherwise and another 20 percent could not answer the question.

Clear the browser cache: only one person (12.5 percent) answered that they clean the cache, 5 people (65.5) never clean it, 2 people admitted they do not know what that means (25 percent).

Close the browser window/tab: 40 percent admitted they end their session by closing the tab/window; the rest denied using this method.

From these results we can conclude, that not only are the users disregarding the common security measures, they are doing so due to lack of basic knowledge about security. The lack of such knowledge is highly concerning and sets the bar for an education starting point significantly low.

6.2.2 General Security Awareness

What do you understand under the term "Information Security"?

From the 15 employees who answered this question, four people answered honestly, that they do not understand what the term means. Seven people provided the vague explanation which was mostly based on the wordplay on information security. Only four people knew the exact meaning of the term and could provide a comprehensive answer to this question.

Do you have any prior knowledge (or experience) about Information Security?

Surprisingly, only one person answered positively to this question. 13 people which make up roughly 54 percent have stated, that they have heard about it but do not have

any specific knowledge about the topic. Ten people, 42 percent answered simply with a no, meaning they do not have any knowledge or experience in this field.

Do you consider Information Security and Data Protection to be the important aspects of provided online services?

Two people did not consider these aspects important for their everyday use of online services; the rest 22 participants understand the necessity of IS and data protection and feel that it should be a part of any service provided online. Most of them justified their positive answer with their wish to have their undisturbed privacy. Several people provided a nonspecific explanation for their answer. Only one person refrained from explaining their previous answer.

Do you know what a phishing attack is?

None of the participants know what a phishing attack is, hence everyone answered this question with a "no".

Do you know what an email scam is and how to identify one?

Half of the survey participants admit they know what it is, another half did not know the meaning of this term. None of them know how to identify an email scammer.

Have you ever shared your password with someone else?

This question split the respondents in who equal groups - 50 percent admit that they share their password, but only with their relatives; the rest deny having ever shared a password with another person.

Do you keep your passwords written down (e.g. on paper or on the phone)?

Half of the questioned employees keep their passwords written down in some form; another half prefers remembering their passwords without having to store them on some media.

		Written password		
		Yes	No	Total
Password sharing	Yes, but only with relatives	10	2	12
	No, never	2	10	12
Total		12	12	24

Table 16: Cross-tabulation of shared passwords and stored passwords

The cross-tabulation results show that in their majority, people who share their passwords with others are the same people who store their passwords written down. This fact indicates, that these specific respondents have very little to no knowledge about basic security measures.

The next two questions provided the users with a hypothetical scenario where the respondents had to choose their according behavior.

Situation: an unknown person sends you an email with an attachment or a hyperlink, what do you do?

75 percent of respondents would choose to refrain from opening an unknown attachment or proceeding to the address provided by a hyperlink. 25 percent would adhere to their curiosity and check out the attachment, even though they do not know who the sender is.

Situation: you receive an email or SMS from your bank with a request to verify your credentials and personal information (e.g. bank account, card number, expiration date etc.):

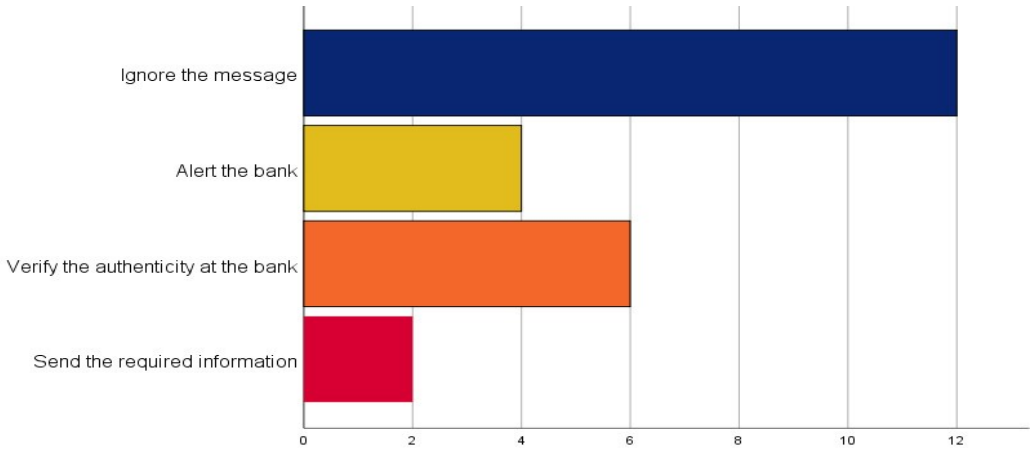


Figure 26: Behavior in case of receiving an unsolicited message from the bank

The majority of respondents who made up 50 percent (12 respondents), answered that they would simply ignore this sort of correspondence from their bank. 25 percent (6 respondents) would ask the bank to confirm the authenticity of the received message while the 16.7 (4 respondents) percent would contact the bank to report the suspicious messages that are being sent in the name of the bank. 8.3 percent (2 respondents) would provide the information requested information without verification of the authenticity.

To understand the respondents' attitude and perception of their own security, they were asked to indicate whether they agree or disagree with the following premises:

	Strongly agree	Agree	Disagree	Strongly disagree
My computer has no value for the hackers, they do not target me	5 22.7%	10 45.5%	5 22.7%	2 9.1%
My computer is secured enough	2 9.5%	9 42.9%	7 33.3%	3 14.3%
I have sufficient knowledge about Information Security and Data protection	2 10%	7 35%	5 25%	6 30%
I would like to receive more information about Information Security	8 38.1%	10 47.6%	0 0%	3 14.3%

Table 17: Survey results

From these answers, it can be concluded, that most of the customers consider themselves safe from an intrusion into their privacy. However, when asked to explain this attitude in a personal conversation it was revealed, that they do not understand the full picture. The fact that they do not store any interesting or valuable (in their opinion) documents and files, does not exclude them from a potential ill-wishers' list; the most valuable asset that can be stolen from a bank customer is the information.

Without a deeper knowledge of potential security issues and pitfalls, it is easy for a person to presume, that they by employing the basic security tools they provide themselves with a sufficient level of security. The respondents' answers indicate that only roughly half of them have this potentially false sense of security. Simultaneously, slightly more than half of them agree that they do not possess enough knowledge and vast majority feel the need of getting more information about security-related topics.

In summary, this short survey provided us with a fix starting point and allowed us to set the bar at a certain level in order to start the evaluation of the SA tool. The results show that majority of respondents do not have enough knowledge about IT security topics; part of them have an imprecise or even false understanding of the issues of information security and privacy.

These findings support the results of an empirical study conducted countrywide in Georgia, that identified a strong need of educating the bank customers and general populous about common topics of information technologies, information security, data protection and privacy.

6.3 The Second Questionnaire Responses - Outcome

Upon completion of the testing, participants were asked to fill out a second questionnaire which consisted of two parts.

6.3.1 Determining the Attitude and Readiness

The survey part of the questionnaire was aimed to evaluate overall usability of the program, the level of its usefulness and relevance for the participants.

	Strongly agree	Agree	Disagree	Strongly disagree
The provided information about IT Security topics was easy to understand	12 50%	10 41.6%	1 4.2%	1 4.2%
The provided information about IT Security topics was interesting	10 41.6%	13 54.2%	1 4.2%	0 0%
I found the information to be useful for me	9 37.5%	12 50%	1 4.2%	2 8.3%
This experience woke my interest to receive an even more in-depth knowledge about this topic	7 29.1%	15 62.5%	1 4.2%	1 4.2%
I was comfortable with the tempo of delivered information	18 75%	5 20.8%	1 4.2%	0 0%
I was satisfied with the method of information delivery	15 62.5%	8 33.3%	1 4.2%	0 0%
I found the messages annoying / the messages distracted me from work	0 0%	2 8.3%	18 75%	4 16.7%
I learned something new every day	8 33.3%	12 50%	3 12.5%	1 4.2%
I felt motivated to log in to my account and learn more	15 62.5%	7 29.1%	1 4.2%	1 4.2%
I found the new educational feature of the electronic banking helpful	10 41.6%	12 50%	2 8.3%	0 0%
I fully understood the intention of the educational tool	20 83.3%	4 16.7%	0 0%	0 0%

Table 18: Heat map of survey results

The heat map of the survey answers clearly shows that majority of respondents have positive experiences with the SA tool. Participants found the provided information easy to understand and easy to follow, which serves a positive reinforcement for learning and motivates and maintains their interest in learning more. No less interesting is the find, that the content was also considered interesting and helpful. Interesting topics engage learners into the process, and the fact that they are determined to use the gained knowledge in the future guarantees that it will not be forgotten right after the learning process ends.

Nearly everyone found the learning pace comfortable. It means that the initial concern that each message should be repeated several times before it could be marked as accomplished, is not justified.

The delivery method was also acceptable to most of the participants. A form of message delivery form is an important part of the program design. If it is not appealing to customers, they might lose interest in the process of learning and might start to think it is bothersome or annoying. This brings us to the following premise: "*I found the messages annoying / the messages distracted me from work*". This question presents an outlier on the heat map, due to it being inverted. Part of the reason for it was to check whether the respondents pay close attention to the survey questions and carefully think their answers through, eliminating thus the "automatic" all-positive answers.

Cumulatively 83.3 percent of the test participants stated learning new information with every message. This fact is not surprising, considering the extremely low level of awareness they had before the interaction with the SA tool; every topic was new and helpful.

22 people (or 91.6 percent) found the idea of an integration of the tool into an eBanking system to be helpful. Moreover, in the conversation afterwards, when asked about the preferred method of learning about Information Security and related topics, 63.6 percent of the respondents answered that they would like to receive this information via technology that saves their time by being integrated with the services they are already using; 27 percent would prefer an option to participate in a seminar or a lecture offered by the experts of the field. Nine percent stated that they would like to learn about information security through a full-scale online course with the program and modules developed for students.

6.3.2 Assessment of the Acquired Knowledge

The second part of the questionnaire consisted of open questions and was aimed to assess the gained knowledge by the participants after the completion of the evaluation process.

Open questions, in this case, allowed participants to formulate their opinions and express themselves in their answers, rather than choosing the answer. This way we got an unambiguous picture of their gained awareness level.

To the question about most interesting messages and topics, the respondents gave mostly clear and well-formed answers. In general, the SA tool includes 40 different messages on five general topics, which were described in chapter 4. Each of these messages was mentioned at least by one of the test participants. It was possible to identify the top 20 subjects which received the majority of votes.

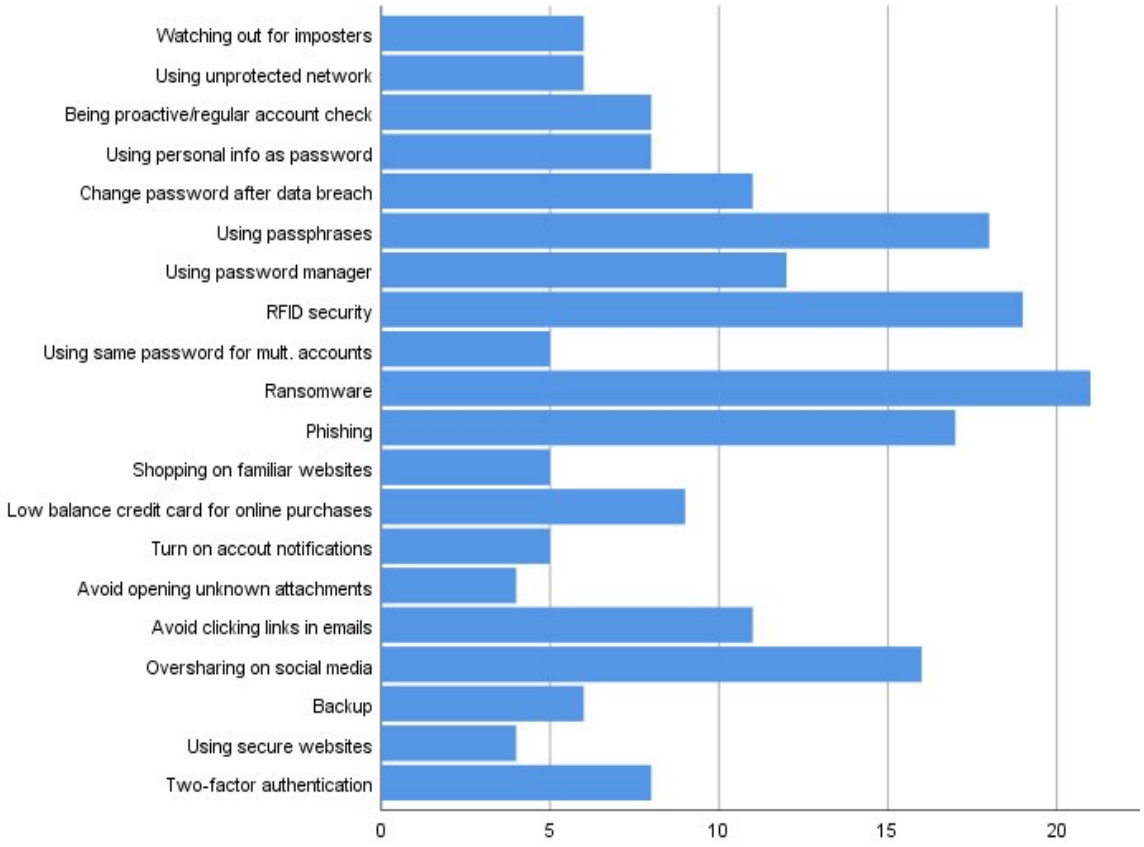


Figure 27: Messages considered most interesting by users

Particularly popular is the most actual topic for 2017 - ransomware. It can be concluded that this increased interest in it is caused by the fact that this subject was discussed quite extensively in the news over the past few months. It is known, that the familiar topics cause the greatest interest. Following the ransomware, is the information about RFID protection, succeeded by strong password creation tips such as passphrase use; the topic of phishing, which according to the first questionnaire was not known to any of the test participants, also turned out to be in top five of most interesting issues. Next comes the message about the rational use of social networks and maximum level of vigilance when sharing any data or information about oneself.

From these answers, it can be concluded that users are mostly interested in large-scale topics, such as cyber-attacks, scamming and social engineering and only then, the aspects of protection from unauthorized use of their data.

Which topic did you consider to be difficult?

Ten out of 24 people left this question unanswered. Another five wrote, that they had no difficulties with any of the message they have received during testing. The rest had several topics they have found to be problematic for them.

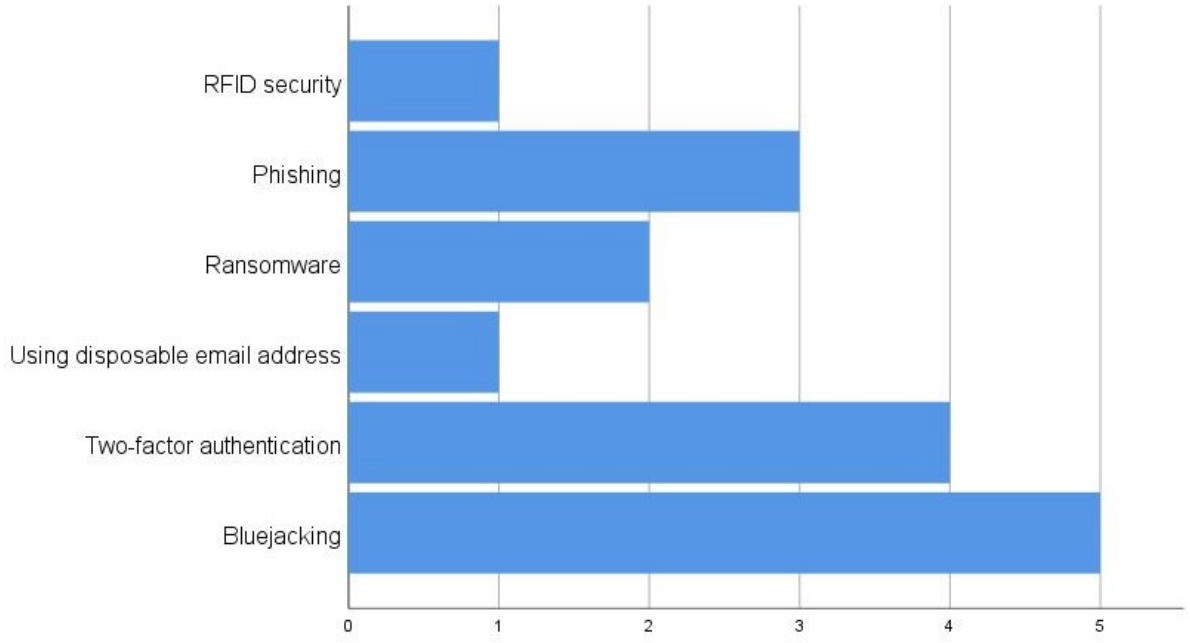


Figure 28: Messages considered difficult by users

Bluejacking was the most misunderstood message. The respondents wrote that they did not quite understand the mechanics of this attack and therefore its severity and counter measures. Two-factor authentication proved to be a difficult topic, for one respondent, because they feel they will not manage the technical part of the process itself; for other three respondents, the notion itself proved to be difficult to understand. The same level of misunderstanding was caused by the notions of phishing, ransomware and RFID security. The difficulty of the message about disposable email address was explained by the technical side of having and managing multiple emails with their corresponding passwords.

Did your views on Information Security change (please describe your stand on the topic)?

From 24 respondents only 18 chose to answer this question. Majority of them underline the newly acquired approach to password creation and management; Three employees stated, that their views on sharing information on social media have changed and they now feel slightly "paranoid" and will avoid sharing all of the information about themselves on the internet in general. Altered views on increased caution with the online transactions and handling unknown emails were mentioned by seven of the test participants. However, arguably a most important turnaround was the changed attitude towards the importance of protecting their sensitive information by five out of 24 participants. They stated, that their previous opinion about the attractiveness of their computer and their data for hackers has changed; meaning that if they did not pay too much attention to protecting their data before, now they have enough understanding about the crucial importance of security for their privacy.

Information Security is an important topic because (please, elaborate):

The corresponding question in the pre-test survey was asking the participants to explain their understanding of the term "Information Security", to which they gave mostly very vague, and plain answers that was based on the wordplay of the term itself.

Unlike those answers, here the respondents formulated their opinion with greater volume and preciseness. From the accuracy and overall correctness of the answers, we can conclude, that majority of the SA tool evaluation participants, when provided the information, could grasp and comprehend it very well. Moreover, the information was able to form a right attitude towards the topic itself.

Do you know what a phishing attack is (please, give a short description)?

None of the 24 questioned employees knew the definition of a phishing attack before testing the prototype. After an interaction with the program for the short evaluation period, three people of 24 could give a correct and elaborate answer to this question; five more gave the approximate description. The rest had to admit, they were not sure what the answer was.

This is certainly not a dramatic turnaround, however taking into consideration the facts that this topic belonged to the highest level and the users did not have too much time for the evaluation process, the results are still meaningful.

Do you know how to avoid email scammers (please, give a short explanation)?

More than half of the respondents (or 16 employees) answered and formulated the correct meaning of scamming and the telltale signs of it. Majority of the right answers fell back to the hypothetical situation given in the first questionnaire and provided the right response to it. Three people gave vague answers to the question, the rest provided no answer.

6.4 Summary

The results of the evaluation show the quality of the tool and its design, idea behind it and the execution.

The purpose of this chapter was to identify indicators of the effectiveness of a support tool in terms of increasing consumer knowledge of information security. The task was to identify the availability of the proposed information in terms of intelligibility, lucidity, ease of understanding, wording and the appropriate volume of delivered information; Additionally, we were determined to figure out the level of usefulness of such a tool for the users.

The attitude and level of knowledge of the test participants were assessed prior to the use of the program. The study showed that consumers had initially a fairly low level of knowledge on this topic. The questions, which carried the purpose of revealing the behavioral habits of the tested employees showed that many of them did not have the elementary skills related to information security.

Whether this was caused by a lack of awareness or a lack of interest was later determined with the help of an informal interview, conducted after the testing was completed; the aim of an interview was to fill in the missing data which could not be collected by the questionnaires only, and with that compile a full picture of the current state of affairs. Nearly in every case when the user's behavior did not meet the established safety standards, this was due to lack of awareness about the correct

behavior in this situation. For example, many of the respondents admitted that they write their passwords on paper or on the phone because they do not see anything dangerous in doing so. Many of them believed that they cannot be a subject of interest for hackers because they do not do anything interesting for them and do not store any documents or information important for malicious intruders on their computer. This attitude towards the security is a clear indicator that the user does not have sufficient knowledge to understand how wrong this assumption might be. More than half of the respondents were surprised by the fact that their personal information can become a key for any hacker who aims to harm not only themselves but also the bank or other organization through them.

After the testing of the program was completed, consumers were asked to fill out another questionnaire where they were given the opportunity to evaluate the operational functionality and helpfulness of the program; they were given an opportunity to formulate answers to the questions on the topic by themselves, without any external help, relying solely on their knowledge.

Certainly, it is pointless to expect a dramatic shift after such a short testing time, however, the result showed itself. The attitude to the program, its functionality and the idea behind it, was accepted positively by all participants with a little exception. This fact provides a positive preliminary assessment of this project and gives an impulse to develop it further and introduce it into the existing CRM system.

In terms of learning, the results were more modest. Nevertheless, they were there. Several participants stood out as outliers; they showed positive changes in their attitude towards security and their understanding of it. It cannot be expected that in a short time people who perceive information at different rates will show the same result. Therefore, the fact that a shift in the right direction occurred in amongst quarter of the participants is already a progress.

One of the next steps will be full-scale testing, in which there will be at least several hundred test cases.

Chapter 7 | Results and Discussion

Education of customers about the safe use of banking systems is one of the major aspects of the security, which is, however, very much disregarded in Georgia. Raising customer awareness about IT security issues is usually narrowed down to formally written security guideline that is placed on the website of the bank. There exists no fundamental education for the new customers, no training for the existing ones. The average Georgian e-Bank consumer is not aware of the most basic IT security issues. This attitude poses a threat to the wholesomeness of the security package provided by the bank, creating, therefore, a backdoor for potential criminal cases, loss of information and risk of compromising the general integrity of the system. From the bank perspective, there is a general assumption, that the customers, who use the e-Banking services, have enough information to help them meet the safety measures from their side. The survey, conducted for the purposes of this thesis, shows that most of the customers do not have sufficient awareness level about functionality or security of the system. A vast majority of customers are convinced, that their bank has absolute security and they, as customers, do not have anything further to do.

An average Georgian bank provides a security information for their customers via bank's website and in form of the occasional intra-system message, that reminds a customer about general security measures. While the information provided on the website is moderately abundant, only the truly determined customers are able to find it. The system messages are addressed directly to customers, however even in this case, they are constantly overlooked and considered to be an annoying waste of time. In fact, only 56% of customers are actually informed about security measures by these ways. Another 29% would choose to overlook such information for various reasons. Only 34% of online banking users feel they have sufficient or partial information, roughly half of whom indicate, that their awareness comes from other sources, rather than a bank.

The empirical study showed the disturbingly low level of awareness about security issues among customers of the Georgian bank. Furthermore, the behavioral characteristics and attitudes towards the aspects security amongst the customers were proved to be conditional and depending on the lack of awareness.

The aim of the literature study was identifying the effective methods for educating the working adults. The main methods for changing customers' attitude and behavior were established; additionally, the technical aspects, necessary for the implementation of the mentioned methods into the program were studied. The studied methods were then applied in the implementation of the prototype, which is designed to realize the relationship with a customer.

After the completion of the design and implementation process, the tool was tested on a group of employees of an NGO. The main task of this testing was to establish the attitude of users to the topic of information security, check their level of knowledge about Information Security and the impact of the program itself on change of attitude and level of knowledge in a positive way.

For an accurate interpretation of the test results, a preliminary questionnaire was conducted for the test group. The questionnaires did not differ much from those that were applied for the empirical study, this was done purposefully; firstly, in order to confirm the correctness of a general picture obtained from the empirical study; on the other hand, to collect and maintain a material for comparison with those results that would have been obtained after carrying out the evaluation.

The results of the preliminary questionnaire practically coincided in general with the full-scale study conducted earlier. This allows us to conclude that the situation in Georgia can be displayed on the cutting edge of potential customers without particularly prominent changes. The results again showed disturbingly low level of customers' awareness of security and accordingly their behavior online, which can pose a potential threat not only for protecting their personal information but it can also create breaches in the security system of a bank through the backdoors.

The testing took place over a limited amount of time and on a limited number of participants, therefore it did not provide enough quantitative material for carrying out a volumetric statistical analysis. Nevertheless, the set goal to reveal the indicators of the accessibility, effectiveness, and helpfulness of the tool, was reached.

A repeated survey showed that working with SA tool, even within a short period of time, gave its positive results. Certainly, it would be unreasonable to expect equal results for every customer. After all, the whole principle of this work is to find an

approach that will provide a continuous education for people who perceive the information provided to them at different rates. Therefore, the conclusion on effectiveness can be made only after long-term and full-scale testing and research.

Despite these limitations, the above results showed impressive positive shifts amongst nearly a quarter of the testing participants. They could answer test questions in the questionnaire, which were intended for trainees who had a high level of knowledge. Given the fact that the same participants did not have knowledge on these issues in the preliminary questionnaire, it can be concluded that they managed to complete the full cycle of the program, completing all five levels successfully, and at the same time they managed to hold on to the acquired knowledge.

This fact proves that the studied methods of teaching, both literary and technical, were implemented correctly and found their confirmation and justification in practice.

7.1 Limitations

The main obstacle to the realization of a full-scale study was the geographical factor. Since the research was aimed at the Georgian target audience, the remote communication was a rather big problem in this case. This can be explained by many factors, the main factor being the inaccessibility of the computer and the Internet for Georgian consumers. This does not always mean physical inaccessibility but implies a lack of knowledge of handling this technology. Although, it is worth noting that physical availability is also often a problem.

The time factor was also important in this case. If there was an opportunity to conduct the study and be present in Georgia, have enough time to conduct full-scale testing, the results would be much more accurate and revealing.

7.2 Future work

The topic of this thesis rather extensive and gives a researcher the opportunity to deploy it in a variety of different directions.

One of the many possible steps is the completion of the program and its integration into the existing CRM system of a bank. The tool makes it possible to supplement it with additional components to fine-tune its work. The tool can be extended with a plug-in that provides a connection to analytical CRM; relying on the actual customers' data stored in the system, the levels of awareness will be determined more clearly with the help of a precise clustering of the bank customers. This is an important factor when it comes to maximum individualization of the delivered information.

The next step in the development may be the implementation of the reward system. The reward system would provide an additional boost for customers to actively participate in the security procedures, and over time such an impulse of active participation will grow into a healthy habit that will accompany the customers everywhere on the Internet.

As an additional step, an introductory course for new e-banking customers can be implemented into the tool. This will establish the initial level of knowledge and provide them with the basic operational and security information; without a base level of knowledge, it is practically impossible to work with electronic banking without making potentially utmost serious mistakes. It will need to be designed in a way, to engage the customers and not scare them off from using the service.

Additionally, it will be reasonable to develop and include customer quizzing at random times. The quiz will check the compliance of the client to the security and their awareness level. Furthermore, customers will be able to validate their knowledge with an option allowing them to upload the IT and information security certificates and diplomas they currently hold.

As already mentioned, the potential of this topic is extensive and it can be developed virtually indefinitely, especially considering the ever-changing nature of Information Security and related topics.

Chapter 8 | Conclusion

The overriding purpose of this study was to create and maintain customer awareness level about IT security issues. To accomplish that goal the prerequisite objectives were reached. An empirical study was conducted in order to identify the overall customer attitude towards and knowledge of Information Security, as well the potential security issues perceived by the customers of Georgian banks. An analysis of the results of the study identified the sensitive areas and common issues with regards to customer education and countrywide general awareness level of an average bank customer. These findings determined the following steps of this work and provided the knowledge on which the program model and subsequent prototype were based. An in-depth literature review, conducted for the purposes of determining the optimal ways for increasing customer awareness level, covered the theoretical material from different fields of science.

To provide for the possibility that an implementation of support tool providing the educational information to the customers could be perceived and measured as a viable component of these theoretical constructs, a process-oriented model was developed. In order to fully encompass the aspects of human-technology interaction and develop an opportunity to test the theoretical findings on the real-life target audience a prototype of a support tool was created.

The testing and evaluation of the prototype showed, that the program is able to embody the theoretical aspects identified from the literature analysis and implemented in a model design. It has proved to be effective in identifying the actual awareness level of a user/customer and determining the necessary level of complexity of the information to be delivered to that customer. Furthermore, the positive feedback received from the test participants indicates at the high level of acceptance of this new technology and justifies the used methods for delivering the information to the customers.

It can be concluded, that this master's thesis succeeded in designing and creating an encouraging learning environment for the customers where they can receive information about Information Security according to their prior knowledge and

preferred learning rate. Consequently, the goal, set in the beginning of this work, was reached.

Bibliography

Books

1. Andress, Amanda (2003): *Surviving security. How to integrate people, process, and technology*. 2nd ed. Boca Raton, FL: Auerbach Publications.
2. Atteslander, Peter; Cromm, Jürgen (2003): *Methoden der empirischen Sozialforschung*. 10., neu bearb. und erw. Aufl., 104. - 111. Tsd. Berlin [u.a.]: De Gruyter (De-Gruyter-Studienbuch).
3. Baron, Robert A.; Byrne, Donn Erwin (1982): *Exploring social psychology*. 2nd ed. Boston: Allyn and Bacon.
4. Baron, Robert A.; Greenberg, Jerald (2008): *Behavior in organizations*. 9th ed. Harlow: Prentice Hall.
5. Clark, Ruth Colvin; Mayer, Richard E. (2011): *E-learning and the science of instruction. Proven guidelines for consumers and designers of multimedia learning*. 3rd ed. San Francisco CA: Pfeiffer.
6. Cohen, Arthur R. (1964): *Attitude change and social influence*. 9th ed. New York: Basic Books (Basic topics in psychology).
7. Elias, John L.; Merriam, Sharan B. (1995): *Philosophical foundations of adult education*. 2nd ed. Malabar, Fla.: Krieger Pub. Co.
8. Gkoutzinis, Apostolos Ath (2014): *Internet Banking and the Law in Europe. Regulation, Financial Integration and Electronic Commerce*. Cambridge: Cambridge University Press.
9. Hovland, Carl Iver; Janis, Irving L.; Kelley, Harold H. (1982, 1953): *Communication and persuasion. Psychological studies of opinion change*. Westport Conn.: Greenwood Press.
10. Kahraman, Erkan (2005): *Evaluating IT security performance with quantifiable metrics*. Universitas Regia Stockholmiensis. Institutionen for Data- och Systemvetenskap, checked on November 2017.
11. King, Brett (2012): *Bank 3.0. Why Banking Is No Longer Somewhere You Go But Something You Do*. New York: Wiley. Available online at http://onlinelibrary.wiley.com/book/10.1002/9781119198918.
12. Lacey, David (2009): *Managing the human factor in information security. How to win over staff and influence business managers*. Hoboken, N.J.
13. Mitnik, Kevin D.; Simon, William L. (2003): *The Art Of Deception. Controlling the Human Element of Security*. 1st ed.: John Wiley & Sons.
14. Pavlovič, Jan (2009): *Process-Oriented Modeling and Infrastructure for Remedial Decision Support System*. Ph.D. Masaryk University. Faculty of Informatics, checked on June 2017.
15. Purtschert, Robert (2005): *Marketing für Verbände und weitere Nonprofit-Organisationen*. 2., erg. und aktualisierte Aufl. Bern: Haupt.
16. Veseli, Ilirjana (2011): *Measuring the Effectiveness of Information Security Awareness Program*. Master's Thesis. Gjøvik University College, Gjøvik, Norway. Department of Computer Science and Media Technology.
17. Zinnbauer, Markus; Eberl, Markus (2002): *Bewertung von CRM-Aktivitäten aus Kundensicht. eine empirische Untersuchung*. Ludwig-Maximilians-Universität München, München, Deutschland. Institut für Unternehmensentwicklung und Organisation.

Journal Articles and Reports

18. Abraham, Sherly; Chengalur-Smith, InduShobha (2010): An overview of social engineering malware. Trends, tactics, and implications. In *Technology in Society* 32 (3), pp. 183–196. DOI: 10.1016/j.techsoc.2010.07.001.

19. Belk, Russel W. (1975): Situational variables and customer behavior. In *The Journal of Consumer Research* vol. 2, pp. 157–164, checked on January 2016.

20. BGLN - Bank Governance Leadership Network (2013): Addressing cybersecurity as a human problem. Viewpoints. With assistance of Inc. Tapestry Networks.

21. Bonanno, Philip (Ed.) (2010): DESIGNING TECHNOLOGY-ENHANCED LEARNING FROM A PROCESS-ORIENTED PERSPECTIVE. ICL2010. Hasselt, Belgium, September 15 -17. University of Malta, checked on June 2017.

22. CapGemini (2016): World Payments Report. With assistance of BNP Paribas.

23. Chen, Injazz J.; Popovich, Karen (2003): Understanding customer relationship management (CRM). In *Business Process Mgmt Journal* Vol. 9 (5), pp. 672–688. DOI: 10.1108/14637150310496758.

24. Chopra, Abhimanyu; Prashar, Abhinav; Saini, Chandresh (2013): Software Project Models. In *INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH* Vol. 1 (4), pp. 135–139.

25. Chris Rygielski, Jyun-Cheng Wang, David C. Yen (2002): Data mining techniques for customer relationship management. In *Technology in Society* Vol. 24, pp. 483–502, checked on January 2016.

26. Clouse, Shawn F.; Evans, Gerald E. (2003): Graduate Business Students Performance with Synchronous and Asynchronous Interaction e-Learning Methods. In *Decision Sciences Journal of Innovative Education* Vol. 1 (2), pp. 181–202. DOI: 10.1111/j.1540-4609.2003.00017.x.

27. Ernovianti, Etri; Nik Mat, Kamariah; Kassim, Umar; Rashid, Rashdan; Shaari, Mai Syaheera Meor (2012): The Usage of Internet Banking Service among Higher Learning Students in Malaysia. In *American Journal of Economics*, pp. 105–108. DOI: 10.5923/j.economics.20120001.24.

28. European Central Bank (2013): Recommendations for the security of internet payments. Final version after public consultation. Frankfurt am Main, Germany.

29. European Law Enforcement Agency (2016): IOCTA 2016. Internet Organized Crime Threat Assesment. With assistance of Rob Wainwright. EUROPOL.

30. Furnell, S. M.; Gennatou, M.; Dowland, P. S. (2002): A prototype tool for information security awareness and training. In *Logistics Information Mngt* Vol. 15 (5/6), pp. 352–357. DOI: 10.1108/09576050210447037, checked on January 2016.

31. Gal, Vladimir (2005): CRMсистемы в банковском бизнесе. In *СТАТЬИ ПАРТНЕРОВ Softline Solutions* (4), pp. 64–68, checked on November 2017.

32. Gerrard, Philip; Barton Cunningham, J.; Devlin, James F. (2006): Why consumers are not using internet banking. A qualitative study. In *Journal of Services Marketing* 20 (3), pp. 160–168. DOI: 10.1108/08876040610665616, checked on May 2016

33. Gribanova; E. B. (2015): Процессно-ориентированное моделирование систем массового обслуживания в Excel. In *Journal of Applied Informatics* Vol. 6 (60), pp. 83–90, checked on September 2017.

34. Guriting, Petrus; Oly Ndubisi, Nelson (2006): Borneo online banking. Evaluating customer perceptions and behavioural intention. In *Management Research News* Vol. 29 (1/2), pp. 6–15. DOI: 10.1108/01409170610645402.

35. Hentea, Mariana; Dhillon, Harpal; Dhillon, Manpreet (2006): Towards Changes in Information Security Education. In *Journal of Information Technology Education* Vol. 5, pp. 221–233. DOI: 10.28945/2954.

36. Hertzum, Morten; Jørgensen, Niels; Nørgaard, Mie (Eds.) (2004): Usable Security and E-Banking. Ease of use vis-a-vis security. In *AJIS* Vol. 11 (2). DOI: 10.3127/ajis.v11i2.124.

37. HILDUM, D. C.; Brown, R. W. (1956): Verbal reinforcement and interviewer bias. In *Journal of abnormal psychology* Vol. 53 (1), pp. 108–111.

38. Hsieh, Nan-Chen (2004): An integrated data mining and behavioral scoring model for analyzing bank customers. In *Expert Systems with Applications* Vol. 27 (4), pp. 623–633. DOI: 10.1016/j.eswa.2004.06.007.

39. Ivanyos, Janos (2009): Implementing COBIT based Process Assessment Model for Evaluating IT Controls. Memolux Ltd.

40. Jahangir, Nadim; Begum, Noorjahan (2008): The role of perceived usefulness, perceived ease of use, security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking. In *African Journal of Business Management* Vol. 2 (1), pp. 32–40. Available online at http://www.academicjournals.org/AJBM, checked on April 2017.

41. Kelman, H. C. (1953): Attitude change as a function of response restriction. In *Human Relations* Vol. 6 (3), pp. 185–214.

42. Kruger, H. A.; Kearney, W. D. (2006): A prototype for assessing information security awareness. In *Computers & Security* Vol. 25 (4), pp. 289–296. DOI: 10.1016/j.cose.2006.02.008.

43. Kumra, Rajeev; Mittal, R. K. (2001): E-CRM in Indian Banks. An Overview. In *Delhi Business Review* Vol. 2 (1), checked on October 2017.

44. LeClair, Jane; Abraham, Sherly; Shih, Lifang (2013): An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. In Michael E. Whitman, Humayun Zafar (Eds.): Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13. the 2013. Kennesaw GA, USA, 12-Oct-13 - 12-Oct-13. New York, New York, USA: ACM Press, pp. 71–78, checked on November 2016.

45. Lee, JinKyu; Bagchi-Sen, Sharmistha; Rao, H. Raghav; Upadhyaya, Shambhu J. (2010): Anatomy of the Information Security Workforce. In *IT Professional* Vol. 12 (1), pp. 14–23. DOI: 10.1109/MITP.2010.23.

46. Mannan, Mohammad, Van Oorschot,P.C. (2008): Security and Usability: The Gap in Real-World Online Banking. DOI: 10.1145/1600176.1600178.

47. Medyawati, Henny; Christiyanti, Marieta; Yunanto, Muhammad (2011): E-Banking Adoprion Analysis using Technology Acceptance Model (TAM): Empirical Study of Bank customers in Bekasi City. In *2011 International Conference on Innovation, Management and Service* Vol. 14, pp. 91–95, checked on January 2016.

48. Metalidou, Efthymia; Marinagi, Catherine; Trivellas, Panagiotis; Eberhagen, Niclas; Skourlas, Christos; Giannakopoulos, Georgios (2014): The Human Factor of Information Security. Unintentional Damage Perspective. In *Procedia - Social and Behavioral Sciences* Vol. 147, pp. 424–428. DOI: 10.1016/j.sbspro.2014.07.133.

49. Milheim, Karen L. (2011): The Role of Adult Education Philosophy in Facilitating the Online Classroom. In *Adult Learning* Vol. 22 (2), pp. 24–31, checked on November 2016.

50. Nasri, Wadie (2011): Factors Influencing the Adoption of Internet Banking in Tunisia. In *IJBM* Vol. 6 (8). DOI: 10.5539/ijbm.v6n8p143.

51. Peppard, Joe (2000): Customer Relationship Management (CRM) in financial services. In *European Management Journal* 18 (3), pp. 312–327. DOI: 10.1016/S0263-2373(00)00013-X.

52. Popova, Viara; Sharpanskykh, Alexei: Process-Oriented Organization Modeling and Analysis. Vrije Universiteit Amsterdam.

53. Rehman, Sana (2012): E-Commerce as a hi-tech tool for creating profitable customer relationships management in banks. In *International Journal of Marketing and Technology* Vol. 2 (8), pp. 289–303.

54. PWC (2017): Strengthening digital society against cyber shocks. Key findings from The Global State of Information Security. Survey 2018. With assistance of Christopher Castelli, Barbara Gabriel, Jon Yates, Philip Booth. Available online at https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf, checked on November 2017.

55. Schlienger, Thomas; Teufel, Stephanie (2003): Information Security Culture. From Analysis to Change (31), pp. 46–52, checked on May 2017.

56. Schoonderwoerd, Ruud: Process-oriented modeling for SOA. A technique for process decomposition. How to specify process models that align business processes with SOA. With assistance of IBM developer Works.

57. Shaw, R. S.; Chen, Charlie C.; Harris, Albert L.; Huang, Hui-Jou (2009): The impact of information richness on information security awareness training effectiveness. In *Computers & Education* Vol. 52 (1), pp. 92–100. DOI: 10.1016/j.compedu.2008.06

58. Siponen, Mikko T. (2000): A conceptual foundation for organizational information security awareness. In *Info Mngmnt & Comp Security* Vol. 8 (1), pp. 31–41. DOI: 10.1108/09685220010371394.

59. Soliman, Hisham S. (2011): Customer Relationship Management and Its Relationship to the Marketing Performance. In *International Journal of Business and Social Science* Vol. 2 (10), checked on September 2017.

60. Stefanou, Constantinos J.; Sarmaniotis, Christos; Stafyla, Amalia (2003): CRM and customer-centric knowledge management. An empirical research. In *Business Process Mgmt Journal* Vol. 9 (5), pp. 617–634. DOI: 10.1108/14637150310496721.

61. Subsorn, P.; Limwiriyakul, S. (2012): A Comparative Analysis of Internet Banking Security in Thailand. A Customer Perspective. In *Procedia Engineering* Vol. 32, pp. 260–272. DOI: 10.1016/j.proeng.2012.01.1266.

62. Sun, Pei-Chen; Tsai, Ray J.; Finger, Glenn; Chen, Yueh-Yang; Yeh, Dowming (2008): What drives a successful e-Learning? An empirical investigation of the critical factors influencing learner satisfaction. In *Computers & Education* Vol. 50 (4), pp. 1183–1202. DOI: 10.1016/j.compedu.2006.11.007.

63. Syed Shan e Raza (2011): Impact of User IT and Internet Skills on Online Banking,. Input to Innovative Banking Strategies. In *INTERNATIONAL JOURNAL OF SOCIAL SCIENCES AND HUMANITY STUDIES* Vol. 3 (1), pp. 477–786.

64. TBC Bank (2015): Annual Report 2015. Investing in Opportunity. Tbilisi, Georgia, checked on May 2017.

65. Thomson, M. E.; Solms, R. von (1998): Information security awareness. Educating your users effectively. In *Information Management & Computer Security* Vol. 6 (4), pp. 167–173. DOI: 10.1108/09685229810227649.

66. Tisdell, Elizabeth J., Waylor, Edward W. (2001): Adult Education Philosophy Informs Practice. In *Adult Learning/Bringing Our Philosophies into Practice*, pp. 6–10, checked on November 2016.

67. University of London (2016): Law and Regulation of Electronic and Internet Banking. SOAS University of London.

68. Wang, Victor C. X.; Sarbo, Linda (2016): Philosophy, Role of Adult Educators, and Learning. In *Journal of Transformative Education* Vol. 2 (3), pp. 204–214. DOI: 10.1177/1541344604265105.

69. Whitman, Michael E.; Zafar, Humayun (Eds.) (2013): Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13. the 2013. Kennesaw GA, USA, 12-Oct-13 - 12-Oct-13. New York, New York, USA: ACM Press.

70. Xu, Mark; Walton, John (2005): Gaining customer knowledge through analytical CRM. In *Industrial Management & Data Systems* Vol. 105 (7), pp. 955–971. DOI: 10.1108/02635570510616139.

71. Zaabi, Khulood Al; Tubaishat, Abdallah (2015): Security Awareness Program for Customers Using Online Banking. In *GSTF J Comput* Vol. 4 (3). DOI: 10.7603/s40601-014-0019-3.

72. Zanoon, Nabeel; Gharaibeh, Natheer (2013): The Impact of Customer Knowledge on the Security of E-Banking. In *International Journal of Computer Science and Security (IJCSS)* Vol. 7 (2), pp. 81–92.

Standards and Regulations

73. Bank of Russia (06.21.2010): ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ. РС БР ИББС2.42010.

74. 2007: IT Governance using COBIT and Val IT:, checked on November 2017.

75. European Network and Information Security Agency, June 2006: How to Raise Information Security Awareness, A User's Guide.

76. European Union (8/30/2014): ASSOCIATION AGREEMENT. L 261. Source: Official Journal of the European Union. In *Official Journal of the European Union* vol. 57. Available online at https://eeas.europa.eu/sites/eeas/files/association_agreement.pdf, checked on May 2017.

77. NIST Special Publication 800-16, April 1998: Information technology security training requirements: a role- and performance-based model. Available online at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf.

78. NIST Special Publication 800-50, October 2003: Building an Information Technology Security Awareness and Training Program. Available online at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf.

79. PCI Data Security Standard (PCI DSS) 1.0, October 2014: Information Supplement: Best Practices for Implementing a Security Awareness Program, checked on January 2016.

Internet Documents

80. Binjo (2016): Electron: от мотивации до публикации. Habrahabr. Available online at https://habrahabr.ru/post/316880/, updated on December 2016, checked on November 2017.

81. Burgess, Thomas F. (2001): Guide to the Design of Questionnaires. A general introduction to the design of questionnaires for survey research. Information Systems Services. University of Leeds. Available online at http://iss.leeds.ac.uk/downloads/top2.pdf, checked on March 2017.

82. CBW - Causasus Business Week: Minimum subsistence level decreased in July 2016. Available at http://cbw.ge/economy/subsistence-minimum-decreased-july-2016/, Checked on April 2017.

83. Centre for Financial and Management Studies, SOAS, University of London (2007): Law & Regulation of Electronic Finance & Internet Banking. Introduction and Overview.

84. DarthGelum (2016): Собираем грабли Electron.js или десктопные JS-приложения на практике. Habrahabr. Available online at https://habrahabr.ru/post/278951/, updated on March 2016, checked on November 2017.

85. Dillon, Andrew (2001): The evaluation of software usability. Edited by W. Karwowski. Encyclopedia of Human Factors and Ergonomics. London: Taylor and Francis. Available online at https://www.ischool.utexas.edu/~adillon/BookChapters/Dillon-evaluation%20of%20software%20usab.htm, checked on December 2017.

86. Forbes Georgia (2015): საარსებო მინიმუმი საქართველოში. Available at http://forbes.ge/blog/121/saarsebo-minimumi-saqarTveloSi , cheched on April 2017.

87. Hebert, Paul (2007): It's a "Sprint" not a "Marathon". Available online at http://incentive-intelligence.typepad.com/incentive_intelligence/2007/06/its_a_sprint_no.html/, updated on 12 June, 2007, checked on September 2017.

88. Howarth, Fran (2014): The Role of Human Error in Successful Security Attacks. With assistance of Security Intelligence. Available online at https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/, updated on 9/2/2014, checked on October 2016.

89. IT Governance Institute (2000): COBIT: Management Guidelines. Available online at http://slideplayer.com/slide/6355136/, checked on October 2015.

90. Infosesinstitute (2015): Session Hijacking Cheat Sheet. Available at http://resources.infosecinstitute.com/session-hijacking-cheat-sheet/#gref, checked on April 2017.

91. Java Exam (Ed.) (2012): Tutorial: Design of Software Architecture for the Java Architect Exam. Available online at https://www.java-forums.org/ocmjea/58406-tutorial-design-software-architecture-java-architect-exam.html, updated on April 2012, checked on November 2017.

92. Meparishvili M. (2010): Electronic Commerce in Georgia. Edited by netgazeti.ge. Available online at http://netgazeti.ge/news/8465/, checked on May 2017.

93. Power Objects (2017): The CRM Book. Plug-Ins. Available online at https://crmbook.powerobjects.com/extending-crm/plug-in-development-and-workflow-extensions/plug-ins/, checked on November 2017.

94. Raab, Andrea: Statistische Auswertungsverfahren mit SPSS. Skript. Fachhochschule Ingolstadt. Available online at http://www.professor-raab.com/files/u1/080530%20SASPSS_Skript_final.pdf, checked on July 2017.

95. Stepanov, Dmitri (2008): Роль CRM-системы в работе с клиентами банка. With assistance of Kari Opdal. Available online at http://www.crm-practice.ru/articles/362/, checked on November 2016.

96. SurveyMonkey: Likert Scales. Available online at https://www.surveymonkey.com/mp/likert-scale/ , checked on May 2017

97. Winnefeld, James A., JR.; Kirchhoff, Christopher; Upton, David M. (2015): Cybersecurity's Human Factor: Lessons from the Pentagon. Harward Business Review. Available online at https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon.

98. Yaroslavceva, Anna (2013): Развитие проекта по фронт-офису в банке «Российский Капитал»: «Легкий» фронт-офис, ДБО и CRM. Interview with Artem Oganesyen.

APPENDIX

Appendix 1: Questionnaire for an Empirical Study

Questionnaire

As part of the Master Thesis from University of Vienna we are conducting a research study of E-Banking use in Georgia and we will appreciate your cooperation in this regard by filling up the questionnaire carefully. We hereby assure you that the information provided by you will be kept confidential and will be used for academic purpose only. Please mark the appropriate boxes with ✖ or ✓.

Personal details

Age group

- ☐ 20 or under
- ☐ 21 - 30
- ☐ 31 - 40
- ☐ 41- 50
- ☐ 51 and over

Highest completed level of education

- ☐ Middle school
- ☐ High school or equivalent
- ☐ Other (please specify _____)
- ☐ Bachelor's degree
- ☐ Master's degree
- ☐ Doctoral degree

Occupation

- ☐ Government job
- ☐ Private job
- ☐ Business
- ☐ Other _____

Social status

- ☐ Student
- ☐ Employed
- ☐ Housewife
- ☐ Retired
- ☐ Unemployed

Income group (Lari p/m)

- ☐ less than 500
- ☐ between 500 and 1000
- ☐ more than 1000

Do you own a PC?

- ☐ Yes
- ☐ No

Do you have access to Internet?

- ☐ Yes
- ☐ No
- ☐ I don't know what that means

Questions

Q1) Do you have an account in a bank?

- ☐ Yes
- ☐ No

Q2) While opening the account, were you or have you been made aware of E-banking services provided by your bank?

- ☐ Yes
- ☐ No (**If NO, go to question #10 directly**).

Q3) if answer to question #2 is YES, which of the following E-banking services are you aware of?

- ☐ Internet Banking
- ☐ Mobile Banking
- ☐ Phone Bank
- ☐ ATM

Q4) Are you using E-banking services?

- ☐ Yes
- ☐ No (**If NO, go to question #10 directly**).

Q5) How convenient do you find accessing your bank online?

- ☐ Easy
- ☐ Normal
- ☐ Difficult

Q6) if answer to question #4 is YES, how frequently do you use each of the following services?

	Every day	Once a week	Several times a week	Several times a month	Once a month	Rarely
Internet banking						
Mobile banking						
Phone banking						
ATM						

Q7) How satisfied are you with E-banking services of your bank?

- ☐ Highly Satisfied
- ☐ Satisfied
- ☐ Neutral
- ☐ Dissatisfied
- ☐ Highly Dissatisfied

Q8) Which of the following factors influence you the most to use E-banking services?

	Strongly	More than average	Average	Less than average	not at all
Availability (24h)					
Ease of use					
Security					
Nearness					
Direct access					
Status symbol					
Friends/Relatives					

Q9) Which of the following benefits accrue to you, while using E-banking services?

- Time saving
- Inexpensive
- Easy processing
- Easy money Transfer
- Any other_____

Q10) Please rate the following reasons enlisted for not using the E-banking services?

	Most important	More than average	Average	Less than average	Least important
No need (Satisfied with traditional banking)					
It seems like a botheration					
Possible security threats (fear of hackers)					
No access to internet/mobile					
Lack of operational knowledge					
Fear of losing money					
Hidden costs					

If any other, please specify_____

Q11) In your opinion what are the potential problems identified in E-banking services?

- Time consuming
- Security issues
- Lack of legal regulations
- Lack of information/awareness
- Internet connectivity issue
- Password forgotten
- Difficulty in claiming false transactions

Q12) Are you aware of/were you informed about IT security issues and measures for the use of E-banking services?

- Yes
- No

Q13) How did you get that information? (you can choose multiple answers)

- Bank website
- Brochure
- Verbally at the branch
- Other non-bank related sources (please specify)

  _____

Q14) If your answer to question #13 includes WEBSITE, how complete did you find the information provided?

- Not complete enough/too general
- Sufficient
- More than enough

Q15) If you use the services, rate your online banking facility on the following criteria using a scale of 1 to 5 (where 1 is very dissatisfied and 5 is very satisfied)

	1	2	3	4	5
Quality of provided information					
Quality and quantity of content					
Security of personal information					

Q16) Did you search for security information on purpose?

- Yes
- No

Q17) If your answer to question #15 was YES, how easy was it to find the information?

- Easy
- Normal
- Complicated
- I tried, but could not find any

Q18) Have you ever received a message on your personal online banking page?

- Yes
- No
- I don't know

Q19) If your answer to question #18 was YES, how informative was it?

- Very general
- Sufficient
- I don't know, I did not read it

Q20) Do you usually take that information into consideration?

- Yes
- No
- Rarely

Q21) if your answer to question #20 was NO, what is the reason for that?

- It is too superficial for me
- It is too complicated for me
- Those messages are annoying
- I do not have time to read messages
- I know better
- I have never noticed message function on my page

Q22) Overall, do you feel you have sufficient knowledge about IT security?

- Yes
- No
- I am not sure

Q23) If your answer to question #4 was YES (you are using E-banking services), would you like to receive useful information and tips about IT security topics in a form that is more suitable to you than current one?

- Yes
- No

Q24) If your answer to question #4 was NO (providing, you are not using E-banking services), would you consider using e-Banking services, provided you will be guided by the system step by step with useful information on operating and managing your e-Banking account, securing your transactions and using the advantages of electronic banking in general?

- Yes
- No

Q25) If your answer to question #4 was YES (providing, you are using E-banking services), how do you end the session after using the services?

- Logout
- Close the tab
- Close the browser
- Leave it open
- I don't know

Q26) Do you share your username, password or telephone code with anyone (e.g. friends, relatives)?

- Yes
- No

Q27) How often do you change your password?

- Every 30 days
- Every other month
- Every 6 months

- ☐ Once a year
- ☐ Whenever it is demanded by the system

Q28) Where do you normally use E-banking services?

- ☐ Only at home
- ☐ Home and workplace
- ☐ Anywhere, including public places

Q29) How often do you clear browser cache and cookies?

- ☐ After every session
- ☐ At the end of the day
- ☐ Every now and then
- ☐ Never
- ☐ I don't know what that means

Q30) Do you have an up-to-date Antivirus software installed on your computer?

- ☐ Yes
- ☐ No
- ☐ I don't know

Remarks:

_____

_____

_____

_____

Place and date:

_____

Thank you for your participation in this survey!

Appendix 2: Evaluation Questionnaire

Questionnaire Part 1

Please fill out the questionnaire as accurately as possible. We hereby assure you that the information provided by you is anonymous and will be used for academic purposes only. Please mark the answers with ☑

Date ____/_____

Section I - eBanking Use

1. Do you use online banking? [6]

☐ Yes	☐ No

2. What browser do you use for online banking?

☐ Chrome	☐ IE	☐ Other
☐ Opera	☐ Firefox	☐ I don't know

3. What operating system do you use for online banking?

☐ Windows	☐ Mac	☐ Linux	☐ I don't know

4. Do you keep your operating system up-to-date ?

☐ Yes	☐ No	☐ I don't know

5. Do you have the anti-virus tools installed on your computers?

☐ Yes	☐ No	☐ I don't know

6. Do you keep your anti-virus tools up-to-date with updates and security patches?

☐ Yes	☐ No	☐ I don't know

7. How frequently do you change your online banking password?

☐ Every month	☐ Every year	☐ Never	☐ I don't know

8. How often do you check your bank statements?

☐ Every day	☐ Every week	☐ Every month	☐ Rarely	☐ Never

9. Did you read your banking agreement, privacy and security policies of your bank?

☐ Yes	☐ No	☐ I don't know	☐ I wasn't provided with those

10. Do you use a unique password (i.e., not related to your other passwords) for online banking?

☐ Yes	☐ No	☐ Sometimes	☐ I don't know

[6] If you do not use eBanking services please skip this section, continue with section II

11. Have you logged into your eBanking account using public computers or public Wi-Fi?

☐ Yes	☐ Never	☐ I don't know

12. When you are finished with an online banking session which of the following do you do promptly:

Sign-out from your bank	☐ Yes	☐ No	☐ I don't know
Clear the browser cache	☐ Yes	☐ No	☐ I don't know
Close the browser	☐ Yes	☐ No	☐ I don't know

Section II - General Security Awareness

1. What do you understand under the term "Information Security"?

2. Do you have any prior knowledge (or experience) about Information Security?

☐ Yes	☐ No	☐ Some	☐ I don't know

3. Do you consider Information Security and Data Protection to be the important aspects of provided online services?

☐ Yes	☐ No

3.1 Why (please fill out in case of either answer)?

4. Do you know what a phishing attack is?

☐ Yes	☐ No

5. Do you know what an email scam is and how to identify one?

☐ Yes, I know what it is	☐ Yes, I can identify it	☐ No

6. Have you ever shared your password with someone else

☐ Yes	☐ Yes, only with relatives	☐ No

7. Do you keep your passwords written down (e.g. on paper or on the phone)?

☐ Yes	☐ No

8. Situation: an unknown person sends you an email with an attachment or a hyperlink, what do you do:

☐	I'll open the attachment / click on the link to see what it is
☐	I will check the senders credentials, maybe it is a colleague sending me something important
☐	I will refrain from opening the unknown file/link in any case
☐	I will mark it as spam

9. Situation: you receive an email or SMS from your bank with a request to verify your credentials and personal information (e.g. bank account, card number, expiration date etc.):

☐	I will send the needed information to the bank
☐	I will call the bank and require whether or not they have sent me the SMS/email
☐	I immediately contact the bank and let them know that someone is sending these SMS/emails from their name
☐	I will ignore the SMS/email

10. Please, indicate your level of agreement to the following:

	Strongly agree	Agree	Disagree	Strongly disagree
My computer has no value for the hackers, they do not target me				
My computer is secured enough				
I have sufficient knowledge about Information Security and Data protection				
I would like to receive more information about Information Security and Data protection				

Thank You for your Participation!

Appendix 3: Evaluation Questionnaire

Questionnaire Part 2

Please fill out the questionnaire as accurately as possible. We hereby assure you that the information provided by you is anonymous and will be used for academic purposes only. Please mark the answers with ☑

Date ____/_____

Please, rate how accurate do you find the following statements:

	Strongly agree	Agree	Disagree	Strongly disagree
The provided information about IT Security topics was easy to understand				
The provided information about IT Security topics was interesting				
I found the information to be useful for me				
This experience woke my interest to receive an even more in-depth knowledge about this topic				
I was comfortable with the tempo of delivered information				
I was satisfied with the method of information delivery				
I found the messages annoying / the messages distracted me from work				
I learned something new every day				
I felt motivated to log in to my account and learn more				
I found the new edu feature of the electronic banking helpful				
I fully understood the intention of the educational tool				

1. Which topics did you find most interesting?

2. Which topic did you consider to be difficult?

3. Which topic, in your opinion, should be covered in more detail?

4. Did your views on Information Security change (please describe your stand on the topic)?

5. Information Security is an important topic because (please, elaborate):

7. Do you know what a phishing attack is (please, give a short description)?

8. Do you know how to avoid email scammers (please, give a short explanation)?

9. Additional remarks:

Thank You for your Participation!

Appendix 4: Security checklist for a major Georgian bank

Electronic banking security information Checklist

Checklist consists of six main security feature categories and is used for comparative* analysis on availability of electronic banking security features and sufficient information about them in Georgian banks.

*Comparative analysis between existing (actual) features and required by the regulation, in this case by the checklist.

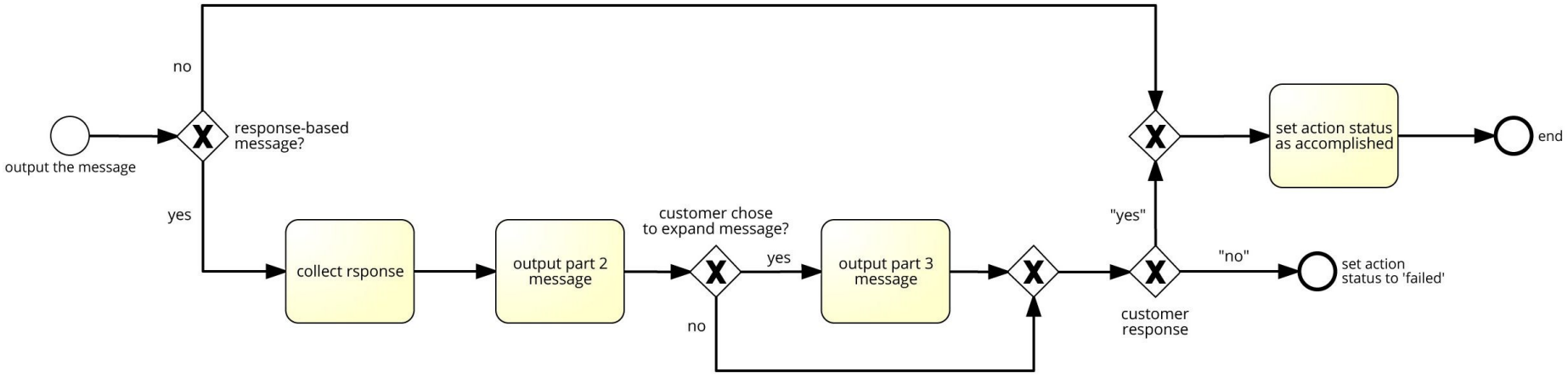
#	Category names	Descriptions
1	General online security and privacy information to the internet banking customers	account aggregation or privacy and confidentiality losses compensation guarantee online/internet banking security information bank security mechanism system
2	Information Technology (IT) assistance, monitoring and support	hotline/helpdesk service availability internet banking transaction monitoring by the banks
3	Software and system requirements and settings information	compatibility “best” with the popular internet browsers internet banking user device system and browser setting requirement free/paid sec
4	Bank site authentication technology	employed encryption and digital certificate technologies
5	User site authentication technology	two-factor authentication for logon and/or for transaction verification available logon requirement, failure limitation and user input type scramble an on-screen input keypad password restriction/requirement transaction verification
6	Internet banking application	automatic timeout feature for inactivity

✓ - Provided
X - Not provided
NI - No information on the Website
R - Provided if/when required

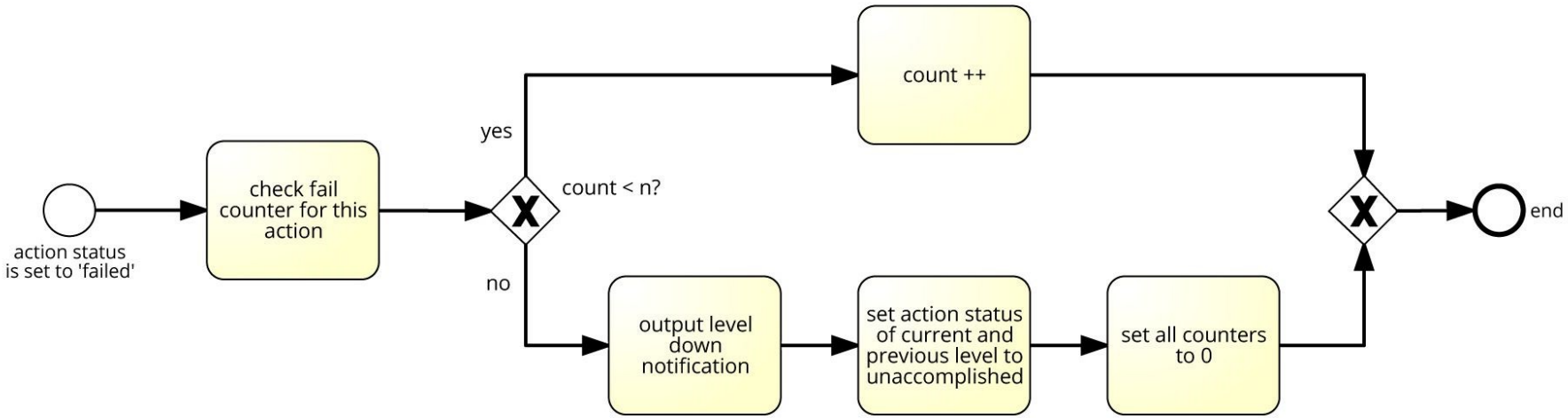
Category	Descriptions	Provided
General online security and privacy information to the internet banking customers	**Account aggregation or privacy and confidentiality**	
	Complied with the national privacy principles and privacy law	NI
	Losses compensation guarantee	
	Responsibility with conditions provided by the bank	✓
	Online banking security information	
	Hoax email, scam, phishing and spyware	✓
	Trojan and virus	✓
	Keylogger	NI
	General online security guidelines	✓
	Security alert/up-to-date issue	NI
	Provides password security tips	✓
	Other security information	✓
	Bank security mechanism system	
	Antivirus protection	NI
	Data encryption	✓
	Firewall	NI
	Intrusion Detection System/alert system	NI
	Other	
Information Technology (IT) assistance, monitoring and support	**Hotline/helpdesk service availability**	
	24/7 customer contact centre by phone	✓
	Not 24/7 customer contact centre by phone	
	Via email	R
	Secured email	X
	FAQ/online support/chat	✓
	E-Banking transaction monitoring by the banks	
	Provides dedicated team and technology	✓
Software and system requirements and settings information	**Compatibility with internet browsers**	NI
	Internet banking user device system and browser setting requirement	NI
Bank site authentication technology	**Employed encryption and digital certificate technologies**	
	SSL encryption	
	Extended validation SSL certificates	(NI) ✓
	Signing Certificate Authority	NI
	Two factor authentication for logon and/or for transaction verification available	
	Token device	X

User site authentication technology	SMS	✓
	Email	R
	Not in use	
	Logon requirement	
	Bank/credit card number/customer ID or email address	✓
	Password/personal code or security number	✓
	Other (e.g. CAPTCHA)	X
	Two-factor authentication	X
	Logon failure limitation	
	Max. (times)	NI
	Logon user input type	
	Keyboard	✓
	Keypad	X
	Scramble an on-screen input keypad	X
	Password restriction/requirement	
	Enforce good password practice	✓
	Password length (in characters)	8
	Combination of letters and numbers	✓
	Combination of upper and lower cases	✓
	Special characters	✓
	Different passwords every time	✓
	Automatically check password strength when creating or changing password	✓
	Transaction verification	
	Some external transactions required token/SMS/email	✓
	Password	X
Internet banking application	**Automatic timeout feature for inactivity**	
	Max. (mins)	NI
	In use but does not specify timeout length	✓
	Logging information	
	Last login	✓
	Activity log	NI
	Notifications/alerts	
	Via email	NI
	System message	NI
	SMS	NI
	No alerts	NI
	Sessions management	NI
	Languages	
	Support other languages	✓

Appendix 5: Message output sub-process (Figure 13, p. 77)



Appendix 6: Fail handling sub-process (Figure 14, p. 78)



Abstract

Information systems security is a crucial aspect of any organization, especially for the financial institutions. The most common eBanking security threats for last five years have been the attacks that target directly the customers and their computers. In Georgia, the IT security systems of a bank are developing and reaching highest international standards. Whereas the notion of customer education is virtually non-existent. Consequently, there arises the need for security awareness amongst eBanking customers, in order to eliminate the vulnerability that is posed by the human factor.

The present master's thesis identifies the existing IT security issues that the customers of electronic banking in Georgia are facing day to day. The research is based on the analysis of results collected by conducting an empirical research. Furthermore, a Security Awareness tool is created for raising and maintaining the high level of IT security awareness among the customers.

This thesis also contains an evaluation of an implemented prototype tool by a small sample group of users. The results of the evaluation indicate at a high level of technology acceptance by the users and effectiveness of the tool for creating and raising their awareness about information security topics.

Zusammenfassung

Sicherheit von Informationssystemen ist ein kritisches Thema für jede Organisation, insbesondere für die Finanzinstitute. Die häufigsten Bedrohungen für die Sicherheit des elektronischen Bankings in den letzten fünf Jahren waren Angriffe, die direkt auf die Kunden und deren Computer abzielten. In Georgien entwickeln sich die IT-Sicherheitssysteme einer Bank und erreichen höchste internationale Standards. Allerdings ist der Begriff der Kundenbildung praktisch nicht existent. Deshalb entsteht der Bedarf nach Sicherheitsbewusstsein bei den Kunden des eBanking, um die Schwachstelle zu beseitigen,die durch den menschlichen Faktor entsteht.

Die vorliegende Masterarbeit identifiziert die bestehenden IT-Sicherheitsprobleme, mit denen die Kunden des Electronic Banking in Georgien täglich konfrontiert werden. Die Forschung basiert auf der Analyse von Ergebnissen, die durch eine empirische Untersuchung gesammelt wurden. Darüber hinaus wird ein Security-Awareness-Tool erstellt, um das Niveau des Sicherheitsbewusstseins der Kunden zu erhöhen und aufrechtzuerhalten.

Diese Arbeit enthält daneben eine Evaluierung des implementierten Prototyps durch eine kleine Zielgruppe von Benutzern. Die Ergebnisse der Evaluierung zeigen ein hohes Maß an Technologieakzeptanz durch die Nutzer und die Wirksamkeit des Tools zur Schaffung und Anhebung des Bewusstseins über Informationssicherheitsthemen.