HÖGSKOLAN SKÖVDE

School of Humanities and Informatics
Dissertation in Computer Science 30hp
Advanced level
Spring term 2009

Using a Chatbot to Prevent Identity Fraud by Social Engineering

Joakim Björnhed

Using a Chatbot to Prevent Identity Fraud By Social Engineering

Submitted by Joakim Björnhed to the University of Skövde as a dissertation towards the degree of M.Sc. by examination and dissertation in the School of Humanities and Informatics.

September 25, 2009

I here by certify that all material in this dissertation which is not my own work has been identified and that no work is included for which a degree has already been conferred on me.

Signature: _____

Supervisor: Marcus Nohlberg

Examiner: Mikael Berndtsson

Using a Chatbot to Prevent Identity Fraud By Social Engineering

Joakim Björnhed

Abstract

Social engineering is a threat that is expanding and threatens organisations existence. A social engineer can get hold of crucial business information that is vital for the organisation and by this threaten the organisation. To prevent successful fraud attempts the organisations need to educate their employees about social engineering fraud techniques that can be used for gaining information. Hence, information security education needs new educational approaches to cope with the threats.

A solution to the problem is the use of an automated chatbot that gives the employees knowledge about a threat that is difficult to spot. To understand if an automated chatbot is a possible solution to educate the users, an investigation about the applicability is conducted. The investigation is based on a survey that compares traditional security education that is based on reading a written informational text and the use of an automated chatbot that simulates a fraud attempt with the purpose to steal an identity. The education with the automated chatbot is to be exposed to an identity fraud attempt in a controlled environment and then get an explanation of what have happened and way.

The automated chatbot is developed with a fraud attempt that looks like a normal market research approach, the market research where conducted with question that gather information that is important for identity thefts.

The result of the investigation shows that it may be possible to use an automated chatbot for educating in social engineering fraud attacks. However there is still a need to solve several major problems before there are possible to make sure the concept is fully feasible.

Key words: Social Engineering, Security Awareness, Chatbots, Information Security.

“Amateurs hack systems, professionals hack people.”

— Bruce Schneier

Acknowledgements

I would first of all thank my supervisor Ph.D. Marcus Nohlberg. For your outstanding supervision and all of your comments during the entire dissertation.

I also want to thank my examiner and program coordinator Ph.D. Mikael Berndtsson. For advises and other good information under the last 3 years.

At last I want to thank the entire School of Humanities and Informatics at University of Skövde for good courses and good teaching.

To all of you.
Keep up the good work!

Joakim Björnhed
September 25, 2009

Contents

Part 1
Preface

1 Introduction

Social engineering attacks are increasingly common for organizations and users. Social engineering attacks can be used for espionage or economic crimes and other crimes as well where the users have knowledge that can be used in a crime. Harl (1997) defines social engineering to be "…art and science of getting people to comply with your wishes". Social engineering can also be explained by have access to personal information that a person shouldn't have access to. Users are subject to social engineering much because of the lack of awareness of the fraud types that are developing. The problem is that users do not have awareness about social engineering fraud attacks (Mitnick & Simon, 2002).

Social engineering frauds are a problem that is not isolated to large countries as USA or United Kingdom. Today, the problem exists also in Sweden, the Swedish newspaper Dagens Nyheter (2008) reported about a homeless man that used a Korean business mans identity to get over expensive electronic equipment. An example from the Guardian (2006) newspaper in United Kingdom reports about an incident that shows how easy it is to gather personal information. A piece of paper, a boarding card, that has been thrown away in a dustbin one a train, could tell the passenger name and travel route. The card could also tell that the passenger had gold standard and the frequently-fly number could be found on the card. By this it was possible to login to the passengers account and get hold of personal information as passport number, date of birth, and nationality.

There may be a need to help organisations to learn about social engineering threats that exist. Traditionally users are referring to use traditional education methods like reading a paper or a book (Mitnick & Simon, 2002). To help users to learn about social engineering attacks and increase their knowledge about social engineering frauds, an educational chatbot will be tested to evaluate if chatbots have a higher educational level than traditional methods. The demonstrator should have the opportunity to give the user a higher awareness about social engineering. Social engineering is a technique that is not commonly discussed, since the area is new and organizations do not want to go public if they have been attacked or simply that they do not know if they have been attacked. An aggressor does not speak out loud if they have done a successful fraud, there is a possibility that the attack can be using the same attack again and that the attacker does not want to get arrested (Mitnick & Simon, 2002). The goal for this thesis is to let the users experience an automated social engineering attack that could be performed, this gives the user a better understanding of social engineering frauds. To measure how efficient a chatbot is compared to other classical security training as reading a written informational text. The target readers of this work is the information security research community and other master students that wants to continue this work and improve it.

Section 2 provides a background about social engineering and how to counteract on fraud attacks, and the background about the use of chatbots in education. In section 3 the research question and objectives of this thesis is presented with the research question also the expected result for the thesis is presented. Section 4 explains the methods that are going to be used in each objective. Section 5 describes how the objectives were realized and the result of the realisation in each objective will be presented. In section 6 gives the result and an analysis of the realized evaluation. Section 7 holds a reflection of the realization and the result and analyzes. Finally, last section presents the conclusions of this thesis and suggestions for future work.

2 Background

This section provides a background of the concepts will be used throughout this thesis. First, in subsection 2.1 presents the concepts in information security. This is followed by subsection 2.2 with a presentation of the concepts for social engineering and a description of social engineering. Subsection 2.3 presents the background for chatbot and how they are used in education at present time. Finally, in subsection 2.3 previous works is presented.

2.1 Information Security

Information security is a basic framework for all security that has a connection to information systems in organizations. The Swedish Standardization of Information Technology (SIS, 2003) defines information security as

> *"Security regarding information resources that are concerning retaining desired confidentiality, integrity, and availability. But also accountability and non-repudiation."*

SIS (2003) also mentions if security measures are compromised it will lead to the information may come into the hand of unauthorized personal, be destroyed, or in other means become inaccessible. To prevent information losses, security is an important part to efficiently prevent information damage or loss.

To describe information security there are several models that can be used for this purpose. Each model has its own strengths and weaknesses for the modelling of information security. The model that is described is the most used models, for information security. The most common model in Sweden is the model by SIS (2003), the model divides information security into technical security and administrative security. Technical security is divided into IT security and physical security. IT security is divided into computer security and communication security. As seen in figure 1.

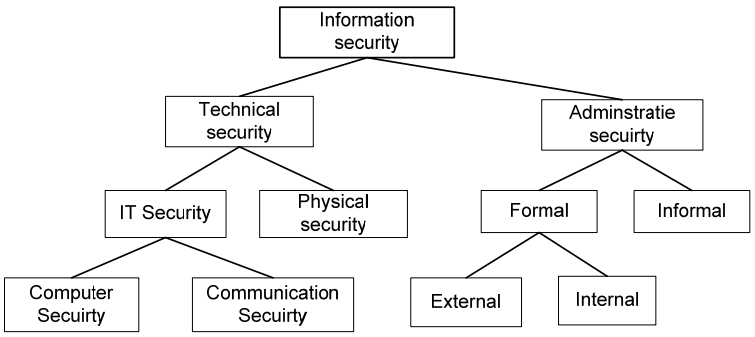


Figure 1 - Extended Information Security model from Åhlfeldt (2008, p. 224).

The model in figure 1 shows all the parts that are need for achieving a satisfactory information security. The model is good for addressing information security in a general purpose, but to use the model for social engineering some problems occur. The model is according to Nohlberg (2008) suboptimal especially in areas of administrative security when trying to apply social engineering to it. Social engineering addresses most of the security measures that the model holds. This makes it apparent that the model isn't created with an intention to cover social engineering (Nohlberg, 2008).

To overcome some of the disadvantages Åhlfeldt et al (2007) developed an improved security model based on SIS (2003). The administrative security has been more

divided so that it can be more usable for non-technical security like socio-organizational security. Åhlfeldt et al (2007) have divided administrative security into formal and informal security, and formal security into external and internal.

2.2 Social engineering

Social engineering is a research area in information security. Social engineering also belongs to other research areas of sociology, psychology, and criminology (Nohlberg, 2008). A social engineer has a very good knowledge about how to read a person's feeling when they are talking to them. This gives importance knowledge to the social engineer if they are going to get the information that they are after (Mitnick & Simon, 2002). To obtain the information the social engineer uses a variety of techniques to obtain information, the techniques are explained in this chapter.

2.2.1 Concepts

The term social engineering is new in the security area, the technique of social engineering is old. Because that threats looks like an ordinary case for the users in the organizations, and that the technical solutions for security is useless to threats in social engineering. All security that is applied is most on the technical side, by implementing firewalls, passwords and other secure increasing products that are more or less based on technology (Mitnick & Simon, 2002; Kajava & Siponen, 1997; Cisco, 2009). Social engineering is an area that not many users have any knowledge about. Social engineering is by Harl (1997) described as "...the art and science of getting people to comply with your wishes". The attacker is using the weakest spots in the human, the mind, when the aggressor is attacking (Harl, 1997; Sasse et al, 2001). Social engineering can be divided into a number of sub areas.

Phishing

Phishing is the most used attack method today. The technique has been around for some time and has been quite successful. The difference between phishing (computer based attack) and social engineering (human based attack) is that phishing is more of a technique that aims against multiple targets (The Swedish Post and Telecom Agency, 2009; The Swedish Police Service, 2009). The goal of phishing is to obtain information through spoofing. This technique can be limited by using techniques that is built in to the web browsers (Microsoft, 2007a).

Spear Phishing

Spear phishing is a focused attack that seems to be coming from people that is known to the receiver and in a context. If the user is in an organisation the spear phishing attack may look like it comes from a source inside the organisation and by this appear genuine (Microsoft, 2007b)

Dumpster diving

Dumpster diving could be a vital part of social engineering or a technique of its own. When the attacker is collecting information before doing the attack, the dumpster could be a gold mine for finding information. By searching through the dumpster and the trash from the organisation, important information can be found, like invoices, and other usable information that can be used in an attack on the organisation (Long, 2008).

Reverse Social Engineering

Reverse engineering happens when the target make the initial approach and offer the attacker the information. As an example, help desk support have access to all information and don't need to ask for password or user ID. A social engineering attack creates a situation, advertises a solution, and provides assistance when requested (Microsoft, 2006; Granger, 2001).

A real world example that can be found in Secret & Lies by Schneier (2000) is a hacker that posted flyers on company bulletin board announcing a new help-desk phone number, his own. The user uses the phone number when there is a problem with the personal computer. When the problem is solved the hacker suggests that the user install a little program that will help to prevent future problems. The program is downloaded from the internet and installed. Now the hacker has access to the user's computer.

Personal approach

A human based approach is the simplest way to perform an attack, the approach is based on human relations and deception (NIST, 2003). With the use of intimidation, persuasion, and assistance the attack can be performed.

> **Intimidation**: By using impersonation of authority to coerce a target to comply with a request.
>
> **Persuasion**: Is the basic method for social engineering, by using impersonation, ingratiation, conformity, diffusion of responsibility, and friendliness it's possible to get information of a user.
>
> **Assistance**: The attacker can by offering help get over information from the user, but it may take some time.

This approaches succeed because that the user believe that the person that they are talking to is truthful (Mitnick & Simon, 2002; Microsoft, 2006).

2.2.2 Attack model

There are several attack methods that can be used. The lowest common denominator between these attack methods is the pattern that is used for a social engineering attack. The pattern is often recognizable and preventable. There are many models that support the concepts of social engineering, the model that has been selected is the conceptual model by Nohlberg & Kowalski (2008).

Nohlberg & Kowalski (2008) have come up with a new conceptual model for the social engineering attack cycle. The new model describes also the defenders and the victim. The attack cycle concerns the behaviour of the attacker that will be used in the attack. In figure 2 the circle shows the attack cycle, the parts of the cycle is presented below.

- *Goal & Plan*: The purpose of the attack and how the attack may be performed.
- *Map & Bond***:** Tries to obtained information need for the attack with traditional social engineering techniques or obtain data from data warehouses. The victim is manipulated into trusting the aggressor with different techniques.
- *Execute*: the aggressor performs an illegal attack like asking the target for the password.
- *Recruit & Cloak*: the aggressor use hiding techniques to hide the attack.

- *Evolve/Regress*: The attacker have two choices, the attack evolves and move into a new stage or the attacker regress after a successful attack (Nohlberg & Kowalski, 2008).

Figure 2 - The attack cycle starts with Goal & Plan (Nohlberg & Kowalski, 2008, p. 5)

2.2.3 Counter measure

The possibility that social engineering attacks works will always be good. Much because of that the people is by nature willing to help and they see them self as team players in the organisation (Schenier, 2000). The counter measures that can be used have the effect that may delay or obstruct an attacker from obtaining the goals. To get an understanding about how the different parts fit into the concept, figure 3 illustrates the concept of counter measure. Examples of counter measures that can be implanted:

Information Security Policy: a policy that ensure a clear direction on what is expected of the users in the organisation. This involves the usage of email, computer systems, telephone, and network (Allen, 2007).

Security Culture: by building a security culture in the organization new users will follow it from the beginning. It also helps the user to be aware of security issues and encouraging a communication between managers, user, and the security personal (Allen, 2007).

Incident Management: When users are discovering a possible attack, users have the opportunity to report the incident to management or a security personal. This improves the organization against attacks (Allen, 2007).

Awareness & Education: Education and awareness training give the users more awareness to threats that exist. By giving the users the ability to have the courage to question a person or a call that comes to the organization, this simple methods can stop an upcoming attack (Allen, 2007).

Operating Procedures: Procedures for creating new passwords that involves verification of the user with secure questions that have to be answered right before any creation. Password is not e-mail to users. This can stop an aggressor from getting access to a network (Allen, 2007).

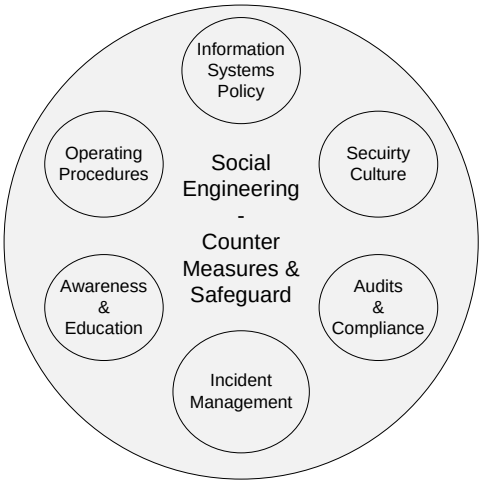


Figure 3 - Counter Measure & Safeguards For Social Engineering (Thaper, 2009, pp.8).

Nohlberg & Kowalski (2008) have constructed a defence cycle. The defence cycle can be seen in figure 4 as the second layer. To be successful in the defence the following must be done.

- *Deter*: A way to reach the goal is be known to report all incidents to the police.
- *Protect*: A solution to reach the goal is to educate the users about the risks & methods used by an aggressor.
- *Detect*: If the users is well-trained there are a possibility to detect when being asked illicit questions.
- *Respond*: If the organization is well-trained, information about occurred attack can increase the awareness for new attacks.
- *Recover*: If the organization has well-designed policies the experience can be used as learning process (Nohlberg & Kowalski, 2008).

There are other counter measures and safeguards that also can be used, much of the counter measures depend on the organization. When the counter measures are operative they have to be maintained, by using regular reviews an acceptable standard is maintained. Other methods to perform a review is to perform a simulated attack, this method is not very common. It depends on the information that can be obtained on the public domain (Allen, 2007).

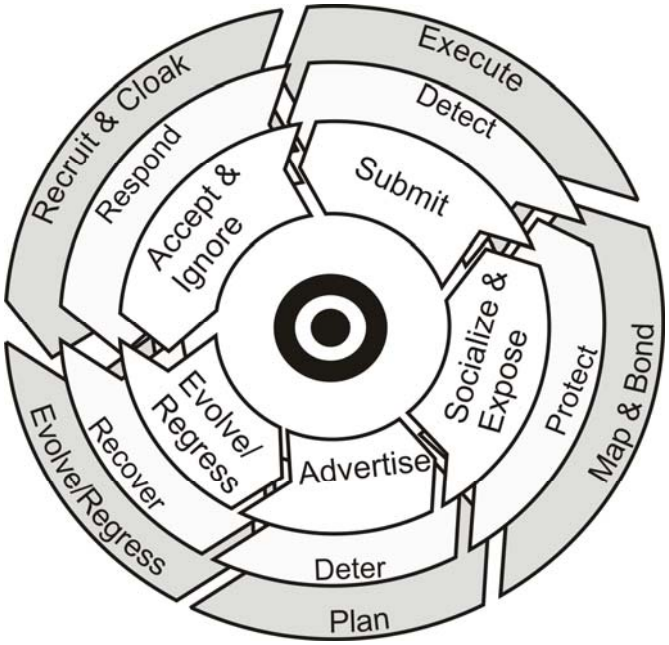


Figure 4 - The Cycle of Deception, starts with Advertise/Deter/Plan

(Nohlberg & Kowalski, 2008, p. 8)

The attack cycle and defence cycle by Nohlberg and Kowalski (2008) also have a victim cycle. All the three cycles' creates the cycle of deception. The victim cycle focuses on the behaviour of the targeted victim. When analysing the attack the victim is often forgotten and the attacker comes into focus, by the usage of the victim cycle the victim becomes more in the focus. By focusing on the victim after the attack, the insight gives an opportunity to understand the attack and to prepare for future attacks (Nohlberg & Kowalski, 2008). The inner circle of figure 4 shows the victim cycle. The part of the cycle is shown below:

- *Advertise*: the victim knowingly or unknowingly makes something of value known and by this becomes a target.
- *Socialize & expo*: when the victim is exposed to an attacker, the victim will be exposed for deception and available for an attack.
- *Submit*: under the attack the victim accepts that it has become hoaxed to reveal information.
- *Accept & ignore*: after the attack the victim accepts that the attack has been executed on tries to believe that non vital information has been exposed. Or the victim ignores the attack or is unknown to the attack.
- *Evolve / regress:* by the knowledge from the attack the victim become harder to victimize in the future. But if the victim just accepts that the attack have happened and don't learn from it will probably be more available for future attacks (Nohlberg & Kowalski, 2008).

The three cycles are merged into one cycle the outcome is a more holistic view that prerequisites of a social engineering attack. If a social engineering attack is to be successful. At least the three first steps have to be successful in the attack for it could be successful. For the attacker to continue the attack fourth and fifth step must be fulfilled (Nohlberg, 2008).

2.3 Chatbot

Chatbots or AI-bots can be used in a variety of way. The more known chats bot in Sweden is IKEA. Ikea's chatbot is a support tool on Ikea's home page and answer questions about the product line at IKEA, but also questions about IKEA's history and homepage. The communication with the IKEA bot is done with keystrokes on the keyboard (IKEA, 2008). Another chatbot that have voice recognition is Telias automated telephone answering system. When calling Telia this system asks after the purpose for the call. The user tells why the call has been made and the system connects the call to the right location. If the system don't recognise what the user says in the phone, it explains that it don't understand the answer and begs the user to repeat what the purpose for the call (Telia, 2009).

2.3.1 Background

ELIZA was the first program that tried to conduct communication with humans. Its creator Joseph Weizenbaum at Massachusetts Institute of Technology (MIT) developed the system on an IBM 7094. The communication with the human was performing through a keyboard and monitor, the input to the computer was written in natural language with normal punctuation and sentence structure. The only charterer that wasn't allowed were the question mark, it interpreted as line delete in the system (Weizenbaum, 1966). From here the development has been going forward to the present AI-bot A.L.I.C.E, stands for Artificial Linguistic Internet Computer Entity. A.L.I.C.E is somewhat a extension to the ELIZA program, but the two chatbots cannot be compared because of the huge amount of knowledge that have been presented to A.L.I.C.E. A.L.I.C.E is an artificial intelligence natural chat robot that is based on Alan M. Turing's experiment from 1950 (Wallace, 2009).

A.L.I.C.E first implementation was conducted in 1995 in the SETL programming language. In 1998 A.L.I.C.E was migrated to the JAVA-platform for platform-independence. At the same time a development of the Artificial Intelligence Markup Language (AIML) programming language for A.L.I.C.E was conducted, AIML is a XML like syntax (Wallace, 2009).

In 1997 a new chatbot was introduced, Jabberwacky. The development began 1988 and it is unique among AI-Chatbots, much because of that it saves all conversations and tries to learn from them. Jabberwacky is a chatbot that tries to simulate natural human chat in an interesting, entertaining and humorous manner (Carpenter, 2009). The only input that Jabberwacky gets is the interaction with users. This means that if the Jabberwacky is exposed to a foreign language it will learn it over time with the interaction by users. By using the contextual pattern matching technique that is the core for the Jabberwacky it can chat with users (Carpenter, 2009).

2.3.2 Chatbots in education

There are several available chatbots to use in educational purposes, but there are only a few that is used for that purpose in education. The few that is in use have the main purpose of language education.

In China teacher often have complaint about lack of time to have conversation with students in English. The solution that have arises is to use a computer based dialogue system to be a role play conversational partner to the students. Because that the system is developed to be a virtual chatting partner, the system only have the most fundamental chatting functions (Jia, 2009). Computer Simulator in Educational

Communication (CSIEC) is a web based tool for the problem above. The system is using a natural language human computer communication system, in the system there are four personalities to chose from. The avatars that can be chosen between is *Christine* a avatar that tells stories, jokes and world news, *Stephan* listens quietly when the users share their experience, *Emina* that is a curious girl that asks all kind of questions that is related from the user input, and *Ingrid* that responses as a comprehensive virtual chatting partner (Jia, 2009).

CLIVE is a chatbot that is used for language learning. The purpose is to help users with limited knowledge in language to learn a new language, CLIVE can understand several languages. To interact with CLIVE the user has to use an instant messaging interface to send text, to receive an answer from Clive it can be both text and voice response. Clive was developed through the MyCyberTwin platform (Zakos & Capper, 2008).

The intelligent tutoring model that is mention by Kerly et al. (2006) was used in a wizard-of-Oz experiment. The users that participated in the experiment negotiated with what they believed were the AI-Chatbot. The negotiating with the chatbot increased the user's interaction (Kerly et al, 2006). When there is interaction with a chatbot in education the student that used the system were more interested to use the system as a search engine to answer assignment question than us it as a conversational tutor (Schumaker et al, 2006). When implementing the ALICE bots the usage of mass knowledge acquisition will improve the domain-specific response (Schumaker et al, 2006).

2.3.3 AIML

Artificial Intelligence Markup Language (AIML) is an easy to learn language for customizing an ALICE bot or creating a bot from scratch. AIML resembles muck like XML, AIML consist of data objects that is made from topics and categories. Categories are the main tags for knowledge in an AIML file. Categorise holds a question (pattern) and a response (template). When using AIML there are some important units to know about (ALICE, 2009).

- <aiml> begins and end an AIML document
- <category> marks "unit of knowledge" in the knowledge base
- <pattern> contain the pattern that matches the users input
- <template> contains the response to user based on the input

There are more than 20 other tags that can be used in the AIML file (Ringate, 2001). An AIML file may look like:

```
<aiml version="1.0">
        <Category>
                <pattern>Hello</pattern>
                <template>Hello there</template>
        </category>
</aiml>
```

There are several ways to extend the AIML file to respond to different inputs. With the usage of wild cards characters like '*' and '_'. By using wild card '*' in the pattern tag, it will ignore what the user have put after 'Hello'. The answer will be Hello there!

```
<aiml version="1.0">
```

```
        <category>
                <pattern>Hello *</pattern>
                <template>Hello there!</template>
        </category>
</aiml>
```

The answer from ALICE will be Hello there! With the usage of '_' in the pattern tag, the result will be the opposite to '*'. Every word before 'Hello' will be ignored.

```
<aiml version="1.0">
        <category>
                <pattern>_ Hello</pattern>
                <template>Hello there!</template>
        </category>
</aiml>
```

When the user inputs 'Well Hello' the answer will be 'Hello There!' (Ringate 2001).

2.4 Previous work

There are some work done in implementing bots in various kinds, but there is a small amount of implementation in the area of using bots as security awareness training resources. Nohlberg & Kowalski (2008) had an initial thought to investigate the use of AI-bots for training in security awareness. Nohlberg & Kowalski (2008) initial thoughts where the research aim for Walentowicz and Mozuraite Araby (2008) master thesis at Royal Institute of Technology. The scope of the thesis was to develop a case study where a chatbot for security information training were used. The focus for Walentowicz and Mozuraite Araby (2008) chatbot was security awareness in a bigger perspective, on all parts of security that is needed in an organization. The user could chat with bot about information security and by this learn of the questions. The chatbot was tested in a large organization with a good result. The bot showed that it was possible to use this educational method to educate the users in security awareness.

Another master thesis by Huber (2009) describes the use of a chatbot as an automated social engineering (ASE) resource in social networking sites, as Facebook. A chatbot can be used as a faster way to collect information about the target than traditional methods like dumpster diving. Huber (2009) also used the Turing test to investigate if the users could make out any differences between the messages sent by Anna (ASE bot) or Julian (real person). Almost immediately, users that were messaging Anna could tell it was an AI-bot. Users that were messaging Julian could almost as fast tell that it were a real person behind the questions that were answered. Because of ethics the test of the ASE-bot could not be tested properly. The experiments that were conducted concluded that the ASE-bot could gather information on predefined information (Huber, 2009).

3 Problem

In this section the problem description for this thesis will be introduced. The research question and objective will be described. Identified delimitations for the thesis are given. Finally the expected results for the thesis are presented.

3.1 Problem domain

Frauds have been around since the dawn of human civilization, and nowadays social engineering frauds on the internet is grooving and here to stay (Jakobsson, 2008). Social engineering attacks can be performed in various kinds. The most known is phishing. Phishing is a mass fraud technique that concentrates upon a large number of targets. Personal social engineering concentrates on only one or few targets. When an aggressor is planning an attack there is not much that can be done to stop the attack. This is because of that the aggressor is very good at manipulating the target to perform the way that the aggressor wants. The unawareness about social engineering attacks is a large threat to the organizations.

Accordingly to Schneier (2000) users in an organisation see them self as team players, this may cause problems. Much because if somebody calls and tells that they have some kind of problem, which is related to the organization, the user will probably try to help the caller to fix the problem in the easiest possible way. This involves answering any questions that the caller may have without critically thinking about whom and why the caller is asking these questions. Mitnick & Simon (2002) believes that this depends on that the human is accommodating and helpful in the genes. A study by Furnell et al (2008) shows that users are extremely vulnerable to online attacks because of the lack of knowledge about threats.

This lack of knowledge is making the users the weakest link in the security chain (Nohlberg, 2008; Mitnick & Simon, 2002). Because that the users are the weakest link there is a need to give the users a possibility to learn about threats. A solution could be computer based training system. By using a computer based training system the users can be exposed to a social engineering attack with the purpose to gather information without to expose vital organizational information. The usage of computer based training is what Mitnick & Simon (2002) argues for, much because of that the training is always available for the users. A computer based training resource that can be used is a chatbot. Walentowicz and Mozuraite Araby (2008) have used a chatbot to get the users to gain knowledge about information security and awareness.

The outcome of Walentowicz and Mozuraite Araby (2008) master thesis was to develop a chatbot for security awareness training. The chatbot had been programmed for general information security knowledge. The chatbot was tested in a leading global telecommunication organization. The result showed that two out of three participants increased their learning experience with the use of a chatbot. Two out of three participants would use a chatbot in the future, the last part of the participants may use a chatbot in the future. By using a chatbot for security awareness training the users knowledge about information security have increased much because of that the resource were available all the time. The accessibility of the chatbot, denoted that the use of the resource weren’t fixed to specific time of the day.

Huber (2009) tested to use an automated chatbot to gather information in a social network, Facebook[1]. When the predefined search criteria were meeting the chatbot started an automated social engineering attack with the purpose to gather important information from the users and later recruit them or cloak the attack. The criteria were in this case members that displayed that they worked in one of five Swedish multinational corporations. By using an automated chatbot the social engineering takes a step further, the use of an automated chatbot makes the possibilities to perform an attack much cheaper according to Huber (2009).

The techniques that have been used by Huber (2009) and Walentowicz and Mozuraite Araby (2008) could also be used in developing information security awareness training systems. A combination of the two master theses gives a solution that can educate company employees in discovering social engineering frauds with the help of an automated chatbot that exposes them to a fraud technique and later gives feedback on what have happened. The automated chatbot could expose the company users to different methods of social engineering fraud attacks and by this the users can obtain knowledge about social engineering.

The use of an automated chatbot that educate in social engineering fraud attacks gives a new level of security education. By giving the users an experience of a social engineering fraud with the purpose of stealing information as an identity. The understanding of the threat can be more accessible than through classic security education. By using an automated chatbot for the education, the training is conducted in a controlled environment where the expose is harmless and the ethics is considered. This gives the advantage that the user gets to understand the threats of social engineering frauds by being exposed to them and by this learn what to look out for in the real world.

This gives the goal to let the users experience an automated social engineering attack that could be performed, this gives the user a better understanding of social engineering frauds. To measure how efficient a chatbot is compared to other classical security training as reading a written informational text. This condition gives the following research question that can be found in section 3.2.

3.2 Research question

How efficient can present and freely/openly accessible AI-bot technology be applied for education about social engineering attacks such as identity theft?

3.3 Objectives

The objectives for achieving the aim in this dissertation are:

- Evaluate various social engineering techniques that can be used in an implementation of a social engineering AI-bot.
- Build a demonstration prototype that can emulate a social engineering attack in an educational context.
- Test and evaluate the prototype through a usability test comparing it with an academic reference group with non specialist security education.

[1] http://www.facebook.com

3.4 Delimitations

A delimitation that is necessary to mention is that there are several social engineering methods that can be used in a social engineering attack. The focus in this thesis will be on the most usable social engineering method. The most suitable method will be implemented in to the prototype. The method that is chosen have to meet the criteria of the limitations of the technology in the chatbot.

The chatbots will use artificial intelligence. The purpose of the thesis is not to make any improvements on the AI technology. The knowledge that is not specific for the thesis is going to be given to the chatbots through pre-programmed files that are available through ALICE.org.

3.5 Expected Result

The expected result is a demonstrational prototype that uses an automated chatbot that can be used for security training with focus on social engineering fraud attacks. The result should show how efficient an automated chatbot is compared to classical security education such as a written informational text.

Part 2
Realization

4 Method

This section describes the methods for each of the identified objectives. Each objective will separately be allocated with a suitable method that suits the objective and a motivation for the chosen method will also be presented. The aim of this work will be achieved by the completion of the objectives and with the method. The following subsection will provide a summary of the selected methods.

4.1 Summary of methods

The research model in figure 5 illustrates how the objectives fit in to the research question. The method for the first objective described in section 4.2 takes up an open interview with a domain expert for starting to identify a attack scenario. The interview is followed by a literature analysis that identifies the scenario for objective two. The second objectives method described in section 4.3 involves implementation with the purpose of realizing the objective. A process to identify a suitable AI-bot for the testing and evaluation of the prototype is also done. Finally, the third objective that is described in section 4.4 involves testing, and evaluation of the prototype and the result. This means that a development model as the waterfall model will be used (Pressman, 2005).

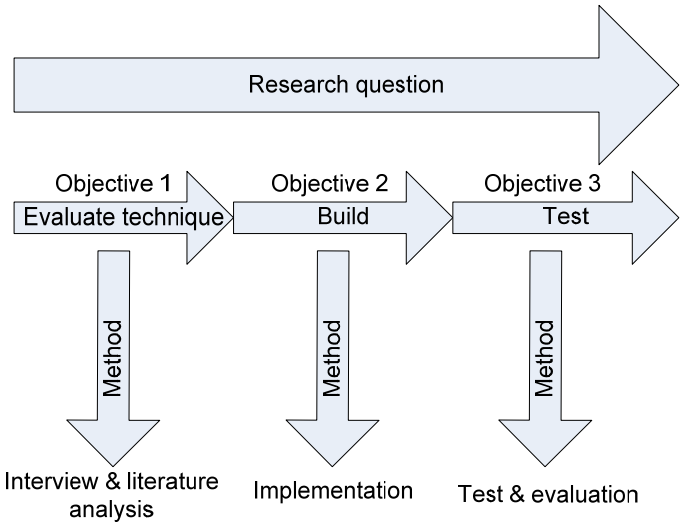


Figure 5 - Research model

4.2 Selecting suitable social engineering attack

The purpose of this objective is to find a suitable attack scenario that can set the foundation of this work. The methods used in this thesis are interview and literature analyses. Both methods are going to be used in this work.

The Interview with the domain expert can emphasize knowledge about social engineering that can be hard to acquire through the literature analysis. When performing interviews it is important to get the interviewee to answer the questions that is important for the thesis. In this thesis an open interview (Berndtsson et al, 2008) is the best interview method available, by using an open interview a more deep going interview can be established on the information that comes from the interviewee. The open interview method makes the interview to evolving and in the end the outcome of the interview has come to an expected result.

To continue to identify a possible scenario with guidance from the information of the interview a literature analyses with a systematic examination on published material is conducted. By using a literature analysis on published material, important parts of social engineering for the scenario will be uncovered. The method can uncover important information that can be used in the work. After selecting a suitable social engineering attack scenario the implementation in the next objective can then be started.

4.3 Implementation of chatbot

The purpose of this objective is to implement the chosen attack scenario that where identified in objective one. To reach the objective it is necessary to implement the knowledge that is acquired in the previous objective. The first thing that has to be done is construction of flow charts that models the flow in the attack scenario. The flow charts model the preferred flow and the show expected and unexpected problems (Pressman, 2005). After the modelling a suitable AI-bot have to be found that full fills the needs for the purpose. In this case it should have a text-to-speech engine that can give the AI-bot a character.

The implementation is going to be conducted into a chatbot and its AIML files. Under the implementation a good software development practice will be followed as coding principles (Pressman, 2005). This objective will result in a finished implemented prototype that will be ready for testing and evaluation in the next objective.

4.4 Evaluate the prototype

The purpose of this objective is to test and evaluate if the prototype fulfils the expected result of the research question. When it comes to testing there are several types of testing that needs to be done to make sure that prototype will work properly before the finale user evaluation can be conducted. When the AIML file have been written it have to be loaded into the chatbot and verified to make sure that the AIML file is working as expected. To verify the AIML file, sequential testing will be conducted to secure that all independent paths within the module have been exercised at least ones (Pressman, 2005). Integration testing will also be used to secure that the external data do not include errors that make behaviour errors (Pressman, 2005).

When the demonstrational prototype has been integration tested and works as expected the evaluation phase is starting. To evaluate how well the prototype is function it will be evaluated against a traditional education method as a written informational text. Group one will use the demonstrational prototype for education in social engineering attack. After finished education the group will answer a survey. Group two will use traditional education method to be educated in social engineering attack. After finished education the group will answer a survey. Group three will not have any access to education but only carry out the survey. The administration of the groups will be automated by the survey application, this ensure that there will be no disequilibrium. The result of the survey will be measured with Qualitative methods as behaviour, attitude, and knowledge (BAK) (Kruger et al, 2006). To investigate the independence and strength of the result a statistical methods as Chi-square test will be used (Preacher, 2001).

5 Realization

This section describes how to identify and implement the chatbot case. Each section describes all of the key parts that are need for implementing the chatbot as an educational prototype.

5.1 Selecting suitable social engineering attack

The goal is to use an automated chatbot to educate the users in social engineering. By using a chatbot there is a possibility to use a social engineering attack to show how it may feel to be attacked. The problem with this is that the chatbot cannot sense any emotions from the victim. By this there is a limitation in what the chatbot can do. A social engineer is often reacting to emotions that a victim sends out under a conversation. This means that the chatbot will have a rather straightforward approach and are limited to an approach that not uses feelings or audible functionality. The chatbot cannot use the act of persuasion when the victim is having problems to decide if they should give out information. The same can be said about the chatbot when it comes to use intimidation. The chatbot cannot come with threats or raise the voice to get the victim to obey the attacker in a believable manner.

Through the limitations a questions rise about how to make a scenario that could fit in to the usage of an automated chatbot.

- What kind of scenario will give the users most understanding about social engineering?
- What scenario is possible to use in an automated chatbot?
- How can the victims of the automated attack learn from the experience?
- What kind of attack can be used considering the ethical conditions?

To answer these questions both an interview and a literature survey had to be done. The interview was conducted with a leading domain expert in information security and social engineering. Only one interview was conducted, because of that there are only one known domain expert available in Sweden and the interview that where conducted more or less become a structured discussion. The purpose with the interview was to obtain information about a feasible case that could be used in the chatbot. The knowledge that is extracted in the structured discussion is the base for the scenario that the chatbot will use in the educational attack on the users. The structured discussion with the domain expert was to be conducted as an open interview that is explained in Berndtsson et al. (2008). The open questions that were used in the structured discussion were:

- Tell me about your background?
- How is Social engineering working?
- If you want to obtain a Swedish citizen identity, what information do you need to obtain to reach the goal?
- Explain how you would obtain the information you want?

The purpose of these questions was to start the structured discussion with the domain expert and gain knowledge that could be used in an educational attack scenario for the chatbot. With the structured discussion as the base for the further research, information about the attack scenario where also found in the information review that

had to be done. The result of these activities can be found in the following sub chapters.

5.1.1 Result of structured discussion with domain expert

The domain expert started with research in information security and social engineering as a Ph.D. student for 7 years ago. At present time the domain expert have a Ph.D. in Computer and Systems Sciences with a focus on Information Security. The purpose of the structured discussion was to gain knowledge about how a attack could be designed for use in Sweden. The literature in the subject is more targeted on other countries in the world with different law systems than Sweden. There are differences in how to design a fraud in Sweden and in for example USA. The law systems are so different that the pattern for the fraud is vital.

This crime involves social engineering and has impacts on the citizens. In general the same problems have not yet started to be the same problems in Sweden. But there are reported cases that the usage of identity thefts has been used. In Sweden there is not a crime to obtain another's persons identity, but to use other persons identity is prohibited by the law. The domain expert explained what information that was needed for an identity theft. Why this information is important in a case like this. The following information is important to do efficient identity thefts:

- Yearly revenue
- Employer
- Where the person lives
- Interest
- What bank is used
- Do the person have credit card
- What kind of credit card
- Shopping behaviour

This information together with information about their economy, an active economy has many transactions in a month. The active economy can also be shown through the use of the credit card. Is the credit card used regular there is a smaller chance that they will discover unknown transactions. Their living conditions have an impact, if they live in a house or in a flat. Is the person living in a flat the post box will be harder to empty than if they live in a house? If they live in a house the post box will probably be outside and unlocked, the needed information then is to know when the postman is delivering the mail.

It is also good to know how a person looks. If there is a need to make an identity card, it will not look good if using a person that have completely different looks than the person that is going to be on the new card. In Sweden most of the information that is needed is available from different administrative authorities. The criminal that want to do this kind of theft do not want to expose what they are after, that means that they will not contact the different authorities to gain the information when it is more efficient to gain all the information at the same time.

5.1.2 Literature survey

After the structured discussion with the domain expert more specific information about identity theft was needed. The information that is gathered is going to be used in the scenario for the chatbot that is going to show how a social engineering attack can be used to make an identity theft. Identity theft can be described in many different

ways depending on what definition that is used. The Home Office Steering Committee in the United Kingdom (Identitytheft.org.uk, 2009) has defined identity theft as:

> *Identity crime: Generic term that describes creation of false identities or committing identity frauds (Identitytheft.org.uk, 2009).*
>
> *False identity: a fictitious or existing identity that has been altered to create a fictitious identity (Identitytheft.org.uk, 2009).*
>
> *Identity theft: When sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual, the victim is alive or dead. Identity theft can result in fraud affecting consumers' personal financial circumstances as well as costing the government and financial services millions of pounds a year (Identitytheft.org.uk, 2009).*
>
> *Identity fraud: Occurs when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of identity fraud (Identitytheft.org.uk, 2009).*

To protect the personal information users have to be observant on changes in the everyday life, is garbage starting to disappear or is contacts from legitimate organizations as survey institutes starting to be frequent. This can be a sign that someone is collecting information about the user. When it comes to protecting personal information from identity thefts there are several small and easy thing to do. The identitytheft.org.uk (2009) has listed these:

- Keep identity and personal information safe.
- Regularly check the personal credit file to see which financial organizations have accessed your financial details. If an unknown confirmation control paper is appearing control appearing, directly control the source of the financial check.
- If living in a property that have an unlocked post-box, where other people can access the mail, be more careful. Credit card suppliers can arrange collection of credit cards or other important mail in post offices.
- If moving, immediately change your address to the new one and get a redirect from the old address to the new one for at least a year.

Personal information is information that directly or indirectly refers to a natural person that is alive (The Swedish Data Inspection Board, 2009):

- Name
- Personal identity number
- Home address
- Personal picture

For an identity theft or social engineer to collect this information, a good cover is what is needed. If the identity theft wants to collect information from a private person the easiest way to do this is by pretending to be calling from an information collecting institute. When a private citizen is getting a call from a person that says representing a

survey institute, the citizen will answer almost any information just because that the person is representing a legitimate organization.

This is especially true in Sweden were the systems is built upon trust. By the Swedish principle of public access to official records makes Sweden to be relatively spared from identity thefts (Expressen, 2009). A normal citizen believes that they are better to spot deceptions than what others are, also do a normal citizen believe that human disasters will not happen to them (Levine, 2003; Nohlberg, 2008).

5.2 Attack scenario

To identify a scenario that can be used in planning a fraud with the help of a chatbot there is some limitations to take into account. The chatbot cannot associate feelings that the user gives under the conversation. This gives a limitation in how the attack can be done. In general there is a human interaction between the attacker and the user. In the interaction between the victim and the attacker, the attacker reacts to the emotions, credence or suspicion, the victim is giving under the interaction. The attackers senses tell how hard to push the victim. If the victim is passive it could be difficult to obtain all of the information that were planned to obtain from the victim, the solution is to back away and not push the victim. That means that personal approaches are hard to rely on.

Other social engineering methods as spear phishing and reversed social engineering also are limited for the use with a chatbot. To get the chatbot to work, normal conversation is the only working method. By asking question and hopefully the user will answer the questions. Another problem that arises is what the fraud should be established on, what is the goal.

To describe the scenario the cycle of deception by Nohlberg & Kowalski (2008) have been used. The phases plan, map & bond, execute, and Recruit & cloak is the vital phases for a successful attack. In the phase with recruit & cloak, with recruit the chatbot try's to recruit a friend to the victim, cloak is used in the way to hide the purpose of the attack until explanation of the purpose. The phase evolve/regress will be used in limited parts for evaluation if the attack scenario that is used is a working scenario. Flow-charts that describes the attack cycle for the subsections can be found in Appendix A.

5.2.1 Plan

To use the chatbot there are several parts that have to be conducted for use it as an automated social engineering bot. The first part is to obtain an account for an A.L.I.C.E. bot where the aiml files can be tested. Later when the aiml files are tested and a ready for use an account at Sitepal[2] where the bot can get an avatar [3]and voice is created. To obtain any information from the users (victim) there is a need to know what kind of information to gather. The different knowledge part is extracted by using reversed engineering on how to protect from identity theft.

i. Define knowledge

[2] http://www.sitepal.com/
[3] http://en.wikipedia.org/wiki/Avatar_(computing)

The questions purpose is to obtain information for making an identity theft and also order new credit cards. Knowledge that is important to obtain from victim:

- Name
    a. Fore name
    b. Middle name
    c. Sure name
- Personal information
    a. Address
    b. Postal code
    c. City
    d. Country
    e. Kind of post-box (drop down or free standing)
    f. Personal identity number
    g. E-mail address
- Bank information
    a. Bank
    b. Internet banking
    c. Bank accounts
    d. Bank savings
    e. credit cards
        i. invoice
        ii. tied to account
    f. member cards
        i. ICA
- Occupation
    a. Position
        i. Student
        ii. worker
    b. Work location
    c. Working hour
    d. Revenue
- Communication
    a. Mobile phone
        i. Manufacturer
        ii. Type
        iii. Service provider
        iv. Number
    b. Regular phone
        i. Number
- Miscellaneous
    a. Computer knowledge
    b. Spoken languages
    c. Favourite book
    d. Favourite movie
    e. Preferred actor
    f. When the post man delivers the daily mail
    g. Living conditions
        i. Flat
        ii. House

ii. **Implement knowledge.**
Implement needed knowledge into AIML file and import base knowledge files.

iii. **Set chat goal & logic**

- Define chat-logic
- Bonding goal (answer the start question about name)

iv. **Set attack to perform**

- Define chat-logic
- Define attack (request information)

v. **Set post attack actions**

- Educate about social engineering
- Cloak (e.g. hide intension)
- Recruit (e.g. friends of the victim)

5.2.2 Map & Bond

Because the purpose of the chatbot is to educate users in social engineering the map & bond phase is a bit special. In ordinary use the victim criteria should be specified in this phase. In the case of this chatbot, the victims will themselves access the chatbot for the education and the target for the chatbot does not have to be specified. The victim that is accessing the chatbot is exposed to the purpose of the chatbot. When the bonding goal is reached the next phase is started.

5.2.3 Execute

Once the victim has answered the first question the chatbot starts the real attack to obtain the wanted information that is specified in the chatbot logic.

5.2.4 Recruit & cloak

Cloak is used to hide the intensions of the attack until the end of the attack when an explanation is delivered. Recruit is used in the end of the attack scenario to recruit new victims to attack. The victim that is already targeted is questioned if they can mention any friends that can be interested to attend in the survey.

5.2.5 Evolve/regress

In this thesis the phase is more for evaluating if the chatbot could obtain any information. For the chatbot to be successful the information required to do an identity theft is gathered completely. If the information gathering is not completed the chatbot have been unsuccessful.

5.3 Development of knowledge

The purpose of the chatbot is to increase the knowledge of social engineering to the users. User is a physical person that can be found in an organization that handles information that is sensitive to the company. The selected language in the chatbot was English. The selected language was the primary language through the survey and demonstrational prototype. These because it should not give any user in the reference group any advantage with the language. In the demonstrational prototype the users

will be exposed to a fraud attack that has as a goal to obtain the information mentioned in section 5.2.1.

The fraud attack is based on several questions like in a survey. To get the user to answer the questions and not hide anything, the use a legitimate organization as a survey institute is going to be used. By telling the user that the questions is coming from a survey institute, the survey in this case is going to be automated, the possibility to get the user to answer the questions increases.

The user will or will not answer the questions that the chatbot is going to ask. When all of the questions have been asked, the chatbot will start to describe what it has done and what kind of information that have been obtained by the chatbot. The purpose of the information will also be presented. The information that is gathered by the chatbot will not be saved in by the chatbot. To increase the functionality for the chatbot an artificial intelligence (AI) mode will be used. The AI will be presented in the .aiml files that are implemented with the knowledge for the chatbot. To give the chatbot more knowledge, default knowledge files are going to be present.

5.3.1 Attack chatbot Emma

The plan for the attack was transferred to flow charts shown in Appendix B. Through the flow charts there was a possibility to get an overview of the attack and how to split up the flowchart in different knowledge files for better performance and easier testing. In Appendix C a list with used aiml files can be found. The files for chatbot contain all the information that is needed to make an attack.

A problem that was discovered was how to get the chatbot to follow the flow that was specified in the flow chart. If the user answered the first question did not mean that the next question came as expected. The answer could be something else, most of the time it was “I have no answer to that”. To solve this problem there were a need to use a new tag <that>, <that> helps the chatbot to remember the last question. In the .aiml file it could look like this:

```
<category>
        <pattern>Hello</pattern>
        <template>Hello my name is Emma, can help you?<template>
</category>

<category>
        <pattern>yes</pattern>
        <that>Hello my name is Emma, can help you?<that>
        <template>What can I help you with?</template>
</category>
```

First the chatbot asks the question ‘Hello my name is Emma, can help you?’, if the user type ‘yes’ and the <that> tag holds the same text string as asked, the answer will be ‘What can I help you with?’. With <this> tag there was a possibility to follow a unique flow.

To increase the interactivity to the knowledge, JavaScript’s where used. By the usage of the JavaScript functionality, there where a possible to present links in the conversations and open links with a click, the link open in a popup windows.

The test was an iterative process. And the test was made on the Pandorabots[4]. Every file was first tested as a standalone file, by inserting a start phrase in every file it was possible to test for errors. When all files were tested as standalone files they were put together and tested with an integration test. The flowcharts were used under the testing to make sure all possibilities were tested. The same was done when the files were put together to one unit.

When all files were running smoothly as expected, other knowledge was put into action to. Now the real problems started, if the user typed 'yes' as answer to a question in the attack files. The answer was overridden by the other knowledge files and the entire flowchart was put out of action. A decision to eliminate all of the original knowledge files was taken. The negative part of this was that the user can not ask other questions as wanted, but if the user answers in other ways as expected in the aiml files the flow will be broken and a "I have no answer to that" will appear. If the flow is broken there is only one way to come back in to the survey questions and that is to start over again.

A problem that arose under the testing were that the text-to-speech engine in the chatbots, the text-to-speech read all of the text in the AMIL file and that meant that the JavaScript also were presented in speech. This could not be solved. To further try to extend the functionality was to get the chatbot to start the conversation with a presentation when the page was accessed the first time. By the usage of AIML that was embedded in the HTML code it was possible to get the chatbot to start the conversation. The existing solution does not work as expected and this extended functionality was abandon.

When a change was made in the aiml file the testing was made one more time to make sure that no errors could be found. When the files were ready to be used in a live environment they were moved to SitePal Artificial intelligence Management Centre (AIMC). At AIMC there are two ways to test the files, as staging bot or as a live bot. Under testing in AIMC a new problem raised, the aiml files could not work in their environment. The problem was the <that> tag was not compatible with the AIMC AI engine.

A quick move back to Pandorabots was made. The choice to use SitePal where the virtual host hade the ability for use of text-to-speech. The same ability could be found in the Pandorabot, but the VH-bot were hosted by SitePal.

The negative part with this is that the Pandorabots server has performance problems and that when staging the bot live, ads will be present in the chatbot web layout. When staging the chatbot the chatbot got the name Emma. Screenshot of chatbot Emma can be found in Appendix D.

5.3.2 Chatbot Maria

The problems that were found in implementing of chatbot Emma could be eliminated in the implementation of chatbot Maria. The chatbot was testes with Pandorabots, the same VH-host were used. Chatbot Maria only has one aiml file, the file name can be seen in Appendix C.

The knowledge that is present in this chatbot is the explanation/education and some key descriptions that are important in social engineering, the explanation/education

[4] http://www.pandorabots.com/botmaster/en/home

text can be found in Appendix F. The keywords are not presented in the Appendix but can be found at wikipedia[5]. A screenshot of chatbot Maria can be seen in Appendix E.

The keyword that is explained in the aiml file is:

- Social engineering
- Social engineer
- Dumpster diving
- Phishing
- Baiting
- Personal approach
- Pretexting
- Reverse engineering
- Spear phishing

5.3.3 Webpage

Under the development of the explanation part for the chatbot Maria, it became clear that it where difficult to understand the explanation of the purpose of the chatbot fraud attempt. To try to solve this problem a webpage where developed as a complement to chatbot Maria's explanation. The webpage was created to display the same information as the chatbot held. The purpose of the webpage is to help the user to an easier understanding of the explanation material. The explanation of the attack is a large amount of text and can be hard to get grip over when displayed in the chatbot tiny window. A webpage that hold the same information as the knowledge file gives the user the possibility to better understand and go back in the text, this was not possible in the chatbot when the chatbot presented the purpose.

5.4 Evaluation of technology

To investigate *"How efficient can present and accessible AI-bot technology be applyed for education about social engineering frauds such as identity theft?"*.

An evaluation with a reference group is initiated. The evaluation will be conduction by using LimeSurvey an open source survey platform. With the use of LimeSurvey the evaluation can be completely automated. The evaluation will have three evaluation groups. The first group will have access to the attack chatbot Emma and then the explaining by chatbot Maria. The second group will have a case that explains about identity theft. The text that is used here comes from CIFAS (2009) and has been edited to better fit in to the purpose. The third group gets no security education through the survey.

All three groups will have a survey with a number of questions that is going to gather vital information for evaluation of the ability to educate with the use of different methods. The questions in the survey are almost the same for all groups, the differences in the questions is because of the educational method each group have. The third group is not having all the questions, questions about the educational method is not present here. The questions are divided up into blocks with different purpose. The first three blocks in the survey for the chatbot and paper case comes before the education. To balance the respondents' participation a PHP script were used to allocate to one of the three surveys.

[5] http://www.wikipedia.org/

To evaluate the results from the survey a qualitative methods will be used for analyzing the data. For this have behaviour, attitude, and knowledge (BAK) method have been used (Kruger et al, 2006). To increase the statistical value of the questions Chi-Square test (c^2 (p)) have been used on questions that have a result that needs to be strenged. In formula 1 the formula for Chi-Square is presented.

$$X^2 = \sum \frac{(O - E)^2}{E}$$

Formula 1- Chi-Square test

O is the observed frequency and *E* is the expected frequency. Questions that have a Chi-Square *p*-value have a better analysis, other questions only have basic statistical analysis. To make the Chi-Square calculations a web based tool has been used (Preacher, 2001).

5.4.1 Pilot study

To evaluate if the education and survey that hade been developed could be used, a pilot study were conducted. The pilot study's purpose were to control if the education where usable and understandable for the participants. The survey questions where evaluated. The pilot study where first conducted on a preferred reference group that were assumed to have normal computer skills and non-security education. An assumed group to represent an ordinary user in the society was selected; the group for this were teacher students because of that the education do not include any higher computer education and non security education. The selected group contained 220 teacher students. Under the begging of the pilot study it became clear that the reference group was not large enough because that they did not do the survey. To get the pilot study usable more participants where added, in this case not the preferred reference group where added. The new invited where 290 nursing students and 154 students from business administration and economics. These students have various levels of computer skills and security educations. The nursing students have a higher level of security thinking because of the patient security thinking that is a large part of there education.

The pilot study could not proper show that the survey where excellent because of the low answer rate, of 664 invited participants only 45 participants answered. However the pilot study showed that the most important survey groups' education and survey did take too long to conduct. Other problems that also where exposed was that not all questions where needed or that they came on the wrong place in the survey. In the comments from the participants it became clear that it was not so good to have the education in the beginning, comments on this were it may frighten participants away from the evaluation. This problems where later addressed and solved to the main evaluation.

5.4.2 Main study

After the pilot study some questions were deleted and other questions were moved to a better location in the survey. The move of the questions resulted in that the measurements of the survey became better. The education with the fraud attempt and the written informational text were moved from the beginning of the survey to after

question block 3. By this the more basic questions of the survey could be conducted without any impact of the coming education. Now could also a more measurable value of the educational value be analyzed by having behaviour questions before and after the education. In Appendix G there are a table that illustrates how the questions are positioned to each other. The questions can be found in Appendix H together with the results.

As before the preferred references group is a group that has normal computer skills and non-security education, this reference group should be as close to an average user in the society.

The evaluation group that where used come from a higher academic education course, in this casa a jurisprudence course. The group were selected because of the variety of backgrounds. The participants are students with different educations or employees that come from different organizations. The variety in the participants' background gives the evaluation a larger believability.

Approximately 400 participants were invited to the survey, 291 of the invited did participate in the survey, and this is approximately 73% of the invited. When the students were invented to the survey, an invitation was sent out through the educational channels for the course, in this case through an online educational system as WebCT. The invitation was sent out in Swedish and with a web link to the survey. With the use of a PHP script the students were allocated to one of the three surveys. This was done for balancing the responses in an even stream to the evaluations.

5.5 Chapter summary

- Conversation impossible to start with out interaction with user.
- Broken flow and continue survey impossible whit out a survey restart.
- The survey group that used the chatbot hade a survey that took more than one hour.

6 Result & analysis

In the following chapter results from the survey will be presented and analyzed. The result from the different parts will be presented first as standalone and then if possible as a group. Some questions is specific for the evaluation group and will marked with which evaluation group the result is coming from. All data that have been gathered can be found in an aggregated form in Appendix H. Qualitative methods will be used for analyzing the data. The responses from the survey, Group 1, used a chatbot for education, Group 2 used a traditional educational method by reading a written informational text, and Group 3 were the control group with no security education and therefore no result is from group 3 is visible in questions where security education is taking in to account.

6.1 Behaviour, attitude, knowledge

To make a qualitative structure of the survey result, behaviour, attitude, and knowledge (BAK) (Kruger et al, 2006) was used.

6.1.1 Behaviour

The questions that are presented here are selected to represent the questions that measure the behaviour of the respondents.

> **Question 12 (Appendix H):** To what extent do you share your computer password with:
>
> - Family
> - Friends
> - Partner
> - Colleagues
> - Acquaintance
> - Some you do not know.

In all three groups the majority do not share their password with colleagues, acquaintance, or with some one they do not know. If there is a need to share the password it will be changed promptly after sharing. Family and partner will more often have access to passwords than friends.

6.1.2 Attitude

The question that is presented here is selected to represent the questions that measure the attitude of the respondents.

> **Question 16 (Appendix H):** Would you reveal sensitive information in the following circumstances:
>
> 1. Someone claims to be calling from your bank and asks questions about your bank accounts?
> 2. Someone claims to be calling from your bank and asks questions about your bank passwords?
> 3. An old friend contacts you and asks if he/she can use your bank account?
> 4. A survey company contacts you and wants you to reveal your personal identity number?
> 5. A person from the social authority contacts you and asks if any of your pupils have parents that are using drugs?

In the first sub question there is almost a complete consensus that the respondents will not leave out information to the caller. In the second sub question there is a larger consensus that the information should not be leaved out. The same can be said about sub question three. In the fourth sub question, all three groups will a large number of participants leave out information to the caller. In the fifth sub question, all three groups have a very high rate of saying no to the request.

> **Question 8 and 17 (Appendix H):** Do you think you can recognize a fraud if you are exposed to it?

Question 8 where asked before the education and question 17 after educations. In the answers to question 8, it shows that the participants believe that they most certainly can discover a fraud if they are exposed to one. In question 17, after the education for the chatbot and the written informational text group, they are not so certain to recognise a fraud. The majority believes that they think that they can recognise a fraud. Some of the participants believe after the education that the chances to discover the fraud are small.

6.1.3 Knowledge

The question that is presented here is selected to represent the questions that test the knowledge of the respondents.

> **Question 5 (Appendix H):** Have you got any security education or training prior to this survey? If yes, from where?

From all three groups there are 251 (86%) of the 291 respondents had no security education or training prior to the test. The remaining 40 (14%) participants of the respondents that hade any kind of security education or training have got it from there work.

> **Question 11 (Appendix H):** To What extent do you keep your computer password private from:
>
> - Family
> - Friends
> - Partner
> - Colleagues
> - Acquaintance
> - Some you do not know.

The major part of the respondents in all three groups never share there passwords with family, if they share their password with the family they change the password after sharing. When comparing with keeping the password hidden from friends the majority keeps it hidden, for the partner the password is not a secret, the respondents more frequently share the password with them. Colleagues, acquaintance, and strangers are kept unaware of the respondents passwords

> **Question 15 (Appendix H):** In a security context, do you know what Social Engineering is?

In all three-survey groups there are 57 (19%) respondents of 291 that know what social engineering is, the respondents that know what social engineering are is almost the same in all three groups. The majority do not know what social engineering is. The calculation with Chi-square gives a p-value of 0.7695, this indicates that the majority of the respondents do not know what social engineering is.

6.2 Method questions

In this section questions about the used educational method will be analyzed. To increase the statistical value of the questions Chi-Square test (c^2 (p)) have been used on important questions.

6.2.1 Educational usefulness

> **Question 24 (Appendix H):** Do you think this education has been useful for you?

61 (62%) of the 97 respondents in Group 1 (chatbot) and 68 (70%) of the 97 respondents in Group 2 (a written informational text) believe that the education has been good for them. The p-value is 0,2869 and tells that both educational methods are good.

6.2.2 Educational method

> **Question 25 (Appendix H):** Do you think this kind of education method is good?

By the respondents the educational methods with the chatbot are good to use. 63 (65%) of the 97 respondents in the chatbot group and 49 (51%) of the 97 respondents in a written informational text group think that the educational method is good. 48 (49%) of the respondents in a written informational text group believe their educational method is not good. A comment tells that the educational concept is good. The p-value is 0,0478, which show that the assumed statement that the chatbot is a good educational method.

> **Question 26 chatbot (Appendix H):** Is the chatbot a better education method than reading a fraud case from a paper?
>
> **Question 26 a written informational text (Appendix H):** Is reading a paper with a fraud case a better educational method than using interactive learning?

By the results from the group with the chatbot, 68 (70%) of the 97 respondents believe that use of a chatbot is more educational than reading the same information from a paper. 55 (57%) of the 97 respondents in the group with the written informational text do not believe that reading a case from a paper is enough educational. The Chi-square p-value is 0,0001, and that shows that the Chabot is a better educational method than the written informational text.

> **Question 29 chatbot (Appendix H):** Do you think that the educational method by using a chatbot is the most useful method for educational purposes?
>
> **Question 29 a written informational text (Appendix H):** Do you think that the educational method by reading a fraud case is the most useful method for education?

52 (57%) of the 97 respondents from the group with the chatbot tell that the chatbot is the most useful educational method. As a contrast the group with a written informational text, 53 (54%) of the 97 respondents believe that reading a case is the most useful educational method. The Chi-square p-value is 0,884 and that tells that the chatbot is not better than a written informational text method in education.

> **Question 30 (Appendix H):** Is interactive learning a possible educational approach for identifying thefts?

68 (70%) of the 97 respondents in the group with a written informational text believes that the usage of another learning method than reading about a scenario is better. 54 (55%) of the 97 respondents in the group that used the chatbot believes that the use of a chatbot is the preferred interactive learning method. The p-value is 0,037 and shows that it is better to use another educational method than reading.

6.2.3 Likeability

> **Question 34 chatbot (Appendix H):** How useful would you say the chatbot was/is?
>
> **Question 34 a written informational text (Appendix H):** How useful would you say a written informational text was/is?

56 (58%) of the 97 respondents in the chatbot group believe that it can be useful to use a chatbot, and 46 (38%) of the 97 respondents in a written informational text group also believe that the method can be useful. In the chatbot group 41 (42%) and in the written informational text 51 (58%) of the participants did not believe that the method is good. The p-value is 0,5085 and that shows nothing conclusive.

> **Question 37 chatbot (Appendix H):** Do you feel that the chatbot had a positive effect on your learning experience?
>
> **Question 35 a written informational text (Appendix H):** Do you feel that this paper had a positive effect on your learning experience?

56 (58%) of the 97 respondents in the chatbot group believe that their learning experience is good. In the written informational text group 53 (54%) of the 97 respondents feels that their learning experience is positive. The p-value is 0,879 and that shows that there is no difference between the two educational methods.

6.2.4 Chatbot questions

> **Question 36 chatbot (Appendix H):** Do you feel that you have gained more knowledge by interacting with a chatbot, than by reading a fraud case?

54 (56%) of the 97 respondents feel that their knowledge has increased by the chatbot. The remaining 48 (44%) respondents do not feel that their knowledge has increased by using the chatbot.

> **Question 38 chatbot (Appendix H):** Do you feel that the chatbot simulation of an identity theft is believable?

51 (53%) of the 97 respondents believe that the scenario for the chatbot was believable. The remaining 49 (47%) disagree to the statement.

6.3 Survey summary

The merged result from the survey shows that it cannot be determined conclusively that the chatbot is a better educational method than reading an informational text. However the result shows that the use of a chatbot as an educational method is good and traditional education as reading an informational text is still a strong competitor to the chatbot.

The respondents' use of the chatbot has shown it exists a possibility for the educational method to be good. The respondents believe that there capacity to spot a theft attacks have increased. The respondents also believe that the use of a chatbot is better than traditional education

The question about security training prior to the survey showed that few of the respondents in the survey hade security training prior to this education. The education or training that the respondents' hade gotten was either from their work. The respondents hide their passwords from colleagues, acquaintances, and unknown persons. If there is a need to share their password with anyone in their proximity like family, partner, or friends a change of password is made promptly.

When it comes to revealing information the respondents in the chatbot group believes that they will not reveal information if asked, the other groups is not so certain about not revealing information. When it comes to sharing passwords it is more likely that a dependent person is getting the password, than it is that a remote relative to the respondent is getting a password.

The main group of the respondents is female in an age of 18 to 29 years old. The respondents use internet several times a day, with an approximate time of one to five hour a day. The majority is concerned about their security when using the internet, approximately half of the respondents also use some kind of social networking site to stay in contact with acquaintances and friends.

Respondents believe that after the education that they will be more conservative with leaving out information, but they believe that they will not be more conscious after education.

The educational methods that were used, is by the respondents roughly equal to use. The educational method that has been the best for the respondents is the use of chatbot, by this the respondents believe that the use of a chatbot is better than using traditional methods. But the respondents in the chatbot group believe that the chatbot is the most useful educational method, and the group using traditional educational method believes that a written informational text is better.

Interactive learning is by the chatbot and a written informational text group a form of education that is possible to use for identifying thefts, but the respondents in the chatbot group do not believe that the education have prepared them to prevent identity theft. The usefulness of the chatbot is better than by traditional learning. This means that the use of a chatbot in the form in the survey is good enough for education in identity theft.

The result from the control group is almost the same as from the other groups. The control groups result is only presented with the other groups where there is a value to use and that is from questions that did not need any security education. In this case the value is presented when behaviour, attitude, and knowledge (BAK) (Kruger et al, 2006) was used.

6.4 Chapter summary

- The respondents in the chatbot group and in the written informational text group believe that the use of a chatbot is more educational than other methods.
- The learning experience for both chatbot and a written informational text group is not as good as hoped for.
- The respondents in the chatbot group and in the written informational text group believe to some degree that interactive learning is a good educational method.
- The control group shows almost the same values as the other groups.

Part 3
Conclusion

7 Reflection

The hypothesis for this master thesis is: *How efficient is present and accessible AI-bot technology be applied for education about social engineering frauds such as identity theft*. After the realization of the thesis it was discovered that it may be possible to use a chatbot to give knowledge about identity frauds and the use of social engineering. By the different survey groups, chatbot group, and the written informational text group, the result shows that the chatbot is useful. But there are functions in the chatbot that can be improved and these functions may be the parts that have made some of the respondents not fully positive to use the chatbot. The Chi-square p-value result from question 26 tells that the use of a chatbot is more educational than reading the same information from a paper.

However in question 29 in the chatbot group only 54% believes that the chatbot is the best educational method. Which shows that the chatbot may have some flaws that have to be adjusted before it can be considered to be a much more educational method, but this also depends on which learning style that the respondents prefer in their learning. When comparing the result with the group that read a written informational text, the result shows that the group believes that reading a written informational text is the most educational method. The problem with this questions is that the survey group with a written informational text have nothing to compare with, this problem where discovered after the survey hade been conducted.

The length of the education and survey is not optimal for this kind of study, for the chatbot group the education takes approximately 30 minutes and the survey that takes more then 30 minutes to go through. This means that the education and survey takes to long time to finish and this can affect the result in a negative way for the chatbot evaluation.

Another problem with the use of the chatbot that could be considered to be difficult, is if a respondent answered in a wrong way that were not expected the chatbot answered “I have no answer to that”. To come back to the survey the only possible way was to start all over again, this can have happen for some of the participants. When reading the statistics over how many that have started and ended the education with the chatbot a guess is that some of the respondents got the problem stated above and because of this choose to quit the survey.

When comparing the material in the two different educations, the materials for the written informational text group were of a higher educational standard and did come from a British governmental home page about identity thefts. The material on this page is developed by the British governmental agencies who are experts about identity theft, the text holds a very high educational level and has been written in away to be easily understood for everyone. The material in the chatbot does not have the same high standard as for a written informational text group. These differences of the material can have a large impact on how the respondents will learn the material and answer the questions in the survey.

The chatbot functionality problems can be divided into two groups. The attack scenario and the underlying technology to perform the attack. These two parts follow each other hand in hand through the whole scenario. Under the development of the attack scenario the expectations were that the chatbot could chat about anything that the users wanted to chat about, and at the same time it tried to gather information. The gathering of information is rather important and the initial idée were that the

participants should not understand that information was gathered under the chat. This initial idée was not possible to realize because that the ALICE bots cannot be controlled in sufficient manner. The ALICE bots AI can only ask questions that are either randomized from the different aiml files or through the chat logic that tries to detect what the user wants to chat about. If there are several questions in an aiml file it will hopefully ask one of them to the user. When there are several aiml files the possibility to get the chatbot to ask all the questions that is need is out of scope. If the user answered a question with for example a number, the logic automatically searched through the aiml files and answered with the first possible hit that could be found in the aiml file. This meant that it never were the expected answer from the chatbot. When this happened it was impossible to continue the fraud attempt that was specified. The only way to continue was to start over again.

The conclusion is that it is very hard to get the chatbot to use custom made knowledge files before the predefined knowledge files. By the usage of the custom files the chatbot can only answer “I have no answer to that” when the user is typing in something that is not predefined as an answer in the custom files.

Another problem that was found was that is not possible to get the chatbot to start the fraud without the initial interaction from a user. The user hade to start the chat by typing hello to the chatbot, when this was done the chatbot could perform what is designed for. The solution that was found on the problem were to include a aiml block in the beginning of the html page were the chatbot were going to be hosted, the meaning with this solution was that when the html page were loaded the aiml file should be loaded in to the chatbot. The solution did not work, this gave some limitations on how to use the chatbot.

Under analyzis of the survey results, it was discovered that to get a good result a full-scale fraud attack after some time was needed. A later fraud attack was needed to analyse how well the respondents have gained the knowledge from the education. This is however impossible because of the ethical considerations that have to be taken into account and the time constraints in this thesis.

As a summery of the reflection is that the there are many unknown variables that have an effect on the outcome on the result in the evaluation. But as the analysis and result show is that it may be possible to use a chatbot as the hypothesis suggested. To get the chatbot to be considered a much better educational method than the use of a traditional educational method as reading an informational text, the chatbot have to be easier to control. In this thesis the chatbot should be seen as an mock up prototype that have some errors that have to be solved before any conclusion about how well the educational method can be used.

8 Conclusion

In the following chapter result from previous chapter will be presented. Experience that has been gained under the work will be discussed. Future work to this thesis will also be presented.

8.1 Discussion

In section 8.1.1 describes how the objectives where used under the work. In section 8.1.2 the result is discussed.

The research question for this master thesis is: *how efficient is present and accessible AI-bot technology is applied for education about social engineering frauds such as identity theft*

This research question cannot be meet because of the limitation that where discovered under the development. The limitations have an impact on the result in the survey. The limitations and problems that where recognized can be found in chapter 7.

As a result of the work with this thesis several important impressions and experiences have been gained. Most of the impressions and experience have a connection to the chatbot. In the beginning of the thesis the expectations on the functionality of the chatbot was rather high. This was most on the chatbots functionality. Under the work it appeared that the present solutions in the chatbots is not enough useful for this kind of work. Limitations in giving the chatbot knowledge and how to get the chatbot to interpret the tags in the knowledge files where substantial. The second limitation of this two has a huge impact on the work because it gave so big limitations in how the chatbot were going to serve. To get the chatbot to work properly, further work or development of a chatbot must be considered.

8.1.1 Objectives

To address the hypothesis three objectives where produced:

1. Evaluate various social engineering techniques that can be used in an implementation of a social engineering AI-bot.
2. Build a demonstration prototype that can emulate a social engineering attack in an educational context.
3. Test and evaluate the prototype through a usability test comparing it with an academic reference group with non specialist security education.

To start the theses work the first objective hade to be fulfilled. The chatbots initial limitations made the social engineering techniques limited. The chatbot limitations that can be found from the beginning are that it cannot be used for understanding emotions, or it cannot use persuasion because it cannot feel emotions. By this the useable techniques where limited. To start the evaluation an open interview with a domain expert were conducted. To conduct an interview is rather difficult, the error that was made where that not enough questions was prepared beforehand and not enough knowledge about the interview process and structure hade been gained before the interview. The experience by the interview is to prepare several main question and several follow up questions beforehand. If this is done an interview can be very useful. After the interview the domain experts' answers were transcribed and send for validation by the interviewee. The interview was the base for a more deep-going analyzes of the social engineering techniques that was possible to use. This analysis

ended in an evaluation about possible social engineering techniques to use in the chatbot.

The chosen technique for the chatbot where implemented in objective two. To perform the implementation models hade to be developed, the first model is the attack cycle that tells what the purpose of the chatbot is, the second model is flowcharts, and this can be found in Appendix B. The attack model explains what the main purpose and end result of the attack are. By this it is possible to develop the fraud attempt that the users are going to be exposed to. The content in the models where converted in to knowledge files that the chatbot could read and this was done with use of artificial Markup language (aiml).

To get the user to learn from the chatbot other knowledge file where constructed with an explanation on the purpose of the fraud attempt, this explanation described what hade happened and what would happen if the fraud attempt where conducted by a theft. The text can be found in Appendix F. Because of the difficulty to read or listen to the explanation in the chatbot, a webpage with the same content where developed. Several problem where discovered under the development. An explanation to them can be found in chapter 7.

The third objective evaluation where conducted in several phases. The first phase were to evaluate the functionality of the knowledge files and the chatbot functionality. In this phase it was to run through the chatbot and control that everything worked as expected. Several problems in this phase were detected, they are described in chapter 7. To get an evaluation of the hypothesis, it hade to be evaluated against another educational method. In this case it where traditional security education by reading a written informational text, the case comes from CIFAS (2009). The evaluation was conducted by making surveys with several questions before and after the education. The questions before the education were to get to know the participants behaviour before the education. The questions after were made to evaluate if and how the participants have gained any understanding of the education.

The experience that has been gained under the work with the objectives is that there is a need to investigate what technology differences online chatbots have. They can be built with the same technique but that do not make sure that they are working in the same way. There is always a need to have a backup plan to fall back to when it starts to go wrong in any way. Maybe the biggest experience is that how much planning and preparatory work that is made everything takes much more time than expected.

8.1.2 Result summary

The result from the survey were evaluated and analyzed to get an understanding about how useful the chatbot have been in the education. The analysis showed that the participants conclusively believed that the chatbot have potential to be an educational tool in social engineering and information security training. However traditional educational methods are still a strong competitor to the chatbot. Not many of the respondents in the survey have any security training, this shows that there is a need for security training to a population so they have the opportunity to some kind of defence against fraud attacks that they can be exposed too. The result also shows that the users have a good knowledge about basic security as, not leaving out passwords and if they do share a password they promptly change the password afterwards.

The respondents in the chatbot evaluation group believes that they will not leave out information after the education, the other two groups are not so curtain that they will

leave out information after the education. The respondents that got a security education will be more conservative with leaving out information but they believe that they will not be more conscious after the education. A problem with this evaluation is that it is not possible to know for how long the knowledge remains in the participants' memory. To evaluate this, a new survey has to be conducted after some time or to make a fraud attack attempt on the participants. Both of this solution is out of question because of time constraints for this work and because of ethical considerations to take into account.

The evaluation group comes as close as possible to a group that have normal computer skills and non-security education. The evaluation group should display an average citizen. The evaluation group have age differences and both male and female participants. The education in the evaluation group has a large range. What can compromise the result is that it is a group of academics that have participated. This can change the result from what an average citizen should have answered. The result with the used evaluation group should be satisfactory when 291 (73%) of the 400 invited answered the survey and that means that there are 97 participants in each of the three survey groups.

8.2 Contribution

This thesis extends the work by Walentowicz and Mozuraite Araby (2008) and Huber (2009). The contrast to this two works are in Walentowicz and Mozuraite Araby (2008) case the use of a chatbot to educate users by giving a hands on experience about a social engineering attack, and in the case of Huber (2009) use a automated chatbot to gather information by giving the user a hands on experience on how a possible social engineering attack may be performed.

The result in this work proves that it may be possible to use a chatbot for educating users in spotting fraud attempts that uses a social engineering technique. However several problems reduce the functionality and solving these problems should increase the chatbot ability to educate. What is proven is that the chatbot have the ability to educate in preventing social engineering attacks in it is current form. By giving the users the needed knowledge it is possible to minimize the risk that classified information in organisations will be lost to unauthorized personal and get the users in the organisations a knowledge that everything is not as it appears. The purpose with the education is to get the users to start questioning occurrences that is unfamiliarly in the every day events. By this the users should ask themselves if they should leave out information in situations that is unfamiliarly.

The use of a chatbot that can educate in other social engineering techniques and other fraud techniques. A more developed automated chatbot for security education has to be constructed and more research has to be conducted before any strong conclusions can be drawn. In section 8.3 suggestions on future work is presented.

8.3 Future work

The main aim of future works should be to develop a chatbot that have extended methods and techniques for social engineering. There are three main directions for future work: *(i)* perform new evaluation of the chatbot in a larger scale. *(ii)* Give the chatbot extended social engineering methods and techniques that give the chatbot a better educational functionality. *(iii)* To extend the chatbot with functionality to sense emotions, develop functionality extending plug-ins, and to give the chatbot the ability to have a conversations with the user.

The first *(i)* future work is improvement of the evaluation of the educational chatbot usefulness. The evaluation in this dissertation has different flaws, another evaluation can show another result. The chatbot can be evaluated in an organisation that could be exposed to fraud attempts. The education and survey can be follow up with a new evaluation after some time, the reviews can show if the users have hade any use ness of the education or if they have changed there behaviour. This can show the real functionality of the chatbot and the result should mirror how well the chatbot is working in a real organisation that has the need for this kind of security education.

A very interesting topic *(ii)* would be to give the chatbot more social engineering techniques that it can use for educating users in different frauds that hey can be exposed to. This can give the user a know-how of what to expect and what to do if they are exposed to any of the social engineering techniques that is available. By this the chatbot can change the technique under an education and expose the user to a variety of different techniques. If the chatbot also are equipped with different fraud methods the variation in the education is almost endless. These combinations can give the user the needed knowledge to respond and counter strike to an attack in the daily work or in their daily occupations. The social engineering techniques that can be extended into the chatbot should follow the order of the techniques that is most used in frauds.

The third *(iii)* future work is to make the technology in the chatbot better and more useful. The chatbot has several technical flaws that can be interesting to solve, the first one is to get the chatbot sense emotions from the user. To get the chatbot to sense emotions sensors are needed, like microphones, stress detectors, eye movement detectors, and other useful detectors. When and if the chatbot can interpret pressure or hesitation it can change it behaviour, by this it can change it persuasion to what is needed at the time.

The functionality in the chatbot can in some cases be limited and have to be extended, by using JavaScript in the aiml file, the functionality can be extended. To extend the chatbot with small extension as a web link in the knowledge files that it will show in text and not in speak, if the chatbot can use a text-to-speech synthesis. Some script language or other technology needs to be implemented to prevent the chatbot to use a web link in another way than expected. This gives the chatbot a more flexible usage, another way to extend the functionality is to use plug-in instead of JavaScript in the aiml file. By giving the chatbot a new functionality the chatbots behaviour can be changed and the usage of the chatbot can be extended.

To get the chatbot to have a more flexible education it has to interact with the user. By a microphone the user can talk to the chatbot and by this have an interaction. In the interaction between the user and the chatbot, it should be possible for the user to ask the chatbot a question under the education and the chatbot should not forget the main topic and continue after it have answered the question. If the chatbot have a conversation with the user and under the conversation asks the user a question it should not forget what the conversation is about and only continue the conversation. This can give the chatbot a new dimension in education. If the chatbot have the ability to ask the user questions under a conversation it will extend the educational method. The approach makes it possible to give the user a new experience and by this give the user a more meaningful education.

If the text-to-speech is used and there are JavaScript in the aiml file, the voice synthesis will read all of the JavaScript to the user. There are several ways to solve the problem. The first one is to develop a tag that tells the voice synthesis that here

comes a text that should not be read to the user. This involves developing a text-to-speech engine that understand the new tag and ignores it. The second solution is to develop a new text-to-speech engine that can recognize a JavaScript or other code and by this ignore these parts. The last solution is to use a plug-in system that eliminates the problem completely, to implement this solution a complete new bot has to be developed. All of the mentioned future works in this category have the intention to extend the experience in the education for the user and by this give a better learning about social engineering techniques and fraud methods.

References

ALICE Artifical Intelligence Foundation. (2009). *AIML: Artificial Intelligence Markup Language.* [Online]. Available From: http://www.alicebot.org/aiml.html. [6 March 2009].

Allen, M. (2007). *Socail Engineering: A Means To Violate A Computer Crime.* [Online]. SANS Institute. Available From: http://www.sans.org/reading_room/whitepapers/engineering/social_engineering_a_means_to_violate_a_computer_system_529. [20 February 2009].

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis Projects - A Guide for Students in Computer Science and information Systems.* Skövde: Springer-Verlag London Limited.

Carpenter, R. (2009). *Jabberwacky.* [Online]. Available From: http://www.jabberwacky.com/. [22 February 2009].

CIFAS. (2009). *Identity Fraud and Identity Theft.* [Online]. CIFAS. Available From: http://www.cifas.org.uk/default.asp?edit_id=561-56. [23 April 2009].

Cisco. (2009). *Protect Against Social Engineering.* [Online]. Availabla From: http://www.cisco.com/web/about/security/intelligence/mysdn-social-engineering.html. [21 February 2009].

Dagens Nyhter. (2008). *Hemlös man stal vd:s identitet.* [Online]. Available From: http://www.dn.se/nyheter/sverige/hemlos-man-stal-vds-identitet-1.686486. [12 August 2009].

Expressen. (2009). *Utan skuld – men satt i konkurs.* [Online]. Available From: http://www.expressen.se/1.1551888. [12 May 2009].

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Secuirty Beliefs and Barriers for Novice Internet Users. *Computers & Security , 27*, 235-240.

Granger, S. (2001). *Social Engineering Fundamentals, Part I: Hacker Tactics.* Avalible From: http://www.securityfocus.com/infocus/1527. [20 February 2009].

Guardian. (2006). *What could a boarding pass tell an identity fraudster about you?* [Online]. Available From: http://www.guardian.co.uk/business/2006/may/03/theairlineindustry.idcards. [12 August 2009].

Harl. (1997). *People Hacking: The Psycklogy of Social Engineering.* [Online]. Available From: http://packetstormsecurity.nl/docs/social-engineering/aaatalk.html [Accessed 20 February 2009].

Huber, M. (2009). *Automated Socail Engineering Proof Of Concept.* Master thesis, Department of Computer and Systems Science. Stockholm Univeristy/Royal Institute of Technology of Stockholm.

Identitytheft.org.uk. [Online]. Available From: http://www.identitytheft.org.uk. [25 March 2009].

IKEA. (2008). *ANNA.* [Online]. Available From: http://193.108.42.79/ikea-se/cgi-bin/ikea-se.cgi. [22 February 2009].

Jakobsson, M. (2008). *Social Engineering 2.0: What´s Next.* [Online]. McAfee. Available

From:http://www.mcafee.com/us/local_content/misc/threat_center/msj_social_engineering_2.pdf. [Accesssed 11 Aug 2009].

Jia, J. (2009). *CSIEC: A Computer Assisted English Learning Chatbot Based On Textual knowledge and Reasoning.* Elsevier B.V.

Kajava, J., & Siponen, M. T. (1997). *Social Engineerig - IT Security Threat of Informatics.* [Online]. Iris 20. Available From: http://web.archive.org/web/20040422210025/http://iris.informatik.gu.se/conference/iris20/9.htm#E19E207. [21 February 2009].

Kerly, A., Hall, p., & Bull, s. (2006). Bringing Chatbots Into Education: Towards Natural Language Negotiation of Open Learner Models. *Knowledge-Based Systems , Vol. 20*, pp. 177-185, (2007).

Kruger, H.A. & Kearney, W.D. (2006). A prototype for assessing information security awareness, Computers & Security 25, 4, 289 – 296.

Levine, R. (2003). *The Power of Persuasion.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Long, J. (2008). *No Tech Hacking.* Burlington: Syngress Publishing, Inc.

Microsoft. (2006). *How to Protect Insiders from Social Engineering Threats.* [Online]. Avaliable From: http://technet.microsoft.com/en-us/library/cc875841.aspx. [5 March 2009].

Microsoft. (2007a). *Anti-phishing Technologies Overview.* [Online]. Available From: http://www.microsoft.com/mscorp/safety/technologies/antiphishing/overview.mspx. [20 February 2009].

Microsoft. (2007b). *What Is Social Engineering?* Available From: http://www.microsoft.com/middleeast/athome/security/email/socialengineering.mspx. [20 February 2009].

Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Secuirty.* Indianapolis, USA: Wiley Publishing, Inc.

NIST. (2003). *A Proactive Defence to Social Engineering.* FIPS PUB 1999. [Online] Avalablie From: http://www.sans.org/reading_room/whitepapers/engineering/a_proactive_defence_to_social_engineering_511. [5 March 2009].

Nohlberg, M. (2008). *Securing Information Assets: Understanding, Measuring and Protecting Against Socail Engineering Attacks.* Diss: Department of Computer and Systems Science. . Stockholm: Stockholm University/Royal Instituet of Technology.

Nohlberg, M., & Kowalski, S. (2008). The Cycle of Deception - A Model of Social Engineering Attacks, Defence and Victims. In Procedings of the Second International Symposium on Human Aspects of Information Security and Assurance (HISA 2008).

Preacher, K. J. (2001). *Calculation for the chi-square test: An interactive calculation tool for chi-square tests of goodness of fit and independence*. [Online] Available from http://www.quantpsy.org. [30 August 2009].

Pressman, R. S. (2005). *Software enigneering - A Practitioner´s Approach.* McGraw-Hill.

Ringate, T. (2001). *AIML Primer.* [Online]. Available from: http://www.alicebot.org/documentation/aiml-primer.html#pattern%20match. [6 March 2009].

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' - a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology , 19* (3), pp. 122-131.

Schneier, B. (2000). *Secret & Lies: Digital in a Networked World.* New York, USA: John Wiley & Sons, Inc.

Schumaker, R. P., Liu, Y., Ginsburg, m., & Chen, H. (2006). Evaluating mass knowledge acquisition using the ALICE chatterbot: The AZ-ALICE dialog system . *International Journal of Human-Computer Studies, 64 (11)* , pp. 1132-1140.

SIS. (2003). *SIS Handbok 550. Terminologi för Informationssäkerhet.* Stockholm: SIS Förlag AB.

Telia AB. (2009). *Automated helpdesk answering system.* [Online] Available From: 90200 [March 2009].

Thaper, A. *Social Engineering - An Attack Vector most inticate to tackle!* Available From: http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf. [20 February 2009].

The Swedish Data Inspection Board. (2009) *Personal Dat Act (1998:204).* [Online] Available From: http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf. [31 August 2009].

The Swedish Police Service. (2009). *Nätfiske - phishing.* [Online] Available From: http://www.polisen.se/inter/nodeid=30914&pageversion=1.jsp. [5 March 2009].

The Swedish Post and Telecom Agency. (2004). *Phishing - en ny form av Internetbedrägeri.* [Online] Availabla from: http://www.pts.se/sv/Nyheter/Internet/2004/Phishing%20-%20en%20ny%20form%20av%20Internetbedr%C3%A4geri/. [5 March 2009].

Walentowicz, S., & Mozuraite Araby, R. (2008). *Using Chatbots Within InformationSecurity Education.* Master thesis, Department of Computer and Systems Science. Stockholm Univeristy/Royal Institute of Technology of Stockholm.

Wallace, R. S. (2009). *The Anatomy of A.L.I.C.E.* [Online].A.L.I.C.E Artifical Intelligance Foundation, Inc. Avalilable From: http://www.alicebot.org/anatomy.html. [22 February 2009].

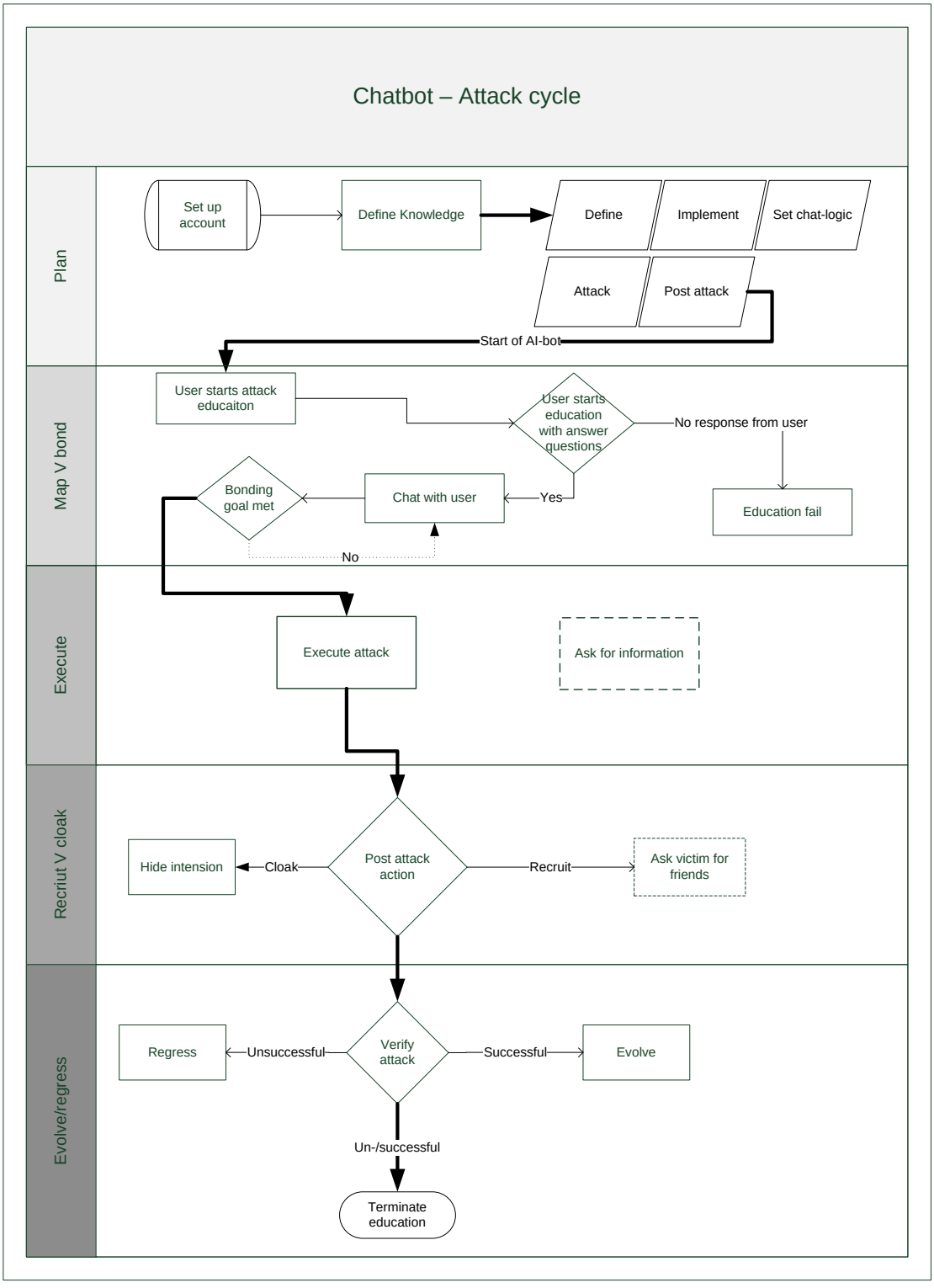
Weizenbaum, J. (1966). *ELIZA - A Computer Program For the Study of Natural Language Communication Between Man And Machine.* Cambridge, Massachusetts, USA: Communication of the ACM, 26 (1). pp.36-45.

Zakos, J., & Capper, L. (2008). *CLIVE - An Artificially Intelligent Chat Robot for Conversational Language Practice.* Springer Link.

Åhlfeldt, R.-M., Spagnoletti, P., & Sindre, G. (2007). Improving the Information Security Model by using TFI. Sandton, South Africa: Conference Proceedings of the 22th IFP TC-11 International Information Security Conference.

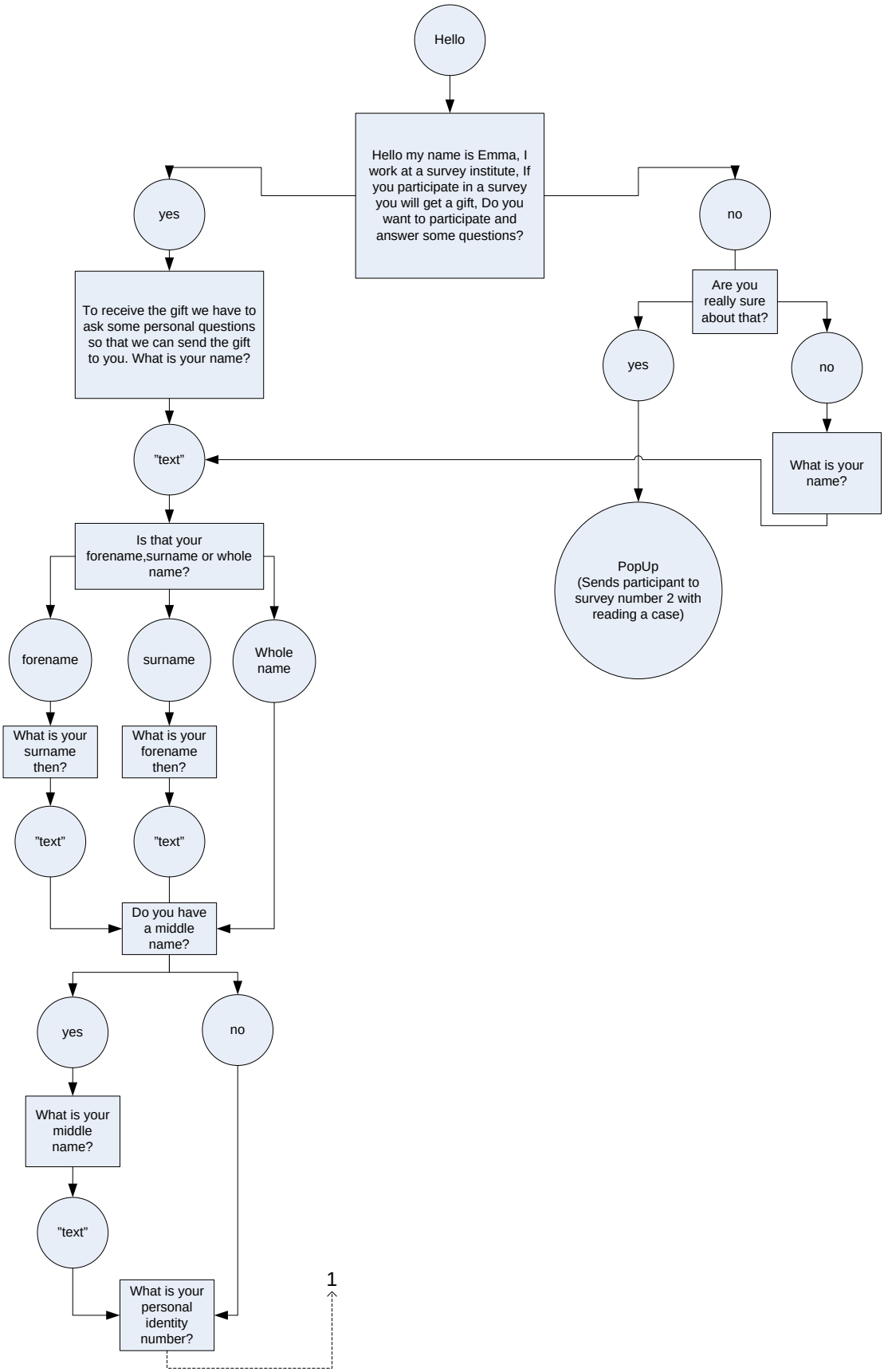
Index for Appendix

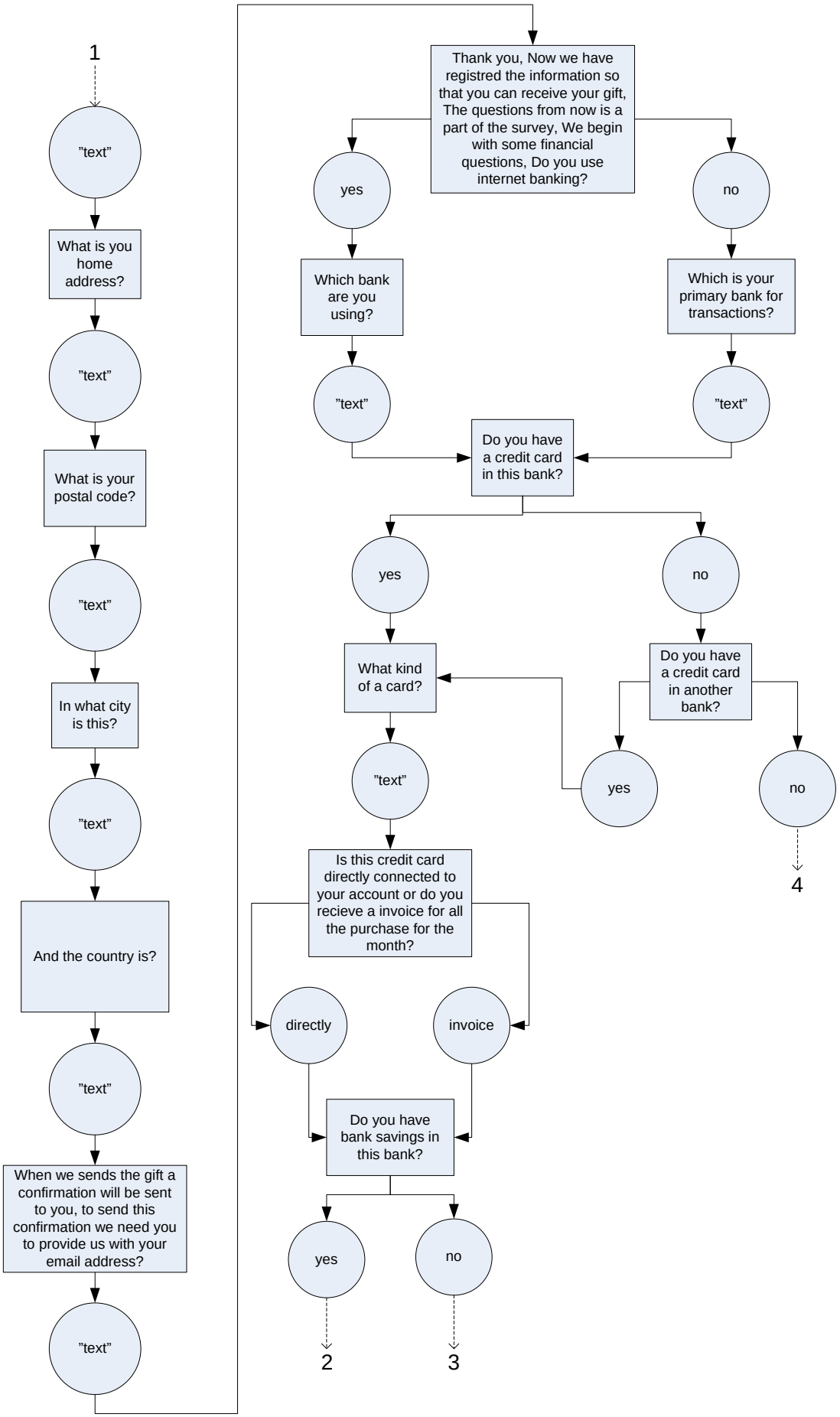
Appendix A

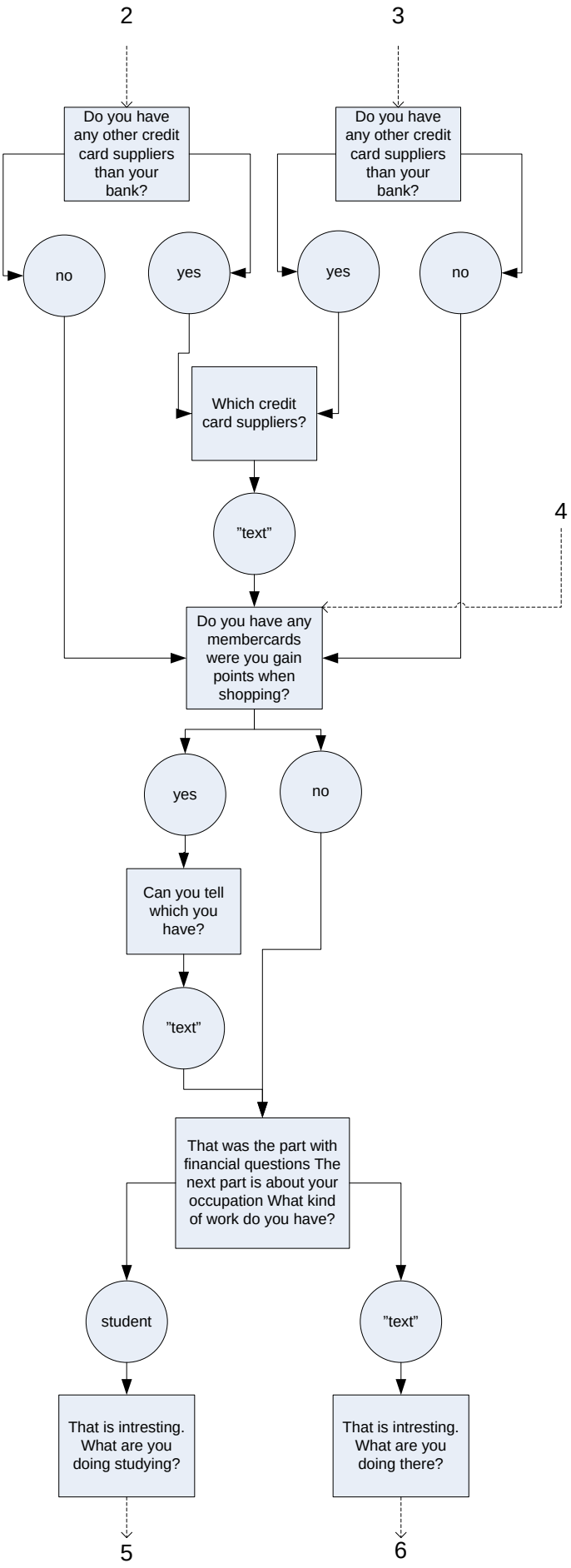

Chatbot – Attack cycle
Plan
Set up account
Define Knowledge
Define
Implement
Set chat-logic
Attack
Post attack
Start of AI-bot
Map V bond
User starts attack educaiton
User starts education with answer questions
No response from user
Education fail
Yes
Chat with user
Bonding goal met
No
Execute
Execute attack
Ask for information
Recriut V cloak
Hide intension
Cloak
Post attack action
Recruit
Ask victim for friends
Evolve/regress
Regress
Unsuccessful
Verify attack
Successful
Evolve
Un-/successful
Terminate education

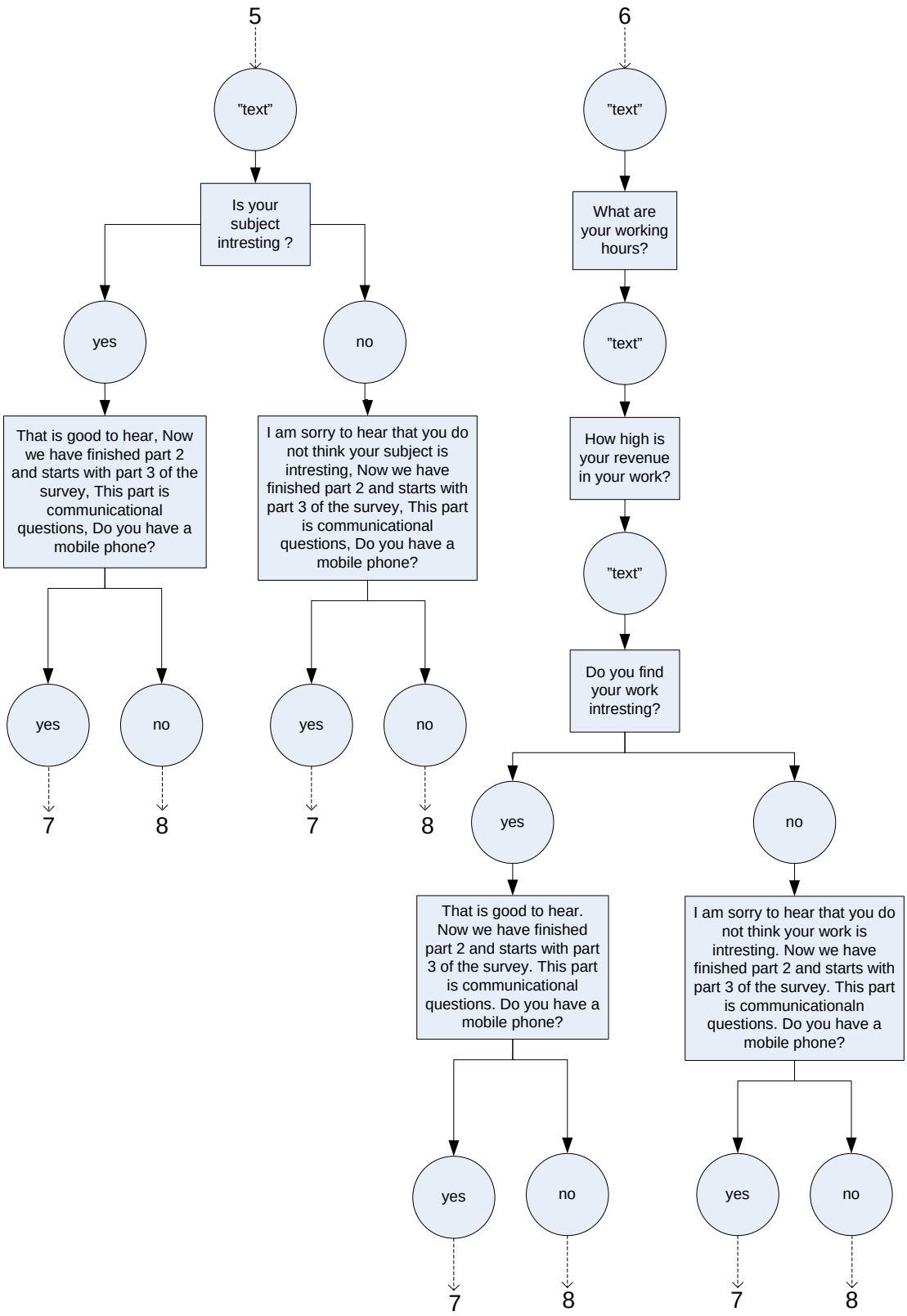
Appendix B

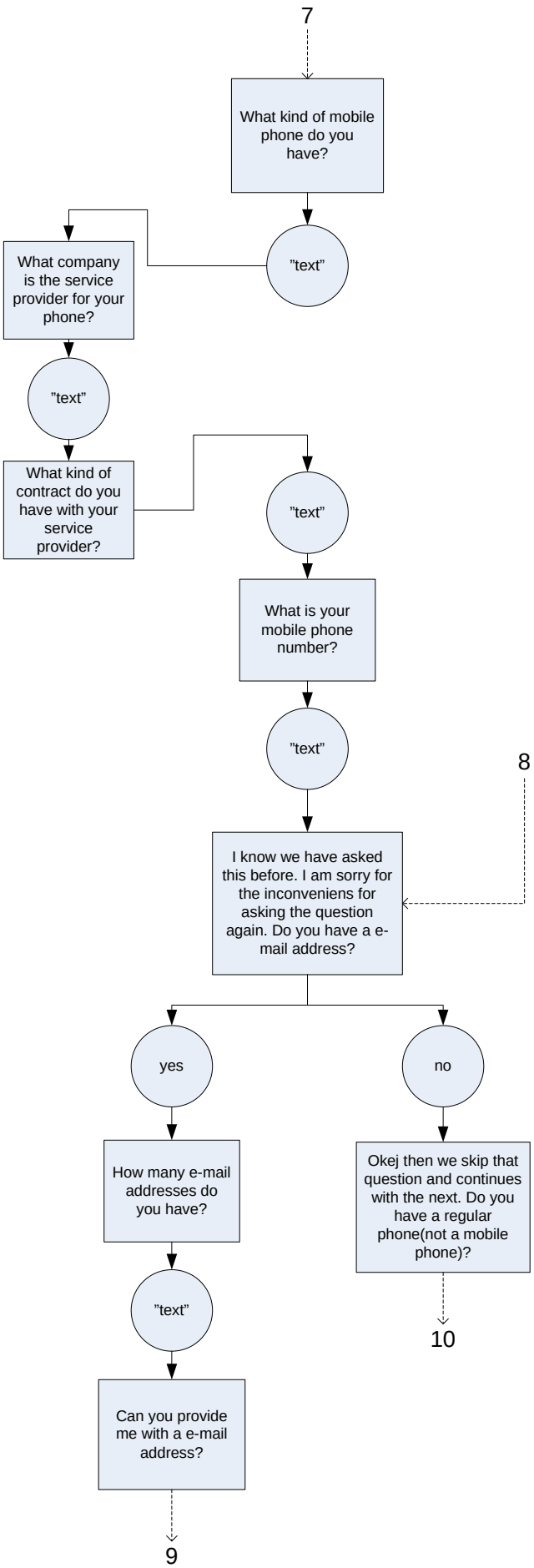
Flow charts

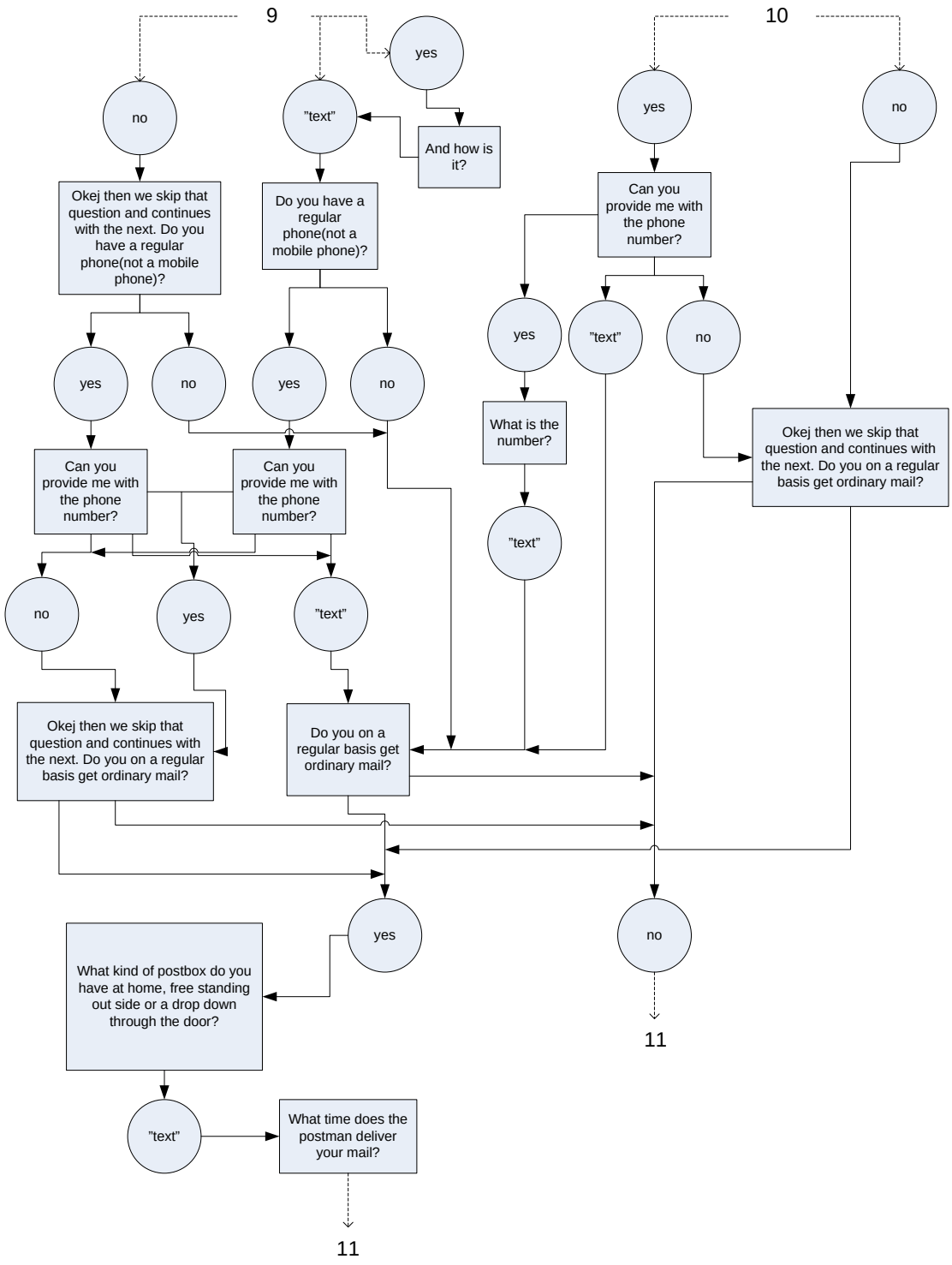


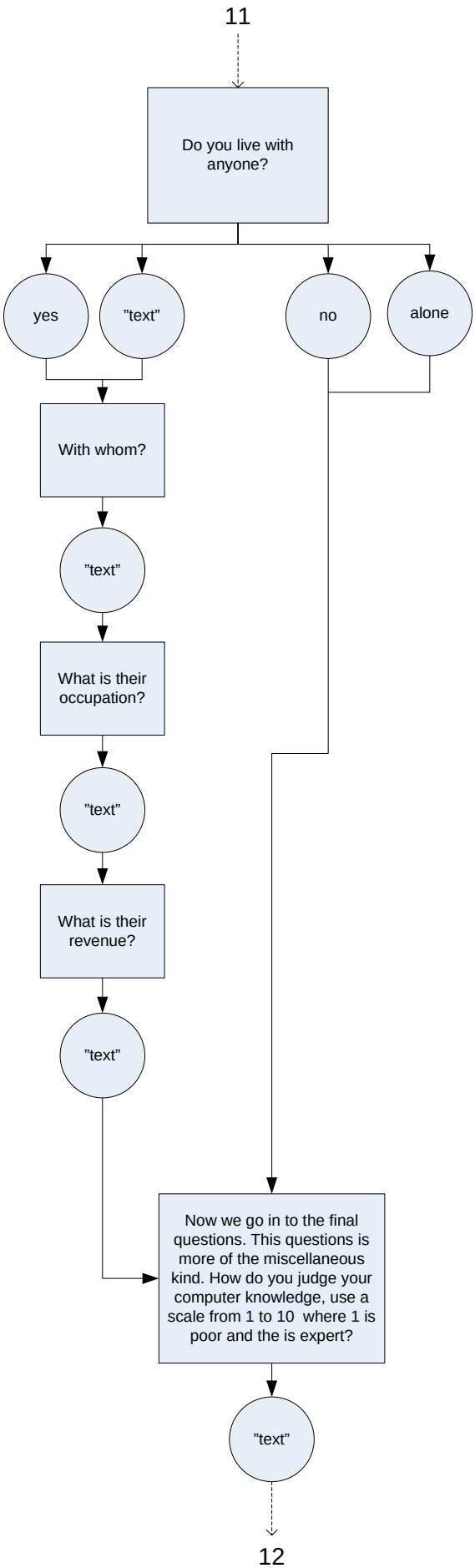

1
"text"
What is you home address?
"text"
What is your postal code?
"text"
In what city is this?
"text"
And the country is?
"text"
When we sends the gift a confirmation will be sent to you, to send this confirmation we need you to provide us with your email address?
"text"
Thank you, Now we have registred the information so that you can receive your gift, The questions from now is a part of the survey, We begin with some financial questions, Do you use internet banking?
yes
Which bank are you using?
"text"
no
Which is your primary bank for transactions?
"text"
Do you have a credit card in this bank?
yes
What kind of a card?
"text"
Is this credit card directly connected to your account or do you recieve a invoice for all the purchase for the month?
directly
invoice
Do you have bank savings in this bank?
yes
2
no
3
no
Do you have a credit card in another bank?
yes
no
4

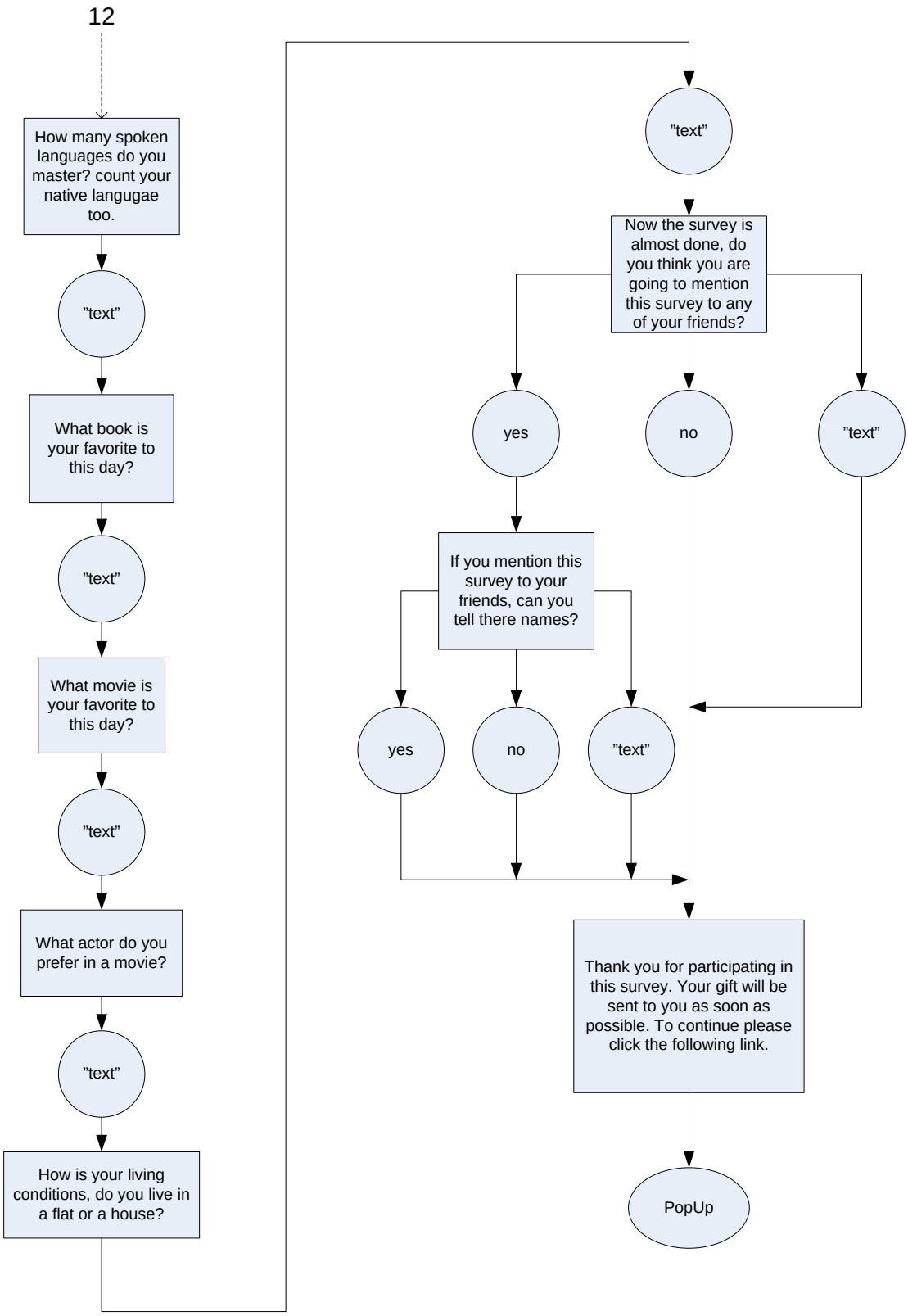

2
3
Do you have any other credit card suppliers than your bank?
Do you have any other credit card suppliers than your bank?
no
yes
yes
no
Which credit card suppliers?
”text”
4
Do you have any membercards were you gain points when shopping?
yes
no
Can you tell which you have?
”text”
That was the part with financial questions The next part is about your occupation What kind of work do you have?
student
”text”
That is intresting. What are you doing studying?
That is intresting. What are you doing there?
5
6


5
"text"
Is your subject intresting ?
yes
no
That is good to hear, Now we have finished part 2 and starts with part 3 of the survey, This part is communicational questions, Do you have a mobile phone?
I am sorry to hear that you do not think your subject is intresting, Now we have finished part 2 and starts with part 3 of the survey, This part is communicational questions, Do you have a mobile phone?
yes
no
yes
no
7
8
7
8
6
"text"
What are your working hours?
"text"
How high is your revenue in your work?
"text"
Do you find your work intresting?
yes
no
That is good to hear. Now we have finished part 2 and starts with part 3 of the survey. This part is communicational questions. Do you have a mobile phone?
I am sorry to hear that you do not think your work is intresting. Now we have finished part 2 and starts with part 3 of the survey. This part is communicationaln questions. Do you have a mobile phone?
yes
no
yes
no
7
8
7
8


7
What kind of mobile phone do you have?
"text"
What company is the service provider for your phone?
"text"
What kind of contract do you have with your service provider?
"text"
What is your mobile phone number?
"text"
8
I know we have asked this before. I am sorry for the inconveniens for asking the question again. Do you have a e-mail address?
yes
no
How many e-mail addresses do you have?
Okej then we skip that question and continues with the next. Do you have a regular phone(not a mobile phone)?
"text"
10
Can you provide me with a e-mail address?
9


9
10
yes
no
"text"
And how is it?
Okej then we skip that question and continues with the next. Do you have a regular phone(not a mobile phone)?
Do you have a regular phone(not a mobile phone)?
yes
no
yes
no
Can you provide me with the phone number?
Can you provide me with the phone number?
no
yes
"text"
Okej then we skip that question and continues with the next. Do you on a regular basis get ordinary mail?
Do you on a regular basis get ordinary mail?
yes
no
What kind of postbox do you have at home, free standing out side or a drop down through the door?
"text"
What time does the postman deliver your mail?
11
yes
"text"
no
Can you provide me with the phone number?
What is the number?
"text"
yes
no
Okej then we skip that question and continues with the next. Do you on a regular basis get ordinary mail?
11


11
Do you live with anyone?
yes
”text”
no
alone
With whom?
”text”
What is their occupation?
”text”
What is their revenue?
”text”
Now we go in to the final questions. This questions is more of the miscellaneous kind. How do you judge your computer knowledge, use a scale from 1 to 10 where 1 is poor and the is expert?
”text”
12


12
How many spoken languages do you master? count your native langugae too.
"text"
What book is your favorite to this day?
"text"
What movie is your favorite to this day?
"text"
What actor do you prefer in a movie?
"text"
How is your living conditions, do you live in a flat or a house?
"text"
Now the survey is almost done, do you think you are going to mention this survey to any of your friends?
yes
no
"text"
If you mention this survey to your friends, can you tell there names?
yes
no
"text"
Thank you for participating in this survey. Your gift will be sent to you as soon as possible. To continue please click the following link.
PopUp

Appendix C

AIML files for chatbot Emma:

personal_brain.aiml

financial_brain.aiml

occupation_brain.aiml

communication_brain.aiml

miscellaneous_brain.aiml

AIML files for chatbot Maria:

social_enigeering.aiml

Appendix D

Screenshot chatbot Emma

Tell Emma:

Say

Powered by Pandorabots.

Appendix E

Screenshot chatbot Maria

Tell Maria:

Say

Powered by Pandorabots.

Appendix F – Purpose of chatbot behaviour

What you just have gone through is a social engineering attack with the goal to steal your identity. Social engineering is the act of manipulating people into performing actions or divulging confidential information.

All the questions that you have answered are publicly available information for an attacker (also called social engineer) in Sweden. A social engineer don't want to spend much time gathering basic information to decide if there is any meaning to perform an attack on a person. The easiest way to do this is by making you give the information to an automated chatbot. The automated chatbot can be found in social networking sites as Facebook, but there could be ordinary websites with the same feature. By using a chatbot the attacker minimize the interaction with the victim. To get the victim (you) to really participate in the survey the attacker says he/she is going to give away a gift. With the gift as bait the attacker increases the possibility for the victim to finish the survey. The information from the attack is a vital part for the attacker to understand who you are and if there is any reason to undertake a full scale attack with the subject to steal your identity.

The attacker's purpose of stealing your identity can be to open bank accounts, obtain credit cards, finance, loans and mortgages, to obtain goods or services, or to claim benefits.

By explaining the purpose of the questions, it is possible for you to see why the questions have been asked. Your name and address makes it easy for the attacker to track you in registers. Your personal identity number makes it even easier. The combination of name, address, and personal identity number gives the opportunity to order new identification cards with your name but with attacker's picture. When the attacker has an identification card there is almost nothing that can stop the attacker from doing whatever he/she wants with your finances. The attacker can go in to a bank and order a new credit card or get the password to your internet bank.

The only thing that can slow the attacker down is how the mail is delivered. If you live in an apartment that have a mailbox in your door or the new mailboxes with a lock in the entrance to your house delays the attacker some. The problem is bigger if you live in a villa with a post-box at the gate to your property. It is very easy for an attacker to pass by and empty the post-box if it doesn't have a lock. What the attacker needs to know for doing this safely, are your working hours and when the mailman is delivering the mail in your area.

The attacker is especially interested in persons that have a good economy, which is a person that often lives in villas and have a large income every month and uses the credit part of the credit cards. These persons often have more economical transactions. The attacker orders new credit cards in your name and picks them from your mail before you get home. There is a probability that you not will discover the new credit card(s) before its too late.

The more information the attacker can gather around a victim, the probability that the victim will discover the fraud or identity theft decreases. But it's not always that the attacker wants to steal something from you either. Sometimes they want to get hold of an account were they can launder money from criminal activities without your knowledge or they want to have a username and password for access to a network from where they can commit a crime.

But do not panic now. There are ways for you to reduce the possibility to be a victim. There are a few simple precautions you can take to help prevent your identity from being used in this way:

Protect your personal details and think before you give them away: Who precisely is asking for my details? What details are they asking for? And why do they need these details?

Dispose of your documents securely. Any document containing any of your personal details is potentially useful to a fraudster.

The possibility for this to happen in Sweden today is far beyond what happening in the USA. BUT it have started, there are reports that tell that house owners have been getting mortgage on their houses whitout their knowledge.

Appendix G

Table shows in which group the questions is asked. Grey and white fields show question blocks. The letters in the table, c stands for question specific for group with chatbot and r specific for group with reading a case.

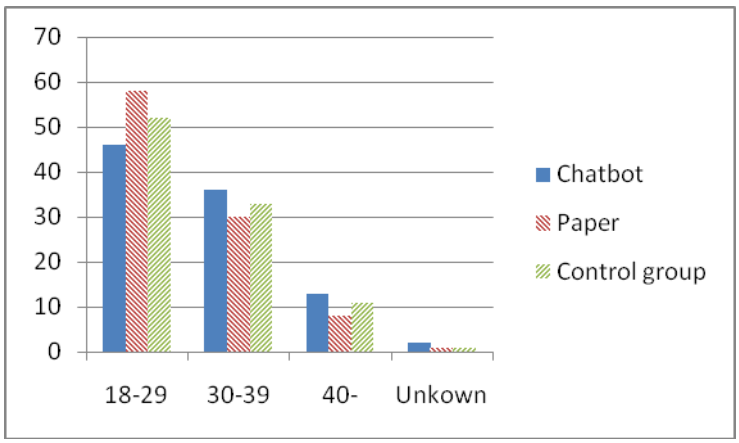
Question Nr.	Group 1	Group 2	Group 3	Question Nr.	Group 1	Group 2	Group 3
1	X	X	X	20	X	X	
2	X	X	X	21	X	X	X
3	X	X	X	22	X	X	X
4	X	X	X	23	X	X	X
5	X	X	X	24	X	X	
6	X	X	X	25	X	X	
7	X	X	X	26	X (c)	X (r)	
8	X	X	X	27	X	X	
9	X	X	X	28	X	X	
10	X	X	X	29	X (c)	X (r)	
11	X	X	X	30	X	X	
12	X	X	X	31	X	X	X
13	X	X	X	32	X	X	X
14	X	X	X	33	X	X	
15	X	X	X	34	X (c)	X (r)	
16	X	X	X	35	X (c)	X (r)	
17	X	X	X	36	X (c)	X (r)	
18	X	X	X	37	X (c)		
19	X	X		38	X (c)		

Appendix H

Block 1 - Basic questions about you and your habits

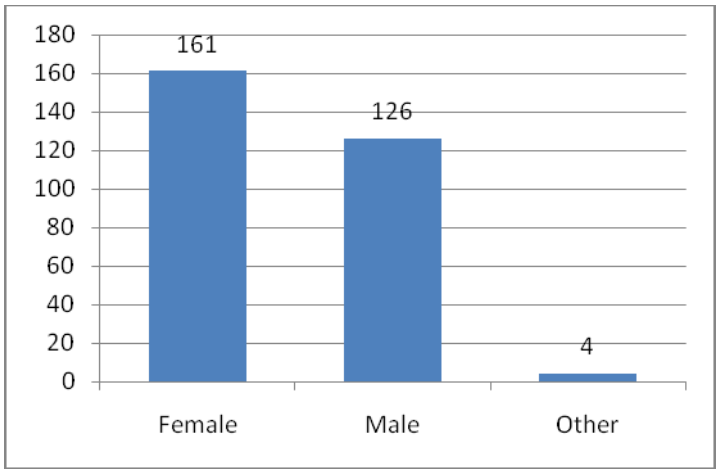
Question 1: What is your age?

	Chatbot	Paper	Control group	Total
18-29	46	58	52	156
30-39	36	30	33	99
40-	13	8	11	32
Unkown	2	1	1	4



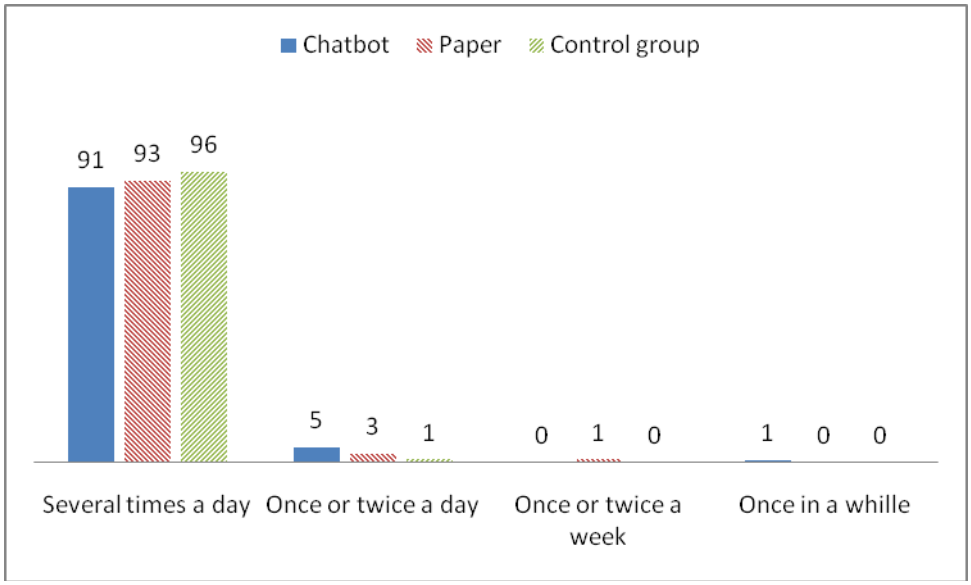
Question 2: What is you gender?

	Chatbot	Paper	Control group	Total
Female	55	52	54	161
Male	41	44	41	126
Other	1	1	2	4



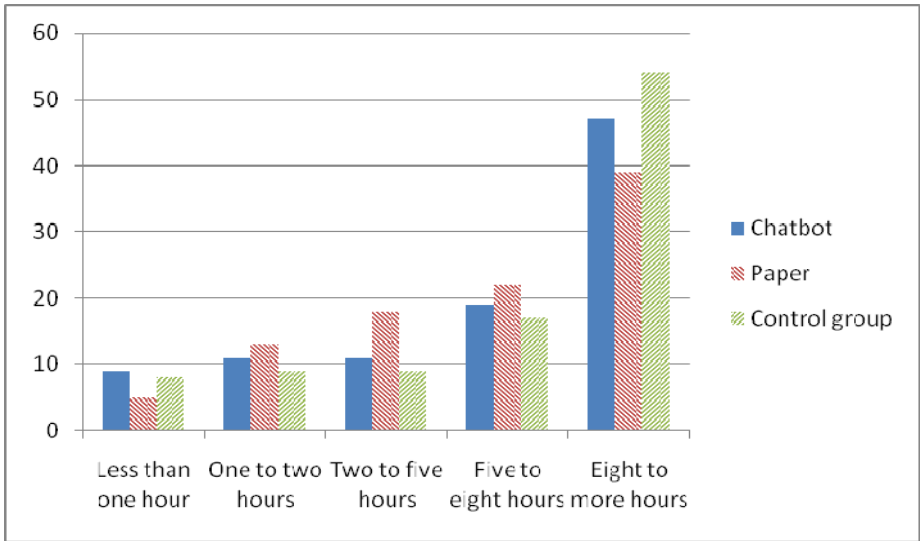
Question 3: How often do you use Internet?

	Chatbot	Paper	Control group	Total
Several times a day	91	93	96	280
Once or twice a day	5	3	1	9
Once or twice a week	0	1	0	1
Once in a whille	1	0	0	1



Question 4: How much time a day do you spend online?

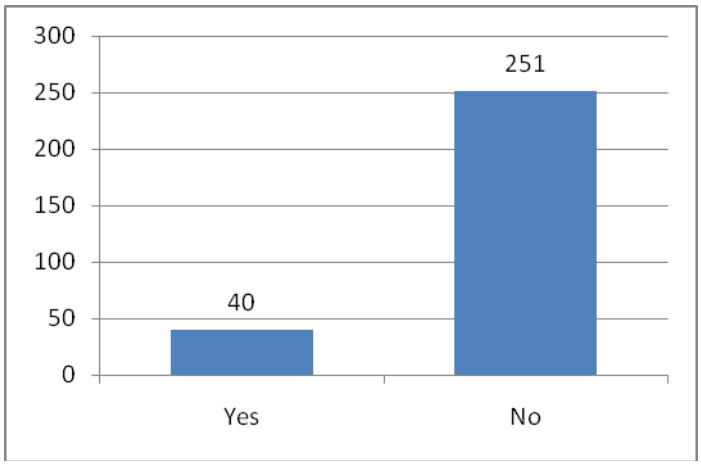
	Chatbot	Paper	Control group	Total
Less than one hour	9	5	8	22
One to two hours	11	13	9	33
Two to five hours	11	18	9	38
Five to eight hours	19	22	17	58
Eight to more hours	47	39	54	140



Question 5: Have you got any security education or training prior to this survey? If yes, from where.

	Chatbot	Paper	Control group	Total
Yes	14	11	15	40
No	83	86	82	251

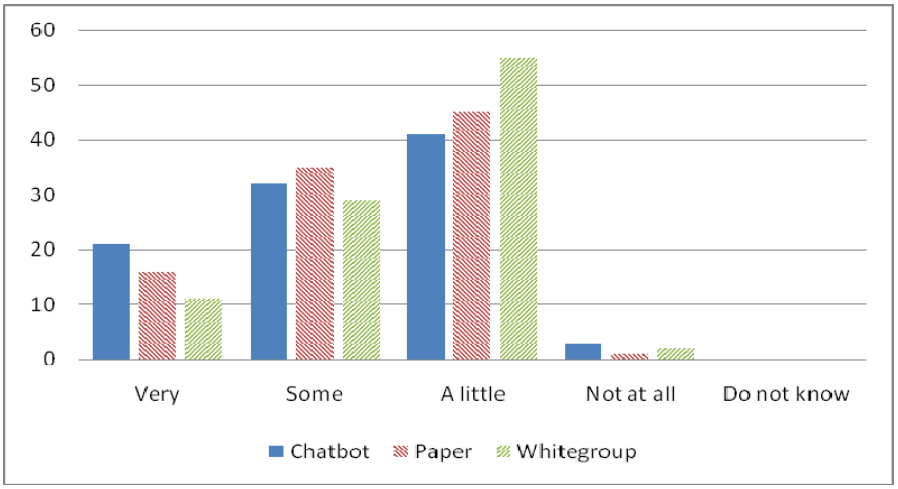
Comments: From work



Block 2 - Considerations in the daily routine on the internet

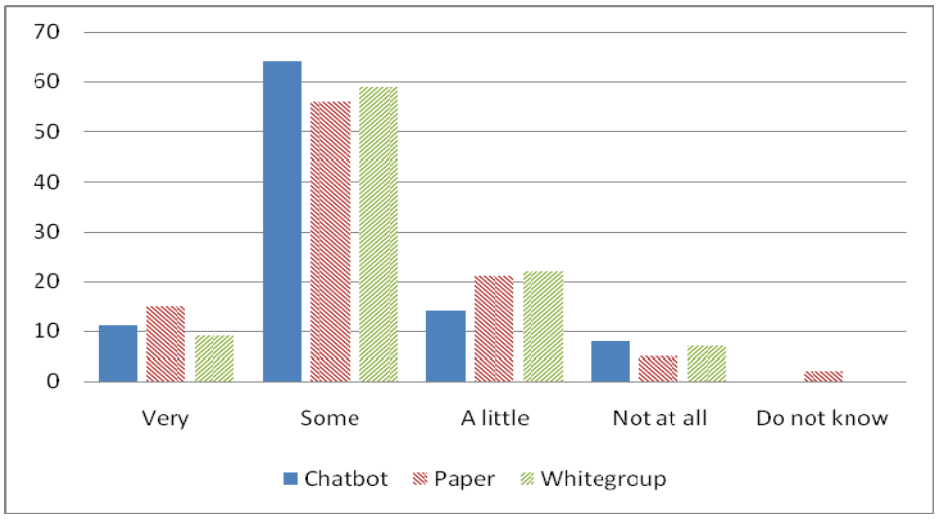
Question 6: Do you consider yourself to be concerned about security when using the Internet?

	Chatbot	Paper	Control group	Total
Very	21	16	11	48
Some	32	35	29	96
A little	41	45	55	141
Not at all	3	1	2	6
Do not know	0	0	0	0



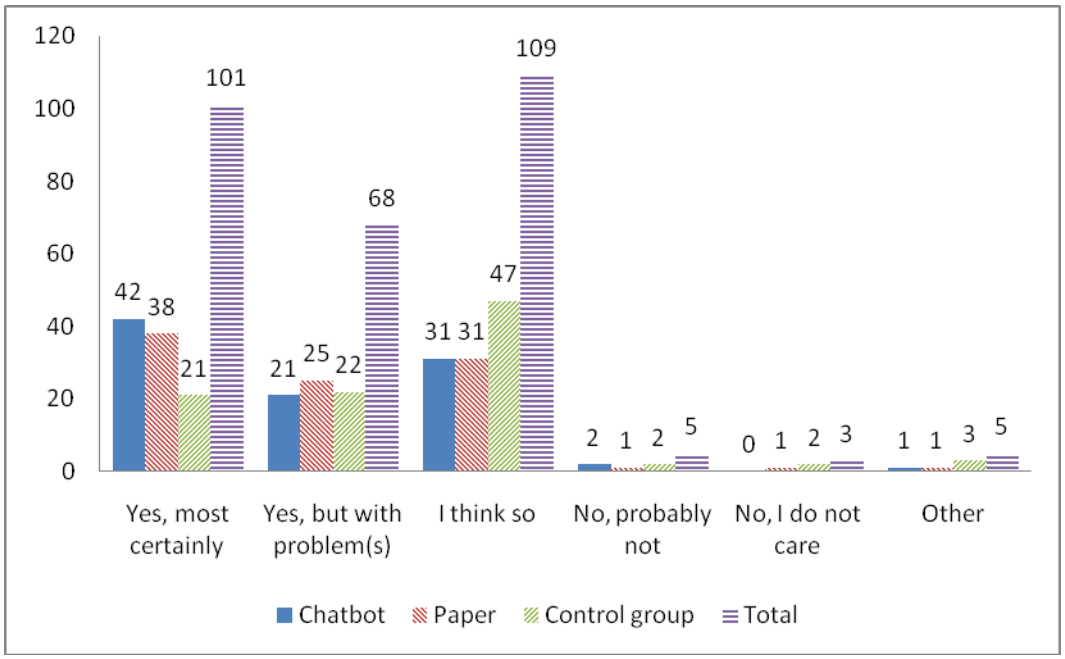
Question 7: Do you consider yourself to be good at detecting frauds on the Internet?

	Chatbot	Paper	Control group	Total
Very	11	15	9	35
Some	64	56	59	179
A little	14	21	22	57
Not at all	8	5	7	20
Do not know	0	2	0	2



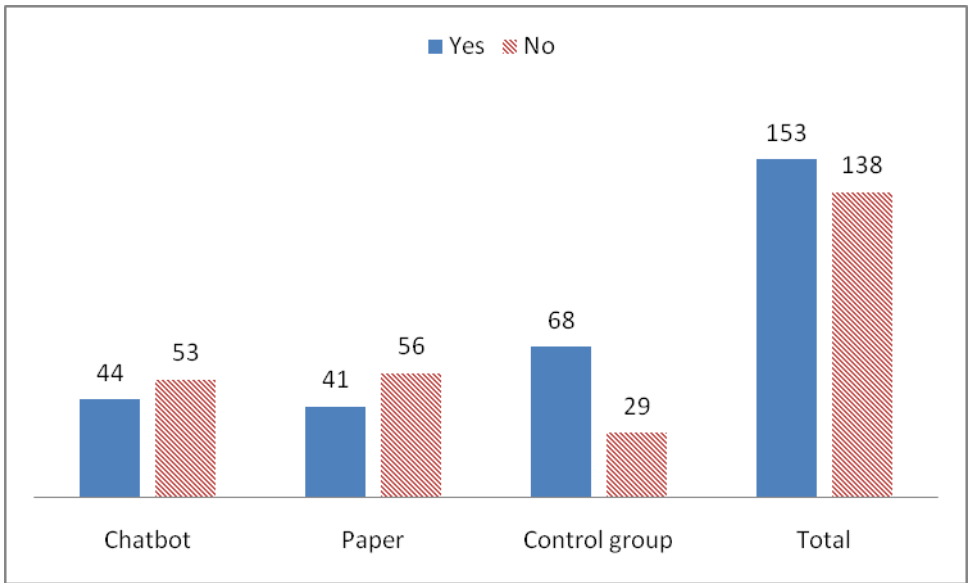
Question 8: Do you think you can recognize a fraud if you are exposed to it?

	Chatbot	Paper	Control group	Total
Yes, most certainly	42	38	21	101
Yes, but with problem(s)	21	25	22	68
I think so	31	31	47	109
No, probably not	2	1	2	5
No, I do not care	0	1	2	3
Other	1	1	3	5



Question 9: Do you know what to do if a stranger calls and starts to ask questions?

	Chatbot	Paper	Control group	Total
Yes	44	41	68	153
No	53	56	29	138

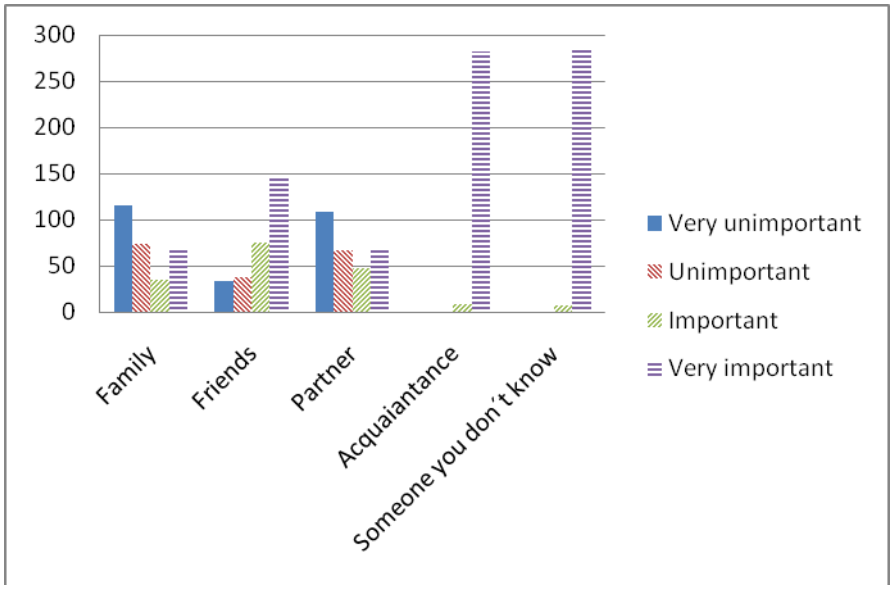


Block 3 - Your Security considerations that you take in the daily life

Question 10: How important do you feel it is to keep your password private and secure from:

How important do you feel it is to keep your password private and secure from:					
		Very unimportant	Unimportant	Important	Very important
Chatbot	Family	41	28	11	17
	Friends	13	12	24	48
	Partner	37	24	14	22
	Acquaiantance	0	0	2	95
	Someone you don´t know	0	0	2	95
Paper	Family	39	24	15	19
	Friends	11	11	28	47
	Partner	34	22	18	23
	Acquaiantance	0	1	2	94
	Someone you don´t know	0	1	2	94
Control group	Family	35	22	9	31
	Friends	9	14	23	51
	Partner	37	21	15	24
	Acquaiantance	0	0	4	93
	Someone you don´t know	0	0	3	94

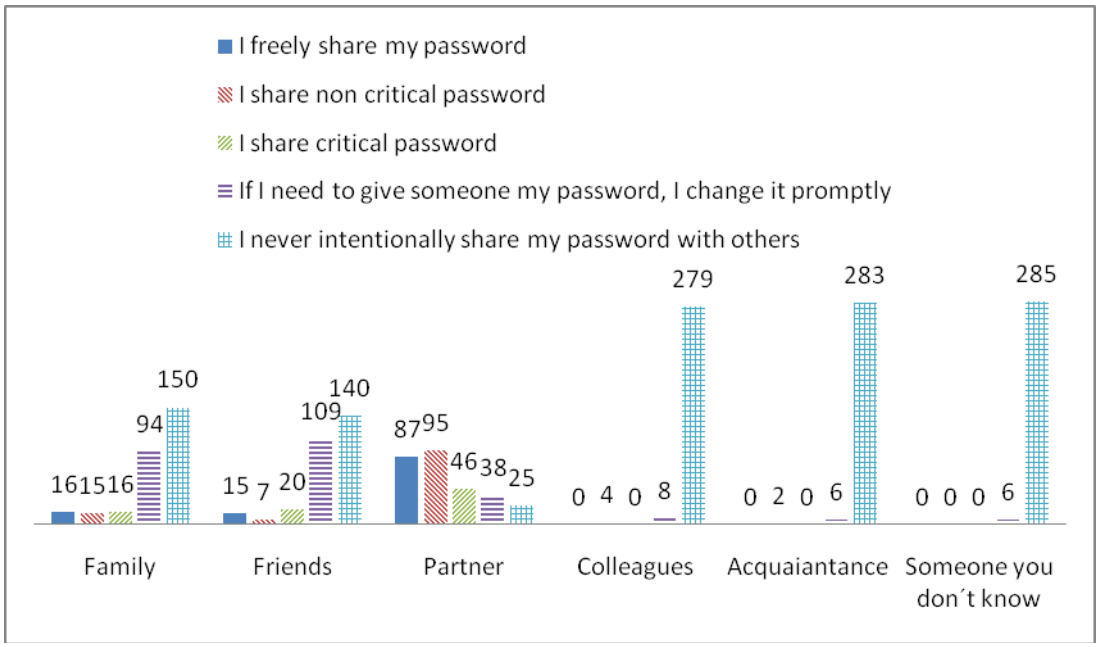
	Very unimportant	Unimportant	Important	Very important
Family	115	74	35	67
Friends	33	37	75	146
Partner	108	67	47	69
Acquaiantance	0	1	8	282
Someone you don´t know	0	1	7	283



Question 11: To what extent do you keep your computer password private from:

To what extent do you keep your computer password private from:						
		I freely share my password	I share non critical password	I share critical password	If I need to give someone my password, I change it promptly	I never intentionally share my password with others
Chatbot	Family	6	2	4	33	52
	Friends	5	2	8	42	40
	Partner	26	31	15	11	14
	Colleagues	0	0	0	2	95
	Acquaiantance	0	1	0	3	93
	Someone you don´t know	0	0	0	3	94
Paper	Family	6	8	6	25	52
	Friends	4	3	4	42	44
	Partner	31	35	13	12	6
	Colleagues	0	2	0	1	94
	Acquaiantance	0	0	0	1	96
	Someone you don´t know	0	0	0	1	96
Control group	Family	4	5	6	36	46
	Friends	6	2	8	25	56
	Partner	30	29	18	15	5
	Colleagues	0	2	0	5	90
	Acquaiantance	0	1	0	2	94
	Someone you don´t know	0	0	0	2	95

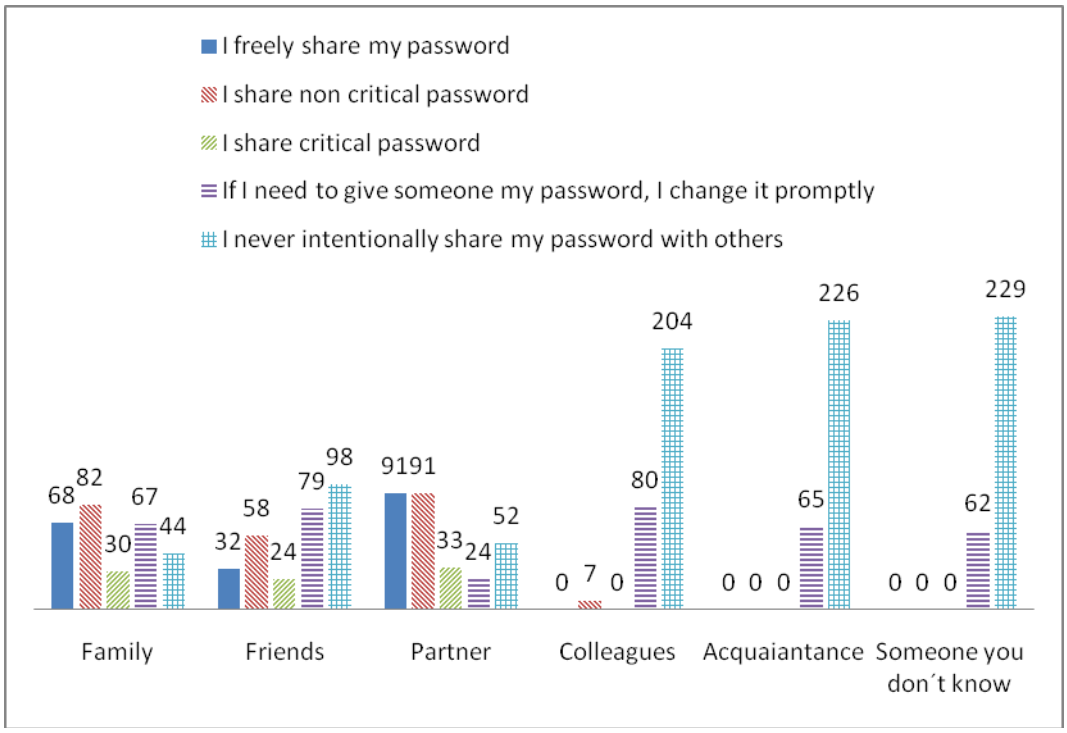
	I freely share my password	I share non critical password	I share critical password	If I need to give someone my password, I change it promptly	I never intentionally share my password with others
Family	16	15	16	94	150
Friends	15	7	20	109	140
Partner	87	95	46	38	25
Colleagues	0	4	0	8	279
Acquaiantance	0	2	0	6	283
Someone you don´t know	0	0	0	6	285



Question 12: To what extent do you share your computer password with:

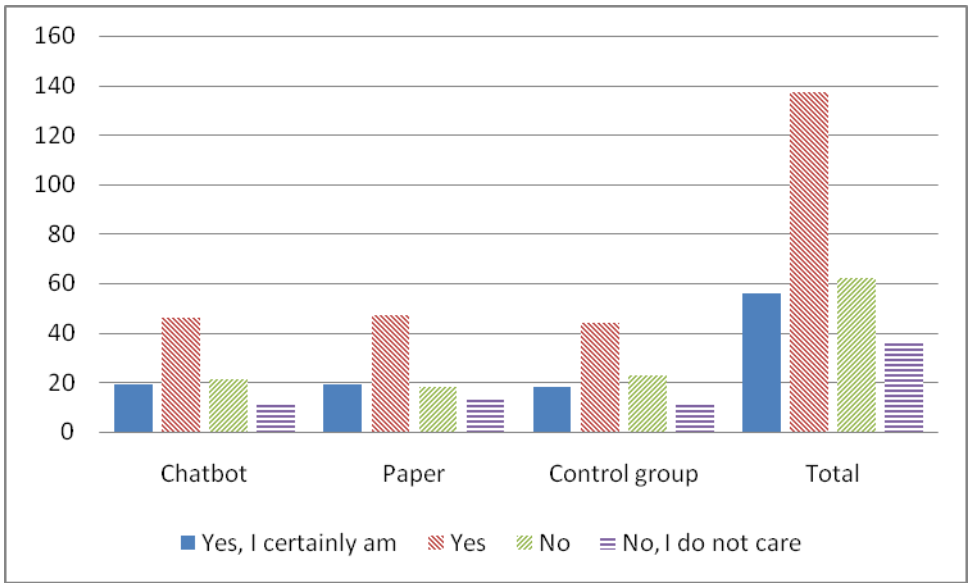
To what extent do you share your computer password with:		I freely share my password	I share non critical password	I share critical password	If I need to give someone my password, I change it promptly	I never intentionally share my password with others
Chatbot	Family	24	30	10	19	14
	Friends	8	18	8	29	34
	Partner	32	32	5	5	23
	Colleagues	0	2	0	27	68
	Acquaiantance	0	0	0	24	73
	Someone you don´t know	0	0	0	22	75
Paper	Family	21	25	11	25	15
	Friends	13	19	8	24	33
	Partner	28	31	15	11	12
	Colleagues	0	3	0	28	66
	Acquaiantance	0	0	0	21	76
	Someone you don´t know	0	0	0	20	77
Control group	Family	23	27	9	23	15
	Friends	11	21	8	26	31
	Partner	31	28	13	8	17
	Colleagues	0	2	0	25	70
	Acquaiantance	0	0	0	20	77
	Someone you don´t know	0	0	0	20	77

	I freely share my password	I share non critical password	I share critical password	If I need to give someone my password, I change it promptly	I never intentionally share my password with others
Family	68	82	30	67	44
Friends	32	58	24	79	98
Partner	91	91	33	24	52
Colleagues	0	7	0	80	204
Acquaiantance	0	0	0	65	226
Someone you don´t know	0	0	0	62	229



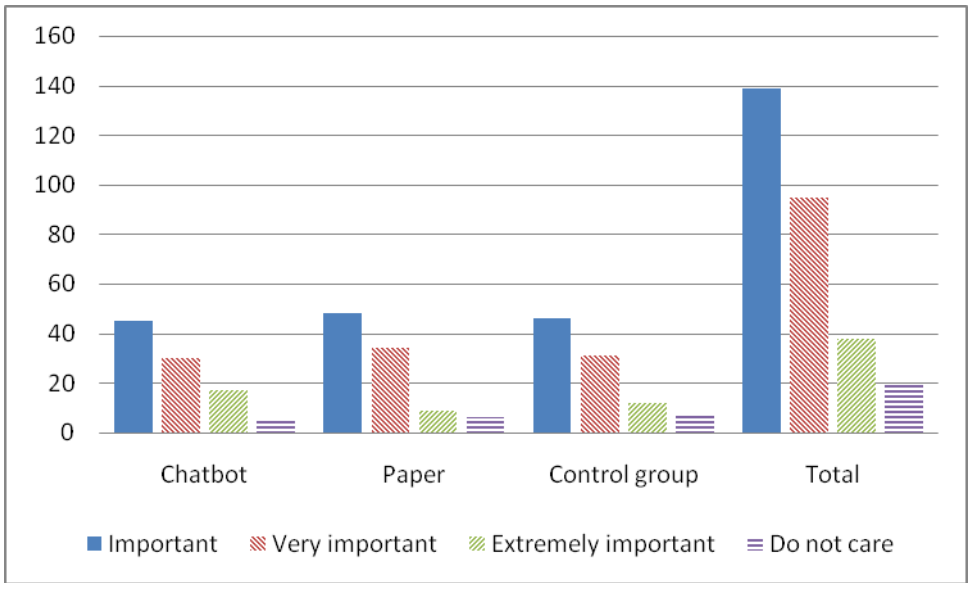
Question 13: Are you concerned about your computer security?

Concerned about computer security				
	Chatbot	Paper	Control group	Total
Yes, I certainly am	19	19	18	56
Yes	46	47	44	137
No	21	18	23	62
No, I do not care	11	13	12	36



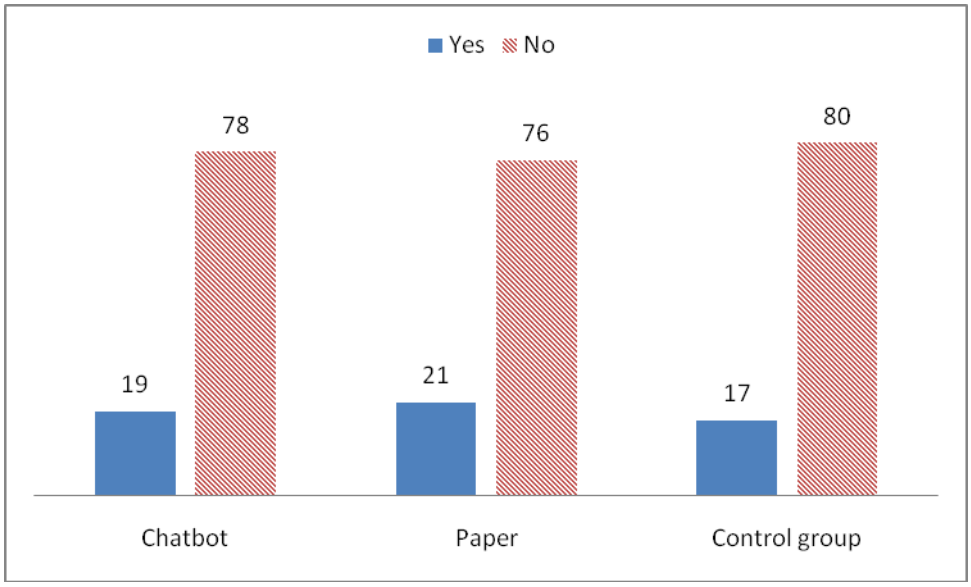
Question 14: How important is information security for you?

Information security				
	Chatbot	Paper	Control group	Total
Important	45	48	46	139
Very important	30	34	31	95
Extremely important	17	9	12	38
Do not care	5	6	8	19



Question 15: In a security context, do you know what Social Engineering is?

	Social Engineering			
	Chatbot	Paper	Control group	Total
Yes	19	21	17	57
No	78	76	80	234



Block 4 - Your considerations and abilities to discover frauds that are coming from the daily life.

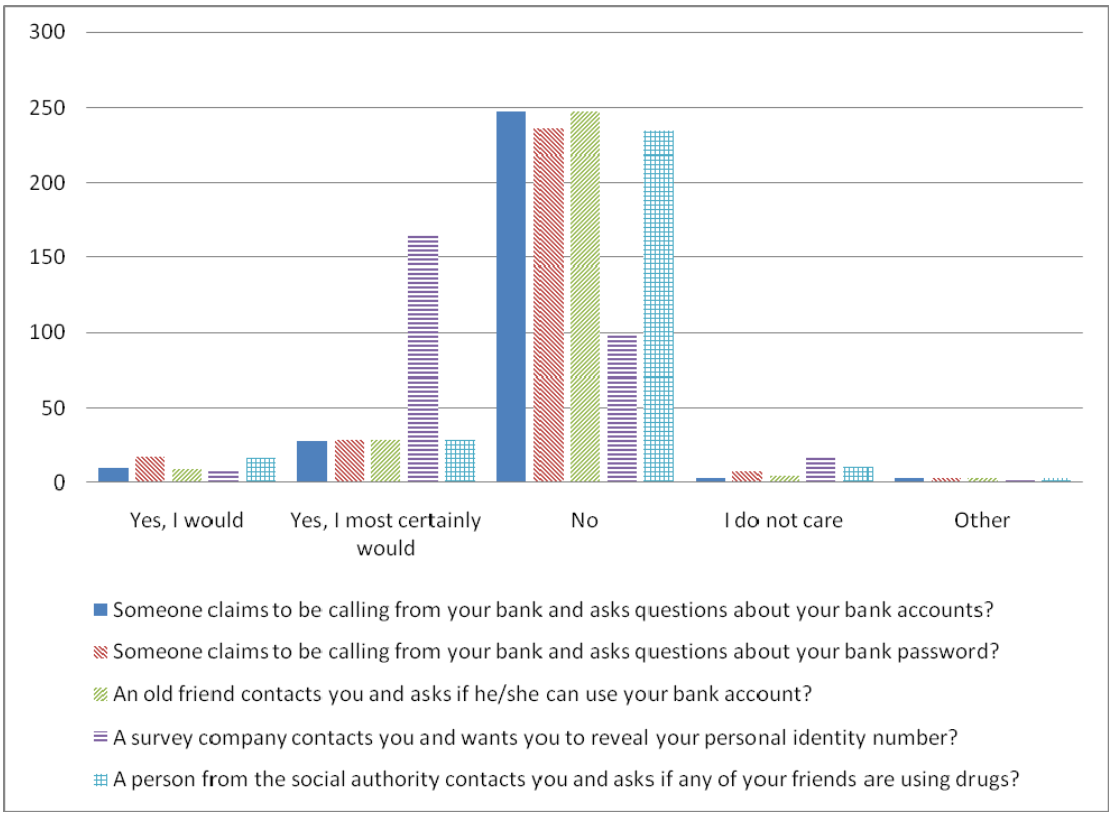
Question 16: Would you reveal sensitive information in the following circumstances:

		Someone claims to be calling from your bank and asks questions about your bank accounts?	Someone claims to be calling from your bank and asks questions about your bank password?	An old friend contacts you and asks if he/she can use your bank account?
Chatbot	Yes, I would	0	4	0
	Yes, I most certainly would	11	11	11
	No	82	78	82
	I do not care	1	1	1
	Other	3	3	3
Paper	Yes, I would	5	5	4
	Yes, I most certainly would	8	8	8
	No	83	83	84
	I do not care	1	1	1
	Other	0	0	0
Control group	Yes, I would	5	8	5
	Yes, I most certainly would	9	9	9
	No	82	75	81
	I do not care	1	5	2
	Other	0	0	0

A survey company contacts you and wants you to reveal your personal identity number?	A person from the social authority contacts you and asks if any of your friends are using drugs?

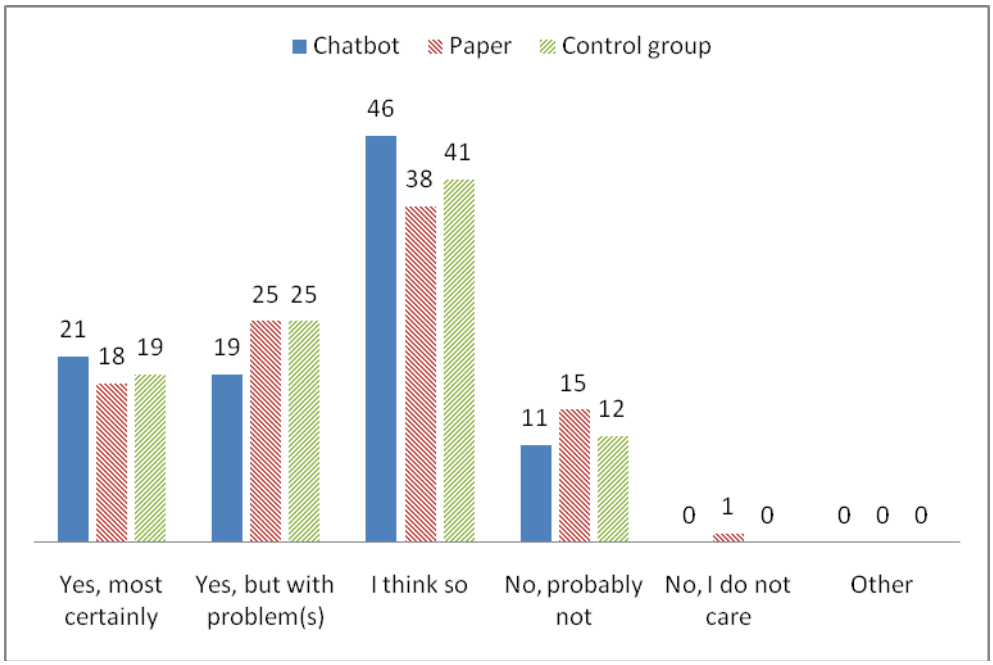
Chatbot	Yes, I would	0	0
	Yes, I most certainly would	56	11
	No	37	82
	I do not care	1	1
	Other	3	3
Paper	Yes, I would	6	8
	Yes, I most certainly would	62	8
	No	22	76
	I do not care	7	5
	Other	0	0
Control group	Yes, I would	2	8
	Yes, I most certainly would	48	9
	No	39	76
	I do not care	8	4
	Other	0	0

	Yes, I would	Yes, I most certainly would	No	I do not care	Other
Someone claims to be calling from your bank and asks questions about your bank accounts?	10	28	247	3	3
Someone claims to be calling from your bank and asks questions about your bank password?	17	28	236	7	3
An old friend contacts you and asks if he/she can use your bank account?	9	28	247	4	3
A survey company contacts you and wants you to reveal your personal identity number?	8	166	98	16	3
A person from the social authority contacts you and asks if any of your friends are using drugs?	16	28	234	10	3



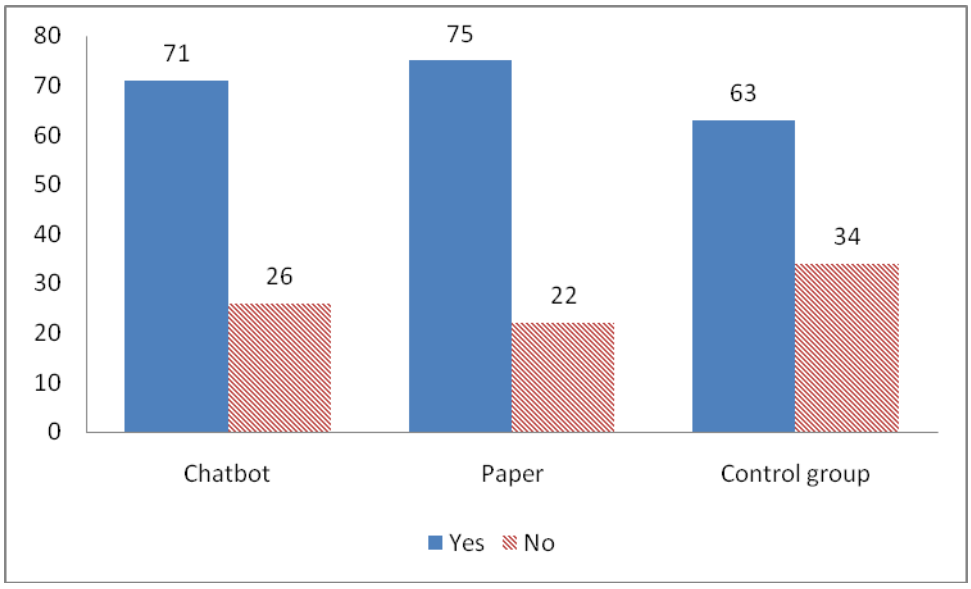
Question 17: Do you think you can recognize a fraud if you are exposed to it?

	Chatbot	Paper	Control group	Total
Yes, most certainly	21	18	19	58
Yes, but with problem(s)	19	25	25	69
I think so	46	38	41	125
No, probably not	11	15	12	38
No, I do not care	0	1	0	1
Other	0	0	0	0



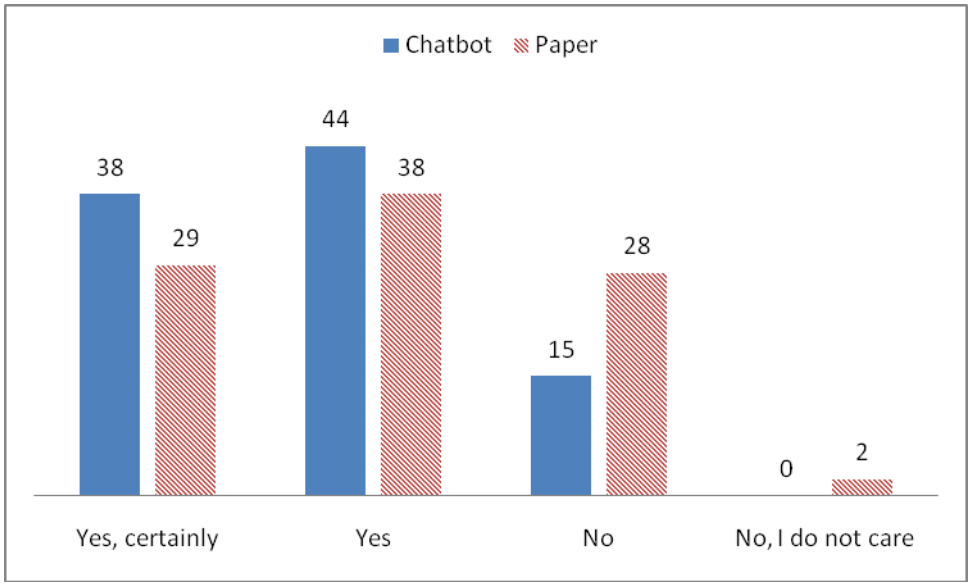
Question 18: Do you know what to do if a stranger calls and starts to ask questions?

	Chatbot	Paper	Control group	Total
Yes	71	75	63	209
No	26	22	34	82



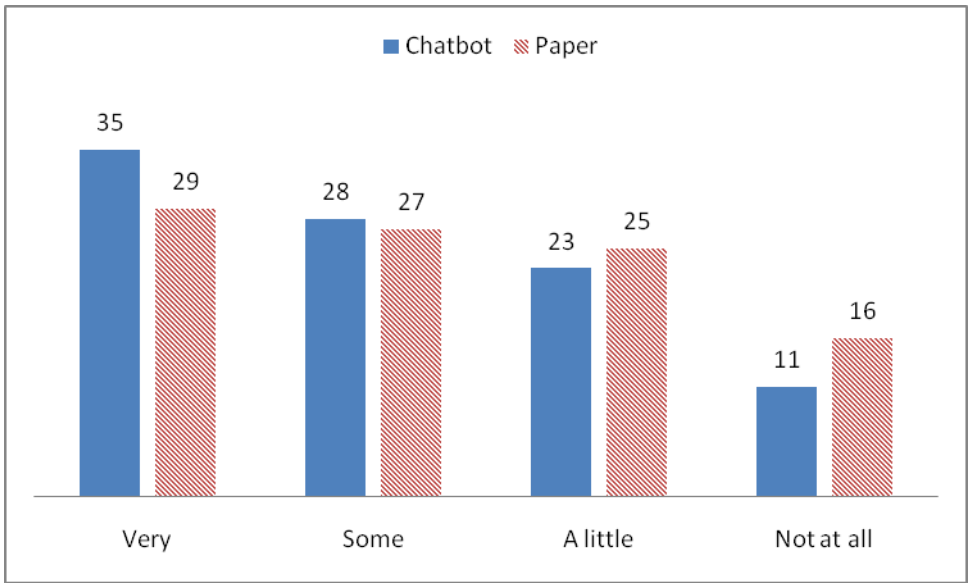
Question 19: Do you think that the knowledge you have obtained in this education will help you to be more conservative with leaving out information?

	Chatbot	Paper	Total
Yes, certainly	38	29	67
Yes	44	38	82
No	15	28	43
No, I do not care	0	2	2



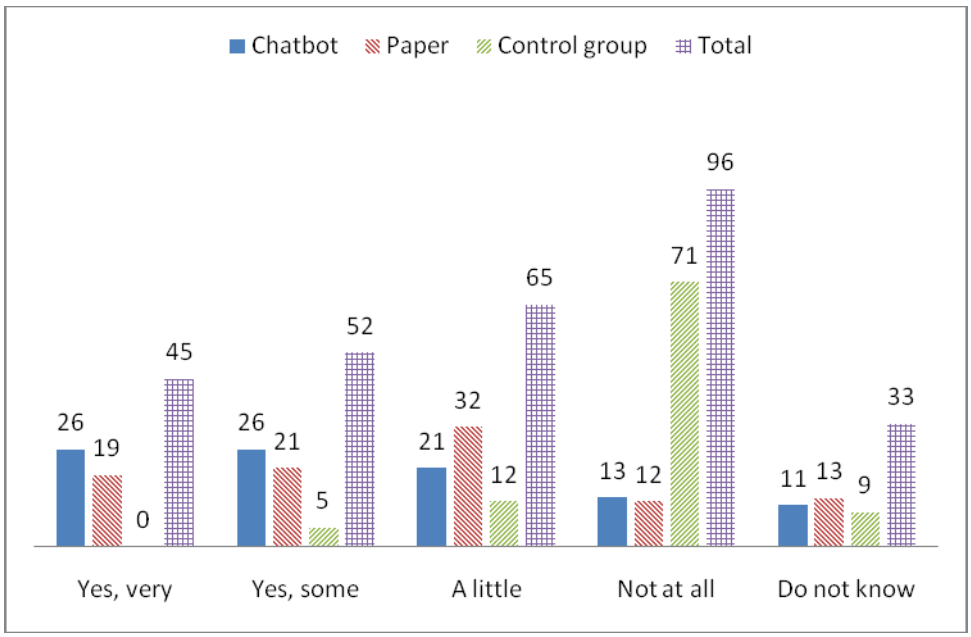
Question 20: Do you consider yourself be more conscious about security after this study?

	Chatbot	Paper	Total
Very	35	29	64
Some	28	27	55
A little	23	25	48
Not at all	11	16	27



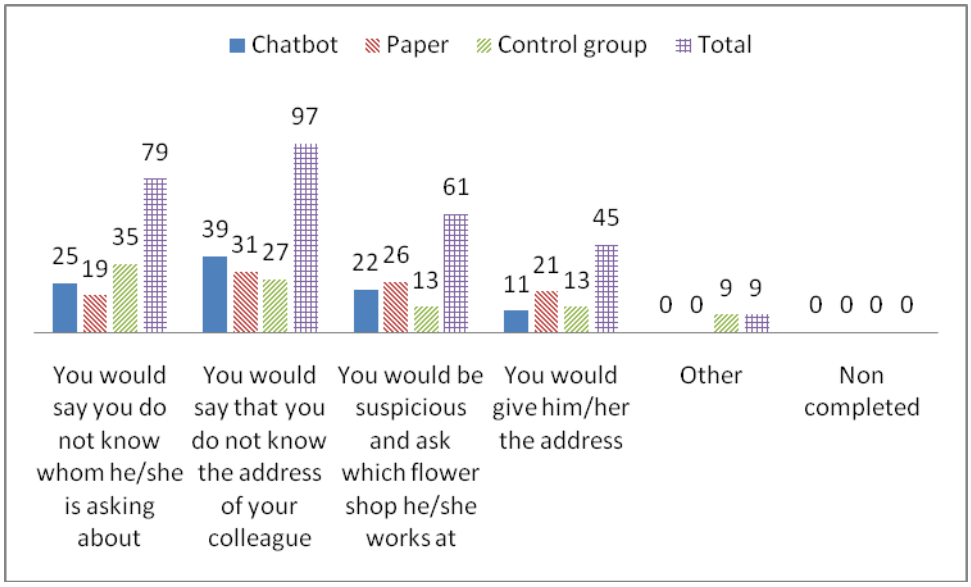
Question 21: Do you consider yourself to be better at discovering information stealing attempts after this education?

	Chatbot	Paper	Control group	Total
Yes, very	26	19	0	45
Yes, some	26	21	5	52
A little	21	32	12	65
Not at all	13	12	71	96
Do not know	11	13	9	



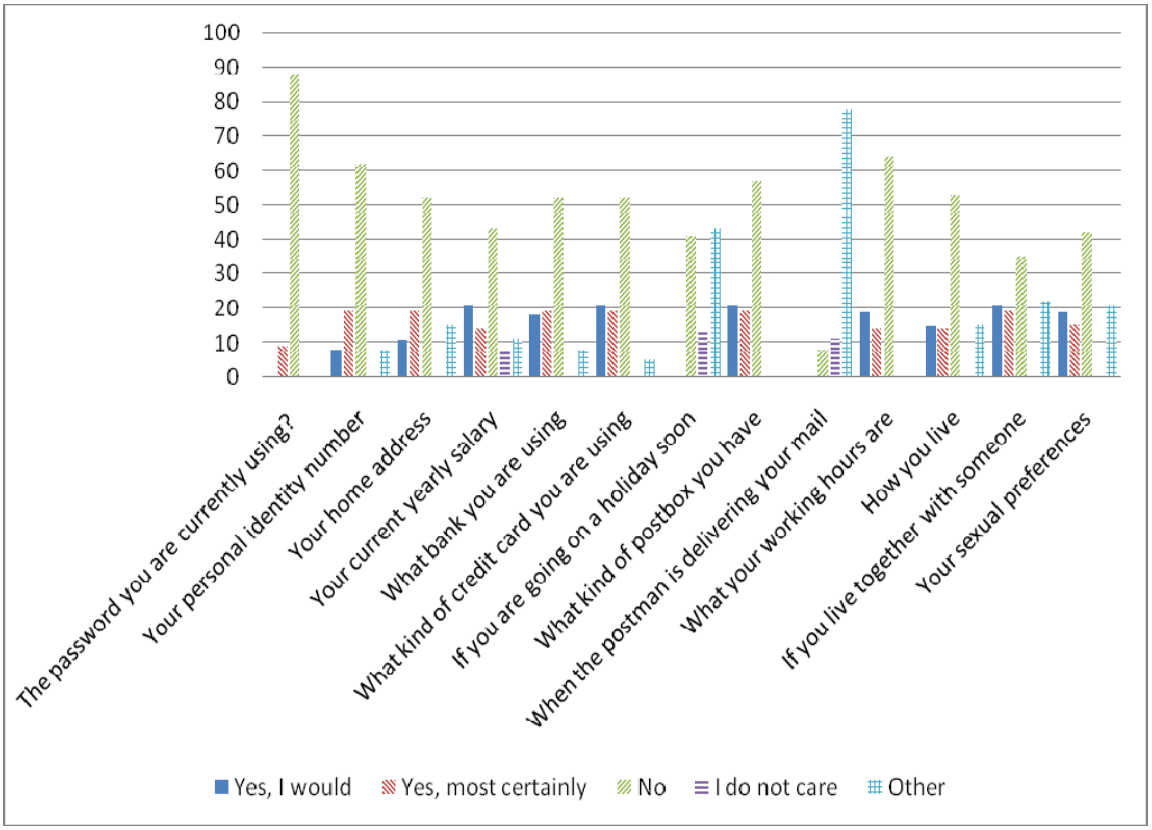
Question 22: Imagine the following scenario. You are at work and get a phone call on the office phone. The person phoning you claims to work at a flower shop. He/she wants to know the address of one of your colleagues for a flower delivery. How would you respond to this request?

	Chatbot	Paper	Control group	Total
You would say you do not know whom he/she is asking about	25	19	35	79
You would say that you do not know the address of your colleague	39	31	27	97
You would be suspicious and ask which flower shop he/she works at	22	26	13	61
You would give him/her the address	11	21	13	45
Other	0	0	9	9
Non completed	0	0	0	0

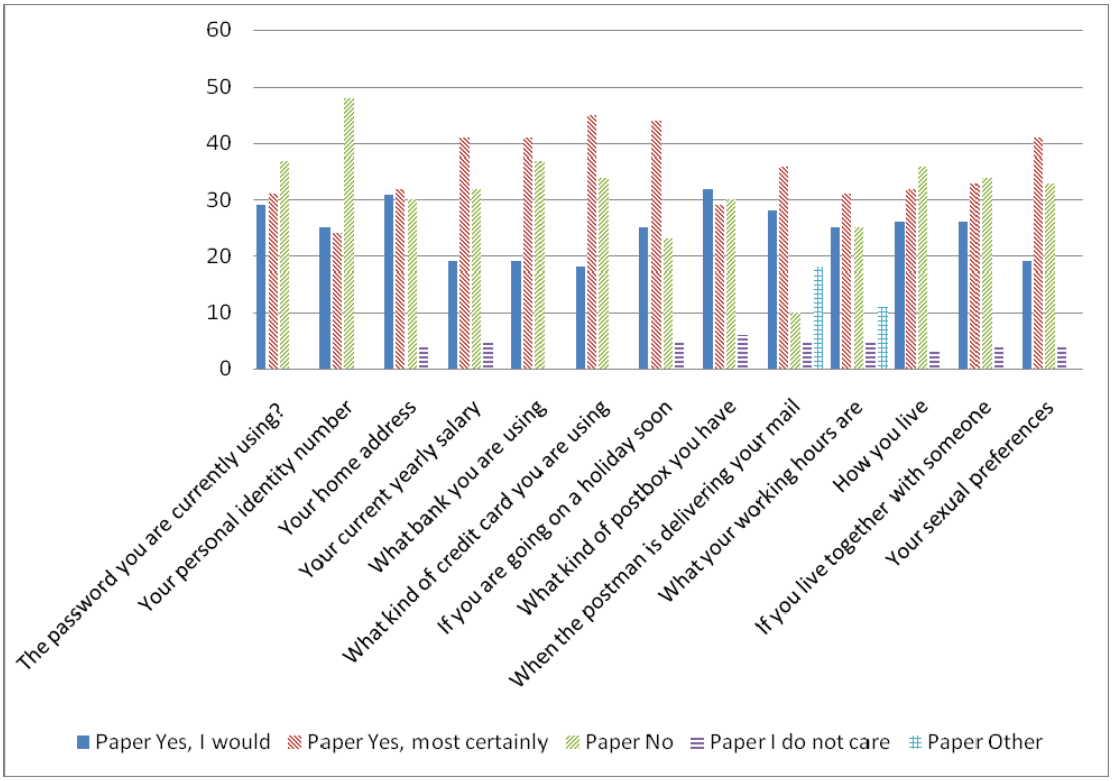


Question 23: Imagine the following scenario. You receive a phone call from a person who claims to be calling from a market survey institute. Would you reveal information about the following?

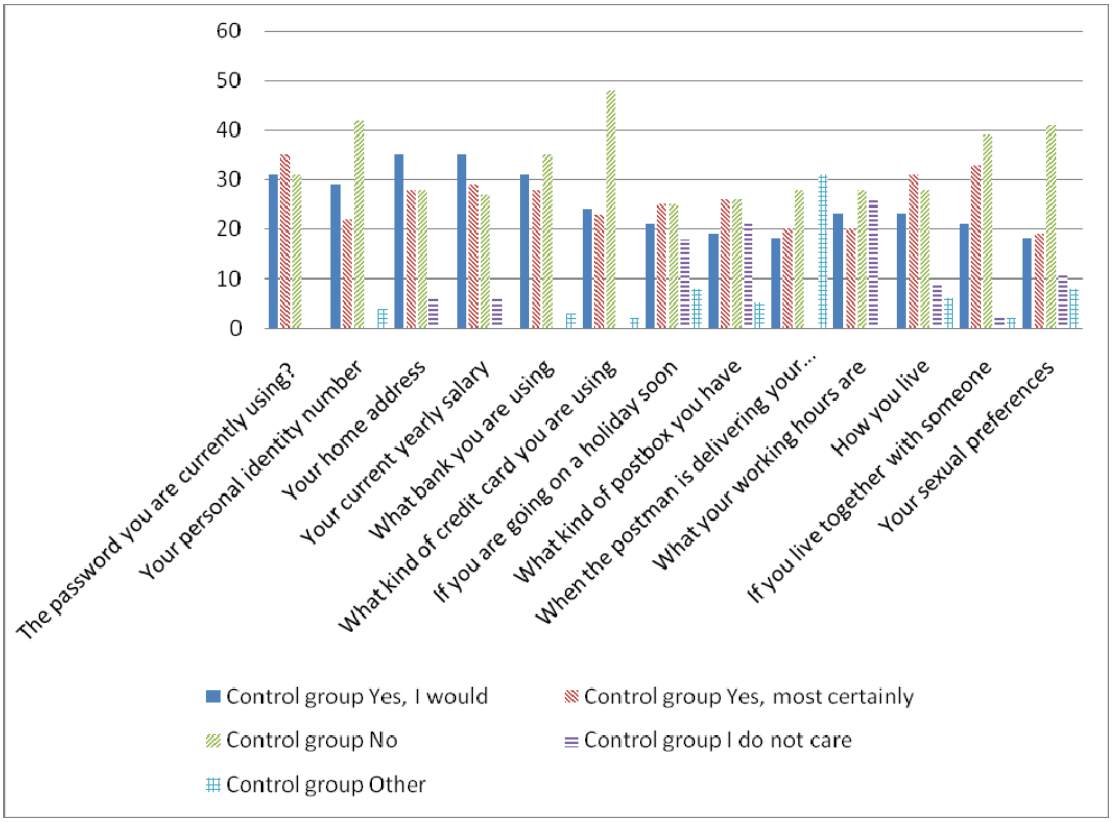
	Chatbot				
	Yes, I would	Yes, most certainly	No	I do not care	Other
The password you are currently using?	0	9	88	0	0
Your personal identity number	8	19	62	0	8
Your home address	11	19	52	0	15
Your current yearly salary	21	14	43	8	11
What bank you are using	18	19	52	0	8
What kind of credit card you are using	21	19	52	0	5
If you are going on a holiday soon	0	0	41	13	43
What kind of postbox you have	21	19	57	0	0
When the postman is delivering your mail	0	0	8	11	78
What your working hours are	19	14	64	0	0
How you live	15	14	53	0	15
If you live together with someone	21	19	35	0	22
Your sexual preferences	19	15	42	0	21


100
90
80
70
60
50
40
30
20
10
0
The password you are currently using?
Your personal identity number
Your home address
Your current yearly salary
What bank you are using
What kind of credit card you are using
If you are going on a holiday soon
What kind of postbox you have
When the postman is delivering your mail
What your working hours are
How you live
If you live together with someone
Your sexual preferences
Yes, I would
Yes, most certainly
No
I do not care
Other

	Paper				
	Yes, I would	Yes, most certainly	No	I do not care	Other
The password you are currently using?	29	31	37	0	0
Your personal identity number	25	24	48	0	0
Your home address	31	32	30	4	0
Your current yearly salary	19	41	32	5	0
What bank you are using	19	41	37	0	0
What kind of credit card you are using	18	45	34	0	0
If you are going on a holiday soon	25	44	23	5	0
What kind of postbox you have	32	29	30	6	0
When the postman is delivering your mail	28	36	10	5	18
What your working hours are	25	31	25	5	11
How you live	26	32	36	3	0
If you live together with someone	26	33	34	4	0
Your sexual preferences	19	41	33	4	0


60
50
40
30
20
10
0
The password you are currently using?
Your personal identity number
Your home address
Your current yearly salary
What bank you are using
What kind of credit card you are using
If you are going on a holiday soon
What kind of postbox you have
When the postman is delivering your mail
What your working hours are
How you live
If you live together with someone
Your sexual preferences
Paper Yes, I would
Paper Yes, most certainly
Paper No
Paper I do not care
Paper Other

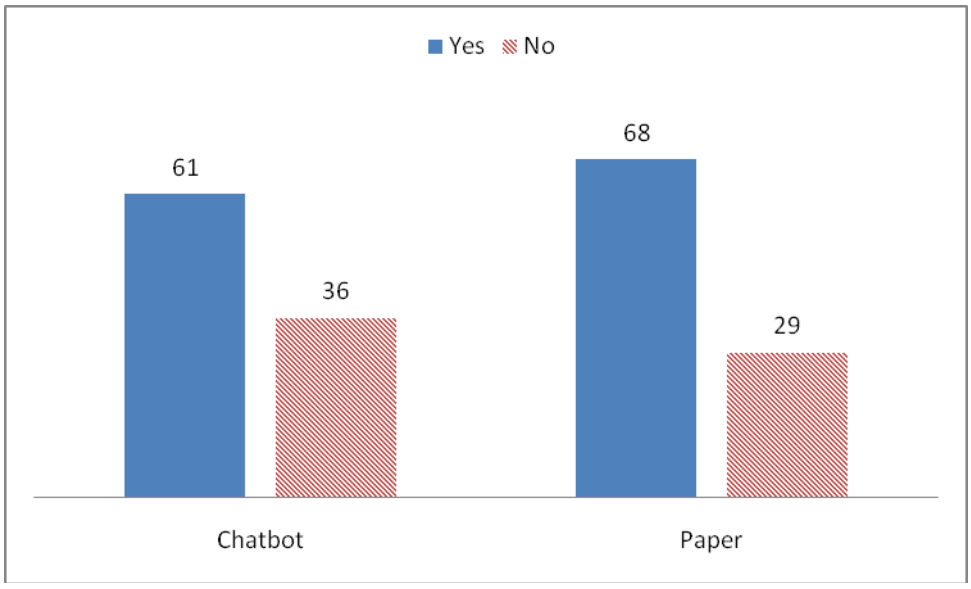
	Control group				
	Yes, I would	Yes, most certainly	No	I do not care	Other
The password you are currently using?	31	35	31	0	0
Your personal identity number	29	22	42	0	4
Your home address	35	28	28	6	0
Your current yearly salary	35	29	27	6	0
What bank you are using	31	28	35	0	3
What kind of credit card you are using	24	23	48	0	2
If you are going on a holiday soon	21	25	25	18	8
What kind of postbox you have	19	26	26	21	5
When the postman is delivering your mail	18	20	28	0	31
What your working hours are	23	20	28	26	0
How you live	23	31	28	9	6
If you live together with someone	21	33	39	2	2
Your sexual preferences	18	19	41	11	8



Block 5 - Your opinion about the educational method.

Question 24: Do you think that this education has been useful for you?

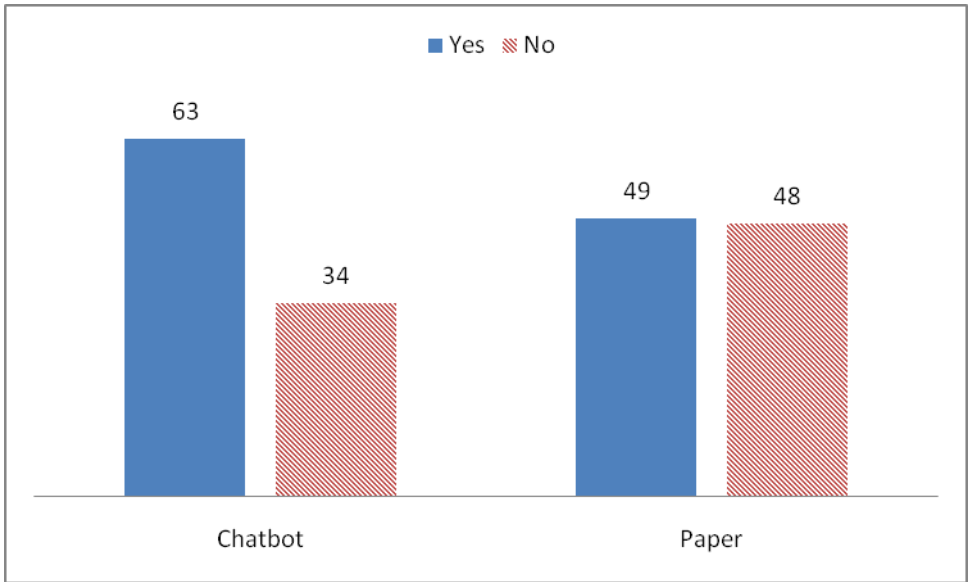
	Chatbot	Paper
Yes	61	68
No	36	29



Question 25: Do you think this kind of education method is good?

	Chatbot	Paper
Yes	63	49
No	34	48

Comments: The educational concept is good

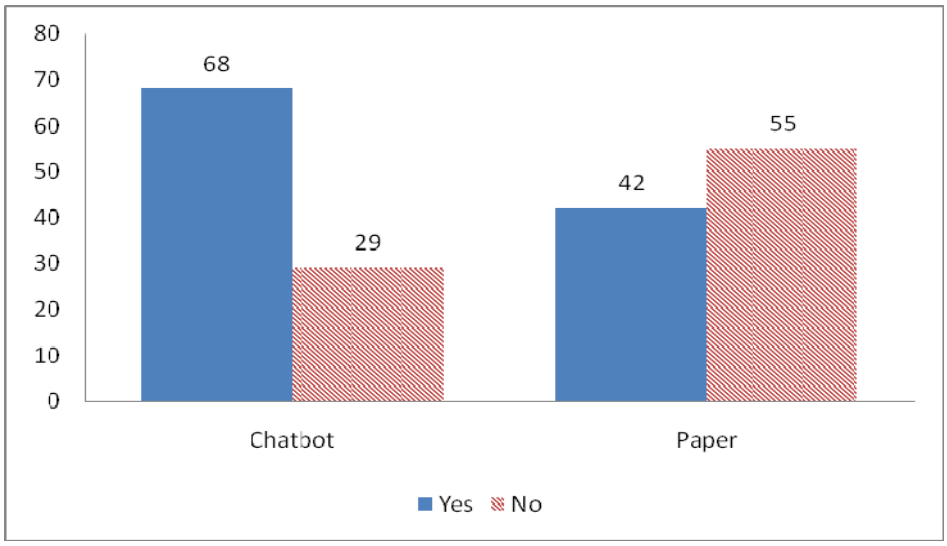


Question 26 for Chatbot: Is the chatbot a better educational method than reading a fraud case from a paper?

	Chatbot
Yes	68
No	29

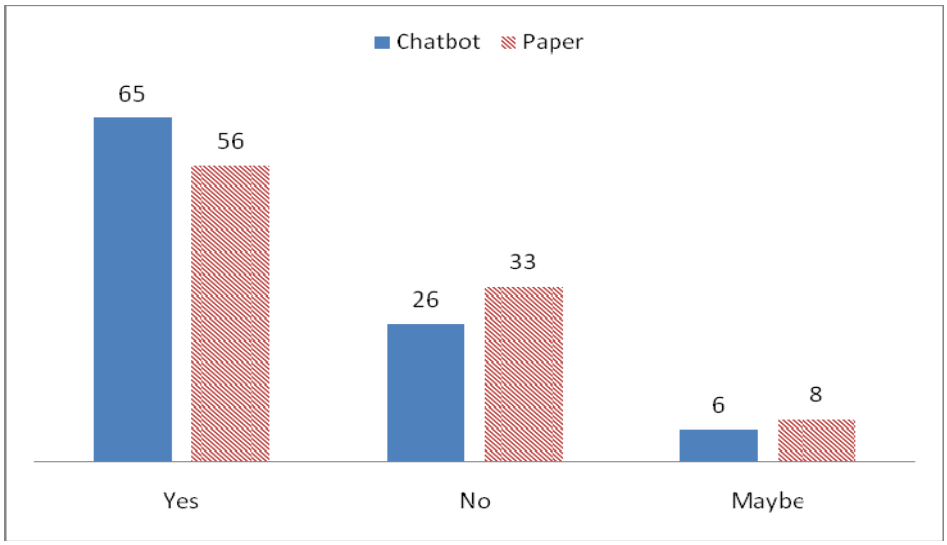
Question 26 for a written informational text: Is reading a paper with a fraud case a better educational method than using interactive learning?

	Paper
Yes	42
No	55



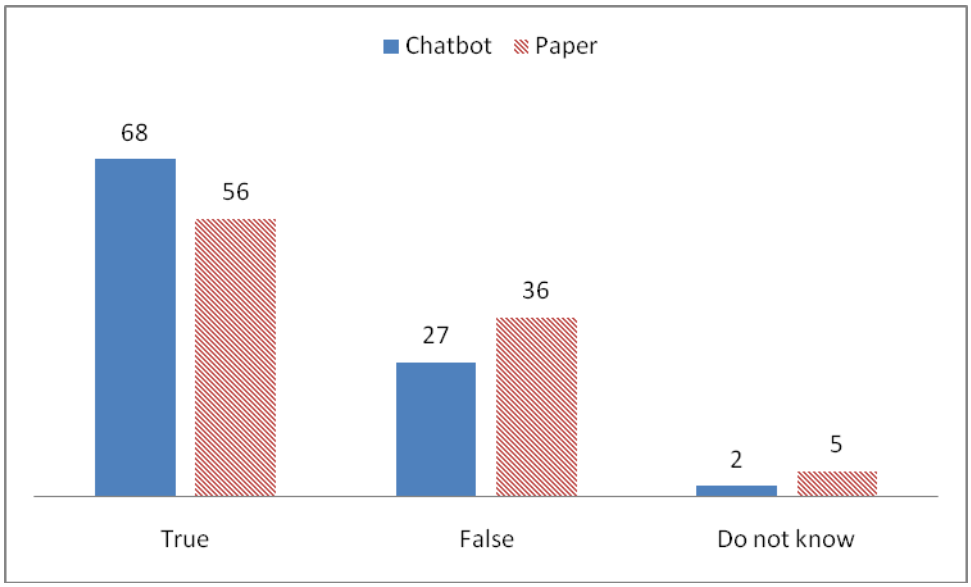
Question 27: Information security is a subject that ranges from data protection to digital locks. Is information security something that you believe is important in your work or in your future work?

	Chatbot	Paper
Yes	65	56
No	26	33
Maybe	6	8



Question 28: In your occupation or in your future occupation, you may handle information that should be kept from other persons. Is the security of this information your personal responsibility?

	Chatbot	Paper
True	68	56
False	27	36
Do not know	2	5

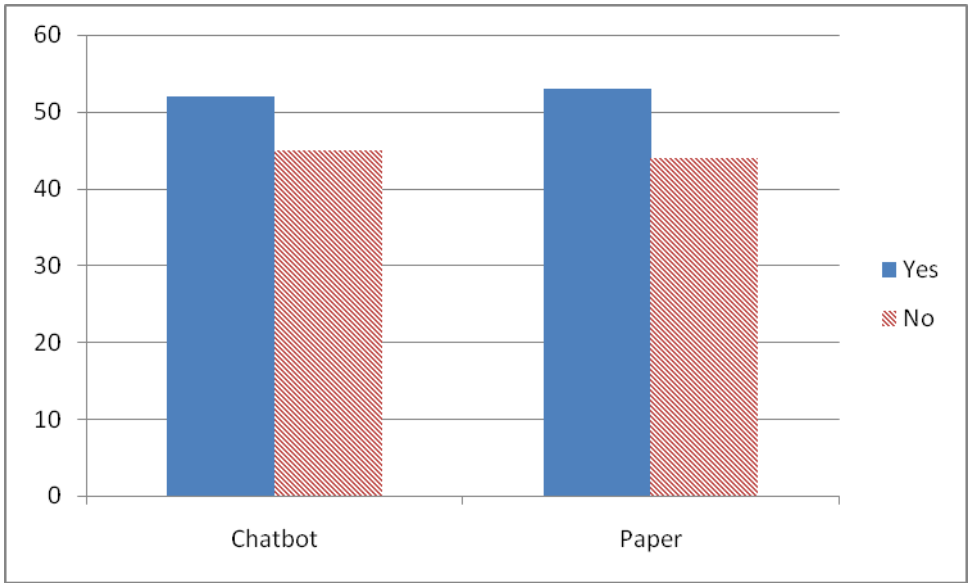


Question 29 for Chatbot: Do you think that the educational method by using a chatbot is the most useful method for educational purposes?

	Chatbot
Yes	52
No	45

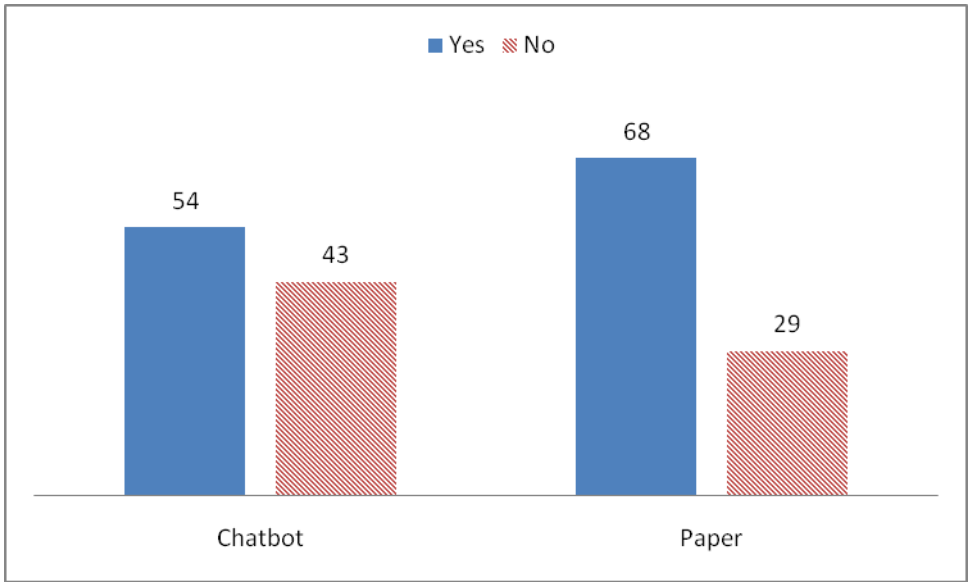
Question 29 for a written informational text: Do you think that the educational method by reading a fraud case is the most useful method for education?

	Paper
Yes	53
No	44



Question 30: Is interactive learning a possible educational approach for identifying thefts?

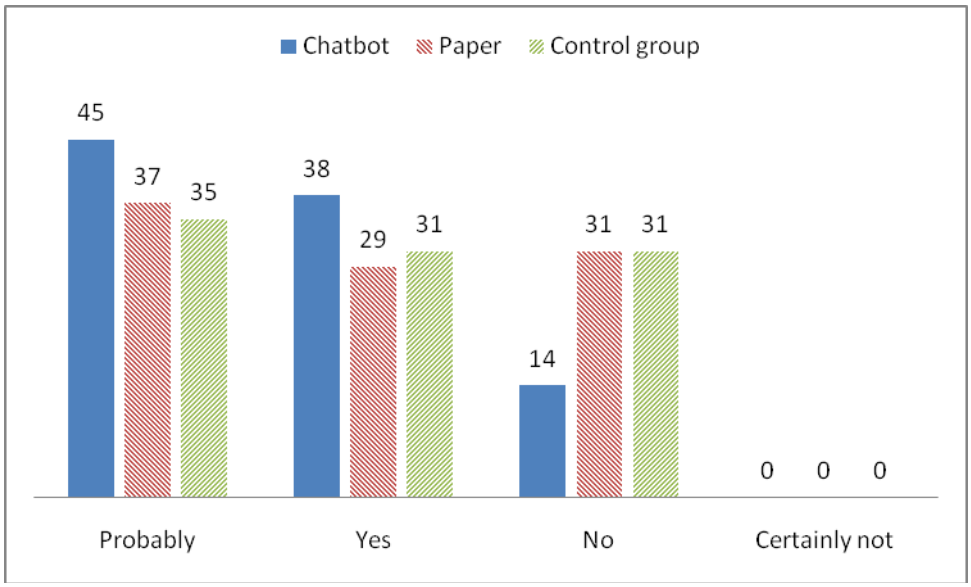
	Chatbot	Paper
Yes	54	68
No	43	29



Block 6 - Do you believe your ability has increased.

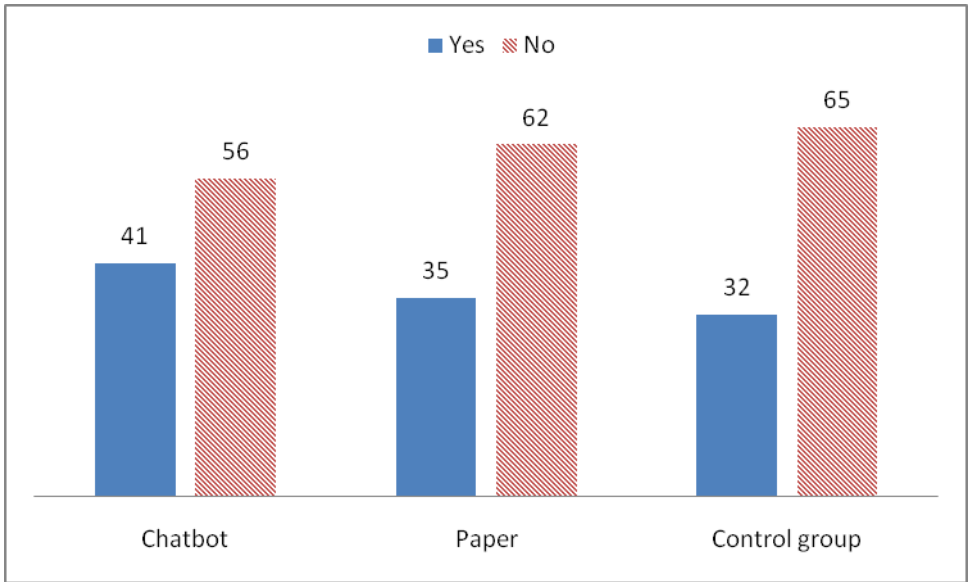
Question 31: Do you think that you could be subjected to identity theft?

	Chatbot	Paper	Control group
Probably	45	37	35
Yes	38	29	31
No	14	31	31
Certainly not	0	0	0



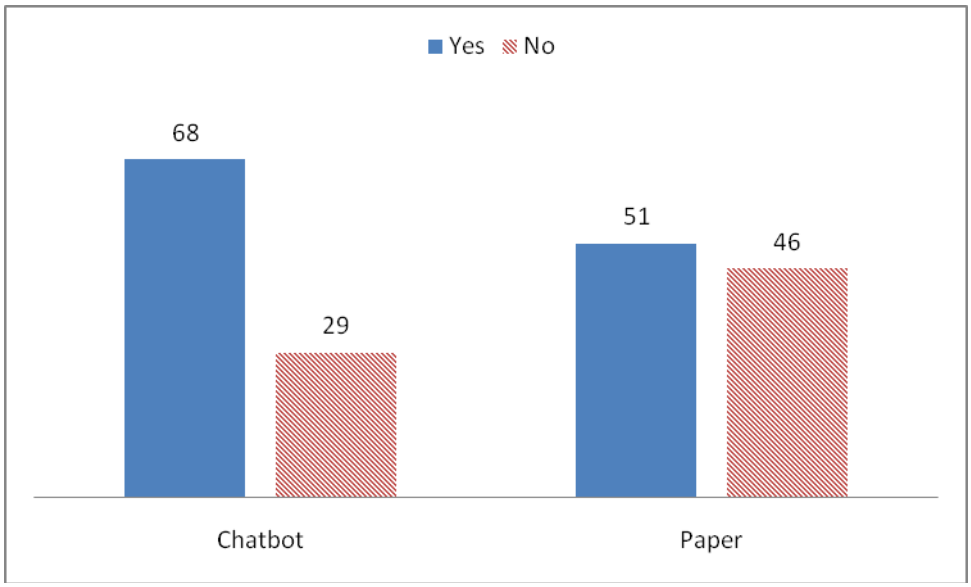
Question 32: Is identity theft something that worries you?

	Chatbot	Paper	Control group
Yes	41	35	32
No	56	62	65



Question 33: Do you think that you will be better prepared to prevent identity thefts from being subjected to you after this education?

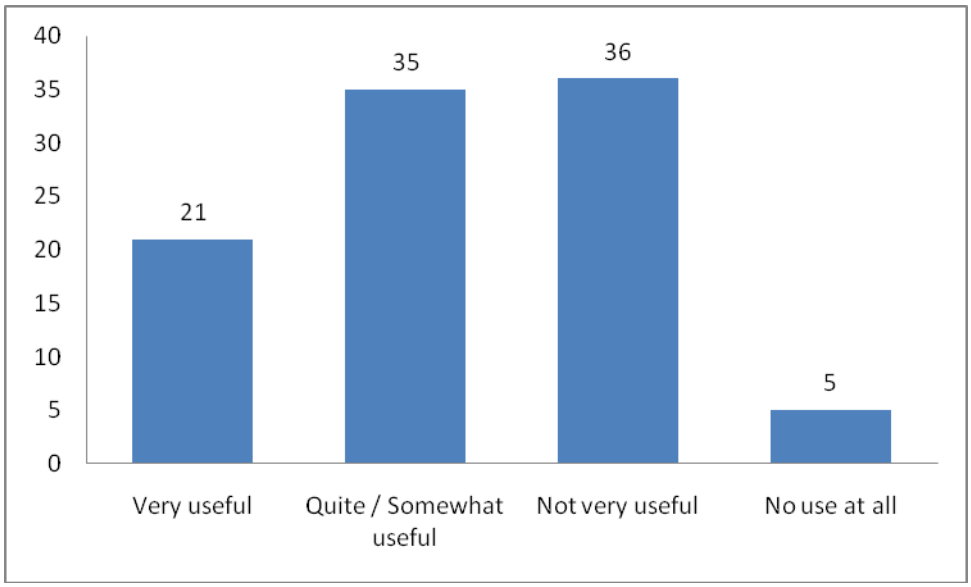
	Chatbot	Paper
Yes	68	51
No	29	46



Block 7 - Your opinion on the

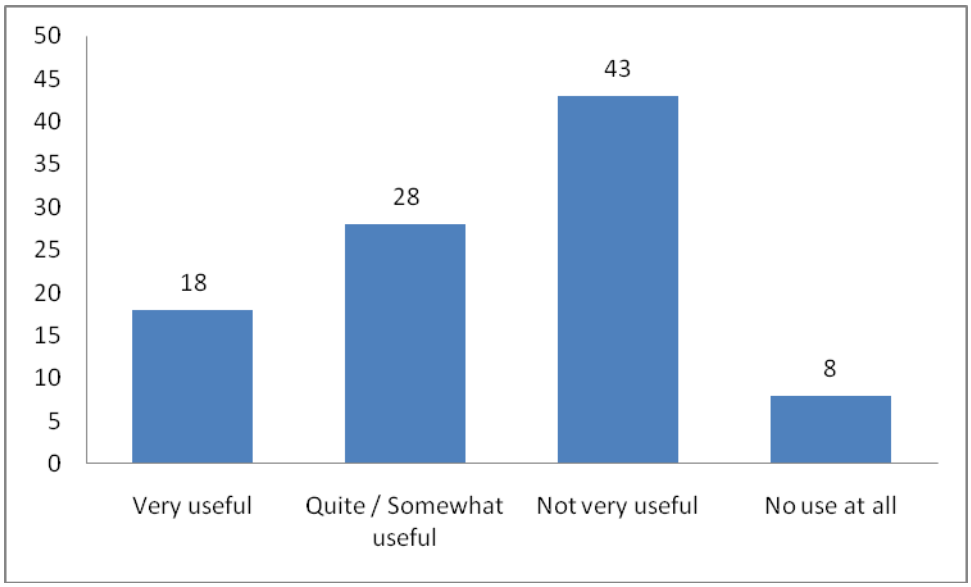
Question 34 for Chatbot: How useful would you say the chatbot was/is?

	Chatbot
Very useful	21
Quite / Somewhat useful	35
Not very useful	36
No use at all	5



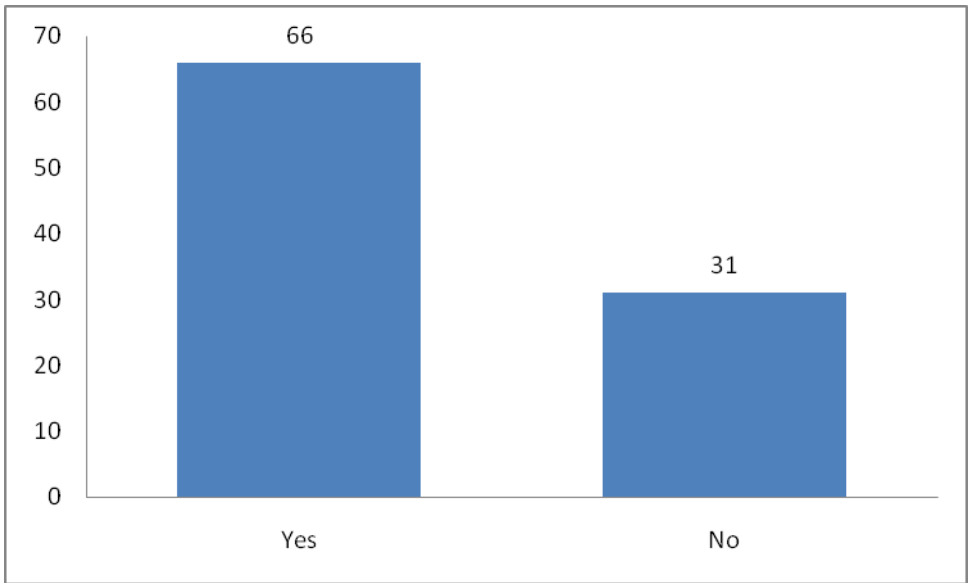
Question 34 for a written informational text: How useful would you say the a written informational text was/is?

	Paper
Very useful	18
Quite / Somewhat useful	28
Not very useful	43
No use at all	8



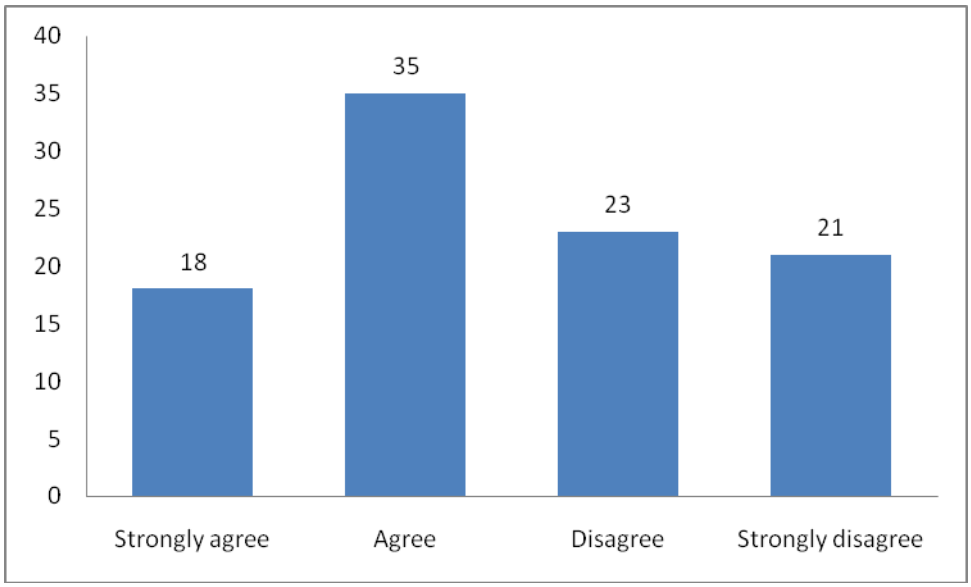
Question 35 for Chatbot: Would you want to use a chatbot for your own education in the future?

	Chatbot
Yes	66
No	31



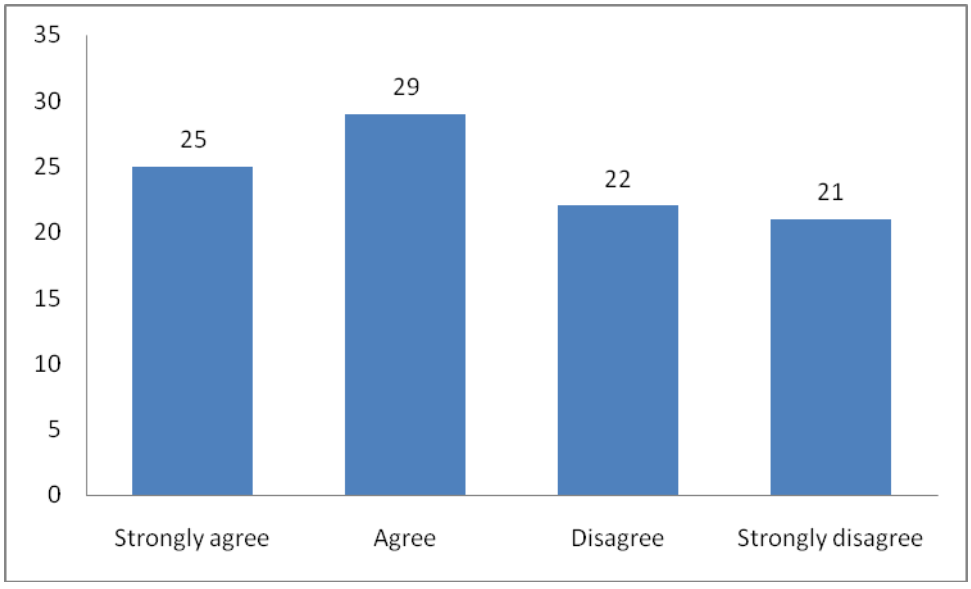
Question 35 for a written informational text: Do you feel that this paper had a positive effect on your learning experience?

	Paper
Strongly agree	18
Agree	35
Disagree	23
Strongly disagree	21



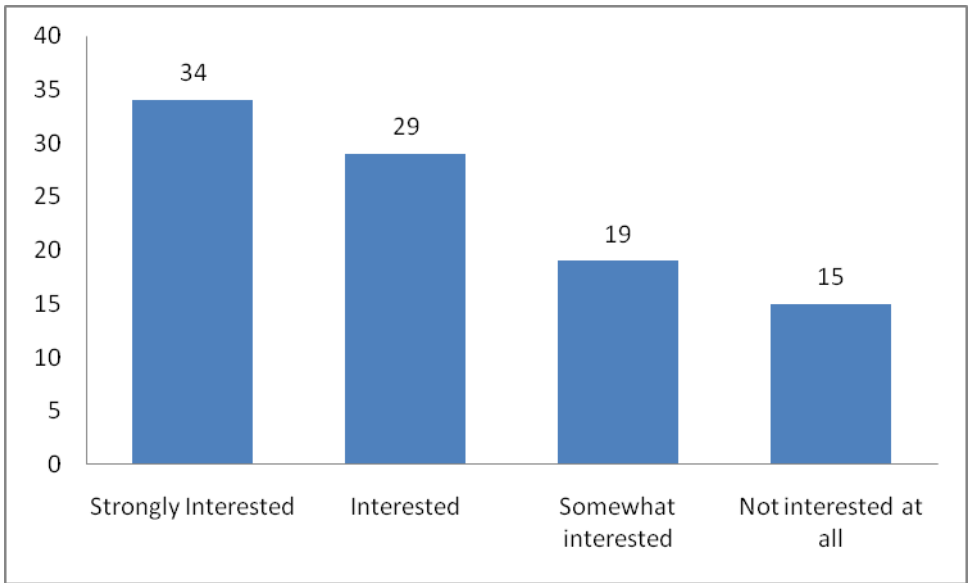
Question 36 for Chatbot: Do you feel that you have gained more knowledge by interacting with a Chatbot, than by reading a fraud case on paper?

	Chatbot
Strongly agree	25
Agree	29
Disagree	22
Strongly disagree	21



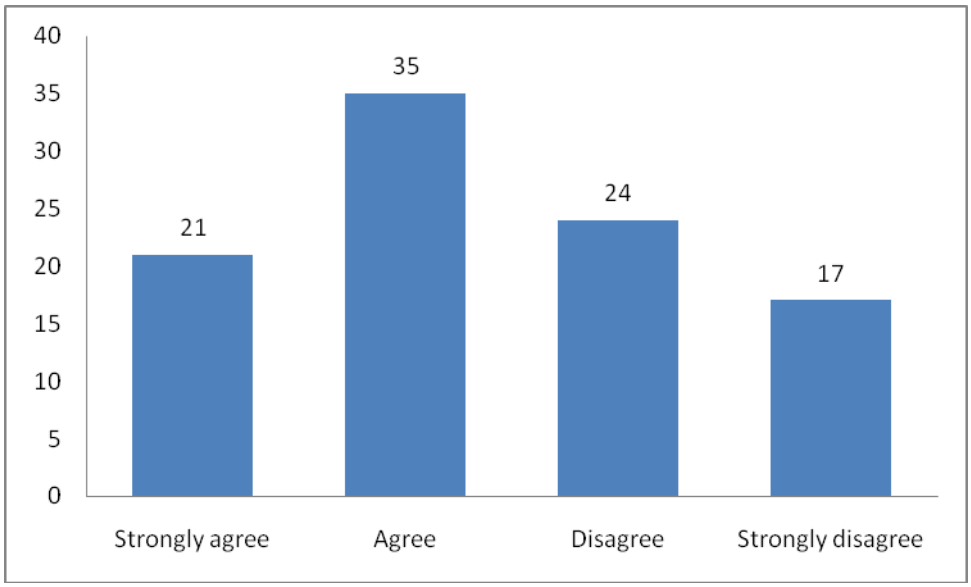
Question 36 for a written informational text: Would you be interested in receiving training through other approaches, for example a computer program that lets you experiences an identity theft attack?

	Paper
Strongly Interested	34
Interested	29
Somewhat interested	19
Not interested at all	15



Question 37 for Chatbot: Do you feel that the Chatbot had a positive effect on your learning experience?

	Chatbot
Strongly agree	21
Agree	35
Disagree	24
Strongly disagree	17



Question 38 for Chatbot: Do you feel that the chatbot simulation of an identity theft attack is believable?

	Chatbot
Strongly agree	5
Agree	46
Disagree	35
Strongly disagree	11