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

ITC70LT

Sten Mäses

EVALUATION METHOD FOR HUMAN ASPECTS OF INFORMATION SECURITY

Master thesis

Supervisor:
Aare Klooster MSc

Co-supervisors:
Rain Ottis PhD
Liina Randmann PhD

Tallinn 2015

Author Declaration

I hereby declare that this thesis is the result of my own research except as cited in the references. The thesis has not been submitted for any other degree.

Sten Mäses

….. …..

(date) (signature)

List of Acronyms and Abbreviations

HAIS – Human aspects of information security

HAIS-Q – Human aspects of information security questionnaire

KAB model – model of knowledge, attitude and behaviour

SD – Standard deviation

TPB – Theory of planned behaviour

U.S. – The United States of America

Abstract

It is increasingly acknowledged that an organisation's approach to information security should focus on employee behaviour, as many threats to an organisation's computer systems can be attributed to the human factor in information security. In order to reduce the risk related to it, a fast and affordable evaluation method is needed, that would enable employees to get actionable feedback regarding their weaknesses. Various approaches exist addressing the assessment of human factor, but they are either too narrow, too shallow or too expensive and time consuming.

The objective of this paper is to propose an evaluation method for human aspects of information security that uses an online framework in order to give employees fast and personalised feedback based on their self-reported knowledge, attitude and behaviour across different focus areas. An empirical study is performed to aid in validating the proposed evaluation method for human aspects of information security. Results from 108 respondents indicate that the method proves to be valid and usable as a basis for improving human aspects of information security by giving employees actionable feedback based on their self-reported behaviour. Ideas for future research to further develop and test this evaluation method for human aspects of information security are outlined.

This thesis is written in English and is 56 pages long, including 5 main chapters and 3 appendices, 12 figures and 11 tables.

Annotatsioon

Infoturbe inimfaktori hindamismeetod

Võimalused inimloomust suhteliselt lihtsalt ärakasutada on tekitanud olukorra, kus mitmed ründed keskenduvad inimfaktori nõrkustele. Selleks, et vähendada infoturbe inimfaktoriga seonduvaid riske, on tarvis kiiret ning odavat meetodit, mis võimaldaks töötajatel oma turvateadlikku käitumist hinnata. Erinevad infoturbe inimfaktori hindamismeetodid juba eksisteerivad, kuid on liiga kitsad, liiga pealiskaudsed või liiga ressursimahukad. Ettevõtted ja organisatsioonid vajavad usaldusväärset meetodit, mis võimaldaks töötajate seas turvateadlikku käitumist propageerida.

Antud töö eesmärgiks on esitleda üht võimalikku meetodit, mis võimaldab töötajatel hinnata oma infoturbega seonduvaid teadmisi, suhtumist ja käitumist erinevate valdkondade lõikes. Meetodis kasutatav ja selle tarbeks spetsiaalselt arendatud interaktiivne veebipõhine test annab testi sooritajale kohese tagasiside loetledes üles tema hinnangulised tugevused ja nõrkused. Lisaks kuvatakse testi läbinud töötajale soovitused edasiseks turvateadliku käitumise parendamiseks.

Meetodi kontrollimiseks viidi läbi mitu testivooru kokku 140 inimesega. Viimases voorus läbisid testi 108 töötajat, kelle tulemuste analüüs kinnitab meetodi usaldusväärsust ning sobivust kasutamiseks turvateadlikku käitumise propageerimisel. Lisaks on töös ära toodud ideed edasisteks uuringuteks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 56 leheküljel, 5 peatükki ning 3 lisa, 12 joonist, 11 tabelit.

Table of Contents

1. Introduction

1.1. General Background

Laziness is built deep into the nature of humans. If there are several ways of achieving the same goal, people will eventually gravitate to the least demanding course of action. [1] Implementing security measures requires extra effort. Therefore the security guidelines are often only partially followed or completely bypassed, diminishing the value of technological security solutions that require human interaction [2].

Furthermore, humans by nature can't analyse every decision fully [3] and are not adept at making rational and systematic security trade-offs. Instead, we have shortcuts, rules of thumb, stereotypes, and biases – generally known as "heuristics". [4] Attackers try to take advantage of this, using a variety of influence methods to force their victims to operate in a heuristic mode and therefore having much less access to their psychological defences. [5] These kind of attacks against the human factor in information security are often called social engineering – skilfully maneuvering human beings to take action in some aspect of their lives. [6]

All these mentioned vulnerabilities of humans have brought us to a situation where human factor is the weakest link of information security [7] and consistently under attack [8]. Many organisations and researchers have realised the seriousness of this threat [9] and therefore multiple ways to mitigate this risk have been worked out. In general, there are four main ways to manage risk: risk avoidance, risk transfer, risk retention and risk reduction [10]. When it comes to managing threats to human aspects of information security such as social engineering [11], then in most cases it is not realistic to avoid the risk. In order to remove human aspect from information systems, an autonomous computer system should be developed. Without interacting with humans most systems lose their value and therefore it is not suitable to avoid human factor entirely. Risk transfer and risk retention by definition do not help to solve the essence of the threat. They only help to give a systematic approach how to deal with the risk without addressing the core issue.

Risk reduction deals more with the source of the risk trying to lessen the probability and/or negative consequences associated with the risk. Technical measures are often used, but they have only a limited effect due to the mentioned vulnerabilities of humans [12]. According to the notorious social engineer and security trainer Kevin Mitnick [13] the only way to mitigate the threat of social engineering is to have a trained and security aware workforce. [7]

In order for the employees to be security aware they have to realise that that IT security is critical because a security failure has potentially adverse consequences for everyone [14]. To improve their behaviour it would be beneficial to go through an evaluation process that would give feedback about the strengths and weaknesses of employees. This kind of evaluation process is often part of a security audit [15]. A thorough security audit can give valuable metrics that help evaluate risks and take decisions accordingly, but the auditing process can be very time consuming and expensive. [16]

1.2. Problem Statement

The weakness of human factor of information security (HAIS) endangers the overall security of every organisation [7]. In order to reduce the risk related to it, a fast and affordable evaluation method is needed that would enable employees to get actionable feedback about their weaknesses related to HAIS.

A formal security audit can be used for the evaluation of HAIS, but it is often both time consuming and too expensive for regular security checks [17]. In addition it requires special attention to avoid ethical and legal misunderstandings (e.g. damage done during a penetration test) [18].

To sum up, the main problems addressed by this thesis are:

1. lack of information security due to human vulnerabilities,
2. available evaluation methods for human aspects of information security are expensive and time consuming.

1.3. Contribution of the Author

The goal of this thesis is to develop an evaluation method for human aspects of information security (HAIS) that would be based on solid scientific research, and also relatively fast and cheap to implement.

The contribution of the author is the following:

- developing an empirically validated evaluation method for human aspects of information security, implemented in an online framework that provides employees with personalised and actionable feedback.

The evaluation method was tested and compared with similar research in order to ensure its validity. The resulting method may be used in various ways, e.g.

- to raise general awareness regarding human aspects of information security,
- to be used for self-assessment during cybersecurity trainings.

1.4. Outline of the Thesis

The goal of this thesis is to produce a low-cost, fast and empirically validated method for evaluating people in their working environment (employees) in terms of information security. The main part of this paper is organised as follows:

- Chapter 1. Introduction – gives a general overview and introduction to the topic.
- Chapter 2. Analysis of the Current Situation – defines the scope of this study, analyses the current situation and highlights the gap in evaluation methods.
- Chapter 3. Methodology – goes through the underlying methodology and design process of the evaluation method.
- Chapter 4. Application / Implementation – describes the implementation of the

evaluation method and the according results.

- Chapter 5. Discussion and Conclusions – provides additional discussion regarding the results and the method, and also ideas for further research.

2. Analysis of the Current Situation

In this chapter the term “security awareness” is defined for the current context. Also the choice of the measurement technique is being discussed and an overview of the related background is given regarding information security surveys and online quizzes.

2.1. Defining Security Awareness

“*What then is security awareness?*
If no one asks me, I know what it is.
If I wish to explain it to him who asks, I do not know.”
Paraphrasing Saint Augustine of Hippo [19]

One of the central terms in the field of human aspects of information security is “security awareness”. Although researchers and practitioners exercise ongoing efforts in this area, their work often lacks a concise definition of the term “security awareness” [20]. Furthermore, different studies have controversial approaches regarding the question whether it is needed to differentiate between security awareness and security training. While many sources make no differentiation between those terms [21], others find it crucial to distinguish security awareness from security training [22].

Several papers (e.g. [23], [24], [25] and [26]) use the security awareness definition set by the U.S. National Institute of Standards and Technology (NIST) that states the following: Awareness is not training. The purposes of awareness presentations are simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. [14] According to NIST SP 800-16, awareness creates the employee's sensitivity to the threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them. The fundamental value of IT security awareness programs is that they set the stage for training by bringing about a change in attitudes which change the organizational culture. [14]

Some scientific papers [27] are citing Wikipedia [28] saying that security awareness is the knowledge and attitude that the members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization. While it might not be a proper definition in the context of this paper, it illustrates well the common pattern of knowledge and attitude used together in order to explain security aware behaviour.

IT security expert Michael Santarcangelo claims that the term "security awareness" is misused and conflated into something far bigger, more complicated, and harder to obtain [29]. He argues, that security awareness is the individual realization of the consequences of actions (with the ability to assess intention and impact) and that the focus of a security awareness program is to provide people with the information and experience to reach individual realization, that sets the stage to demonstrate business value and influence behaviour change. [30]

Hänsch and Benenson have done a comprehensive and systematic study [20] regarding the definition of IT security awareness. They suggest a classification of the different meanings into three groups according to three dimensions extracted from the literature:

1. security awareness as perception,
2. security awareness as protection,
3. security awareness as behaviour.

In the perception group of definitions the term security awareness focuses on the fact that users should know that dangers exist. In the protection group of definitions it is said that users should know more specifically which dangers exist and which measures are needed to protect themselves. In the third group suggested by Hänsch and Benenson, security awareness definitions expresses that the main reason for initiating an awareness program is to effectively reduce security incidents and therefore it is not enough to only have relevant knowledge – what is important is secure behaviour.

Amankwa et al. have used in their study [22] a conceptual analysis based on the existing literature for proposing working definitions, which could be used as a reference point for future information security researchers. Based on the foregoing discussions, they have defined information security awareness as **any endeavour to focus employees' attention on information security in order to ensure that all employees understand their roles and responsibilities in protecting the information that is in their possession by using print or electronic media**. The study by Amankwa et al. [22] also states that the concepts of information security education, information security training and information security awareness can be differentiated with regard to their focus, purpose and methods of delivery.

This paper defines information security awareness as it is suggested by Amankwa et al. [22] and also differentiates the concepts of information security education, information security training and information security awareness accordingly.

2.2. Evaluation Technique

In order to develop a method for evaluating human aspects of information security, it is necessary to choose a measurement technique and then define appropriate metrics for this technique. The purpose of this section is to justify the selection of questionnaires as the evaluation technique for assessing the human aspects of information security.

Questionnaire is a widely utilised tool in scientific research addressing the needs of being fast and low-cost. For example, Ahmadian et al. [31] have performed a systematic review on health information evaluation studies and their study found that the most popular evaluation tools were questionnaires and check-lists and that the most common evaluation methods were survey, interview and observation. Their research brought out that in terms of information system evaluation, questionnaires are usually used to collect respondents' knowledge and attitudes toward systems. They also stated that questionnaires have many advantages such as generating large amounts of data while spending little resources, but they also have some limitations including different conceptual understanding of questionnaire content by respondents and low response rates.

Even the studies that are criticising the shortcomings of questionnaires admit the usefulness of this technique. For example, Guldenmund calls questionnaires a quick and dirty tool for doing scientific research in his paper that discusses the use of questionnaires in safety culture research [32]. Quick, because self-administered questionnaires can be distributed among large groups of people in a relatively short period of time. Dirty due to the possibilities to control unwanted influences affecting the responses being limited and therefore including a lot of random "noise". Despite his criticism, he admits that questionnaires can be very helpful in providing instant quantified results and that a self-administered questionnaire is a valuable tool in scientific research. [32]

The use of questionnaires can be well justified in scientific research and it presents the advantages that are very suitable to the main goal of this thesis – to develop a fast and low-cost evaluation method. There are many scientific surveys using questionnaires to collect data regarding information security – more information about these can be found from the next chapter.

2.3. Scientific Surveys of Information Security

Information security can be measured by surveys that are using questionnaires as the tool for gathering data. There are a number of academic and non-academic projects conducted on this topic.

Although several international organisations conduct yearly surveys related to information security (e.g. PricewaterhouseCoopers [8], Deloitte [33], Ernst & Young [34], Cisco [35], Symantec [36], McAfee [37] and Verizon [38]), these surveys focus mostly on trends regarding reported security incidents and their impact. Those kind of surveys suffer from under- and over-reporting, depending on who collected them, and the errors may be both intentional (e.g., vendors and security agencies playing up threats) and unintentional (e.g., response effects or sampling bias) [39]. For example, the report [38] of one the largest U.S. wireless communications service provider Verizon stresses that mobile devices are not a preferred vector in data breaches. Technology company Cisco that focuses on networking equipment technology design and manufacturing has the according focus in their annual security report [35], where they first bring out the results regarding malicious exploits that are gaining access to web hosting servers, name servers, and data centers. While the biases of these reports might not be intentional it is clear that they do not represent a neutral point of view. On the contrary, it has been found rather common for the surveys to exhibit the pattern of enormous, unverified outliers dominating the rest of the data [40].

There is a number of scientific papers attempting to apply existing behavioural models to the area of information security [41]. This includes models such as theory of planned behaviour (TPB) [42], protection motivation theory (PMT) [43] and knowledge-attitude-behaviour (KAB) model, originally developed in fields such as healthcare, criminology and environmental psychology. According to Parsons et al. [41] and Karjalainen [44], many of these studies may present a biased viewpoint of the area of interest due to focusing solely on theory-verification and validation. In other words, only the variables in the theory are being assessed and other potentially important variables are not considered. [41]

From the practical business perspective, the main problem with the information security surveys is not so much the biased viewpoint as it is the lack of time and cost efficiency. Although there are papers explaining why return of investment and similar financial tools are not advisable for evaluating the merits of security projects [45], the economic model of cost and benefit remains the main structure behind leadership decisions in organisations [46]. Therefore it is needed to have a balance between scientific accuracy and low cost of delivering the results. In the traditional scientific surveys it can take months to collect and analyse the data and the result is usually a generalised feedback report. Kruger and Kearney [47] assessed information security awareness in an international gold mining company with the help of questionnaires and gave the recommendation of developing a web-based tool for automating the information gathering process. The goal of this paper is to develop such tool, but in addition to accelerating the information gathering process it should provide a faster and more efficient way to give personalised feedback.

Next chapter looks at online quizzes – i.e. web sites that focus on providing fast personalised feedback for those who fill in questionnaires.

2.4. Online Quizzes Regarding Information Security

Online quizzes are a good way to provide computer users with fast and individual feedback. As a part of this thesis a comprehensive review of different online security quizzes was carried through. A list of websites was compiled using the three most popular search engines [48] available in English – Google, Bing and Yahoo. The keywords “security” and “awareness” were used in searches in combinations with “test”, “quiz” and “questionnaire”. The results were filtered based on the following requirements:

1. questionnaires are used as testing technique,
2. quiz is freely available,
3. quiz is available in English,
4. quiz provides some sort of differentiated feedback based on results.

All of the freely available quizzes used questionnaire as the testing technique. It is interesting to note that all of the quizzes providing interactive feedback used close-ended type of questions – presumably due to significantly simpler and more reliable interpretation automation process compared to the answers for the open-ended questions. The complete list of inspected sites providing a free security related test in English can be found from Annex 1.

Many shortcomings were found in online quizzes regarding their reliability and validity. Firstly, the questionnaires found by the current study were rather short – some of them containing only five questions. That raises serious doubts regarding the reliability of those questionnaires, because the shorter the questionnaire, the bigger is the likelihood that the results are less differentiated and therefore of low accuracy.

Secondly, the inspected online quizzes were mostly measuring only technical and/or factual knowledge. While the knowledge part is important, it is not sufficient for a more general evaluation of human aspects of information security to only measure factual or technical knowledge. Research shows that security aware behaviour is not in a very strong correlation with security-related knowledge [49].

Thirdly, the online quizzes tend to lack structure. While some of them have some sort of explanation regarding the methodology behind them, nearly all of the inspected sites failed at providing convincing information that would indicate an underlying supporting structure.

In addition, the feedback part of inspected online quizzes typically was lacking content. A usual result displayed a numerical value sometimes accompanied by a short evaluative comment. There was a lack of suggestions or links for further reading.

Also it could be noted that many of the online quizzes lack a user-friendly design, e.g. being not mobile friendly and often having structural inconsistencies due to malformed coding. The further analysis of usability and user-friendliness of web sites is not in the scope of the current study.

To sum up the review of different online quizzes, the following shortcomings can be highlighted:

- lack of validity and reliability,
- lack of constructive feedback.

Security related online quizzes are mostly designed to measure some specific traits of a more general picture without demonstrating the existence of an underlying methodology that would support the results.

3. Methodology

As mentioned beforehand, there are many ways to evaluate security awareness, but taking into consideration the analysis of the current situation (Chapter 2) and limitations set by time and money, the most suitable method for evaluating security awareness in the current context is an online system that is using questionnaire to collect data and can provide fast and personalised feedback.

3.1. Model Behind the Questionnaire

The goal of this thesis is to develop a cost-efficient and fast evaluation method for human aspects of information security. In the previous chapters shortcomings of existing solutions were discussed and the reasoning behind the choice of a suitable evaluation technique was described. The technique itself is not enough to produce a valid evaluation method. A proper evaluation method needs an underlying methodology – some sort of model that would provide it the conceptual basis and an overall structure.

The research of Parsons et al. [41] used the knowledge-attitude-behaviour (KAB) model as the main part for their conceptual model determining employee security awareness. KAB model was initially proposed by Baranowski et al. [50] as a way of explaining the role of knowledge as a logical prerequisite to the intentional performance of health-related behaviours. The KAB model suggests that behaviour changes gradually. As knowledge accumulates in a health behaviour domain, changes in attitude are initiated. Over some period of time, changes in attitude accumulate, resulting in behavioural change. It is important to highlight that the study of Parsons et al. [41] states clearly that they believe that the relationship between knowledge, attitude and behaviour is influenced by many individual, intervention and organisational factors. However, the assessment of the influence of these factors on KAB and the different focus areas was considered to be beyond the scope of their paper.

KAB model was also used by Kruger and Kearney in their effort to create a prototype for assessing information security awareness [47].

Another research paper, written by Study by Khan et al. [51], implements an integration of knowledge-attitude-behaviour (KAB) model and theory of planned behaviour (TPB) for measuring the effectiveness of information security awareness methods. Theory of planned behaviour (TPB) also known as theory of reasoned action is a conceptual framework suggested by Fishbein and Ajzen [52] who found that often attitude was used to explain a wide variety of interpersonal behaviours, but its definition as "learned predisposition to respond in a consistently favourable or unfavourable manner with respect to a given object" did not solve the underlying ambiguity causing disagreements among attitude researchers. Fishbein and Ajzen suggest that attitude and subjective norms together influence the person's intention to perform a behaviour and that a specific behaviour is determined by this intention to perform according behaviour. [52] The model proposed by Khan et al. [51] takes the knowledge attribute from the KAB model, and adds the attributes of attitude and social norms from the theory of planned behaviour. The five step ladder model described by Khan et al. [51] is justified in comparing the effectiveness of different information security awareness methods, but is not well suitable to the current context due to its additional complexity.

Most of scientific research is dealing with knowledge and behaviour. In order to give a more structured approach to the transition from knowledge to behaviour, the concept of attitude was used. It is important to highlight that there are shortcomings in this simplified construct, but in the current context the main goal is to develop an evaluation method that would be fast and relatively easy to comprehend. Therefore the knowledge-attitude-behaviour (KAB) model was found to be the most suitable and is used in the current study. It is worth mentioning that the KAB model is closely related to KAP model that stands for knowledge, attitude and practice, but comparison between those two models is beyond the scope of current study.

3.2. What to Measure

When evaluating the human factor of information security, it is essential to set clearly defined characteristics that should be measured [53].

There are several studies dealing with the security practices by computer users. For example, Rhee et al. [54] have measured the security conscious care behaviour relation to self-efficacy in information security. They ask close-ended questions about file sharing, sensitive information handling and password management.

Kruger and Kearney [47] focused their study on the following six risk categories also named as “Golden rules”:

1. Always adhere to company policies
2. Keep passwords and personal identification numbers (PINs) secret
3. Use e-mail and the Internet with care
4. Be careful when using mobile equipment
5. Report incidents like viruses, thefts and losses
6. Be aware, all actions carry consequences

Thirty-five questions were designed to test the knowledge, attitude and behaviour of respondents regarding the six main focus areas and their factors and sub-factors.

Parsons et al. [41] reviewed several information security policies and used the findings of interviews with senior management to develop seven focus areas:

1. password management,
2. e-mail use,
3. internet use,
4. social networking site use,
5. incident reporting,
6. mobile computing,
7. information handling.

Compared to study by Kruger and Kearney [47] the seven focus areas identified by Parsons et al. [41] are more specific. Furthermore the study of Parsons et al. [41] also clearly defines three representative sub-areas for every focus area.

The relevance of focus areas defined in mentioned scientific papers was cross-checked with studies related to social engineering attacks. The paper by Nyamsuren [55] confirms the risks related to mobile devices, e-mail and information management. Paper by Parmar [56] affirms the rising trend of attacks through social media and phishing e-mails. Study by Krombholz et al. [57] outlines the advanced social engineering attacks including baiting attack – i.e. leaving malware-infected storage media in a location where it is likely to be found by future victims. Study by Abraham and Chengalur-Smith [58] describes how social engineering malware proliferates through a variety of channels, including e-mail, social software, websites, portable storage devices, and mobile devices.

Additionally, a series of interviews with senior management was conducted to identify the relevant focus areas in information security related to the human factor. As a result, the approach by Parsons et al. [41] was adopted to be the basis of the questionnaire due to its specific and relevant contents. The evaluation method being developed in this paper is addressing unintentional (in)security behaviour or naive mistakes as defined in the analysis of end user security behaviours by Stanton et al. [59]. That is also in accordance with the interviews and the study by Parsons et al. [41] who are focusing their study mostly on the neutral (accidental) behaviours – i.e. harmful behaviour without malicious intentions.

It must be highlighted that the likelihood of intentional malicious behaviour of employees might be underestimated due to optimistic bias described by Rhee et al. [60]. The paper [60] shows that factors such as perceived controllability and close social distance of a comparison target can have a significant influence on risk perception. The focus on the neutral behaviours was chosen in order to avoid the additional complexity that arises when trying to evaluate intentional malicious behaviour. Motivating mischievous employees to answer honestly and reliably to a security related questionnaire is an extremely challenging task. [61] Therefore it was consciously left out from the scope of the current study.

In the current thesis knowledge, attitude and behaviour are measured in seven focus areas. These areas are:

1. password management,
2. e-mail use,
3. internet use,
4. social networking site use,
5. incident reporting,
6. working remotely,
7. information handling.

These areas were adapted from the model of Parsons et al. [41] with the only difference in renaming "mobile computing" to "working remotely" because the term "mobile" was considered to be slightly misleading due to the strong associations with mobile phones, and weak associations with other mobile equipment such as laptops. Working remotely keeps the original idea and clarifies it in order to avoid misunderstandings.

For each of these representative areas three sub-areas adapted from the paper of Parsons et al. [41] were used. That resulted in 21 sub-areas as follows:

1. Password management
    - 1.1. Locking workstations
    - 1.2. Password sharing
    - 1.3. Choosing a good password
2. Email use
    - 2.1. Opening attachments
    - 2.2. Opening links
    - 2.3. My level of responsibility regarding e-mails
3. Internet use
    - 3.1. Installing unauthorised software
    - 3.2. Accessing dubious web sites
    - 3.3. Inappropriate use of internet
4. Social networking site (SNS) use
    - 4.1. Amount of work time spent on social networking sites
    - 4.2. Consequences of social networking sites

4.3. Posting about work on social networking sites

5. Incident reporting
   5.1. Reporting suspicious individuals
   5.2. Reporting bad behaviour by colleagues
   5.3. Reporting all security incidents
6. Working remotely
   6.1. Physically securing personal electronic devices
   6.2. Sending sensitive information via mobile networks
   6.3. Checking work email via free network
7. Information handling
   7.1. Disposing of sensitive documents
   7.2. Inserting DVDs/USB devices
   7.3. Using encryption to store confidential information

All the sub-areas are the same as validated by Parsons et al. [41] except sub-area 2.2. In Parsons et al. [41] the respective sub-area was "forwarding e-mails", but this was replaced by "opening links" in validity testing phase of this study (more details in chapter 4.1).

3.3. Designing the Statements

For each of the representative areas one specific knowledge statement, one specific attitude statement and one specific behaviour statement was developed. Three representative areas were chosen to maintain a balance between the scientific need for accuracy and the practical need to limit the length of the questionnaire. [41] This means that the KAB part of the questionnaire consists of 63 statements.

The statements used in the current study were designed to be more specific than other information security surveys that tend to measure it in a rather general manner. E.g. [49] uses "*I know what information security is.*" as a knowledge statement and "*My practice in exercising care when opening a suspicious email is a wise move.*" as an attitude statement. These statements are prone to response bias as they are ambiguous. A positive answer to the statement "*I know what information security is.*" does not give any information whether the respondent has a false understanding about information security or not, because it is not testing any specific piece of knowledge. "*My practice in exercising care when opening a suspicious email is a wise move.*" statement assumes that the respondent is exercising care when opening a suspicious email and does not specify what does it actually mean to exercise care.

Every statement was designed to follow good survey statement practices such as those described by Munn and Drever [53]. The main guidelines that were used in the statement design phase, were the following:

- avoiding leading questions,
- being brief and concrete,
- focusing on a single topic or issue in one statement,
- using simple language (avoiding very specific technical terminology).

In order to better quantify and compare the results, a five point Likert scale was used for all the items. Statements regarding knowledge and attitude were rated on a scale from "Strongly disagree" to "Strongly agree" and statements regarding behaviour were rated on a scale form "Never" to "Always".

3.4. Designing the Online Framework

It was the goal from the beginning to provide an online environment to carry out the research. The following requirements were set in order to choose the most suitable online platform:

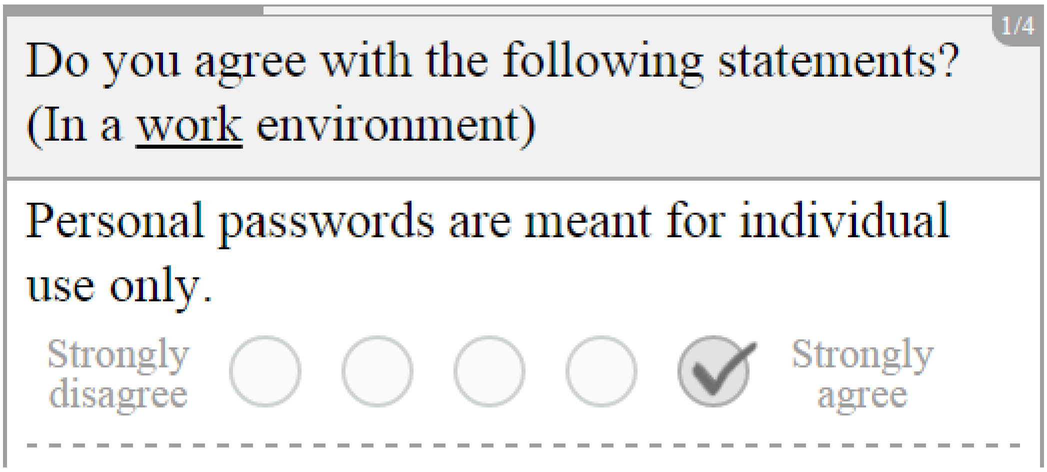
1. mobile-friendly design,
2. cross-browser usability,
3. similar design in different devices in order to exclude other potential influencing factors such as placement of questions,
4. lack of distractions – advertisement free and using neutral colours, especially on the questionnaire form itself,
5. customisable results shown after filling in the survey,

6. control over the collected data to ensure anonymity of the respondents,
7. possibility to add custom pages explaining the privacy policy and the project in more details.

A comparative analysis of existing survey services (Appendix 2 – Survey Platform) revealed that there was not a suitable solution fulfilling all the requirements. Therefore, an online platform was created specifically for this survey.

Taking into account the anonymity of the respondents, no tracking JavaScript and no tracking cookies were used. The submitted results are not accessible to others. All the user input is escaped and only the owner of the file has the rights to access the file with the results.

A neutral colouring scheme was used for the main part of the questionnaire in order to minimise the potential influence to the respondent. Therefore only grayscale colours were used (Figure 1).



1/4

Do you agree with the following statements? (In a work environment)

Personal passwords are meant for individual use only.

Strongly disagree ○ ○ ○ ○ ☑ Strongly agree

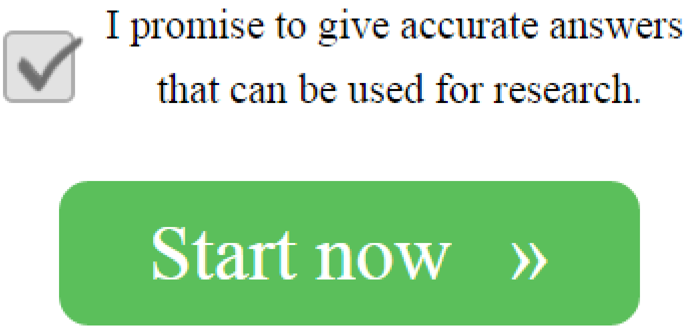
Figure 1: Main part of the questionnaire using neutral colours

The system is designed to be robust and scalable. The platform is written in PHP, HTML, CSS and JavaScript and it is functional also in browsers with no JavaScript and/or CSS support. The platform was created with best coding practices in mind. The website was validated to be mobile friendly by Google mobile friendly test [62] and valid HTML and CSS by W3C validators ([63] and [64] respectively). The system is usable even with text-only web browsers (tested with Links [65]).

3.5. Improving Validity of Responses

Mechanisms to improve the validity of responses were built into the online framework based on the recommendations of behavioural economist Dan Ariely [66] (who has extensive background in honesty research [61]).

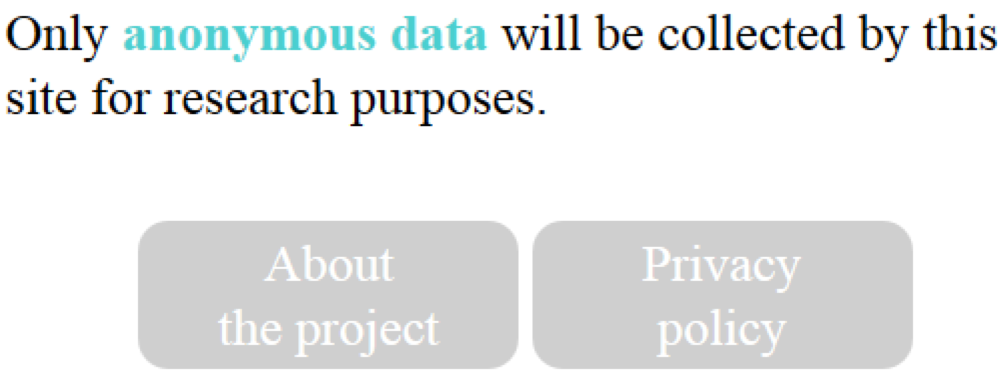
The introduction page at http://testing.planet.ee gives a short overview about the research project, links for further information. This serves the purpose of showing the visitor of the web site that this is not an entertainment quiz, but a serious research project and therefore priming the visitor for honesty [67]. In addition the following honesty question is presented to the visitor: “I promise to give accurate answers that can be used for research” (Figure 2). Ticking the check-box next to the honesty question activates the button to start the test. The honesty question forces the visitor to enter into a social contract and although there are no consequences for not adhering to the contract, this kind of construct has proven to be effective [66].



☑ I promise to give accurate answers that can be used for research.

Figure 2: Consent form needed to check before starting the survey

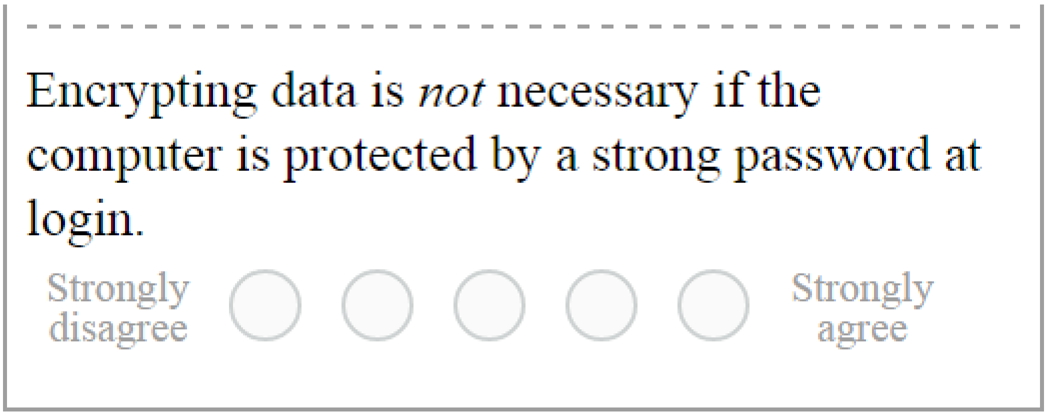
Another important part of the landing page of http://testing.planet.ee is the clear promise to collect only anonymous data (Figure 3). Also a link to the privacy policy page is given where the visitor can find more information about the collection of data in this project. Clearly mentioning anonymity and providing additional relevant information helps to ensure that the respondents do not have reasons to be afraid to answer honestly [66]. The privacy policy is also strictly followed during this research as written on the according web page.



Only anonymous data will be collected by this site for research purposes.

Figure 3: Statement of anonymity and link to privacy policy

Statements containing a negation are emphasising it by using cursive text (Figure 4). That helps to mitigate the risk that respondents might misinterpret the question and give the answer on a falsely reverse scale.



Encrypting data is *not* necessary if the computer is protected by a strong password at login.

Strongly disagree ○ ○ ○ ○ ○ Strongly agree

Figure 4: Negative statements having the negation part in cursive

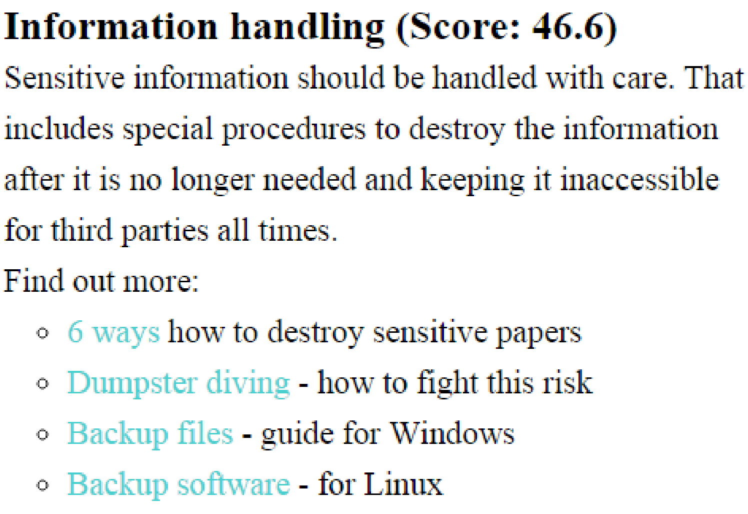
In the end of the questionnaire an additional questions is asked in order to ensure the validity of the results: “Can your answers be used for research?”. The purpose for this question is to give those who have doubts regarding the accuracy of their answers a chance to see their results without affecting the overall quality of the survey.

It is also worth mentioning that usability is a critical software system quality attribute in interactive systems [68] and should not be treated lightly. The ergonomic design helps the respondents to focus on the questions instead of getting distracted by technical issues such as unreadable font or distracting colour scheme. Therefore following good design principles [69] can help to increase the overall validity of the evaluation method.

3.6. Personalised Feedback for Respondents

After the respondent submits the answers to all the questions, a page of individual results is shown with personalised feedback. The design of the feedback starts with emphasising the importance on the security aware behaviour. Then an ordered list of strengths and weaknesses follows based on the answers of the respondent regarding his/her reported behaviour. The list of focus areas is ordered by the score in

Research papers about feedback in education [70], brain-training game [71] and sports [72] were analysed in order to design the proper way and order for displaying feedback. As positive feedback boosts intrinsic motivation through competence and autonomy needs [71] and it is recommended to give it a larger focus than negative feedback [70], then it was decided to start with the list of strengths followed by the list of weaknesses. Concepts of autonomy-supportive change-oriented feedback were adapted from the study of Carpentier and Mageau [72] and tips and links for further reading (Figure 5) were added to the according focus area avoiding person-related statements.



Information handling (Score: 46.6)

Sensitive information should be handled with care. That includes special procedures to destroy the information after it is no longer needed and keeping it inaccessible for third parties all times.

Find out more:

- 6 ways how to destroy sensitive papers
- Dumpster diving - how to fight this risk
- Backup files - guide for Windows
- Backup software - for Linux

Figure 5: Example of feedback for a focus area

In addition a list of all seven focus areas was given with appropriate scores in self-reported knowledge, attitude and behaviour (Figure 6).

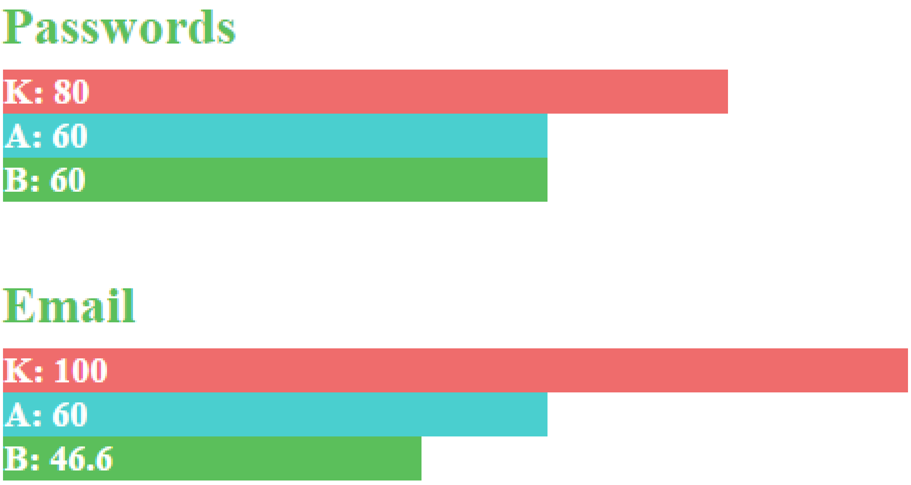


Figure 6: Example of KAB scores in two focus areas

4. Application / Implementation

The evaluation method presented in this paper was carried out in three phases based on the methodology of HAIS-Q [41]. The first was the pre-testing or validity phase which was designed to assess the psychological structure behind the content as well as the accuracy of the statements. The second phase was a pilot study, which was further refining and examining the reliability of the evaluation method. These phases provided initial evidence of validity and confidence to continue with the main study, which is presented in phase three.

4.1. Phase One – Validity Testing

Validity testing was based on the methodology suggested by Parsons et al. [41] where pre-testing techniques were utilised to test the validity and reliability of the survey items. First, an expert of psychology and survey design was asked to analyse the questionnaire and suggest improvements. After analysing the feedback and improving the survey, cognitive interviewing with an IT expert was conducted using the techniques described by Willis [73]. Think-aloud procedure in which subjects are explicitly instructed to "think aloud" as they answer the survey questions was used together with concurrent and retrospective verbal probing – e.g. the expert was asked additional questions regarding the comprehension of questions and reasons for hesitations.

Cognitive interviewing techniques helped to identify some additional ambiguities and problematic items of the questionnaire that were addressed before the pilot study with a larger audience.

4.2. Phase Two – Pilot Study

A pilot study by its definition is a trial, which is conducted before the main study takes place. The purpose of the pilot study is to help the researcher to ensure whether or not the study is appropriate in terms of validity. Should any problems be encountered during the pilot study; necessary adjustments can be made before the main study. [74] A quantitative analysis approach based on Likert style questionnaire was employed to evaluate the human factor of information security as described in this paper.

Pilot study was carried out with 28 IT students. Participants were asked to fill in the questionnaire consisting of 21 knowledge statements, 21 attitude statements, 21 behaviour statements and questions about their background. Background questions included name/nickname (optional), age, gender and working experience. Working experience question was: “Are you working?” with three options provided for answer: “I am working”, “I was working” and “I never worked”. Only the participants with the previous working experience were included – i.e. three participants who answered “I never worked” were excluded from the results. Out of 25 valid responses 15 were male and 10 female. Respondents were aged between 20 and 34 years. Participant took an average of 11 minutes and 40 seconds (SD = 2 min and 48 s) to complete the survey.

The average results in focus areas and the according standard deviations are shown in Figure 7 where letters K, A and B stand respectively for knowledge, attitude and behaviour and numbers from 1 to 7 note the focus areas as follows:

1. password management,
2. e-mail use,
3. internet use,
4. social networking site use,
5. incident reporting,
6. working remotely,
7. information handling.

Therefore, e.g. the blue bar in the Figure 7 marked as A5 notes the average score given to attitude statements regarding incident reporting. The according standard deviations are shown by black error bars (twice the length of SD) and also as orange bars for a better comparison across the focus areas. Figure 8 shows the overall average results by KAB main construct categories. The same logic for visualisation is followed as for the previous figure.

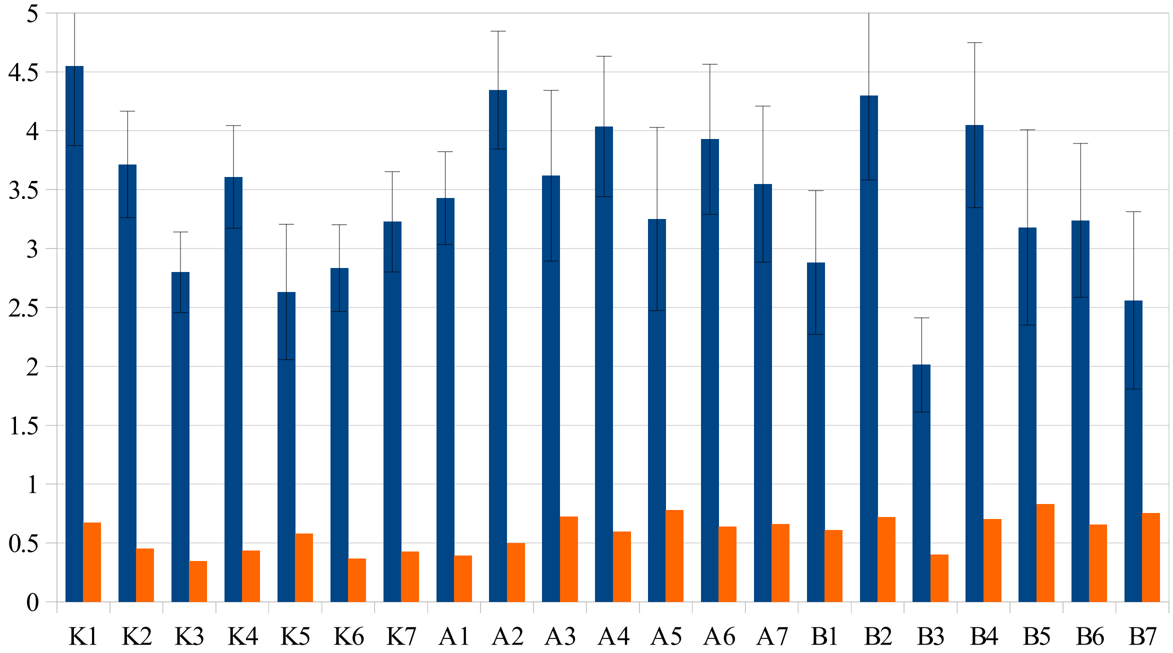


Figure 7: Average results per focus area with the according standard deviations for the pilot phase

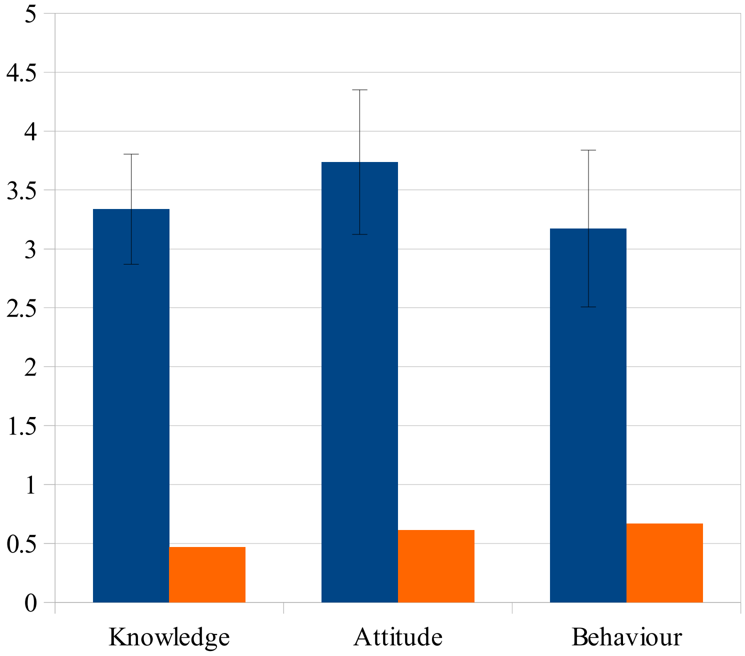


Figure 8: Average results per KAB constructs with appropriate average standard deviations for the pilot phase

A series of Pearson correlation coefficients were calculated to test the relationships between the according items of the three main constructs (knowledge, attitude and behaviour). The correlations sorted by the focus areas were the following:

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.263	1	-	-	-	-	-
3. Internet use	0.017	-0.068	1	-	-	-	-
4. Social networking site use	-0.123	0.183	-0.056	1	-	-	-
5. Incident reporting	-0.530	-0.262	0.004	0.172	1	-	-
6. Working remotely	-0.149	-0.421	-0.211	0.167	0.087	1	-
7. Information handling	-0.247	-0.101	-0.350	0.164	0.017	0.301	1

Table 1: Correlations for knowledge in pilot phase

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	-0.173	1	-	-	-	-	-
3. Internet use	-0.070	0.002	1	-	-	-	-
4. Social networking site use	0.300	0.095	0.242	1	-	-	-
5. Incident reporting	0.081	-0.040	0.168	0.299	1	-	-
6. Working remotely	0.066	-0.332	-0.088	0.080	0.204	1	-
7. Information handling	0.435	0.368	0.131	0.292	0.216	-0.274	1

Table 2: Correlations for attitude in pilot phase

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	-0.186	1	-	-	-	-	-
3. Internet use	0.008	0.072	1	-	-	-	-
4. Social networking site use	-0.279	0.124	0.035	1	-	-	-
5. Incident reporting	0.153	-0.065	-0.137	0.121	1	-	-
6. Working remotely	0.305	-0.327	-0.049	0.039	0.549	1	-
7. Information handling	-0.375	0.012	-0.119	-0.291	-0.607	-0.556	1

Table 3: Correlations for behaviour in pilot phase

The correlations of the results of the pilot study were demonstrating very weak relationships between the main constructs. It indicated a high likelihood of serious flaws in questionnaire design needed to be identified. In order to address the issue, another round of cognitive interviewing was conducted with a different IT expert to get a fresh perspective. Think-aloud and verbal probing identified multiple weak parts in the statements that were fixed.

After cognitive interview with the IT expert, the statements were reviewed once again together with an expert in psychology in order to ensure the alignment with the KAB method. Some shortcomings were identified regarding the lack of connections between different statements designed to evaluate the same focus area. These shortcomings explain the weak correlations of the results of the pilot study.

Before the main study also several improvements were made to the background information part of the questionnaire in order to further ensure the validity of the results:

- The question about the working experience was specified from “Are you working?” into “Are you working in an organization where you are using a computer in your daily work?” This kind of rephrasing helps to filter out the respondents that are out of the scope of the current study – i.e. not having relevant work experience.
- Additional control question was added: “Was it your first time to complete this test?” The purpose of this question is to filter out duplicate respondents.
- Additional control question was added: “Can your answers be used for research?”. The purpose of this question is to help eliminating inaccurate respondents from the results.
- The question about the name or nickname was removed as it did not give any extra value being optional and the observation during the pilot study showed that it touched multiple respondents too personally and therefore contradicted the idea of anonymity.

Also an issue with usability arose in the pilot study phase – namely, the participants of the study could submit the results without filling in any personal information. Additional client side and server side checks were added in order to eliminate this problem.

4.3. Phase Three – Main Study

4.3.1. Collecting Data

The prototype tool was applied to three different groups of people:

1. Cybersecurity specialists – a special link was sent to a group of cybersecurity master students and graduates. Potentially some of the lectures might have filled it in as well, but it does not influence the validity of the group as cybersecurity specialists.
2. IT specialists working in software development and testing who performed the test in controlled environment.
3. Others who filled in the survey that was promoted using snowball sampling [75].

The reason for differentiating those three groups is to provide additional possibilities to ensure the validity of the results. Cybersecurity specialists from the first group are expected to have higher results than people from the third group. Second group consisting of IT specialists serves as a valuable reference point because the test was performed in a controlled environment and therefore the likelihood of bogus responses is significantly lower than in general.

Altogether there were 108 participants out of whom 12 were cybersecurity specialists and 25 IT specialists. The first priority after collecting the data was to validate it according to the requirements specified in the following chapter.

4.3.2. Data Validation

This section describes different mechanisms and methods how the data was cleaned in order to improve its validity.

Participants were asked the following question: “Are you working in an organization where you are using a computer in your daily work?” There were three answers to choose from:

- I am working,

- I was working,
- I have never worked.

Participants that chose the last option ("I have never worked") were excluded from the study as only people with relevant working experience were in the scope of this study.

Participants were asked the following question: "Was it your first time to complete this test?" with the options of "Yes" and "No" to choose from. Respondents who chose "No" were excluded from the study.

Participants were asked the following question: "Can your answers be used for research?" with the options of "Yes" and "No" to choose from. Respondents who chose "No" were again excluded from the study.

A test run was conducted to evaluate the time needed to fill in the survey. The time measured was the time between opening the questionnaire and submitting the filled in questionnaire. The timing tests showed that it takes approximately 3 minutes to read through all the questions and fill in the questionnaire without thinking about the answers and approximately 4 minutes to read through the questions and answer quickly in case the questions are already familiar. It was decided that responses that are faster than 5 minutes would be checked individually.

The fastest time for filling in the questionnaire in controlled environment was 8:25 (8 minutes and 25 seconds). The overall fastest time for filling in the online questionnaire was 02:47 and the second fastest time was 06:04. The respondent with the time 02:47 was considered to be invalid as it is unlikely that a questionnaire could have been filled in so fast correctly.

The longest time for filling in the questionnaire in controlled environment was 20:33 (20 minutes and 33 seconds). The overall longest time for completing the questionnaire was 02:03:06 (2 hours 3 minutes and 6 seconds) that indicated that the respondent could have been dealing with other things in the middle of filling in the questionnaire. The longest time was considered to be a reasonable time period that would not impact the results and therefore no participant was excluded due to too long time taken to complete the questionnaire.

4.3.3. Results

After validating data and excluding the responses that did not fulfil the requirements of this survey there were 95 respondents left (from the initial 108 respondents). Out of these respondents 59 were male and 36 female (Figure 9). 51 respondents reported their age to be under 30 years and 44 respondents reported their age to be 30 years or more (Figure 10). It should be noted that the response from the group of cybersecurity specialists where the reported age was 70 years was considered to be unlikely, but the further analysis of according responses did not give any additional reasons to doubt its validity and therefore it was not excluded from the study.

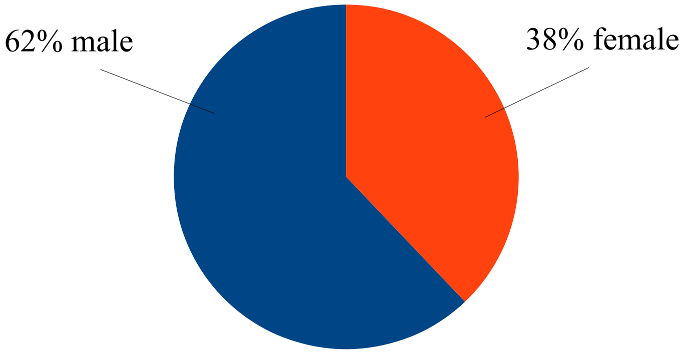


Figure 9: Distribution between male and female respondents

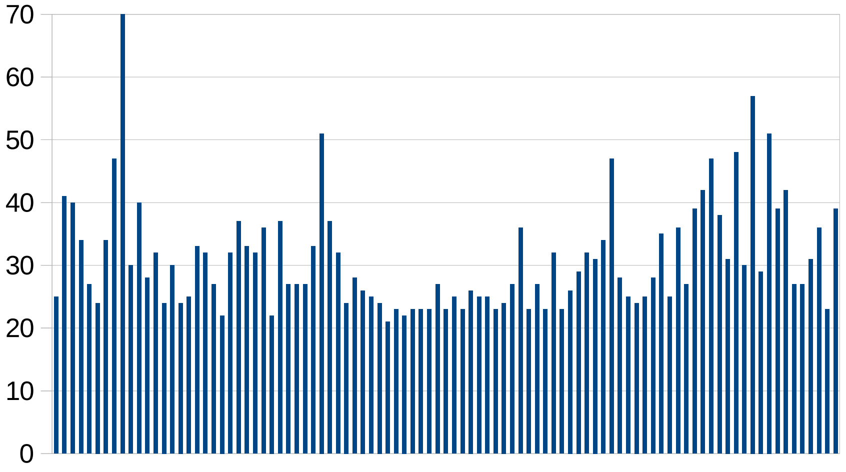


Figure 10: Distribution of reported age of respondents

The average results of 95 responses are shown in Figure 11 where letters K, A and B stand respectively for knowledge, attitude and behaviour and numbers from 1 to 7 note the focus areas as follows:

1. password management,
2. e-mail use,
3. internet use,
4. social networking site use,
5. incident reporting,
6. working remotely,
7. information handling.

Visualisations follow the same logic as Figure 7 and Figure 8 in the pilot phase – i.e. the blue bars in the Figure 11 are noting the average score given to the respective KAB constructs and according standard deviations are shown by black error bars (twice the length of SD) and also as orange bars for a better comparison across the focus areas. Figure 12 shows the overall average results by KAB main construct categories.

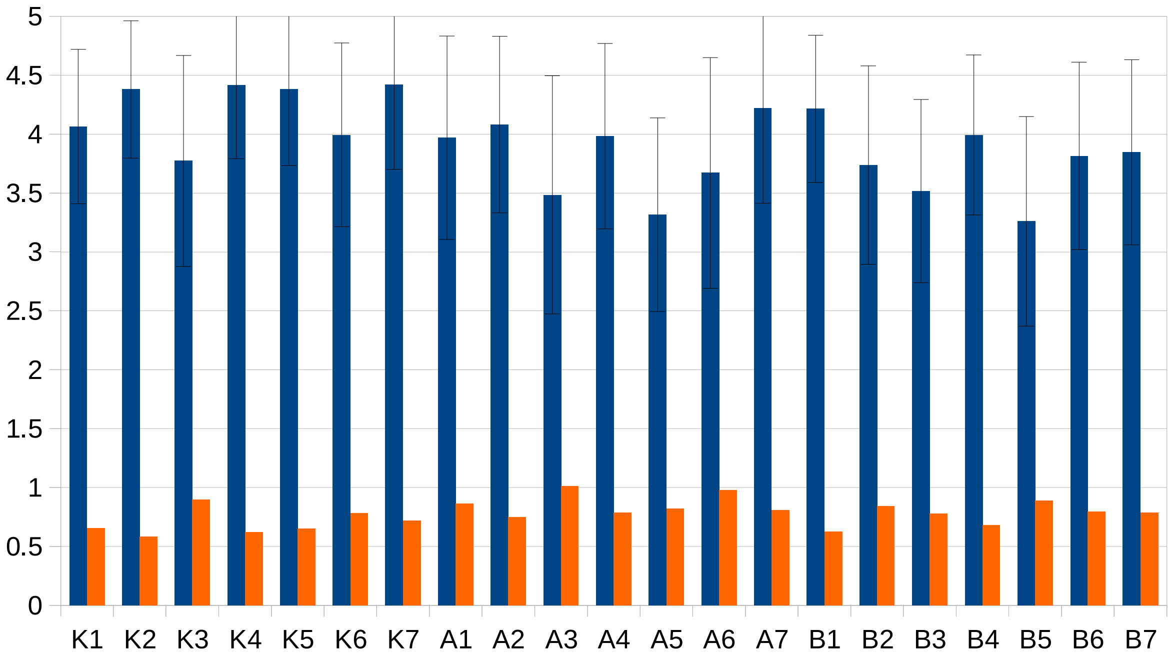


Figure 11: Average results per focus area with the according standard deviations for the main study

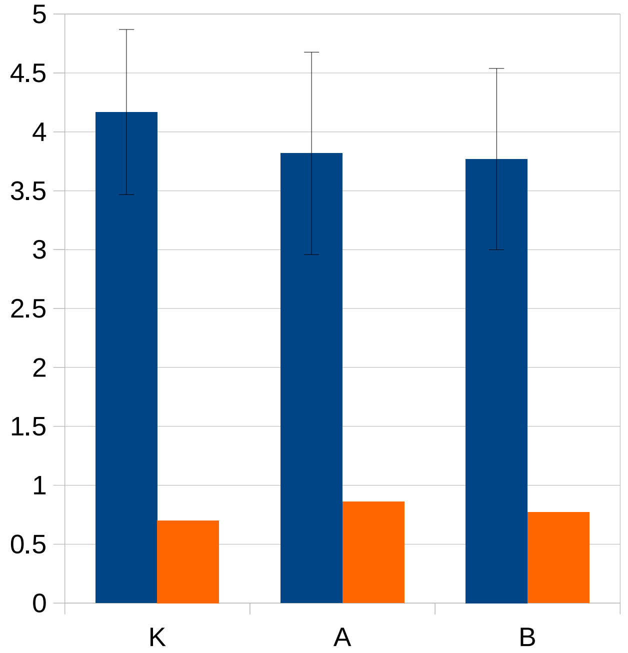


Figure 12: Average results per KAB constructs with appropriate average standard deviations for the main study

Correlations between the focus areas were calculated for statements regarding knowledge (Table 4), attitude (Table 5), and behaviour (Table 6). Compared to the HAIS-Q survey done by Parsons et al. [41] the current study shows slightly weaker correlations. Further analysis comparing the correlation tables according to the groups (see Appendix 3 – Correlation Tables for the Main Study for more detailed info) shows that the weak correlations are caused by the third loosely controlled group who performed the test in not controlled environment. Correlations in the group of cybersecurity specialists and in the group of IT specialists showed correlations in the range from 0.462 to 0.961 and 0.730 to 0.988 respectively, while the correlations in the third group stayed in the range of 0.103 to 0.671.

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.516	1	-	-	-	-	-
3. Internet use	0.414	0.432	1	-	-	-	-
4. Social networking site use	0.350	0.384	0.670	1	-	-	-
5. Incident reporting	0.331	0.365	0.575	0.560	1	-	-
6. Working remotely	0.358	0.331	0.455	0.440	0.488	1	-
7. Information handling	0.512	0.506	0.422	0.472	0.435	0.530	1

Table 4: Correlations for knowledge in the main study

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.399	1	-	-	-	-	-
3. Internet use	0.403	0.429	1	-	-	-	-
4. Social networking site use	0.255	0.378	0.523	1	-	-	-
5. Incident reporting	0.441	0.404	0.462	0.454	1	-	-
6. Working remotely	0.435	0.341	0.682	0.504	0.448	1	-
7. Information handling	0.450	0.553	0.481	0.434	0.392	0.526	1

Table 5: Correlations for attitude in the main study

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.358	1	-	-	-	-	-
3. Internet use	0.155	0.208	1	-	-	-	-
4. Social networking site use	0.165	0.350	0.578	1	-	-	-
5. Incident reporting	0.235	0.362	0.248	0.1849	1	-	-
6. Working remotely	0.495	0.364	0.378	0.4156	0.172	1	-
7. Information handling	0.331	0.510	0.254	0.2773	0.403	0.459	1

Table 6: Correlations for behaviour in the main study

Cronbach's alpha was calculated for each of the three main constructs – knowledge, attitude and behaviour – to test the internal consistency of the survey items. Table 7 shows that Cronbach's alpha was in the recommended range of 0.70 until 0.95 [76] which provides evidence of high degree reliability and indicates that the scales are measuring the same underlying construct [41].

Constructs	**Cronbach's alpha**
Knowledge of security practices	0.850
Attitude towards security practices	0.850
Self reported security aware behaviour	0.771

Table 7: Cronbach's alpha coefficients for the KAB components in the main study

In general, it can be said that the results of the main study show significant improvements compared to the pilot phase proving that the conducted changes had a significant effect on the validity of the method.

5. Discussion and Conclusions

The qualitative measures justify the validity and reliability of the developed method and although it can be improved, the prototype has proven to be an effective and cost efficient tool for evaluating human aspects of information security. Although it is likely to be less accurate than a thorough security audit, it is available for free and enables users to perform a fast self-assessment test.

5.1. Future Work

The statements in the questionnaire could be improved even more based on feedback received. The main issue mentioned in the feedback is that the statements are graded in the scale of true and false (or right and wrong) and that the real situations are more context-dependent. For example it is not always possible to use a password that is at least 10 characters long and it might not be needed due to other security measures. Similarly, it might be reasonable to leave a mobile device unattended in specific context, e.g. the mobile device is password protected and the working environment is highly secured. This kind of feedback is justified and it is true that in real life there is not always a clear line between secure and insecure behaviour. In the current study a purposefully simplified measuring scale was used for rough estimations without the intentions to achieve a high accuracy comparable to a thorough security audit. In future research, a more complex method could be developed with a more differentiated scale.

The evaluation method developed in this paper could be used together with a different type of assessment to investigate the patterns discovered by different methods. For example, a study of Kearney and Kruger [77] conducted a questionnaire based survey and then followed up with a practical e-mail based phishing exercise. Such approach was out of the scope of the current study due to additional ethical and legal constraints. It could, however, provide interesting results and ways to further validate and examine the underlying psychological mechanisms that influence people to act in a security aware way.

The evaluation method developed in this paper could be used to measure the effectiveness of security awareness trainings. That would need additional research to analyse and avoid possible biases that would arise when, for example, the results of the questionnaire would influence the success rating of a training. Also the impact of recurrent measurements could be investigated further. Additionally, the evaluation method could be used in order to indicate the need for a security training or to differentiate different study groups for security training based on their weaknesses. In that case, the issues regarding anonymity should be thoroughly analysed. For example, the higher importance of the security test results might influence the honesty of respondents [61].

A possibility to assign different weights reflecting the importance of measured focus areas in order to develop a metric characterising the overall score could be considered. Also it could be a promising idea to make an online system with dynamic scales configurable according to the priorities of a specific organisation.

The psychological factors influencing the study could be researched more thoroughly. For example, using virtual presence and survey instructions to minimise careless responding [78] could be used – a technique that is also aligned with the recommendations of Dan Ariely [66].

5.2. Conclusions

The sample size for the study was not ideal, but an approximate 95% confidence range for a sample size of 100 is around +/- 10% and the sample size needs to be increased quite substantially, to 1000, to reduce the margin of error significantly (+/-3.0%). [53] For the sample size of 95 the Pearson correlation coefficient has to be 0.333 or larger in order to be statistically significant (two-tailed probability, $p < 0.001$). Both groups of cybersecurity specialists and IT specialists were all exceeding this level. The largest p-value (p ≈ 0.321) was present in the correlations of behaviours of the third group. This is well aligned with the remarks by Parsons et al. [41] who brought out the potential problems with Internet data collection and mentioned that the lack of interaction with the researcher might result in less accountability. However, the same study also outlined that increased anonymity may increase the probability of authentic responses and that the Internet data collection can also provide a wider distribution of demographic sample than a local study. One of the main goals of the current study was to make the implementation of the evaluation method publicly available and the resulting trade-off in lower validity of data was found to be well justified, because the main purpose of this study was to address the problem of human factor weaknesses regarding information security and to target as wide audience as possible.

References

[1] D. Kahneman, *Thinking, Fast and Slow*, Reprint edition. New York: Farrar, Straus and Giroux, 2013.

[2] T. Herath and H. R. Rao, “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,” *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, May 2009.

[3] R. B. Cialdini, *Influence: The Psychology of Persuasion, Revised Edition*, Revised edition. New York, NY: Harper Business, 2006.

[4] Bruce Schneier, “The Psychology of Security,” presented at the Africacrypt 2008, Casablanca, Morocco, 2008, pp. 50–79.

[5] K. D. Mitnick and W. L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Indianapolis, IN: Wiley, 2005.

[6] C. Hadnagy and P. Wilson, *Social Engineering: The Art of Human Hacking*, 1 edition. Indianapolis, IN: Wiley, 2010.

[7] K. D. Mitnick, W. L. Simon, and S. Wozniak, *The Art of Deception: Controlling the Human Element of Security*, 1 edition. Indianapolis, Ind: Wiley, 2003.

[8] PricewaterhouseCoopers International Limited, “Global State of Information Security Survey: 2015 results by industry,” *PwC*. [Online]. Available: http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml. [Accessed: 14-Mar-2015].

[9] M. T. Dlamini, J. H. P. Eloff, and M. M. Eloff, “Information security: The moving target,” *Computers & Security*, vol. 28, no. 3–4, pp. 189–198, May 2009.

[10] M. S. Dorfman, *Introduction to Risk Management and Insurance*, 9 edition. Upper Saddle River, N.J: Prentice Hall, 2007.

[11] S. Gold, “Social engineering today: psychology, strategies and tricks,” *Network Security*, vol. 2010, no. 11, pp. 11–14, Nov. 2010.

[12] D. Ashenden, “Information Security management: A human challenge?,” *Information Security Technical Report*, vol. 13, no. 4, pp. 195–201, Nov. 2008.

[13] B. Gengler, “Super-hacker Kevin Mitnick takes a plea,” *Computer Fraud & Security*, vol. 1999, no. 5, p. 6, May 1999.

[14] M. Wilson, S. I. Pitcher, J. D. Tressler, J. B. Ippolito, and D. E. de Zafra, “Information Technology Security Training Requirements: A Role- and Performance-Based Model,” *National Institute of Standards and Technology Special Publication 800-16*, Apr. 1998.

[15] L. J. Semer, “EVALUATING the Employee Security Awareness Program,” *Internal Auditor*, vol. 69, no. 6, pp. 53–56, Dec. 2012.

[16] H. S. B. Herath and T. C. Herath, “IT security auditing: A performance evaluation decision model,” *Decision Support Systems*, vol. 57, pp. 54–63, Jan. 2014.

[17] “Cyber governance health check: 2013 - Publications - GOV.UK.” [Online]. Available: https://www.gov.uk/government/publications/cyber-governance-health-check. [Accessed: 22-May-2015].

[18] J. Yeo, “Using penetration testing to enhance your company’s security,” *Computer Fraud & Security*, vol. 2013, no. 4, pp. 17–20, Apr. 2013.

[19] St. Augustine, *The Confessions of Saint Augustine*. CreateSpace Independent Publishing Platform, 2013.

[20] N. Hänsch and Z. Benenson, “Specifying IT Security Awareness,” in *2014 25th*

International Workshop on Database and Expert Systems Applications (DEXA), 2014, pp. 326–330.

[21] H. Pern Chia, "How to Study Home Users," presented at the TKK T-110.5190, Seminar on Internetworking, 2007.

[22] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for*, 2014, pp. 248–252.

[23] N. Kolb and F. Abdullah, "Developing an Information Security Awareness Program for a Non-Profit Organization," *International Management Review*, vol. 5, no. 2, pp. 103–107, Dec. 2009.

[24] E. B. Kim, "Recommendations for information security awareness training for college students," *Information Management &amp; Computer Security*, vol. 22, no. 1, 2014.

[25] L. Taylor and M. Shepherd, "Chapter 9 - Addressing Security Awareness and Training Requirements," in *FISMA Certification and Accreditation Handbook*, L. Taylor and M. Shepherd, Eds. Burlington: Syngress, 2007, pp. 139–148.

[26] A. Tsohou, M. Karyda, and S. Kokolakis, "Analyzing the role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs," *Computers & Security*.

[27] A. Bashorun, A. Worwui, and D. Parker, "Information security: To determine its level of awareness in an organization," in *2013 7th International Conference on Application of Information and Communication Technologies (AICT)*, 2013, pp. 1–5.

[28] "Security awareness," *Wikipedia, the free encyclopedia*. 15-Feb-2015.

[29] M. Santarcangelo, "Why conflating security awareness beyond this definition reduces the effectiveness of your program," *CSO Online*, 24-Feb-2014. [Online]. Available: http://www.csoonline.com/article/2136751/security-leadership/why-conflating-security-awareness-beyond-this-definition-reduces-the-effectivene.html. [Accessed: 08-Mar-2015].

[30] Michael Santarcangelo, "Why the definition of security awareness matters," *Security Catalyst*. [Online]. Available: http://securitycatalyst.com/why-the-definition-of-security-awareness-matters/. [Accessed: 08-Mar-2015].

[31] L. Ahmadian, S. Salehi Nejad, and R. Khajouei, "Evaluation methods used on health information systems (HISs) in Iran and the effects of HISs on Iranian healthcare: A systematic review," *International Journal of Medical Informatics*, vol. 84, no. 6, pp. 444–453, Jun. 2015.

[32] F. W. Guldenmund, "The use of questionnaires in safety culture research – an evaluation," *Safety Science*, vol. 45, no. 6, pp. 723–743, Jul. 2007.

[33] Deloitte Touche Tohmatsu Limited, "2014 Deloitte-NASCIO Cybersecurity Study." [Online]. Available: http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf.

[34] Ernst & Young Global Limited, "Get ahead of cybercrime EY's Global Information Security Survey 2014." [Online]. Available: http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf. [Accessed: 14-Mar-2015].

[35] "Cisco 2014 Annual Security Report." [Online]. Available: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf. [Accessed: 14-Mar-2015].

[36] "Internet Security Threat Report 2015 | Symantec." [Online]. Available: http://www.symantec.com/security_response/publications/threatreport.jsp. [Accessed: 16-May-2015].

[37] "McAfee Labs^{TM} Report Previews 2015 Developments in Exploits and Evasion | McAfee Press Release." [Online]. Available: http://www.mcafee.com/us/about/news/2014/q4/20141209-01.aspx. [Accessed: 16-May-2015].

[38] “Data Breach Investigations Report,” *Verizon Enterprise Solutions*. [Online]. Available: http://www.verizonenterprise.com/DBIR/. [Accessed: 16-May-2015].

[39] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, “Measuring the Cost of Cybercrime,” in *The Economics of Information Security and Privacy*, R. Böhme, Ed. Springer Berlin Heidelberg, 2013, pp. 265–300.

[40] C. H. Dinei Flo, “Sex, Lies and Cyber-crime Surveys,” *Microsoft TechReport*, vol. MSR-TR-2011–75, Jun. 2011.

[41] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q),” *Computers & Security*, vol. 42, pp. 165–176, May 2014.

[42] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *Management Information Systems Quarterly*, vol. 34, no. 3, pp. 523–548, Sep. 2010.

[43] A. Vance, M. Siponen, and S. Pahnila, “Motivating IS security compliance: Insights from Habit and Protection Motivation Theory,” *Information & Management*, vol. 49, no. 3–4, pp. 190–198, May 2012.

[44] M. Karjalainen and M. Siponen, “Towards a A New Meta-Theory for Designing IS Security Training Approaches,” University of Oulu, Oulu, 2011.

[45] C. C. Wood and D. B. Parker, “Why ROI and similar financial tools are not advisable for evaluating the merits of security projects,” *Computer Fraud & Security*, vol. 2004, no. 5, pp. 8–10, May 2004.

[46] B. Srinidhi, J. Yan, and G. K. Tayi, “Allocation of Resources to Cyber-Security: The Effect of Misalignment of Interest between Managers and Investors,” *Decision Support Systems*.

[47] H. A. Kruger and W. D. Kearney, “A prototype for assessing information security awareness,” *Computers & Security*, vol. 25, no. 4, pp. 289–296, Jun. 2006.

[48] “Search engine market share.” [Online]. Available: http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0. [Accessed: 21-May-2015].

[49] J. Kaur and N. Mustafa, “Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME,” in *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 2013, pp. 286–290.

[50] T. Baranowski, K. W. Cullen, T. Nicklas, D. Thompson, and J. Baranowski, “Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts?,” *Obesity Research*, vol. 11, no. S10, p. 23S–43S, Oct. 2003.

[51] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, “Effectiveness of information security awareness methods based on psychological theories,” *African Journal of Business Management*, vol. 5, no. 26, pp. 10862–10868, 2011.

[52] M. Fishbein and I. Ajzen, *Belief, attitude, intention, and behavior: an introduction to theory and research*. Reading, Mass.: Addison-Wesley Pub. Co., 1975.

[53] P. Munn and E. Drever, *Using Questionnaires in Small-Scale Research. A Teachers' Guide.* Scottish Council for Research in Education, 15 St. John Street, Edinburgh, EH8 8JR, Scotland, United Kingdom., 1990.

[54] C. K. Hyeun-Suk Rhee, “Self-efficacy in information security: Its influence on end users' information security practice behavior,” *Computers & Security*, vol. 28, no. 8, pp. 816–826, 2009.

[55] H.-J. C. E. Nyamsuren, “Preventing Social Engineering in Ubiquitous Environment,” pp. 573–577, 2008.

[56] B. Parmar, “Employee negligence: the most overlooked vulnerability,” *Computer Fraud & Security*, vol. 2013, no. 3, pp. 18–20, Mar. 2013.

[57] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *Journal of Information Security and Applications*.

[58] S. Abraham and I. Chengalur-Smith, “An overview of social engineering malware: Trends, tactics, and implications,” *Technology in Society*, vol. 32, no. 3, pp. 183–196, Aug. 2010.

[59] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, “Analysis of end user security

behaviors," *Computers & Security*, vol. 24, no. 2, pp. 124–133, Mar. 2005.

[60] H.-S. Rhee, Y. U. Ryu, and C.-T. Kim, "Unrealistic optimism on information security management," *Computers & Security*, vol. 31, no. 2, pp. 221–232, Mar. 2012.

[61] D. Ariely, *The (Honest) Truth About Dishonesty: How We Lie to Everyone---Especially Ourselves*. New York: Harper, 2012.

[62] "Mobile-Friendly Test." [Online]. Available: http://www.google.com/webmasters/tools/mobile-friendly/. [Accessed: 21-May-2015].

[63] "The W3C Markup Validation Service." [Online]. Available: http://validator.w3.org/. [Accessed: 21-May-2015].

[64] "The W3C CSS Validation Service." [Online]. Available: http://jigsaw.w3.org/css-validator/. [Accessed: 21-May-2015].

[65] "Twibright Labs: Links." [Online]. Available: http://links.twibright.com/. [Accessed: 21-May-2015].

[66] D. Stanley, "4 Helpful Tips for Better Survey Responses," *Research Access*. .

[67] M. T. Vinski and S. Watter, "Priming honesty reduces subjective bias in self-report measures of mind wandering," *Consciousness and Cognition*, vol. 21, no. 1, pp. 451–455, Mar. 2012.

[68] N. Juristo, A. M. Moreno, and M.-I. Sanchez-Segura, "Analysing the impact of usability on software design," *Journal of Systems and Software*, vol. 80, no. 9, pp. 1506–1516, Sep. 2007.

[69] A. Chevalier and M. Kicka, "Web designers and web users: Influence of the ergonomic quality of the web site on the information search," *International Journal of Human-Computer Studies*, vol. 64, no. 10, pp. 1031–1048, Oct. 2006.

[70] L. Voerman, P. C. Meijer, F. A. J. Korthagen, and R. J. Simons, "Types and frequencies of feedback interventions in classroom interaction in secondary education," *Teaching and Teacher Education*, vol. 28, no. 8, pp. 1107–1115, Nov. 2012.

[71] C. Burgers, A. Eden, M. D. van Engelenburg, and S. Buningh, "How feedback boosts motivation and play in a brain-training game," *Computers in Human Behavior*, vol. 48, pp. 94–103, Jul. 2015.

[72] J. Carpentier and G. A. Mageau, "When change-oriented feedback enhances motivation, well-being and performance: A look at autonomy-supportive feedback in sport," *Psychology of Sport and Exercise*, vol. 14, no. 3, pp. 423–435, May 2013.

[73] G. B. Willis, *Cognitive interviewing: a tool for improving questionnaire design*. Thousand Oaks, Calif.: Sage Publications, 2005.

[74] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp. 304–312, Sep. 2014.

[75] H. K. E. Vervaeke, D. J. Korf, A. Benschop, and W. van den Brink, "How to find future ecstasy-users: Targeted and snowball sampling in an ethically sensitive context," *Addictive Behaviors*, vol. 32, no. 8, pp. 1705–1713, Aug. 2007.

[76] M. Tavakol and R. Dennick, "Making sense of Cronbach's alpha," *International Journal of Medical Education*, vol. 2, pp. 53–55, Jun. 2011.

[77] W. D. Kearney and H. A. Kruger, "Considering the influence of human trust in practical social engineering exercises," in *Information Security for South Africa (ISSA), 2014*, 2014, pp. 1–6.

[78] M. K. Ward and S. B. Pond III, "Using virtual presence and survey instructions to minimize careless responding on Internet-based surveys," *Computers in Human Behavior*, vol. 48, pp. 554–568, Jul. 2015.

Appendix 1 – List of Online Security Tests

This list is far from being conclusive, but is characterising a random sample found from different search results. Five search engines (google.com, baidu.com, bing.com, ask.com and duckduckgo.com) were used to find quizzes based on keywords such as “security test”, “awareness test”, “security quiz”, “computer security test”, “security awareness quiz”. Only free options were considered.

Results are displayed in the table below with the following information on each row:

1. reference number (that is used in this thesis in order to refer to a particular site),
2. URL of the website,
3. short description of the quiz,
4. indications whether the quiz is measuring knowledge, attitude and/or behaviour presented in the columns that are marked by K, A and B respectively.

	Website	Description	Measuring		
			K	A	B
1.	https://msdn.microsoft.com/en-us/magazine/cc982154.aspx	Security quiz measuring knowledge of C language	+	-	-
2.	http://netsecurity.about.com/cs/compsecurity101/	Computer Security 101 course with short quizzes in the end of each chapter. Unlimited tries until each question gets correct answer.	+	-	-
3.	http://www.proprofs.com/quiz-school/story.php?title=it-security-quiz	36 IT-related questions testing the knowledge. A score on a scale up to 100 is given as result with no further explanations.	+	-	-
4.	http://www.proprofs.com/quiz-school/story.php?title=end-user-security-awareness-quiz	20 questions testing end user security knowledge. A score on a scale up to 100 is given as result with the list of correct and incorrect answers. No further explanations nor links for further reading are given.	+	-	-
5.	http://www.softwareunlimited.com/securityquiz.htm	Simple test with 10 yes/no questions. Result is the count of “yes” answers.	+	-	+
6.	http://mediasmarts.ca/game/how-cyber-savvy-are-you-cyber-	Simple test of 11 questions focused on buying music online.	+	-	+

	Website	Description	Measuring		
			K	A	B
	security-quiz				
7.	http://www.agnitum.com/vote/stquiz/start.php	15 security questions put together by the security experts at Agnitum, evaluated on a scale up to 30 points.	+	-	-
8.	http://newsroom.cisco.com/feature/515300/Security-Quiz	10 questions, unlimited tries to get an answer right. Only correct answers allow to continue the test.	+	-	-
9.	http://netsecurity.about.com/od/quizzesandpolls/ss/secdayquiz.htm	Not an interactive quiz. 8 questions and answers in the end.	+	-	-
10.	https://www.hsbc.com.hk/1/2/special/banking/prom076	6 questions with feedback after each answer. Results include recommendations for further reading.	+	-	-
11.	http://timoh6.github.io/WebAppSecQuiz/	18 technical questions. Number of right and wrong answers are shown in the end and commented answers on a separate page.	+	-	-
12.	http://www.cba.ca/asptools/en/cyber.php	10 questions with feedback after each answer. Feedback occasionally included links for further reading.	+	+	+
13.	http://home.mcafee.com/SafetyQuiz/QuizShopping.aspx	10 questions regarding online shopping with commented answers and two links for further reading.	+	-	-
14.	http://home.mcafee.com/SafetyQuiz/QuizTeen.aspx	10 mostly true/false questions where attitude and knowledge statements were often united into one question. Feedback includes links for further reading.	+	+	-
15.	http://www.csmonitor.com/USA/2011/0420/How-much-do-you-know-about-cybersecurity-Take-our-quiz/william-gibson-neuromancer	24 questions testing factual knowledge plus one question half-jokingly testing behaviour (testing the readiness to insert personal information in order to win a prize). Result page includes the list of correct answers.	+	-	+
16.	http://computer.howstuffworks.com/computer-security-quiz.htm	10 questions testing IT terminology with feedback after every answer. Feedback consists of short description of the correct answer.	+	-	-
17.	http://simplisafe.com/resource/digital-security/	Colourful and responsive web site that contains 13 questions focusing mostly on secure behaviour. Feedback is given after each answer with relevant links. Many questions are ambiguous, e.g. it is difficult to give a yes/no answer to the following question: “Do you know how strong your passwords are?”	+	-	+
18.	http://www.bankersonline.com/technology/tech_infosecquiz.html	5 questions long information security quiz with instant feedback after each answer.	+	-	-
19.	http://searchsecurity.techtarget.com/quiz/Quiz-Building-a-risk-based-compliance-program	5 questions long quiz focusing on risk-based compliance program knowledge. Results page has feedback for every question and according links for further reading.	+	+	-

	Website	Description	Measuring		
			K	A	B
20.	http://www.cio.gov.bc.ca/local/cio/informationsecurity/March2015MatchingQuiz/March2015MatchingQuiz.htm	Three test pages each containing 8 terms in two columns that need to be paired. Result page shows the number of correct questions, total questions (3), accuracy (%) and attempts.	+	-	-
21.	http://www.cio.gov.bc.ca/local/cio/informationsecurity/Feb2015Quiz/Feb2015Quiz.htm	8 questions testing factual knowledge of IT security and related events. Result page shows the number of correct questions, total questions (8), accuracy (%) and attempts.	+	-	-
22.	http://www.gocertify.com/quizzes/comptia/security-plus-sy0301.html	15 questions long practice test for Comptia Security+ certification exam. Most of the questions ask what should be done in some particular situation.	+	-	-

Table 8: List of online security tests

Appendix 2 – Survey Platform

Here is a list of different online survey platforms that were considered for the evaluation method for human aspects of information security. None of these sites were found suitable based on the requirements listed in the Chapter 3.4 – Designing the Online Framework.

1. https://kwiksurveys.com
2. https://www.questionpro.com
3. https://freeonlinesurveys.com
4. https://www.surveygizmo.com
5. http://www.zoomerang.com
6. http://www.zoho.com/survey
7. https://www.mysurvey.com
8. https://www.smartsurvey.co.uk
9. https://www.murvey.com
10. https://www.globaltestmarket.com
11. https://survs.com
12. http://www.snapsurveys.com

Appendix 3 – Correlation Tables for the Main Study

Here are the correlation tables of the main study according to the groups.

Correlations for knowledge

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.973	1	-	-	-	-	-
3. Internet use	0.798	0.764	1	-	-	-	-
4. Social networking site use	0.934	0.931	0.832	1	-	-	-
5. Incident reporting	0.977	0.988	0.770	0.923	1	-	-
6. Working remotely	0.933	0.935	0.840	0.949	0.945	1	-
7. Information handling	0.966	0.981	0.827	0.956	0.963	0.947	1

Correlations for attitude

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.884	1	-	-	-	-	-
3. Internet use	0.832	0.789	1	-	-	-	-
4. Social networking site use	0.862	0.920	0.880	1	-	-	-
5. Incident reporting	0.940	0.866	0.900	0.877	1	-	-
6. Working remotely	0.827	0.741	0.934	0.879	0.841	1	-
7. Information handling	0.897	0.892	0.781	0.830	0.907	0.730	1

Correlations for behaviour

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.916	1	-	-	-	-	-
3. Internet use	0.838	0.748	1	-	-	-	-
4. Social networking site use	0.936	0.907	0.839	1	-	-	-
5. Incident reporting	0.903	0.776	0.867	0.809	1	-	-
6. Working remotely	0.931	0.912	0.770	0.906	0.798	1	-
7. Information handling	0.954	0.924	0.821	0.923	0.892	0.930	1

Table 9: Correlations for the group of cyberspecialists

Correlations for knowledge

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.875	1	-	-	-	-	-
3. Internet use	0.747	0.820	1	-	-	-	-
4. Social networking site use	0.910	0.939	0.819	1	-	-	-
5. Incident reporting	0.874	0.939	0.801	0.920	1	-	-
6. Working remotely	0.855	0.857	0.832	0.879	0.840	1	-
7. Information handling	0.930	0.881	0.783	0.961	0.895	0.909	1

Correlations for attitude

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.749	1	-	-	-	-	-
3. Internet use	0.722	0.741	1	-	-	-	-
4. Social networking site use	0.597	0.587	0.644	1	-	-	-
5. Incident reporting	0.702	0.644	0.572	0.661	1	-	-
6. Working remotely	0.792	0.775	0.829	0.586	0.556	1	-
7. Information handling	0.845	0.913	0.756	0.649	0.711	0.758	1

Correlations for behaviour

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.681	1	-	-	-	-	-
3. Internet use	0.691	0.725	1	-	-	-	-
4. Social networking site use	0.771	0.646	0.835	1	-	-	-
5. Incident reporting	0.598	0.612	0.626	0.647	1	-	-
6. Working remotely	0.815	0.683	0.718	0.805	0.462	1	-
7. Information handling	0.617	0.724	0.662	0.631	0.575	0.607	1

Table 10: Correlations for IT specialists

Correlations for knowledge

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.467	1	-	-	-	-	-
3. Internet use	0.406	0.428	1	-	-	-	-
4. Social networking site use	0.334	0.395	0.671	1	-	-	-
5. Incident reporting	0.259	0.295	0.612	0.588	1	-	-
6. Working remotely	0.326	0.303	0.413	0.404	0.457	1	-
7. Information handling	0.490	0.500	0.394	0.449	0.406	0.499	1

Correlations for attitude

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.411	1	-	-	-	-	-
3. Internet use	0.351	0.415	1	-	-	-	-
4. Social networking site use	0.306	0.372	0.584	1	-	-	-
5. Incident reporting	0.384	0.378	0.444	0.523	1	-	-
6. Working remotely	0.404	0.347	0.661	0.528	0.424	1	-
7. Information handling	0.430	0.555	0.477	0.489	0.362	0.559	1

Correlations for behaviour

Focus area	1	2	3	4	5	6	7
1. Password management	1	-	-	-	-	-	-
2. E-mail use	0.344	1	-	-	-	-	-
3. Internet use	0.103	0.187	1	-	-	-	-
4. Social networking site use	0.129	0.310	0.592	1	-	-	-
5. Incident reporting	0.185	0.343	0.211	0.178	1	-	-
6. Working remotely	0.479	0.290	0.379	0.3736	0.121	1	-
7. Information handling	0.294	0.470	0.208	0.2245	0.393	0.411	1

Table 11: Correlations for others (group 3) in the main study