Investigating personal determinants of phishing and the effect of national culture

Waldo Rocha Flores
Department of Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, Sweden
Hannes Holm
Swedish Defense Research Agency (FOI), Linköping, Sweden
Marcus Nohlberg
School of Informatics, University of Skövde, Skövde, Sweden, and
Mathias Ekstedt
Department of Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, Sweden

Received 5 May 2014
Revised 29 July 2014
Accepted 1 August 2014

Abstract

Purpose – The purpose of the study was twofold: to investigate the correlation between a sample of personal psychological and demographic factors and resistance to phishing; and to investigate if national culture moderates the strength of these correlations.

Design/methodology/approach – To measure potential determinants, a survey was distributed to 2,099 employees of nine organizations in Sweden, USA and India. Then, the authors conducted unannounced phishing exercises, in which a phishing attack targeted the same sample.

Findings – Intention to resist social engineering, general information security awareness, formal IS training and computer experience were identified to have a positive significant correlation to phishing resilience. Furthermore, the results showed that the correlation between phishing determinants and employees' observed that phishing behavior differs between Swedish, US and Indian employees in 6 out of 15 cases.

Research limitations/implications – The identified determinants had, even though not strong, a significant positive correlation. This suggests that more work needs to be done to more fully understand determinants of phishing. The study assumes that culture effects apply to all individuals in a nation. However, differences based on cultures might exist based on firm characteristics within a country. The Swedish sample is dominating, while only 40 responses from Indian employees were collected. This unequal size of samples suggests that conclusions based on the results from the cultural analysis should be drawn cautiously. A natural continuation of the research is therefore to further explore the generalizability of the findings by collecting data from other nations with similar cultures as Sweden, USA and India.

Originality/value – Using direct observations of employees' security behaviors has rarely been used in previous research. Furthermore, analyzing potential differences in theoretical models based on national culture is an understudied topic in the behavioral information security field. This paper addresses both these issues.

Keywords Cultural differences, Social engineering, Direct observation, Phishing, Security behavior

Paper type Research paper

Information & Computer Security
Vol. 23 No. 2, 2015
pp. 178-199
© Emerald Group Publishing Limited
2056-4961
DOI 10.1108/ICS-05-2014-0029

1. Introduction

Ensuring information security within an enterprise is highly prioritized among enterprise decision-makers. The reason for this is that any event that leads to companies' information assets being lost or compromised can be very costly and can even lead to bankruptcy (Moskal, 2006). Thus, it is imperative to make every effort to ensure that a company's information systems are protected against the growing range of threats that is arrayed against its information systems. Traditionally, the dominant part of investments to threats to information security has been spent on countermeasures of technical nature, and over the years, the effectiveness and robustness of those technical countermeasures have increased substantially. This development has made it more difficult to successfully attack an organization's information systems using purely technical means. As a consequence, attackers have developed techniques that bypass the robust technical controls by attacking the human element in an organization (Applegate, 2009). These techniques are used to manipulate people into performing actions that benefit the attacker and goes under the name of social engineering. One type of social engineering is phishing, which is a social engineering attack launched through e-mail. Phishing includes some type of deceptive technique to make victims click on a malicious link and install malware on their computers or reveal personal passwords (Mitnick and Simon, 2002). To help organizations successfully combat phishing in practice, researchers need to understand why some organizational employees resist phishing better than others; that is, what factors shapes the behavior of employees who do not fall victim to phishing. Limited empirical research has, however, been conducted in professional organizations where the study setting reflects actual attacks targeting employees that have not been debriefed previous to the study. One explanation for this is that obtaining data of employees' actual behavior is a challenging endeavor (Crossler *et al.*, 2013). This can be explained by the difficulties to convince organizational managers to participate in studies in which their employees' actual behavior is being measured without debriefing them. Furthermore, few empirical studies have identified personal psychological and demographic factors that correlate with employees' phishing resilience (with an exception of Workman, 2007; Holm *et al.*, 2013 and Rocha Flores *et al.*, 2014). In this paper, the first purpose is to extend the understanding of phishing behaviors in practice by examining why some employees do not fall victim to phishing; hence, we aim at identifying significant personal psychological and personal demographic determinants of resistance to phishing. The personal psychological determinants of resistance to phishing tested in the current study where identified in previous work (Rocha Flores and Ekstedt, 2012, 2013). To fulfill the first purpose of the study, the following research question was formulated:

RQ1. Which personal psychological and demographic factors significantly influence employees' resistance to phishing?

To answer the research question, we conducted empirical studies at nine organizations in Sweden, USA and India, in which we first distributed a survey capturing personal psychological and personal demographic measures to a sample of 2,099 employees of the participant organizations. Then, we conducted an unannounced phishing exercise targeting the same sample.

As we collected data from three different countries, an interesting question can now be raised: are the determinants of resistance to phishing consistent across those different national cultures? Behavioral information security research studies that have tested different theories (e.g. deterrence theory, theory of planned behavior) explaining reasons why some employees engage in risky behavior have provided inconsistent results (D'Arcy and Herath, 2011; Sommestad and Hallberg, 2013). One proposed explanation for these disparate findings is that the theories have not been tested for their validity across different cultural settings (Karjalainen *et al.*, 2013; Sommestad and Hallberg, 2013). This implies that national culture could have a moderating effect on the theoretical relations, hence changing the strength of the correlations by making them stronger, weaker or non-significant. Therefore, the second purpose with the research presented in this paper is to examine if the effect of personal psychological and demographic factors on employees phishing security behaviors differs based on national culture. We analyzed data collected from Sweden, USA and India; and, according to Hofstede's (2014) national culture indices, these countries are culturally different. To attain the second objective of the study, the following research question was specified:

RQ2. Will the effect of psychological and personal factors on employees' resistance to phishing differ between Swedish, US and Indian employees?

The conceptual model that combines those two purposes is presented in Figure 1.

The rest of the paper unfolds as follows. The next section presents a literature review and the study's proposed hypotheses. The section that follows discusses the methodology of the research conducted. Then, the results of the empirical studies are presented. The last section of this paper is devoted to discussing the findings and conclusions.

2. Literature and hypotheses

Existing empirical work on phishing behavior captured through unannounced phishing experiments aims at obtaining a better sense of the actual level of security among individuals. Jagatic *et al.* (2007) phished university students to acquire the students login information and investigated if including context information related to the victim in the e-mail increases the probability for a successful attack. The results showed that when context data gathered from social networks are used in the e-mail, 72 per cent of the students submitted valid logins, while when not using context data collected from social networks, 16 per cent fell for the attack. West Point Military Academy used phishing experiments to train their students to more effectively resist phishing (Dodge *et al.*, 2007). Their approach was to conduct two phishing attacks, and assess if training efforts given by discussing the first attack were effective. The first attack deceived 80 per cent of the students, while the second only managed to deceive 40 per cent. Mohebzada *et al.* (2012) conducted a phishing exercise in a university community and performed two phishing attacks that targeted a sample of

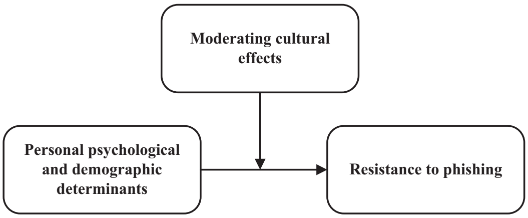
Moderating cultural effects
Personal psychological and demographic determinants
Resistance to phishing

Figure 1.
Conceptual model

10,000 individuals, including university faculty, staff and students. The results showed that 8.7 per cent fell for the first attack and 2 per cent fell for the second attack. In an experiment conducted by Bakhshi *et al.* (2009), a phishing mail was sent out to organizational employees as a mean to provide empirical evidence of how many employees succumb to social engineering. The experiment was ceased after approximately 3.5 hours. During that period of time, 23 per cent of recipients were fooled by the attack. The e-mail included factors related to how the attacker constructs the attack (e.g. trusted e-mail source, attention-grabbing subject and type of social engineering technique used) to understand why people fall victim to social engineering.

While all aforementioned phishing studies provide empirical evidence of how many organizational employees fall victim to phishing, they fail to provide empirical data on personal factors shaping behaviors to resist phishing collected by conducting unannounced phishing experiments in professional organizations. In fact, we only found three studies (Workman, 2007; Holm *et al.*, 2013; Rocha Flores *et al.*, 2014) that managed to capture personal factors explaining resistance to social engineering through conducting unannounced phishing experiments at professional organizations.

2.1 Personal psychological determinants of phishing

As previously mentioned, we identified personal psychological variables that may have an effect on social engineering security behaviors in previous work. This was conducted through two inductive studies (Rocha Flores and Ekstedt, 2012; Rocha Flores and Korman, 2012). Among the identified variables, we wanted to test the direct effect of five variables:

(1) intention to resist social engineering (I);

(2) self-efficacy regarding phishing (SE);

(3) information security policy awareness (ISPA);

(4) general information security awareness (GISA); and

(5) formal IS training (FT).

The interested reader can turn to the aforementioned sources for further details on how the variables were established. Based on the identification of potential personal psychological antecedents of resistance to phishing, the following hypotheses were formally stated:

H1. There exists a positive correlation between employees' intention to resist social engineering and their actual phishing behavior.

H2. There exists a positive correlation between employees' self-efficacy regarding phishing and their actual phishing behavior.

H3. There exists a positive correlation between employees' ISPA and their actual phishing behavior.

H4. There exists a positive correlation between employees' GISA and their actual phishing behavior.

H5. There exists a positive correlation between FT and employees' actual phishing behavior.

2.2 Personal demographic determinants of phishing

To capture personal demographic determinants of phishing, we included *age* and *gender* in the survey instrument. Age and gender have been studied on previous occasions (Workman, 2008; Dhamija *et al.*, 2006; Sheng *et al.*, 2010). Furthermore, *computer experience* has been studied on several occasions and operationalized in various ways, e.g. as general knowledge of computer and as the number of hours an individual spend on a computer each week (Moos and Azevedo, 2009; Rhee *et al.*, 2009). This study operationalizes *computer experience* as the number of years an employee has utilized information technology products and services (e.g. computers, Internet access, e-mail, etc.). Based on the identification of potential personal demographic determinants of resistance to phishing, the following hypotheses are formally stated:

H6. There exists a positive correlation between employees' computer experience and their actual phishing behavior.

H7. There exists a positive correlation between employees' age and their actual phishing behavior.

H8. There exists a positive correlation between employees' gender and their actual phishing behavior.

2.3 The role of national culture

A predominantly used cultural framework in the IS research context (Srite and Karahanna, 2006) is the framework proposed and validated by Hofstede (1993), in which culture is defined as: "the collective programming of the mind that distinguishes one group or category of people from another" (Hofstede, 1993). The cultural framework is currently based on five distinct dimensions: power distance (PDI), individualism versus collectivism (IDV), masculinity versus femininity (MAS), uncertainty avoidance (UAI), pragmatism (PRA) and indulgence (IND) (Hofstede, 2014). Further, the theoretical arguments are given for devising hypotheses about national culture. An important note is that we only test the relationship between personal psychological factors and phishing behaviors; hence, not all relationships are tested for the potential changes in their strengths based on national culture. The reason is that it is theoretically difficult to argue that culture moderates all relationships.

According to Hofstede, US persons are individualists in nature, while both Swedish and Indian persons pertain to a collectivist culture. In a collectivist culture, persons perceive opinion of their colleagues and others' peers to be important, while in individualist cultures, such as the American culture, persons care less about the opinions of their peers and, therefore, can be optimistic about their actions and behaviors. Goal- and achievement-oriented individuals from a masculine culture will, furthermore, be more prone to act based on their individually formed convictions, which are not evident for individual to form a feminine society, and the fact that Americans have the most individualistic drive in the world leads to all Americans showing their masculine drives individually.

Sweden and India scores higher on the pragmatism dimension than the USA, which is considered a less pragmatic society. The fact that Americans strive for quick results within the work place, together with the fact that Americans have the "can-do" mentality, as mentioned above, may lead to them strongly believing that they can predict their behavior accurately based on their individual perceptions, while more pragmatic individuals recognize their limitations and predict their behavior differently. Based on the theoretical arguments presented above, we propose that the effect of intention and self-efficacy on their actual phishing behavior will vary between Americans, Swedish and Indian employees. Hence:

H9a. The correlation between employees' intention to resist social engineering and their observed phishing behavior differs between Swedish, US and Indian employees.

H9b. The correlation between employees' self-efficacy regarding phishing and their observed phishing behavior differs between Swedish, US and Indian employees.

The critical role of technology awareness has previously been tested by Dinev *et al.* (2009) in the context of information security policy compliance. The authors believe that the formation of user attitudes and behavioral intention would differ based on culture. They argue that it is important to understand how awareness of an existing problem would influence the formation of an individual's attitude toward a specific security behavior related to the problem. Sweden and USA score high in the indulgence dimension, which indicates that those cultures are of indulgence, while India receives a low score in this dimension; hence, it is a restrained culture. Individuals from a society of indulgence tend not to control their desires and impulses for enjoying life and having fun, but, as they are normative, they work hard and strive for quick results within the work place. This leads to the contradictory attitudes such as: "work hard and play hard". On the contrary, societies with a low score in this dimension, such as India, have a tendency to cynicism and pessimism. Consequently, a person who is aware of a problem and who comes from an indulgent society is more optimistic toward the issue. Furthermore, culture with both higher masculinity (achievement, "can-do", "act-now" attitude) and higher individualism ("act regardless of what others think") may influence the effect of security awareness and training endeavor. Hence:

H9c. The correlation between employees' information security policy awareness and their observed phishing behavior differs between Swedish, US and Indian employees.

H9d. The correlation between employees' general information security awareness and their observed phishing behavior differs between Swedish, US and Indian employees.

H9e: The correlation between formal IS training and observed phishing behavior differs between Swedish, US and Indian employees.

To conclude the section in which the description of how the hypotheses were formed, all hypotheses are presented in Figure 2.

3. Methodology

This section presents how our instrument to measure the study constructs was developed, and how we measured the study participants' actual phishing behavior through direct observation. Figure 3 illustrates the main stages of the empirical study conducted in the current study.

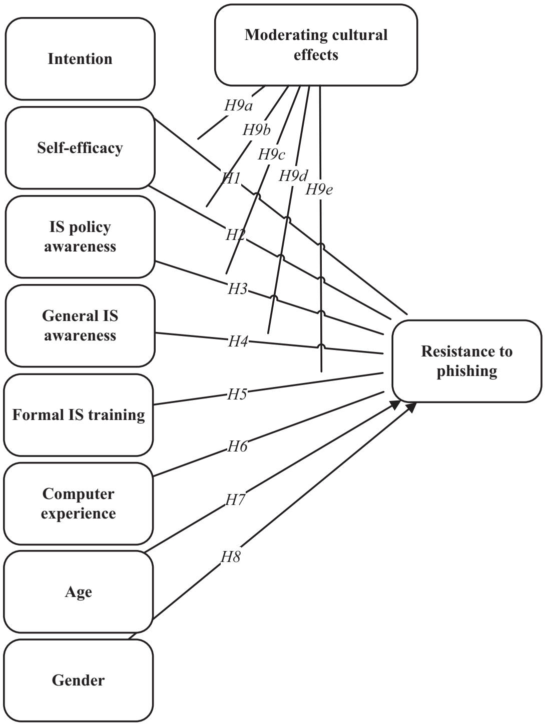

Figure 2.
The study's proposed hypotheses

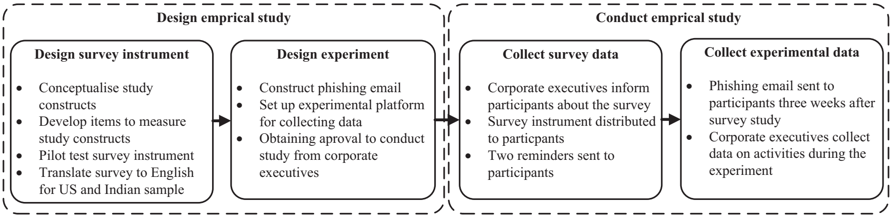
Design emprical study
Design survey instrument
Conceptualise study constructs
Develop items to measure study constructs
Pilot test survey instrument
Translate survey to English for US and Indian sample
Design experiment
Construct phishing email
Set up experimental platform for collecting data
Obtaining aproval to conduct study from corporate executives
Conduct emprical study
Collect survey data
Corporate executives inform participants about the survey
Survey instrument distributed to particpants
Two reminders sent to participants
Collect experimental data
Phishing email sent to participants three weeks after survey study
Corporate executives collect data on activities during the experiment

Figure 3.
Main stages of empirical study

3.1 Design survey instrument

To assure that the studied personal psychological constructs include items that actually capture the theoretical meanings of the constructs (i.e. establish construct validity), effort was placed on the instrument validation process, as recommended by MacKenzie *et al.*, 2011. Among the investigated determinants, ISPA and GISA had not been tested in behavioral information security research domain to the same extent as the intention and self-efficacy constructs, which are derived from the well-established theory of planned behavior (Ajzen, 1991). Therefore, we decided to conceptualize these two constructs to avoid problems with construct validity (due to measurement issues) and statistical conclusion validity (due to biasing effect of measurement model misspecification) (MacKenzie *et al.*, 2011). For the interested reader, the conceptualization process can, in more detail, be found in the study by Rocha Flores and Korman (2012). Below is a short summary of this process.

The conceptualization of constructs in this study had three main objectives:

(1) provide a clear, concise and unambiguous conceptual definition of the constructs;

(2) specify the conceptual theme of the constructs (e.g. assessing if the construct is unidimensional or multidimensional); and

(3) evaluate the comprehensiveness of the constructs' dimensions (i.e. the relevance each dimension has to its focal construct and if any dimensions are missing to capture its construct).

In line with those objectives, the following two steps were carried out:

(1) effort was spent on defining the constructs as clear and unambiguous as possible; and

(2) a survey – capturing data on our proposed conceptual definitions, our assessment of the construct conceptual theme and the comprehensiveness of the constructs' dimensions – was designed and distributed to 120 content experts.

Using content experts, rather than members from enterprises, has shown to provide reliable results and is commonly used in health research where the quality of measurement instrument is of significant importance (Lynn, 2006). In all, 18 content experts completed the survey. To capture data on our conceptual definitions and assessment of the construct conceptual theme, open-ended questions were included.

The following step was taken to generate a set of measurement items that represents the conceptual domain of the constructs. As the intention and self-efficacy constructs are derived from the well-established theory of planned behavior, and tested in behavior information security research domain in a vast amount of studies (Sommestad and Hallberg, 2013), the items were developed inspired on existing scales that have been proven reliable (Bulgurcu *et al.*, 2010). However, we attempted to develop the items in the context of social engineering security attacks. Therefore, the items were written in a form that conveys information about social engineering. For instance, for the intention construct, we included phrases such as: "[…]. I suspect that the request originates from a non-legitimate sender […]", "[…] who I suspect of being non-legitimate from installing malicious software […]", "[…] who I suspect of being unauthorized or non-legitimate from gaining access to my work computer by means of a security attack.". For the ISPA and GISA constructs, which we perceived not as validated as the other two constructs, we first wanted to assess the content validity of the items before colleting primary data, as recommended by MacKenzie *et al.* (2011).

3.1.1 Content validity assessment and pilot testing. Content validity is "the degree to which items in an instrument reflect the content universe to which the instrument will be generalized (Straub *et al.*, 2004, p. 424)", is an assessment that consists of two stages: development and judgment-quantification (Lynn, 2006). The development stage consists of identification of study constructs, item generation and instrument. Judgment-quantification, entails asking a number of experts to evaluate the validity of the items and as a set (DeVellis, 1991). In the present study, we quantitatively assessed the content validity using the item-sorting method proposed by Anderson and Gerbing (1991). The investigated items were tested for their content validity by collecting data using an e-mail survey distributed to 452 content domain experts, of which 51 completed the survey. We also asked for comments on wording, if the survey items were clearly understood and if they perceived that any items were missing to represent the constructs. Based on this pre-test, the measurement instrument was revised, and the initial item pool of developed items representing the ISPA and GISA constructs was reduced to six items with an adequate degree of content validity (for more information on specific changes, the interested reader is referred to Rocha Flores and Antonsen, 2013). All developed items capturing the four personal psychological constructs were measured on an eleven-point Lickert scale from 0 to 10 inspired by Paternoster and Simpson (1996) and Siponen and Vance (2010).

The entire survey was developed in Swedish, and was pilot tested by 47 professional information technology (IT) users, which completed the survey and were asked for comments on wording, if the survey items were clearly understood and if the survey could be improved. Based on this pre-test, minor corrections were made to the wording of the items. Then, the instrument was proofread and translated to English by a professional translation and interpreting company (the final items measuring the study constructs can be found in Appendix 1).

3.2 Design of experiment

The attack in the experiment concerned an update of well-known software for displaying, printing and managing documents which was used on all computers in the enterprise. In this paper, the name of the software is Knylo Reader (the name is obfuscated through ROT10). The software product, that the e-mail claims to update, is in the enterprise updated through a service which is installed along with the application. The attack is not targeted at any particular user or organization; from an attackers perspective, a recipient is the only information that is required. To ensure that the used phishing e-mail reflects a generic real-world phishing e-mail, the content of the e-mail was written based on real phishing e-mails retrieved from the Web site www.millersmiles.co.uk. Furthermore, social engineering techniques such as attention-grabbing subject and potential psychological triggers were used (informing the recipient that it would be beneficial and important for the recipient to install the software upgrade). Prior to the current study, a smaller study was conducted (Holm *et al.*, 2013) that gave the researchers valuable information on what could be improved when conducting the phishing experiments. For instance, the e-mail was reviewed by senior executives of the participant organization, and participant feedback captured by a follow-up survey gave the researchers knowledge about performing the experiment, which was then used as an input to plan and perform the current study. In the current study, the IT managers of the participant organizations, and two Chief Executive Officer's (CEO's) of the participant organizations, reviewed the e-mail once again. No comments regarding potential improvement or changes to the structure of the e-mail was received. Thus, we concluded that the structure and content of the e-mail was satisfying and ready to be used in the current study (the structure of the final phishing e-mail can be found in Appendix 2).

As the research approach involved deception, we made everything possible to assure ethical treatment of the human subjects (e.g. all information had to be handled in a manner that ensured integrity and confidentiality of data), and followed the guidelines by Jakobsson and Ratkiewicz (2006). To collect data on phishing behavior, an SMTP server (Postfix) and an HTTP server (Apache) were set up at the university. A small Ruby script was used to automate the process of interfacing with the SMTP server, and a "malicious" e-mail was sent to each employee. Every e-mail included a link to the HTTP server at the university. Each of these links included a unique argument that could be used to identify the "victim". The e-mail was spoofed from support@knylo.com and the user was requested to download the latest version of their software (version 11, which was not released yet at the time of the study). When an employee clicked on the link in the e-mail, he or she reached the HTTP server at the university. The domain (www.knldownloads.com) was used to point to the "malicious" HTTP server at the university. The HTTP server was set up to:

- log user information through a PHP script; and
- to automatically send a "malicious" binary (written in C++ and compiled for Windows systems) to anyone browsing its contents.

This binary did not install anything on the system – it served as a one-time SMTP client. When executed, it read the name of the system and the logged-in user, and sent this information to the e-mail account of one of the researcher (through the mentioned SMTP server at the research department). When the binary had read the system variables and sent these to the researcher, it abruptly ended, giving the end-user an error message. The binary had a credible product icon, but with no real certificate (thus, required the victim to click "yeas" on the "run untrusted product dialogue" given by Windows operating systems for software without trusted certificates). The researchers were then notified that the binary had been executed, when it was executed, whom that executed it and on which system that it was executed. System compromise for the experiment could thus occur both by execution of the binary and by simply browsing the content of the Web server, i.e. a drive-by-download (Provos *et al.*, 2008). The latter is a frequently used means of malware infection (e.g. used by the black hole exploit kit) and involves exploitation of a vulnerability in the Web browser (or its resources) of a visiting user.

2.3 Conduct empirical study

Empirical data were collected from May 2012 to June 2013. As already mentioned, the data collection consisted of two parts:

(1) a survey was distributed, which included questions to measure the study constructs; and

(2) direct observations were performed through an unannounced phishing experiment.

Before collecting data, corporate executives from each participant organization were contacted to get their approval for the study. These individuals were also the only employees aware of the study beforehand. Furthermore, corporate executives facilitated the data collection by sending out a message to the participant employees who were encouraged to complete a survey managed by researchers interested in measuring perceptions on IT usage. Hence, the employees were not informed that the survey collected data on information security and their risk behavior. We were then provided with each organization's company directory including e-mail addresses to each participant. First, each participant in each organization was contacted by e-mail and asked to complete the questionnaire survey, and they were assured of the confidentiality of their responses. The survey was hosted by a widely used Internet-based application (SurveyMonkey). Two reminders were sent to non-responding participants after a first week and a third week to increase the response rate. Then, a phishing experiment was conducted three weeks after the deadline of the survey. During the experiments, the corporate executives involved in the studies collected data during the attacks including employee reactions.

3.4 Characteristics of participant organizations

The nature of the study is such that details about the organizations cannot be presented, but general characteristics of the participant organizations and respondents are shown in Tables I and II.

4. Results

Before conducting correlation tests, we needed to conduct an exploratory factor analysis to ensure that the unidimensionality criterion is satisfied, which refers to items converging in the corresponding constructs; hence, each construct has items that are related to it better that to any other construct (Urbach and Ahlemann, 2010). If each item loads on the construct, they intend to capture with a coefficient value above 0.6, the unidimensionality criterion is deemed to be satisfied (Gerbing and Anderson, 1988). Furthermore, for adequate internal consistency, Cronbach's alpha values should be higher than 0.7. High Cronbach's alpha value assumes that all items related to a construct measure the same thing (Nunnally and Bernstein, 1994). As Table III shows, all items load to their respective construct with a value above the threshold value of 0.6, and the Cronbach's alpha values are above the recommended threshold value of 0.7. This suggests that problems with unidimensionality and internal consistency reliability were not an issue in this study.

4.1 Survey results

The survey was sent to the 2,099 participants of the study. In total, 431 respondents (20.5 per cent) completed the survey. To enable correlation tests, mean value of the items was calculated, which yielded a unique construct score per respondent. Descriptive results are displayed in Table IV.

Table I.
Characteristics of participant organizations

Organization	No. of employees in the study ($N = 2{,}099$)	Industry	Country
1	20	IT industries	Sweden
2	49	Energy	Sweden
3	23	Manufacturing	Sweden
4	37	Municipality	Sweden
5	1,123	Manufacturing	Sweden
6	564	Manufacturing	USA
7	20	IT industries	Sweden
8	32	Energy	Sweden
9	231	Manufacturing	India

Information about respondents	Frequency	(%)
Gender		
Male	324	75
Female	107	25
Age (years)		
18-24	10	2
25-34	85	20
35-44	117	27
45-54	136	32
55 or older	83	19
Computer experience		
1-4	5	1
5-9	21	5
10-14	80	19
15-20	126	29
20 or more	199	46
Formal training		
Training	98	23
No training	333	77

Table II. Information about respondents

Construct	Item	Loading	Cronbach's alpha
Intention	I1	0.831	0.879
	I2	0.853	
	I3	0.876	
	I4	0.754	
	I5	0.757	
ISP awareness	ISPA1	0.887	0.879
	ISPA2	0.879	0.746
	ISPA3	0.810	
	ISPA4	0.680	
General IS awareness	GISA1	0.791	
	GISA2	0.823	
Self-efficacy	SE1	0.906	0.950
	SE2	0.894	
	SE3	0.911	
	SE4	0.897	

Table III. Scales, loadings and Cronbach's alpha

Descriptive survey results	Mean	SD	*N*
I	9.667	0.815	431
SE	7.891	2.262	431
ISPA	6.807	2.473	431
GISA	8.000	1.962	431

Table IV. Descriptive survey results

4.2 Experiment

An overview of the results from the phishing experiment can be seen in Table V. The malicious Web site was visited 257 times by 193 unique participants, or 9.2 per cent of the participants. Thus, there were several participants that clicked on the malicious link more than once. There were 151 executions of the malicious binary by 103 unique participants or 4.9 per cent of the participants. A remarkable finding was that two participants with administrator credentials executed the binary several times (two and four times, respectively). During the experiment, senior IT managers received reports from security-aware employees. As the experiment was supposed to be representative to an actual attack in practice and we wanted to capture management behavior during this event, the IT managers were told to act as they normally do in an event of a security attack. Therefore, the experiment was ceased by the IT managers sending out a warning about the e-mails, after approximately 30 minutes. However, there were still employees trying to access the malicious Web site after the official warning (and knowing that it in fact was malicious). The last attempt to access the malicious Web site occurred 64 hours after attack. We can think of two possible reasons that explain this phenomenon:

(1) curiosity; and

(2) not knowing the dangers involved when browsing malicious Web sites.

4.3 Factors explaining why employees resist phishing

One of our purposes was to evaluate individual factors that explain why some employees resist phishing better than others. To analyze the relationship between study constructs and observed behavior, point-biserial correlation was used. The point-biserial correlation coefficient is a special case of Pearson correlation and can handle dependent variables that are operationalized as scale variables and dichotomous variables. For the dichotomous variable, the values typically are 1 (presence) and 0 (absence) (Glass and Hopkins, 1995). Thus, this analysis technique fits the purpose of study and the observed phishing behavior was used as a dichotomous variable with two states: 1 (did not resist phishing) and 0 (did resist phishing).

To maximize the sample size for the correlation analysis, the analysis was based on individuals clicking on the "malicious" link. Furthermore, we could only use data from participants who had completed the distributed survey ($n = 431$), and among those participants 82 participants clicked on the "malicious" link. The results from the correlation analysis are shown in Table VI. The personal psychological factors that we found had a positive significant correlation to an employee's phishing behavior which were intention ($r = 0.125$**), GISA ($r = 0.100$*) and FT ($r = 0.122$**). While, neither age nor gender had a significant correlation to phishing resilience, computer experience ($r = 0.100$*) was identified to have a positive significant correlation to phishing resilience.

Table V. Overall results from the phishing experiment

Phishing attack	No.	(%)
Click link	193	9.2
Execute binary	103	4.9

4.4 Analysis on national cultural differences

To examine if the correlation between the determinants of phishing differs based on national culture, the data set was split in three groups: Swedish, US and Indian employees. The same point-biserial correlation test that was conducted for the full data set was then performed for each group. The results of these tests are shown in Table VII. Table VII shows that a positive correlation between intention and observed behavior for the Swedish sample exists (r = 0.114*); however, the correlation is non-significant for the US and Indian sample. The same holds for the correlation between GISA and observed behavior; the correlation is significant for the Swedish sample (r = 0.151*), but non-significant for the US and Indian sample. The correlation between FT and phishing resilience were stronger for the US sample (r = 0.200*) than the Swedish sample (r = 0.108*), while non-significant for the Indian sample.

We found significant correlation for one sample, while non-significant correlation for another sample leads to the conclusion that there clearly is a difference of correlation between the two cultures; that is, the correlation holds for one cultural context while not for another culture. In one group comparisons (FT), we identified positive and significant correlation for at least two cultures, and we therefore conducted a test to identify if the difference between the two independent correlation coefficients were significant. The test was conducted based on the recommendations by Preacher (2002): first, each correlation coefficient is converted into a z-score using Fisher's r-to-z transformation. Then, making use of the sample size used to obtain each coefficient, these z-scores are compared using formula 2.8.5 from Cohen and Cohen (1983, p. 54). The

Constructs	Resistance to phishing (r)
Intention	0.125**
Self-efficacy	0.024 ns
Information security policy awareness	0.003 ns
General information security awareness	0.100*
Formal IS training	0.122*
Computer experience	0.100*
Age	0.020 ns
Gender	0.050 ns

Notes: *Indicates statistically significant at $p < 0.05$; and **$p < 0.01$

Table VI. Significance of individual antecedents

	Resistance to phishing (r)		
Constructs	Sweden (N = 280)	USA (N = 111)	India (N = 40)
Intention	0.114*	0.090	0.216
Self-efficacy	0.065	−0.037	−0.073
Information security policy awareness	0.026	−0.060	0.022
General information security awareness	0.151*	0.044	−0.129
Formal IS training	0.108*	0.200*	0.097

Note: *Indicates statistically significant at $p < 0.05$

Table VII. Overall results from testing the effect of culture

result of this test is shown in Table VIII, and it shows that no significant difference of correlation coefficients between FT and phishing resilience were identified (– stands for a significant correlation for one sample, while non-significant correlation for another sample; n/a stands for both correlations being non-significant).

5. Discussion and conclusions

The first main objective with the research presented in this paper was to determine which personal psychological and demographic factors significantly influence employees' resistance to phishing. The second purpose was to examine if the effect of psychological and personal factors on employees' resistance to phishing differ between Swedish, US and Indian employees. The discussion is organized around these two main objectives.

The first objective was attained through testing eight hypotheses, which aimed at identifying significant determinants of phishing resilience. To test the hypotheses, a survey instrument was first developed to measure the investigated factors, and used to collect empirical data at nine organizations in Sweden, USA and India. Then, to capture observed behavior, we performed an unannounced phishing experiment at the same organizations. The personal psychological factors that we found had a positive significant correlation to an employee's phishing behavior which were intention, GISA and FT. While, neither age nor gender had a significant correlation to phishing resilience, computer experience was identified to have a positive significant correlation to phishing resilience. This answers *RQ1* posed by the study.

Intention to resist social engineering, GISA, FT and computer experience had, even though not strong, a significant positive correlation. This suggests that it could be reasonable for managers to both assess phishing resilience in an organization using various surveys measuring those constructs and working with changing the employees' intentions, GISA and implement formal computer and IS training programs to enhance resistance to phishing.

The phishing experiment resulted in many employees falling victim to phishing. This is quite alarming in general. In essence, many attacks only require that one host is infected to spread malware to further spread or targeted attacks to move further toward its final goal. The phishing mail sent in the experiment was designed as a generic or traditional mail and not targeted at any particular user or organization; from an attackers perspective, a recipient is the only information that is required. This suggests that it would still be possible for attackers to get a foothold within organizations with a quite moderate effort. Furthermore, multiple individuals browsed the server several

Table VIII. Significance of correlation coefficient differences for Swedish, US and Indian sample (RtP = resistance to phishing)

	Δ Correlation coefficient		
Relationship	Sweden–USA	Sweden–India	USA–India
Intention → RtP	–	–	n/a
Self-efficacy → RtP	n/a	n/a	n/a
Information security policy awareness → RtP	n/a	n/a	n/a
General information security awareness → RtP	–	–	n/a
Formal IS training → RtP	0.092 ns	–	–

Note: ns indicates statistically non-significant times even though they knew that it was "malicious". This clearly shows that some individuals do not understand the dangers involved in browsing the Web. Organizations should, therefore, direct efforts on educating their employees on risks associated with clicking on links, and also enforce warnings about correct and secure behavior in the event of an attack.

The second objective was to examine if the effect of psychological and personal factors on employees' resistance to phishing differ between Swedish, US and Indian employees. The results show that for Swedish employees the intention and GISA were significantly correlated with behavior, while these correlations were non-significant for US and Indian employees. Hence, as argued in the hypotheses section, the results of the study points at differences in how Swedish, US and Indian employees perceive their intention to resist social engineering and how they behave in practice. One explanation for this difference could be that in Sweden – which is seen as a less individualist, feminine country – employees tend to not try to lift themselves above others, as the Swedish culture is based around not too much, not too little; thus, everything should be conducted in moderation (Hofstede, 2014). Hence, employees from a more feminine country may not want to stand out by overestimating their intention about performing a behavior in question and their information security awareness and, therefore, predict behavior more accurately, while goal- and achievement-oriented individuals from masculine cultures such as the USA and India will be more prone to act based on their individually formed convictions, which leads to less accurate and non-significant predictions.

For the Swedish and US sample, we identified a significant positive correlation between FT and resistance to phishing, and it appeared stronger for the US sample. This relationship was, however, non-significant for the Indian sample. This difference is a cumulative result of the cultural dimensions individualism, masculinity, uncertainty avoidance, pragmatism and indulgence. However, at this point, we do not have a stronger explanation why this difference exists. More studies are required to more fully understand why this relationship differs between cultures. One explanation could, however, be that US security executives are more prone to implement FT programs to assure information security in their organization, while this might not be the case for Swedish and Indians organizations. This implies that US organizations may feel the need to develop policies centrally, make them visible and strongly enforce them. The results are consistent with the cultural theories explaining that a manager from a more individualist and masculine culture perceives the need to control their employees and not involve them in decisions (Jackson, 2000). Two examples showing the need for more or less control among executives from a more individualist culture is revealed in the 2013 Global State of Information Security Survey conducted by PWC Advisory Services & Security. The results from the survey showed that 54 per cent of North American have implemented employee security awareness training programs, while 42 per cent of European firms have implemented the same information security measures (PWC Advisory Services and Security, 2013). The results highlight the importance of understanding that national culture influences the relationship between an employee's intention and his or her behavior. Hence, national culture should be considered when designing effective information security programs that fit the cultural context of the country in which the firm operates.

Understanding that there is not a general solution to increase security awareness within an organization that works worldwide and that culture affects the behaviors and decision-making of their employees is especially important for organizations operating in a global environment. In summary, our results show that national culture has an influence on the correlation between phishing determinants and employees' observed phishing behavior differs between Swedish, US and Indian employees in 6 out of 15 cases (cf. Table VIII). This answers the second research question posed by the study (*RQ2*).

5.1 Limitations and future work

There exist several limitations which should be taken into account when interpreting the results. First, a general limitation is that we assume that the studied determinants can be measured using survey methods. Second, the correlations of the identified significant relationships are relatively weak, which points to the fact that other factors may have a stronger influence on phishing reliance. However, a similar study conducted in a professional organization in the USA (Workman, 2007) revealed that correlations between other investigated variables and social engineering security behavior had similar strengths, e.g. threat severity (0.12, $p < 0.05$); vulnerability (0.14, $p < 0.05$); trust (0.16, $p < 0.05$); and obedience (0.11, $p < 0.05$). A previous study (Rocha Flores *et al.*, 2014) conducted in three professional organizations in Sweden by the first two authors of this paper identified two personal psychological factors that had stronger correlation: trust (0.285, $p < 0.05$) and risk behavior (0.305, $p < 0.05$). Finally, the study by Halevi *et al.*, 2013 identified neuroticism as a predictor of phishing behavior (0.501, $p < 0.05$). However, this study was conducted among university students, and not among organizational employees. As the existing literature lacks in studies that have measured behavior using observations such as phishing experiments, this research can be seen as exploratory and more work needs to be done to fully understand determinants of phishing.

Third, while we focused on national culture, difference might exist between firms within a country. Hofstede's cultural measures – that are used in our study – generalize culture to an entire national population; that is, there is an assumption that culture effects apply to all individuals in that nation. This assumption has been challenged and that culture should be studied at the individual level as well (Markus and Kitayama, 1991; Kolodziej-Smith *et al.*, 2013). In our study, we did not test if characteristics of a firm (e.g. size, industry in which the firm operate in) yield differences in the examined correlations. Differences between firms within a country could be identified based on firm characteristics. We acknowledge the potential impact of these factors and, therefore, recommend including them in future work.

Fourth, limited research has been conducted to examine cross-cultural influences on information security behavior (Crossler *et al.*, 2013). Our study has investigated determinants of actual phishing behavior, and if these determinants differ based on national culture. To the best of our knowledge, this is the first study investigating both these issues. The study can, therefore, be seen as exploratory (this in particular is the case for the effect of national culture), which limits the generalizability of our findings. The Swedish sample is dominating, while we only collected responses from 40 Indian employees. This unequal size of samples suggests that conclusions based on the results from the cultural analysis should be drawn cautiously. A natural continuation of our research is, therefore, to further explore the generalizability of our findings by collecting data from other nations with similar cultures as Sweden, USA and India.

Finally, although we did not construct our own "malicious" Web site, which has shown to increase individuals' phishing vulnerability (Dhamija *et al.*, 2006), many employees still fell victim to phishing. We can only speculate the difference in the number of employees falling victim to the phishing attack if we had spoofed a legitimate Web site or constructed our own Web site that serves the purpose of the study.

References

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211.

Anderson, J.C. and Gerbing, D.W. (1991), "Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities", *Journal of Applied Psychology*, Vol. 76 No. 5, pp. 732-740.

Applegate, S.D. (2009), "Social engineering: hacking the wetware!", *Information Security Journal: A Global Perspective*, Vol. 18 No. 1, pp. 40-46.

Bakhshi, T., Papadaki, M. and Furnell, S. (2009), "Social engineering: assessing vulnerabilities in practice", *Information Management & Computer Security*, Vol. 17 No. 1, pp. 53-63.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Cohen, J. and Cohen, P. (1983), *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*, Erlbaum, Hillsdale, NJ.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90-101.

D'Arcy, J. and Herath, T. (2011), "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings", *European Journal of Information Systems*, Nature Publishing Group, Vol. 20 No. 6, pp. 643-658.

DeVellis, R.F. (1991), *Scale Development: Theory and Applications*, Sage, Newbury Park, CA.

Dhamija, R., Tygar, J.D. and Hearst, M. (2006), "Why phishing works", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, *Montreal*, pp. 581-590.

Dinev, T., Goo, J., Hu, Q. and Nam, K. (2009), "User behaviour towards protective information technologies: the role of national cultural differences", *Information Systems Journal*, Vol. 19 No. 4, pp. 391-412.

Dodge, R., Carver, C. and Ferguson, A. (2007), "Phishing for user security awareness", *Computers & Security*, Vol. 26 No. 1, pp. 73-80.

Gerbing, D.W. and Anderson, J. (1988), "An updated paradigm for scale development incorporating unidimensionality and its assessment", *Journal of Marketing Research*, Vol. 25 No. 2, pp. 186-192.

Glass, G.V. and Hopkins, K.D. (1995), *Statistical Methods in Education and Psychology*, 3rd ed., Allyn & Bacon.

Halevi, T., Lewis, J. and Memon, N. (2013), "A pilot study of cyber security and privacy related behavior and personality traits", *Proceedings of the 22nd International Conference on*

World Wide Web Companion, *Rio de Janeiro*, International World Wide Web Conferences Steering Committee, pp. 737-744.

Hofstede, G. (1993), "Cultural constraints in management theories", *Academy of Management Perspectives, Academy of Management*, Vol. 7 No. 1, pp. 81-94.

Hofstede, G. (2014), "National cultural dimensions", National Cultural Dimensions, available at: http://geert-hofstede.com/dimensions.html (accessed 17 March 2014).

Holm, H., Rocha Flores, W. and Ericsson, G. (2013), "Cyber security for a smart grid – what about phishing?", *Proceedings of the 4th European Innovative Smart Grid Technologies (ISGT) Conference*, *Lyngby*.

Jackson, T. (2000), "Management ethics and corporate policy: a cross-cultural comparison", *Journal of Management Studies*, Vol. 37 No. 3, pp. 349-369.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007), "Social phishing", *Communications of the ACM*, Vol. 50 No. 10, pp. 94-100.

Jakobsson, M. and Ratkiewicz, J. (2006), "Designing ethical phishing experiments", *Proceedings of the 15th International Conference on World Wide Web – WWW '06*, ACM Press, New York, NY, p. 513.

Karjalainen, M., Siponen, M., Petri, P. and Suprateek, S. (2013), "One size does not fit all: different cultures require different information systems security interventions", *PACIS 2013 Proceedings*, *Jeju Island*, Paper 98.

Kolodziej-Smith, R., Friesen, D. and Yaprak, A. (2013), "Does culture affect how people receive and resist persuasive messages? Research proposals about resistance to persuasion in cultural groups", *Global Advances in Business Communication*, Vol. 2.

Lynn, M.R. (2006), "Determination and quantification of content validity", *Nursing Research*, Vol. 35 No. 6, pp. 382-386.

MacKenzie, S.B., Podsakoff, P.M. and Podsakoff, N.P. (2011), "Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques", *MIS Quarterly*, Vol. 35 No. 2, pp. 293-334.

Markus, H.R. and Kitayama, S. (1991), "Culture and the self: implications for cognition, emotion, and motivation", *Psychological Review*, Vol. 98 No. 2, pp. 224-253.

Mitnick, K. and Simon, W. (2002), *The Art of Deception: Controlling the Human Element of Security, Controlling the Human Element of Security*, Wiley Publishing, Indianapolis, IN.

Mohebzada, J.G., Zarka, A., El, Bhojani, A.H. and Darwish, A. (2012), "Phishing in a university community: two large scale phishing experiments", *2012 International Conference on Innovations in Information Technology (IIT)*, *Abu Dhabi*, pp. 249-254.

Moos, D.C. and Azevedo, R. (2009), "Learning with computer-based learning environments: a literature review of computer self-efficacy", *Review of Educational Research*, Vol. 79 No. 2, pp. 576-600.

Moskal, E. (2006), "Business continuity management post 9/11 disaster report methodology", *Disaster Recovery Journal*, Vol. 19 No. 2.

Nunnally, J.C. and Bernstein, I. (1994), *Psychometric Theory*, 3rd ed., McGraw Hill, New York, NY.

Paternoster, R. and Simpson, S. (1996), "Sanction threats and appeals to morality: testing a rational choice model of corporate crime", *Law & Society Review*, Vol. 30 No. 3, pp. 549-584.

Preacher, K.J. (2002), "Calculation for the test of the difference between two independent correlation coefficients", available at: www.quantpsy.org

Provos, N., Mavrommatis, P., Rajab, M.A. and Monrose, F. (2008), "All your iFRAMEs point to us", *Proceedings of the 17th Conference on Security Symposium, USENIX Association, San Jose, CA*, pp. 1-15.

PWC Advisory Services and Security (2013), "The global state of information security® survey 2013", available at: www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

Rhee, H.-S., Kim, C. and Ryu, Y.U. (2009), "Self-efficacy in information security: its influence on end users' information security practice behavior", *Computers & Security*, Vol. 28 No. 8, pp. 816-826.

Rocha Flores, W. and Antonsen, E. (2013), "The development of an instrument for assessing information security in organizations: examining the content validity using quantitative methods", *Proceedings of the 2013 International Conference on Information Resources Management*, *Natal, 22-24 May*.

Rocha Flores, W. and Ekstedt, M. (2012), "A model for investigation organizational impact on information security behavior", *Proceedings of the 7th Annual Workshop on Information Security and Privacy*, *Orlando, FL, 16 December*.

Rocha Flores, W. and Ekstedt, M. (2013), "Countermeasures for social engineering-based malware installation attacks", *Proceedings of the 2013 International Conference on Information Resources Management*, *Natal, 22-24 May*.

Rocha Flores, W., Holm, H., Svensson, G. and Ericsson, G. (2014), "Using Phishing Experiments and Scenario-based Surveys to Understand Security Behaviours in Practice", *Information Management & Computer Security*.

Rocha Flores, W. and Korman, M. (2012), "Conceptualization of constructs for shaping information security behavior: towards a measurement instrument", *Proceedings of the 7th Annual Workshop on Information Security and Privacy*, *Orlando, FL, 16 December*.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Sheng, S. (2010), "Who falls for phish?", in *Proceedings of the 28th International Conference on Human Factors in Computing Systems – CHI '10, ACM Press, New York, NY*, p. 373.

Sommestad, T. and Hallberg, J. (2013), "A review of the theory of planned behaviour in the context of information security policy compliance", in Janczewski, L.J., Wolfe, H.B. and Shenoi, S. (Eds), *Security and Privacy Protection in Information Processing Systems*, IFIP Advances in Information and Communication Technology, Springer Berlin Heidelberg, Berlin, Vol. 405, pp. 257-271.

Srite, M. and Karahanna, E. (2006), "The role of espoused national cultural values in technology acceptance", *MIS Quarterly, Society for Information Management and The Management Information Systems Research Center*, Vol. 30 No. 3, pp. 679-704.

Straub, D., Boudreau, M.-C. and Gefen, D. (2004), "Validation guidelines for is positivist research", *Communications of the Association for Information Systems*, Vol. 13 No. 1, pp. 380-427.

Urbach, N. and Ahlemann, F. (2010), "Structural equation modeling in information systems research using partial least squares", *Journal of Information Technology Theory and Application (JITTA)*, Vol. 11 No. 2.

Workman, M. (2007), "Gaining access with social engineering: an empirical study of the threat", *Information Systems Security*, Vol. 16 No. 6, pp. 315-331.

Workman, M. (2008), "Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security", *Journal of the American Society for Information Science and Technology*, Vol. 59 No. 4, pp. 662-674.

Appendix 1. Items for study construct

Intention

I will not install software if I suspect that the request originates from a non-legitimate sender.

I intend to prevent anyone who I suspect of being non-legitimate from installing malicious software on my computer by means of a security attack.

I will not disclose my computer password to anyone who I suspect is not a legitimate party or authorized to receive such information.

I intend not to disclose my computer password to anyone who I suspect is not a legitimate party or authorized to receive such information.

I will prevent anyone who I suspect of being unauthorized or non-legitimate from gaining access to my work computer by means of a security attack.

Self-efficacy

I am confident about my ability to prevent unauthorized individuals from accessing confidential information, such as my work computer password.

I am confident about my ability to prevent individuals from installing malicious software on my work computer.

I am confident about my ability to identify unauthorized, unexpected or suspicious requests in e-mails.

I am confident about my ability to identify unauthorized, unexpected or suspicious requests to do with my work computer password.

Information security policy awareness

I am aware of how acceptable use of IT products and services (e.g. computers, the Internet, e-mail, etc.) is described in our policy.

I am aware of how acceptable installation of software is described in our policy.

I know how our policy governs management of sensitive and confidential information.

I am aware of my obligations under our policy regarding the use and management of passwords for my work computer.

General information security awareness

I am aware of the potential threats and negative consequences that inadequate information security in my work can cause.

I understand the risks posed by inadequate information security in general.

Formal IS training

Have you had any formal IT training and/or IT security training?

Appendix 2. Outline of phishing e-mail

<from> support@knylo.com</from>

<subject> Knylo PDF Reader Update </subject>

<content>

Dear Knylo Acrobat Reader Customer,

A new version of Knylo Reader (version 11.xx) was recently released.

This update includes new enhanced features for viewing, creating, editing, printing and sharing of PDF documents.

It also includes several important security improvements.

The update is available for download on the following location: www.knldownloads.com/?reader=11xx

Regards,

Knylo support

</content>

About the authors

Waldo Rocha Flores is a PhD student at the Department of Industrial Information and Control Systems at the Royal Institute of Technology (KTH) in Stockholm, Sweden. He received his MSc in Electrical Engineering at the Royal Institute of Technology (KTH) in 2008, and his MSc in Business Administration and Economics at Stockholm university school of business in 2013. He does research in the field of information security governance, and socio-organizational aspects of information security. Waldo Rocha Flores is the corresponding author and can be contacted at: waldorf@kth.se

Hannes Holm is a Researcher at the Swedish Defense Research Agency (FOI) in Linköping, Sweden, where he conducts research within IT security. Hannes holds a PhD from the Department of Industrial Information and Control Systems at the Royal Institute of Technology (KTH) in Stockholm, Sweden. He received his MSc in management engineering at Luleå University of Technology.

Marcus Nohlberg is an Assistant Professor at the School of Informatics at the University of Skövde, Sweden. He received his BSc in systems development in 2000, his MBA in Electronic Commerce in 2004 and his PhD from Stockholm University in 2009. He does research in the field of information security, focusing on social engineering, phishing and frauds.

Mathias Ekstedt is an Associate Professor at the Royal Institute of Technology (KTH) in Stockholm, Sweden. His research interests include systems and enterprise architecture modeling and analyses with respect to information and cyber security, in particular for the domain of electric power systems.

This article has been cited by:

1. M. Junger, L. Montoya, F.-J. Overink. 2017. Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior* **66**, 75-87. [CrossRef]
2. W.D. Kearney, H.A. Kruger. 2016. Can perceptual differences account for enigmatic information security behaviour in an organisation?. *Computers & Security* **61**, 46-58. [CrossRef]
3. Waldo Rocha Flores, Mathias Ekstedt. 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security* **59**, 26-44. [CrossRef]