Spear Phishing in Organisations Explained

Bullee, Jan Willem; Montoya, Lorena; Junger, Marianne; Hartel, Pieter

DOI
10.1108/ICS-03-2017-0009

Publication date
2017

Document Version
Final published version

Published in
Information and Computer Security

Spear phishing in organisations explained

Jan-Willem Bullee and Lorena Montoya
Faculteit Elektrotechniek Wiskunde en Informatica, Universiteit Twente, Enschede, The Netherlands

Marianne Junger
Faculteit Gedrags- Management- en Maatschappijwetenschappen, Universiteit Twente, Enschede, The Netherlands, and

Pieter Hartel
Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, The Netherlands

Received 1 March 2017
Accepted 1 July 2017

Abstract

Purpose – The purpose of this study is to explore how the opening phrase of a phishing email influences the action taken by the recipient.

Design/methodology/approach – Two types of phishing emails were sent to 593 employees, who were asked to provide personally identifiable information (PII). A personalised spear phishing email opening was randomly used in half of the emails.

Findings – Nineteen per cent of the employees provided their PII in a general phishing email, compared to 29 per cent in the spear phishing condition. Employees having a high power distance cultural background were more likely to provide their PII, compared to those with a low one. There was no effect of age on providing the PII requested when the recipient's years of service within the organisation is taken into account.

Practical implications – This research shows that success is higher when the opening sentence of a phishing email is personalised. The resulting model explains victimisation by phishing emails well, and it would allow practitioners to focus awareness campaigns to maximise their effect.

Originality/value – The innovative aspect relates to explaining spear phishing using four socio-demographic variables.

Keywords Gender, Culture, Age, Spear phishing, Years of service

Paper type Research paper

1. Introduction

Cyber security has for a long time primarily been treated as a technical problem (Rhee *et al.*, 2009; Waldrop, 2016). However, cyber security incidents are often caused by human failure (Chan *et al.*, 2005) rather than by technical failure (Schneier, 2000). Developing stronger

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TREsPASS).

This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.

Furthermore, the authors would like to thank Wouter Bakker, Berber Bokkes, Shannon Cleijne, Wouter Horlings and Koen Zandberg for their efforts in the data collection. In addition, a special thank goes to Human Resource Manager Cathelijne de Carpentier Wolf - de Vin for providing relevant data.

Information & Computer Security
Vol. 25 No. 5, 2017
pp. 593-613

2056-4961
DOI 10.1108/ICS-03-2017-0009

digital security alone will not result in a viable long-term solution against cyber security. Instead, the solution should involve solving human errors (Waldrop, 2016). As people do not have sufficient cognitive capacity to process all sensory input, their decision-making involves using rules of thumb (i.e. heuristics; Cialdini, 2009). Heuristics work well in most circumstances, until a heuristic fails and a cognitive bias occurs (Gigerenzer, 1991; Tversky and Kahneman, 1974). Offenders are well aware of the flaws in human logic and nudge the heuristics of their targets into systematic errors (i.e. cognitive biases) to make them comply (Bosworth *et al.*, 2014; Dang, 2008; Kennedy, 2011; Luo *et al.*, 2011; Twitchell, 2009). This kind of trickery is referred to as social engineering. This paper focusses on social engineering via email, also known as phishing. In particular, it aims to establish whether victimisation differs for general and spear phishing (i.e. targeted or personalised) emails in the context of an organisation. Second, it aims to establish whether socio-demographic characteristics of targets influence victimisation. The reason behind this is 3-fold:

(1) It finds out who is most vulnerable and could benefit most from training.

(2) It reduces cost and time for those who give and receive training.

(3) It prevents training fatigue and adverse training effects.

It is argued that the possibility of adverse effects emphasises the need to study the effectiveness of interventions before their launch (Junger *et al.*, 2017).

Some have argued that most forms of cyber crime are not unique to the online world because they have long-established terrestrial counterparts (Grabosky, 2001; McCusker, 2006; Neve and Hulst, 2008) which pre-date the internet but have found new forms of life online. For example, hacking activities could be seen as computer-aided versions of trespassing as the attacker is entering another person's property without authorisation. In addition, when a hacker purposely changes a website or destroys data, the action is comparable to vandalism. Similarly, phishing emails are comparable to the classical confidence tricks (e.g. scams or fraud), leading to theft (Montoya *et al.*, 2013). The *modus operandi* includes both building a trust relation with the target and then using psychological tricks (e.g. abuse the credulity of the target) to defraud it.

Data collection for both traditional and digital past crime experiences often involves finding case studies and filling in surveys (e.g. Lee and Soberon-Ferrer, 1997; Titus *et al.*, 1995). Although these are useful methods for data collection, the following three issues can be identified:

(1) the representativeness of the sample;

(2) controlling for opportunity; and

(3) unawareness of victimisation.

For example, as there are case studies stating that older adults were victimised; therefore, it is assumed that the elderly are more vulnerable. However, these individual case studies do not constitute a representative sample of victims (Ross *et al.*, 2014). Carrying out a survey on people can be used to overcome this. However, simply asking people for their experience regarding fraud will bias the outcome. In many cases, there is no control for an opportunity (i.e. whether one receives an attempt) in the survey (Ross *et al.*, 2014). Not being exposed to a fraudulent request will never make one become victimised. Only a few studies take this into account, e.g. Titus *et al.* (1995). Another drawback of surveying fraud is that some respondents were unaware of being defrauded, forgot the episode, misremembered or felt too ashamed to admit (Ross *et al.*, 2014).

It is argued that it is best to do experiments and observe behaviour rather than to either ask subjects how they think they would behave in a given scenario or to recall a reaction (Petrova *et al.*, 2007). When experimenting in an organisational context, Pfeffer (1985) argues that inclusion of socio-demographic variables helps better understand the organisation. Employees are not a homogeneous group of entities and are hence diverse regarding, e.g. age and years of service (YoS). The increase of women and different ethnic groups in the workforce has been further increased diversity (Shenhav and Haberfeld, 1992). It must be noted that conducting experiments regarding fraud and cyber crime requires careful planning and consideration. As this typically involves conducting experiments on humans (e.g. employees), ethical considerations must be taken into account (Belmont Report, 1979). Particular challenging is the use of deception because it conflicts with ethical principles (Code of Federal Regulations, 2005). Furthermore, people who are aware of being in an experimental setting would be suspicious and hence biased. It is unlikely that they would have similar levels of suspicion outside of the experiment (Parsons *et al.*, 2013; Furnell, 2007; Anandpara *et al.*, 2007).

1.1 Phishing

"Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target" (Lastdrager, 2014). The definition contains two parts:

(1) Scalability relates to how easy it is for the offender to approach the targets. Therefore, all non-mass-media (i.e. face-to-face interaction or telephone calls) do not constitute phishing.

(2) Deception by impersonation to obtain information is, for example, claiming to be from someone's bank to obtain information.

When the offender does not use impersonation, it is a non-fraudulent request for information, and therefore, it cannot be classified as phishing.

1.1.1 Spear phishing. Spear phishing is a particular type of phishing, in which the target and context are investigated so that the email is tailored to receiver. If the process of personalisation is scalable, spear phishing falls in the consensus definition of phishing (Lastdrager, 2014). The rationale behind putting additional effort in personalising the emails relates to the "higher return on investment". It is believed that spear phishing emails are successful because personalisation creates trust (Sparshott, 2014).

The rational choice theory (Cornish and Clarke, 1987) provides underpinning for our study. Actions in this theory are based on a conscious evaluation of the utility of acting in a certain way (i.e. cost vs benefit). In the field of crime and security, this translates into the weighing of the value to be gained by committing the act versus the negative consequences (Cornish and Clarke, 1987). Hong states that offenders are changing their focus from a wide to narrow range of targets (Hong, 2012). Offenders used to send out mass emails, hoping to trick anyone; now they are more selective and use relevant context information in emails to trick specific targets (Hong, 2012). Based on this theory, we hypothesised that spear phishing is more attractive for two reasons:

(1) It involves targeting fewer people than in general phishing, the likelihood of a negative consequence is lower because the number of attempts the offender has to make is lower.

(2) As the emails are personalised, the target is more likely to assume that the email is legitimate, translating into a higher compliance rate.

There is limited empirical work on the effectiveness of spear phishing. The Scopus query "TITLE-ABS-KEY (spear phishing)" returned 66 articles; the majority of the studies discuss computer algorithms that aim to detect spear phishing emails, whereas there are three studies about sending (spear) phishing emails to human subjects. However, none of them investigated the success of spear phishing for different types of people. Nevertheless, studies that did investigate socio-demographic variables and "general" phishing are discussed next.

In a field study, the effect of spear phishing was tested on 581 college students (age 18-24 years). Those in the control group ($N = 94$) received a phishing email from a fictitious person requesting to enter their login credentials on an untrusted website, whereas those in the experimental group ($N = 487$) received the same email supposedly from one of their friends. The subjects who received the email from a "friend" entered their credentials 4.5 times more often than those who received the email from a stranger (16 per cent vs 72 per cent) (Jagatic *et al.*, 2007).

In another field study, 158 employees distributed over five organisations in Sweden were approached under two conditions (Holm *et al.*, 2014). All employees first received the general email (written in English) with the request to download software from an untrusted website. Later, all employees received another email (written in Swedish), using the name of the employee, the name of the organisation and the name of an executive to persuade them to download an add-on to the virus scanner. Those who received a spear phishing email were 5.3 times more likely to click the link in the email (27.2 per cent vs 5.1 per cent) and 2.8 times more likely to execute a binary (8.9 per cent vs 3.2 per cent) than those who received a general phishing email (Holm *et al.*, 2014).

The following four sections discuss the influence of gender, age, YoS and culture on the compliance to phishing.

1.1.2 Age. A survey of a national representative sample including 957 adults in the USA found a negative significant effect of age on victimisation, meaning that older persons are less likely to be victims of fraud (Lee and Soberon-Ferrer, 1997). It was not mentioned whether the survey asked if the subject had been exposed to attempted fraud; hence, there was no control for opportunity. A national telephone survey, representing a relative probability sample of 1,246 respondents also found a negative age victimisation relation (Titus *et al.*, 1995). Titus *et al.* argued that older people are more experienced regarding fraud and, therefore, less vulnerable (Titus *et al.*, 1995). In a 400-respondent telephone survey, comparable to that of Titus *et al.*, no age effect was found (Van Wyk and Benson, 1997). The latter two surveys did control for opportunity.

For phishing emails, Sheng *et al.* (2010) collected data regarding phishing experience and victimisation in an online survey among 1,001 respondents (containing a mix of US and non-US citizens, students and non-students) using Amazon.com's Mechanical Turk. Of their subjects, 52 per cent indicated that they would click on links in the phishing emails. Furthermore, they found a negative relation between age and falling for phishing. People in the age group 18-25 were more likely to fall for phishing than people in other age groups (Sheng *et al.*, 2010). The authors speculate that this effect is due to this age group having the following:

- a lower level of education;
- fewer years on the internet;
- less exposure to training materials; and
- less of an aversion to risks.

Research results for traditional and digital crime show either a negative or no effect of age. Therefore, there is not enough evidence to suggest that age should be discarded as a predictor of phishing. For a summary of the studies, refer to Table I.

Table I.
Summary table of presented literature on phishing studies and socio-demographic predictors

						Most at risk					
N	Type	Population[a]	Opportunity	Data collection[b]	Type[c]	Gender	Age	YoS[d]	Culture	Success[e]	Reference
957	Classical	Mix	Uncontrolled	Telephone Survey	–	No effect	Younger	–	–		Lee and Soberon-Ferrer (1997)
1246	Classical	Mix	Controlled	Telephone Survey	–	No effect	Younger	–	–		Titus *et al.* (1995)
400	Classical	Mix	Controlled	Telephone Survey	–	No effect	No effect	–	–		Van Wyk and Benson (1997)
158	Digital	Staff	Controlled	Single exp. email	Spear	–	–	–	–	5.1	Holm *et al.* (2014)
581	Digital	Students	Controlled	Single exp. email	Spear	Female	–	–	–	16	Jagatic *et al.* (2007)
1001	Digital	Mix	Uncontrolled	Role-play task	–	Female	Younger	–	–	52	Sheng *et al.* (2010)
2624	Digital	Student	Controlled	Single exp. email	–	Female	–	–	–	2.4	Wright *et al.* (2014)
53	Digital	Students	Controlled	Multi exp. emails	–	Female	–	–	–	92.5[f]	Hong *et al.* (2013)
111	Digital	Mix	Controlled	Single exp. email	–	–	Younger	–	High PDI	23.4	Tembe *et al.* (2013)
490	Digital	Staff	Controlled	Single exp. email	–	–	–	Less	–	63.7	Kearney and Kruger (2014)

Notes: [a]Mix refers to a mix of students, and non students; [b]"single email" = the subject received 1 phishing email; "multi emails" = the subject received multiple (non)-phishing emails; [c]Type of phishing email; general phishing or spear phishing; [d]YoS refers to Years of Service at the organisation; [e]Success shows the success of the phishing mail in the control group; [f]Classified at least 1 phishing mail as legitimate

1.1.3 Gender. In traditional fraud, there is generally no gender effect (Lee and Soberon-Ferrer, 1997; Titus *et al.*, 1995; Van Wyk and Benson, 1997). However, a gender effect was found for specific types of fraud. Females were more frequently victims of lottery fraud and males of investment fraud (Deevy *et al.*, 2012).

The 1,001 respondents in the online survey conducted by Sheng *et al.* (2010) found that females fell more for phishing emails than males. The subjects in their sample had an average age of 30 and 48.25 per cent (N = 483) were males (Sheng *et al.*, 2010). After a training session, females and males performed equally (Sheng *et al.*, 2010).

In two studies, university students received a phishing email in their mailbox (Jagatic *et al.*, 2007; Wright *et al.*, 2014). In the control condition, 16 and 2.4 per cent of the participants complied with the phishing mail, respectively. Furthermore, the outcome was that females were more likely to respond than males. Finally, there was one study in which the subjects received a variety of both legitimate and phishing emails (Hong *et al.*, 2013). This latter design allows testing whether the participants in a phishing study become paranoid and classify all emails as phishing. The finding of Hong *et al.* (2013), based on seven phishing and seven non-phishing emails, was that 92.5 per cent of their participants classified at least one phishing email as legitimate. The performance of females was worse than that of males at identifying phishing emails (Hong *et al.*, 2013). These results suggest that females are overall more vulnerable than males to phishing emails (Hong *et al.*, 2013; Jagatic *et al.*, 2007; Sheng *et al.*, 2010; Wright *et al.*, 2014). For a summary of the studies, refer to Table I.

1.1.4 Years of service. In organisational research, the variable tenure or seniority is often included in the analysis and commonly operationalised as YoS at an employer. YoS correlates with job satisfaction in, e.g., academic personnel (Oshagbemi, 2000) hospital employees (Mobley *et al.*, 1978) and insurance company clerks (Waters *et al.*, 1976). An explanation is that employees who are less satisfied will resign, while those who are more satisfied will remain in a job. YoS is also positively correlated with occupational commitments in, e.g., nurses (Jafari Kelarijani *et al.*, 2014) and hotel employees (Sarker *et al.*, 2003). Furthermore, there is also a relation with age, as the YoS cannot exceed the age of a person minus the years of education.

The relation between YoS and victimisation by phishing emails was investigated in (to the best of our knowledge) only one field study (Kearney and Kruger, 2014). The 213 employees involved were persuaded to validate their password on an untrusted website, 63.7 per cent of the recipients responded to the email. A negative YoS age relation was found, meaning that employees who were hired more recently were more often victimised compared to those who were hired less recently (Kearney and Kruger, 2014). Despite the limited empirical evidence, this relation could be important in organisational research on phishing.

1.1.5 Cultural dimensions. Hofstede *et al.* (2010) identified six cultural dimensions and made a comparison across 60 countries. The six dimensions are as follows:

(1) power distance (PDI);
(2) individualism versus collectivism;
(3) uncertainty avoidance;
(4) masculinity versus femininity;
(5) long-term versus short-term orientation; and
(6) indulgence versus restraint (Hofstede *et al.*, 2010).

The cultural dimension PDI is one that could explain the different success rates of phishing emails between citizens of countries. PDI is defined as "the extent to which the less powerful

members of organisations and institutions accept and expect that power is distributed unequally" (Hofstede *et al.*, 2010). A higher PDI score suggests that there is a strongly enforced hierarchy. A lower score suggests that people question authority and strive to decentralise and distribute power more equally. Two aspects indicate obedience to the use of authority in phishing emails:

(1) "Hierarchy in organisations reflects the existential inequality between higher-ups and lower-downs".

(2) "Subordinates expect to be told what to do" (Hofstede *et al.*, 2010).

In the context of information security behaviour, limited research has been conducted on cultural influences. The majority of studies have been conducted in Western countries, occasionally in Asia, whereas the rest of the world has been overlooked. Cross-cultural research is important because culture is likely to have a direct influence (Crossler *et al.*, 2013).

In a survey, 50 US and 61 Indian participants were asked about phishing. Almost everyone in the sample had experienced a phishing attempt. In total, 14 per cent of the US and 31 per cent of the Indian participants reported being victimised (Tembe *et al.*, 2013). The results suggest that Indians are more susceptible to phishing emails. India has a higher PDI (i.e. 77) compared to the USA (i.e. 40); this could explain the difference between the two countries. It must also be noted that the subjects from India were significantly younger than those in from the US sample; therefore, an age effect is not excluded either (Tembe *et al.*, 2013).

1.2 Research question

The contribution of our work is two-fold. First, we provide an experimental design for measuring the effectiveness of two types of phishing emails, which provides real-life empirical data (as oppose to laboratory data or measuring intention). Second, our study gives an insight into how the socio-demographic characteristics of victims predict compliance.

This research aims to answer the following question:

RQ1. "To what extent are people susceptible to phishing emails?"

Five hypotheses were formulated:

H1. Previous research showed that combining the name of the recipient, the name of the organisation, the name of a company executive and a translation to the native language was successful. However, no individual effect was investigated. We, therefore, hypothesise that the opening sentence of a phishing email influences its success.

H2. Previous research showed that females were more vulnerable to phishing emails than males. We, therefore, hypothesise that the success of a phishing email is influenced by the gender of the recipient and that females are more vulnerable.

H3. Previous research regarding phishing emails was inconclusive regarding the effect of age on compliance. We, therefore, hypothesise that the success of a phishing email is influenced by the age of the recipient and that older people are more vulnerable.

H4. As there is limited research regarding the length of employment in the organisation in relation to phishing which involves the organisation, this variable is included in the analysis. We, therefore, hypothesise that the success of a phishing email is influenced by the YoS of the recipient.

H5. As there is limited research regarding the cross-cultural influences in security research, this variable is included in the analysis. We, therefore, hypothesise that the success of a phishing email is influenced by the cultural background of the recipient.

2. Methods

The sample consisted of 593 subjects of both genders who worked in The Netherlands. All employees from one faculty were approached. The materials in this section are based on Bakker *et al.* (2015) and extended where necessary.

2.1 Subject selection

The pool of subjects consists of Professors (Full, Associate and Assistant), Post-Doctoral researchers, PhD candidates and support personnel. The sample consisted of 24.5 per cent females and 75.5 per cent males. The average age of the employees is 39.46 (SD = 12.20) years, ranging between 22 and 76, whereas females were younger (38.08 vs 39.92 years). Regarding YoS, the average is 5.72 (SD = 7.82) years, ranging between 0 and 42. Females had slightly more YoS compared to males (6.23 vs 5.80). Two-thirds of the employees were Dutch ($N = 380$), whereas 196 (34.03 per cent) originated from elsewhere. In this latter group, 77 employees were from Europe, 90 from Asia, 8 from Africa, 2 from North America, 16 from South America and 1 from Oceania. More details can be found in Table II.

2.2 Procedure

Before data collection, our research was approved by the Institutional Review Board of the University. All employees were approached by email on a Monday evening in a regular term week. The subjects had until Thursday evening to respond to the email; the data collection stopped thereafter.

Two types of email were randomly assigned to the subjects. Those in the control group received an email with the opening "Dear employee", whereas those in the experimental group received an email with the opening "Dear [name]". Each employee received the following email:

> Dear employee,
>
> Due to recent changes to the UT computer system, some complications emerged between our database servers. This system, which contains your username and password, is not correctly synchronised.
>
> Your data were not compromised, and the problems are already fixed. To avoid complications in the near future a complete synchronisation between the servers is scheduled. If your account is not correctly synchronised, you cannot login anymore.

Table II.
Origin of subjects (380 Dutch subjects, PDI = 38, are excluded from this overview)

Continent	Countries	N	PDI range	AVG[a]
Africa	5	8	[49, 80]	67.88
Asia	12	90	[54, 104]	71.57
Europe	12	77	[35, 93]	48.23
North America	2	5	[39, 40]	39.75
Oceania	1	1	[36]	36.00
South America	7	16	[63, 85]	71.88
Total	39	196	[35, 104]	61.44

Note: [a] = Weighed average PDI

> This can only be done via login.utwente.nl.
>
> Click on 'Sync password', and your password will be synchronised automatically. Can't find 'Sync password'? This means your password has already been synchronised. If you do not resynchronize your password with this link, you will no longer be able to use the central IT facilities.
>
> The IT-account is used for computer login, email, WiFi, VPN connection and also logging on to various UT web applications.
>
> Synchronise your password within a period of 3 days.
>
> To synchronise your password, click here.
>
> Kind regards,
>
> Jort Welp
>
> Security Manager IT-Helpdesk.

Each employee was subjected to the same request. Following the data collection, employees received a debriefing statement explaining that the phishing email was part of awareness training.

2.2.1 Legitimate versus illegitimate email. The differences between the legitimate and the experimental email and website are discussed. A legitimate email from the ICT Services (ICTS) department has the following characteristics:

- As there are 34 per cent foreign employees in the organisation, important communication from the organisation is sent in two languages (i.e. Dutch and English).
- The sender of the email is always either the ICTS or Facility Management department. In case the ICTS department is the sender, the logos of both the university and the department are used.
- The signatory of the email is never a person, but instead, the contact details of the ICTS department are provided, even if it was sent by the Facility Management staff.

The illegitimate email had three characteristics:

(1) Both the URLs in the email redirected to http://login.utvvente.nl rather than to http://login.utwente.nl (note the difference between in utVVente vs utWente). The website was hosted by a third party which did not relate to the organisation. For a photo of the website used in the experiment and its legitimate equivalent used in the organisation, refer to Figures 1 and 2, respectively.

(2) The signatory was a fictitious person, hence, not a university employee.

(3) IT-Helpdesk was mentioned as the organisational unit in charge of IT rather than ICTS.

2.3 Variables

The variables used in the analysis were as follows: *compliance*, *spear*, *gender*, *age*, *YoS*, *nationality* and *PDI*. The dependent variable *compliance* measured whether the subject complied with providing the requested personally identifiable information (PII) in a web form. The dichotomous variable was dummy coded as 0 = did not comply, 1 = did comply. The independent dichotomous variable *spear* measured the opening the phishing email used

(0 = general, 1 = personalised). The independent dichotomous variable *gender* measured whether the subject was a female or a male and was dummy coded (0 = female, 1 = male). The independent continuous variable *age* measured the age of the subject (25 = 25 years old). The independent continuous variable *YoS* measured the seniority of an employee, operationalised as YoS (5 = 5 YoS). The independent categorical variable *nationality* measured the subject's country of origin. The independent continuous variable *PDI* measured the extent to which a society accepts that power is unequally distributed (low score indicates the tendency to distribute power equally, whereas high scores indicate a confirmation of the hierarchy) (Hofstede *et al.*, 2010). The *PDI* score is based on the variable nationality; for each nationality, the *PDI* values were retrieved from Hofstede *et al.* (2010), the scores range between 11 and 104 (38 = The Netherlands). The cultural scales are validated and correlate with the dimensions from the World Values Survey (Smith and Schwartz, 1997; Hofstede, 2001). Finally, it was tested whether the different type of phishing emails were randomly distributed among the four independent variables (i.e. gender, age, YoS and PDI), no statistical significant differences were found.

Figure 1.
The fake website that was used in the experiment

Figure 2.
The legitimate website of the organisation

2.4 Analysis

The first hypothesis was tested using cross-tabulation and chi-square. The remaining hypotheses were tested using logistic regression. The following two data assumptions must be met for chi-square analysis: independence and minimum frequency of five observations per cell in the cross-tabulation (Field *et al.*, 2012). Independence relates to putting a single observation in only one cell. In case, one assumption is not met, the Fisher's exact test should be used instead. Both assumptions were met, as *i* there were categorical data used in the analysis and the number of observations exceeded the required minimum.

The following three assumptions must be met for logistic regression analysis: sufficient sample size, no outliers and no multicollinearity (Pallant, 2010). First, the dataset should contain at least ten events per variable, which is considered as a minimum required for running a logistic regression (Peduzzi *et al.*, 1996). The dataset contained 593 observations and was, therefore, considered sufficient. Second, for dichotomous variables, one value was placed in exactly one category. Third, the variance inflation factor (VIF) is 1.25, which is below the cut-off value of 10, indicating that there was no evidence of multi-collinearity (Pallant, 2010). For an overview of the VIF statistics, refer to Table III.

One characteristic of age is that it is often non-linearly correlated with other variables. In this study, a u-shaped relation was found with compliance, suggesting a non-linear relation (refer to Figure 3). To overcome this, a straight line needed to be transformed into a curved line (i.e. adding a quadratic coefficient). Carrying out a non-linear regression is as simple as transforming the independent variable and adding it (i.e. age^2) to the equation (Miles and Shevlin, 2001, p. 138). Note that *age* and age^2 are not functionally independent, but linearly independent (Greene, 2011). Addition of the

Variable	VIF	Tolerance	R^2
Spear	1.00	0.997	0.003
Gender	1.02	0.984	0.016
Age	1.58	0.632	0.368
Yos	1.52	0.657	0.344
Pdi	1.10	0.906	0.094
MEAN	1.25		

Table III.
Summary of VIF statistics

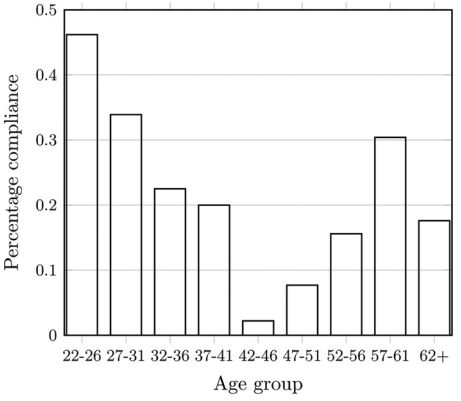

Figure 3.
Percentage compliance per age group

squared term means that the two *age* coefficients cannot be interpreted separately (European Social Survey Education Netu, 2013). Furthermore, we tested whether the simultaneous influence of two variables on a third was non-additive. The relevance is that if two variables interact, the relationship between each of the interacting variables and compliance depends on the value of the other interacting variable. The YoS of an employee is restricted by their age; hence, their correlation (r = 0.587, p = 0.000); therefore, their interaction was tested. Other interactions involve the type of email and socio-demographic variables, where different groups of employees have different responses to the different types of email.

3. Results

3.1 H1 "the opening sentence of a phishing email influences its success"

Compliance of those who received a general phishing email was 19.3 per cent, compared to 28.9 per cent for those who received a spear phishing email (χ^2 = 7.368, df = 1, p = 0.007). *H1* is, therefore, accepted. Those in the spear phishing group had 1.693 times higher odds of compliance (i.e. providing their PII) than those exposed to a general phishing email (odds ratio [*OR*] = 1.693, confidence interval [*CI*] [1.16, 2.48]). Refer to Table IV for descriptive statistics. After controlling for socio-demographic variables, those who received a spear phishing email still had higher odds of compliance (*OR* = 2.418, *CI* [1.22, 4.79]), refer to Table V.

Table IV. Number of observations and percentages per phishing condition

		Spear phishing		
		No	Yes	Total
Complied	No	238 (80.7%)	212 (71.1%)	450 (75.9%)
	Yes	57 (19.3%)	86 (28.9%)	143 (24.1%)
Total		295 (100%)	298 (100%)	593 (100%)

Note: Group general = spear (χ^2 = 7.368, df = 1, p = 0.007)

Table V. Model comparison

Variable	Model 1: spear	Model 2: full
Spear	1.693 (*0.331*) [1.16, 2.48]**	2.418 (*0.843*) [1.22, 4.79]*
Gender		0.825 (*0.230*) [0.48, 1.43]
Age		0.865 (*0.082*) [0.72, 1.04]
Age^2		1.002 (*0.001*) [1.00, 1.00]
YoS		0.855 (*0.043*) [0.77, 0.94]**
ageXyos		1.005 (*0.002*) [1.00, 1.01]*
PDI		1.025 (*0.007*) [1.01, 1.04]***
spearXgender		0.806 (*0.452*) [0.27, 2.42]
spearXage		0.925 (*0.024*) [0.88, 0.97]**
spearXyos		1.259 (*0.093*) [1.09, 1.46]**
spearXpdi		1.014 (*0.014*) [0.99, 1.04]
Consstant	0.239 (*0.035*) [0.18, 0.32]***	1.879 (*3.775*) [0.04, 96.4]

Notes: The columns depict for each variable: the odds ratio (OR), its standard error (between parentheses), its lower and upper 95% CIs [in brackets] and its significance level; *p < 0.05, **p < 0.01, ***p < 0.001; ageXyos = interaction of Age and service; Model 1 (χ^2(1) = 7.41, p = 0.007), N = 593, pseudo R^2 = 0.011; Model 2 (χ^2(11) = 87.16, p = 0.000), N = 462, pseudo R^2 = 0.167; Model 1 = 2 (p = 0.000)

Compliance rates in previous research for general phishing emails ranged between 2.4 per cent (Wright *et al.*, 2014) and 92.5 per cent (Hong *et al.*, 2013), with a weighted average of 21.4 per cent, refer to Table I. In this study, the compliance rate for general phishing was 19.3 per cent and, compared to previous studies, was considered as average.

As those who received a spear phishing email have higher odds of compliance, we tested whether the odds of compliance differed among people with different characteristics. In particular, we tested whether the relation between socio-demographic variables and compliance was influenced by the type of phishing email (i.e. *spear*). The relevance is that if the type of email and the socio-demographic variables interact, the relationship between each of the interacting variables and compliance depends on the value of the other interacting variable. Therefore, for each hypothesis, we also tested whether *spear* moderates that variable.

3.2 H2 "the success of a phishing email is influenced by the gender of the recipient"

No main effect of gender on compliance was found while controlling for socio-demographic variables (*OR* = 0.825, *CI* [0.48, 1.43], $p = 0.492$). Refer to Table V for the full regression model. *H2* is therefore rejected in favour of the alternative *H2a*: "The success of a phishing email is not influenced by the gender of the recipient." The interaction effect between *spear* and *gender* was not statistically significant (*spearXgender*: *OR* = 0.806, *CI* = [0.27, 2.42], $p = 0.700$).

3.3 H3 "the success of a phishing email is influenced by the age of the recipient"

No main effect of age on compliance was found while controlling for socio-demographic variables (*age*: *OR* = 0.865, *CI* = [0.72, 1.04], $p = 0.126$ and age^2: *OR* = 1.002, *CI* = [1.00, 1.00], $p = 0.117$). *H3* is, therefore, rejected in favour of the alternative *H3a*: "The success of a phishing email is not influenced by the age of the recipient.".

A significant interaction effect was found between *spear* and *age* (interaction term *spearXage*: *OR* = 0.925, *CI* = [0.88, 0.97], $p = 0.003$). These results suggest that younger and older employees react differently to the two types of email, whereas the variable *spearXage* indicates how different this is, refer to Figure 4. Compliance to spear phishing emails is higher compared to general phishing emails for younger employees. This difference decreases with age, approaches zero, and the age group of 61+ employees is the most vulnerable to general phishing emails. The OR tells us that as age increases by 1 year, in combination with a general email becoming a spear phishing email, the change in odds of providing PII is 0.925. In particular, *spearXage* is the difference in OR corresponding the change in type of phishing email (from general to spear) in two age homogeneous groups which differ by 1 year.

3.4 H4 "the success of a phishing email is influenced by the years of service of the recipient"

The employees who worked longer for the organisation were less vulnerable to phishing emails (*OR* = 0.855, *CI* = [0.77, 0.94], $p = 0.002$). *H4* is, therefore, accepted.

A significant interaction effect was found between *age* and *YoS* (*ageXyos*: *OR* = 1.005, *CI* = [1.00, 1.01], $p = 0.041$). These results suggest that new employees and those with more YoS react differently to phishing emails for different ages. The OR tells us that as the age of an employee increases by 1 and the YoS increases, the change in OR for complying compared to not complying is 1.005.

Furthermore, a significant interaction effect was found between *spear* and *YoS* (*spearXyos*: *OR* = 1.259, *CI* = [1.09, 1.46], $p = 0.002$). These results suggest that new employees and those with more YoS respond differently to the two types of phishing emails, refer to Figure 5. The OR tells us that as the type of email changes from a general to a spear

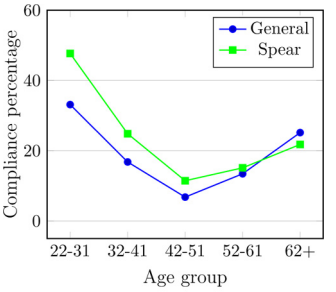

Figure 4.
Compliance percentage for five age groups, for two types of phishing emails

Notes: The sample size for the age groups that received a general phishing email is 89, 52, 47, 37 and 11. The sample size for the age groups that received a spear phishing email is 97, 59, 51, 25 and 16

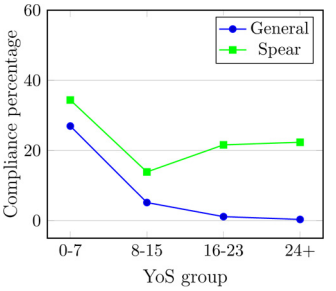

Figure 5.
Compliance percentage for four YoS groups, by two types of phishing emails

Notes: The sample size for the age groups that received a general phishing email is 171, 29, 20 and 11. The sample size for the age groups that received a spear phishing email is 178, 42, 14 and 12

email, in combination with an increase in YoS, the change in OR of compliance compared to non-compliance is 1.259.

The effect of having more YoS is different depending on the age and whether the employee received a general or a spear phishing email. For instance, for the youngest age group (age 22-31), in both the general and spear condition, compliance decreases when YoS increases. For those who received a general phishing email, compliance was 38.5 per cent for those with less that 1 YoS compared to 1.18 per cent for those with 8 YoS, whereas for those who received a spear phishing email, compliance was 52.07 per cent for those with less that 1 YoS and 23.19 per cent for those with 8 YoS. This trend is comparable for the age group

32-41. For employees in the age group 42-51 who received a general phishing email, compliance decreases when the YoS increases, while the compliance does not change for those who received a spear phishing email. For those in the age groups 52-61 and 61+ who received a general phishing email, compliance decreases when the YoS increases, whereas the compliance increases for those who received a spear phishing email. For an overview of the predicted compliance rates for *age* and *YoS* per type of phishing email, refer to Figure 6(a) for general phishing emails and 6(b) for spear phishing emails.

3.5 H5 "the success of a phishing email is influenced by the cultural background of the recipient"

Those with a higher PDI have a higher probability of filling out PII in a phishing email (OR = 1.025, CI = [1.01, 1.04], p = 0.000). *H5* is, therefore, accepted. Furthermore, no interaction effect between *spear* and *PDI* was found (*spearXpdi*: OR = 1.014, CI = [0.99, 1.04], p = 0.326).

4. Discussion

This study investigated the susceptibility to two types of phishing emails and the personal characteristics that influence the probability of compliance.

Personalised phishing emails proved to be more successful than general phishing emails. Those who receive a spear phishing email have 1.7 times higher odds of compliance than those who receive a general phishing mail. These results are in line with Sparshott (2014).

Previous research operationalised spear phishing by supposedly using a friend of the receiver as the sender (Jagatic *et al.*, 2007) or a combination of writing in the native language, using the name of the receiver, using the name of the organisation and the name the organisation's executive (Flores *et al.*, 2015). These have proven to be successful. Our results show that by only using the name of the recipient, a strong spear effect can be established.

As spear phishing emails are more successful, it is suggested that the offender can generate similar benefits by sending fewer emails. From a rational choice perspective, spear phishing is, therefore, a bigger threat than general phishing.

No main or interaction effect of gender was found when controlling for socio-demographic variables i.e. females and males are equally vulnerable. These results suggest

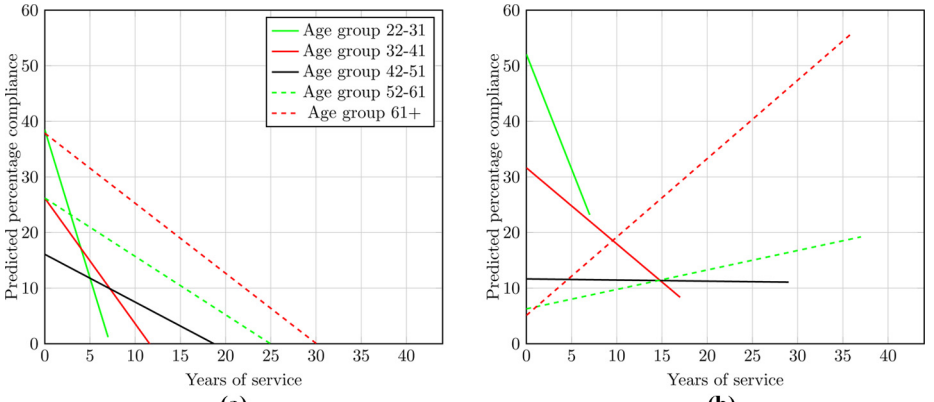

Figure 6. Predicted compliance based on the full model (i.e. spear, gender age, age^2, YoS, ageXyos, pdi, spearXgender, spearXage, spearXyos and spearXpdi) for five age groups by type of email (i.e. spear)

Notes: (a) Received a general email; (b) received a spear email

that females and males are equally capable of identifying (spear) phishing emails. We, therefore, conclude that incorporating a gender-based approach into awareness campaigns or training is unnecessary. One explanation for this finding could be that males are considered to be more tech-savvy, whereas females are considered more risk-averse. It was found in a quantitative study of 1,058 subjects that females had more negative attitudes and more anxiety towards ICT use compared to males (Broos, 2005). Furthermore, of 120 final-year polytechnic students, it was observed that males had acquired more ICT skills compared to females (Murgor, 2013). Regarding females being more risk-averse, experiments have shown that females make more risk-averse choices than males, whereas this effect declines with age (Riley and Chow, 1992; Hersch, 1996; Barsky *et al.*, 1997; Halek and Eisenhauer, 2001). Furthermore, people also tend to perceive and predict that females as more risk-averse than males (Ball *et al.*, 2010). Although it was not tested, it could be that these two effects cancel each other out.

No main effect of age was found when controlling for socio-demographic variables. This result contradicts previous experimental findings (Sheng *et al.*, 2010; Tembe *et al.*, 2013) which found younger people to be more vulnerable. Although Figure 3 suggests there is an effect, this effect disappears once the quadratic term was included in the model. One explanation could be that the other studies did not check or mention whether the relation between age and victimisation was u-shaped and assumed a linear rather than a quadratic model. When we tested the relation between age and compliance in a linear model, we also have found a strong age effect with younger people being more vulnerable. Moreover, although previous research found that younger people are more susceptible than older people, none of them included YoS as a variable in their analysis (Lee and Soberon-Ferrer, 1997; Titus *et al.*, 1995; Sheng *et al.*, 2010; Tembe *et al.*, 2013). Perhaps YoS is a better predictor for victimisation than age. Another explanation could be that older people have more experience regarding fraud (Titus *et al.*, 1995) and phishing, whereas younger people are born with this technology ubiquitously. Both age groups have an advantage which possibly complements one another. The relation between age and compliance is moderated by the type of email that was received. A "general" explanation for the moderation effect of email type could be that general phishing and spear phishing are two different types of crime and should be seen as such. This is comparable to the absence of a gender effect in fraud victimisation (Deevy *et al.*, 2012), whereas zooming in on the specific types of fraud did find gender effects.

It was found that those who worked longer for an organisation were less likely to be victimised by a phishing email. The phishing email used in this study was related to the organisation. Our explanation is that those who worked longer for the organisation are more aware and familiar with the rules and procedures and, therefore, less likely to fall for an organisation-related phishing email. Furthermore, it is important to include the variable YoS in future research involving organisational penetration testing.

The relation between YoS and compliance was moderated by age. As YoS and age are correlated, these two have a relation. In the context of an organisation, it makes sense that employees with more YoS are more familiar with the organisational procedures and customs, whereas those with less YoS, do not have this experience. The results suggest that young employees with few YoS are the group that is most vulnerable to phishing emails. A Human Resource Management strategy that favours focus on short temporary employment contracts, therefore, implies a security challenge! It is our view that this cost-reducing approach not only increases management but also security prevention costs. This trend of focusing on temporary employment contracts also surfaces in the physical security branch of, e.g., a national airport. In a report of the Dutch Federation of Trade Unions, 176 airport service agents were interviewed regarding their workload and safety culture of the airport

(FNV, 2016). It was almost unanimously (99 per cent) stated that it is important for safety and security to have experienced personnel, whereas 73 per cent stated that uncertainty regarding employment negatively affects airport security. The conclusion was that the workload and the security risks are partially caused by high staff turnover and job uncertainty in combination with inexperienced personnel (i.e. interns and temporary staff).

Regarding PDI, the results showed that those with high power distance cultural backgrounds are more vulnerable to phishing emails than those with a low score background. The rationale for this finding is that those with high PDI scores are more inclined to follow those higher in the hierarchy. The signature of the phishing email was from the Security Manager, someone clearly high in the hierarchy. Furthermore, the PDI scale describes "Subordinates expect to be told what to do" as a characteristic for those with a high score (Hofstede *et al.*, 2010). The phishing email had a clear instruction on what to do: "To synchronise your password, click here".

4.1 Implication for practice

This research has the following implications for the practitioners:

- Focus awareness: recently hired personnel and employees with cultural backgrounds that have a high PDI are more vulnerable. Special attention should be paid to this group.
- Content of an awareness campaign: spear phishing emails were more successful than general phishing emails. This knowledge should be included in the awareness training.
- It is advisable to give employees an intervention at the start of their employment.

4.2 Limitations

This study has several limitations:

- The cultural dimension PDI was based on nationality. The variable reflects the country-based average rather than the individual's score. Future research could involve the inclusion of the subject's cultural perception (Hofstede, 1980; Lee *et al.*, 2000; Yoo *et al.*, 2011).
- The dataset that was used in the analysis had missing values for some variables. It should be noted that the outcomes could be different if there were no missing values.

4.3 Future research

Finally, we present five recommendations for future research:

(1) Expansion of the experimental design to include an awareness campaign that counters the effect of phishing emails. An example of such a design is discussed in Bullée *et al.* (2015) and Wright *et al.* (2014).

(2) The usage of a heterogeneous sample for more generalisable results over a homogeneous academic sample.

(3) The usage of persuasion principles (refer to (Cialdini, 2009) for varying experimental conditions.

(4) Time decay effects of an intervention, as described in Bullée *et al.* (2016) and Sutton *et al.* (2011).

(5) The level of seniority was included as YoS. An additional variable to include could be the level of education.

References

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D. and Roinestad, H. (2007), "Phishing IQ tests measure fear, not ability", *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4886 LNCS*, pp. 362-366, doi: 10.1007/978-3-540-77366-5 33.

Bakker, W., Bokkes, B., Cleijne, S., Horlings, W. and Zandberg, K. (2015), "Susceptibility of practical phishing attacks in academic fields", (Unpublished manuscript).

Ball, S., Eckel, C.C. and Heracleous, M. (2010), "Risk aversion and physical prowess: prediction, choice and Bias", *Journal of Risk and Uncertainty*, Vol. 41 No. 3, pp. 167-193, doi: 10.1007/s11166 -010-9105-x.

Barsky, R.B., Juster, F.T., Kimball, M.S. and Shapiro, M.D. (1997), "Preference parameters and behavioral heterogeneity: an experimental approach in the health and retirement study", *The Quarterly Journal of Economics*, Vol. 112 No. 2, pp. 537-579, doi: 10.1162/003355397555280.

Belmont Report (1979), *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*, The Commission.

Bosworth, S., Kabay, M. and Whyne, E. (2014), *Computer Security Handbook*, 6th ed., Wiley, New York, NY.

Broos, A. (2005), "Gender and information and communication technologies (ICT) anxiety: male self-assurance and female hesitation", *CyberPsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, Vol. 8 No. 1, pp. 21-31, doi: 10.1089/cpb.2005.8.21.

Bullée, J.H., Montoya, L., Junger, M. and Hartel, P.H. (2016), "Telephone-based social engineering attacks: an experiment testing the success and time decay of an intervention", in Mathur, A. and Roychoudhury, A. (Eds), *Proceedings of the Singapore cyber-security conference (sg-crc) 2016*, Vol. 14, IOS Press, p. 107-114, doi: 10.3233/978-1-61499-617-0-107.

Bullée, J.H., Montoya, L., Pieters, W., Junger, M. and Hartel, P.H. (2015), "The persuasion and security awareness experiment: reducing the success of social engineering attacks", *Journal of Experimental Criminology*, Vol. 11 No. 1, pp. 97-115, doi: 10.1007/s11292-014-9222-7.

Chan, M., Woon, I. and Kankanhalli, A. (2005), "Perceptions of information security at the workplace: linking information security climate to compliant behaviour", doi: 10.1016/j.cose.2012.04.004.

Cialdini, R. (2009), *Influence*, HarperCollins, New York, NY.

Code of Federal Regulations (2005), *Title 45: Public Welfare, Department of Health and Human Services, Part 46: Protection of Human Subjects*, US Government Printing Office.

Cornish, D.B. and Clarke, R.V. (1987), "Understanding crime displacement: an application of rational choice theory", *Criminology*, Vol. 25 No. 4, pp. 933-948, doi: 10.1111/j.1745-9125.1987.tb00826.x.

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, doi: 10.1016/j.cose.2012.09.010.

Dang, H. (2008), "The origins of social engineering", *McAffee Security Journal*, Vol. 1 No. 1, pp. 4-8.

Deevy, M., Lucich, S. and Beals, M. (2012), "Scams, schemes and swindles a review of consumer financial fraud research", *Technical Report*, Financial Fraud Research Centre.

European Social Survey Education Netu (2013), "Adding interaction terms to OLS regression models", available at: http://essedunet.nsd.uib.no/cms/topics/multilevel/ch1/5.html (accessed 27 June 2016)

Field, A., Miles, J. and Field, Z. (2012), *Discovering Statistics Using R*, Sage Publications, London.

Flores, W.R., Holm, H., Nohlberg, M. and Ekstedt, M. (2015), "Investigating personal determinants of phishing and the effect of national culture", *Information & Computer Security*, Vol. 23 No. 2, pp. 178-199, doi: 10.1108/ICS-05-2014-0029.

FNV (2016), "Onzekerheid, werkdruk en veiligheidsrisico's - een verkennend onderzoek naar de veiligheids- beleving van passagemedewerkers op schiphol (No. 61604)", available at: www.fnv.nl/site/nieuws/webassistent/Jose-Kager/fnvonderzoek-bagage-en-incheckmedewerkers-schiphol-te-weinig-vaste-mensen-voor-veilig-werk-/onzekerheidwerkdrukenveiligheidsrisicosafhandelingschiphol.pdf (accessed 11 January 2017).

Furnell, S. (2007), "Phishing: can we spot the signs?", *Computer Fraud and Security*, Vol. 2007 No. 3, pp. 10-15, doi: 10.1016/S1361-3723(07)70035-0.

Gigerenzer, G. (1991), "How to make cognitive illusions disappear: beyond 'heuristics and biases", *European Review of Social Psychology*, Vol. 2 No. 1, pp. 83-115, doi: 10.1080/14792779143000033.

Grabosky, P.N. (2001), "Virtual criminality: old wine in new bottles?", *Social and Legal Studies*, Vol. 10 No. 2, pp. 243-249, doi: 10.1177/a017405.

Greene, W. (2011), *Econometric Analysis*, Pearson Education, London.

Halek, M. and Eisenhauer, J.G. (2001), "Demography of risk aversion", *The Journal of Risk and Insurance*, Vol. 68 No. 1, pp. 1-24, doi: 10.2307/2678130.

Hersch, J. (1996), "Smoking, seat belts, and other risky consumer decisions: differences by gender and race", *Managerial and Decision Economics*, Vol. 17 No. 5, pp. 471-481, doi: 10.1002/(SICI)1099-1468(199609).

Hofstede, G. (1980), *Culture's Consequences: International Differences in Work-Related Attitudes*, Sage, London.

Hofstede, G. (2001), *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations across Nations*, Sage, London.

Hofstede, G., Hofstede, G.J. and Minkov, M. (2010), *Cultures and Organizations: Software of the Mind, Third Edition*, Mcgraw-hill, New York, NY.

Holm, H., Flores, W.R., Nohlberg, M. and Ekstedt, M. (2014), "An empirical investigation of the effect of target-related information in phishing attacks", *2014 IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*, p. 357-363, doi: 10.1109/EDOCW.2014.59

Hong, J.H. (2012), "The state of phishing attacks", *Communications of the ACM*, Vol. 55 No. 1, pp. 74-81, doi: 10.1145/2063176.2063197.

Hong, K., Kelley, C.M., Tembe, R., Murphy-Hill, E. and Mayhorn, C.B. (2013), "Keeping up with the joneses: assessing phishing susceptibility in an email task", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 57 No. 1, pp. 1012-1016, doi: 10.1177/1541931213571226.

Jafari Kelarijani, S.E., Heidarian, A.R., Jamshidi, R. and Khorshidi, M. (2014), "Length of service and commitment of nurses in hospitals of social security organization (SSO) in Tehran", *Caspian Journal of Internal Medicine*, Vol. 5 No. 2, pp. 94-98.

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, doi: 10.1145/1290958.1290968.

Junger, M., Montoya, L. and Overink, F.-J. (2017), "Priming and warnings are not effective to prevent social engineering attacks", *Computers in Human Behavior*, Vol. 66, pp. 75-87, doi: 10.1016/j.chb.2016.09.012.

Kearney, W. and Kruger, H. (2014), "Considering the influence of human trust in practical social engineering exercises", *Information Security for South Africa, Johannesburg*, p. 1-6, doi: 10.1109/ISSA.2014.6950509

Kennedy, D. (2011), "There's something "human" to social engineering", available at: http://magazine.thehackernews.com/article-1.html

Lastdrager, E.E. (2014), "Achieving a consensual definition of phishing based on a systematic review of the literature", *Crime Science*, Vol. 3 No. 1, pp. 1-10, doi: 10.1186/s40163-014-0009-y.

Lee, C., Pillutla, M. and Law, K.S. (2000), "Power-distance, gender and organizational justice", *Journal of Management*, Vol. 26 No. 4, pp. 685-704, doi: 10.1177/014920630002600405.

Lee, J. and Soberon-Ferrer, H. (1997), "Consumer vulnerability to fraud: influencing factors", *Journal of Consumer Affairs*, Vol. 31 No. 1, pp. 70-89, doi: 10.1111/j.1745-6606.1997.tb00827.x.

Luo, R.X., Brody, R., Seazzu, A. and Burd, S. (2011), "Social engineering: the neglected human factor", *Information Resources Management Journal*, Vol. 24 No. 3, pp. 1-8, doi: 10.4018/irmj.2011070101.

McCusker, R. (2006), "Transnational organised cyber crime: distinguishing threat from reality", *Crime, Law and Social Change*, Vol. 46 Nos 4/5, pp. 257-273, doi: 10.1007/s10611-007-9059-3.

Miles, J. and Shevlin, M. (2001), *Applying Regression and Correlation: A Guide for Students and Researchers*, Sage Publications, London.

Mobley, W.H., Horner, S.O. and Hollingsworth, A.T. (1978), "An evaluation of precursors of hospital employee turnover", *The Journal of Applied Psychology*, Vol. 63 No. 4, pp. 408

Montoya, L., Junger, M. and Hartel, P. (2013). "How digital is traditional crime?", *Intelligence and security informatics conference (EISIC), 2013 European, Uppsala*, p. 31-37, doi: 10.1109/EISIC.2013.12

Murgor, T.K. (2013), "A comparison of technical and vocational acquired skills differences based on gender in Tvet institutions, Uasin Gishu County, Kenya", *Journal of Education and Practice*, Vol. 4 No. 22, pp. 181-187.

Neve, R. and Hulst, R.V.D. (2008), "High-tech Crime: inventarisatie van literatuur over Soorten criminaliteit en hun daders", *Technical Report No. 978-90-5454-998-7*, WODC.

Oshagbemi, T. (2000), "Is length of service related to the level of job satisfaction?", *International Journal of Social Economics*, Vol. 27 No. 3, pp. 213-226, doi: 10.1108/03068290010286546.

Pallant, J. (2010), *Spss Survival Manual: A Step by Step Guide to Data Analysis Using SPSS*, McGraw-Hill Education, New York, NY.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C. (2013), "Security and privacy protection in information processing systems", in Janczewski, L.J., Wolfe, H.B. and Shenoi, S. (Eds), *28th IFIP TC 11 International Conference, Sec 2013, Auckland*, 8-10 July, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 366-378, doi: 10.1007/978-3-642-39218-4 27.

Peduzzi, P., Concato, J., Kemper, E., Holford, T.R. and Feinstein, A.R. (1996), "A simulation study of the number of events per variable in logistic regression analysis", *Journal of Clinical Epidemiology*, Vol. 49 No. 12, pp. 1373-1379, doi: 10.1016/S0895-4356(96)00236-3.

Petrova, P.K., Cialdini, R.B. and Sills, S.J. (2007), "Consistency-based compliance across cultures", *Journal of Experimental Social Psychology*, Vol. 43 No. 1, pp. 104-111, doi: 10.1016/j.jesp.2005.04.002.

Pfeffer, J. (1985), "Organizational demography: implications for management", *California Management Review*, Vol. 28 No. 1, pp. 67-81, doi: 10.2307/41165170.

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, doi: 10.1016/j.cose.2009.05.008.

Riley, W.B. and Chow, V.K. (1992), "Asset allocation and individual risk aversion", *Financial Analysts Journal*, Vol. 48 No. 6, pp. 32-37, doi: 10.2469/faj.v48.n6.32.

Ross, M., Grossmann, I. and Schryer, E. (2014), "Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud", *Perspectives on Psychological Science*, Vol. 9 No. 4, pp. 427-442, doi: 10.1177/1745691614535935.

Sarker, S.J., Crossman, A. and Chinmeteepituck, P. (2003), "The relationships of age and length of service with job satisfaction: an examination of hotel employees in Thailand", *Journal of Managerial Psychology*, Vol. 18 No. 7, pp. 745-758, doi: 10.1108/02683940310502421.

Schneier, B. (2000), *Secrets & Lies: Digital Security in a Networked World*, 1st ed., John Wiley & Sons, New York, NY.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. (2010), "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions", *Proceedings of the Sigchi Conference on Human Factors in Computing Systems, ACM, New York, NY*, pp. 373-382, doi: 10.1145/1753326.1753383

Shenhav, Y. and Haberfeld, Y. (1992), "Organizational demography and inequality", *Social Forces*, Vol. 71 No. 1, pp. 123-143, doi: 10.1093/sf/71.1.123.

Smith, P.B. and Schwartz, S.H. (1997), "Values", in Berry, J.W., Segall, M.H. and Kagitçibasi, C. (Eds), *Handbook of Cross-Cultural Psychology: Social Behavior and Applications*, Allyn & Bacon, Boston, Vol. 3, pp. 77-118.

Sparshott, M. (2014), "The psychology of phishing", available at:www.helpnetsecurity.com/2014/07/23/the-psychology-of-phishing/ (accessed 26 May 2016)

Sutton, R.M., Niles, D., Meaney, P.A., Aplenc, R., French, B., Abella, B.S., Lengetti, E.L., Berg, R.A., Helfaer, M.A. and Nadkarni, V. (2011), "Low-dose, high-frequency CPR training improves skill retention of in-hospital pediatric providers", *Pediatrics*, Vol. 128 No. 1, pp. e145-e151, doi: 10.1542/peds.2010-2105.

Tembe, R., Hong, K.W., Murphy-Hill, E., Mayhorn, C.B. and Kelley, C.M. (2013), "American and indian conceptualizations of phishing", *Third workshop on socio-technical aspects in security and trust, New Orleans, LA*, p. 37-45, doi: 10.1109/STAST.2013.10

Titus, R.M., Heinzelmann, F. and Boyle, J.M. (1995), "Victimization of persons by fraud", *Crime & Delinquency*, Vol. 41 No. 1, pp. 54-72, doi: 10.1177/0011128795041001004.

Tversky, A. and Kahneman, D. (1974), "Judgment under uncertainty: heuristics and biases", *Science* , Vol. 185 No. 4157, pp. 1124-1131, doi: 10.1007/978-94-010-1834-0 8.

Twitchell, D.P. (2009), "Social engineering and its countermeasures", *Handbook of Research on Social and Organizational Liabilities in Information Security*, IGI-Global.

Van Wyk, J. and Benson, M.L. (1997), "Fraud victimization: risky business or just bad luck?", *American Journal of Criminal Justice*, Vol. 21 No. 2, pp. 163-179, doi: 10.1007/BF02887448.

Waldrop, M. (2016), "How to hack the hackers: the human side of cybercrime", *Nature*, Vol. 533, pp. 164, doi: 10.1038/533164a.

Waters, L., Roach, D. and Waters, C.W. (1976), "Estimates of future tenure, satisfaction, and biographical variables as predictors of termination", *Personnel Psychology*, Vol. 29 No. 1, pp. 57-60, doi: 10.1111/j.1744-6570.1976.tb00401.x.

Wright, R., Jensen, M., Thatcher, J., Dinger, M. and Marett, K. (2014), "Influence techniques in phishing attacks: an examination of vulnerability and resistance", *Information Systems Research*, Vol. 25 No. 2, pp. 385-400, doi: 10.1287/isre.2014.0522.

Yoo, B., Donthu, N. and Lenartowicz, T. (2011), "Measuring Hofstede's five dimensions of cultural values at the individual level: development and validation of CV scale", *Journal of International Consumer Marketing*, Vol. 23 Nos 3/4, pp. 193-210, doi: 10.1080/08961530.2011.578059.