Who is more susceptible to phishing emails?: A Saudi Arabian study

Ibrahim Alseadoon
Science and Engineering Faculty
Queensland University of Technology
Brisbane, Australia
Email: ibrahim.alseadoon@student.qut.edu.au

Taizan Chan
Science and Engineering Faculty
Queensland University of Technology
Brisbane, Australia
Email: t.chan@qut.edu.au

Ernest Foo
Science and Engineering Faculty
Queensland University of Technology
Brisbane, Australia
Email: e.foo@qut.edu.au

Juan Gonzalez Nieto
Science and Engineering Faculty
Queensland University of Technology
Brisbane, Australia
Email: j.gonzaleznieto@qut.edu.au

Abstract
Phishing emails cause enormous losses to both users and organisations. The goal of this study is to determine which individuals are more vulnerable to phishing emails. To gain this information an experiment has been developed which involves sending phishing email to users and collecting information about users. The detection deception model has been applied to identify users' detection behaviour. We find that users who have less email experience and high levels of submissiveness have increased susceptibility. Among those, users who have high susceptibility levels and high openness and extraversion are more likely to carry on the harmful action embedded in phishing emails.

Keywords
Phishing emails, phishing attacks, ability to suspect phishing emails, human factors, and human behaviour.

INTRODUCTION

Phishing emails have become a significant threat to online users (Pettey 2006). These emails employ technical and social engineering tricks to increase their appearance of legitimacy (Bose and Leung 2009). The aim of phishing emails is to encourage users to perform actions that are ultimately harmful, such as making users click on an embedded link that takes them to a phishing website that mimics a valid website in order to steal their private information. An example of this would be an attacker designing a website that is identical to a well-known bank website and then sending a mass email to users who may be known to the attacker as clients of the targeted bank. The users click on the link embedded in the email, which takes them to the fake website. After inputting their user name and password and/or revealing other personal information, the attacker may connect these victims to the real bank website to reduce any chance of discovering the intrusion.

The number of phishing emails and their victims is rapidly increasing. According to the Anti-Phishing Working Group (APWG) (2011), the number of phishing attacks is in the millions. The number of unique phishing attacks worldwide was 67,677 in the second half of 2010, which was an increase from the first half of the year (Aaron and Rasmussen 2011). The number of phishing attacks is expected to exceed the number of attacks reported by the APWG, since they are not able to include all Internet users' worldwide in their statistics. In 2009, Trusteer investigated online banking attacks. This study reported that 0.47% of bank customers fall victim to phishing attacks each year. The amount of money lost by these attacks is between US$2.4 million to $9.4 million annually per one million online banking customers (Trusteer 2009). To reduce these numbers, vulnerable users have to be identified and targeted with education and training programs to improve their defences against phishing attacks.

Education programs have been designed to increase users' protection after they fall victim to the email (Arachchilage et al. 2012; Bekkering et al. 2009; Kumaraguru et al. 2009). However, these programs lack the ability to identify users before they become victims because they depend on the users responding to training phishing emails, which may not be identified by vulnerable users because (1) users may not respond to training emails because these email are not attractive to them (2) users may overlook the educational emails because of the amount of emails they receive. There is a need to identify vulnerable users based on their characteristics, and identifying them before they become victims would reduce user, government, and organisational losses caused by these kinds of threats.

Finding vulnerable users begins by understanding the way that they behave when they open a phishing email. We believe there are four phases in the process of detecting deception: susceptibility, detection, confirmation, and action (see Fig. 1). Based on susceptibility levels, users can be classified into three groups: users who detect, users who check, and users who miss the detection. Users who have doubts will confirm or deny their doubts by choosing a suitable confirmation channel. Then, users will decide whether to respond or ignore.

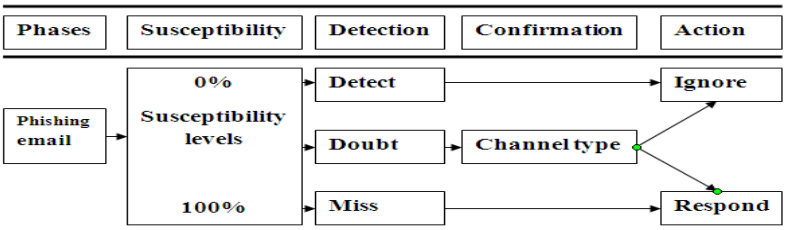

Fig. 1. Users' behaviour in detecting phishing emails.

Aim of the Study

The purpose of this study was to determine the important factors that are responsible for causing Internet users in Saudi Arabia to fall victims to phishing emails. Saudi Arabia is a developing country that aims to employ advanced technology in its government services to its own people. Technology has a negative side, such as phishing emails, which take advantage of the available online services to target vulnerable users and steal their personal information. Identifying vulnerable users would help to improve their protection against these kinds of attacks through education and training. Negative experiences with online services will have a negative impact on implementation of these online services, which may result in expensive financial loss for both organisations and users. Inexperienced users of online services are especially vulnerable targets for advanced and expert attackers. In this research, the model of detecting deception (See Fig. 2) has been applied to identify the impact of individual factors on the process of detecting phishing emails.

The paper is organised as follows: the related empirical work provides an overview of phishing email research. The theoretical model section introduces the theory used in conducting this research. The methodology section explains the methods used in this research. The results section describes the research findings, and the discussion section presents the findings and their importance. Last sections are description of the research limitations and conclusions.

RELATED IMPIRICAL WORK

Phishing email studies show that users can detect phishing emails without taking part in educational programs. In many phishing email studies, up to 40% of the subjects did not fall victim to experimental phishing emails (Dhamija et al. 2006; Jakobsson 2007; Karakasiliotis et al. 2006; Sheng et al. 2010). However, these studies did not investigate the reasons that prevented the users from becoming victims. To understand these reasons, an explanation of the design features of phishing emails is needed.

Wang et al. (2009) conducted a study by analysing 195 phishing emails with an elaboration likelihood model (ELM). The ELM model is based on the idea that the message argument quality is responsible for affecting message receivers' attitude toward message acceptance (Bhattacherjee and Sanford 2006). Argument quality refers to the strength of conviction in the argument that is embedded in the message (Bhattacherjee and Sanford 2006). Gaining acceptance eases any barriers that keep the users from becoming victims; an example of this would be a phishing email telling users that their account has encountered a problem and they need to perform an immediate action or their account will be suspended. Argument here explains the reason why they received the phishing email. Argument quality was employed in the design of this study phishing email.

Wright et al. (2009) conducted a study of phishing emails and found that users' individual factors play an important role in their process of detecting phishing emails. The study found that users' low experience with the Internet and high levels of trust are responsible for causing them to respond to the phishing emails. This study introduces the impact of users' individual factors on their ability to detect phishing emails, as this needs more

investigation. This paper extends the findings by identifying the impact of individual factors on the phases in the model of detecting deception (see Fig. 2). In addition to identifying differences between detectors and victims in their individual factors to shed the light on the reasons why victims are weak in detecting phishing emails.

Vishwanath et al. (2011) found four important factors in the vulnerability to phishing emails: involvement, email load, knowledge, and computer self-efficacy. They found that a high level of attention given to email sources and grammar and spelling mistakes led users to perform elaboration (elaboration is a process of making conscious decision based on comparing observed cues and prior knowledge (Perse 1990)). However, elaboration did not prevent users from choosing to respond to the content of a phishing email. Elaboration is based on previous knowledge; users who do not know the meaning of the observed cues will not detect the phishing emails, as users will examine the emails based on their previous knowledge. The existence of cues that lead to detecting phishing emails will not help users detect deception. Users have to gain knowledge that will allow them to draw attention to specific cues, which will then lead to elaboration. Coronges et al. (2011) reported that warning users about the existence of phishing emails does not stop users from becoming victims. Users' fears of phishing emails also does not increase their ability to detect them (Sven et al. 2007). Grazioli (2004); also found that detectors and victims both suspect the existence of a phishing attack but that victims fail to prove it. The question remains what are the individual factors which improve detectors prior knowledge. Our study tries to answer this question.

THEORETICAL MODEL

Grazioli (2004) proposed a model of deception detection based on the theory of deception (Johnson et al. 2001). This model suggests that the process of detecting deception by individuals is divided into four phases: activation, hypothesis generation, hypothesis evaluation, and global assessment. The process begins when users observe inconsistent cues in emails. Cues can be defined as the signs that make users detect phishing emails such as the existence of spelling mistakes. Grazioli (2004) identified differences between detectors and victims in their detection of deception process. These differences clearly appear in the last two phases of the model of detecting deception (see Table 1). This indicates that detectors and some victims suspect phishing emails but that only detectors are able to identify phishing attempts. Grazioli did not investigate differences between the users.

Table 1. Differences between Detectors and Victims in the Detecting of Deception Model

Model Phases	Detectors	Victims
Activation	Inconsistence cues	Inconsistence cues
Hypothesis generation	Priming not significant	Priming is significant
Hypothesis evaluation	Competence at evaluation	Incapable of evaluation
Global assessment	Assurance cues	Trust cues

The Model of Detecting Deception

By building on the findings by Grazioli (2004), Wright et al. (2009) conducted a study of phishing emails and found two more important factors that are responsible for activating users' suspicion, which is the first phase in the model of detecting deception. These factors are priming and individual factors (see Fig. 2). Priming is defined as any experience that brings a cognitive structure to the mind that makes it available for employment in a subsequent mission (Higgins and Kruglanski 1996). In other words, priming is a mechanism that warns users about possible deceptive behaviour, such as banks inform their clients that they will never ask about passwords via emails. Individual factors are those that differentiate users from each other. Wright et al. (2009) showed that users who have the same training and priming and are faced with the same phishing email have different responses. Some of these users become detectors and others become victims of the phishing email. This means that there are individual factors of the users themselves that make some users detectors and some users victims. These factors should be investigated and identified.

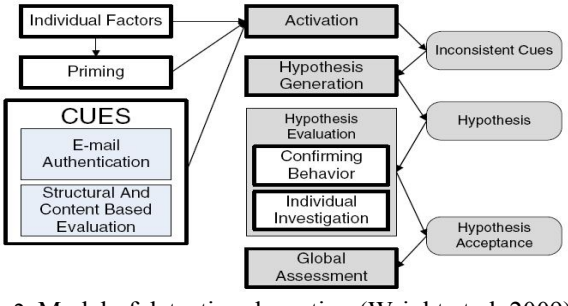

Fig. 2. Model of detecting deception (Wright et al. 2009)

INDIVIDUAL FACTORS ANALYSED

This section includes the research model (see Fig. 3) that illustrates the impact of users' individual factors on their phishing email detection behaviour. The impact of these factors on the process of detection was investigated by testing them with the model of detecting deception. This section describes the reasons behind the choice of these individual factors.

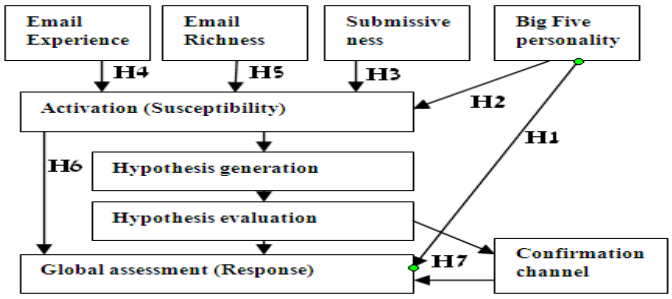

Fig. 3. Research model

Priming

Priming has not been included in this research because this research focuses on the impact of individual factors on detection behaviour. Participants have not been primed to minimize its impact on detection.

The Big Five Personality Dimensions

The big five personality dimensions divide people into five main dimensions: extraversion (H1,2a), agreeableness(H1,2b), consciousness (H1,2c), emotional stability (H1,2d), and openness (H1,2e) (Gosling et al. 2003). These personality dimensions have an impact on individuals' behaviour with other people and entities, such as phishing emails. These factors have also been suggested but not tested as influencing a user's ability to detect phishing emails and whether they follow the instructions in the phishing emails (Parrish Jr et al. 2009). The measure developed by Gosling et al. (2003) that uses 10 items to measure the big five personality traits has been employed.

H1. Each dimension of the Big five personality is responsible for making victims respond to phishing emails.
H2. Each dimension of the Big five personality increases users' susceptibility.

Submissiveness

The nature of phishing emails is to manipulate users to force them perform the actions included in the emails. Detectors of phishing emails refuse to perform those actions, while victims do not question the authenticity or refuse to perform the action proposed (submissive behaviour). Therefore, this research investigated the impact of users' submissiveness on their reactions to the phishing emails. This research measured submissiveness with 16 items developed by Allan and Gilbert (Allan and Gilbert 1997).

Wright et al. (2009) discovered that detectors do not fall victims to the phishing email because they have been instructed several times to not disclose their passwords to anyone, even their closest family members. This suggests that submissive behaviour has an impact on users' ability to protect themselves. To imitate real-world situations, this research investigated the impact of this factor with participants who had not been instructed to protect their passwords.

H3. Submissiveness increases users' susceptibility to phishing emails.

Email Experience and Email Richness

According to the theory of channel expansion (Carlson and Zmud 1999), users who have high experience with email will consider email as a very rich medium (richness is measured by the ability to reproduce information carried by the medium. (Daft and Lengel 1986)). The benefit of having a rich medium is that users have the advantage of being able to observe deceptive cues. These two factors have not been previously investigated with phishing emails. The reason for including these two factors in the research model is because studies of deception have shown that people ability to detect deception in rich mediums (e.g. Face to Face) is higher than low rich mediums (e.g. phone). . This research proposes that users who have high levels of experience and consider email to be a rich medium will be better detectors than those who are low in experience and richness. To measure email richness and experience, this research employed the same measure used in the channel expansion theory, which includes six items to measure experience and four items to measure richness (Carlson and Zmud 1999).

H4. High experiences with email will decreases users' susceptibility to phishing emails.
H5. Perceived email richness by users decreases their susceptibility to phishing emails.

THE FACTORS INVOLVED IN THE PROCESS OF DECEPTION DETECTION

This section delineates the factors investigated in the process of detecting phishing emails. These factors have to be considered because they impact the user's detection process, which begins with suspecting the phishing email (measured by users' susceptibility), continues with a confirmation method and finishes with the user performing or not the requested action (measured by response).

Susceptibility

Susceptibility is the first step in detection and has three levels. Users who have a high level of susceptibility are expected to respond to phishing emails because they never doubt the authenticity of phishing emails. A low level of susceptibility is expected to make users detectors, and the users who are in the middle reduce or sometimes increase their susceptibility through confirmation channels of their choice. In order to measure users' susceptibility, the participants were presented with five phishing emails and asked to evaluate "the likelihood to respond to each email" on a scale of 7 points. The direct impact of this factor on users' response to phishing emails has not been studied before.

This study tried to avoid users' perceptions to each email by presenting them with an introduction that stated the relationship between the receiver and the email type. Participants were informed that the receiver "Mohammed" had a relationship with every organisation in the five emails.

H6. A high level of susceptibility increases users' chances to respond to phishing emails.

Confirmation

Users, who doubt the authenticity of an email, will go through various channels to confirm or deny their doubts. Phishing email research has found that users choose different ways of authentication. These ways can be called confirmation channels, which have not previously been investigated to determine their relationship with users as victims or detectors. This research suggests that strong confirmation channel which cannot be manipulated by attackers will improve users' detection. Therefore, participants were asked in the second survey to identify the type of confirmation channel they chose when they suspected the authenticity of the experimental phishing email.

H7. Strong confirmation channel decreases users' chances of responding to phishing emails.

Response

This is the final action that determined whether users were victims or detectors. This action recorded the users' actual responses when they received the experimental phishing email. Participants were sent two types of phishing emails, reply emails and click emails, which are explained in the following section.

METHODOLOGY

This section explains the experimental process for our research in Saudi Arabia. The first step was translating the English version of the survey into Arabic. The second step was asking students to activate their university email because some of them had not done so. The first survey was sent to collect students' individual factors and then sent normal emails to students before sending the experimental phishing email. The next step was sending the experimental phishing email and a final survey to capture users' behaviour. These steps are explained in this section in more detail.

Translation

The survey we used had been created in English. Since Saudi Arabian students have very limited knowledge of the English language, the survey instruments had to be translated into Arabic. This was done with these steps:

- The survey was translated from English to Arabic using a specialised translation office.
- The resulting Arabic survey was then translated from Arabic back to English by a different translation office. This was done to avoid the chance of it being translated by the same person who had done the first translation, which would affect the ability of the translation to be only based on the Arabic version.
- The two English versions were compared for any changes of meaning. If any changes were found, then the Arabic version was changed to more accurately capture the original meaning.
- The final Arabic survey was then sent to an Arabic teacher to fix any mistakes in spelling, grammar, or overall meaning.

Activate Emails

Participants (students) were asked to activate their university email. This step was necessary because many of the students had never activated their university email and simply used an email address on a different server.

Participants were told that they needed to activate their emails to receive their marks and instruction from their lecturers. Students were not informed that they had been chosen to participate in the experiment. This would have had two main negative impacts on the results: (1) Priming would have improved students' detection of the phishing emails, and (2) caution would have led the students to examine every email in their university inbox. One month after they activated their accounts, the students received their first email from the lecturer that included some instructions and their exam marks.

The Phishing Email

The phishing email informed students about a problem that had occurred in the university system that had damaged some system information. The phishing email emphasised that the participants who received this email were those that had been affected by this recent problem and they had to act fast to solve it. After explaining the reason that they had received the email, the students were prompted to act in order to solve the problem. The solution provided to participants came in a form of two actions: replying to the email address with the requested information or clicking on a link included in the phishing email. Finally, the email was signed with the name of an authentic IT specialist (this name appeared in the address bar as well), along with the name of the university and the Department of Computer Science, where the students were enrolled.

Subjects

This research targeted undergraduate students in Saudi Arabia as they were within the 18-25 age group, which has been reported being the most susceptible to phishing emails (Kumaraguru et al. 2009; Sheng et al. 2010). The purpose of this was to determine the individual differences in the most vulnerable age group. Subjects were 200 students in one unit in the Department of Computer Science. They were informed about the experiment one week after they received the experimental phishing email. Students were not informed about the phishing email ahead of time to avoid unnatural reactions from the students.

Conducting phishing email experiment produce high privacy risk (Jakobsson and Ratkiewicz 2006). This research gained the ethic committee approval. Subjects' information is protected in a secure server and their private information such as email addresses were substituted with numbers for protection.

The Survey

The survey was divided into two parts. The first part took place before the phishing emails were sent and asked participants about their individual factors (the big five personality traits, submissiveness, and susceptibility). The second part asked participants about their interactions with the phishing email experiment and their reactions (e.g., whether they saw the experimental phishing email and how they conducted their investigation if they had doubts about the content of the email).

The Interviews

After collecting all the information from the first and second parts of the survey and the experimental phishing email, students were sent an interview invitation. Six participants responded to the request, but none of them were victims to the experimental phishing email. A follow-up request was sent to the 14 victims, asking them several questions about their responses to the experimental phishing email. Only 4 victims answered these questions. The outcomes of these interviews are provided in the results section.

RESULTS

This research targeted nearly 200 Saudi Arabian students, who were randomly divided into two groups—click emails and reply emails. Fourteen students responded to the phishing email (7% of the population). This finding agrees with the 3% to 11% victim rate of the population targeted by phishing emails (Jakobsson and Ratkiewicz 2006; Knight 2004; Pettey 2006). Most of the responses came from the click email (86% of the victims). This indicates that users were not comfortable revealing their sensitive information via email or by direct request. Click emails do not ask users to reveal their information directly but request the information via a login webpage. This may trick users into forgetting to authenticate the legitimacy of the email.

In order to analyse the data, linear regression for the susceptibility factor (suspicion) and logistic regression for the response factor (action) is used. The results show that the R-square value (R^2) is 0.047 for the regression with susceptibility as the Dependant Variable (DV) and 0.283 for the regression with response as the DV. These results are explained briefly in Table 2 and in more details below.

Table 2. Summary of Hypothesis Test

Hypothesis	Results	Overall conclusion
Hypothesis 1a (Extraversion)	S.E. = 0.356 and p = 0.068	Supported weakly
Hypothesis 1e (Openness)	S.E. = 0.332 and p = 0.015	Supported
Hypothesis 2 (Big Five)		Not Supported
Hypothesis 3 (Submissiveness)	β = 0.253 and p = 0.004	Supported
Hypothesis 4 (Email experience)	β = -0.188 and p = 0.056	Supported
Hypothesis 5 (Email richness)		Not Supported
Hypothesis 6 (susceptibility)	S.E. = 0.280 and p = 0.017	Supported
Hypothesis 7 (confirmation channels)		Not Supported

Big Five Personality Dimensions

The results supported the hypothesis (H1a) and (H1e) and found a significant relationship between the last phase in the model of detecting deception (see Fig. 2) which is responding to the experimental phishing email and users who were more open and extroverted. Openness (S.E. = 0.332 and p = 0.015) and Extraversion (S.E. = 0.356 and p = 0.068). However, the results did not show significant relationship between Big Five personality dimensions and the first phase in the model of detecting deception (see Fig. 2) which is activation. Openness users are those who are open to new ideas and experience. E-commerce in Saudi Arabia is just developing, which explains why these users become victims. It can be said that these openness users are enthusiastic to try and test new experiences provided on the Internet (risk takers). Extraverted users become victims because they may judge phishing emails based on their positive emotions. According to Forgas et al. (2008) users' emotions impact their ability to detect deception. Users detection ability improves when they are feeling sad (Forgas and East 2008). This result shows that users' characteristics influence their response to phishing emails, which is independent from the process of detecting deception. In other words, users may see red flags in the phishing emails but choose to perform the action anyways because of the impact of their personality dimensions.

Submissiveness

High submissiveness increases users' susceptibility to phishing emails (β = 0.253 and p = 0.004). This is an important result since this research did not instruct participants to protect their password. This research found that because of the nature of phishing emails, which introduce a problem and highly recommend performing an action, submissive users are more likely to be susceptible. However, submissiveness can also be used in a beneficial way since these victims have high levels of submissiveness, and organisations or governments can instruct these users not to expose their important information to anyone.

Email Experience and Email Richness

Email experience has been found to negatively affect users' susceptibility to phishing emails (β = -0.188 and p = 0.056). Unfortunately, there was no significant relationship between email richness and users' susceptibility.

Susceptibility

There is a significant relationship between users' susceptibility to phishing emails and their response to phishing emails (S.E. = 0.280 and p = 0.017). This indicates that vulnerable users can be identified by measuring their likelihood to respond to several examples of phishing emails. Moreover, some victims do not perform the two steps in the process of detecting deception (hypothesis generation and hypothesis evaluation). These victims perform the action directly.

This study developed and performed factor analysis and found that all five phishing emails can perform one factor (see Table 3). A reliability test was performed with Cronbach's alpha test (Nunnally and Bernstein 1994), which is designed to measure internal consistency between certain items to construct one factor and the result was 0.6 (see Table 4).

Table 3. Susceptibility Factor Analysis (Component Matrix)

Instrument	Scam	Uni.	PayPal	EBay	Bank
Load	.440	.593	.706	.745	.669

Table 4. Susceptibility Cronbach's Alpha (Reliability Statistics)

Cronbach's Alpha	N of Items
.629	5

Confirmation Channels

Unfortunately, this research did not find any significant relationship between confirmation channels and being victims of phishing emails. The reason is because the number of victims is small. In the interviews, victims

showed that they followed different confirmation channels, but the problem with these channels is they can be controlled by the attackers. For example, one victim suspected the experimental phishing email but he responded to it because he asked his friend who had already received the email and responded to it.

DISCUSSION

This study investigated the impact of Saudi Arabian users' individual factors on their ability to detect phishing emails. The findings suggest that there are various individual factors that affect different phases in the model of detecting deception (see Fig. 2), which implies that individual factors have an impact on the process of detection, as explained in this section.

Activation

The study suggests that there are two main factors that influence users' susceptibility (activation). These factors are submissiveness and email experience. The more submissive the users, the more likely they are to not suspect phishing emails. Submissiveness may make users careless about trusting emails. For example, two users reported that they executed the action in the phishing email because they trusted that the email came from the university. On the other hand, experience with email reduces users' susceptibility to phishing emails. However, this suspicion will not save users from becoming victims if they do not generate a reliable hypothesis, which is the second phase of detecting deception.

Hypothesis Generation

When users suspect an email, they generate a hypothesis. Based on the hypothesis strength, users will choose their method of evaluation. Some hypotheses make users victims, such as those who generate the hypothesis that emails that appear to be from familiar websites or are confirmed by peers are trustworthy. These are weak hypotheses because they can be undermined by various types of phishing emails.

Detectors on other hand have been found to generate strong hypotheses that cannot be undermined by phishing emails. An example of this would be examining the information data in the email by searching for these data in search engines. Detectors consider emails from unknown persons as alarming especially if they have attachments.

Hypothesis Evaluation

This phase included the confirmation channels that users chose to confirm or deny their suspicions. This behaviour has been classified by Wright et al. into two main categories—confirmation and investigative behaviour. Confirmation behaviour involves users who have come to a decision but seek other people to help them confirm their decision. Investigative behaviour involves users who depend on themselves to come to a decision and act based on that decision. Users who chose channels that could not be controlled by the attacker, such as directly asking their lecturer about the email, have been found to be detectors. The results suggest that there are no significant differences in the confirmation or investigative behaviour of the victims and detectors.

Global Assessment

This was the last phase in the detection process where users came to a decision of whether to respond to the phishing email. Users who go through the process of detecting deception may become victims of phishing emails. This is simply because the victims make wrong decisions during the detection process. For example, in our study, two victims reported that they suspected the phishing email, but their way of confirming their suspicion was not a suitable way of detecting phishing emails. One says that he examined the phishing email several times, and the other asked his colleague who was also a victim.

Our research also introduced several factors that impact a user's decision of whether to respond to phishing emails. These factors are users' personality traits and susceptibility levels. Users with extraversion, openness, and high susceptibility are more likely to perform the action in the phishing email. This may be because these types of users have more trust in themselves, which makes them ignore red flags in the process of detecting deception. Finally, some individual factors did not show impact on users' detection of phishing emails, while these same individual factors have been reported in the literature to have a significant impact on detection. The reason behind this could possibly be explained by the users' different cultural backgrounds. These findings need more investigation. Users' ability to detect phishing emails is explained in the following quasi mathematical formula:

Ability to detect phishing emails =	High email experience - Submissive	(Activation)
	+ Strong hypothesis	(Hypothesis generation)
	+ Strong confirmation channel	(Hypothesis evaluation)
	+ Low level of susceptibility - Openness - Extraversion	(Global assessment)

LIMITATIONS

This research investigated phishing emails related to victims' relationships with an impersonal company. To measure susceptibility, avoiding users' predictions is enormously important. Therefore, the relationship between the receiver and the company has to be clarified. Clarification has been done by informing participants that there is a relationship between the organisations and the receiver. However, users' experiences with these organisations have not been captured.

The number of victims in this experiment was very low (7%), but it was in agreement with the average estimated percentage for the general population (3% to 11%). It is very hard for this kind of research to receive ethical approval to target a higher number of participants. For example, to get 50 victims, the experiment needs to send an experimental phishing email to 1,700 participants, which would be hard to receive ethical approval for, especially in a university setting. Finally, the result from this study needs further investigation as the number of participants in the study (200) is much smaller as compared to the web-user community in Saudi Arabia.

CONCLUSION

The aim of this research was to determine Saudi Arabian users' ability to detect phishing emails. The results obtained by this research support the hypothesis that there are several individual factors that affect users' phases of detection as explained in the model of detecting deception (see Fig. 2).

Individual factors have different impacts on users' phases of detection. Specifically, this research found that individual factors have a significant impact on the two main phases in the model of detecting deception (see Fig. 2): activation (susceptibility) and global assessment (response). For the first phase of activation, low email experience and submissive users are more likely to not suspect phishing emails. For the second phase of action, extraversion and openness have the disadvantage of making users become victims to phishing emails. A high level of susceptibility also impacts users becoming victims. The more susceptible they are, the more likely they will perform the action in the phishing email.

This paper suggests that vulnerable users to phishing emails can be identified by their individual factors. These users protection can be improved before phishing emails reach them. In order to increase protection, organisations need to improve users' knowledge about emails in general and phishing emails in particular. Users risk behaviour with phishing emails can be reduced by introducing penalties for those users who are influenced by their personality characteristics to perform risk behaviour.

REFERENCES

Aaron, G., and Rasmussen, R. 2011. "Global Phishing Survey: Trends and Domain Name Use in 2h2010," *Anti-Phisihng Working Group*, Lexington, MA USA

Allan, S., and Gilbert, P. 1997. "Submissive Behaviour and Psychopathology," *British Journal of Clinical Psychology* (36:4), pp 467-488.

Arachchilage, N. A., Love, S., and Scott, M. 2012. "Designing a Mobile Game to Teach Conceptual Knowledge of Avoiding "Phishing Attacks"," *International Journal for e-Learning Security* (2:2), pp 127-132

Bekkering, E., Hutchison, D., and Werner, L. 2009. "A Follow-up Study of Detecting Phishing Emails," *Proceedings of the Conference on Information Systems Applied Research 2009*, Washington DC.

Bhattacherjee, A., and Sanford, C.C. 2006. "Influence Processes for Information Technology Acceptance: An Elaboration Liklihood Model," *MIS Quarterly* (30:4), pp 805-825.

Bose, I., and Leung, A. C. 2009. "Technical Opinion: What Drives the Adoption of Antiphishing Measures by Hong Kong Banks?," *Commun. ACM* (52:8), pp 141-143.

Carlson, J. R., and Zmud, R. W. 1999. "Channel Expansion Theory and the Experiential Nature of Media Richness Perceptions," *Academy of Management Journal* (42:2), pp 153-170.

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J., and Rovira, E. 2012. "The Influences of Social Networks on Phishing Vulnerability," *System Science (HICSS), 2012 45th Hawaii International Conference*, Maui, Hawaii, USA, pp 2366-2373.

Daft, R. L., and Lengel, R. H. 1986. "Organizational Information Requirements, Media Richness and Structural Design," *Management Science*, pp 554-571.

Dhamija, R., Tygar, J. D., and Hearst, M. 2006. "Why Phishing Works," *Proceedings of the SIGCHI conference on Human Factors in computing systems*, New York, NY, USA: ACM, pp 581-590.

Forgas, J. P., and East, R. 2008. "On Being Happy and Gullible: Mood Effects on Skepticism and the Detection of Deception," *Journal of Experimental Social Psychology* (44:5), pp 1362-1367.

Gosling, S. D., Rentfrow, P. J., and Swann, W. B. 2003. "A Very Brief Measure of the Big-Five Personality Domains," *Journal of Research in personality* (37:6), pp 504-528.

Grazioli, S. 2004. "Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception over the Internet," *Group Decision and Negotiation* (13:2), pp 149-172.

Group, A-P.W. 2011. "Phishing Activity Trends Report, 1st Half 2011," *Anti-Phishing Working Group,* pp 1-11

Higgins, E. T., and Kruglanski, A. W. 1996. *Social Psychology* : Handbook of Basic Principles. New York: Guilford Press.

Jakobsson, M. 2007. "The Human Factor in Phishing," *Privacy & Security of Consumer Information*.

Jakobsson, M., and Ratkiewicz, J. 2006. "Designing Ethical Phishing Experiments: A Study of (ROT13) Ronl Query Features," *Proceedings of the 15th international conference on World Wide Web*. Edinburgh, Scotland: ACM, pp 513-522.

Johnson, P. E., Grazioli, S., Jamal, K., and Glen Berryman, R. 2001. "Detecting Deception: Adversarial Problem Solving in a Low Base-Rate World," *Cognitive Science* (25:3), pp 355-392.

Karakasiliotis, A., Furnell, S.M., and Papadaki, M. 2006. "Assessing End-User Awareness of Social Engineering and Phishing," *Proceedings of the 7th Australian Information Warfare and Security Conference*: Citeseer, pp 60-73.

Knight, W. 2004. "Goin' Phishing?," *Infosecurity Today* (1:4), pp 36-38.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A., and Pham, T. 2009. "School of Phish: A Real-World Evaluation of Anti-Phishing Training," *Proceedings of the 5th Symposium on Usable Privacy and Security*. Mountain View, California: ACM, pp 1-12.

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

Parrish Jr, J. L., Bailey, J. L., and Courtney, J. F. 2009. "A Personality Based Model for Determining Susceptibility to Phishing Attacks,", *Decision Sciences Institute,* pp 285-296.

Perse, E. 1990. "Audience Selectivity and Involvement in the Newer Media Environment," *Communication Research* (17:5), pp 675-697.

Pettey, C. 2006. "Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008," Retrieved 2 September, 2009 from http://www.gartner.com/it/page.jsp?id=936913

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 28th international conference on Human factors in computing systems*. Atlanta, Georgia, USA: ACM.

Sven, D., Rachna, D., Vivek, A., Andrew, D., Markus, J., Debin, L., and Heather, R. 2007. "Phishing IQ Tests Measure Fear, Not Ability," *Financial Cryptography and Data Security*. Springer Berlin / Heidelberg, pp 362-366.

Trusteer. 2009. "Measuring the Effectiveness of in-the-Wild Phishing Attacks," *Trusteer*, New York.

Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. 2011. "Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model," *Decision Support Systems* (51:3), pp 576-586.

Wang, J., Chen, R., Herath, T., and Rao, H. R. 2009. "An Exploration of the Design Features of Phishing Attacks," *Information Assurance, Security and Privacy Services* (4), p 29.

Wright, R., Chakraborty, S., Basoglu, A., and Marett, K. 2009. "Where Did They Go Right? Understanding the Deception in Phishing Communications," *Group Decision and Negotiation* (19:4), pp 391-416.

COPYRIGHT