Cultural impact on Users' Ability to protect themselves against Phishing websites

Ibrahim Mohammed Alseadoon1†, Rabie A. Ramadan2†† and Ahmed Y. Khedr3†††,

Hail University, Hail, Saudi Arabia

Summary
Phishing websites are well designed to steal important and sensitive information from Internet users. Especially those users, who are not cautious in using the Internet, are more vulnerable to phishing websites. Mostly, phishing websites and emails are well designed to lure Internet users into believing their authenticity. Quantitative and experimental methods are used to collect and examine cultural factors which make users better protected against phishing websites. The results show that language, surfing duration, and security measures are significantly affecting users' ability to protect themselves from phishing websites.

Keywords:
Phishing, behavior, scam, culture, impact, websites, emails, vulnerability.

1. Introduction

Phishing websites are designed to gain users' trust to steal their important information. One phishing attack, that targets almost 2 million users of a major store in the United States, results in gaining confidential information from users [1]. The number of phishing attacks is enormous. An estimation of the number of attacks can reach 156 million per day [2]. A high number of phishing attacks will in final result in tripping users into their traps. Therefore, organizations have employed security software and measures to prevent users from falling into these attacks. Despite the implemented technology, phishing attacks always find their ways to users. Then, the decision of fall to these traps or not will be depending on the users.
Our study will focus on users' ability to protect themselves from phishing attacks. In addition, to the best of our knowledge, phishing attack studies are mainly focused on users who have western culture. Fewer studies have been focused on users who come from different cultures and the impact of culture on detection. In the Middle East, for example, and particularly in Saudi Arabia users have a different culture than western culture [3]. One of the cultural issues is that most of the security procedures for securing websites and e-mails are developed and presented in English. Where in Saudi Arabia the main language is Arabic and not all users are familiar with the English language. For example, web certificate which identifies websites is presented in the English language. Warning and other security messages are shown in English as well. Additionally, trust behavior will be different towards others on specific websites. For example, a phishing attack which imitates trustworthy website in a certain country will not have the same impact on another country. Also, cultural differences such as power distance which is related to obeying high-rank authority might have an effect on users behavior with a phishing attack. The question is what would be the behavior of these users if the phishing emails impersonate officials of government agencies.

The organization of this paper is as follows: the next section involves the designed survey and modeling; section 3 shows the number and type of participants; the study experiment is explained in section 4; followed by discussion in section 5; finally the conclusion in section 6.

2. Survey and Modeling

Self-reporting method is used in our questionnaire with 5 points Likert scale [4]. To avoid biased towards positive answers, our study adopts anonymity for respondents. Anonymity has also the advantage in making users be comfortable in answering sensitive questions.

The theory of detection proposed by [5], [6], [7] is adopted. The theory of detection indicates that users are able to detect deception by noticing certain cues in received messages from others. In conversation, a detector is observing the other person voice tone body language and face impression searching for cues which can confirm or deny the authenticity of the message. For example, avoiding eye contact while answering certain questions can be a cue of deceptive message [8]. In phishing websites, there are special cues which can lead to detecting deception. For example, phishing websites have domain names (URLs) similar to trusted websites domains. Detection can be obtained by observing mistakes in URLs. However, most of the deception cues which can reveal the identity of phishing websites are proposed and developed in a certain culture. In particular, the English language is the main language used to develop and improve security measures. For other culture which the English language is

Manuscript received November 5, 2017
Manuscript revised November 20, 2017

not the main language such as Saudi Arabia can develop an obstacle for users to identify phishing websites and emails.

Up to our knowledge, not all Saudis are fluent in the English language. The goal of our study is to find the impact of using existence security measure in other culture (Saudi Arabia in particular). To measure the impact of culture, participants were first asked to state their level of English Language. In addition, other factors have been included in our model to find their impact. Gender, awareness about security measures, secure website, protection procedures, and number of hours spent on the Internet and online banking, security practices, Trust, and email richness are also measured in our model. The following subsections will explain the reasons behind choosing previously mentioned factors.

2.1 Gender

Gender is suggested to affect users' ability to detect phishing websites [9]. In particular, females are more trusting and vulnerable to phishing websites than males. The reason for females' vulnerability contributes to three factors: (1) females have less knowledge about security procedures. (2) Females are more susceptible than males. (3) Females are more welling towards trust. Therefore, we developed the first hypothesis as follows:

H1: gender differences affect users' ability to protect themselves from phishing websites

2.2 English Language

The English language has an enormous impact on identifying phishing websites signs. Security measures are mainly presented in the English language. Furthermore, attention to deceptive cues and understanding their meaning is a key factor in detecting phishing websites [10]. Our study suggests that users with high with English language knowledge will be less susceptible to phishing websites.

H2: The English language increases users' ability to protect themselves from phishing websites

2.3 Awareness about Security Measures

Participants were asked about their security measures awareness. High awareness about security measures is expected to reflect on users' behavior with the website. Users who know how to evaluate websites are more likely to be careful in providing their sensitive information to, however, claim them. Users who are aware of the best practice in protecting themselves from attacks are more expected to be more cautious than others. Therefore, users who have high awareness are more likely to be better than fewer awareness users.

H3: Awareness about security increases users' ability to protect themselves from phishing websites

2.4 Protection Procedure

Protection procedures are measured with 4 items. Each item asks participants about their agreement to some protection procedures such as using letters and numbers in passwords and installing security software. Our study is interested in finding the impact of protection procedures in users' ability to detect phishing websites.

H4: protections procedures increase users' ability to protect themselves from phishing websites

2.5 Number of hours spent on the Internet and online banking

A number of hours spent on the internet were measured with 1 item as well as online banking. Experience is measured with 1 item. It is proposed that users who spend more time exploring the internet are more likely to develop an experience. Experience has the benefit of developing a baseline which helps users compare between websites. Where users who spent less time may not be able to distinguish between websites. Users would not know if the current website is odd or normal. Additionally, performing online banking on the internet is expected to give users a better-advanced knowledge than other. Since it involves vital aspect which directly deals with a monetary aspect. Making mistake in online banking has the result of losing money. Users who perform online banking do not have the intention of losing money.

H5: high Surfing time increases users' ability to protect themselves from phishing websites

H6: conducting online banking increases users' ability to protect themselves from phishing websites

2.6 Security practices

Participants were asked to acknowledge if they examine website URL, certificate, and padlock icon. The reason behind asking security practices questions is to know the impact of performing these security practices on identifying phishing websites. Security practices were measured with 3 items.

H7: security practices increase users' ability to protect themselves from phishing websites

2.7 Trust

Phishing which is social engineering act is based on exploiting trust. Phishing websites are exploiting the trust that is given to certain websites to lure users providing sensitive information. Phishing websites are well designed to imitate trustworthy websites. However, phishing

websites include information that can reveal their identities such as different URL and certificate. Users, who are tenderer to trust, will not be careful in examining these cues. Users habit of trust makes users examine fewer cues or deceived by deceptive cues. Trust is measured using Mcknight measure which consists of 3 items [11].

H8: trust increases users' ability to protect themselves from phishing websites

2.8 Email richness

Phishing websites are harmless until users are connected to them. The main method used to drive victims to phish websites is emails. Phishing emails are cautiously designed to hide deception. To identify deception, there is a need for high attention from users to minimal information in phishing emails. Users who consider email as a high rich medium are expected to be able to extract certain information. For example, phishing emails include suspicious links to websites. Examining these links will reveal the deception carried on phishing emails. Email richness was measured to find its impact on users' ability to detect deception carried in phishing emails. Email richness measures users' ability to deal with email as a rich medium. Email richness was measured with 4 items [12].

H9: email richness increases users' ability to protect themselves from phishing websites

2.9 Websites

Participants were examined with trustworthy websites as well as phishing websites. The examination came in a form of image shown to participants. Participants were asked to rate their likelihood to trust shown websites. Some websites are well known and trustworthy websites in Saudi Arabia and the other are phishing websites. Participants can perform detection on this website such as examining URL and the existence of padlock.

3. Phishing experiment

After collecting information from users about their ability to identify websites, it was time to send an actual phishing email. Participants were not informed about the act of sending phishing email beforehand. The reason laid behind not disclosing the sending of phishing email to participants is to obtain a real behavior. If participants were informed about the intention of sending a phishing email, it will have an effect on the results validity. If participants knew about the phishing mail, there will be a negative impact on the results. The negative impact is that participants will raise their level of suspicion in their email account. Participants might inspect every email they will receive hoping to identify the phishing email. Therefore, to obtain a valid and real behavior about phishing email from participants, the act of sending a phishing email was kept hidden from participants until the end of the experiment.

3.1 Participants

Participants are bachelor students majored in computer studies. The main reason for choosing bachelor students is because younger users are more susceptible to phishing attacks than older users [9]. High susceptibility exists because younger users are more willing to take risks than older users who make a mature decision. 200 students were reached to fill in the survey. 134 respondents were accepted after filtering data from mistakes and incomplete survey. Participants demographic include both genders from male and female.

4. Results

From the experiment, nearly 80 percent of participants opened the phishing email. Majority of participants fall for the experiment phishing email which means that users who opened the phishing email are victims. Considering that some phishing emails can install malicious software to victims' devices just by opening these phishing emails. Additionally, from 80 percent of victims opened the phishing emails, only 20 percent clicked on the link embedded in the phishing email. Our study findings suggest that participants examine emails authenticity after opening emails. The examination behaviour can be denoted to participants' culture such as language and behaviour. The following sections present the results obtained from the questionnaire. The analysis was carried out using SPSS software version number 23.

4.1 Descriptive outcomes

The number of male participants is 87 (68%). Where the number of female participants is 47 (35%). The number of employee participants is 51 (38%). The number of students' participants is 83 (62%). Number of years practicing English language has been divided into five categories (less than 3 years, above 3 to 6, above 6 to 9, above 9 to 12, and more than 12 years) each category has received 14 (10%), 25 (19%), 31 (23%), 32 (24%), and 32 (24%) respectively. Participants were asked to rate their level of English language. The level was measured using 5 points Likert scale. Majority of participants reported that they fit in the middle neither expert nor learner. The mean value for the rest of the factors are shown in brackets; awareness about security measures (4.4), websites (4.1), protection procedures (4.3), number of hours spent on the Internet (2.9) and online banking (2), security practices (3.4), trust (3.4), and email richness (3.5).

4.2 Analysis

Reliability was measured by applying Hair et al. measure [13]. Factors should gain 0.7 to match the cut-off measure. Factors that did not match the cut-off are eliminated from the model. Then, factor analysis was conducted to measure factors validity.
After obtaining factors validity, linear regression was applied to measure the relationship between independent factors (model factors except for websites) and dependent factor (websites). The first step in linear regression was testing each independent factor with the dependent factor. Only those factors that showed significant impact are entered into the final model. Then, the final model was tested with only significant independent factors with the dependent factor. The results of the test are presented in table 1 and 2.

Table 1: Beta and P-value

Factors	*Beta*	*P-value*
English knowledge	0.273	0.001
Hours in the Internet	0.235	0.004
Security practices	0.154	0.055

Table 1 shows that there are three factors affecting users' ability to protect themselves from phishing websites. Users who have high knowledge in the English language, spending more time on the Internet, and perform security practices are better protected than others.

Table 2: R Square

Model	*R*	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*
1	0.424a	0.180	0.161	0.87112

Table 2 shows that our model explains nearly 20 percent of the variance in the data (see table 2). Finding that our model explains only 20 percent means that there is a need for further research to find other main factors which can affect users' ability to protect themselves from phishing websites.

5. Discussion

Our findings suggest that users who have high knowledge in English are better able to identify phishing websites. Victims have been found to be classified as beginners in the English language. Therefore, the English language plays an important factor in distinguishing victims from detectors. The English language is a vital factor in detections since most phishing websites, as well as emails, suffer from spelling mistakes. Additionally, security measures are presented in English. Therefore, our study suggests that for organization protection, there is a need to improve their employee English language skills.

A high number of hours spent on surfing the Internet has been found to have a significant impact on users becoming detectors. Spending enormous amount of time on the Internet has the benefit of increase users' experience. The experience can be built by comparing websites between each other. Users can be encountered with different websites (trust or deceptive websites) which will gradually build a baseline for users to compare. For example, some trust websites encourage their users to reveal their identity by examining website certificate or existence of HTTPS in URLs. Building these security habits for users will make them doubt websites which do not provide similar signs. Therefore, our study suggests that organization can improve their employees' protection by exposing them to more trustworthy websites and encourage them to validate these website identities.

Security practices have been found in our research to significantly improve users' ability to detect phishing websites. Users were asked to acknowledge their security behavior in validating websites. The reasons behind asking these questions are: (1) knowing whether users take websites security measures seriously or not, (2) finding whether users understand the meaning of these security measures. Our findings suggest that users do not consider security measures seriously important. Participants rated their answer slightly above the middle with a score of (3.4). However, the existence of these security measures showed significant impact on users' ability to detect phishing websites. The existence of security measures gives users a sense of validity to websites that provide them.
Culture plays an important role in differentiating between users as we found in our study that 80 percent of the participants opened the phishing email. While, the expected percentage of victims of phishing emails in an experimental situation is enormously lower than our study percentage victims [14, 15]. It might be suggested that the culture difference in power distance may play an important role in making users become victims. The reason can be related to the design of the phishing email as it focuses on users who are students in the impersonated university. In addition, other factors need more investigation.

6. Conclusion

To the best of our knowledge, users' culture and background have not been introduced in users' ability to detect phishing websites. In detection, there are certain behaviors which users should perform to identify phishing websites. For example, users should check websites URLs

and certificates which provided in the English language. Additionally, trust on certain websites or scenarios can be perceived differently across cultures. For example, phishing email which pretends to provide users with American green card is different than a phishing email pretends to win the lottery prize. The way of written argument and the provided prize will be received differently. Therefore, culture and beliefs can affect users way of judgment. In our study, we found that the English language plays a significant role in detection. High numbers of hours spent on the Internet as well as performing security checks in websites are increasing users' ability to detect phishing websites. Culture is a major player in the process of detection.

Acknowledgements

Many thanks go to the Research Deanship at the University of Hail for sponsoring and supporting our study. Thanks also to all participants who spear their valuable time to answer our study questionnaire and participate in our research experiment.

References

[1] Dave, P. Email 'phishing' attacks by hackers growing in number, intensity <http://articles.latimes.com/2013/jul/25/business/la-fi-phishing-attacks-20130726>. 2013 [cited 2016].
[2] Safe, G.C. Phishing: How many take the bait? <http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx>. 2015 [cited 2016 21-3-].
[3] Hofstede, G. and M.H. Bond, Hofstede's culture dimensions an independent validation using Rokeach's value survey. Journal of cross-cultural psychology, 1984. 15(4): p. 417-433.
[4] Likert, R., A technique for the measurement of attitudes. Archives of psychology, 1932.
[5] Johnson, P.E., et al., Success and failure in expert reasoning. Organizational Behavior and Human Decision Processes, 1992. 53(2): p. 173-203.
[6] Johnson, P.E., S. Grazioli, and K. Jamal, Fraud detection: Intentionality and deception in cognition. Accounting, Organizations and Society, 1993. 18(5): p. 467-488.
[7] Johnson, P.E., et al., Detecting deception: adversarial problem-solving in a low base-rate world. Cognitive Science, 2001. 25(3): p. 355-392.
[8] Anderson, M., Nonverbal communication. 1987.
[9] Sheng, S., et al. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2010. ACM.
[10] Mannan, M. and P.C. van Oorschot. Security and usability: the gap in real-world online banking. in Proceedings of the 2007 Workshop on New Security Paradigms. 2008. ACM.
[11] McKnight, H., C. Kacmar, and V. Choudhury. Whoops... did I use the wrong concept to predict e-commerce trust? modeling the risk-related effects of trust versus distrust concepts. in System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on. 2003. IEEE.
[12] Carlson, J.R. and R.W. Zmud, Channel expansion theory and the experiential nature of media richness perceptions. Academy of management journal, 1999. 42(2): p. 153-170.
[13] Hair, J.F., et al., Multivariate Data Analysis. 2009.
[14] Sheng, S., et al. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. in Proceedings of the 3rd symposium on Usable privacy and security. 2007. ACM.
[15] Zhang, W., et al. How could I fall for that? Exploring phishing victimization with the heuristic-systematic model. in System Science (HICSS), 2012 45th Hawaii International Conference on. 2012. IEEE.

Ibrahim Mohammed Alseadoon received his Masters from University of Wollongong (UOW), Wollongong, NSW, Australia in 2008 and PhD from Queensland University of Technology (QUT), Brisbane, QLD, Australia in 2014. He is currently an assistant professor at University of Hail, Hail, KSA. He is an author of more than 5 articles in the field of Computer Security and Users Behaviour. He served as general chair and program committee chair for several conferences. In addition, he served as the co-chair of the International Conference on Recent Advances in Computer Systems (RACS-2015) and The 2nd National Computing Colleges Conference (NC3 2017) held at University of Hail.

Rabie A. Ramadan received his Masters and PhD from Southern Methodist University (SMU), Dallas, Texas, USA in 2005 and 2007, respectively. He is currently an associate professor at Cairo University, Cairo Egypt and Hail University, Hail, KSA. He is an author of more than 120 articles in the field of Blended learning, IoT, Computational Intelligence, Sensor Networks, and Brain Computer Interface. He served as general chair, program committee chair, and TPC for many of the conferences and journals. In addition, he served as the co-chair of the International Conference on Recent Advances in Computer Systems (RACS-2015) and The 2nd National Computing Colleges Conference (NC3 2017) held at Hail University He is also a co-founder of IEEE Computational Intelligence, Egypt Chapter.

Ahmed Y. Khedr is an associate professor at Systems and Computer Engineering in Al-Azhar University, Cairo, Egypt. Ahmed is working now in Computer Science and Engineering in Hail University, Hail, Saudi Arabia. Ahmed was funded by the Egyptian government to visit SMU at USA and conduct research in Mobile Computing with the PDA Mobile research group. Ahmed's research area is focused on wireless sensor networks, cloud computing, big data, and e-learning algorithms.