Does Awareness of Social Engineering Make Employees More Secure?

Hussain Aldawood
School of Electrical Engineering and Computing
University of Newcastle
Newcastle, Australia

Tawfiq Alashoor
Mendoza College of Business
University of Notre Dame
Notre Dame, IN, USA
KFUPM Business School[2]
King Fahd University of Petroleum and Minerals
Dhahran, Saudi Arabia

Geoffrey Skinner
School of Electrical Engineering and Computing
University of Newcastle
Newcastle, Australia

ABSTRACT
Social engineering has become one of the biggest security threats facing organizations. Rather than relying upon information security technical-related shortcomings to break into computer networks, social engineers make use of employees' individual and organizational traits to deceive them. In such a scenario, it is crucial for organizations to ensure that their employees not only possess sound knowledge about information security but also about the concept of social engineering and threats emerging from social engineering attacks. This study aims to test whether awareness of social engineering can predict and explain individuals' security-protective practices. We conducted a survey of 265 employees working in different organizations in Saudi Arabia. The results suggest that awareness of social engineering is a positive predictor of security-protective practices above and beyond the predictability power of possessing information security knowledge. Thus, to reduce the probability of potential consequences of social engineering attacks, our study suggests that organizations should not only strive to enhance employees' security knowledge but should also invest in increasing employees' awareness of social engineering.

General Terms
Social Engineering Awareness

Keywords
Cyber Security, Information Security, Social Engineering, Social Engineering Attacks, Social Engineering Awareness, Information Security Awareness, Security Awareness Programs. Information Security Awareness Programs.

1. INTRODUCTION
As civilization evolves and becomes increasingly connected through modern technology, the security of data has become a crucial concern. Cybercrime, which takes place on a computer, has become a major threat for individuals, societies, and the economy, and it is even recognized among primary sources of terrorism (i.e., cyberterrorism). Attacks against businesses have become so resolute that the modern society is incapable of responding to the sheer volume of attacks. In fact, in the year 2016 in an Internet-organized crime threat assessment, it was found that for some European countries, cybercrimes surpassed traditional crimes [1].

Most of the astute criminals have shifted to social engineering as their primary attack vector instead of automated exploits. These attackers are knowledgeable about human flaws and induce the victims to negligently create vulnerabilities. In all attack vectors, attackers use social engineering in order to manipulate people, infect information systems, steal credentials and transfer data [2]. Social engineering is defined as a non-technical method that relies heavily on human interactions and involves tricking people and manipulating them into breaking normal security procedures [3]. Such threats are challenging as they depend on human behavior and take advantage of vulnerable employees [4]. Thus, businesses today should utilize various strategies to improve employees' awareness of social engineering threats and attacks in order to protect their intellectual properties including information assets.

It has been widely accepted that awareness is one of the most important aspects of information security [5, 6]. People using the most secure systems are also often the most vulnerable to social engineering attacks [7]. Employees sometimes ignore time-consuming security procedures in an effort to complete work tasks more quickly. Staff is the most common target of social engineering attackers, as they have access to critical organizational systems.

While social engineering relies on human behavior, attackers mainly focus on the psychological instinct of the victims [8]. The success of manipulating employees is generally achieved by establishing a relationship with the victims, trying to build trust. The victims then release some sensitive information as a result of the trust factor. This form of crime can be further classified into piggybacking, tailgating and telephone phishing (vishing). However, in the case of computer-based social engineering, attackers rely on computer systems or their technological mode of operation such as phishing, fake email, and pop up window attacks [9]. In the last decades, several high-profile cases of social engineering have been recorded. Such attacks have resulted in millions of passwords being leaked. Some of the major victims are global tech giants including Yahoo!, Dropbox, LinkedIn, Facebook, Google, Weebly, MySpace, and many others.

Given the fact that social engineering threats are dynamic and constantly evolving, developing a mitigation strategy becomes a top priority for organizations, including training employees to counter such attacks [7, 10]. This countermeasure includes testing their level of awareness of social engineering from time to time [11, 12]. On the other hand, in order to bolster physical security, measures such as CCTV (closed circuit television) footage supported by clearly defined human parameters, security alarms, motion detectors, and biometrics

have been considered to minimize social engineering threats [12].

Social engineering attacks cost corporations billions of dollars in losses ever year. Due to the ever-changing dynamics in today's information technology world, it has become crucial for managers and employees to be completely aware of their company's security policies and procedures. Also, it is essential for organizations to have a defined set of security rules for attaining maximum efficacy. In addition to protecting companies from attackers, one of the greatest benefits of enforcing security policies is the protection from potential lawsuits that may arise in case of attacks and crack downs from the local authorities [7].

When trying to evaluate human behavior towards online threats, it is crucial to identify the human factors related to those threats. According to the existing literature, demographic factors, Internet use, and security knowledge have been found as some of the major determinants associated with social engineering attacks [13, 14].

Age. According to [13], young Internet users are more susceptible to phishing or social engineering attacks. Similar findings were concluded by Airehrour et al. [14], who stated that people in the age group 28-38 years are less vulnerable to social engineering attacks.

Gender. According to [15], females are more susceptible to social engineering attacks than males because they are more open towards social media usage and are more likely to reply to junk advertisements. Algarni et al. [16] found a significant relationship between gender and susceptibility to social engineering in a study conducted on Facebook users. They recommend that organizations should take this factor into consideration when hiring an employee, particularly in a position of responsibility.

Education Level. Some researchers have identified a relationship between education level and susceptibility to social engineering attacks. This includes the study of [16], wherein the authors found a significant correlation between the two factors, such that those who have a higher level of education are less susceptible to social engineering attacks. However, contradictory findings have been found by Sheng et al. [17] who concluded in their study that education level is not related to social engineering susceptibility.

Internet Use. Iuga et al. [18] assert that excessive Internet usage causes users to be overly confident, leading to risky security behaviors. According to their empirical evidence, experienced and heavy Internet users end up being more susceptible to social engineering attacks because they tend to adopt weak security measures (e.g., transacting with unsecured websites). Snyder [12] argues that we are living in the Internet era with a growing dependence on the Internet. This high dependence on Internet exposes people to different kinds of cybercrimes. We all use the Internet in education, business, healthcare, etc., but Internet experience does not necessarily make us aware of how such crimes work, especially when it comes to social engineering psychological tricks. In another study, Hadlington [19] found that individuals who have high Internet experience are much more susceptible to social engineering attacks as compared to those who are not. Thus, such findings confirm that Internet use or experience may have a negative impact on security practices and hence a higher susceptibility to social engineering attacks. Similar findings have been reported in [12].

Security Knowledge. Users acquire security knowledge through education and experience. Kumar et al. [3] argues that educating employees about information security is extremely important for protecting organizational information assets. In order to be effective, all security policies, procedures and standards must be taught and reinforced to all employees. Education should be an ongoing process. It is not sufficient to publish policies and expect employees to read and understand them. Rather, employees need to be taught why security is important and how security education will help them avoid costly consequences at both the individual and organizational level. The authors suggest several other methods that can be used to keep employees informed and conscious at all times [3]. Past experience is another important factor through which users can enhance their security knowledge. Parrish et al. [20] propose a model showcasing experience as a factor that affects an Internet user's judgment. Albladi and Weir [13] concluded that significant experience in the field of information security impacts an Internet user's chances of being a victim of social engineering attacks. By 'past experiences' the authors refer to previous incidents faced by the users in which they had been victims of any kind of social engineering attacks such as phishing or identity theft. In short, security knowledge is a crucial determinant of security behaviors and acquiring solid security knowledge is therefore a significant antecedent of protection against social engineering attacks.

Security-Protective Practices. One of the most important factors that can impact employees' susceptibility to social engineering attacks is their security practices (e.g., enabling firewalls, installing anti-virus, checking credentials of the email sender, etc.). Abdalla and Abass [21] found that in order for organizations to protect their systems and employees from social engineering attacks, employees should be educated about safe computer behaviors. As employees learn about secured practices (e.g., not clicking on a link received from an unknown source, refusing to disclose sensitive information, etc.), organizations are less susceptible to social engineering attacks. This factor represents the most important behavioral outcome in the domain of social engineering as it represents the technical and psychological loophole that can be exploited by social engineers to attack organizations. Therefore, organizations should invest in enhancing employees' security practices by educating them about best security practices [22].

Next, we present our study in which we aim to predict security-protective practices, which represent a significant proxy for estimating the susceptibility of employees to social engineering attacks. In other words, if employees pursue unsecured (secured) practices, the organization is more (less) susceptible to social engineering attacks. Based on the above discussion, we predict that demographic factors (i.e., age, gender, and education) and Internet use will be associated with security-protective practices. We do not state the direction of these associations given the mixed results from the literature. With respect to security knowledge, there seems to be a consensus that higher security knowledge is positively associated with security-protective practices. Therefore, we predict that employees who have high (less) security knowledge are more (less) likely to utilize security-protective practices. Last, we aim to answer a practically important question: Does awareness of social engineering relate to security-protective practices? The literature is limited as to whether or not awareness of social engineering is a significant predictor of security practices. Indeed, the literature asserts that security knowledge is important. However, we argue that awareness of social engineering can predict and explain

security practices above and beyond security knowledge. We propose that employees who are aware of social engineering are more likely to adopt secured practices, whereas those who do not know the meaning of social engineering and are not aware of social engineering threats will more likely adopt unsecured practices that could potentially put the whole organization at risk. Based on this discussion, we posit the following hypotheses:

Hypothesis 1 (H1): *Security knowledge will be positively associated with security-protective practices.*

Hypothesis 2 (H2): *Awareness of social engineering will be positively associated with security-protective practices.*

Hypothesis 3 (H3): *Frequency of Internet use will be associated with security-protective practices.*

Hypothesis 4 (H4a, b, c): *Demographics [a. age, b. gender, and c. education) will be associated with security-protective practices.*

2. METHODOLOGY

In order to test our hypotheses, a primary study using a survey method was conducted with employees working for various organizations in Saudi Arabia. A closed-ended online questionnaire was administered, and it included a list of questions to measure security knowledge, awareness of social engineering, security-protective practice, Internet use, age, gender, and education. The link to the questionnaire was sent to a list of participants on various social media platforms such as Facebook, Twitter and LinkedIn. After removing responses with missing values, a total of 265 responses constituted our final sample.

3. MEASUREMENTS

Security knowledge was measured using four items on a scale from 1 strongly disagree to 5 strongly agree ("*all passwords that are 5 letters long are safe enough*," "*it is okay to download files from any website as long as it is not demanding money*," "*as long as your antivirus is up-to-date, your computer can't be attacked in any way*," and "*it is not important to update your antivirus regularly because it is only a means for the company to make more money*." These items were reverse coded before creating a mean score (α = .779). Therefore, a high score on this variable indicates high-security knowledge. Awareness of social engineering was measured using two items ("*are you familiar with the meaning of social engineering*?" and "*are you aware of the threats caused by social engineering*?" A composite score ranging from 0 to 2 was created by summing the responses from the original two items (0 = no and 1 = yes). Therefore, a total of 0 indicates low awareness, a total of 1 indicates moderate awareness, and a total of 2 indicates high awareness. Security practices were measured using seven items (e.g., "*is the current firewall on your computer enabled*?" "*do you check the sender's credentials before opening an email*?" "*is there an anti-virus currently installed on your computer*?" "*Have you used your credit cards at unsecured websites*?" This last item was reverse coded). A composite score was created by summing the responses from the original seven items (0 = no and 1 = yes). The composite score ranged from 0 indicating unprotective security practice to 7 indicating protective security practice. Internet use was measured using one item ("*on an average day, how often do you use the Internet*? *1 hour or less, 2-3 hours, 4-5 hours, 6-8 hours, 8 hours or more*). Table 1 presents the demographics and 2 presents the descriptive statistics of our main variables.

Table 1. Demographics (N = 265)

	Frequency	Percent
Internet Use		
Minimal (1 hour or less)	5	1.9
Average (2-3 hours)	45	17.0
Frequent (4-5 hours)	98	37.0
Heavy (6-8 hours)	70	26.4
Constant (8 hours or more)	47	17.7
Age		
Below 20	9	3.4
21-30 years	82	30.9
31-40 years	131	49.4
41-50 years	20	7.5
Above 50 years	23	8.7
Gender		
Male	221	83.4
Female	44	16.6
Education		
Below high school	17	6.4
High school	96	36.2
Undergraduate	122	46.0
Postgraduate	23	8.7
Doctorate	7	2.6

Table 2. Descriptive Statistics (N = 265)

	Security Knowledge	Awareness of SE	Security-Protective Practices
Mean	2.3528	.9245	1.8717
S.D.	.93973	.93438	1.53203
Minimum	1.00	.00	.00
Maximum	5.00	2.00	7.00

4. DATA ANALYSIS AND HYPOTHESIS TESTING

Table 3 presents the correlation matrix. It shows evidence of a moderate positive correlation between our outcome variable (i.e., security-protective practices) and both security knowledge (r = .418**) and awareness of social engineering (r = .300**). There is also a positive correlation between security knowledge and awareness of social engineering (r = .261**) which is expected in a theoretical sense. The demographic variables do not correlate significantly with any of the security-related variables. Internet use is negatively correlated with awareness of social engineering (r = -.173**) which indicates that users who use the Internet more frequently are less likely to be aware of social engineering

threats, which supports previous findings [18, 19]. This is interesting, as theory would suggest that experience with Internet is positively associated with awareness of social engineering. Nevertheless, this correlation could also mean that users who are aware of social engineering tend to use the Internet less frequently to avoid risky consequences emerging from prevalent social engineering practices. Next, we present a regression analysis to test the impact of security knowledge, awareness of social engineering, Internet use, and demographics on security-protective practices.

Table 3. Correlation Matrix

	1	2	3	4	5	6	7
1. Protective Security Practice	1						
2. Security Knowledge	.418**	1					
3. Awareness of Social Engineering	.300**	.261**	1				
4. Internet Use	-.029	-.024	-.173**	1			
5. Age	-.097	.013	-.038	-.100	1		
6 Education	-.056	-.046	-.064	.054	.124*	1	
7. Gender (male = 0, female = 1)	.077	.021	.047	-.060	-.169**	.213**	1

* $p < .05$; ** $p < .01$; *** $p < .001$

Table 4 shows the results of the regression analysis. We ran two models (i.e., Model 1 and Model 2) in order to test whether awareness of social engineering can predict and explain security-protective practices above and beyond security knowledge. The results as indicated in Table 4 support this claim. Model 2 shows that both security knowledge and awareness of social engineering are significantly associated with security-protective practices. More importantly, the explanatory power of Model 2 improved significantly as indicated by the positive change in R^2. The change in R^2 between the two models is significant ($p < .001$). Also, the effect size of security knowledge in Model 1 ($\beta = 678$, $p < .001$) decreased after adding awareness of social engineering in Model 2 ($\beta = 595$, $p < .001$). This suggests that awareness of social engineering contributed significantly to explaining security-protective practices above and beyond security knowledge. Therefore, we rely on Model 2 to test our hypotheses.

The results indicate that employees who have high security knowledge are more likely to pursue protective security behaviors ($\beta = 595$, $p < .001$). Therefore, H1 is supported. In addition, employees who are aware of social engineering are also more likely to pursue protective security practices ($\beta = 326$, $p < .01$). This provides support for H2. The results suggest that none of the other hypotheses pertaining to Internet use (H3) and the demographic variables (H4a, b, c) are supported. Therefore, we found no support for the impact of Internet use, age, education or gender on security-protective practices. These findings add to our knowledge of security practices. Next we conclude with practical implications

Table 4. Ordinary Least Square (OLS) Regression

	Model 1	Model 2
	β $(robust\ s.e.)$	β $(robust\ s.e.)$
$Constant$	.961+ (.568)	.602 (.599)
$Security\ Knowledge$ **(H1)**	.678*** (.104)	.595*** (.108)
$Awareness\ of\ SE$**(H2)**	-	.326** (.103)
$Internet\ Use$ **(H3)**	-.033 (.090)	.016 (.092)
Age **(H4a)**	-.149+ (.085)	-.133 (.086)
$Female$ **(H4b)**	.245 (.216)	.218 (.212)
$Education$ **(H4c)**	-.069 (.103)	-.053 (.101)
$F\ value$	(5, 259) 12.16***	(6, 258) 11.70***
R^2 $(Adjusted\ R^2)$	19.02% (17.45%)	22.59% (20.78%)
N	265	265

+ $p < .10$; * $p < .05$; ** $p < .01$; *** $p < .001$

Dependent Variable: Security-Protective Practices

5. CONCLUSION

The growing usage of digital technology and the Internet have increased the number of risks inherent in information sharing. A total dependence on the World Wide Web is dominating the world today, a fact that is exploited by social engineers every day. The old-fashioned techniques of data theft used by attackers have now been replaced by more sophisticated methods. These methods are not only easier, but also yield results much faster and more effectively as they rely on the human psychology. Additionally, these types of manipulation methods allow attackers to gain access to any information system, irrespective of the platform, software or the technology involved.

Social engineering crimes practiced by attackers are not only aided by necessary technical knowledge, but also by exploitation of human vulnerabilities. In this case, it becomes important that employees possess complete knowledge about the concept of social engineering. Our study, in this respect, focused on factors that can significantly affect employees' security practices, which represent a significant predictor of the susceptibility of employees to fall prey to social engineers. We found that both security knowledge and awareness of social engineering and its threats are significant determinants of security practices. Therefore, organizations should increase employees' awareness of social engineering to avoid the detrimental potential threats of social engineering attacks. The current organizational practices of educating employees about security measures, security policies, and other security concepts need to be accompanied by making employees aware of social engineers. For instance, organizations should deliver interactive lectures to inform employees about the characteristics of and the techniques used by social engineers. Of course, there is no foolproof way to protect oneself against social engineering attacks, no matter what controls are implemented, due to the presence of the human factor. However, there are certain measures that can possibly affect the chances of success of such attacks. Thus, it becomes important for organizations to establish clear and strong security policies that can potentially reduce the threats of social engineering. The steps which are necessary while

designing defensive practices against social engineering include a proper security management framework, defining a set of goals regarding the security plan and its implementation, and finally, periodic risk assessments. Threats do not necessarily represent the same level of intensity for different organizations, so there should be a review of risks of social engineering threats and the danger should be rationalized according to the organization type.

This study has some limitations. Firstly, the field of social engineering is constantly evolving. The tactics applied to solve the problem are limited but new ones are slowly emerging, which have not been covered in this study. Specific models of social engineering attacks can be studied in isolation so that remedial measures can be recommended to organizations to help them support business continuity. In addition, the views of the management were not taken into consideration while comparing employees' level of awareness to the security practices that are applied in organizations. Moreover, our participants were mostly males and covered mainly two groups of education level. We focused on security knowledge and awareness of social engineering as the main determinants of security-protective practices. Future research is needed to examine other factors that can predict security practices (e.g., self-efficacy, security and privacy concerns, etc.). Research in this field can further be extended to the phenomenon of reverse social engineering, as this field has not been widely reported in the online context. This is particularly necessary, as reverse social engineering allows attackers to bypass the behavioral detection techniques, thus making attacks easier.

6. ACKNOWLEDGMENT

The first author would like to acknowledge the full scholarship from the Saudi Ministry of Education to study a PhD degree in the Faculty of Engineering and Built Environment at the University of Newcastle, Australia.

This research was partially supported by GulfNet Solutions (GNS) Company Limited. We are thankful to our colleagues in GNS Cyber Security Division, who provided expertise that greatly assisted the research. We have to express out appreciation to Mr. Omar Aldulaijan, GNS General Manager, for sharing his pearls of wisdom with us during the course of this research.

7. REFERENCES

[1] Breda, F., Barbosa, H. and Morais, T. Social engineering and cyber security. City, 2017.

[2] Salahdine, F. and Kaabouch, N. Social Engineering Attacks: A Survey. Future Internet, 11, 4 (2019), 89.

[3] Kumar, A., Chaudhary, M. and Kumar, N. Social engineering threats and awareness: a survey. European Journal of Advances in Engineering and Technology, 2, 11 (2015), 15-19.

[4] Aldawood, H. and Skinner, G. Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. International Journal of Security (IJS), 10, 1 (2019), 1.

[5] Chan, H. and Mubarak, S. Significance of information security awareness in the higher education sector. International Journal of Computer Applications, 60, 10 (2012).

[6] Yunos, Z., Ab Hamid, R. S. and Ahmad, M. Development of a cyber security awareness strategy using focus group discussion. IEEE, City, 2016.

[7] Aldawood, H. and Skinner, G. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet, 11, 3 (2019), 73.

[8] Ahmad, S. Social Engineering Techniques Contrast Study. International Journal of Engineering, 9, 1 (2017), 105-110.

[9] C, A., Adesegun, O., Y.A, A. and Oludele, A. Social Engineering Attack Awareness : Case Study of a Private University in Nigeria, 2013.

[10] Aldawood, H. and Skinner, G. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. City, 2018.

[11] Daimi, K. Computer and Network Security Essentials, 2017.

[12] Snyder, C. Handling human hacking: creating a comprehensive defensive strategy against modern social engineering (2015).

[13] Albladi, S. M. and Weir, G. R. User characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences, 8, 1 (2018), 5.

[14] Airehrour, D., Vasudevan Nair, N. and Madanian, S. Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. Information, 9, 5 (2018), 110.

[15] Team, C. I. T. Unintentional insider threats: Social engineering. Software Engineering Institute (2014).

[16] Algarni, A., Xu, Y. and Chan, T. An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. European Journal of Information Systems, 26, 6 (2017), 661-687.

[17] [17] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. and Downs, J. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. ACM, City, 2010.

[18] Iuga, C., Nurse, J. R. and Erola, A. Baiting the hook: factors impacting susceptibility to phishing attacks. Human-centric Computing and Information Sciences, 6, 1 (2016), 8.

[19] Hadlington, L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3, 7 (2017), e00346.

[20] Parrish Jr, J. L., Bailey, J. L. and Courtney, J. F. A personality based model for determining susceptibility to phishing attacks. Little Rock: University of Arkansas (2009), 285-296.

[21] Abass, I. A. M. Social Engineering Threat and Defense: A Literature Survey. Journal of Information Security, 9, 04 (2018), 257.

[22] H. Aldawood and G. Skinner, "Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal," International Journal of Security (IJS), vol. 10, no. 1, p. 1, 2019.