Evaluating Contemporary Digital Awareness Programs for Future Application within the Cyber Security Social Engineering Domain

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

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

ABSTRACT
Social engineering is a rising threat to individuals and organizations, causing massive losses every day. Contemporary and innovative methods to mitigate these threats are needed today more than any other time in the past. This study aimed to assess the different awareness programs and techniques being developed or utilized against cyber security social engineering. A systematic review of various studies was performed, identifying that interactive awareness programs against social engineering are far superior and more engaging than traditional training sessions.

General Terms
Cyber Security, Social Engineering, Information Security Awareness.

Keywords
Cyber Security, Social Engineering, Information Security Awareness Programs, Security Awareness, Phishing Awareness, Anti-Social Engineering, Cyber Security Awareness, Information Security Awareness.

1. INTRODUCTION
The cyber-world is involved in increasing connectivity among people across the globe. Data theft has been a critical concern to governments, organizations, and individuals as a result of interconnected information systems [1]. Additionally, in today's business ecosystem, social engineering has emerged as a trending cyber security concern. A social engineering attack can be defined as a set of psychological and analytical techniques that are used with the motive of manipulating the human element of organizations [2-4]. The main path through which social engineers invade organizations is the exploitation of psychological vulnerabilities of employees. Unfortunately, many victims of social engineering attempts purposefully or inadvertently grant social engineers access to critical information or sensitive data that may cause harm to their organization. Researchers in the field confirm that end-users overestimate their detecting capability, which makes them the weakest link in the security chain [5].

Promoting digital awareness among employees plays a major role in covering the knowledge gap of staff members. Awareness programs not only increase the internal immunity of an organization but also tend to bring changes in their behavioral as well as cultural aspects [6]. Over time, adopting traditional safety awareness methods has helped organizations to raise the level of awareness among their employees. However, today, with the increase in the intensity of cybercrimes, modern organizations have shifted their focus to state-of-the-art awareness programs that help their employees to recognize and detect such attacks beforehand [7]. This study reviews relevant esteemed papers from a cyber security perspective to discover best practices and what has been most effective. From this review, solutions will be adapted for use in a cybersecurity social engineering context.

2. METHODOLOGY
2.1 Search Strategy and Selection Process
We used the approach of a systematic review in order to assess awareness efforts regarding social engineering in organizations and eLearning best practices adopted by different enterprises. The findings of various literature accessed via popular databases were examined based on certain inclusion and exclusion criteria. The search strategy was also defined in order to identify the approximate number of studies that exist in this context. Databases included ABI/ INFORM, Ingenta Connect, Taylor and Francis Online, Wiley Online Library, Sage Premier, Emerald Insight, Science Direct, and IEEE Library. Additionally, the study made use of Google Scholar in order to identify any additional studies that may have been missed in other databases. However, we made sure that no published dissertations or theses are included in this review. The main keywords used include cyber security, social engineering, threats, organization, phishing, traditional awareness programs, modern awareness program, attacks, security standards, policies.

2.2 Inclusion Criteria
The studies included in the present research were based on following criteria:

- Available in full access status.
- Published in English.
- Included at least one of the keywords that were relevant according to the present study.
- Published after the year 2014

2.3 Exclusion Criteria
Considering the aim of our study, we developed eligibility criteria to eliminate irrelevant studies. The exclusion criteria are presented as follow:

- Studies that are presented in abstracts and reviews.
- Studies that have very limited information with respect to the topic of the study.
- Published in foreign languages and for whom the content was not available in the English language.

- Published before the year 2014.

3. DISCUSSION

3.1 Traditional Awareness Programs

Today, social engineering has emerged as a primary threat and is considered an entry point for most other significant cyber-attacks. When it comes to attacks that pose a threat to an information system, a tactical and a strategic weapon to mitigate the risk is to provide physiological enhancement to employees in the form of awareness programs on inter-functional and the intra-functional aspects [6]. Awareness in our study refers to the knowledge among the members of organizations with respect to the protection of critical information and their physical assets. This also includes acknowledging that external parties can deliberately steal, damage or misuse data relating to organizations [8]. Until the early-2000s, traditional methods were popularly employed by organizations as a means of keeping their employees abreast of various social engineering attacks. These traditional methods typically included onsite training and awareness camps, screensavers, posters, manual reminders or in some cases, online e-learning courses [9]. However, the major problem with these traditional awareness methods was that they were not interactive and dynamic. Moreover, these traditional programs generally adopted a generalized approach rather than emphasizing different manipulation techniques adopted by attackers. Further, they were conducted in a completely formal setting which had certain limitations such as lack of employee engagement [10]. As mentioned in [11], traditional awareness programs like printing posters and warning messages in the form of screensavers only provided basic awareness regarding such attacks. However, when faced with such attacks in real life, employees usually fail to recognize them due to the lack of practical exposure.

Another shortcoming of traditional awareness programs is their inability to consider the behavioral aspect of employees such as their tendency to trust, which is the key to manipulation by social engineers. Moreover, it has been argued in the literature that the perception of threats is subjective, which is not explored in traditional awareness programs [12]. Furthermore, uncertainty in the mode of these attacks has further come up as a major challenge. For instance, in spite of spending hours undergoing traditional awareness programs, it has been found that employees find it hard to curtail their curiosity in opening suspicious links and emails. Thus, there is an urgent need of advanced awareness methods to better handle the problems of social engineering [13]. Social engineering is dynamic, as newer methods of attacks are constantly being devised. Therefore, new mechanisms to tackle them are mandated. Modern awareness programs

Due to various shortcomings of traditional awareness programs, several modern awareness programs are now being explored and applied by different organizations. These modern security awareness programs involve a much more creative approach than the old posters and the training sessions.

Some of the modern security awareness programs are online awareness approaches that include e-mail broadcasting, online synchronous and asynchronous discussions, information uploading or animation and blogging [11]. Recently, many organizations have developed internal blogs to keep their employees informed regarding forms of social engineering threats. Examples include eBay's online tutorial on email spoofing and Microsoft's phishing tutorials [14]. Another modern awareness program that is adopted by organizations is called WBT, which is a web-based computer security awareness program. This WBT involves user-friendly and flexible modules through which users can increase their security awareness at their own pace. It also provides organizations with flexibility in spreading awareness of organization-wide standards among employees. Security alert messages have also come up as an alternative way of raising awareness levels among employees [15].

Another popular awareness program is a simulation-based security awareness program, under which employees are sent simulated phishing emails to test their awareness and vulnerability to social engineering [16]. Additionally, game-based awareness programs have evolved as a new strategy in organizations against social engineering. The traditional methods, which lacked the scope to engage employees, were ineffective; however, game-based methods are meant to be more fun and engaging. They are emerging as an effective tool to increase employees' security awareness. A good example of those game-based methods is the cyber security requirement awareness game (CSRAG). This game-based tool is designed to make employees aware of the concepts of security, threats, various ways of identifying the threats, and possible solutions to help them safeguard their intellectual property. To achieve better awareness levels, the players are required to play the game multiple times because one session is insufficient to grasp the basics thoroughly, whereas multiple game sessions can unfold various lessons for employees [17].

Additionally, another such game-based awareness program is called Securix, which is a 3D phishing attack awareness game developed in order to enhance social engineering skills. This game is popular among many organizations today due to its effectiveness in developing awareness on three aspects including manipulation, e-mail/spam and website forgery [18]. Several scholars have also developed game-based applications to stimulate interest among employees and engage them in raising awareness regarding social engineering attacks [19, 20].

3.2 Available Digital Interactive Learning Solutions to Raise Awareness

In general, in order to have a more secure information system, end-users should be aware and informed. Some of the various other solutions that are also available to raise information security awareness include a tool called the YooHoo awareness system. This tool has mainly been developed for software developers to raise their awareness considering the number of interrelated codes they are working with on a daily basis. This specific system filters information regarding the changes taking place internally, thus strengthening the internal security system [21].

Furthermore, FASTDASH is an alternative tool that can be used for enhancing awareness levels among employees. FASTDASH stands for fostering awareness for software teams' dashboards which is a visualization tool for software developers. This tool helps organizations maintain better awareness during collaborative training programs [22]. Organizations' information and security policies and standards must be developed and updated in such a manner that they formally and clearly identify and communicate their security rules for internal and external stakeholders. Thus, all organizations, regardless of size, should set security policies and regulations and have them in place. Furthermore, there should be straightforward plans regarding the ongoing

training guidelines and procedures that can help employees to maintain a certain level of awareness of the corporate policies and the standards [23].

Another way to increase awareness among employees is by giving them significant information only as necessary, such as permission to circulate information from internal security assessments. Incidents of near-misses is an important element of awareness and training of employees since people commonly have a habit of underestimating the risk associated with information exchange [24]. Furthermore, realistic case studies and the presentations can further stimulate the thoughts and the discussion on information security issues [25]. Table 1 presents a review of key studies utilized in this study for evaluating the effect of modern awareness programs and techniques in raising social engineering awareness.

Table 1. Evaluation of different awareness programs against social engineering

R	Aim	Method	Findings
[6]	Understand the utility of security awareness programs.	The research is based on the systematic review of the past literature.	The ultimate solution requires a behavioral change that can be brought through awareness.
[8]	Test the quality of information security awareness.	Survey method was adopted which included 100 respondents in Franklin County, USA, using a close-ended questionnaire.	There is a high need to pre-decide the effort and the cost that is required for the cyber security awareness programs in order to get better results.
[9]	Understand what social engineering attacks are, their classification, detection strategies and the prevention procedures.	In-depth examination of secondary data pertaining to social engineering attacks, existing detection, prevention and mitigation techniques and challenges and future directions.	Artificial intelligence-based defense programs are more effective in securing information security systems against such crimes.
[11]	Understand user preference regarding security awareness delivery method.	A qualitative study of 60 participants was conducted on full-time and part-time workers with a private personal computer.	Combined delivery method was a more effective way than a single method.
[26]	Highlighting the major channel of information leakages.	The study is based on a review of past literature.	Spear-phishing evolved as the major channel of information leakages.
[13]	Understand what spear-phishing is.	A survey approach was adopted in the following research. 1359 respondents belonging to a medium-sized firm based in Washington DC using emails as a primary form of communication. The respondents were split into control and treatment groups.	Spear-phishing penetrated due to the lack of awareness among employees.
[14]	Understand the different types of cybercrime.	The study is based on a review of past literature.	Various kinds of attacks include phishing fraud emails and embedded training works better than sending notices.
[18]	Testing the effectiveness of a security game as an effective method of increasing awareness among employees.	A survey approach was adopted in which 50 respondents belonging to different profiles such as teachers, banking staff, and employees of firms. They were given a close-ended questionnaire.	This method was much more fun and engaging. The result was far more effective in enhancing avoidance behavior towards phishing attacks.
[21]	Reviewing approaches that increase the level of security awareness.	The study was based on a review of the literature.	Presenting modern techniques such as FASTDASH, YooHoo that are very effective in raising the awareness levels.
[27]	Reviewing the effectiveness of FASTDASH as an awareness tool.	The study was based on the review of the literature.	FASTDASH is a very effective tool in raising the level of awareness.

[28]	Evaluating the effectiveness of social engineering awareness game on improving overall information security awareness.	A controlled experiment consisting of a control group and experimental groups. 20 employees in the age group 18-40 years participated.	Gaming improved awareness of social engineering by 71%.
[20]	Increase social engineering awareness among employees by using a card game	The experiment was conducted on 30 full-time employees with gaming experience from Frankfurt using a card game developed by authors.	The experiment yielded positive results and showed an enhanced level of awareness post-playing the game.
[29]	Evaluate different game-based learning systems in increasing social engineering awareness	Secondary studies were evaluated to identify the strengths and weaknesses of different games systematically.	Multi-player games are most effective. However, a combination of different games is the best defense against social engineering.
[30]	Evaluate the effectiveness of different gaming applications in improving cyber security awareness	A systematic review method was adopted, utilizing key secondary studies.	Mobile-based gaming applications are far more effective in raising awareness.
[19]	Test a self-developed gamed called What.Hack in increasing awareness of phishing attacks.	39 students from Cornell University were recruited in an experiment involving using the game.	Game-based applications are more effective than traditional training programs and role-play games in raising awareness.

4. 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.

5. CONCLUSION

Since social engineering attacks mainly target the behavioral aspect of employees to extract confidential information pertaining to an organization, the enormity of security concerns is higher because insider access tends to collude with the skills of outside attackers that can completely endanger the entire system. The main aim of this study was to review different awareness efforts regarding social engineering practiced in organizations today so that suitable recommendations can be made to improve the efficiency of such programs. In this regard, the study presented various traditional and modern awareness programs that are used by enterprises to protect their employees from social engineering attackers. It was found that interactive gaming applications can prove to be an effective way of elevating employees' knowledge and hence reducing the incidences of social engineering attacks. These programs, besides increasing awareness, also tend to bring about cultural and behavioral changes among employees. It was further found that traditional methods failed to efficiently equip employees in tackling real-life situations involving social engineering attacks. Further, traditional methods failed to engage the employees' attention. Based on our review, certain recommendations can be provided, which are listed as follow:

- More proactive management strategies should be adopted at the higher levels of the echelon so that it leads to the adoption or establishment of an appropriate volatility management framework. This framework could base its management decision on two main aspects. The first one should focus on the nature of management while the other one should emphasize people's characteristics before planning prevention strategies.
- In order to protect an organization from cyber-attacks, enterprises should focus on designing contemporary interactive awareness programs like game-based tools that take into consideration recent security incidents, employee management issues, and target identification.
- Serious mini-games involving informant design, which have emerged as an effective technique to raise consumer awareness, can be used as the framework to include distinctive stakeholders-specialized inputs while designing the game. This will not only raise the awareness levels but also provide companies with an opportunity to include the needs and preferences of different stakeholders and end-users.

6. REFERENCES

[1] Flores, W. R. and Ekstedt, M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. computers & security, 59 (2016), 26-44.

[2] Aldawood, H. and Skinner, G. A Taxonomy for Social Engineering Attacks via Personal Devices. International Journal of Computer Applications, 975 (2019), 8887.

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

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

[5] Bakhshi, T. Social engineering: revisiting end-user awareness and susceptibility to classic attack vectors. IEEE, City, 2017.

[6] Hauser, D. Social Engineering Awareness in Business and Academia (2016).

[7] Fan, W., Kevin, L. and Rong, R. Social engineering: Ie based model of human weakness for attack and defense investigations. IJ Computer Network and Information Security, 9, 1 (2017), 1-11.

[8] Al-Hamdani, W. A. Assessment of need and method of delivery for information security awareness program. ACM, City, 2006.

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

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

[11] Abawajy, J. User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33, 3 (2014), 237-248.

[12] Sallai, G. Social Engineering Audit and Security Awareness Programme. KPMG (2016).

[13] Caputo, D. D., Pfleeger, S. L., Freeman, J. D. and Johnson, M. E. Going spear phishing: Exploring embedded training and awareness. IEEE Security & Privacy, 12, 1 (2014), 28-38.

[14] Aggarwal, G. General awareness on cyber crime. International Journal of Advanced Research in Computer Science and Software Engineering, 5, 8 (2015), 204-206.

[15] Manadhata, P. K. and Rao, P. V. Security alert prioritization. Google Patents, City, 2015.

[16] Belani, R., Higbee, A. and Greaux, S. Performance benchmarking for simulated phishing attacks. Google Patents, City, 2017.

[17] Yasin, A., Liu, L., Li, T., Fatima, R. and Jianmin, W. Improving software security awareness using a serious game. IET Software, 13, 2 (2018), 159-169.

[18] Onashoga, A. S., Ojo, O. E. and Soyombo, O. O. Securix: a 3D game-based learning approach for phishing attack awareness. Journal of Cyber Security Technology (2019), 1-17.

[19] Wen, Z. A., Lin, Z., Chen, R. and Andersen, E. What. Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. ACM, City, 2019.

[20] Beckers, K. and Pape, S. A serious game for eliciting social engineering security requirements. IEEE, City, 2016.

[21] Holmes, R. and Walker, R. J. Customized awareness: recommending relevant external change events. ACM, City, 2010.

[22] Soares, A. G. M., dos Santos, C. G. R., Mendonça, S., Carneiro, N. J. S., Miranda, B. P., de Araújo, T. D. O., de Freitas, A. A., de Morais, J. M. and Meiguins, B. S. A review of ways and strategies on how to collaborate in information visualization applications. IEEE, City, 2016.

[23] Bauer, S. and Bernroider, E. W. From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48, 3 (2017), 44-68.

[24] Chinta, M., Alaparthi, J. and Kodali, E. A Study on Social Engineering Attacks and Defence Mechanisms (

[25] Wilcox, H. and Bhattacharya, M. Countering social engineering through social media: An enterprise security perspective. City, 2015.

[26] Shakti, S. and Dhanoa, R. CYBER – CRIME AWARENESS. International Journal in Multidisciplinary and Academic Research, Vol. 2, No. 2 (2015).

[27] Ng, K. K. Technology Solutions to Fight Cybercrime. City, 2010.

[28] Olanrewaju, A.-S. T. and Zakaria, N. H. Social engineering awareness game (SEAG): an empirical evaluation of using game towards improving information security awareness. City, 2015.

[29] Awojana, T. and Chou, T.-S. Overview of Learning Cybersecurity Through Game Based Systems (2019).

[30] Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M. A review of using gaming technology for cyber-security awareness. Int. J. Inf. Secur. Res.(IJISR), 6, 2 (2016), 660-666.