Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review

Hussain Aldawood
School of Electrical Engineering and Computing
University of Newcastle
Newcastle, Australia
hussain.aldawood@uon.edu.au

Geoffrey Skinner
School of Electrical Engineering and Computing
University of Newcastle
Newcastle, Australia
geoff.skinner@newcastle.edu.au

***Abstract*—Social engineering, due in part to the increasing popularity and advancements in information technology and ubiquity of devices, has emerged as one of the most challenging cyber security threats in the contemporary age. In the context of cyber security, social engineering is the practice of taking advantage of human weaknesses through manipulation to accomplish a malicious goal. This literature review identifies various social engineering cyber security threats in diverse environments. Exploiting humans as the weakest security link in such environments, as opposed to technical vulnerabilities and system protocols, has led to increased calls for raising information security awareness among users. One of the most straightforward solutions is through effective training and education programs. As such, the paper details how innovative information security education programs can effectively increase user/employee awareness and ultimately reduce cyber security incidents.**

Keywords—social engineering, phishing, anti-social engineering, cyber security awareness, information security awareness

I. INTRODUCTION

With the ever-growing advancements in technology, security threats and risks are on the rise. Cybercriminals are getting increasingly sophisticated with the ways they exploit technology, making it difficult to eliminate risks. Cyber-attacks can be on technological infrastructure, in the form of malware and viruses, or on human personnel, in the form of social engineering or cyber bullying [1][2]. Recently, some of the fastest-growing corporate crime threats have steered away from exploiting systems or vulnerabilities on information security, and instead have focused on humans, a target considered to be the weakest link in every enterprise [3]–[6].

Recent digital improvements have altered the general landscape of cyber security. Conversely, individuals and organizations have been exposed to social engineering threats today more than ever before. Social engineering is the art of manipulating human weaknesses in order to attain a malicious goal [7]. The growth of cyber security attacks has largely been characterized by the increase in social engineering attacks as well. The nature of social engineering attacks is complicated since attackers exploit human vulnerabilities, which cannot easily be secured automatically [8]. Previous studies have indicated that social sites are the primary source for the attacks. However, according to the principles of persuasion, people are more likely to observe and consent to a particular communication if the way in which the communication is packaged makes it look legitimate [9]. According to [10], this is dependent on a number of elements that are likely to influence the supposed legitimacy of a source.

In the context of information security, attackers breach regulations and usually target certain human elements to access their sensitive information. Cyber criminals tend to lure their victims into breaking the security prescript, confiscating effectual information that can be used for a more severe attack, such as blackmailing [11]. In an attempt to tame and reduce social engineering fraud, enterprises and institutions are advised to establish comprehensive protocols and clear policies [12]. Several studies suggest comprehensive information security programs that include awareness and training programs to safeguard information assets and ensure business continuity [12][13]. To prevent opportunistic attacks, scholars suggest increasing the level of information security awareness and implementing training programs for employees and members of organizations so that they know how to safeguard their own information and systems [3][11][13]–[18]. This literature review analyzes the social engineering threats in various institutions, as well as how implementing information security awareness programs can be an effective way to raise employee awareness to prevent cyber-crimes.

II. BACKGROUND

In modern information technology, the world of information security has developed as a vital subject, with the human factor constituting the majority of security breaches [19]. According to a study on cyber security by hacking of employees, the security of information is dependent on three primary foundations: people, processes and technology [20]. Researchers and experts found that even in situations where different organizations have polished procedures and sophisticated technology, the weakest link still lies in the human personnel in the process. This brings into context the scope within which this review is applicable. It shows how widely the cyber security through social engineering issue can have influence since human personnel is present in very small and medium enterprises, as well as in enormous organizations.

Many conducted studies confirm that most computer users have a lack of information security knowledge due to insufficient awareness. It has also been shown that both academic institutions and governments have been making efforts to provide security awareness to enhance public understanding of cyber security risks and threats [16]. The Anti-Phishing Work Group (APWG) is one example of a non-

978-1-5386-6522-0/18/$31.00 ©2018 IEEE 4-7 December 2018, Wollongong, NSW, Australia
2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)

profit organization running to provide anti-phishing training to increase the public understanding and awareness of information security. The U.S. Computer Emergency Readiness Team is another example that presents free advices on its website about popular security breaches and cracks for computer users who lack computer security knowledge.

Social engineering occurs when confidential information or valuable assets are obtained by manipulating legitimate users or owners [20]. Social engineering attackers select their target organizations based on several factors while considering the amount of sensitive data that they could possibly get as a result of an attack. Large telecommunication companies and other similar organizations with large customer bases and a vast collection of sensitive data tend to be very appealing targets for social engineering attacks. Farooq et al. [21] indicate that educational institutions, especially universities, are also seen as great potential targets for attackers because of their computing power and due to the fact that they grant open access to the public.

Accessing social media sites from an organization's network is becoming another major challenge for scholars, as it has been identified as a leading issue that puts organizations at risk of being targeted by social engineers. Wilcox et al. [22] described the rise in the number of staffs who frequently use social media in the workplace as one that has produced serious challenges to information security professionals in terms of people, process and technology. Furthermore, recent cyber-attacks via the use of social media have been causing distress because of the tendency of those social engineers who target employees via these social platforms to raid information assets existing in organizations [23].

In [24], a team of researchers from Google, the University of California, Berkley, and the International Computer Science Institute clarified the idea of how dire the situation of protecting data has become. They looked at billions of stolen credentials to understand how those credentials were taken, how they were used, and possible impacts on later stages. Out of all the participants in the joint study, they identified 788,000 possible targets of off the-shelf key loggers, more than 12 million probable targets of phishing kits, and about 2 billion credentials in the form of usernames and passwords that have been exposed through social engineering. This type of study confirms the need to educate and train employees in every enterprise to raise the level of their awareness and safeguard valuable information assets.

A. Contextual Definition of Terminologies

Phishing is one of the most prevalent examples of social engineering techniques in which a potential target is sent a message that impersonates an authentic source or organization. Phishing is used to mislead users, and it exploits weaknesses in today's web security. Phishing message delivery can take several forms such as instant messaging and Voice over Internet Protocol (VoIP), but the most popular medium for phishing remains emails and phishing websites [25]. In this study, phishing is defined as the impersonation of a legitimate source to acquire confidential information.

To have a better understanding of the definition, we need to explain the basic mechanism of how phishing works. Usually, a malicious link or attachment appears as a benign linked Google Doc while the user is redirected to an identical copy of the real website to enter personal details. After the targeted user has finished filling in the details on the fraudulent website, a copy of these details is sent to the attacker. The attacker can then use the harvested information in various ways. Phishing attacks are serious security challenges because they depend on individuals' or subscribers' conduct and behaviour instead of a security vulnerability, making phishing one of the most common and successful techniques of social engineering [16][26].

B. Review Methodology

With a complete review of literature in the research field of social engineering and information security awareness, the objective of this paper is to synthesize existing knowledge. The methodology of this research consists of two stages. The first phase includes searching for relevant literature in both fields: social engineering and programs for raising information security awareness. The other phase is to analyze the selected literature to identify the most common social engineering threats. It contributes to the research field by summarizing how education programs on information security can play a key role in increasing the overall level of awareness of computer users. The objective is to help organizations prevent being victims of cyber-attacks through social engineering.

TABLE I. AVERAGE YEAR AND NUMBER OF CITATIONS FOR REFERENCES USED PER SECTION

Research Area	Average Year	Average Number of Citations
III - Social Engineering (SE) in a Cyber Security Context	2012	29
IV - Information Security Awareness (ISA)	2012	49
V - ISA on SE	2012	44

III. SOCIAL ENGINEERING IN A CYBER SECURITY CONTEXT

Social engineering is defined as the manipulation of the human aspect of technology use by deception [8][27]. According to the published report by the Centre for the Protection of National Infrastructure, social engineering has been defined based on security and psychological terms by various organizations and individuals [28]. In [29], SE is defined as a breach in an organization's security through interactions with staff and personnel. Kevin Mitnick as an individual, explains it as exploiting a person's naivety using influence and persuasion to access pertinent information [30]. Social engineering is also identified as a method that uses communication between humans to gain entry into a system in an illegitimate way [20]. Such attacks can happen on both a psychological (human-based attack) and physical level (computer-based attack) [19][28]. In this paper, social engineering is defined as manipulating and persuading people to disclose sensitive information or grant access to restricted areas or systems.

Reviews, like Verizon's "Data Breach Investigations Report 2012" [31], confirm that social engineering threatens not only government agencies and enterprises, but also individuals, including those who suffer from identity theft. An internationally recognized incident featured in the news showed that Snowden convinced several colleagues effectively to gain login authorizations of NSA accounts in Hawaii leading to the release of top classified and confidential data [32]. The incident is an example of how social engineering can bypass every digital and physical security platform because it mainly relies on manipulating humans [8].

Social engineering attacks can be performed in several ways including face-to-face, as well as through information technology. In the case of performing a digital attack, the social engineer can automate several malicious attempts and lower the costs of the attacking process by sending phishing emails, for example, exploitation via the digital domain [25][33]–[36]. Other social engineering experiments are very well examined in several studies such as those conducted on college users and tested in a university setting [25], the individual weakness [35] or how to understand the profile of victims [36], and the vulnerability associated to users' character [34].

Regarding private information collected through social networks, Huber et al. [37] present an attack called "automated social engineering," that aimed to gather information that is accessible in a social network, and to communicate with individuals by those social networks to obtain information. Scholars in literature usually include the exploitation of the trust and emotions in their studies of social engineering malware [38], privacy- training and education [19] or weakness to social engineering as a whole [39]. Social engineering is also studied as the most common technique used in Advanced Persistent Threat attacks [40].

Social engineering attacks take advantage of their targets following a typical cycle to gather information or access information systems. The attack cycle typically begins with information gathering [41], from public sources including social media posts, phone books, jobs portals, web pages, among others to develop a mutual relationship with the target. Once a relationship is established, the attacker gets the target to reveal sensitive information such as credit card numbers, login credentials and other valuable data [28]. Gaining this type of information can either be the ultimate goal of the attacker, or the beginning of a major cyber-attack.

Social engineering assaults can include interpersonal interaction involving direct communication (e.g. by telephone) or indirect communication through electronic means (e.g. by email). Either way, social engineering relies on deceiving others for the purpose of information gathering, fraud, identity theft, or gaining computer system access [42].

IV. Information Security Awareness

Information security awareness is an essential component of organizations' information security. Employees are important organizational assets because of their capability to make crucial information security decisions when the need arises [15]. Information security awareness programs can support and develop such capabilities. In this paper, information security awareness is defined as ensuring that all members in an organization understand their roles in protecting data and information. Organizations need to verify that all staff know their roles and responsibilities in safeguarding the information that is in their possession.

The significance of safeguarding information assets and resources has been extensively recognized recently. Today, organizations care more about protecting their information security than ever before. This is to keep intellectual properties safe and to maintain their business continuity without being disrupted. Literature indicates that information security professionals argue that personnel play important roles in the overall information security of organizations [43][44]. However, this importance relies on users' competence to make significant information security decisions. All users must be educated about information security threats and understand their role in the security process [21]. Rather than being part of the problem, end-users, with education and awareness, can be part of the solutions. Experts encourage organizations to develop security plans that adopt and include information security awareness programs and implement proper training for computer users. Ensuring that all computer users have the adequate and sufficient knowledge creates a security culture.

TABLE II. List of Articles on Awareness and Training

[13]	Awareness and education programs positively influence staff attitude and behavior towards information security
[51]	Information security is in continuous need for higher levels of awareness and education
[52]	Information security awareness is a lot more effective than other methods
[53]	Implementing information security awareness programs is probably the greatest countermeasure for its efficiency, as it increases understanding and awareness
[54]	Information security training has a positive effect on employees' behavior for compliance
[55]	Employee contribution and knowledge conception integrate positive changes regarding information security awareness and behavior in organizations
[56]	Information security awareness has a significant effect on staff compliance and attitude

Currently, evolving technologies and technology use have rapidly changed the way society functions [45]. The constant and fast development process of information technology has pushed enterprises to focus on solutions that involve encryption, access control, CCTV and many others [46]. Most of information security attacks today are attributed to human exploitation due to a lack of awareness regarding information security [16][47][48]. Consequently, providing technical solutions is not enough. It is important to also enhance training and make provisions for raising the awareness of computer users about how to manage the human elements of security. The user's errors related to technology use cannot be solved by increasing technical tools alone, but an awareness training program can yield excellent results [15][49].

Table II shows a summary of articles published on the significance of information security awareness. The

publications also discuss the influence of education and compliance on information security efficiency. The articles support the notion that information security awareness programs help organizations to create a safer computing and data environment in order to keep information properties protected from such malicious attacks. The training of staff enables them to effectively adhere to sound cyber security practises. Hence, awareness and training programs complement each other, influencing users to develop their security behaviour for managing possible cyber-attacks [3][6][21][50].

V. Information Security Awareness in a Social Engineering Context

Computer technical attacks differ from social engineering attacks based on the technical level of personnel involved in the security breach. Common technical attacks would most likely involve staff from IT departments, which probably have in-house experts with security and technical knowledge to handle it. However, social engineering attacks target all levels in organizations, from cleaners who work after regular working hours up through executives. Targeted personnel might have insufficient technical experience or may be unaware of social engineering concerns. For example, a large number of employees do not know the exact classification of information in their possession (e.g. general use, sensitive, classified). It is practically impossible to eliminate social engineering breaches without working on improving the level of information security awareness among all staff. A multilayered approach with a combination of technical security and increasing the information security awareness level of members, is necessary in order to build a great defence against social engineering attacks [28].

Literature suggests implementing and introducing information security awareness programs to protect the firewall composed of the human mind against social engineering strategies. Mouton et al in [7] for example, listed some recommendations to reduce the risks related to various social engineering attacks. They argue that there is a necessity for organizations to provide educational training for every single employee to help them establish an information security culture in the workplace and make employees aware of the different methods used or followed by attackers. Similarly, [50] notes the need to underline the security of a person's information security awareness within the whole organization to avoid a possible leakage of any confidential data. Furthermore, other studies like [3][13][15][21][55][57]–[59] confirm that as long as staffs are not conscious and aware of possible threats caused by social engineering, technical measures are insufficient.

In terms of the individual awareness level on social engineering threats, several studies have highlighted users' lack of understanding of security and privacy threats associated with personal smart devices they tend to use. For instance, it is noted in literature that users of various technological e-health devices are not aware enough of the latest threats and social engineering techniques that can take advantage of their shared personal data [10]. Additional human factors were also studied by Bellekens et al. in [60] in which they collected survey data from students and professionals in various universities across the United States to investigate the privacy and security risk associated with social engineering in personal e-health services. Those who participated in the survey showed very poor understanding along with a lack of knowledge regarding the technologies they elected to use. As a result, researchers argue that new security and confidentiality actions should be developed with an emphasis on improving the user overall threat awareness caused by similar smart devices. [60][61].

Human aspects are major factors in safeguarding information properties that could be sources of harms to the overall safety of an establishment. Trust is among the leading security elements that is associated with human's nature. Researchers argue that trust is vital in every aspect of an information security system and may affect security conduct considerably [8][10][62]. For instance, [16] is a trust survey indicating that most computer users lack security awareness and tend to be overly trusting of strangers. This study, like many others, concluded that when computer users are aware of the risks surrounding them and the signs of a potential threat, self-security against trust can be significantly improved.

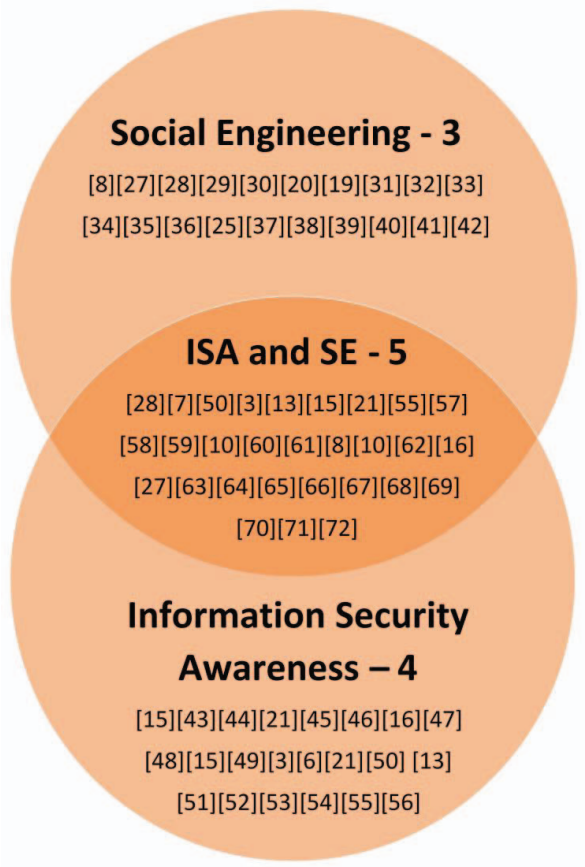

Fig. 1. References used in core sections.

There are several surveys that studied the teaching method of information security awareness programs as a non-technical answer to alleviate social engineering attacks. Literature suggests that information security teaching techniques should appeal to users' consideration so as to improve awareness and ensure that trainees are able to remember the knowledge gained for an extended time [27]. Training activities must take into account knowledge acquisition, recollection, and transfer.

Effective training should provide an opportunity for users to become familiar with and regularly practice the content, making training an ongoing and constant activity. In brief, organizations have more responsibility today to ensure that their employees are cautious of all the serious consequences that may arise from social engineering. Implementing and delivering different methods of information security awareness programs can help organizations to maintain the minimum security level to safeguard their intellectual properties.

It is largely recognized within current literature that information security awareness is a key component in an overall effective security strategy [52][57][62]–[70]. Consequently, delivering a well-designed information security awareness program would contribute to thwarting trust threats, especially those caused by social engineering attacks. In summary, the best preventive measure for anti-social engineering attacks is education and awareness, which need to be considered in any organization.

In terms of engineering the next generation of learning technologies for information security education, the following methods have the potential for development:

- Online delivery methods including e-mail broadcasting, social media advertising, online synchronous and asynchronous discussion, blogging, and animation.
- Game-based delivery methods, which can challenge, motivate and engage members of an organization.
- Video-based and self-paced delivery methods that allow personnel to study independently.
- Simulation-based delivery methods including simulated phishing emails to assess users' susceptibility and measure the level of awareness.

Several studies introduced innovative learning platforms to replace traditional classroom-based delivery with e-learning techniques. For instance, [46] is an e-learning platform proposal to guide and monitor the impact of employees' progress through a learning management system. Furthermore, Beckers et al. [71] introduce the use of gamification to raise employees' awareness regarding information security. This proposed game considers the users in an organization and draws upon principles of human behavior that social engineers tend to exploit. Combining gamification with security awareness programs creates an effective training experience. Using gamification has been identified in literature as an effective method in which computer users learn about social engineering threats in a systematized method [72]. Through this approach, employees experience threats they may encounter in their daily activities and begin to develop a sense of suspicion and mistrust regarding potential attacks. Implementing any of the identified information security educational methods would provide computer users with knowledge to safeguard their own data and minimize the risks of being a victim.

VI. Research Limitations

There are some limitations in relation to the used search terms to identify literature. There were only English search terms used to find related articles. Publications in other languages were not included in this paper. Furthermore, some contributions might not be covered in this literature review due to the fact that books might include valuable contributions and they were not widely explored in this paper. The proliferation of terms to describe similar concepts is identified as a big challenge for information security research. For example, information security education (ISE), information security training (IST) and information security awareness (ISA) have been defined differently by several researchers around the world, each with a different focus and purpose. Decker [73] displays the lack of correlation between ISA, ISE and IST as a result of unclear definitions for the three concepts.

VII. Conclusion and Future Work

Today, organizations are greatly dependent on information systems. This reliance has led to being vulnerable to information security threats that put systems at risk. Furthermore, social engineering fraud has been rising significantly with advancements in technology. Criminals are getting more sophisticated in finding new ways to attack. As a result, organizations have been increasing their investments in cyber security initiatives to safeguard their data. This paper presented an overview of the major social engineering threats, as well as how implementing information security education programs can be an effective way to increase user awareness for reducing and hopefully preventing cyber-crimes.

Some governments such as Australia and the U.S. have started legislating different laws and regulations against cyber criminals to ensure the protection of citizens and organizations from social engineering attacks and other cyber-related crimes. Meanwhile, organizations have been adjusting their security policies to cope with the current social engineering threats that could disturb their business continuity. However, keeping up with perpetrators is challenging. Information security awareness is a crucial step towards having a secure cyber environment in which users of all ages can freely use technology to conduct positive and self-developing activities. It is considered as the most effective way to deal with social engineering threats as technology development has made humans potential targets of hackers and cyber criminals.

Future studies can focus on additional factors that influence employees' information security awareness and behavior in order to fill a noticeable gap in literature. Due to the majority of quantitative work that has been done, qualitative studies like interview studies might add value to the research field. Moreover, intention and actual social engineering security behaviors should be given more attention. More research including experiments and case studies will lead to a better understanding of the flaws in self-reporting as an indicator of employees' actual behavior.

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.

REFERENCES

[1] D. Sarathchandra, K. Haltinner, and N. Lichtenberg, "College students' cybersecurity risk perceptions, awareness, and practices," in *Proc. Cybersecurity 3rd Symp. (CYBERSEC '16)*, Coeur d'Alene, ID, 2016, pp. 68–73.

[2] S. S. Tirumala, H. Sathu, and V. Naidu, "Analysis and prevention of account hijacking based incidents in cloud environment," in *Proc. Int. Conf. Information Technology (ICIT '15)*, Singapore, 2015, pp. 124–129.

[3] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' information security awareness and behavior: A literature review," in *Proc. 46th Hawaii Int. Conf. System Sciences (HICSS '13)*, Wailea, HI, 2013, pp. 2978–2987.

[4] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of unintentional insider threats deriving from social engineering exploits," in *Proc. IEEE Security and Privacy Workshops (SPW '14)*, San Jose, CA, 2014, pp. 236–250.

[5] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. & Security*, vol. 56, pp. 70–82, Feb. 2016.

[6] A. Tsohou, M. Karyda, and S. Kokolakis, "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs," *Comput. & Security*, vol. 52, pp. 128–141, Jul. 2015.

[7] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in *Information Security for South Africa (ISSA '14)*, Johannesburg, South Africa, 2014, pp. 1–9.

[8] S. Uebelacker and S. Quiel, "The social engineering personality framework," in *Proc. 8th Workshop on Socio–Technical Aspects in Security and Trust (STAST '14)*, San Juan, PR, 2014, pp. 24–30.

[9] J.–W. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. H. Hartel, "The persuasion and security awareness experiment: reducing the success of social engineering attacks," *J. Experimental Criminology*, vol. 11, no. 1, pp. 97–115, Jan. 2015.

[10] W. Kearney and H. Kruger, "Considering the influence of human trust in practical social engineering exercises," in *Proc. Information Security for South Africa (ISSA '14)*, Johannesburg, South Africa, 2014, pp. 1–6.

[11] S. Mohammed and E. Apeh, "A model for social engineering awareness program for schools," in *Proc. 10th Int. Conf. Software, Knowledge, Information Management & Applications (SKIMA '16)*, Chengdu, China, 2016, pp. 392–397.

[12] Y. Chen, K. Ramamurthy, and K.–W. Wen, "Impacts of comprehensive information security programs on information security culture," *J. Comput. Inform. Syst.*, vol. 55, no. 3, pp. 11–19, Dec. 2015.

[13] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. & Security*, vol. 42, pp. 165–176, May 2014.

[14] M. M. Al-Daeef, N. Basir, and M. M. Saudi, "Security awareness training: A review," in *Lecture Notes in Engineering and Computer Science*, 2017, vol. 2229, pp. 446–451.

[15] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *Proc. 9th Int. Conf. Internet Technology and Secured Transactions (ICITST '14)*, London, UK, 2014, pp. 248–252.

[16] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: a phishing threat avoidance perspective," *Comput. Human Behavior*, vol. 38, pp. 304–312, Sep. 2014.

[17] W. Ashford, "Lack of cyber security awareness putting UK organisations at risk," *ComputerWeekly.com*, Mar. 2016.

[18] B. K. Eyong, "Recommendations for information security awareness training for college students," *Inform. Manage. & Comput. Security*, vol. 22, no. 1, pp. 115–126, 2014.

[19] G. L. Orgill, G. W. Romney, M. G. Bailey, and P. M. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems," in *Proc. 5th Conf. Information Technology Education (CITC5 '04)*, Salt Lake City, UT, 2004.

[20] Z. L. Svehla, I. Sedinić, and L. Pauk, "Going white hat: Security check by hacking employees using social engineering techniques," in *Proc. 39th Int. Conv. Information and Communication Technology, Electronics and Microelectronics (MIPRO '16)*, Opatija, Croatia, 2016, pp. 1419–1422.

[21] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Information security awareness in educational institution: an analysis of students' individual factors," in *Proc. 13th IEEE Int. Symp. Parallel and Distributed Processing with Applications (ISPA '15)*, Helsinki, Finland, Aug. 2015, vol. 1, pp. 352–359.

[22] H. Wilcox and M. Bhattacharya, "A framework to mitigate social engineering through social media within the enterprise," in *Proc. 11th IEEE Conf. Industrial Electronics and Applications (ICIEA '16)*, Hefei, China, Oct. 2016, pp. 1039–1044.

[23] R. Heartfield, G. Loukas, and D. Gan, "An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks," in *Proc. 15th IEEE Int. Conf. Software Engineering Research, Management and Applications (SERA '2017)*, London, UK, Jun. 2017, pp. 371–378.

[24] K. Thomas et al., "Data breaches, phishing, or malware? Understanding the risks of stolen credentials," in *Proc. ACM SIGSAC Conf. Computer and Communications Security*, Dallas, TX, Oct. 2017, pp. 1421–1434

[25] J. G. Mohebzada, A. E. Zarka, A. H. Bhojani, and A. Darwish, "Phishing in a university community: Two large scale phishing experiments," in *Proc. Int. Conf. Innovations in Information Technology (IIT '12),* Abu Dhabi, UAE, Jun. 2012, pp. 249–254.

[26] T. Kathirvalavakumar, K. Kavitha, and R. Palaniappan, "Efficient harmful email identification using neural network," *British J. Math. & Comput. Sci.,* vol. 7, no. 1, p. 58, 2015.

[27] A. S. Alazri, "The awareness of social engineering in information revolution: Techniques and challenges," in *Proc. 10th Int. Conf. Internet Technology and Secured Transactions (ICITST '15)*, London, UK, Dec. 2015, pp. 198–201.

[28] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in *Proc. 4th IEEE Int. Conf. Future Internet of Things and Cloud (FiCloud '16)*, Vienna, Austria, Aug. 2016, pp. 145–149.

[29] M. Bezuidenhout, F. Mouton, and H. S. Venter, "Social engineering attack detection model: SEADM," in *Proc. Information Security for South Africa (ISSA '14)*, Johannesburg, South Africa, Aug. 2010, pp. 1–8.

[30] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security.* Indianapolis, IN: Wiley, 2011.

[31] V. R. Team, "Data breach investigations report (2012)," ed, 2012.

[32] M. Hosenball and W. Strobel. (2013, Nov. 7). *Exclusive: Snowden persuaded other NSA workers to give up passwords – sources.* [Online]. Available: https://www.reuters.com/article/net-us-usa-security-snowden/exclusive-snowden-persuaded-other-nsa-workers-to-give-up-passwords-sources-idUSBRE9A703020131108

[33] M. Workman, "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security," *J. Assoc. Inform. Sci. Technol.*, vol. 59, no. 4, pp. 662–674, 2008.

[34] J. L. Parrish Jr., J. L. Bailey, and J. F. Courtney, "A personality based model for determining susceptibility to phishing attacks," in *Proc. Southwest Decision Sciences Institute Annu. Meeting (SDSI '09)*. Oklahoma City, OK, 2009, pp. 285–296.

[35] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Syst.*, vol. 51, no. 3, pp. 576–586, Jun. 2011.

[36] A. Darwish, A. El Zarka, and F. Aloul, "Towards understanding phishing victims' profile," in *Proc. Int. Conf. Comput. Sys and Industrial Informatics*, Sharjah, UAE, Dec. 2012, pp. 1–5.

[37] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites," in *Proc. Int. Conf. Computational Science and Engineering*, Vancouver, Canada, Aug. 2009, vol. 3, pp. 117–124.

[38] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technol. in Soc.*, vol. 32, no. 3, pp. 183–196, 2010.

[39] J. W. Scheeres, "Establishing the human firewall: reducing an individual's vulnerability to social engineering attacks," MS thesis, Dept. Elec. & Comput. Eng., Air Inst. Technol., Dayton, OH, 2008.

[40] I. Ghafir and V. Prenosil, "Proposed approach for targeted attacks detection," in *Advanced Computer and Communication Engineering Technology: Proceedings of ICOCOE 2015* (Lecture Notes in Elect. Eng, vol. 362), H. A. Sulaiman, M. A. Othman, M. F. I. Othman, Y. A. Rahim, and N. C. Pee, Eds. Cham, Switzerland: Springer, 2016, pp. 73–80.

[41] A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: Affect-based model," in *Proc. 8th Int. Conf. Internet Technology and Secured Transactions (ICITST '13),* London, UK, Dec. 2013, pp. 508–515

[42] A. Kumar, M. Chaudhary, and N. Kumar, "Social engineering threats and awareness: a survey," *European J. Advances Eng. & Technol.*, vol. 2, no. 11, pp. 15–19, 2015.

[43] E. Albrechtsen and J. Hovden, "The information security digital divide between information security managers and users," *Comput. & Security*, vol. 28, no. 6, pp. 476–490, Sep. 2009.

[44] A. Da Veiga and J. H. Eloff, "A framework and assessment instrument for information security culture," *Comput. & Security*, vol. 29, no. 2, pp. 196–207, Mar. 2010.

[45] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behavior & Inform. Technol.*, vol. 33, no. 3, pp. 237–248, Aug. 2014.

[46] J. Holdsworth and E. Apeh, "An effective immersive cyber security awareness learning platform for businesses in the hospitality sector," in *Proc. 25th IEEE Int. Requirements Engineering Conf. Workshops (REW '17),* Lisbon, Portugal, Sep. 2017, pp. 111–117.

[47] K. Korpela, "Improving cyber security awareness and training programs with data analytics," *Inform. Security J.: A Global Perspective*, vol. 24, no. 1–3, pp. 72–77, Jun. 2015.

[48] M. Junger, L. Montoya, and F. J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Comput. Human Behavior*, vol. 66, pp. 75–87, Jan. 2017.

[49] R. Butler, "Investigation of phishing to develop guidelines to protect the internet consumer's identity against attacks by phishers," *South African J. Inform.Manage.*, vol. 7, no. 3, Sep. 2005.

[50] W. Rocha Flores and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," *Comput. & Security*, vol. 59, pp. 26–44, Jun. 2016.

[51] M. E. Whitman, " In defense of the realm: understanding the threats to information security," *Int. J. Inform. Manage.*, vol. 24, no. 1, pp. 43–57, Feb. 2004.

[52] J. Merete Hagen, E. Albrechtsen, and J. Hovden, "Implementation and effectiveness of organizational information security measures," *Inform. Manage.& Comput. Security*, vol. 16, no. 4, pp. 377–397, 2008.

[53] Q. Ma, M. B. Schmidt, and J. M. Pearson, "An integrated framework for information security management," *Rev. Bus.*, vol. 30, no. 1, p. 58, 2009.

[54] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: An action research study," *MIS Quarterly*, pp. 757–778, 2010.

[55] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Comput. & Security*, vol. 29, no. 4, pp. 432–445, Jun. 2010.

[56] M. Siponen, M. A. Mahmood, and S. Pahnila, "Employees' adherence to information security policies: an exploratory field study," *Inform. & Manage.*, vol. 51, no. 2, pp. 217–224, 2014.

[57] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523–548, 2010.

[58] P. Kathryn, M. Agata, P. Malcolm, B. Marcus, and J. Cate, "A study of information security awareness in Australian government organisations," *Inform. Manage. & Comput. Security*, vol. 22, no. 4, pp. 334–345, 2014.

[59] A. Wilk, "Cyber security education and law," in *Proc. IEEE Int. Conf. Software Science, Technology and Engineering (SWSTE '16)*, Beer-Sheva, Israel, Jun. 2016, pp. 94–103.

[60] X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen, and A. Seeam, "Pervasive eHealth services a security and privacy risk awareness survey," in *Proc. Int. Conf. Cyber Situational Awareness, Data Analytics and Assessment (CyberSA '16),* London, UK, Jun. 2016, pp. 1–4.

[61] R. Alavi, S. Islam, and H. Mouratidis, "Human factors of social engineering attacks (SEAs) in hybrid cloud environment: Threats and risks," in *Proc. Int. Conf. Global Security, Safety, and Sustainability*, London, UK, Sep. 2015, pp. 50–56.

[62] C. Colwill, "Human factors in information security: The insider threat–who can you trust these days?," *Inform. Security Tech. Rep.*, vol. 14, no. 4, pp. 186–196, Nov. 2009.

[63] N. F. Doherty, L. Anastasakis, and H. Fulford, "The information security policy unpacked: A critical study of the content of university policies," *Int. J. Inform. Manage.*, vol. 29, no. 6, pp. 449–457, Dec. 2009.

[64] H. Mouratidis, H. Jahankhani, and M. Z. Nkhoma, "Management versus security specialists: An empirical study on security related perceptions," *Inform. Manage. & Comput. Security*, vol. 16, no. 2, pp. 187–205, 2008.

[65] K. J. Knapp, T. E. Marshall, R. Kelly Rainer, and F. Nelson Ford, "Information security: management's effect on culture and policy," *Inform. Manage. & Comput. Security*, vol. 14, no. 1, pp. 24–36, 2006.

[66] E. McFadzean, J.-N. Ezingeard, and D. Birchall, "Perception of risk and the strategic impact of existing IT on information security strategy at board level," *Online Inform. Rev.*, vol. 31, no. 5, pp. 622–660, 2007.

[67] J. L. Spears and H. Barki, "User participation in information systems security risk management," *MIS Quarterly*, pp. 503–522, Sep. 2010.

[68] M. Siponen and A. Vance, "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS Quarterly*, pp. 487–502, 2010.

[69] F. Cervone, "Understand the big picture so you can plan for network security," *Comput. in Libraries*, vol. 25, no. 3, pp. 10–15, 2005.

[70] D. Tse, Z. Xie, and Z. Song, "Awareness of information security and its implications to legal and ethical issues in our daily life," in *Proc. IEEE Int. Conf. Industrial Engineering and Engineering Management (IEEM '17)*, 2017, pp. 1236–1240.

[71] K. Beckers and S. Pape, "A serious game for eliciting social engineering security requirements," in *Proc. 24th IEEE Int. Conf. Requirements Engineering (RE '16)*, Beijing, China, Sep. 2016, pp. 16–25.

[72] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Game based cybersecurity training for high school students," in *Proc. 49th ACM Tech. Symp. Comp. Sci. Educ. (SIGCSE '18)*, Baltimore, MD, Feb. 2018, pp. 68–73.

[73] L. Decker, "Factors affecting the security awareness of end-users: A survey analysis within institutions of higher learning," PhD dissertation, School of Bus. & Technol., Cappella Univ., Minneapolis, MN, 2008.