EPiC Series in Education Science

Volume 5, 2023, Pages 69–78

Proceedings of NEMISA Digital Skills Conference 2023: Scaling Data Skills For Multidisciplinary Impact

Factors Contributing to Cybersecurity Awareness, Education and Training

Prince Zaqueu[1] and Tendani Mawela[1]

[1] University of Pretoria, Hatfield, South Africa

u16232683@tuks.co.za, tendani.mawela@up.ac.za

Abstract

This paper aims to identify the contributing factors for successful cybersecurity awareness, education, training, programs. The study adopted the systematic literature review method and included 58 primary studies. The study explores approaches for cybersecurity awareness, education and training to improve cybersecurity skills and practice in the extant literature. The study noted several recommendations towards effective cybersecurity awareness, education and training programs. These include considerations focused on the importance of assessing the awareness levels of users, selection of pedagogical approaches, design of the curriculum and supporting organisational and demographic aspects.

Keywords: Digital Skills, Cybersecurity, Cybercrime, Awareness, Education, Training

1 Introduction

The past few decades have seen an increasing reliance on information and communication technologies (ICT's) and the internet throughout various sectors of society. With this growing reliance on technology there has also been an upsurge in cyber threats and cyber related crimes (Muthuppalaniappan & Stevenson, 2021). Additionally, it is noted that during the recent COVID-19 pandemic an increasing number of organisations shifted to digital modes of operation due to the social distancing requirements (Naidoo, 2020). Consumers have also progressively accepted more online formats of shopping, education, entertainment and digital communication channels as their new normal. It is evident that the internet permeates many areas of society (Akdemir & Lawless, 2020). The context of the COVID-19 pandemic also further exacerbated the challenges faced with cyber related crimes (Naidoo, 2020) (Muthuppalaniappan & Stevenson, 2021). Even as we enter a post-pandemic phase the trend in people falling prey to cybercrimes continues on an upward trajectory (Monteith, et al., 2021). Literature reports that the human elements are a dominant component of cybersecurity since people's behaviours, personality traits, online activities, and attitudes towards technology impact their

vulnerability online (Monteith, et al., 2021). The human aspects are the main facilitator of victimisation in cybercrime (Akdemir & Lawless, 2020) and humans are often referred to as the weakest link in cybersecurity (Aldawood & Skinner, 2018). The literature highlights that one of the ways to fight cyber related crimes and particularly address weaknesses related to the human element is to increase awareness, education and training programmes (Bele, Dimc, Rozman, & Jemec, 2014) (Aldawood & Skinner, 2018). This study sought to understand the contributing factors for successful cybersecurity awareness, education, training, and skills programs as reported in the extant literature. The study adopted the systematic literature review (SLR) method to identify awareness, training and education approaches that may support safer cybersecurity practices, reduce cybersecurity incidents and cyber related crime.

2 Cybersecurity Overview

Cybersecurity is defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies" that are used to protect users from cybercrimes (Von Solms & Van Niekerk, 2013). Cybersecurity can also be understood as securing hardware, software, data and information that exists in an online system from various types of breach (Tirumala, Valluri, & Babu, 2019).

Cybercrime is a broad term and encompasses criminal activity involving computers or computer networks. Examples of cybercrimes range from advanced fee fraud scams and general online confidence schemes to unauthorized access and copyright infringement. Despite continuous intervention by private institutions and governments to curb the rise of cyber criminality, millions of people worldwide are continuing to be negatively affected by cybercrimes annually, due to increasing digital interconnectivity. Cybersecurity awareness, education, and training are three areas that can be considered to improve a user's cybersecurity detection and prevention competencies and skills (Holdsworth & Apeh, 2017).

2.1 Impact of Cybercrime

There are various types of cybercrime that organisations may suffer as identified by (Paoli, Visschers, & Verstraete, 2018) and these include: the illegal access to IT systems, cyber espionage, data or system interference, cyber extortion and internet fraud. Individuals are increasingly becoming targets of phishing attacks resulting in billions of dollars lost annually (Jensen, Dinger, Wright, & Thatcher, 2017). Individuals can be attacked by malware, trojans, ransomware, identity theft and loss of sensitive information such as credit card details or passwords. Organisations on the other hand suffer losses due to cybercrime which can be related to: material costs (e.g. damage to infrastructure), personnel costs (the time spent by employees addressing the cyber incidents), hardware and software replacement, loss of assets, revenues lost, reputational harm and loss of privacy (Paoli, Visschers, & Verstraete, 2018).

Approximately 15 million data records were exposed worldwide through data breaches over the 3rd quarter of 2022 representing a 37% increase from the previous quarter (Statista, 2022). There is a concern that these trends will continue to grow. Governments from around the world have observed the destruction caused by cybercrimes and are continuously trying to combat these activities. Government approaches for combating cybercrimes vary but generally involve collaborating with other governments and agencies to better police the wide geographical reach of the crimes; and criminalizing cybercrimes broadly to discourage the behaviour (Broadhurst, 2006). Organisations and institutions also implement special protection and securities to reduce system vulnerabilities, but it is still almost impossible to

prevent cyberthreats, especially from a global perspective (Broadhurst, 2006). Although the increasing policing, regulations and security advances assist in mitigating and preventing some of the damage caused by cyber criminals, cybercrime continues to be a burdening issue affecting millions of people, organisations, and governments every year. A significant contributing factor to the prevalence of cyber security is vulnerabilities in systems and as well as in people (Platsis, 2019).

2.2 Cybersecurity Awareness, Education and Training

Cybersecurity awareness is the understanding and awareness of cybersecurity threats to enhance a person's ability protect themselves against cyber-attacks in the online context (Muhirwe & White, 2016). It is the ability of being mindful and alert by performing tasks in a secured manner when utilizing a computer or mobile device. The factors that contribute to cybersecurity awareness are the users knowledge, attitude and behaviours (Muhirwe & White, 2016). Efforts towards user awareness and ongoing education are both considered essential in the fight against of cyber threats (Smyth, Curran, & McKelvey, 2019). Awareness, educational programmes and training can drive an effective and appropriate cybersecurity culture (Smyth, Curran, & McKelvey, 2019).

The goal of cybersecurity education and training is to instill long lasting skills and change behaviours . However, it is noted that organisation may find that implementing effective cybersecurity education and training is challenging. Cybersecurity education should assist users in understanding various concepts (Javidi & Sheybani, 2018) and additionally it should be targeted such that it helps users stop old behaviours and adopt new practices aligned with internet safety (Smyth, Curran, & McKelvey, 2019).

3 Research Method

The study adopted the SLR method and aimed to address the following research question: "what are the contributing factors for effective cyber security education, training, and awareness programs?". The SLR approach is explained below.

3.1 Search, Screening and Selection Process

Journal articles and conference papers for this systematic literature review were searched for using the following key terms: Critical success factors, Cybersecurity, Awareness, Education, Training.

The search was conducted by using the following databases: IEEE Xplore Digital Library; WorldCat Discovery Service; Emerald Insight; ProQuest; and ScienceDirect. The search resulted in 3927 articles that were returned.

These were evaluated against the predefined inclusion and exclusion criteria:

Table 1: SLR Inclusion and Exclusion Criteria

Inclusion Criteria		Exclusion Criteria	
1.	Publications written in the English language.	1.	Publications where only the abstract but not the full text is available.
2.	Publications that presents a method, technique, or process for educating, training, or raising awareness regarding cyber security and cybercrime.	2.	Duplicate papers.
		3.	Publications not relating to cybercrime or cyber security.
3.	Publications that show how education, training, and awareness programs have worked.	4.	Publications focused on technological applications to deter cybercrimes, not

4.	Publications explaining cyber security and cybercrime.		relating to education, training and awareness.
5.	Publications that were published between 2005 and 2020.		

After evaluating the articles 66 eligible articles remained. These were then taken through a quality assessment process.

3.2 Quality Assessment and Data Analysis

A further evaluation of the articles was conducted using the following quality assessment questions:

1. The study details research related to either cyber security education, training and / or awareness programs?
2. The study discusses factors necessary for the successful implementation of cyber security education, training, and awareness programs clearly?
3. Does the article specify/discuss the research design and justify the appropriateness of the research design/methodology?

A scoring system for each question was adopted as follows: 1 point for yes, 0.5 points for partly and 0 points for no. The scoring of the articles was done to assist in weighing the importance of the studies identified during the primary study selection and ensuring that the results of the selected studies would be appropriate to answer the research question. This resulted in a final set of 58 papers that were used in the SLR analysis and discussion. The data from the studies (articles) was analysed using the thematic analysis approach as per the guidelines of Maguire and Delahunt (2017) with the aim of identifying factors contributing to cybersecurity awareness, education and training to support appropriate skills and behaviour.

4 Findings and Discussion

The following sections discuss the factors that may be considered for successful cybersecurity awareness, education, training, and skills programs.

4.1 Assessing Cybersecurity Awareness

The first theme and contributing factor is related to assessing the cybersecurity awareness of users. It is vital to ensure that the attendees of the awareness programs are categorized so that the correct awareness message is directed towards the right participants (Rahim, Hamid, Mat Kiah, Shamshirband, & Furnell, 2015) (Shah, Jones, & Choudrie, 2019) (Takata & Ogura, 2019). Thus, before developing a cybersecurity education, training, and awareness program, it is important to assess individuals and tailor the programs for the users perceived vulnerabilities. By changing the behaviour of individual users, the entire organisational approach to cybersecurity can improve (Chen, Dawn Medlin, & Shaw, 2008).

There are multiple methods used to assess cybersecurity awareness such as: survey- based questionnaires, vocabulary tests, observations, gaming tools, focus groups, direct classroom training, text-based training, discussions in teams, interviews, accessing user responses to emails, document reviews, and elements of situational awareness, which uses scenario-based content to bring security threat awareness to the users (Chen, Dawn Medlin, & Shaw, 2008). These methodologies should be combined as appropriate for the context since as it will better determine user's awareness and allow for

a more focused education and training intervention (Bishop , et al., 2017) (Sari & Prasetio, 2017) (Tschakert & Ngamsuriyaroj, 2019).

Users should be assessed based on their vulnerabilities in cybersecurity awareness and education as generic, non-customised training has its drawbacks. The education and training should be based on the person or groups actual responsibilities and use of the internet (Aldawood & Skinner, 2019).

4.2 Pedagogical Approaches

There are two broad types of training which are computer-based training and instruction-led training. Computer-based training can be conducted via training videos, guided instructions, interactive applications, web-based courses, and it may use assessments, quizzes, and mini-challenges to assess the trainee's knowledge (Ghafir, et al., 2018). The advantages of computer-based training are that it is a cost-effective training method, that is easy to deliver and has a flexible structure that provides easy access to information. Unfortunately, computer-based training does not provide sufficient support or help and can also feel redundant for a skilled trainee (Ghafir, et al., 2018). Instruction-led training has proven to be a very effective method for behaviour development. This method of training can be structured as training events or workshops (Ghafir, et al., 2018). This approach is effective because it is tailored towards the security needs of the organisation or trainees and there is an opportunity for immediate feedback and face to face communication. Instruction-led training is however costly and often requires a lengthy amount of time to deliver.

Training may also be introduced through a phased approach consisting of two phases. The first phase involves creating awareness and giving users knowledge of common and modern cybersecurity threats they may face, the ability to distinguish between these cybersecurity threats, and the ability to identify phishing emails and fake websites (Frauenstein & von Solms, 2014). The second phase is to train the users and provide them with the competencies needed to use the technological controls that assist in combatting phishing attacks (Frauenstein & von Solms, 2014).

Individual security awareness training programs help users to improve the way they protect themselves from cyber threats and report any security violations they may witness (Hagen, Albrechtsen, & Ole, 2011) (McCrohan, Engel, & Harvey, 2010). These awareness programs do not last indefinitely in the users' memory, so they should be performed regularly as opposed to once-off. It is also effective to incorporate cybersecurity education in the schooling system and institutions of higher learning as it allows young students to be aware of cybersecurity issues (Ahmed, et al., 2019) which can be taken forward into their personal lives and careers.

Another approach that may be considered is gamification. Gamification, in the context of cybersecurity training, is a technique that uses game design and game principles to provide cybersecurity education. Gamification is a tool that allows e-learning to be interesting and engaging thus capturing the user's full attention and leading to better retention (Holdsworth & Apeh, 2017). The benefits of this technique are that there is direct communication, in that, the need for user participation and feedback are highlighted in the game design, thus improving the results with regards to changes in users cybersecurity awareness and behaviour in an appealing and enjoyable manner (Alotaibi, Furnell, Stengel, & Papadaki, 2017) (Tioh & Mina, 2015).

This approach of active engagement greatly improves the retention of knowledge amongst the trainees and the game design additionally allows for flexibility and inclusivity in any topic (Alotaibi, Furnell, Stengel, & Papadaki, 2017) (Labuschagne, Veerasamy, Burke, & Eloff, 2011). Gamification also improves richness of the information. The richness of security awareness information refers to the

various forms of media that can be used, such as hypermedia, multimedia, and hypertext. The use of these media types allows for training material to be presented visually and highlight critical concepts and the relationships between the concepts clearly (Labuschagne, Veerasamy, Burke, & Eloff, 2011).

Gamification usually works by simulating cybersecurity threats. The scenarios typically include topics such as identity theft, password management, dealing with worms and trojans, filters, patches, and working with links (Labuschagne, Veerasamy, Burke, & Eloff, 2011). In the training environment, anytime a risk is identified the application shows short, eye catching tutorials, that explain the problem concisely (Kirlappos & Sasse, 2012). Game-based learning is noted as an effective approach. The effect of structuring the knowledge and education in the appearance of a game, makes it easier for adoption (Tioh & Mina, 2015). Games generally have a short feedback cycle and so users would get their penalties or rewards quickly, reinforcing the concepts (Tioh & Mina, 2015). Gamification is a valuable and critical technique to incorporate into a cybersecurity awareness, training and education program.

4.3 Curriculum Considerations

These programs should teach concepts that address a wide range of cybersecurity threats and the curriculum should be tailored to the user's needs. Awareness topics are classified into novice/beginner, intermediate, and advanced levels and users are assessed on each level. Awareness training should not only be limited to computers but also mobile phones and any interaction users may have on the internet (Zeybek, Yilmaz, & Alper Dogru, 2019).

The following cybersecurity training topics should be included in programs:

- Password usage and management. Techniques to crack passwords are getting more sophisticated and teaching proper password management and frequent changing is essential (Nagarajan, Allbeck, Sood, & Janssen, 2012).
- Protection from malware and spam. A complete program must cover topics of the use and maintenance of anti-virus and anti-malware tools (Nagarajan, Allbeck, Sood, & Janssen, 2012).
- Teaching patch management. Patch management is very critical as patches fix security faults in the software (Nagarajan, Allbeck, Sood, & Janssen, 2012).
- Social engineering prevention. Social engineering techniques are a big threat to security systems because they focus on the human element and do not get prevented by tools and software. Awareness can only be achieved through regular cybersecurity training programs that focus on social engineering techniques that are employed by cyber criminals (Nagarajan, Allbeck, Sood, & Janssen, 2012).
- Behavioural cybersecurity, game theory and risk management is also recommended to be in the curriculum (Patterson, Winston, & Fleming, 2016).
- Online self-efficacy is an individual's belief in their ability to detect and mitigate cybersecurity threats. Online self-efficacy can be increased by training and is thus a key topic (Teimouri, Benrazavi, Griffiths, & Hassan, 2018).

It is very important that users are provided with continuous information about the topics on a regular basis, as continuous exposure creates true understanding of the cybersecurity topics (McCrohan, Engel, & Harvey, 2010). Thus the curriculum needs to be updated regularly to reflect current threats.

4.4 Organisational and Demographic Aspects

To have a successful cybersecurity awareness programs, there are a few key attributes that must be incorporated into the program. These attributes include: ensuring support from top management, aiming for a creative, fun, and interesting learning process, and ensuring that content is relevant to the audience that is receiving it. Additionally clear content and explanations of the impact of the cybersecurity threats, and the use of different kinds of media, reward systems for users, continuously reminding the users of what they have learnt, and making sure there is a way to measure the effect and impact that the program are important factors (Sari & Prasetio, 2017).

The language, gender, lifestyles, and ethnicity of the users also need to be considered as this impacts the adoption of the cybersecurity initiatives (Alarifi, Tootell, & Hyland, 2012) (Aldawood & Skinner, 2019). The user's computer experience also has a significant impact on their cybersecurity awareness (Rocha Flores, Holm, Svensson, & Ericsson, 2014). Special consideration must be given to these factors, especially language, as users have higher cybersecurity awareness when they are assessed in their mother tongue (Kruger, Flowerday, Drevin, & Steyn, 2011). In the case of the adoption of security controls, particularly in mobile phones, one study noted that female users tend to have a lower awareness and adoption than male users (Parker, Ophoff, Van Belle, & Karia, 2015).

5 Conclusion

Several success factors needed for cybersecurity awareness, training, and education were identified in this study. This systematic literature review search resulted in 3927 articles, and through a screening and data quality assessment, identified 58 articles that discuss key considerations for developing and implementing cybersecurity awareness, training, and education programs. The key considerations focused on the importance of assessing the awareness of users, selection of appropriate pedagogical approaches, design of the curriculum and supporting organisational and demographic aspects. The factors identified in this SLR may be used to inform the creation of cybersecurity awareness, training, and education programs towards building the skills and competencies of internet users. By incorporating the factors identified in this review, educators may create programs that benefit users of the cyberspace.

References

Ahmed, N., Islam, M., Kulsum, U., Islam, M., Haque, M., & Rahman, M. (2019). Demographic Factors of Cybersecurity Awareness in Bangladesh. . *2019 5th International Conference on Advances in Electrical Engineering (ICAEE)* (pp. 685–690). Dhaka,: IEEE.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. *Internet Research, 30*(6), 1665-1687.

Alarifi, A., Tootell, H., & Hyland, P. (2012). A study of information security awareness and practices in Saudi Arabia. *2012 International Conference on Communications and Information Technology* (pp. 6-12). Hammamet: IEEE.

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)* (pp. 62-68). Wollongong, Australia: IEEE.

Aldawood, H., & Skinner, G. (2019). Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. *2019 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 111-117). Melbourne: IEEE.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2017). Enhancing cyber security awareness with mobile games. *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 129–134). Cambridge: IEEE.

Bele, J. L., Dimc, M., Rozman, D., & Jemec, A. S. (2014). Raising Awareness of Cybercrime--The Use of Education as a Means of Prevention and Protection. *10th International Conference Mobile Learning 2014* (pp. 281-284). Madrid: International Association for the Development of the Information Society.

Bishop , M., Burley , D., Buck , S., Ekstrom , J., Futcher , L., Gibson , D., . . . Parrish , A. (2017). Cybersecurity Curricular Guidelines. In L. F. M. Bishop (Ed.), *IFIP World Conference on Information Security Education. 503*, pp. 3-13. SPRINGER.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*.

Carlisle, D. (2010, April). *graphicx: Enhanced support for graphics.* Retrieved from http://www.ctan.org/tex-archive/ help/Catalogue/entries/graphicx.html

Chen, C. C., Dawn Medlin, B., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security, 16*(4), 360–376.

Frauenstein, E., & von Solms, R. (2014). Combatting phishing: A holistic human approach. *Information Security for South Africa 2014* (pp. 1-10). Johannesburg: IEEE.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., . . . Baker, T. (2018). Security threats to critical infrastructure: The human factor. *The Journal of Supercomputing : An International Journal of High-Performance Computer Design, Analysis, and Use, 74*(10), 4986–5002.

Hagen, J., Albrechtsen, E., & Ole, J. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security, 19*(3), 140–154.

Holdsworth, J., & Apeh, E. (2017). An Effective Immersive Cyber Security Awareness Learning Platform for Businesses in the Hospitality Sector. *25th International Requirements Engineering Conference Workshops (REW)*, (pp. 111–117). IEEE.

Holdsworth, J., & Apeh, E. (2017). An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)* (pp. 111-117). IEEE.

Javidi, G., & Sheybani, E. (2018). K-12 cybersecurity education, research, and outreach. *2018 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). San Jose, CA, USA: IEEE.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, 597-626.

Kirlappos, I., & Sasse, M. (2012). Security Education against Phishing: A Modest Proposal for a Major Rethink. *Security & Privacy, 10*(2).

Kruger, H., Flowerday, S., Drevin, L., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *2011 Information Security for South Africa (ISSA)* (pp. 1-7). Johannesburg: IEEE.

Labuschagne, W., Veerasamy, N., Burke, I., & Eloff, M. (2011). Design of cyber security awareness game utilizing a social media framework. . *2011 Information Security for South Africa (ISSA)* (pp. 1-9). Johannesburg: IEEE.

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education, 9*(3).

McCrohan, K., Engel, K., & Harvey, J. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce, 9*(1), 23–41.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports, 23*(18), 1-9.

Muhirwe, J., & White, N. (2016). Cybersecurity Awareness and Practice of Next Generation Corporate Technology Users. *Issues in Information Systems, 17*(2).

Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care, 33*(1), 1-4. doi:10.1093/intqhc/mzaa117

Nagarajan, A., Allbeck, J., Sood, A., & Janssen, T. (2012). Exploring game design for cybersecurity training. . *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)* (pp. 256– 262). Bangkok: IEEE.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems, 29*(3), 303-321.

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. *Crime, Law and Social Change, 70*(4), 397-420.

Parker, F., Ophoff, J., Van Belle, J.-P., & Karia, R. (2015). Security awareness and adoption of security controls by smartphone users. *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)* (pp. 99–104). Cape Town: IEEE.

Patterson, W., Winston, C., & Fleming, L. (2016). Behavioral Cybersecurity: A needed aspect of the security curriculum. *SoutheastCon 2016* (pp. 1-7). Norfolk: IEEE.

Platsis, G. (2019). The human factor: Cyber security's greatest challenge. *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, 1-19.

Rahim, N. H., Hamid, S., Mat Kiah, M. L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes, 44*(4), 606-622.

Rocha Flores, W., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security, 22*(4), 393–406.

Sari, P., & Prasetio, A. (2017). Knowledge sharing and electronic word of mouth to promote information security awareness in social network site. *International Workshop on Big Data and Information Security (IWBIS)*, (pp. 113-117).

Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: Promising organisational practices. *Information Technology & People, 32*(5), 1125–1129.

Smyth, S. J., Curran, K., & McKelvey, N. (2019). The Role of Education and Awareness in Tackling Insider Threats. In I. Vasileiou, & S. Furnell, *Advances in Information Security, Privacy, and Ethics (AISPE) Book Series* (pp. 33-51). IGI Global.

Statista. (2022, November 29). *Number of data records exposed worldwide* . Retrieved from https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/

Takata, T., & Ogura, K. (2019). Confront Phishing Attacks—From a Perspective of Security Education. *2019 IEEE 10th International Conference on Awareness Science and Technology (ICAST)* (pp. 1-4). IEEE.

Teimouri, M., Benrazavi, S., Griffiths, M., & Hassan, M. (2018). A Model of Online Protection to Reduce Children's Online Risk Exposure: Empirical Evidence From Asia. *Sexuality & Culture : An Interdisciplinary Quarterly, 22*(4), 1205–1229.

Tioh, J., & Mina, M. (2015). Digital defenders: Computer security literacy via game- based learning. *2015 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). IEEE.

Tirumala, S. S., Valluri, M. R., & Babu, G. A. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. *2019 International Conference on Computer Communication and Informatics.* Coimbatore: IEEE.

Tschakert , K., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon, 5*(6).

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, *38*, 97-102.

Zeybek, M., Yilmaz, E., & Alper Dogru, I. (2019). A Study on Security Awareness in Mobile Devices. . *2019 1st International Informatics and Software Engineering Conference (UBMYK)* (pp. 1-6). Ankara: IEEE.