Diving Deep into Human Centric Issues within Cyber Security

Kalpit Jadhav[1,2], Sherif Haggag[3] and Hussein Haggag[4]

[1]The University of Adelaide, Adelaide, Australia
[3]The University of Adelaide, Adelaide, Australia
[4]Umeå University, Sweden

Abstract

Computer security is more than just about the technological systems; it also relates to the people that use the systems and how their different behaviours may be exploited. Organizations are prone to security breaches, which sometimes are caused by human error. As a result, organizations should seek to improve their employees' knowledge about cyber security and their capability to engage in secure cyber behaviours. It is possible to target groups ranging from basic users who need some basic understanding of the current threat environment and how to utilize the associated preventive mechanisms, to security experts who need practical exposure in responding to security incidents. Risk-taking preferences, decision-making styles, demographics, and personality characteristics, such as gender, age, culture and emotions, have been found to significantly affect the predictive ability of good security behavior. How gender and age mediate the influences on cyber security beliefs and behaviours among employees is quite interesting. Using behavioural cyber security and human factors to provide insight into relevant theories and principles, this paper proposes an interdisciplinary framework that combines these disciplines.

Keywords

cyber security, human factors, social engineering, framework

1. Introduction

Humans play an important role in security measures, thus research on security-related decisions and actions based on human "information-processing and decision-making principles" is necessary [1]. Cyber security's "human factors" are concerned with the role that human behaviour plays in preventing and responding to cyberattacks [2]. Additionally to cyberattacks aimed at targeting network infrastructures, a variant of cyberattack, designed specifically to exploit the vulnerabilities of individuals; these are social engineering attacks [2]. Social engineering aims to obtain illegal access to sensitive and confidential information by manipulating individuals' psychological states [3]. Because employees can contribute to protect the interests of organizations in the face of social engineered attacks, organizations find the need to implement information security awareness programs to secure their data [3]. Understanding the security behaviour of both men and women, and whether their security behaviours are similar or different, is essential to developing effective cyber security programs for the workplace [4]. In addition to training materials, policies and frameworks, information about preventive measures to be followed before and after an attack must also be undertaken.

The age, gender, or cultural background may make a person more susceptible to some malicious act [5, 6]. Researchers have found that women are more likely to fall victim to phishing scams than men, and so are people between 18 to 25 years of age [7]. In order to combat such limitations and biases, companies should establish clear security guidelines and educate their employees about them. Organizations can achieve satisfying results in response to social engineering attacks by improving their information security frameworks including the training and awareness programs.

In this research we aim to address the two key research questions:

RQ1 – What factors that influence human susceptibility to cybercrime and social engineering attacks are reported in the peer reviewed literature?

Individuals are more susceptible to social engineering attacks for a variety of reasons. In general, social engineering attempts appear more effective if the attacker is able to establish trust with the victim, putting them at greater risk [8]. Individual factors or personality traits can also increase the likelihood of someone falling victim to social engineering attacks. It is possible to increase the effectiveness of phishing emails and illegitimate websites by using a number of strategies. In

Asia-Pacific software engineering and diversity, equity, and inclusion (APSEDEI), Japan, Nov. 15-21, 2022

*Corresponding author.
†These authors contributed equally.
kalpit1612kpj@gmail.com (K. Jadhav);
sherif.haggag@adelaide.edu.au (S. Haggag);
hussein.haggag@umu.se (H. Haggag)
0000-0002-XXXX-XXXX (K. Jadhav); 0000-0001-XXXX-XXXX (S. Haggag); 0000-0002-XXXX-XXXX (H. Haggag)

this research, we highlight the various human factors that can make an individual more susceptible to attack as reported in the academic literature.

RQ2 – Why do we need a personalised cyber security framework for training employees within an organisation?
Personalized cyber security frameworks will enhance the existing security protocols and methodologies followed during training and will incorporate new security layers which will consider even the human factors that impact an individual's cyber behaviour and awareness.

Section 2 of this research highlights the aims and challenges that this paper intends to overcome. Section 3 presents literature review studied from different research papers in order to formulate results. The design and plan followed in this research has been presented in section 4. The results identified and formulated have been explained and tabulated in section 5.

2. Aims and challenges

Training and awareness programs present several challenges such as "business environmental, social, constitutional, organizational, economical, and personal". 'Trusting nature of humans' is another factor that hinders awareness and training programs against social engineering is a low level of interest found within the personnel. Moreover, problem with modern training techniques is that they take a lot of time and even lack training budget [3].

The absence of cybercrime, which is instrumental in exploiting both the vulnerabilities of systems and human weaknesses, is one of the biggest obstacles to implementing digital transformation strategies. Employees must be provided with the proper training in order for them to be able to recognize, flag, evade, and disable malicious attacks [3]. To upgrade the cyber security training programmes more human centric, an awareness or training framework must be implemented for all personnel, which include the major cyber risk aspects and its awareness factors [5].

There is a need to investigate the similarities and differences between men and women with regard to cyber security beliefs and behaviours like personality, cultural background, emotion reaction, age, and motivation.

3. Literature review

Hatzivasilis et al. in [5], describe a methodology to adapt cyber security training programmes dynamically. They mention how a trainee consumes the primary teaching materials such as lectures, tutorials, videos, etc. and goes on to more advanced learning methods which involve multiple hands-on exercises on emulated/simulated components [5]. The performance is evaluated and a preliminary application is presented, where a training programme for smart shipping personnel is established [5].

Factors that may help overcome the difficulties posed by implementing a training and awareness program against social engineering are studied in research by Aldawood and Skinner [3]. The authors describe the need of information security training and awareness programs is to harness employees with skills to identify, disable, and report any social engineering attempts to misuse their resources. The study also makes recommendations based on the viewpoint of security decision makers within organizations on how to address challenges [9, 10, 11, 12].

Key issues faced by cyber security training and awareness programs have been identified in research by Korpela [7] and the probable benefits that can be derived by combining existing data sources to enhance these programs using learning analytics which is an upcoming field in data analytics has been explained. The author even mentions that in order to potentially improve cyber security metrics, organizations and professionals should harness the use of data analytics to tackle the issues of how users fail to identify risks and a 'lack of understanding on how cyber security is best learned by its users [7].

Importance of putting in place formal educational and training standards to enable organisations to manage human factors related to cyber security effectively has been highlighted in the research of Nifakos et al [2], ultimately reducing cyber risks. The research examined human factors, but a systematic methodology for harmonising the research findings should be developed to allow cyber security experts to objectively evaluate these findings in order to support securing the IT infrastructure of healthcare facilities in future research [2].

How an interdisciplinary approach based on a human factors approach can contribute to the science of security has been conveyed in the research of Proctor and Chen [1]. The authors describe the importance of human factors in security by using two examples that illustrate the contribution of a scientific approach to security detection of phishing attacks and the selection of mobile applications [1]. Finally, they conclude that in order to contribute to cyber security, human factors experts should utilize their existing knowledge of applied information processing and decision making [1].

Methods for measuring, quantifying, and evaluating human organizations' security posture, especially those within large corporations and government organizations have been investigated by Brian et al in their research [13]. The study presents the results of two rounds of experiments conducted at Columbia University using bo-

gus phishing emails to train approximately 4000 staff and students [13]. The authors further suggest that it is possible to train users using decoy technology to anticipate possible threats, and the measurements can be applied to multiple organizations in order to gauge their security posture as compared to each other [13].

Correlation of human characteristics with cyber security behaviour intentions has been researched by Gratian et al [14]. The study estimated that 5 to 23 percent of the variance in the reported cyber security behaviour intentions was attributable to individual differences based on demographic factors, personality traits, risk-taking preferences, and decision-making styles in 369 students, faculty, and staff at a large public university [14].

The purpose of study by Anwar et al. [4] was to investigate the effect of gender as a deciding variable in the relationship among the psychosocial factors and self-reported cyber security behaviours among staff of diverse organizations. The results of this study indicate statistically significant differences between men and women in terms of computer skills, prior experience, cues-to-action, and security self-efficacy. Self-efficacy among women is significantly lower than that among men, so they could be possibly targeted for intervention [4]. Thus, they conclude that by addressing the relevant constructs of the cyber security behaviour, we can develop gender-specific cyber security training and interventions to improve employees' attitudes and behaviour [4].

Human factor is one of the major contributors to the vulnerabilities of an information system, and disparate attack vectors which are being utilized today to exploit human weaknesses have been examined in research by Radu et al [15]. The authors further state that a social engineering awareness and training program must ensure that employees have a basic understanding of how social engineering attacks are conducted [15]. Furthermore, employees must have the knowledge and training necessary to detect an attack, respond appropriately, and find a way to prevent exposure to social engineering threats [15].

Review of relevant theories and principles which provide insight through an interdisciplinary framework that encompasses human factors, behavioural cyber security, and modelling and simulation has been carried out Maalem et al [16]. The authors mention that it is important to customize cyber awareness training to employees considering their different credentials and levels of access. They further state that employees need to be trusted, but they must also be taught technology and cyber awareness, and compliance needs to be verified [16].

An extensive financial institution in Thailand conducted study in research by Daengsi et al. [17] to assess cyber security awareness among approximately 20,000 employees. An initial phishing attack was conducted where knowledge transfer was achieved and followed by a second phishing attack that had different content [17]. According to the results of the study, gender plays a significant role in cyber security awareness within the Thai cyber ecosystem since Thai female employees have a higher level of cyber security awareness than male employees as well as the differences between the ages of Thai users' cyber security awareness [17]. Although this research is just limited to Thai employees but can be considered in general sense too.

By identifying effective ways to encourage cyber security education development and address gender gaps in the cyber security workforce, the overall goal in study by Amo et al. [18] is to contribute to the literature on cyber security education. Their findings indicate that female students were significantly more engaged and efficacious in cyber security, which is quite promising in regards to gender gaps in cyber security [18].

The study by Gillam and Waite [19] sought to identify the psychological factors that influence workplace IT end users' motivation to learn about cyber awareness and avoid threats. As a result of this study, gender-related considerations were revealed that can be used to guide cyber security training of IT end-users such as threat avoidance in human resource development contexts, especially when it comes to motivation [19].

Study of 'Gender and locale differences in cybercrime awareness among adolescents' was conducted by Thakur and Kaur [20]. The findings showed that there were significant gender differences between rural and urban young males and young females in terms of cybercrime awareness.

By bringing together research from unique and diverse disciplinary backgrounds, study by Jeong et al. [21] enables us to increase our understanding and provide a framework for effective cyber security strategies by providing a comprehensive overview of the socio-cultural dimensions of cyber security. This special issue addresses people, culture, and cyber security research that enriches our understanding of them. Following the expert review process, a framework and assessment tool were developed to highlight strengths, weaknesses, and opportunities [21].

The analysis in research by Creese [22] identifies that on the basis of their development and the extent of their Internet use, some countries have demonstrated greater maturity in capacity building than were expected. Through a cross-national and cross-regional comparison of capacity building, this paper shows regional differences are largely influenced by two key national differences in the extent of Internet use and the level of development [22].

A three-part study of people's perceptions of cyber security is presented by Renaud et al [23]. Several aspects of people's lived cyber security experiences were confirmed by the investigation where one blind spot issue

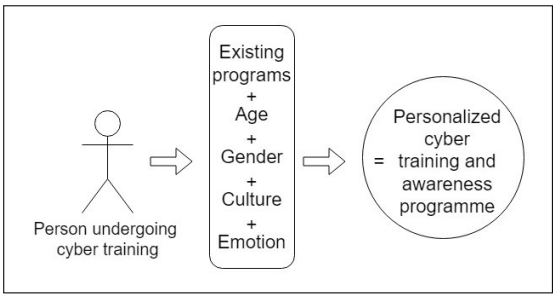

Figure 1: Research design

was identified along with negative attitude of people toward cyber security that are widespread but not universal is studied [23].

Using open-ended responses from a pilot study and congressional debates, research by Cheung-Blunden et al. [24] sought to identify behavioral categories in cyber security solutions. By distinguishing fear, three types of safety behaviors which are avoidance, surveillance and vigilance were identified in this study and were expected to be mutually exclusive because emotion was expected to have unique motivational power [24].

A hacking of one's smart security camera represents one of the most emblematic examples of a cyber security breach, and study by Budimir et al. [25] explored which personality characteristics systematically relate to these processes. An important link between a cyber security breach situation and possible long-term mental health effects was discovered in this study [25].

4. Research plan and Methodology

The research implementation is carried out in two phases. The first phase is about carrying out an in depth analysis and researching into the topic of human centric issues of cyber security. It involves referring of research papers and articles through the use of university library and other platforms. Investigation on the importance of human centric aspects in cyber security, how to build apps and training materials applicable with personality, gender, cultural background, emotion reaction, age, motivation, and hidden biases is carried out. The second phase involves development of a framework which includes the above-mentioned aspects and to provide guidelines as to how the framework can be useful for organizations for carrying out cyber trainings and awareness programmes.

A secondary research methodology is employed in this research, since this study relies on already existing data. Various sources such as published journals and reports in the University library and websites are used for the collection, organization, and analysis of data.

The figure 1 shows that existing cyber training and awareness programs are modified by adding the different human factors which have been mentioned in the paper. This helps to develop a personalised cyber training framework. The framework developed and evaluated would be used to train an individual exhibiting specific human centeric factors to build their cyber awareness.

5. Results

5.1. Gender:

Study has been conducted for cyber risk assessment where as a part of the test, a phishing email offering more Gmail storage was sent by the experts [17]. The data from this test was gathered, processed, and analysed and found that female employees' responses were always lower than those of male employees [17]. It indicates that females have a better level of cyber security awareness of phishing than males [17]. A positive growth pattern in cyber security self-efficacy is observed in females compared to males and females gained more problem-solving proficiency than males over time [18]. While young females have higher mean values than young males in cases where there is a high level of cybercrime awareness, they are ahead in cases of medium levels, and in cases where there is a low level of cybercrime awareness, young females tend to have higher mean values than young males [20].

Males tend to react more aggressively to cyberbullying and have a deeper emotional response in situations of hacking, while females tend to have more intense emotional reactions. Using digital technologies, cyberbullying involves repeated behavior meant to intimidate, anger, or shame the target [26]. Mobile phones, messaging platforms, gaming platforms, and social media platforms can all be used for this [26]. 'Remote sexual abuse' occurs more often against women and girls than men - coerced to pose naked online or stalked via internet [27]. The term cyberstalking means stalking someone through the use of the internet. Stalkers are using email message applications, posting messages on the web, and sometimes even social media, such as Facebook, Instagram, and many more, to continually try to approach someone online without their consent [27].

Based on the observations and results of the studies that have been referred to for this research, the Table 1 shows the things that need to be considered for cyber training specific to an individual's gender.

5.2. Age:

A person's age can also be considered a crucial factor when determining a person's identity, since people at

Table 1
Cyber-awareness required for specific Gender

Identifying as Male	Identifying as Female
Phishing crimes	Phishing crimes
Develop cybercrime awareness	Develop cybercrime awareness
Building self-efficacy	Improving self-efficacy
Generating strong passwords	Generating strong passwords
Awareness of cyberbullying	Awareness of cyberbullying
	Build online sexual abuse awareness
	Awareness against cyber-stalking and cyber-harassment

different stages of life experience different social, organizational and environmental challenges and contexts [17]. Self-efficacy and precautionary behavior were significantly positively correlated with self-efficacy in youngsters, but in older group the correlation was negatively significant, but not statistically significant [19].

Adolescents are most at risk for Cybercrime due to their attraction to the internet [20]. Therefore, adolescents are very much in need of awareness/knowledge related to cybercrime, since failure to do so can harm them financially or emotionally [20]. The teenager is already seeking the truth only through his own experiences, if the child is ready to obey the authority of an adult, this is the age of active knowledge and personal development [28]. Teenagers often commit acts that can lead to undesirable consequences for the simple reason that they try to protect themselves from adults' influence, and they are easy targets for criminals because of their curiosity, openness, and lack of experience [28].

People between 18 and 25 years old are more vulnerable to phishing scams [7]. Every day, college students use the internet for work and pleasure - to complete research for essays and assignments, to stay connected on social media, to make online purchases, and to keep up-to-date on entertainment news [29]. In the age of cybercrime, the sheer amount of data we share online puts us all at risk. It is more likely that young people and college students will fall for fraud scams as they use social media at higher rates than other age groups and are statistically more susceptible to fraud scams [29].

A survey of data protection and privacy professionals found that 66 percent believed their employees were the weakest link in protecting their organizations from cyberattacks [30]. In spite of the automation of tedious cyber security tasks, it's still a good idea to provide employees with online security awareness trainings such as password security, phishing and importance of backing up files to prevent future issues [30].

Table 2
Cyber-awareness required for specific Age

0-18	18-25	25–50	50+
Self-efficacy	Cybercrime awareness	Awareness of phishing	Awareness of phishing
Internet addiction	Internet addiction	Financial attacks	Financial attacks
Fraud attacks	Awareness of phishing	Password security	Knowledge of viruses and software
	Fraud attacks	Backing up files	Fraud attacks
	Knowledge of viruses and software		Password security
	Knowledge of Cyberbullying		

As internet use among seniors increases, the elderly have become more vulnerable to online scams [31]. A majority of seniors don't protect their internet-connected devices with passwords, leaving them vulnerable to those who pick them up [31]. This group is also more likely to be at risk because they share their personal information through social media platforms like Facebook and Twitter, as well as have to use online services and apps to access health care, insurance, housing, voting, financial, and voting services [31].

Based on the observations and results of the studies that have been referred to for this research, the Table 2 shows the things that need to be considered for cyber training specific to an individual's age.

5.3. Culture:

Social identity plays a definite role in how passwords are generated in different countries, with different users' attitudes towards passwords [21]. Cyber security attitudes, values, and practices vary even among countries that share the same values, attitudes, and practices due to differences in development and Internet usage across nations [21]. There is a significant difference between the average maturity stage of Europe and Americas compared with those of other regions, and the difference is large enough, that average maturity stages are the same across all regions [22]. There is no statistically significant difference in the average maturity stage between the African and Asian regions, leading us to conclude that they are approximately equal in maturity [22].

America's national and economic security is at risk from malicious cyber activity [32]. A key objective of the

Table 3
Cyber-awareness required for specific Cultural background

America	Europe	Asia and Africa
Awareness of Ransomware	Awareness of Ransomware and Malware	Awareness of Ransomware
Knowledge of politically motivated attacks	Awareness of politically motivated attacks	Awareness of politically motivated attacks
Awareness of Business Email Compromise	Awareness of Crypto-jacking	Awareness of Business Email Compromise
Personal motive attacks	Denial of service attacks	Awareness of server attacks
	Online payment frauds	Command-and-control server attacks

FBI's cyber strategy is to put cyber adversaries at risk and impose consequences on them, and to change the behavior of criminals and nation-states, who are confident they can compromise U.S. networks, steal intellectual property and financial assets, and threaten critical infrastructure without taking any risks themselves [32].

Based on publicly available data, ENISA Threat Landscape presents an overview of threats, threats agents, and threats trends in Europe, providing an independent view of observed threats, agents, and trends [33]. Threats, major trends, threat actors, and attack techniques such as ransomware and malware, cryptojacking and online payment frauds are outlined in the 2021 report, along with mitigation measures [33].

Due to their weak cyber defenses, African countries have become a favourite target of international cybercriminals, and financial institutions are in particular at risk of financial fraud, data theft, and malware attacks [34]. The biggest cyber threats in an African context include: online scams (such as phishing), digital extortion, business email compromise, ransomware and botnets [34]. More than half of Asian companies (64 percent) have been affected by cyberattacks, and privacy breaches are the top concern for nearly 7 out of 10 respondents (68 percent), followed by ransomware (58 percent) [35]. The majority of Asians perceive privacy breaches and data loss as the top cyber threats, but 26 percent haven't improved their security systems, while 31 percent haven't improved their data protection [35].

Based on the observations and results of the studies that have been referred to for this research, the Table 3 shows the things that need to be considered for cyber training specific to an individual's culture.

5.4. Emotions:

Cyber security response is not captured meaningfully on a sad–happy scale, but may vary based on context, individual identity, and action [23]. Cyber security is viewed negatively by most people and these negative emotions are expressed unprompted [23]. To ensure that unfamiliarity does not lead to uncertainty or negativity, cyber security training must take specific steps to ensure that they are sensitive to the fact that the concepts being introduced could trigger negative emotions and take particular measures to avoid this [24].

The emotions of women were more intense and affective, and the feelings of men were more likely to be fight/flight reactions [25]. A female typically experiences more intense emotional reactions, more emotion during instances of cyberbullying, and is more prone to anxiety during instances of hacking. A male typically reacts more aggressively during such situations [25]. Similarly, older people experience less negative affective events and have better emotion control skills, older people were more likely to have proactive and cognitive/motivational replies [25].

Cyber criminals often involve peoples' fears as primary weapons [36]. The ransomware that affects corporate networks has caused havoc, and, while online media stokes people's fears, it may be easy to trick them into clicking links or opening emails that exploit these fears [36]. A data breach or other security incident tends to stress everyone out and can lead to a variety of feelings, including denial in the first moments, panic, anger, anxiety, even guilt [37]. In the midst of a crisis, and even before it begins, it is imperative to remain calm and collected [37]. There has always been a reluctance among companies to disclose data breaches, much of it due to simple embarrassment [38]. A malicious actor can misuse curiosity to boost the effectiveness of their campaign by weaponizing it [39]. Our curiosity can lead us to act impulsively, without thinking things through, and sometimes even in an irrational manner [39]. The ability to manipulate the target so the malicious actors can get away with mistakes or inconsistencies that the target would otherwise notice allows them to get away with mistakes [39].

Based on the observations and results of the studies that have been referred to for this research, the Table 4 shows the things that need to be considered for cyber training specific to an individual's emotions.

Thus, the above results, studied and observed from the previous studies referred for this research highlights the need of a personalised cyber security framework, answering the research questions (RQ1 And RQ2).

Table 4
Cyber-awareness required for specific Emotion

Anger	Curiosity	Embarrassment	Fear
Data breaches	Phishing	Data breaches	Phishing
	Smishing	Ransomware	Ransomware

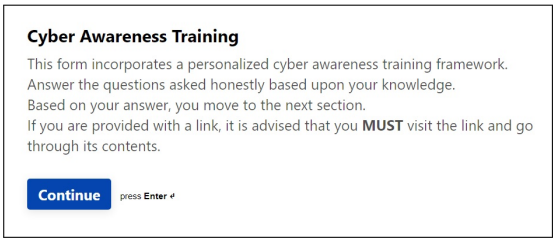

Figure 2: Framework Introduction

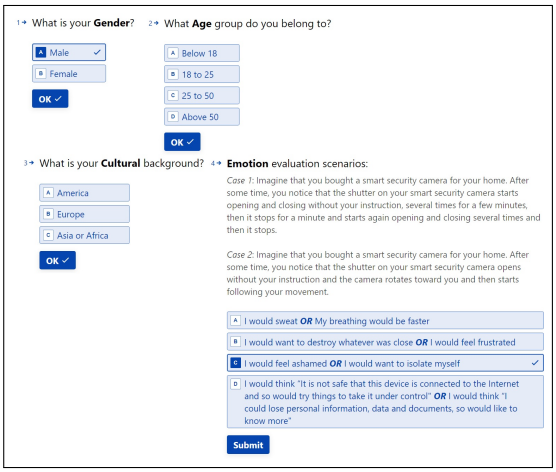

Figure 3: Questions on Human Factors

5.5. Framework Implementation

Based on the observations and results, a personalised framework is developed using Typeform forms [40]. The framework associates for cyber awareness training program for individuals. Guideline for the framework is provided in its introduction as shown in figure 2.

Referring to figure 3, the ideology is, first questions specific to the human factor (gender, age, culture and emotion evaluation) are asked. For emotion factor, two case scenarios are presented and options for individual's emotional reactions are provided. According to the options selected, the individual's emotional behaviour will be identified.

As shown in figure 4, based on the responses to the

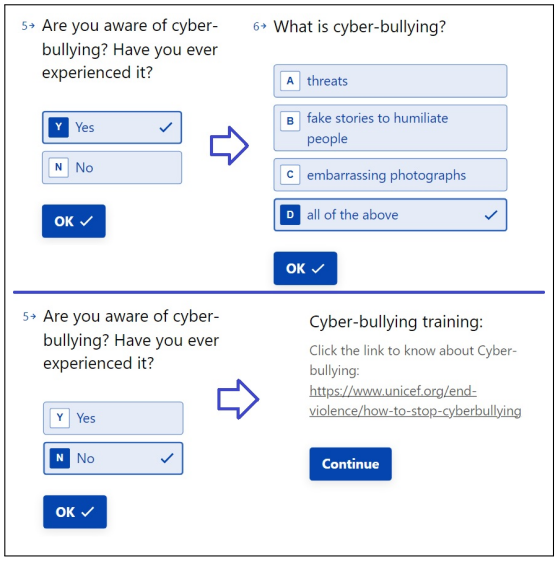

Figure 4: Awareness question example

four human factors, questions related to awareness/-knowledge of specific topics are asked. If the individual is not aware of a particular topic, he/she will be guided to a link, providing the required knowledge. However,if an individual answers "yes", he/she will be provided with a test question to test their knowledge regarding the respective topic. If the answer is correct, they move to the next topic. However, if the test question is answered wrong, they will be provided with a training link that must be viewed to impart awareness about cyber influence of that particular human behavior.

The link to the developed personalised framework is - https://5ugrgg9qtya.typeform.com/to/mvoXaGVn

6. Conclusion

Research on existing cyber training and awareness programmes has been carried out. Its pros and cons were noted and impact of human factors such as gender. age, culture and emotions in context of cyber security were studied. The research conducted, helped develop a framework incorporating personalised training programme for trainees within organization. The personalised framework would help achieve the aims of this paper and overcome challenges from previous studies. The program would help an individual with specific age, gender, culture and emotions to build cyber awareness. The purpose of this framework is to help organisations review their security standards and improve them.

References

[1] R. W. Proctor, J. Chen, The role of human factors/ergonomics in the science of security: Decision making and action selection in cyberspace, Human factors 57 (2015) 721–727.

[2] S. Nifakos, K. Chandramouli, C. K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis, S. Bonacina, Influence of human factors on cyber security within healthcare organisations: A systematic review, Sensors (Basel, Switzerland) 21 (2021) 5119–.

[3] H. Aldawood, G. Skinner, Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues, Future internet 11 (2019) 73–.

[4] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, L. Xu, Gender difference and employees' cybersecurity behaviors, Computers in human behavior 69 (2017) 437–443.

[5] G. Hatzivasilis, S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis, H. Koshutanski, Modern aspects of cyber-security training and continuous adaptation of programmes to trainees, Applied sciences 10 (2020) 5702–.

[6] O. Haggag, J. Grundy, M. Abdelrazek, S. Haggag, A large scale analysis of mhealth app user reviews, in: Empir Software Eng 27, 196 (2022), 2022.

[7] K. Korpela, Improving cyber security awareness and training programs with data analytics, Information security journal. 24 (2015) 72–77.

[8] K. Parsons, A. McCormac, M. Butavicius, L. Ferguson, Human Factors and Information Security: Individual, Culture and Security Environment, 2010.

[9] O. Haggag, Better identifying and addressing diverse issues in mhealth and emerging apps using user reviews, in: The International Conference on Evaluation and Assessment in Software Engineering 2022, 2022, pp. 329–335.

[10] O. Haggag, S. Haggag, J. Grundy, M. Abdelrazek, Covid-19 vs social media apps: Does privacy really matter?, in: 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS), IEEE, 2021, pp. 48–57.

[11] O. Haggag, J. Grundy, M. Abdelrazek, S. Haggag, Better addressing diverse accessibility issues in emerging apps: A case study using covid-19 apps, in: 9th IEEE/ACM International Conference on Mobile Software Engineering and Systems 2022 (MobileSoft 2022), 2022.

[12] M. Fazzini, H. Khalajzadeh, O. Haggag, Z. Li, H. Obie, C. Arora, W. Hussain, J. Grundy, Characterizing human aspects in reviews of covid-19 apps, in: 9th IEEE/ACM International Conference on Mobile Software Engineering and Systems 2022 (MobileSoft 2022), 2022.

[13] B. M. Bowen, S. J. Stolfo, R. Devarajan, Measuring the human factor of cyber security, Homeland security affairs 8 (2012).

[14] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, A. Ginther, Correlating human traits and cyber security behavior intentions, Computers security 73 (2018) 345–358.

[15] M. R., Aspects of human weaknesses in cyber security, Scientific Bulletin ("Mircea cel Bătrân" Naval Academy) XXII (2019) 163–170.

[16] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, M. Kumar, Review and insight on the behavioral aspects of cybersecurity, Cybersecurity 3 (2020) 1–18.

[17] T. Daengsi, P. Pornpongtechavanich, P. Wuttidittachotti, Cybersecurity awareness enhancement: A study of the effects of age and gender of thai employees associated with phishing attacks, Education and information technologies 27 (2021) 4729–4752.

[18] L. C. Amo, R. Liao, E. Frank, H. R. Rao, S. Upadhyaya, Cybersecurity interventions for teens: Two time-based approaches, IEEE transactions on education 62 (2019) 134–140.

[19] A. R. Gillam, A. M. Waite, Gender differences in predictors of technology threat avoidance, Information and computer security 29 (2021) 393–412.

[20] A. Thakur, T. K. Kang, Gender and locale differences in cyber crime awareness among adolescents, Indian journal of health and wellbeing 9 (2018) 906–916.

[21] J. J. Jeong, G. Oliver, E. Kang, S. Creese, P. Thomas, The current state of research on people, culture and cybersecurity, Personal and ubiquitous computing 25 (2021) 809–812.

[22] S. Creese, W. H. Dutton, P. Esteve-González, The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions, Personal and ubiquitous computing 25 (2021) 941–955.

[23] K. Renaud, V. Zimmermann, T. Schürmann, C. Böhm, Exploring cybersecurity-related emotions and finding that they are challenging to measure, Humanities social sciences communications 8 (2021) 1–17.

[24] V. Cheung-Blunden, K. Cropper, A. Panis, K. Davis, Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences, Emotion (Washington, D.C.) 19 (2019) 1353–1365.

[25] S. Budimir, J. Fontaine, N. M. Huijts, A. Haans, G. Loukas, E. Roesch, Emotional reactions to cybersecurity breach situations: Scenario-based survey study, Journal of medical Internet research 23 (2021)

e24879–e24879.

[26] Cyberbullying: What is it and how to stop it, ???? URL: https://www.unicef.org/end-violence/how-to-stop-cyberbullying.

[27] Cyber stalking and harassment on women, ???? URL: https://www.legalserviceindia.com/legal/article-909-cyber-stalking-and-harassment-on-women.html.

[28] E. Chernova, I. Gavrilova, Training teenagers to ensure their own cybersecurity, 2020. doi:10.2991/aebmr.k.200312.417.

[29] Cybersecurity awareness for students, 2022. URL: https://www.cyberdegrees.org/resources/internet-safety-for-college-students/.

[30] R. Security, Cyber security training for employees, 2022. URL: https://blog.rsisecurity.com/cyber-security-training-for-employees/.

[31] Training – cyber security for seniors, 2021. URL: https://www.illuminancesolutions.com.au/digital-literacy-seniors/.

[32] Cyber crime, 2016. URL: https://www.fbi.gov/investigate/cyber#Overview.

[33] Threat landscape, 2022. URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

[34] J. Mitchell, J. Mitchell, Africa faces huge cyber crime threat as the pace of digitalisation increases, 2022. URL: https://www.investmentmonitor.ai/analysis/africa-cyber-crime-threat-digitalisation.

[35] Livemint, 64 percent of firms in asia have been impacted by cyberattacks: Survey, 2022. URL: https://www.livemint.com/technology/tech-news/64-of-firms-in-asia-have-been-impacted-by-cyberattacks\-survey-11657000676429.html.

[36] J. Bolden, Cybercriminals and the exploitation of fear, 2022. URL: https://www.questsys.com/security-blog/Cybercriminals-and-the-Exploitation-of-Fear/.

[37] A. Fiscutean, The emotional stages of a data breach: How to deal with panic, anger, and guilt, 2022. URL: https://www.csoonline.com/article/3646616/the-emotional-stages-of-a-data-breach-how-to-deal-with\-panic-anger-and-guilt.html.

[38] E. Schuman, Don't let embarrassment about a data breach cost you even more, 2016. URL: https://www.csoonline.com/article/3052193/don-t-let-embarrassment-about-a-data-breach-cost-you\-even-more.html.

[39] How hackers exploit curiosity, ???? URL: https://www.hoxhunt.com/blog/youve-been-mentioned-how-hackers-exploit-curiosity.

[40] Forms that perform: Get feedback and leads with ease, ???? URL: https://try.typeform.com/home/.