Human Centric Framework for Customising and Producing Effective Cybersecurity Training Materials

Ashwinraj Giriraj[1,*,†], Sherif Haggag[2,‡] and Hussein Haggag[3,§]

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

Abstract

These days organizational security breaches are widespread, and many of them can be traced back to human errors. As a result, companies must improve employee security awareness and their ability to engage in safe cybersecurity practices. To accomplish so, organizations should spend on cybersecurity training and awareness programs to urge employees to take an active role in adhering to security policies. Numerous organizations' cybersecurity training and awareness activities, on the other hand, fall short of their goals since most training programs focus solely on technical issues, leaving many human factors unaddressed, resulting in training failure. Unlike most other cybersecurity training programs, this study emphasizes the importance of human factors in cybersecurity and the need for successful cybersecurity training and awareness programs in businesses and provides best practices that will assist organizations in developing and implementing effective cybersecurity programs that account for human factors. Also, the end objective of this research is to implement a framework that will suggest personalized cybersecurity training materials based on the end-user's knowledge about cybersecurity.

Keywords
Cybersecurity, human factors, framework

1. Introduction

Several successful cyberattacks against businesses have occurred in recent years. Consequently, more companies have become concerned, and cybersecurity is now one of the most important concerns in today's corporate world. People are commonly acknowledged as the biggest threat in the cybersecurity chain (Singer and Friedman, 2014 cited in [1]). As security protection technologies improve, attackers are particularly focusing on people as potential targets for organizational vulnerabilities. If users aren't properly trained or educated, even the most advanced security systems will not assist much. From one of IBM's security intelligence reports ,it is evident that more than 80 percent of cybersecurity-related issues are due to humans (IBM 2014, cited in [1]).

For enhancing employee security behavior, firms must analyze the most common challenges in existing security training and awareness programs, as well as strategies to increase the training's effectiveness. Understanding the security behavior of both men and women, and the similarities and differences of their security behaviors [2], as well as human factors such as age, interest, determination, motivation, perceived knowledge, cues to action, and so on, are all important considerations when developing effective cybersecurity training programs for employees in the workplace [2]. The end-user might have different skill sets and will be working on different roles in an organization. So, the training for an employee who is working in an IT domain must be different from the training of a non-IT employee.

The following is how the rest of our research will be organized. Firstly, we will have a section for Motivation where we will cover the existing issues within cybersecurity training programs and we will go over some of the best practices to create an effective cybersecurity training program. Also, we will be addressing two key research questions. Then in the literature review, we have summarised our findings from various pieces of literature. The Methodology section will summarize the framework design which accounts for various human factors and thereby suggests an end-user with appropriate cybersecurity training materials. The results section will have the evidence for our findings after conducting extensive research. The last two sections will talk about our future work and conclusion respectively.

2. Motivation

After going through the literature, we found many non-technical issues which are causing resistance to cybersecurity training programs to be successful. After referring to various online resources, it can be said that the following are some of the most common issues with

APSEDEI2022: 1st Asia-Pacific Software Engineering and Diversity, Equity, and Inclusion (APSEDEI)

[*] Corresponding author.

ashwinraj.giriraj@adelaide.edu.au (A. Giriraj); sherif.haggag@adelaide.edu.au (S. Haggag); hussein.haggag@umu.se (H. Haggag)

cybersecurity training programs that are persisting:

- Firstly, the employees of different organizations are bored with the content of cybersecurity training programs which often contains dull statements of policies and procedure. So the employees often do not pay enough attention to the content and are just concerned with completing the training as quickly as possible. (Adam 2018, cited in [1])
- Secondly, as most organizations do not provide any bonuses or benefits for employees who finish security training, many employees lack excitement, interest, and motivation. (Gross 2018; Kostadinov 2018, cited in [1])
- Thirdly and most importantly, several people feel that the training materials are too broad and feel that they are not streamlined. So, the people do not feel the relevancy and often do not engage. (Adams 2018; Winkler 2016, cited in [1, 3])
- Lastly, as different people have different learning styles since the training programs lack personalization people find it difficult to follow the cybersecurity training programs. (Kostadinov 2018; Nadkarni 2012, cited in [1])

After some research on this study, we found several cybersecurity experts recommendations on some of the best practices that can be followed for having successful cybersecurity training programs. For instance, this section provides some of the example practices suggested by various experts.

1. Enforce Accountability- Address how detrimental a lack of information and ignorance can be. Instead of focusing on who failed the assessment, conversely, focus on who did the right thing. Individuals who do not follow the rules should not be punished; instead, those who do should be rewarded. Ascertain that cybersecurity is included in each employee's performance objectives.
2. Relevancy- While framing the content of cybersecurity training materials, try to relate some employees life scenarios like personal online safety. Thereby, it will them in better engagement. Also, there is evidence that employees tend to focus if the information they receive is immediately relevant to them, not only at work but also personally. (Adams 2018, cited in [1])
3. Create a testing environment where people can practically demonstrate the learned skills. This will act as a reinforcement for their learning and people will know what action to take at the time of necessity.
4. The culture within an organization must also be prioritized, as this has a greater impact on having secure cyberspace as compared to secure technologies [4]. If there is a good culture, employees will feel relaxed thereby they tend to be more productive and can react quickly at times of negative security events if need be [1].
5. Organizations should invest in advanced technologies that can minimize the number of false-positive threat alerts. This will help in reducing the security fatigue [1] for the employees.

In this research we aim to address the two key research questions:
RQ1 – Why do we need to consider human factors in cybersecurity training?
Many companies have their cybersecurity training programs, but still, they are facing cybersecurity issues of one form or the other, like data breaches, ransomware attacks, etc. For a successful cybersecurity training program, it is vital to change employees' attitudes and actions and make them more mindful of security and accountability. For which relating the awareness with their personal life is essential (Gross, 2018, cited in [1]). After weighing the importance of each human factor through the associated drawback, it has on the outcome of a training program which can be seen from the human factors table in the results section, it is important to account for those factors and rectify the drawbacks. In this RQ, we propose a framework that will account for age, gender, motivation and self-determination, and emotion.
RQ2 – Why do we need personalization in cybersecurity training program?
In all organizations, there will be different departments. Employees from each department will be having different knowledge about cybersecurity. An employee from IT department might need different training from an employee from a non-IT department as for the latter part it would be enough to just have the basic cyber-awareness whereas that's not the case for an employee from the IT department. Providing generic cybersecurity training is one of the most important existing issues as it can be seen from the motivation section. In this study, we describe the imperative need by emphasizing the importance of successful cybersecurity training programs and provides personalised cybersecurity training materials through a framework that accounts for various human factors like age, gender, self-efficacy, motivation, and emotion, and suggests what areas to focus through cybersecurity training materials to improve cyber-awareness based on the end user's cyber-awareness. The above-mentioned human factors were selected after weighing the importance of each human factor through the associated drawback it has towards the outcome of a training program and based on the finding which we have from our human factors table in the results section and considering the importance, the top four factors that contributed to the

success of a cybersecurity training program were age, gender, self-determination, motivation and emotion.

3. Literature Review

As cybersecurity has been an important area of focus for quite some time, in this paper we have chosen 20 different papers of different areas of focus like existing issues within cybersecurity, training methods, human factors within cybersecurity, modeling cybersecurity training materials, and so on.

Authors of [1] have examined the approaches and provides valuable insights that will help enterprises design and implement cost-effective, effective, and stimulating cybersecurity training and awareness programmes. Many of the conclusions and recommendations in this study are based on a survey of information from non-peer reviewed websites and blogs, despite the fact that they provide important insights and actionable suggestions for developing successful cybersecurity training and awareness programmes.

The focus in [2] is to look into the parallels and differences in cybersecurity views and behavior between men and women. The purpose of this study is to investigate the differences between men and women (gender as a moderating factor) in terms of the above-mentioned components that influence cybersecurity beliefs and practices. The findings reveal women's self-efficacy was much lower than men's, so it could be a focus for improvement as the attackers might launch gender-specific attacks.

In another research, the theoretical background was based on self-determination theory and interest theory. These theories when combined, highlight the importance of interest in employees motivation for undergoing successful cybersecurity training. Individuals natural interest in cybersecurity had mild moderating impacts on the links between self-determination and its important antecedents, according to their findings. Situational interest established during training, on the other hand, directly enhances motivation for cybersecurity training. Overall, their study emphasizes the interaction between interest and self-determination. The findings lead them to believe that training programmes require a UI that uses the principles of this model-based system [5]. In [4], the authors proposed a method that seeks to promote a user-centered, info-driven, thorough, and systematic approach to healthcare cybersecurity analysis and management. As a result, a range of non-technical remedies is offered in order to enhance organizations human components and help them become more competent in the face of cyber-attacks and dangers. Their findings show that a Just Culture can aid organizations in understanding the various cybersecurity risks that their employees confront. [6] was showcasing the fieldwork that directly affects the wider population and is applicable around the globe, as well as non-technical viewpoints on the human elements of cybersecurity. Although there is a lot of research focusing on technical measures for improving cybersecurity, this paper tells the other part of the story where the users perception and emotion are regarded as elements that influence actual cybersecurity conduct. In [7], the cyber behavior of mobile phone users in the region of Czech was investigated by polling 331 people who had no advanced experience in information technology. The researchers combined the health belief model and a motive theory in their work. While having a general understanding of digital security is crucial, their findings suggest that a greater focus on smartphone training to enhance smartphone security behavior is also required.

The authors of [8] is on the behavioral aspects of cybersecurity awareness. The researchers of this study used a gamified method to train and discovered that gamifying cybersecurity training led to greater self-reported scores on mindsets, control beliefs, intents, and behavior when compared to both non-cyber security games. The researchers of [9] focused another aspect of protection motivation theory, where the work to highlight the relationship between risk perception and actual behavior that either effectively nullifies or magnifies anticipated susceptibility to common cyber-based concerns. The authors also conducted a survey for students from various backgrounds on their awareness of cybersecurity. The findings indicated that the anticipated vulnerability may be more dependent on one's appraisal of experience than one's actual knowledge or competence [9]. Then in [10], the focus was shifted to the emotional consequences of being a victim. The author gathered some participants who described their breach experiences as containing emotion components, remedy action tendencies, and psychological reactions. The results indicated that most people have had strong stressful reactions and are highly uncertain to take the right steps to handle the security issues.

[11] was talking on feelings about privacy. The authors reviewed data from different persons recruited through an agency who had been questioned about security problems related to their website access as the emphasis for the study. According to the outcomes, respondents in this study were more anxious about people whom may share accessibility to their digital information than about the measures in place to protect their information.

In [12], the authors were interested in privacy transgressions that are capable of damaging victims. Using a study technique and polling some guardians of aged persons with psychological disabilities through interviewers, the authors were able to find the opportunities and barriers that were employed to safeguard persons confidentiality. The thematic analysis found three key tactics commonly used to assist preserve privacy in this population: limiting private information, minimizing online publication of personal information, and giving prompt and frequent instantaneous guidance and training. The significance of the last piece is focused on the way the technology can be used to develop remedies to reduce reliance on caretakers for privacy protection. A revolutionary approach has been introduced in [13] to portraying cyberspace that allows for a thorough examination of all aspects. It presents a three-dimensional model of the environment, based on past research, that is optimized to better comprehend how its qualities, attributes, and threats can be understood at any location and time in addition to highlighting an organization's cybersecurity strategy in [14]. The primary goal for the authors of the paper [15]is to have a human-centric approach that is based on humanism and conservative principles that may be traced back to the Reformation, the early Middle Ages, and even ancient Greece. It prioritizes human people as key security targets, regardless of nationality or citizenship. Rather than emphasizing networks' territorial sovereignty, this perspective sees them as an integral aspect of the modern exercise of human rights, such as access to information, freedom of thought, and freedom of association. The caveats of the cyber risks posed by the infodemic are explored in [16], as well as what it means for the broader network of cybersecurity and the protection of human rights in cyberspace. It also looks into the harm caused by cyberattacks on vulnerable groups, especially in light of COVID-19. With a focus on age and gender, the authors of [17, 18, 19, 20, 21] reported a simulated phishing experiment that targeted a large subset of employees from the university. They found substantial effects on various age groups, on email types, and barely significant gender differences after analysing human characteristics.

In another interesting research, the authors in [22] used a training system to study different people and how they behave when it comes to a phishing scenario. The research couldn't find any significant evidence which shows that a particular gender group is more vulnerable, instead the research showed that the people of age between 18 to 25 are the most vulnerable to phishing. There was another research by the authors of [23], that just shows exactly the opposite of what the authors of [22] had proved. It showed that the younger age group people have a higher awareness on cybersecurity than that of older aged people. The Netherlands-based researchers [24] analysed a very large number of employees and discovered that people under the age of 26 were the least likely to view phishing links, while those over 46 were significantly more likely than the people under the age of 26. And finally, the authors of [25] concludes that women are noticeably more likely than men to fall victim to phishing. Also, in the same paper the authors have quoted that several other previous studies shows that women are more susceptible to cyber-attacks and differences in gender causes different perception of technologies.

4. Methodology

As the objective of this research study is to provide efficient cybersecurity training materials, the framework is designed with two major components, as seen in Figure 1. The first component of the framework will be responsible for identifying human-centric issues. The framework will have questions associated with human factors like age, gender, self- efficacy, motivation, and emotion.The second component will test the user's knowledge of cyber awareness through a set of topic-specific questions relating to phishing, password strength, malware, and cyber hygiene. The reason for having the topics mentioned above is because testing the people on just one topic won't be of any use, nor does testing everyone on technical topics like offensive security, as everyone doesn't need to know too many technical details regarding cybersecurity. So, to have a fair awareness test, it would be appropriate to test them on basic cybersecurity topics. To cover the basics, there are a few important areas that everyone must be aware of. The cybersecurity topics like cyber-hygiene, password strength, phishing, malware, etc., are some of the important primary topics which everyone should know about. So, we chose these as our topics for testing cyber-awareness.

Then, we primarily worked on implementing our framework mentioned in Figure 1, which was our goal. Initially, to start with, we started building framework questions that will help us to assess the human factors associated with each individual. We primarily focused on human factors like age, gender, motivation and self-determination, self-efficacy, and emotion.So each of these human factors will have some questions in the framework, and the questions framed will have predefined answers to assess the human elements. For each human factor, there will be a baseline score. If the user scores below the baseline score, that user is considered to have an issue concerning the associated human factor. If not, the user has no problems concerning the above-mentioned human factors. We will store the results from the first component before moving to the second component of the framework. The second component will assess the end user's knowledge of cybersecurity. To do that, we first collected topic-specific framework questions relating to essential cybersecurity and then started to build the scoring system. Building the scoring system was the most challenging task, as we had to find a way to display an individual's top three weakest areas in cybersecurity.

The logic behind the scoring system is that we had

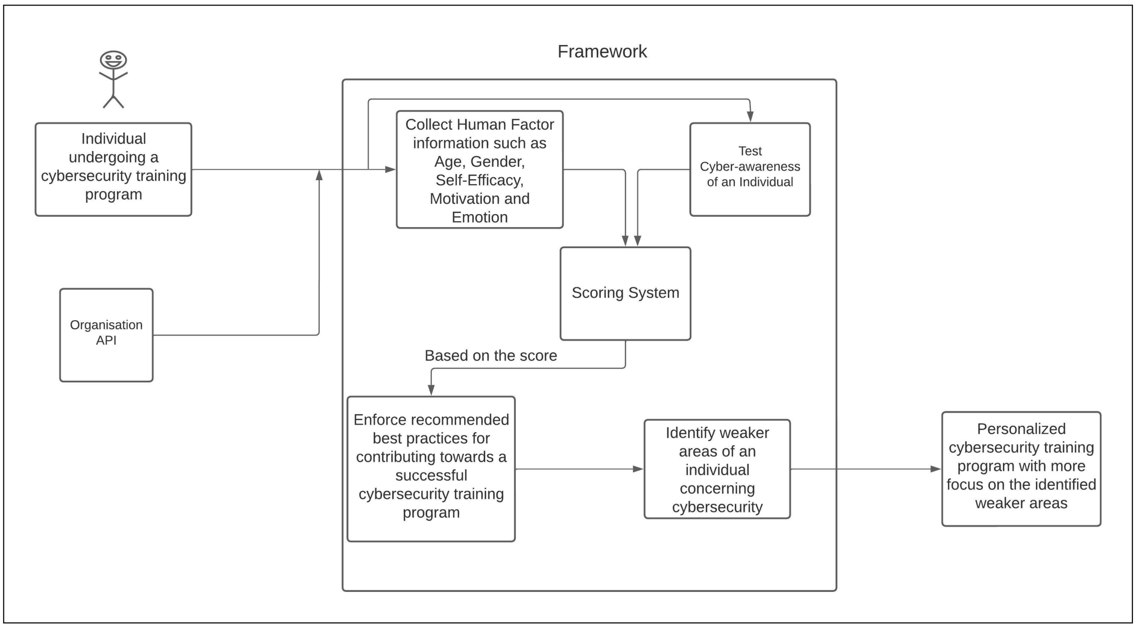

Framework
Individual undergoing a cybersecurity training program
Organisation API
Collect Human Factor information such as Age, Gender, Self-Efficacy, Motivation and Emotion
Test Cyber-awareness of an Individual
Scoring System
Based on the score
Enforce recommended best practices for contributing towards a successful cybersecurity training program
Identify weaker areas of an individual concerning cybersecurity
Personalized cybersecurity training program with more focus on the identified weaker areas

Figure 1: Cybersecurity Training Framework

a baseline score for each topic; if the individual scores below the baseline, that will be flagged. In the end, the weakest three flagged areas will be displayed as the areas to be given importance in cyber awareness training. If the user scores below the baseline score on all the topics, then it is best advised to train that individual on all the essential topics in cybersecurity. So, with the help of our first component, we will be able to identify the issue associated with the human factors, if any. Based on that, best practices are recommended to ensure that the human factor issue is taken care of through the suggested training material.

Similarly, with the help of the second component, an individual's weaker areas regarding cybersecurity will be identified, if any. And based on that, the framework will suggest the training materials focusing on the identified weaker areas and the same will be sent as an email to the user's mail.Sending automated emails is possible because we are using a client-server modeled server configured with google API, and that sends the final recommendations that are being generated to the user as an email to the user's mail.. To conclude, we call the framework personalized because the training materials are recommended based on human factors and the cyber-awareness knowledge associated with each user. Therefore, the training materials suggested for each user are unique and help the framework overcome the issue of suggesting generic cybersecurity training material.

To summarize all the technologies we have used in building our framework from scratch : To build the frontend of the framework, we primarily used javascript, and in some instances, we used typescript and converted that to javascript. For the backend, we adapted the express framework i.e Express.js, as it is open-source and supports multi-page and hybrid web applications. Since our framework is a multi-page web application, we used the express framework. Finally, to host the framework, we used an application called netlify, which is, again, a free cloud computing company that offers a development platform that includes build, deploy, and serverless backend services for web applications and dynamic websites. Also, netlify supports git integration, so if we set up the git repository, whenever we push some changes in the git repository, the changes get deployed automatically in the web application because of the git integration feature offered by netlify.Also, since the backend service has to be built as a top layer of a server, we used an application called heuroko, which is a platform as a service cloud provider that supports multiple programming languages. So, we configured the server with a google API, so whenever the framework analyzes a user and gives a recommendation, the same is sent to the user's email, which the user enters initially at the basic information page

Previously, all the existing research was all about safe and recommended practices that would help the training

Table 1
Human factors considered in our Framework.

Human Factors	Findings	Proposed Solution
Age	If we consider the age group of 19-30, 31-40, 41-65, and 65+, the youngest age group is less susceptible to cyber-attacks and is more cyber aware.As the age increases, the susceptibility also increases, and the older age groups (45-65 and 65+) are the most susceptible specially to phishing attacks. [23]	The framework will account for the age factor. Based on the age factor, the intensity of the cybersecurity training program will be formulated. Like if the individual undergoing training is younger, then the individual is expected to be more cyber-aware than the other age groups, so less intensive training. Also, the formulated intensity will again be verified with the individual's cyber-awareness. If both matches, then the intensity of the personalized cybersecurity training program will be less else vice versa.
Gender	Women's self-efficacy is much lower than men [2]. Differences in gender cause different perceptions of technologies. Several studies show that women are more susceptible to cyber-attacks than men. [25]	The framework will account for the gender factor. As the attackers might launch gender-specific attacks targeting women's self-efficacy, the cybersecurity training program for women, in general, will have resources to boost their morale and confidence. So, this ensures that there is equal fairness for all genders in accessing technologies.
Motivation and Self-Determination	Motivation is an important factor for training programs to be successful. There was research based on self-determination theory and interest theory. When these theories are combined, it also highlights the importance of interest in employee's motivation.[5]	The framework will account for the motivation factor. The cybersecurity training program will enforce accountability, and relevancy and makes sure that everyone understands the importance of cyber-awareness. Thereby, instilling motivation.
Emotion	It is an important element that influences actual cybersecurity conduct [9]. When people are stressed, they are highly uncertain to take the right steps to handle the security issues. [10]	In the personalized cybersecurity training program produced by our framework, there will be a testing environment where people can demonstrate learned skills. As this acts as reinforcement for their learning, at times of necessity, people will know what action to take.

program to be successful. In our framework, the final recommendations are adapted from the existing research that are proven to positively affect training programs. But the framework to analyze the issues associated with human factors and cyber-awareness knowledge of each user was designed by us entirely from scratch.

5. Results

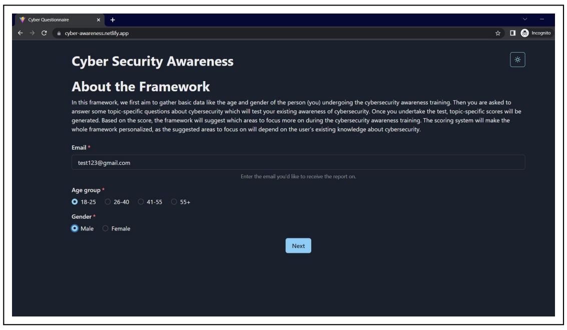
Through our extensive research, we found that Generic cybersecurity training material hinders the success of a cybersecurity training program (Adams 2018; Winkler 2016, cited in [1]). Human factors must be considered while designing a cybersecurity training program. In Table 1, we describe the human factors considered in our framework and the associated findings. The proposed solution will account for the human factors, recommended practices, and the framework where we will identify the weaker areas of an individual concerning cybersecurity. The recommended best practices for the associated human factor will be generated and stored. This will be done with the help of a few questions that collect information about the human factors associated with the individual, and based on that, the scores for the associated human factor will be generated. As seen from the methodology, if need be, recommended practices for the associated human factor will be generated depending on the score. Also, the user will be entitled to answer questions in the framework focusing on topics like cyber-hygiene, phishing, password strength, malware, and physical security. So, all the people undergoing training will have to answer these questions, with which the individual's cyber-awareness will be measured with the help of the scoring system we have designed. Through scores, the framework will identify the weaker areas of the individual, and the suggested training material will focus more on the weaker areas, thereby avoiding suggesting a generic cybersecurity training material which is one of the significant challenges in having a successful training program. So, with the help of this framework, it will be possible to create a personalized cybersecurity training program based on the needs of everyone. The workflow of our framework from the start can be seen below:

1. Firstly, the user is prompted to give basic information like user email, age, and gender, as seen in Figure 2.
2. Secondly, the user will be taken to a second screen, where the framework will collect human-factor information with the help of section-wise questions on motivation, self-efficacy, and emotion, as seen in Figure 3. The questions that we use to test the factors mentioned above can be found in the miscellaneous section.
3. After collecting the human factor information and

assessing them, the user will be taken to the cyber-awareness test, as seen in Figure 4, where they will be entitled to answer topic-wise questions relating to cybersecurity.

4. Finally with the help of the scoring system, we display the recommended best practices to improvise the associated human factor - only if we analyze that there are issues specific to any of these human factors: Motivation, Self-Efficacy, and Emotion. Since, at this point, the end-user's knowledge is already tested, based on the identified weaker areas, appropriate recommendations along with the learning resource for each section are displayed in the final recommendations page.Also, the final recommendations for each user will be automatically sent to the user's email which they enter and a sample image of the received email by the user can be seen in Figure 6.

Let's say the user takes the test and is identified with a low self-efficacy factor to demonstrate a scenario. Also, in the cyber-awareness test, the user is assessed to be weak in physical security, phishing, and ransomware attacks. In this case, the final recommendations screen will look like the one in the Figure 5.



Cyber Security Awareness

About the Framework

In this framework, we first aim to gather basic data like the age and gender of the person (you) undergoing the cybersecurity awareness training. Then you are asked to answer some topic-specific questions about cybersecurity which will test your existing awareness of cybersecurity. Once you undertake the test, topic-specific scores will be generated. Based on the score, the framework will suggest which areas to focus more on during the cybersecurity awareness training. The scoring system will make the whole framework personalized, as the suggested areas to focus on will depend on the user's existing knowledge about cybersecurity.

Email *

test123@gmail.com

Enter the email you'd like to receive the report on.

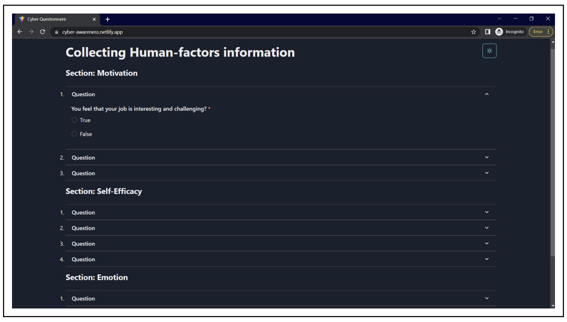
Age group *

● 18-25 ○ 26-40 ○ 41-55 ○ 55+

Gender *

● Male ○ Female

Figure 2: Collecting basic information through the framework



Collecting Human-factors information

Section: Motivation

1. Question

You feel that your job is interesting and challenging? *

○ True

○ False

2. Question
3. Question

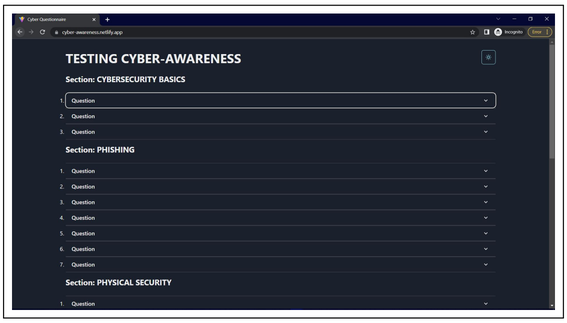
Section: Self-Efficacy

1. Question
2. Question
3. Question
4. Question

Section: Emotion

1. Question

Figure 3: Collecting human-factor information through the framework



TESTING CYBER-AWARENESS

Section: CYBERSECURITY BASICS

1. Question
2. Question
3. Question

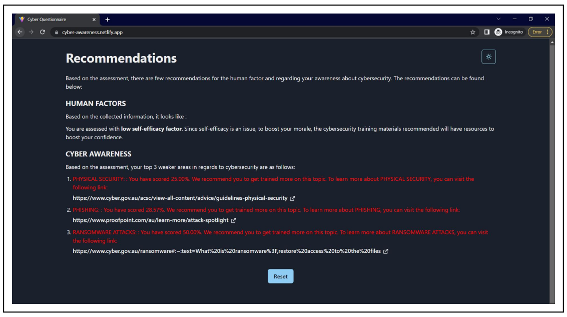
Section: PHISHING

1. Question
2. Question
3. Question
4. Question
5. Question
6. Question
7. Question

Section: PHYSICAL SECURITY

1. Question

Figure 4: Cyber-awareness test screen in the framework



Recommendations

Based on the assessment, there are few recommendations for the human factor and regarding your awareness about cybersecurity. The recommendations can be found below:

HUMAN FACTORS

Based on the collected information, it looks like :

You are assessed with **low self-efficacy factor**. Since self-efficacy is an issue, to boost your morale, the cybersecurity training materials recommended will have resources to boost your confidence.

CYBER AWARENESS

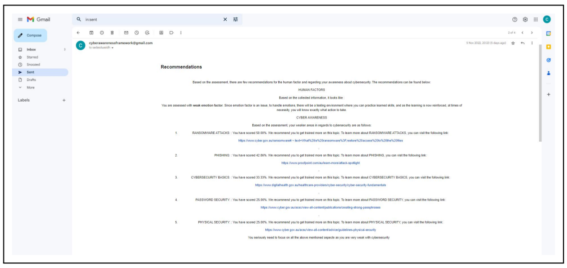
Based on the assessment, your top 3 weaker areas in regards to cybersecurity are as follows:

1. PHYSICAL SECURITY: : You have scored 25.00%. We recommend you to get trained more on this topic. To learn more about PHYSICAL SECURITY, you can visit the following link:
   https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-physical-security
2. PHISHING: : You have scored 28.57%. We recommend you to get trained more on this topic. To learn more about PHISHING, you can visit the following link:
   https://www.proofpoint.com/au/learn-more/attack-spotlight
3. RANSOMWARE ATTACKS: : You have scored 50.00%. We recommend you to get trained more on this topic. To learn more about RANSOMWARE ATTACKS, you can visit the following link:
   https://www.cyber.gov.au/ransomware#:~:text=What%20is%20ransomware%3F,restore%20access%20to%20the%20files

Figure 5: Final Result- Recommendations screen

6. Conclusion

To provide effective cybersecurity training, this study accounts for the importance of human factors in cybersecurity. It is evident from the study that there is a need for a successful cybersecurity training program and to have a positive outcome on the training program, this study also provides the best practices that will assist organizations in achieving successful cybersecurity training programs. One of the most important issues of an organization's cybersecurity training was the training being generic, which will be resolved with our proposed framework. As our framework considers various human factors and identifies weak areas of each individual undergoing the cybersecurity training, a personalized cybersecurity training material will be suggested focusing more on the individual's weaker areas.



cyberawarenessframework@gmail.com
to sadasduasidh

5 Nov 2022, 20:23 (5 days ago)

Recommendations

Based on the assessment, there are few recommendations for the human factor and regarding your awareness about cybersecurity. The recommendations can be found below:

HUMAN FACTORS

Based on the collected information, it looks like :

You are assessed with **weak emotion factor**. Since emotion factor is an issue, to handle emotions, there will be a testing environment where you can practice learned skills, and as the learning is now reinforced, at times of necessity, you will know exactly what action to take.

CYBER AWARENESS

Based on the assessment, your weaker areas in regards to cybersecurity are as follows:

1. RANSOMWARE ATTACKS: : You have scored 50.00%. We recommend you to get trained more on this topic. To learn more about RANSOMWARE ATTACKS, you can visit the following link:
   https://www.cyber.gov.au/ransomware#:~:text=What%20is%20ransomware%3F,restore%20access%20to%20the%20files
2. PHISHING: : You have scored 42.86%. We recommend you to get trained more on this topic. To learn more about PHISHING, you can visit the following link:
   https://www.proofpoint.com/au/learn-more/attack-spotlight
3. CYBERSECURITY BASICS: : You have scored 33.33%. We recommend you to get trained more on this topic. To learn more about CYBERSECURITY BASICS, you can visit the following link:
   https://www.digitalhealth.gov.au/healthcare-providers/cyber-security/cyber-security-fundamentals
4. PASSWORD SECURITY: : You have scored 25.00%. We recommend you to get trained more on this topic. To learn more about PASSWORD SECURITY, you can visit the following link:
   https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases
5. PHYSICAL SECURITY: : You have scored 25.00%. We recommend you to get trained more on this topic. To learn more about PHYSICAL SECURITY, you can visit the following link:
   https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-physical-security

You seriously need to focus on all the above mentioned aspects as you are very weak with cybersecurity

Figure 6: Final Recommendations Mail received by the user

7. Future Work

As of now, the framework can identify the issues related to human factors associated with each user and identify weaker areas of the individual regarding cybersecurity. Based on that, we will recommend how to improve those human factors and the weaker cybersecurity areas to focus on. For now, as a recommendation to enhance weaker cybersecurity topics, we put up a resource link for the associated issues where the user can learn more about the topic. This is done since, to suggest cybersecurity training materials based on the knowledge of each user, we need an extensive data set of cybersecurity training materials. We are still collecting the training materials. In the future, when we have enough datasets, the framework will be able to suggest cybersecurity training materials rather than putting up resource links.

8. Miscellaneous

In the framework, we have two sections where the user has to go through a set of questions for the framework to assess the user.The framework can be accessed through this link: https://cyber-awareness.netlify.app/. The user won't be able to navigate to a different question without answering the first question. The user will be navigated to the next question automatically once the first question is answered. Once the user answers all the questions displayed under the framework, the user will be assessed both for the issues associated with the human-factors and cybersecurity awareness, and the respective recommendations will be displayed in the end.

References

[1] W. He, Z. J. Zhang, Enterprise cybersecurity training and awareness programs: Recommendations for success, Journal of organizational computing and electronic commerce 29 (2019) 249–257.

[2] 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.

[3] 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.

[4] A. Pollini, T. C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, D. Guerri, Leveraging human factors in cybersecurity: an integrated methodological approach, Cognition, technology work 24 (2021) 371–390.

[5] H. Kam, D. K. Ormond, P. Menard, R. E. Crossler, That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training, Information systems journal (Oxford, England) (2021).

[6] S. M. Debb, Keeping the human in the loop: Awareness and recognition of cybersecurity within cyberpsychology, Cyberpsychology, behavior and social networking 24 (2021) 581–583.

[7] L. Knapova, A. Kruzikova, L. Dedkova, D. Smahel, Who is smart with their smartphones? determinants of smartphone security behavior, Cyberpsychology, behavior and social networking 24 (2021) 584–592.

[8] T. van Steen, J. R. Deeleman, Successful gamification of cybersecurity training, Cyberpsychology, behavior and social networking 24 (2021) 593–598.

[9] S. M. Debb, M. K. McClellan, Perceived vulnerability as a determinant of increased risk for cybersecurity risk behavior, Cyberpsychology, behavior and social networking 24 (2021) 65–611.

[10] S. Budimir, J. R. Fontaine, E. B. Roesch, Emotional experiences of cybersecurity breach victims, Cyberpsychology, behavior and social networking 24 (2021) 612–616.

[11] V. Kisekka, J. S. Giboney, The effectiveness of health care information technologies: Evaluation of trust, security beliefs, and privacy as determinants of health care outcomes, Journal of medical Internet research 20 (2018) e107–e107.

[12] J. N. Rocheleau, H. Chalghoumi, J. Jutai, S. Farrell, Y. Lachapelle, V. Cobigo, Caregivers' role in cybersecurity for aging information technology users with intellectual disabilities, Cyberpsychology, behavior and social networking 24 (2021) 624–629.

[13] A. Venables, Modelling cyberspace to determine cybersecurity training requirements, Frontiers in education (Lausanne) 6 (2021).

[14] M. Bada, J. R. Nurse, Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (smes), Information and computer security 27 (2019) 393–410.

[15] R. J. Deibert, Toward a human-centric approach to cybersecurity, Ethics international affairs 32 (2018)

411–424.

[16] T. Smith, The infodemic as a threat to cybersecurity, The international journal of intelligence, security, and public affairs 23 (2021) 180–196.

[17] F. L. Greitzer, W. Li, K. B. Laskey, J. Lee, J. Purl, Experimental investigation of technical and human factors related to phishing susceptibility, ACM transactions on social computing 4 (2021) 1–48.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. Blair, T. Pham, School of phish: a real-world evaluation of anti-phishing training, in: Proceedings of the 5th Symposium on usable privacy and security, SOUPS '09, ACM, 2009, pp. 1–12.

[23] E. Kim, J. Yoon, J. Kwon, T. Liaw, A. M. Agogino, From innocent irene to parental patrick: Framing user characteristics and personas to design for cybersecurity, in: Proceedings of the Design Society, volume 1, Cambridge University Press, Cambridge, 2019, pp. 1773–1782.

[24] A. Baillon, J. de Bruin, A. Emirmahmutoglu, E. van de Veer, B. van Dijk, Informing, simulating experience, or both: A field experiment on phishing risks, PloS one 14 (2019) e0224216–e0224216.

[25] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, J. Downs, Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions, in: Proceedings of the SIGCHI Conference on human factors in computing systems, CHI '10, ACM, 2010, pp. 373–382.