IJITLS

International Journal of Information Technology and Language Studies (IJITLS)

Comparison between Gamification and Instructor-Led as User Methods for Effective Cyber Security Awareness Delivery

Augustine D. Yeboah[1] and Ernest B. B.Gyebi[2]

[1]Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana
[2]Department of Computer Science, University of Ghana, Ghana

dayeboah21@st.knust.edu.gh; egyebi@ug.edu.gh

Article Information

Article type: Article

Article history:

Received: July 18, 2023
Revised: November 08, 2023
Accepted: May 18, 2024

Keywords:

Cyber security awareness
Gamification
Cyber security education
Awareness delivery methods
Instructor Led delivery

Abstract

Several cyber security awareness methods have been developed to raise awareness among people in mitigating cyber security threats. The effectiveness of cyber security awareness programs is determined by how the information is presented. As a result, appropriate methods for educating users and raising awareness should be researched. Gamification has recently gained enormous momentum in the academic community. The use of game mechanics has been shown to be effective, but is this what users want? Instructor Led delivery is also a way of educating users on cyber security. This works through a variety of formal presentations, such as seminars and classroom type workshops facilitated by local or external information security specialists. As a result, this study compared gamification to instructor-led cyber security awareness delivery methods, with the results indicating that instructor delivery is more effective in this study. The study's findings also revealed that users preferred instructor led delivery over game-based delivery.

1. INTRODUCTION

Individuals and both organisations have benefited greatly from technological development since its inception. Organisations of all sizes have become more reliant on information technology to gain a sustainable competitive edge and enhance services provided to all. However, these advantages are accompanied with significant dangers to information security (Smith & Ali, 2019). Presently, mobile devices, computers and cloud hold and handle a significant quantity of data, including confidential material such as contacts, emails, photographs, and videos. Currently, even bank account details can be found on mobile phones which if not protected cyber criminals will gain access. In today's technologically advanced society, information has become a precious asset for both individuals and companies.

To defend oneself from different cyber attacks, both businesses and people must be aware of cyber security threats and how to protect themselves. It is becoming extremely difficult to secure new technology against harmful activity (Al-Janabi & Al-Shourbaji, 2016). Cyber security risks have been hurting individuals, as well as organisations. This has to do with many people inadvertently downloading viruses and other dangerous things and facing the repercussions. As an example, the botnet responsible for one third of all spam sent out in 2010 paid its owners about $2.7 million, while global spam protection costs likely topped a billion dollars (Anderson et al., 2013). This amount is going to keep on increasing if users are not made aware of these issues. Cyber criminals will keep on making themselves rich while victims suffer the consequences.

Cyber crime frequently leads not only in stolen assets and lost revenue, but also causes harm to a company's image, which may also affect the organisation's stock market price. Cyber crime also affects how individuals see and purchase from a company. For example, one of the largest data leakage occurred in 2016 where yahoo reported over 500 million user accounts were exposed. The company was affected financially and also lost some clients. According to Smith and Ali (2019), cybercrime will cost businesses billions of dollars each year in prevention efforts and damage to a company's reputation which can lead to lost businesses. This happens as a result of petty mistakes made by individuals during their daily routine in using technology and handling data.

Mobile devices are subjected to a variety of security threats, mostly as a result of user behaviour and actions that render the device open to attacks (Yaokumah, 2016). These devices are also prone to cyber attacks as user's lack understanding and experience with the device's functions and their inability to implement device security measures. Information and data is a sought after good due to the sheer importance that many organisations and private persons attempt to illegally access (Stefaniuk, 2020). Information is very susceptible to theft as an examination of recent media headlines on cyber security paints a bleak image of the modern world.

Employees who intentionally or unintentionally provide information about their companies become targets for highly contextualised social engineering attacks such as tailored malware, spear phishing and advanced persistent threats (Dincelli & Chengalur-Smith, 2020). It is known that many incidents of cybercrime go undetected as it is impossible to precisely assess losses from cybercrime. Many cyber crime activities go unreported and the perpetrators go free. The total cost of cybercrime for firms in the US economy was over 400 billion dollars in 2015 (Smith & Ali, 2019).

The human aspect is frequently the weakest link hence security awareness is an essential component of any security architecture. Customers lose trust and interest in firms when they believe their private details and transactions are not secure in their hands. This is understandable as leaking private data breaches our privacy. Gamebased, instructor led, videobased, and text based are some of the various techniques for delivering cyber security awareness yet attackers tend to find their way most of the time. It is seen that these delivery methods are not being effective. Cyber security awareness is the process of making users aware of various cyber threats and how to counter those threats (Abawajy, 2014).

Enhancing employee cyber literacy decreases a company's risk of a cyber security breach as they are aware of the threats and how to defend themselves (Filipczuk et al., 2019). Humans, unlike computers and software, cannot be patched whenever a new vulnerability is identified but rather they can be made aware of cyber security threats. In combating cyber security threats, several cybersecurity camps and awareness methods have been created. This is to raise awareness among people and promote safe web and device usage. Businesses and government agencies have recognised the necessity of teaching their workers about cyber security dangers in order to protect themselves from these threats. This can be noticed as the government of Ghana has set up various cyber security agencies to combat mobile money fraud in collaboration with the telecommunications companies.

Different cyber security initiatives such as security training, and awareness programmes, as well as security policies are implemented by organisations in reducing security risks (Dincelli & Chengalur-Smith, 2020). Games, instructor-led and online text based methods have been used by organisations and governments to educate users on cyber security issues for some time now. When game related features are brought to non game situations, this is referred to as gamification (Malone et al., 2021). Instructor delivery refers to a range of lectures, such as brown bag seminars and classroom style workshops, guided by local or external information security professionals and intended to improve employee knowledge of cyber security (Abawajy, 2014).

However, these awareness activities for the most part do not bring the threat to the forefront as cyber crime keeps increasing. This might be related to the method of awareness delivery used by the various cyber security initiatives. As a result, relevant methods for empowering users and increasing awareness should be investigated (Bahrini et al., 2019). This research seeks to provide relevant information on effective awareness delivery methods.

2. RELATED WORKS

Cyber security has been defined by many but every definition takes a different approach. In the past few years, the term ”cyber security” has become more popular with professionals using it more frequently (Schatz et al., 2017). Governments have been talking about security more recently than ever before. The adoption of technology in all sectors of government has made security become a vital issue. The notion of cyber security has its origins in cyberspace which has been described in many ways. According to Schatz et al. (2017), there appears to be a misunderstanding of what the term ”cyber defence” actually implies. Cyber defence can be defined as the mechanisms that are adopted to defend systems from cyber criminals.

However, according to von-Solms and van-Niekerk (2013), the term cybersecurity and information security are frequently used interchangeably. From literature reading it can be identified that cyber security and information security is being used interchangeably by researchers. As with many trendy terms, there appears to be little grasp of what the phrase actually means and what it entails. Various researchers have defined information security and cyber security in a variety of ways, using a variety of qualifiers. This shows how important security is to all users in using these devices. The goal of cyber security is to keep vital information technology services running at acceptable levels (Tasevski, 2016).

This can be debated as the user is also part of cyberspace. The user should also be able to protect themselves from cyber criminals as the human is being exploited often. According to von-Solms and van-Niekerk (2013), cyber security extends beyond conventional information security to incorporate not just the protection of information assets, but also the protection of other resources including the person himself/herself. Thus, cyber security can be defined as approaches that are frequently specified in publications and organisations that attempt to safeguard a user’s or institution’s cyber environment from cyber criminals. Seemma et al. (2018) concur with Schatz et al. (2017) that cyber security may also be referred to as information technology security. Tasevski (2016) contends that the goal of information technology security is to decrease business risk to acceptable levels while also protecting complete information and information systems critical to companies.

This means that information security focuses more on safeguarding the data being generated by using these systems. Based on these reasons, we may define information security as the method and techniques utilised to secure and preserve private information when technology is in use. It can also be seen that information security is different from cyber security as information security doesn’t include safeguarding the user but rather the data.

2.1 NEED FOR CYBER SECURITY AWARENESS

Cyber threats have existed since the introduction of the internet and network technologies. Training is an excellent method of boosting security awareness, and one of the duties that managers must undertake is to provide training programs to staff (Sharif & Ameen, 2020). The lack of knowledge among end users in cyber security will continue to be a problem organisations face. As the human is known to be the weakest link there is need for awareness in cyber security. This necessitates more studies into effective ways of delivering cyber security awareness to users. Control systems such as intrusion detection systems and antimalware software, are used to minimise the risk associated with cyber threats and protect assets but it doesn’t seem to be enough.

According to Sharif and Ameen (2020) and Grassegger and Nedbal (2021), companies should not rely just on technology-based approaches to maintain cyber security but also on policy and its successful execution. This is due to the fact that the majority of cyber criminals such as hackers currently target humans rather than technology being used. Tasevski (2016) contends that creating cyber security knowledge among all actors and stakeholders is essential but insufficient in combating cybercrime. This means that, even with increased knowledge, companies and individuals should continue to invest in cyber security awareness training. According to Venter et al. (2019), cyber security education has two components: first, individuals need to become aware of the need to take measures, and then teachers must impart the skills necessary to take the necessary safeguards.

This is necessary for effective awareness training content and users will gain the required skills. According to Qusa and Tarazi (2021), the expanding number of cyberattacks indicates that conventional training and awareness techniques

are still inadequate to develop the required cyber security skills and abilities, but there is no relevant data to back it up, necessitating the need to evaluate which awareness method users prefer. Nguyen and Pham (2020) concur with Qusa and Tarazi (2021) that earlier information security training research included theories from a variety of areas, including gaming, behaviour, social psychology, and learning. This indicates how important it is for organisations to know which method is effective in order to train their staff.

2.2 CYBER SECURITY AWARENESS DELIVERY METHODS

One of the primary goals of cyber security awareness training is to increase users knowledge of cyber security in an organisation. The effectiveness of cyber security awareness programs, like any other program, will be highly dependent on how the awareness material is presented (Abawajy, 2014). There are several cyber security awareness delivery approaches from literature. These approaches all have different ways of giving the training to users. These approaches are capable of promoting user awareness about a wide range of cyber security issues. There are several cyber security issues ranging from spam and phishing to well planned cyberattacks designed to damage systems or steal data. The part that follows will give context for the subsequent discussion of this study by studying the different cyber security awareness delivery methods that are widely utilised. This provides information on how each delivery method is handled.

2.2.1 Gamification

The endeavour to increase cyber security awareness is broad and expanding as cyber crime increases. There is a strong trend in the business and academia to utilise amusing ways in education, such as Gamification, to teach people (Van Steen & Deeleman, 2021). People have been playing games since Nintendo days and currently with the introduction of smartphones, games have become more common. The increased severity of cybercrime has made modern businesses turn their attention to cutting edge awareness programmes that assist their staff to protect themselves from cyber threats. These technologies are believed to give users the enthusiasm to take part in awareness programs. The number of tech games has increased considerably in recent years, and game creation has become predominant (Sharif & Ameen, 2020). Gamification does not mean the creation of a game, but rather the goal of making education more enjoyable and engaging while preserving its legitimacy (Muntean, 2011). The inclusion of playful elements into learning recently has resulted in a very distinct concept of game based learning. Game Based training may provide staff with a visually appealing and exciting atmosphere (Nguyen & Pham, 2020).

According to studies and reviews, games can provide an interesting interface to improve training as well as providing quality content. According to Nguyen and Pham (2020), Gamification is suggested as the primary cyber security training delivery and testing technique in order to overcome the shortcomings of earlier approaches, which include unrealistic and unattractive training materials. This on a broader aspect can be true but 18is game based learning what users want? Gamification has lately grown more prominent and has been utilised to teach people a wide range of issues such as cyber security and its awareness as well as other disciplines. It is thought that the majority of cyber security threats are connected to the human component. This has not altered significantly in recent years as social engineering continues to increase (Chang & Coppel, 2020;, (Lika et al., 2018). Instead of computerised breaches, most clever criminals have switched to social engineering as their major crime route which has proven to be rewarding.

People still have a similar point of view and respond to the same stimuli, which implies that skilled criminals may plan to purposefully exploit these emotions over and over (Lika et al., 2018). Some ignorant user behaviour affects security and this not only facilitates broad hacking, but also leads to countless incidents of theft within institutions and organisations. Unfortunately, people continue to postpone and reject maintaining their system which could have helped prevent breaches. People tend to do updates on their own terms rather than what manufacturers want to be done to make a system stable or employ a preventive security solution for enough confidence. Important games would have instructional elements and need players to participate regularly in order to be effective (Lika et al., 2018). Serious games and electronic games centred on computer security/privacy lessons might be expanded to also include high involvement rates by giving the proper context, themes, and storytelling components (Karagiannis et al., 2020).

These stories help make the games interesting to the player to grasp the content. Most cyber security training delivery techniques are considered unintuitive, and unappealing to consumers hence effective and preferred delivery methods need to be investigated. Some writers have attempted to adopt gaming tactics to give individuals the best visual experience. This is believed to give users an exciting atmosphere, engaging, and delight. A typical computer user can get information through gamification that can defend them from future assaults (Lika et al., 2018). Gamification when combined with other conceptual models for cyber security awareness programs may increase training value and performance.

A number of studies have found that those who play games, either competitive level or cooperatively, have the best grasp of mastery goals (Lika et al., 2018). This is one of the reasons gamification is believed to be the new way for cyber security awareness delivery.

2.2.2 Instructional Delivery Methods

An instructor can detect nonverbal student indications, change educational methods correspondingly and respond to learner questions as it is done in the classroom context. This is one advantage of the instructor led delivery approach as it is done in a professional manner to suit users. Workers' cyber security knowledge is raised through a range of formal presentations guided by local or outside cyber security specialists in instructor-led delivery (Abawajy, 2014). These techniques are aimed at a wider public usually in a top down scenario and attempt to have an influence on an individual level via an expert based manner.

Although many individuals are interested in school environment delivery techniques as they find it professionally appealing, they have their own limitations. Individuals who engaged in instructor based information security education had such a higher acquisition of information. It also fails since it is focused on rote learning and does not require the user to consider and practise cyber security ideas (Cone et al., 2007). It is considered that practice makes students remember what they have learnt and instructor led doesn't include practice but theory. One approach to overcome these weaknesses is for workers in an institution to contribute their expertise and experiences through engagement, collective conversations and deliberations, and group procedures (Albrechtsen & Hovden, 2010). This sharing is intended to help users understand the consequences of not taking cyber security seriously and also what others have done to protect themselves.

In the attempt to increase the likelihood of common understanding among staff, group based exchange of expertise and observations among workers and information security experts is critical for cyber security to work (Abawajy, 2014). However, this method implies that the people are informed on the issue being addressed and the importance.

3. METHODS

This study uses a pretest and posttest experimental research design as used similarly by (Abawajy, 2014). In experimental research, a pretest and posttest technique are commonly used to assess whether there is a difference between groups in terms of some variable of interest following the application of an intervention. A quantitative technique allowed for the identification of participants' levels of awareness and knowledge.

This is frequently used to validate alternative concepts using a number of participants, as Larson (2015) used in a similar study. The quantitative study in this research is carried out using an online survey technique. An online survey is a handy technique since it allows for the involvement of a diverse audience that is sometimes difficult to reach through conventional ways such as face to face interviews. The online method was also used since social distance is required in the COVID-19 period. Furthermore, individuals from various regions and backgrounds were simply invited to participate in the survey.

3.1 Study Participants and Sampling

Sampling is the method of selecting individuals from a large population for research purposes. Participants in the study are chosen because they can offer detailed descriptions of their experiences to support this research. This research has a total of 30 willing participants as a comparable study by (Abawajy, 2014) employed. The participants were selected in

such a way that the demography is reflective of the real world circumstances. The participants had different educational backgrounds and age groups. Pretest questions were completed by each participant before exposure to the delivery methods. The questions showed that each participant had a different level of cyber security awareness and game knowledge. All participants had smart phones either using it at work or at home. The participants also indicated they each had access to the internet. This demography is typical of real world settings since users have variable and uneven levels of security knowledge.

3.2 Ethical Considerations

There is no physical, psychological, or emotional danger to participants in this study. All information provided is guaranteed to be anonymous and confidential. The study is described in detail to participants so that replies are not skewed. Participants are completely informed that they have the option to withdraw from the research at any time.

3.3 Data Collection Procedure

The purpose of this research is to examine the efficacy of two cyber security awareness delivery strategies, as well as which approach is favoured by the users for organisations to adopt. The study focused on phishing as the human is the weakest link, phishing is deemed fit to educate users in. Also according to the literature study, phishing is one of the most advanced types of cyber threats that has lately made waves. Furthermore, it is one of the most important strategies for leveraging the human element of information security that is sometimes neglected or not well taken care of.

3.4 Study Comparison Approaches

According to (Abawajy, 2014) there is a significant level of user unfamiliarity with popular phishing scams, indicating that users should be educated about online safety measures. The most significant aspect in phishing prevention is cyber security awareness since it deals directly with the human. People are a prime target for phishing fraudsters looking to get sensitive and confidential information or gain access to a system. People find it difficult to identify phishing web sites and emails since they frequently appear authentic or received from trusted sources.

Cyber security awareness programmes assist users establish secure behaviours in handling devices. This leads to a secure workplace environment and data and may prevent security breaches. This study used game based and instructor led security awareness delivery techniques to conduct two cyber security awareness workshops for phishing attacks. These methods teach individuals how to avoid falling victim to phishing attempts. Furthermore, the potential threat and the increasingly various tactics employed by cyber criminals looking to exploit consumers are thought using these two methods.

The participants in this study were randomly allocated to one of the two sessions. Game based cyber security awareness or instructor led cyber security awareness. As a result, this study was able to randomly allocate 15 participants to each experimental group. For example, one group began with game based awareness and then moved on to the instructorled delivery style. It is crucial to highlight that at any one time, one group receives just game based awareness sessions, while another group receives only instructor-led awareness sessions.

The study collected data after each distinct awareness delivery technique to evaluate if the awareness strategy increased the participants' understanding of phishing. Specifically, after each session, respondents must complete the Posttest questions. This was meant to measure their ability to protect themselves from phishing attacks. For example, at the end of a session, participants' ability to detect phishing web sites from a collection of actual and phishing web sites. This allows the participants to reflect on the understanding they received from the previous session.

3.5 Selecting Awareness Delivery Methods

According to Abawajy (2014), increasing general users' understanding of cyber security is frequently dependent on the delivery technique utilised. As previously mentioned, there are several approaches for delivering cyber security awareness. As stated, when picking the delivery modalities, this study took an intentional decision to focus on delivery

methods that haven't been compared yet. Also to minimise the time the individuals spent on the task to a minimum. Furthermore, the contents were made simple to understand for non-technical users.

Most importantly the content was made brief, to the point, and easily accessible through a web browser. For the game based approach, this study searched for a study that is simple to use and built on sound learning science principles. This is to ensure a high degree of knowledge retention while playing the game. A study by Filipczuk et al. (2019) was selected for the game approach. The study focused on materials that were concise, to the point, and easily accessible for download via a web browser.

Each form of delivery addressed the same security awareness issues, and every attempt was made to make each session as similar across the two models as feasible. The chosen training materials highlight warning signs for phishing tactics such as phishing emails and describe easy measures that users may take to protect themselves. This study utilised a brief online article that outlines phishing and anti phishing tactics, including the use of fraudulent emails, for both delivery methods.

This study reviewed the literature and chose Filipczuk et al. (2019) study as the game based information security awareness delivery technique. The reason for selecting Filipczuk et al. (2019) study is that it is incredibly simple to use and requires practically little training. After finishing a game a feedback page appears displaying the scores.

3.6 Metrics for Effectiveness

To measure the effectiveness of the cybersecurity awareness delivery methods, specific metrics were employed. An ANOVA analysis was conducted using SPSS, comparing means derived from the experiment (refer to Table 1). The analysis revealed the instructor-led delivery technique's superiority in boosting users' cybersecurity awareness. The mean scores, mean differences, and awareness level changes provided quantifiable measures of the methods' effectiveness.

3.7 User Preference Measurement

User preference was assessed through participants' votes on their preferred delivery method. A bar chart (refer to Fig. 1) visually represents participants' awareness delivery preferences. At the study's conclusion, participants were queried about their preferred mode of delivery. The options included game-based and instructor-led approaches.

4. RESULTS AND DISCUSSION

The evaluation is carried out in stages. The first step focuses on collecting responses from participants via pretest survey questions in order to assess their phishing attack knowledge levels. Each delivery mode received its own questionnaire, which was suited to the topic's focus. Participants took part in posttest data collection after being exposed to the two delivery techniques. The same questionnaire as the pretest study survey was used, with slight changes to assess any differences in responses. The study's next stage is to determine the preferred delivery mechanism.

4.1 Findings

This part addresses the research questions based on the findings of the research experiment procedure.

4.1.1 User Cyber Security Awareness Delivery Preference

Findings here showed the method of delivery users preferred after the experiment. Fig. 1 is a bar chart showing participants' awareness delivery preference. At the conclusion of the study, participants were asked about their preferred manner of delivering awareness. Participants had to choose between two strategies for delivering cyber security awareness. Surprisingly, just 40% of respondents representing 12 participants chose the game based delivery approach. This was despite the fact that 53.3% or 16 of the respondents said they played games frequently. This indicates that the majority of people were familiar with and comfortable with games, at least when playing for pure amusement. The instructor-led delivery approach, on the other hand, is preferred by 53.3% of the participants. This was intriguing because some game players favoured instructors who led learning to game based instruction.

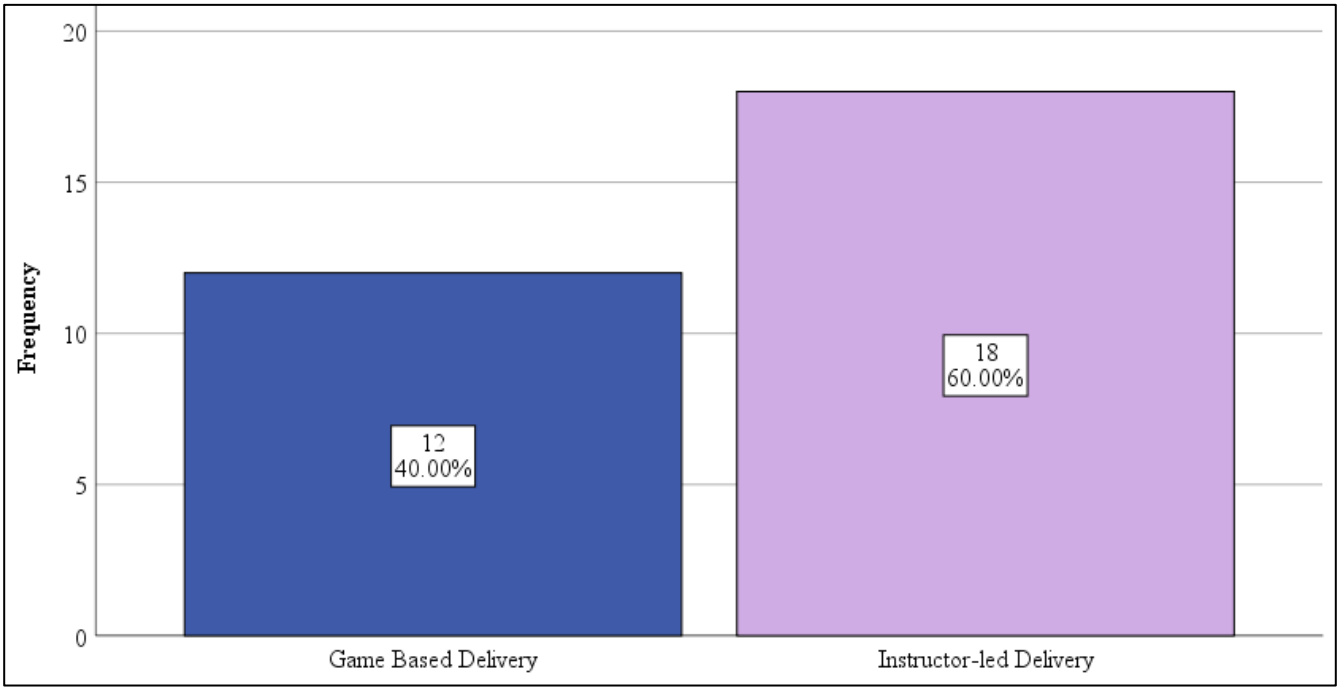

Figure 1. Bar graph of users preference of awareness delivery method.

4.1.2 Effective Cyber Security Awareness Delivery Method

Table 1 represents the results of the study conducted. The table is about cybersecurity awareness delivery preference. The table shows the most effective method of delivery between game-based and instructor-led approaches. An ANOVA analysis was used to compare means of the experiment. As shown in Table 1, the instructor-led delivery technique outperformed the game-based strategy in terms of boosting users' cybersecurity awareness. An ANOVA test was conducted in SPSS to compare the means of the four tests. The pretest's mean difference is 0.067, indicating little differences. Although the instructor-led delivery fared better in terms of mean scores, both delivery modalities raised users' awareness levels. The instructor delivery method was found to be more effective than the game-based distribution strategy based on the means in table 1.

	N	Mean	Std. Deviation	StD. Error	Lower Bound	Upper Bound	Minimum	Maximum
Instructor-led delivery pretest	15	7.40	1.595	.412	6.52	8.28	4	10
Game-based Delivery pretest	15	7.33	1.047	.270	6.75	7.91	6	10
Instructor-led delivery posttest	15	9.40	.632	.163	9.05	9.75	8	10
Game-based Delivery posttest	15	9.13	.743	.192	8.72	9.54	8	10
Total	20	8.32	1.420	.183	7.95	8.68	4	10

Table 1. Statistical data of experiments test scores

4.2 Effective Instructor-Led Cybersecurity Awareness Delivery

The study's exploration of cybersecurity awareness delivery methods revealed that the instructor-led approach emerged as not only more effective but also preferred by users. The success of the instructor-led method can be attributed to various factors contributing to heightened awareness levels and user satisfaction. Firstly, the personalised interaction facilitated by direct engagement between the instructor and participants proved highly effective, allowing for immediate clarification of complex concepts. Real-world application, through the incorporation of relevant examples, enhanced the method's effectiveness by making content more relatable. The structured learning environment provided by instructor-led sessions positively influenced retention and comprehension. Timely feedback, authoritative presence, and tailored adaptation to participants' needs further distinguished the instructor-led approach. Users, despite familiarity with gaming, expressed a preference for the instructor-led method, valuing its personalised, practical, and adaptable characteristics. In summary, the success of the instructor-led delivery method in cybersecurity awareness underscores the significance of tailored and interactive approaches for effective learning.

5. CONCLUSION

Governments and other organisations can successfully improve people's cyber security by addressing concerns of cyber security. One of the key conclusions is that the user prefers instructor led delivery over game based training. Despite the fact that the majority of the participants in the study were frequent game players, they favoured classroom based learning. The study also discovered that instructor delivery is more successful than game based learning in improving user awareness. These data support the underlying idea that the efficiency of awareness is determined by the way of delivery. Users who are more aware will be more inclined to implement better security procedures. As a result, it's possible that increasing cybersecurity awareness could be one of the most effective ways to address the issues surrounding cyber security.

In addition, frequent game players do not want to learn through games, according to the study findings. Furthermore, the majority of the participants had undergraduate or diploma level education. The research has identified numerous critical elements in the analysis that might be used as focal points for further research or future research projects.

5.1 Research Achievements

The purpose of this research was to find a solution to the problem of cyber security threats by using cyber security awareness distribution methods as a crucial answer. The literature review for this study covered a wide range of cyber security problems and numerous delivery techniques. When it comes to cyber security awareness delivery methods, the study has also added valuable materials to the research database. For instance the study has provided knowledge about the preferred delivery method for users as well as the effectiveness of these methods.

5.2 Research Limitations

The study focused on cyber security awareness delivery methods, which is one of the most important aspects of the cyber world. In terms of dangers and steps to be done to protect against cyber security it has a broad reach. Given this, the study concentrated on phishing, which is a disadvantage because there are other other cyber security challenges to address. The number of participants in the study was also a restriction, and in the future, the number of participants will be expanded in order to reach a more generalised conclusion.

5.3 Future Work

Further investigation reveals that the findings in this study also serve as a solid foundation for future research in awareness delivery strategies. Combining the insights collected about preferred user awareness to age groups is one topic of future exploration. In the future, more study is being planned. Furthermore, the intention is to duplicate this experiment by increasing the population size and observing any side effects throughout the learning experience, such as gender and age discrepancies, educational level inequalities, and efficiency in terms of time spent. Although many of the concepts addressed in cyber security awareness training are universal, it is frequently necessary to tailor such training to the specific needs of the participants. As a result, one way to broaden our research is to look into how different firms have different wants, but the delivery model ignores this thereby broadening the model's applicability to all enterprises of all types and sizes.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237–248. https://doi.org/10.1080/0144929x.2012.708787

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432–445. https://doi.org/10.1016/j.cose.2009.12.005

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. Journal of Information & Knowledge Management, 15(01), 1650007. https://doi.org/10.1142/s0219649216500076

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In The Economics of Information Security and Privacy (pp. 265–300). Springer Berlin Heidelberg.

Bahrini, M., Volkmar, G., Schmutte, J., Wenig, N., Sohr, K., & Malaka, R. (2019). Make my phone secure!: Using gamification for mobile security settings. Proceedings of Mensch Und Computer 2019.

Baral, G., & Arachchilage, N. A. G. (2019). Building confidence not to be phished through a gamified approach: Conceptualising user's self-efficacy in phishing threat avoidance behaviour. 2019 Cybersecurity and Cyberforensics Conference (CCC).

Canova, G., Volkamer, M., Bergmann, C., & Borza, R. (2014). NoPhish: An anti-phishing education app. In Security and Trust Management (pp. 188–192). Springer International Publishing.

Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. Computers & Security, 97(101959), 101959. https://doi.org/10.1016/j.cose.2020.101959

Cone, B. D Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. Computers & Security. https://doi.org/10.1016/j.cose.2006.10.005

Dincelli, E., & Chengalur-Smith, I. (2020). Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. European Journal of Information Systems: An Official Journal of the Operational Research Society, 29(6), 669–687. https://doi.org/10.1080/0960085x.2020.1797546

Filipczuk, D., Mason, C., & Snow, S. (2019). Using a game to explore notions of responsibility for cyber security in organisations. Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems.

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. Procedia Computer Science, 181, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Karagiannis, S., Papaioannou, T., Magkos, E., & Tsohou, A. (2020). Game-based information security/privacy education and awareness: Theory and practice. In Information Systems (pp. 509–525). Springer International Publishing.

Larson, S. (2015). The cyber security fair: An effective method for training users to improve their cyber security behaviors. Information Security Education Journal, 2(1), 11–19.

Lika, R. A., Murugiah, D., Brohi, S. N., & Ramasamy, D. (2018). NotPetya: Cyber Attack Prevention through Awareness via Gamification. 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE).

Malone, M., Wang, Y., James, K., Anderegg, M., Werner, J., & Monrose, F. (2021). To gamify or not?: On leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention. Proceedings of the 52nd ACM Technical Symposium on Computer Science Education.

McCoy, C., & Fowler, R. T. (2004). You are the key to security: Establishing a successful security awareness program. Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services.

Mccoy, C., & Fowler, R. T. (2004). You are the key to security: Establishing a successful security awareness program. In Proceedings of the 32nd annual ACM SIGUCCS conference on User services.

Muntean, C. I. (2011). Raising engagement in e-learning through gamification. Proc. 6th International Conference on Virtual Learning ICVL, 1, 323–329.

Nguyen, T. A., & Pham, H. (2020). A design theory-based gamification approach for information security training. 2020 RIVF International Conference on Computing and Communication Technologies (RIVF).

Qusa, H., & Tarazi, J. (2021). Cyber-hero: A gamification framework for cyber security awareness for high schools students. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC).

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. The Journal of Digital Forensics Security and Law. https://doi.org/10.15394/jdfsl.2017.1476

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125–128.

Sharif, K. H., & Ameen, S. Y. (2020). A review of security awareness approaches with special emphasis on gamification. 2020 International Conference on Advanced Science and Engineering (ICOASE).

Smith, D. T., & Ali, A. I. (2019). YOU'VE BEEN HACKED: A TECHNIQUE FOR RAISING CYBER SECURITY AWARENESS. Issues in Information Systems, 20(1).

Stefaniuk, T. (2020). Training in shaping employee information security awareness. Journal of Entrepreneurship and Sustainability Issues, 7(3), 1832–1846. https://doi.org/10.9770/jesi.2020.7.3(26)

Tasevski, P. (2016). IT and cyber security awareness – raising campaigns. Information & Security An International Journal, 34, 7–22. https://doi.org/10.11610/isij.3401

van Niekerk, J., Thomson, K.-L., & Reid, R. (2013). Cyber safety for school children: A case study in the Nelson Mandela metropolis. In Information Assurance and Security Education and Training (pp. 103–112). Springer Berlin Heidelberg.

Van Niekerk, J., Thomson, K.-L., & Reid, R. (2013). Cyber safety for school children: A case study in the Nelson Mandela metropolis. In Information Assurance and Security Education and Training (pp. 103–112). Springer.

van Steen, T., & Deeleman, J. R. A. (2021). Successful gamification of cybersecurity training. Cyberpsychology, Behavior and Social Networking, 24(9), 593–598. https://doi.org/10.1089/cyber.2020.0526

Van Steen, T., & Deeleman, J. R. A. (2021). Successful gamification of cybersecurity training, " Cyberpsychol. Cyberpsychol. Behav. Soc. Netw, 24(9), 593–598.

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's." Heliyon, 5(12), e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Yaokumah, W. (2016). The influence of students' characteristics on mobile device security measures. International journal of information systems and social change, 7(3), 44–66. https://doi.org/10.4018/ijissc.2016070104