Journal of Cybersecurity and Privacy

MDPI

Article

A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania

Rosemary Cosmas Tlatlaa Panga [1,*], Janeth Marwa [1] and Jema David Ndibwile [2]

[1] School of Computational and Communication Sciences and Engineering, Nelson Mandela African Institution of Science and Technology, Arusha P.O. Box 447, Tanzania; janeth.marwa@nm-aist.ac.tz
[2] College of Engineering, Carnegie Mellon University Africa, Kigali BP 6150, Rwanda; jndibwil@andrew.cmu.edu
* Correspondence: rozie.tlatlaa@gmail.com

Abstract: Recently, phishing attacks have been increasing tremendously, and attackers discover new techniques every day to deceive users. With the advancement of technology, teenagers are considered the most technologically advanced generation, having grown up with the availability of the internet and mobile devices. However, as end-users, they are also considered the weakest link for these attacks to be successful, as they still show poor cybersecurity hygiene and practices. Despite several efforts to educate and provide awareness on the prevention of phishing attacks, less has been done to develop tools to educate teenagers about protecting themselves from phishing attacks considering their differences in social-economic and social culture. This research contributes a customized educational mobile game that fits the African context due to the participants' existing differences in social-economic and social culture. We initially conducted a survey to assess teenagers' phishing and cybersecurity knowledge in secondary schools categorized as international, private, and government schools. We then developed a customized mobile game based on the African context taking into consideration participants' differences in social-economic and social culture. We compared the performance of phishing knowledge of teenagers using a game and a traditional teaching method. The traditional teaching method was presented by the reading notes method. The results revealed that teenagers' phishing and cybersecurity knowledge differs based on their socioeconomic and social culture. For instance, international, private scholars, and those who live in urban areas have better phishing knowledge than those from government schools and those who live in rural areas. On the other hand, participants who had a poor performance in the first assessment improved their knowledge after playing the game. In addition, participants who played the game had retained their phishing knowledge more, two weeks later, than their counterparts who read only notes.

Keywords: phishing; teenagers; cybersecurity; customized mobile game

Citation: Panga, R.C.T.; Marwa, J.; Ndibwile, J.D. A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania. *J. Cybersecur. Priv.* **2022**, *2*, 466–489. https://doi.org/10.3390/jcp2030024

Academic Editor: Danda B. Rawat

Received: 20 April 2022
Accepted: 15 June 2022
Published: 22 June 2022

1. Introduction

Rapid technological change has brought about massive communication technologies across the world through internet services aimed at information exchange [1]. However, increased use of technology has been misused, causing greater losses to organizations and users [2]. In recent years, we have witnessed a significant increase in the use of communication technologies, especially mobile phone communication, in developing nations; Tanzania is one of them [3]. The mobile communication rate increased by 21% in 2019, while internet users increased to 29,071,817 in March 2021 [4]. These technologies are new in developing countries. Therefore, crimes associated with these technologies are also unfamiliar to people.

Children and adolescents are known as the digital group that developed with the presence of the internet [5]. This group has been exposed to smartphones, tablets, and gaming systems due to the advancement of technology [6]. In developed countries, 69%

of children under 12 years of age have smartphones [7]. On the other hand, in Tanzania, about 50% of the teenagers reported having their own mobile phones, where almost 60% own SIM cards. Those who own SIM cards report borrowing or renting phones from friends and parents. Furthermore, about 76% admitted using mobile phones at home, and 86% reported having an internet connection [8]. Again, mobile phone usage is based on shared access [9]. Therefore, teenagers use mobile phones to engage in online activities such as social networking, playing games, and watching videos on sites such as YouTube and Vimeo due to the interactive capabilities of the mobile phone and the low cost of the internet [5]. However, the extensive use of social networks by teenagers has created privacy and security issues [10].

According to [5,11], teenagers are still characterized by poor cybersecurity hygiene and practices; therefore, as end-users, they are the weakest link for these attacks to succeed. As a result, this group becomes a potential victim and is vulnerable to cyberattacks [12]. This calls for attention towards educating teenagers about various cyberattacks, including phishing attacks [13].

Phishing is a social engineering attack in which criminals impersonate a trusted third party to persuade people to visit fraudulent websites or download malicious attachments or links [14]. These actions compromise the security of individuals and organizations. Phishing attacks could be initiated using deceptive email addresses or instant messages that appear to be from trusted sources, leading them to click on malicious links [15]. Attacks are based on a combination of tactics that influence human decision-making through authority, time pressure, and polite tones. Phishing attacks increase gradually every year and doubled in 2020 due to the COVID-19 pandemic, which forced many activities, such as conferences, workshops, and classes, to be conducted online [16]. Attackers exploit human curiosity and fear to manipulate victims [17].

End-users who have inadequate information and cybersecurity awareness find it difficult to distinguish between phishing and legitimate information, and as a result, they become substantial victims. The increasing trend of phishing attacks has resulted in various repercussions due to end-users' lack of knowledge and awareness. The damage from phishing attacks has cost the world USD 6 trillion in 2021, up from USD 3 trillion in 2015 [18]. One million children in developed countries have also been victims of ID theft which cost USD 2.6 billion. In developing countries, 71% of the users have also been victims and suffered the negative impacts of phishing. Moreover, 54% of Tanzanian teenagers have reported having received improper information at least once, and they usually forward this to people on their network.

Several studies have exploited the use of games and different training materials to aid in cybersecurity and phishing awareness. For example, [19] designed a game to measure the digital literacy of children's online password behavior. In addition, [12] has conducted training for children aged 9–12 years to teach them how to combat phishing. However, without knowledge, the repercussions of these attacks on internet and mobile device users are still difficult to counteract. However, most of the research on phishing detection has focused on adults and university students, while teenagers remained an understudied population [5]. Furthermore, to our knowledge, no research addresses the differences in phishing knowledge and attitudes of teenagers based on social-economic and social culture, especially in developing countries. With the increase in the use of mobile devices, the internet, and social networks as the primary platforms for attackers to manipulate users, it is critical to investigate the cybersecurity and phishing expertise of teenagers, as well as contributing factors.

This study aims to explore the access of teenagers to mobile phones, the internet, social networks, and email accounts. In addition, we examine the impact of socioeconomic status and social culture on awareness of phishing and cybersecurity among adolescents. Initially, we surveyed 121 teenagers with an average age of 17 years from international, government, and private schools to determine their knowledge about phishing and cybersecurity and the use of the internet, social networks, and mobile devices. We hypothesize that social-

economic and cultural differences reflect phishing and cybersecurity awareness among teenagers. Furthermore, we posit that urban adolescents have better knowledge of phishing than those in rural areas. Due to the disparities in their academic orientations, we believe that international school teenagers have a better comprehension of phishing than teenagers from government and non-international private schools. In Tanzania, international schools are considered to be of higher educational quality than other schools such as government and non-international private schools. Furthermore, their students are those with good socioeconomic status and have exposure to different lifestyles.

Our contributions are as follows.

1. Assess the use of the internet, mobile devices, and email among adolescents in developing countries (the case of Tanzania).
2. Assess the level of cybersecurity and phishing knowledge and the differences between adolescents in social-economic and social culture.
3. Improve the knowledge of teenagers about phishing using a customized mobile game based on the results obtained and the relevance of the social culture of the participants.

Notes, videos, and email bulletins have recently been adopted to teach cybersecurity and phishing; however, their impact on user engagement, knowledge retention, and habit transformation has been minimal [20]. We believe that due to differences in social culture and socioeconomic status, knowledge of cybersecurity and social engineering, such as understanding of phishing, will vary substantially between teenagers. Some studies have attempted to make similar comparisons in adolescents, but only in developed countries [19,21–23]. Little or no information is available in developing countries, such as those in Sub-Saharan Africa, where there are vast differences in living styles and classes. Additionally, those studies did not incorporate all phishing metrics in one package. As a departure from previous research, this study presents a mobile game that could teach teenagers about various phishing methods, how they are perpetrated, and how they can be avoided to protect their online safety in an African-themed environment.

Our findings suggest that most teenagers (60.75%) use mobile devices, the internet (64.46%), email (74%), and social media platforms (92.6%). Furthermore, their socioeconomic and cultural disparities are related to their phishing knowledge ($R = 0.56$, $p < 0.001$). However, with greater variance in their social culture and economics, their level of knowledge is unpredictable. In this sense, if no intervention is provided, teenagers in our scope of experiment are more likely to fall victim to phishing attacks in the future [24].

In contrast, educational games have been proven to effectively teach diverse cybersecurity topics such as cautious and secure online habits, threats and attacks, malware, and other issues that compromise cybersecurity [25]. However, previous studies have only looked at one parameter of the phishing tactic. For example, [26] teaches how to detect phishing URLs, [19] examines user password behavior, and [27] teaches general cybersecurity concepts that are not specific to phishing.

The proposed game incorporates several parameters of phishing scams used by attackers, such as short messages, email, and phone calls. We chose these parameters because in our first survey, most of the participants reported having experienced suspicious calls (52%), messages (70.5%), and emails (41.1%) compared to other techniques used to initiate phishing attacks. In addition, this game has covered the differences in social-economic and social culture. For social-economic reasons, the game will be available for free on the Google Play Store. Moreover, participants in this study preferred the game to be on Android mobile phones (59%) than other devices because Android mobile phones are relatively cheaper and are easily accessible to most groups of people.

In addition, the game is developed with African contexts in mind for social culture, including the environment and objects used based on things familiar in the environments of participants. Therefore, we used African characters and African-themed environments to make it easier for participants to acquire the intended knowledge. The majority of teenagers, 99% of boys and 94% of girls, play video games [28] and it is estimated that teenagers spend more than 20 h a week playing games [29]. Therefore, we hypothesize that

it could be easier to transfer knowledge through mobile games than traditional methods such as books, notes, and lectures.

2. Background and Related Work

This section highlights numerous efforts to avoid phishing and the value of educational games in teaching users how to avoid phishing attacks.

2.1. Phishing

Phishing sites have become more prevalent. Recently, there has been a gradual increase due to the COVID-19 pandemic forcing many activities, such as conferences, workshops, and classes, to be conducted online [30]. Furthermore, during the 2016 US presidential election, fake Google security emails were used to trick staff into sharing passwords and accessing sensitive information. However, unlike the consequences of other phishing assaults, this one attempted to disclose their contents and inner workings in order to tarnish their reputations [31].

Inappropriate and time-consuming user training in cybersecurity contributes to vulnerabilities like these [20]. Individuals are prone to phishing attempts since mimicked websites look very similar to legitimate ones, and even when participants are told about the risk of such assaults, they have difficulty identifying phishing sites [32]. These attacks not only affect and target adults; they also significantly affect young people [5]. Statistics show that phishing was ranked among the top seven digital threats for teenagers and children [33]. The lack of cybersecurity education in children and poor digital hygiene contribute to successful attacks [11]. Furthermore, teens are the target group for obtaining their identity details and using their personal information to earn money and credit cards [34].

Teenagers are the most vulnerable and weakest target group for phishing attacks for several reasons. First, they are exposed to the internet and social networks early [5]. Furthermore, they prefer to use simple passwords with their important personal details, leaving footprints on social networks such as phone numbers, email addresses, and date and year of birth [19]. Teenagers also have the culture of sharing sensitive data with friends on social networks [35]. The attackers collect this information and use it to target individuals together with family members and other people connected to the victim's network [12].

2.2. Anti-Phishing Efforts in Children and Teenagers

The rise of phishing and its consequences have led researchers to develop and establish various tools and mechanisms to protect people from phishing attacks. For example, Kumaraguru et al. [36] implemented the email system teaching people how to be protected from phishing while communicating via email. Investigations were carried out on the phishing training incorporated into the design. As a result, training was seen as more effective compared to the practice of sending security notices. More research has been conducted; for example, [5] focused on phishing detection and prevention in teenagers focusing on phishing susceptibility. However, the overall performance of the phishing detection of the participants was poor due to risk-taking characteristics and a lack of awareness of the phishing tactics.

Lastdrager [12] has implemented phishing prevention training for children aged 9 to 12. The training took the form of a story told during a class lecture, followed by a paper-based test for the kids to identify phishing and authentic emails and websites. Children's ability to recognize phishing has improved due to training. However, the children's skills deteriorate in the 2–4 weeks after training. More efforts have been explored; for example, [5] has explored the identification and prevention of phishing in adolescents and has focused on the susceptibility of phishing in a population. However, the overall performance of the participants in phishing detection was poor, which is determined by risk-taking attributes and a lack of awareness of phishing tactics. Kumaraguru et al. [26] created a PhishGuru training system to teach people not to fall for phishing attacks. The

system was also designed to measure the retention of knowledge by participants for longer periods of time. However, the results revealed that teenagers were more susceptible to phishing attacks than their older counterparts during the study period. Furthermore, in an investigation of user susceptibility to phishing by delving into the mechanisms that can influence individual victimization, 47% of the participants were found to have disclosed personally identifiable information on a bogus page, and the findings suggest that students are a particularly vulnerable target for phishing attacks. As a result, it is recommended that end-user solutions be developed to combat phishing attempts [37].

2.3. Educational Mobile Games

Anti-phishing protection has great difficulty capturing the attention of end-users. Notes, videos, and email bulletins are all common resources that users use to address and educate users about phishing assaults. Their application, on the other hand, has had a negligible influence on user engagement, information retention, and habit change [20]. Educational games, on the other hand, have been shown to be useful techniques to teach a variety of cybersecurity topics, including safe and secure online habits, threats and assaults, malware, and other cybersecurity issues [25].

Mobile games have been viewed as effective training and a tool for persuading players to change their habits [21]. However, games only provide learners with interactive opportunities if certain aspects are included, such as user requirements and needs [38]. As a result, more research should be focused on the evolution of educational games in the supply of cybersecurity education, particularly anti-phishing awareness. Other tools, training programs, and procedures have also been found to be less effective in influencing user behavior and logical thinking than games [39].

Several educational games have already been developed; for example, Maqsood [19] created a game to assess children's digital literacy with respect to their online password habits. The game was designed to assess literacy in children aged 11 to 13. The results showed that the knowledge and behavior of the children changed immediately after playing the game and a week later. However, the design relied on procedural rhetoric and did not employ other mechanisms and principles, such as refection and conceptual principles. Additionally, when evaluating the completion of the task by the players, the game does not include time, which can lead to a learning process that is not exciting for the players.

The work of Patrickson et al. [22] presents a 2D game to teach students about phishing. The game improved the knowledge of the participants from 20% to 80% from the pre-test and post-test. However, the game involves only one phishing parameter, while several parameters are used to initiate these attacks. Additionally, players do not receive immediate feedback based on their actions and the reasons for failure during gameplay. This may cause players not to be attentive and forget and repeat their unusual behaviors, causing them to fall for phishing attacks continuously. Wen et al. [20] introduced anti-phishing training using a role-playing phishing simulation game to teach people how to defend themselves from phishing. The game has been effective in helping to improve the knowledge of participants compared to other training tools. However, it addresses only a single phishing parameter. Furthermore, it relies only on the use of email rules, while these rules are subject to change based on new tricks introduced every day by attackers to deceive users. In addition, the content of the game requires the player to read more, making it boring and tiresome. Instead, some graphics and animated objects may be used to increase user engagement and make the game fun. The work also limited the scope of participants to professionals, while those who do not have computer skills remained understudied.

Baslyman et al. [23] present a board game that teaches about online phishing scams. The results show that the game improved the knowledge and awareness of the participants and was engaging and fun. However, the game component for reward and punishment involves police, whereby it is biased and causes feelings of inferiority in some groups of participants such as children since most people hesitate to go to jail or visit a police station; hence, players will not be flexible and free to play the game. Moreover, some features

require players to visit an online link to receive some instructions, which may lead them to incur some cost. The design also requires participants to have expertise in the computer field, which may limit the scope of users when it may be required for knowledge delivery in other groups. Dixon et al. [21] designed a game to engage users in an educational game to combat phishing. However, participants found the game difficult because it does not consider cultural differences. The contents used were unfamiliar to most of the participants, and hence it made it difficult for the users to play and acquire the intended knowledge. The limitations of the previous work are summarized in Table 1.

Table 1. Summary of the limitations of related works.

Related Works	Limitations
[18]	- Did not employ other mechanisms and principles such as refection and conceptual principles.
[19]	- Address only single phishing parameter. - Relies only on the use of email rules which are subject to change. - Limited the scope of participants to professionals.
[20]	- Used contents unfamiliar to most of the participants.
[21]	- Involved only one phishing parameter. - No immediate feedback for players.
[22]	- Some game features require players to visit online link to receive some instructions. - Needs participants to have expertise in the computer field.

Currently, despite the multiple studies mentioned above, only a handful of them have begun to investigate the role of younger generations in phishing. However, most studies have not taken into account phishing and cybersecurity awareness due to social-economic and cultural variations among teenagers.

Furthermore, just a little research has examined the game's performance in terms of knowledge transfer, and most of the studies above do not include knowledge retention. As a result, the objective of this study was to create a game that addressed knowledge differences between teenagers based on differences in their socioeconomic and cultural backgrounds. The game will be available for free download from the Google Play Store for social reasons. Because Android phones are very inexpensive and accessible to most people, participants in this survey opted to play the game on them (59%). Additionally, the game is structured to take into account the African setting of social culture, including the environment and objects used, based on things that participants are familiar with. To make learning easier for participants, the game was created with African characters and African-themed environments. Most teenagers (99% of males and 94% of females) play video games [28] and are said to spend more than 20 h a week doing so [29]. As a result, it is thought that learning through mobile games would be easier than learning through traditional means such as books, notes, and lectures. Furthermore, due to its advantages in retaining knowledge longer than other traditional techniques, the game can teach phishing and other cybersecurity topics to people of various ages.

3. Part 1 of the Study

This section explains how we conducted our first study on evaluating teenagers' phishing and cybersecurity expertise, including the study approach, data collection and analysis, and the results.

3.1. Participants Recruitment

For this part of the study, we surveyed 121 teenagers, males (51.2%) and females (48.8%), with an average age of 17 in three secondary school categories; government, international, and private. We recruited participants using random sampling techniques.

All participants provided their informed consent in a written form and were compensated for their time. In Tanzania, however, an adult is 18 years old; hence, volunteers under the age of 17 were unable to provide their own consent. Instead, we requested their guardians, in this case, their teachers, to offer their written informed consent to engage in the study on their behalf. The proportion of participants with school categories is shown in Table 2.

Table 2. Participants in school categories.

School Categories	Participants
International	33.88%, n = 41
Private	33.06%, n = 40
Government	33.06%, n = 40

3.2. Study Method

The design science research methodology and a quantitative method were used. The survey, which consisted of multiple-choice questions, was performed both physically and online using Google Forms. The questions were divided into two sections. The first section was about the demographics of the participants, including age, gender, and education level, and the second section asked about cybersecurity behavior and phishing knowledge (e.g., 'Is the device you are using protected by a password/fingerprint/pattern?', 'Do you share your device secret information (username, password) with friends?', 'Should you download any app or attachment from unknown sources or sent to you by an unknown sender?', 'Imagine your close relative texting you from a new number saying that he had a bad motorcycle accident and asking you to send him money right away so he can get first aid, what will be your response?'). The aim is to assess participants' general phishing and cybersecurity knowledge and awareness regarding their differences in social-economic and social culture.

3.3. Results for Part 1

This subsection summarizes the findings of our first survey of participants' cybersecurity and phishing expertise based on their school categories and residences.

Teenagers' Phishing and Cybersecurity Knowledge

We analyzed teenagers' phishing and cybersecurity knowledge according to school categories and residence places. Participants in international schools were found to have more knowledge about phishing (58%) than those in private schools (25%) and the government (19%), based on high scores on questions measuring knowledge about phishing, as shown in Figure 1.

Furthermore, teenagers living in urban areas are more knowledgeable than those in suburban and rural areas by 59%, 28%, and 13%, respectively, as indicated in Figure 2. The reasons could be having more exposure, better social-economic background, and different social culture than their counterparts. Tucker et al. [40] discovered that participants with a higher socioeconomic status had greater knowledge levels. Good social-economic background enables them to frequently access mobile phones, the internet, and social networks, allowing them to learn several issues from others and gain self-experience.

Although a few participants showed better knowledge for those living in town and from international schools, a significant proportion of participants still had very little cybersecurity awareness. This is indicated by the participants (54%, n = 65) who said that they would likely download applications and attachments from untrustworthy sources, which is a common way to launch phishing attempts. Furthermore, 53.7% of the participants who reported sharing their mobile phones with friends described the most threatening risky behavior and poor cybersecurity hygiene. Sharing devices creates a loophole for many users to be easily exploited once their confidential information is accessed by third parties and shared publicly, either intentionally or accidentally. In addition, it is not easy

to trace the activities performed by those who share devices. These may result in the further propagation of attacks on individual networks, communities, or family members. These attacks are the ones that are mainly easy to carry out. They have a high effect, which requires no sophisticated tools; it is just a mind game or psychological manipulation. Therefore, it is important for these teenagers to avoid phishing by being aware of the tactics used by attackers.

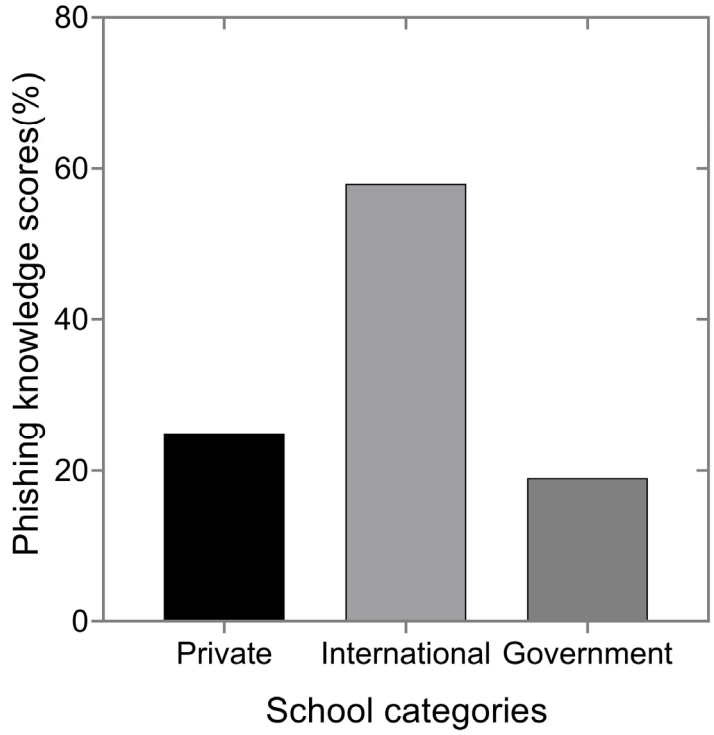


Figure 1. Teenagers' phishing knowledge performance based on school categories.

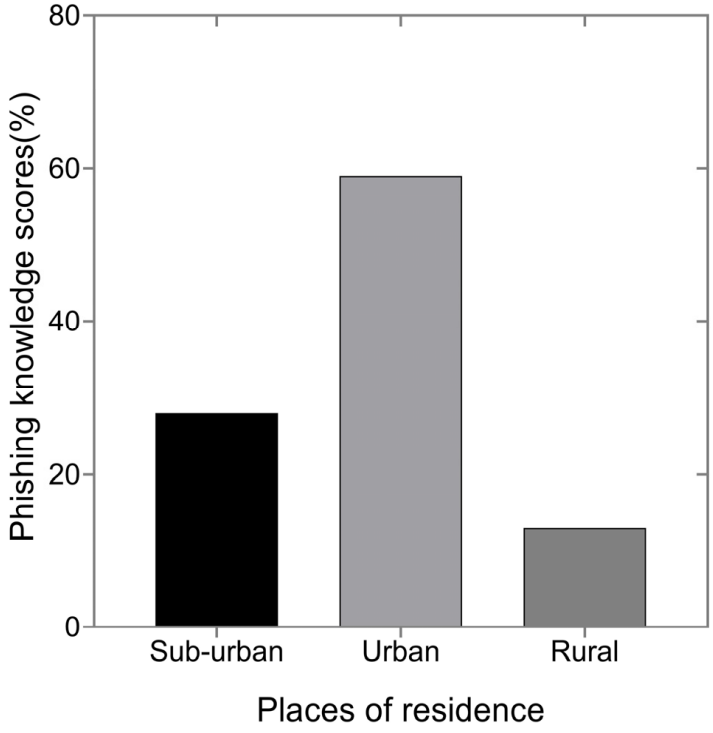


Figure 2. Teenagers' phishing knowledge performance based on their places of residence.

We see the need to educate teenagers on how to prevent phishing attacks using a mobile-based educational game. The research by [21,25,38] found that the game is an effective tool to teach various cybersecurity topics such as safe and cautious online habits, threats and attacks, malware, and other cybersecurity topics. The game has been considered a useful training tool and gives encouragement for a change in player habits. However, it always gives learners interactive methods only if some features, such as user needs and requirements, and the specific issue, have been incorporated within. Therefore, we developed a customized mobile game to teach teenagers some common parameters that attackers mostly use to initiate phishing, such as emails, messages, and phone calls.

4. Part 2 of the Study

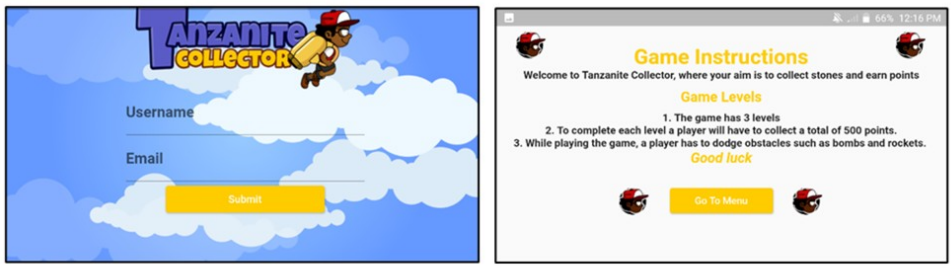
This section highlights the second part of the study, which used a customized mobile game to improve the performance of teens' phishing expertise. This section includes strategies for game creation and implementation, as well as testing procedures and results.

4.1. Game Design and Implementation Methods

We developed a game called Tanzanite Collector using a Flutter framework with the Fame game engine and Dart language. Tanzanite is the name of a popular blue gem that is only commercially produced in a small area of Tanzania [41]. We chose the name Tanzanite because it is familiar in our participants' environment. The design came from the first study, in which 35% of the participants chose the environment of the African theme and the African character over other themes of the games presented. The preferred features were winner/loser (50%), and the character chosen was animated people (35%). Tanzanite Collector is designed to teach teenagers about accuracy and assurance of information to enable them to make the best decision once they face unsafe incidents in real life that compromise individual security and the security of personal data.

4.1.1. Storyline

Tanzanite collector is the main character of the game. The Tanzanite Collector game has a welcome screen with a form to fill in players' details such as a username for identifying a player by her name while playing the game, as depicted in Figure 3a. Furthermore, another screen has game instructions for a player, as indicated in Figure 3b. The task is to collect authentic Tanzanite stones and avoid malicious ones. A player must earn five hundred points to complete a specific level before running out of time, while avoiding obstacles such as bombs and rockets. Illegitimate Tanzanite stones represent one phishing parameter at each level. Once a player collects good stones, she earns ten points, and she loses five points by collecting bad stones.



(a) (b)

Figure 3. The starting screen interfaces of the game; (**a**) A Welcome screen with a form to fill in players' username and Email to reflect a player by her name while playing the game; (**b**) General game instructions for players.

Furthermore, a player can increase her life by collecting red copper lifeline stones, as depicted in Figure 4. The lifeline can increase the player's life by one life, and one lifeline is reduced after a player is bombed or hit by obstacles such as rocket bombs and wall

angels. On the other hand, a player can lose the game by collecting up to ten malicious stones, running out of time (three minutes) per level and losing all life by being bombed and hitting the obstacles. When losing a game by collecting up to ten malicious stones, the game ends, and a player must read phishing notes to improve her knowledge and play again until she succeeds with one level before moving into the next higher level. When the player completes one level, she is awarded points and an additional airtime voucher to motivate her in the next level, as indicated in Figure 5. Finally, a summary of the phishing concept is incorporated into a game at the end of each level, as shown in Figure 6.

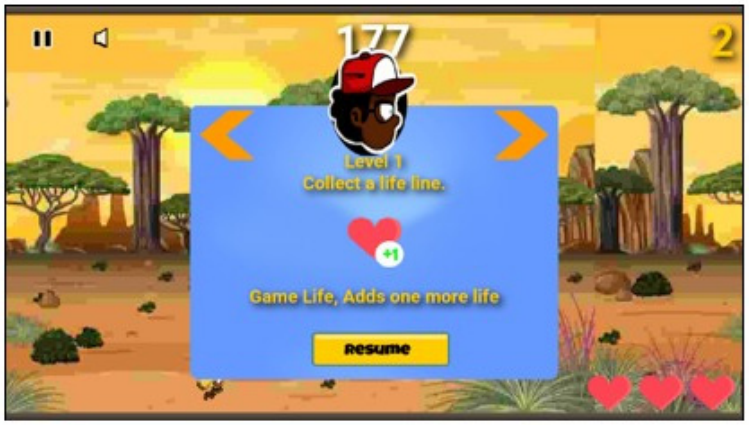


Figure 4. The lifeline stone to add a players' life during the game play.

Figure 5. The rewards that are given to a player after succeeding at the game level.

Figure 6. The example of the summary embedded at the end of a specific game level that teaches a player the indicators of phishing emails such as emails that start with generic names instead of a personal name.

4.1.2. Technology

There are mixed numbers of legitimate and illegitimate Tanzanite stones of different colors, together with lifelines at each level, as shown in Figure 7. To engage the user and make the game enjoyable, we employ background music, additional graphics, and different colors at each level. Furthermore, we applied the theory of pull of gravity to allow the collector to move up and down during the game play, as denoted in Figure 8. Additionally, different sounds have been embedded with each stone during collection to make the player feel and notice the differences with respect to her actions when collecting stones.

Figure 7. Illegitimate Tanzanite stones with different colors representing phishing concepts (emails, messages, and calls) embedded in level 1, level 2, and level 3, respectively.

Figure 8. The up and down movement of a Tanzanite collector applied using the theory of pull of gravity.

4.1.3. The Game Design Principles

The main objective of the Tanzanite Collector game is to teach how messages, emails, and phone calls are used to initiate phishing attacks. We use the refection principle and the conceptual and procedural principles to achieve these objectives, adopted from [42]. In the refection principle, we summarize the phishing concept at the end of each level of the game. Furthermore, the procedural and conceptual principles are applied in a game. For example, the game will display different stones, which requires the player to identify which one reflects phishing (procedural) as shown in Figures 7 and 9, and teaching a player

concept such as emails which start with generic salutations such as 'Dear valued member', 'Dear account holder', or 'Dear customer', without specifying a username being phishing emails (conceptual), as indicated in Figure 6.

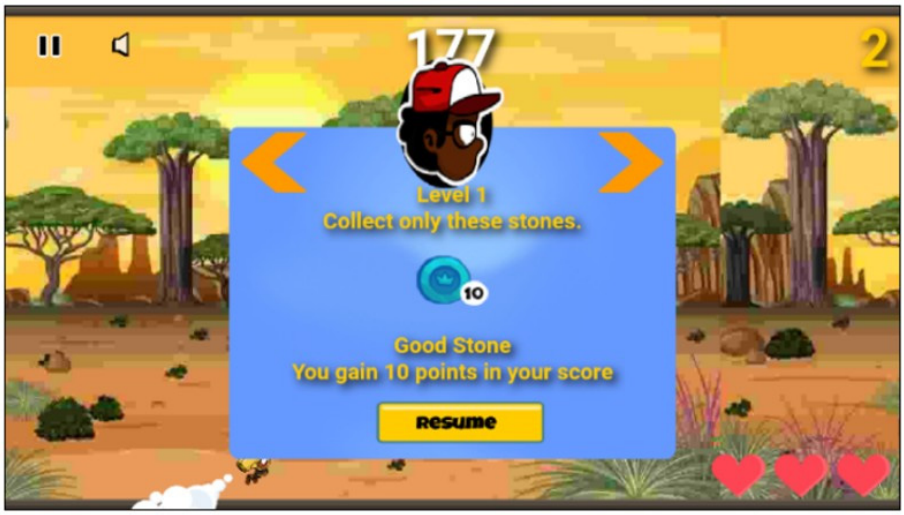


Figure 9. The legitimate Tanzanite stone required to be collected by a player.

4.1.4. Game Mechanics

The game is divided into three levels where a timer is set at each level that only gives participants three minutes to complete the level. The collector is provided with several Tanzanite stones in two categories, legitimate stones (Figure 9) and one representing a phishing concept for the player to learn, as depicted in Figure 7. The player taps a mobile phone screen to move around a collector to collect genuine Tanzanite stones and skip the fraudulent ones. On successfully collecting the good stones, she is awarded ten points, while if she collects up to ten bad stones, a severe penalty is given by losing a life, and the game ends. The player is then warned to improve her knowledge by reading the notes and repeating the specific level, as indicated in Figure 10. Small penalties are given to a player by reducing five points in a score per each illegitimate stone collected. The player is warned to stop misbehaving by exposing herself to attackers and increasing exploited vulnerabilities when collecting the illegitimate stone, as indicated in Figure 11. In addition, once the player fails because of collecting more illegitimate stones up to ten, the game terminates and displays a warning message. Then, a player must read the notes embedded to improve her knowledge and then repeat playing the specific level until she succeeds. To make the game interactive, enjoyable, user-oriented, and challenging, the collector must avoid obstacles such as bombs, moving rockets, and brick walls and skip malicious stones. To succeed in a level, a player must reach the required points, not collect more than ten illegitimate Tanzanite stones, and maintain life. The game summarizes a specific phishing concept embedded in that level at the end of each level, as depicted in Figure 6. Furthermore, we placed the questions at the end of each level to assess the understanding of the players and the increase in concentration, as indicated in Figure 12. The players must answer all the questions correctly to be allowed to move to the next level. Failure to answer all questions precisely requires the player to repeat reading the summary and answering the questions before going to the next level.

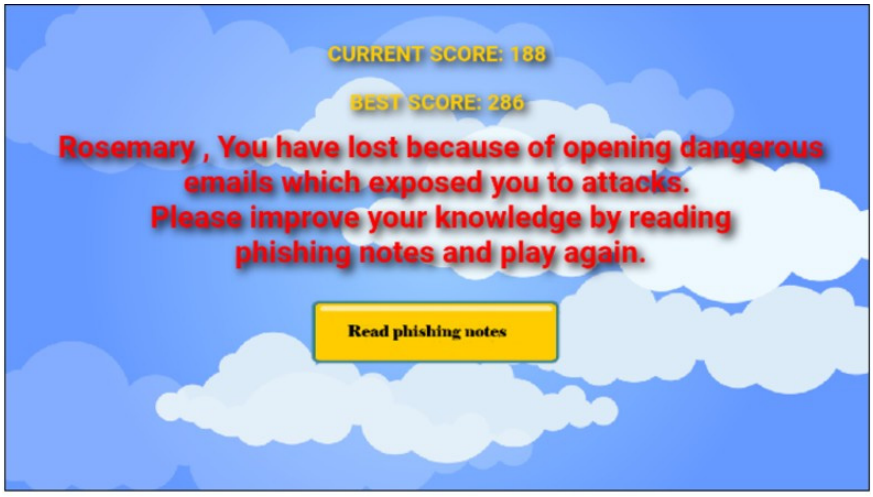


Figure 10. The message displayed after the game terminates when a player collects phishing stones.

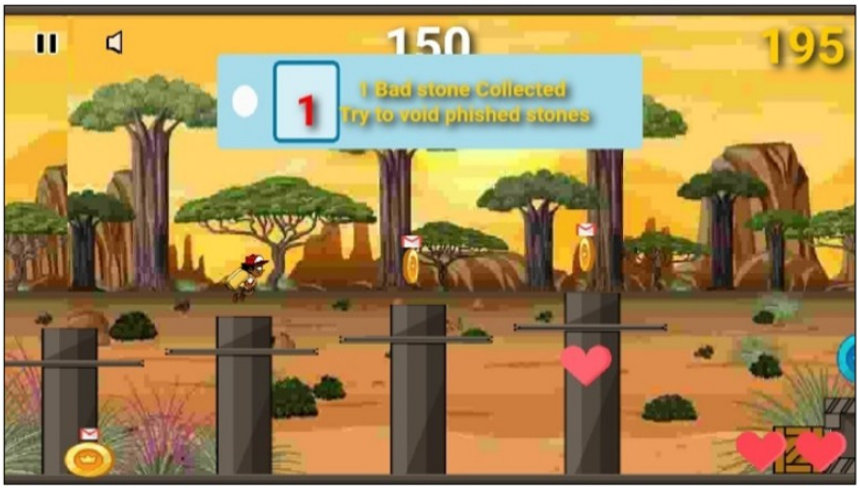


Figure 11. The warning message displayed when a player collects illegitimate stones.

Figure 12. Evaluation questions embedded at the end of the level to assess players' understanding.

4.1.5. How Phishing Concepts Are Incorporated in a Game

The Tanzanite Collector game teaches three parameters mostly used to initiate phishing attacks: emails, messages, and phone calls. One phishing concept is embedded at each level

of the game. Tanzanite stones were used to represent phishing concepts in a game, and the player must collect legitimate stones and skip illegitimate ones. During the collection of Tanzanite stones, players should be careful to make the right decision and accurately identify which stone is legitimate and which is not. If the correct stone is collected, a player is rewarded by increasing her scores by ten. On the other hand, if the player collects the illegitimate stone, she will be penalized by reducing the scores by five. Moreover, a player is warned of her actions once she collects illegitimate stones, as shown in Figure 11. To complete a level, the player must score a maximum of five hundred points at the end of a specific level. The player can learn while playing using a summary given for a particular phishing concept at the end of the corresponding level, as shown in Figure 6.

4.2. Game Testing Methods and Procedures

This part describes the methodology and study procedures we used to test the effectiveness of the designed game and compare it with the traditional teaching method, reading notes in our case.

4.2.1. Participants and Sample Size

Our experiment included 30 participants, with an average age of 17, who were chosen at random from a government school and were among those who took part in the first part of the study. They were those who did poorly in the initial survey, resided in rural areas, attended government schools, and were in poor socioeconomic and cultural environments. We split the participants into two groups: experimental and control. The control group had 14 participants and the experimental group had 16 participants. The characteristics and statistical mean differences for the participants in the control and experimental groups are shown in Table 3.

Table 3. Characteristics of the participants in control and experimental groups.

Coefficients	Control Group	Experimental Group
Gender	Female *n* = 7 (46.7%) Male *n* = 7 (46.7%)	Female *n* = 8 (53.3%) Male *n* = 7 (53.3%)
Socioeconomic and cultural status	Mean = 0.313	Mean = 0.322
Score of phishing	Mean = 0.689	Mean = 0.71
knowledge Place of residence (Rural)	N = 14 (46.7%)	N = 16 (53.3%)
School category (Government)	N = 14 (46.7%)	N = 16 (53.3%)

4.2.2. Study Methodology and Design

The experimental design was used in the second part of this study, where experimental and survey methods were applied. First, we divided the participants into two groups, a control group and an experimental group, where the former would not be exposed to the phishing game and the latter would be exposed to the game. Instead, the control group was given phishing notes to read. Finally, the two groups were evaluated using a paper questionnaire to see if the experimental group could outperform the control group. The questions were obtained online from various sources.

4.2.3. Materials Used

Participants in the experimental group were given Android devices with which to play the game and test its functionality and usability. Using real devices instead of emulators helps to evaluate the compatibility, interaction, and user experience of the game in a real-world setting. The phones had an Android 10 operating system, 2GB of RAM, 8GB of internal memory, and an MHZ processor. In addition to that, we provided the phishing notes using paper-based reading materials given to the control group participants. The content of the phishing notes was obtained from a variety of sources on the web. It detailed how phishers utilize email, text messages, and phone calls to defraud users.

4.3. User Experiment Procedures

We divided the participants into experimental and control groups. This subsection describes the procedures we used to conduct our experiment among the participants in these groups.

4.3.1. Experimental Group

Participants were given a game to play for five days consecutively. The game has three levels, and participants were required to play and learn each parameter of the phishing concept at a specific level to acquire the points needed, succeed at the level, and answer the questions at the end before moving on to the next level of the game. For example, level one teaches how a player can identify phishing emails, level two introduces how short messages are used in phishing, and the last level describes phishing calls. At each level, there are legitimate and illegitimate stones. Therefore, the player must identify and avoid illegitimate stones and collect only legitimate Tanzanite stones. At the same time, she must overcome obstacles such as huddles and rocket bombs, increase lifelines, and earn points. Once the player finishes the level successfully, she receives points and vouchers as an additional motivation award. To ensure that the player has acquired knowledge at a particular level, she must answer the questions at the end of the level before moving to the next higher level. If she answers them correctly, she is allowed to go to the next level. Otherwise, the player must review the summary and correctly answer all the questions to advance to the next step. Each participant has to play and complete all levels at least three times a day for a maximum of one week. Playing the first time allows them to familiarize themselves with the game, and repeating it enables them to understand and acquire the concept and knowledge in the game. Subsequently, they complete a questionnaire to measure their phishing knowledge after playing the game.

4.3.2. Control Group

Participants were given phishing study materials to examine for five consecutive days at their convenience. These materials cover the same phishing concepts and tactics used to manipulate users as those incorporated in a game. However, the participants received no clarification or lecture on phishing. Then, they were assessed using the same questionnaire used to assess their counterpart, the experimental group.

4.4. Procedures for Comparing the Two Training Methods in Knowledge Retention

To assess the effectiveness of the two training tools used, we analyze and compare the levels of performance of the participants in the control group and the experimental group over time. Therefore, each group was tested twice to evaluate their knowledge retention. Two weeks later, the group participants were given the same questionnaire used during the experiment. The period to estimate knowledge retention was adopted from previous research by [12,19].

5. Results for Part 2

The usefulness and usability of the Tanzanite Collector game are discussed in this section. First, we compared the performance of those who played the game with those who read the notes in terms of phishing knowledge. The information retention of the individuals in the two groups was then assessed over time.

5.1. Usability of the Game

The participants in the experimental group evaluated the usability of the game. In the questionnaire, we presented questions such as confidence in playing the game, ease of navigating the game, and whether the game was enjoyable. Likert scale questions ranging from Strongly Agree to Strongly Disagree were included. Most of the participants had positive responses to the interactivity of the game activities, the content of the game, the genres used, and the narration of the story line to teach the concepts of phishing,

as shown in Table 4. The results showed that almost all the participants (100% n = 16) found the game useful, and the game activities and the storyline reflected the teaching of phishing prevention.

Table 4. Evaluation of the Usability of the Game.

Summary of Questions	Participant Evaluation Scores%
Game satisfaction	100%
Confident playing game	94%
Relation of storyline and activities to teach phishing	100%
Easy to navigate and enjoyable	94%
I prefer games in learning	100%
Have a game on their mobile phones	100%

A sufficient number of participants (94%) say that the game is easy, enjoyable, and inspires confidence in its use. However, very few (6%) who reported not being used to playing mobile games completed the three levels, describing the game as difficult. A few teenagers involved in this experiment were unfamiliar with games because we took the slot of participants in the first study who do not have good knowledge of phishing and have less exposure to smartphone devices and the internet. Therefore, this indicates that some users who are not used to playing games may need more time to familiarize themselves with the app, while for this case, we only have a period of one week.

Furthermore, most of the participants (100%, n = 16) suggested that they would rather learn about phishing through mobile games than other training methods such as reading notes and lectures. This is because they find that the learning process through the game is interactive and interesting and engages them directly. Consequently, the feedback from the participants is a shred of evidence that games could be the most useful and preferred tool in teaching phishing concepts. However, it could also be applied to teach other classroom subjects because it transfers knowledge while it offers interaction, fun, and user engagement. Additionally, the design should consider the differences in the ability of participants in social culture and environments to acquire the intended knowledge using things that are familiar in their environment. Therefore, our game used an African themed environment, African people, and objects recognizable to our target participants.

5.2. Teenagers' Phishing Knowledge Performance

We measured the phishing knowledge performance of two groups of teenagers: the experimental and control group. First, we computed the scores for each participant and calculated the average scores of the overall participants for each group. Then, the mean average of the performance for each group was calculated to compare the results of the two groups. Finally, we used a t-test to calculate and compare the average mean of two data sets from the groups. The t-test approach we used is an independent sample t-test, enabling us to see whether there are performance differences among the groups tested and whether the difference is statistically significant or occurred by random chance. The results show that those who played the game performed better (88.2%) than their counterparts who read the notes (43.1%), with mean standard error marks of 2.4 and 4.6, respectively, as indicated in Figure 13. Furthermore, the group that played the game had low mean error marks, indicating greater accuracy in scoring correctly than those who read the notes. Finally, we compared the mean difference in performance of each group in all questions and found that it was statistically significant ($t = 8.7$, $p < 0.0001$). Therefore, the analysis shows that the performance results are statistically significant and not by random chance.

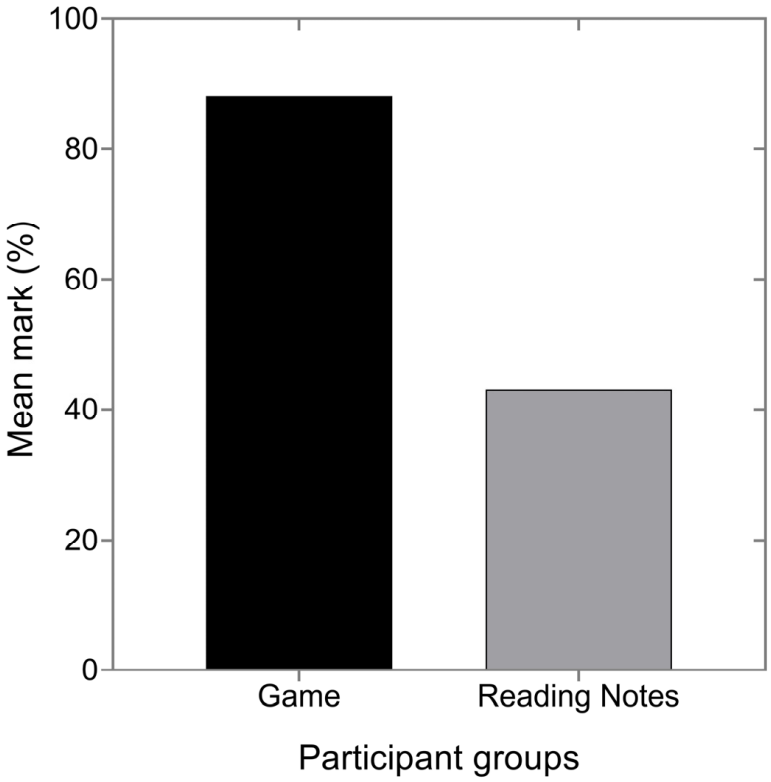


Figure 13. Teenagers' phishing knowledge performance after playing the game and reading notes.

5.3. Knowledge Retention

We measured the retention of knowledge among the two groups; those who played and those who read the notes. We used the t-test used to compare the mean difference of the performance of each group across all questions in the pre-test experiment and two weeks later and found that it has great statistical significance. The mean marks of the game players and notes reader groups are 88.2% and 43.1%, respectively (t = 8.7, p-Value < 0.0001) in the pre-test experiment and 82.1% and 37.99% (t = 6.9, p-Value < 0.0001) two weeks later, as indicated in Figure 14. However, the performance of the participants who played the game did not differ significantly between the pre-test (88.2%) and two weeks later (82.1%) (t = 0.0056, df = 21.228, p-Value = 0.8998). Moreover, reading notes has not improved the knowledge of the participants in the control group; rather they continue to have lower performance in pre-test (43.1%) and two weeks later (37.9%). The statistical results depicted that there were no significant differences in their knowledge through reading notes from the two experiments (t = 0.012, df = 41.89, p-Value = 0.9999). The performance of the two groups has been seen to drop slightly in almost equal dimensions between the first experimental results and two weeks later. Those who played the game dropped from 88.2% to 82.1%, and those who read the notes dropped from 43.1% to 37.9%. Despite the slight decrease in performance of both groups, the group that played the game maintained at least 80% of their knowledge from the previous experiment, which is still reasonable knowledge retention since they only played the game a few times. On the contrary, the group that read the notes exhibited a continuous drop in performance. Therefore, the game enabled the participants to retain their knowledge of how to protect themselves from phishing at a higher rate than notes reading; however, the rate would have been higher if participants had been given more time to play the game.

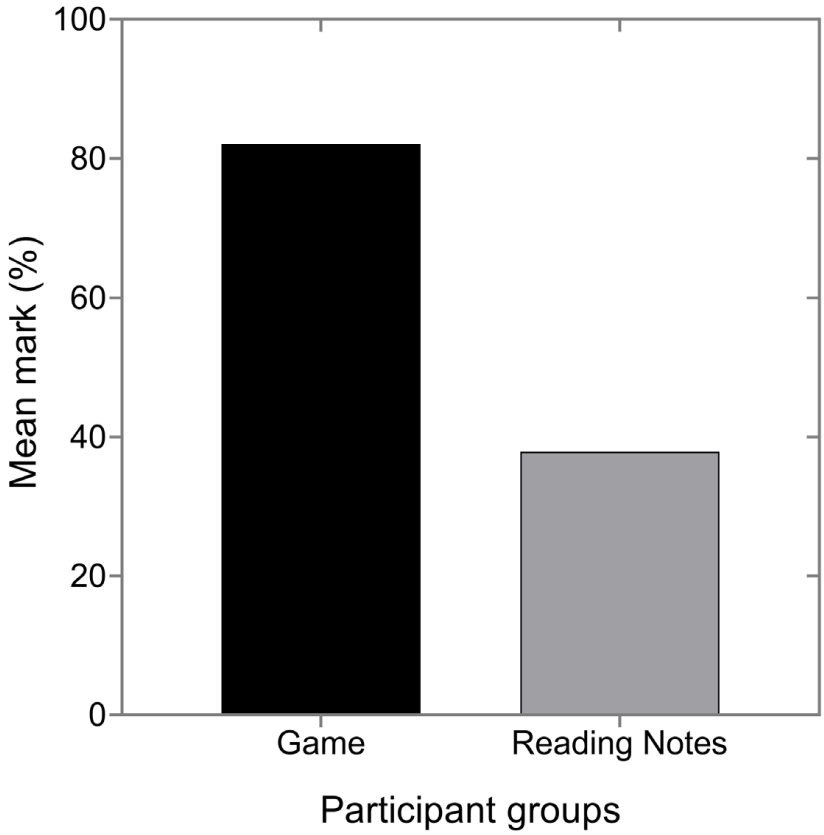


Figure 14. Teenagers' phishing knowledge retention two weeks later after playing the game and reading notes.

6. Discussion

In this section, we discuss the knowledge of phishing and cybersecurity of teenagers based on differences in social-economic and social culture. Furthermore, we give details on how the game we developed improved teenagers' performance over other traditional training tools.

6.1. Teenagers' Phishing Awareness

The phishing knowledge of teenagers varies according to their school category and their place of residence. For example, those studying at international or private schools, and those living in urban areas showed a better understanding of phishing and cybersecurity measured in our pre-test evaluation. The reason could be early exposure to the internet and easy access to mobile devices such as smartphones, making users familiar with various issues in cyberspace. The research by [24] found that users who have exposure and prior phishing knowledge and those who have previously experienced phishing attacks performed better than others.

Furthermore, the difference in the educational posture of teenagers significantly contributes to their knowledge about phishing and cybersecurity. For example, in Tanzania, in international schools, teenagers are allowed to use mobile phones and have internet access even at school, allowing them to easily connect to social networks. In contrast, students studying in private and government schools are not allowed to use mobile phones at school. However, those who study in private schools have access to computer labs in their schools with internet access compared to their counterparts in government schools. On the other hand, only a few government schools have computer labs and no internet infrastructure. Therefore, considering these variations, it is evident that those with a better social-economic and social culture could have better phishing knowledge because they are familiar and have self-experience while connected to the internet and have exposure to mobile devices.

Furthermore, we investigated the existing linear relationship between mobile phone use and knowledge of phishing in teenagers. We found a strong linear relationship between the frequent use of mobile devices and phishing knowledge, as indicated in Figure 15. Therefore, those who frequently use mobile phones seem to have better understanding than others. Additionally, the more people use mobile phones, the better their knowledge of phishing. The correlation coefficient (R = 0.62) and ($p < 0.001$) show a strong relationship between the frequency of mobile phone use and the knowledge of phishing in teenagers, and this relationship is statistically significant.

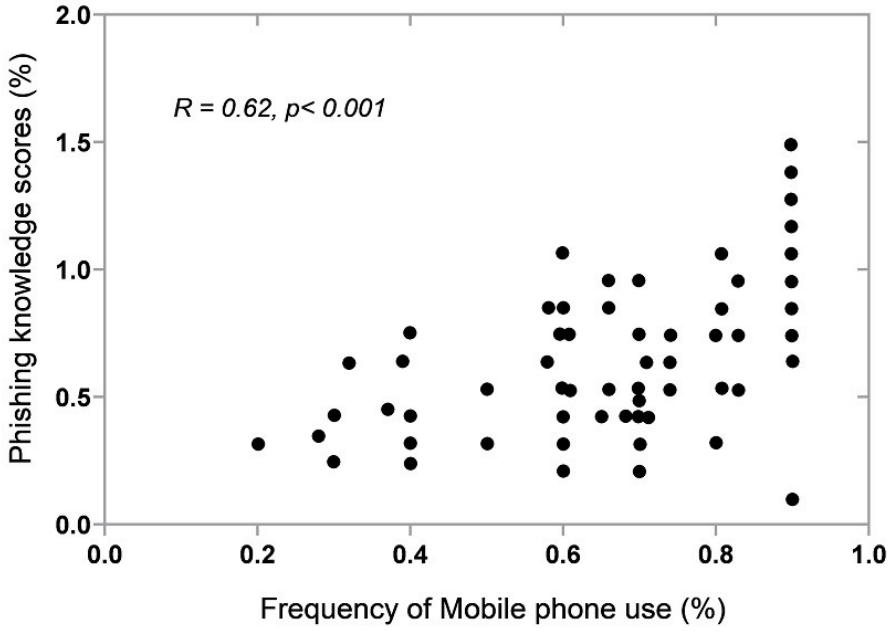


Figure 15. Correlation between the frequency of mobile phone use and phishing knowledge.

The strong relationship could be due to exposure to various advertisements, news, and warnings. In addition, the users may already have experience with several circumstances and tactics used by attackers, such as short messages asking for personal credentials, being asked to send money to unfamiliar contacts, and receiving suspicious calls and emails. These could have caused teenagers to gain experience and additional knowledge, making them different from those who rarely use mobile phones or do not use them.

We further investigated the relationship between teenagers' social-economic and social-cultural differences and phishing knowledge. We found that the better the social-economic and social culture, the higher the phishing knowledge. Therefore, those with a better socioeconomic and social culture have performed well and seem to have a better understanding than others. The correlation of the coefficients tested, as shown in Figure 16, is positive as the value of (R = 0.56) and ($p < 0.001$), which means that the existing relationship is statistically significant. The reasons may be high exposure to technology, including access to mobile phones, television, laptops, tablets, and the internet. Other reasons could also be receiving education from different platforms such as social networks, getting to know how-to from parents and schools that allow the use of these devices, and teaching computer subjects in their curriculum. Therefore, exposure to the internet and access to mobile devices significantly contribute to the knowledge of phishing in teenagers, despite some being unable to own and obtain access to the internet due to poverty and the limited position of their study environment.

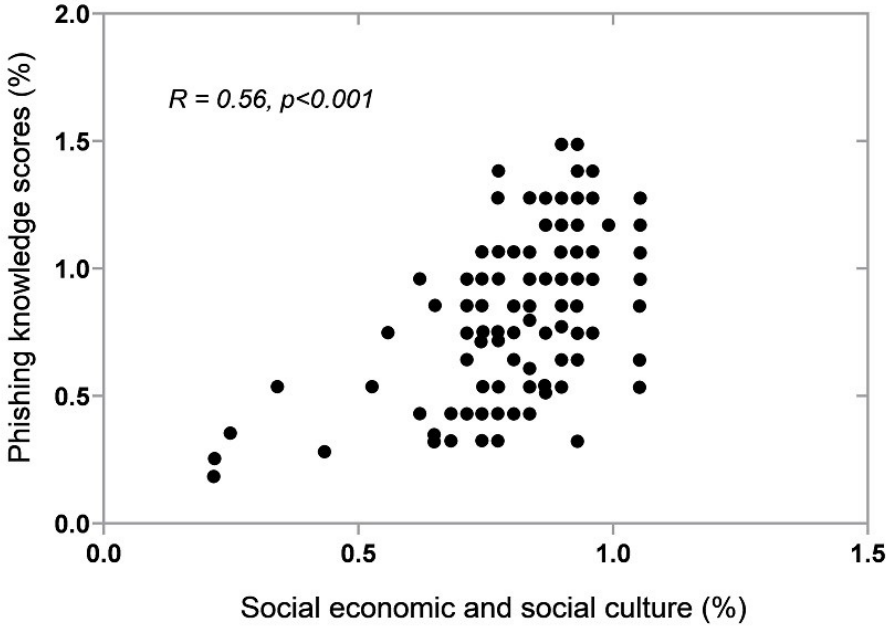


Figure 16. Correlation between teenagers' social-economic, social-cultural, and phishing knowledge.

6.2. Improved Teenagers' Phishing Knowledge Using a Customized Game

The performance of phishing knowledge of teenagers has improved from the pre-test (before being exposed to a game and reading notes), as indicated in the results of the first study for the post-test (after being exposed to a game and reading notes of phishing). In the pre-test, teenagers living in rural areas and government scholars showed poorer phishing understanding than those living in urban areas and international and private scholars, as indicated in Figures 1 and 2. In our experiment using a game and reading notes, we involved those participants from rural and government schools who had shown poor knowledge in the first study to see if the game could improve their performance.

We also compared the two teaching methods, the traditional teaching method (reading notes), and the developed game. We found a significant improvement in the performance of teenagers after the first study assessment and after exposure to a game. Those who played the game scored 88.2%, and those who read the notes scored 43.1%. The improvement in the performance of teenagers' knowledge could be due to consideration of their differences in social-economic and social culture in the design and development of the game. Knowledge gaps between these groups may endure if discrepancies in social-economic status and cultural norms are not eliminated.

Therefore, to eliminate existing differences in knowledge among teenagers with better and poorer social-economic and social cultures, it is important to consider developing applications based on their variations. Therefore, this could help teenagers who had poor knowledge due to poor social-economic and social culture to improve their knowledge as much as those who had better social-economic and cultural status. Moreover, our game has an African context in which we use familiar environments and objects in game design and development to make teenagers acquire knowledge easily. Previous research by [43] has reported that game development and design must adhere to indigenous culture and customs to facilitate community participation, easy game play, and success in delivering knowledge.

We evaluated teenagers' phishing performance using a game and traditional methods of teaching; in this case, we used reading notes. Those who played the game outperformed those who read the notes. The reason could be that the game is engaging and fun and players learn by seeing consequences and results based on their actions. Reading is just a matter of memorizing and imagination, but it could not help to learn practically. We also evaluated the performance of teenagers two weeks later after playing the game and reading

the notes to measure the retention of knowledge between those who played the game and the participants who read the notes. The aim was to determine which learning method between the game and recitation of notes could help teenagers retain their knowledge even for a longer period after being trained. Participants who played the game have been shown to have retained their knowledge more than those who read the notes. The game has been seen as an effective tool to teach since it engages, and motivates, is enjoyable, and requires a player to complete a task while playing, thus it is suitable in delivering knowledge in any lesson. As a result, the player understands the knowledge deployed within [1,44]. On the other hand, traditional teaching methods such as books, notes, and lectures have also been used to teach cybersecurity and phishing concepts. However, its application has shown relatively little impact in allowing users to easily learn and retain their knowledge for a long time [12].

6.3. Teenagers' Knowledge Retention between a Game and Traditional Teaching Methods

We measured the retention of knowledge of the participants using the two methods two weeks after playing the game and reading the notes to evaluate the effectiveness of the two teaching methods in the delivery of knowledge. The participants who played the game and those who read the notes retained their knowledge by 82.1% and 37.9%, respectively. The performance of the two groups has been seen to drop slightly in almost equal dimensions between the first experimental results and two weeks later. Those who played the game have dropped from 88.2% to 82.1%, and those who read the notes have dropped from 43.1% to 37.9%. Despite the slight decrease in performance of both groups, the group that played the game maintained at least 80% of their knowledge from the previous experiment, which is still reasonable knowledge retention since they only played the game a few times. Repeat and multiple training sessions for longer periods would increase participants' performance and ability to retain acquired knowledge for a longer period [26]. Therefore, the results could be improved if the users had played the game several times. On the contrary, the group that read the notes exhibited a continuous drop in performance. The reason could be difficulty memorizing concepts by only reading notes since the method does not support participation of the participants and participation of the actions. Therefore, it takes more effort and time to acquire and maintain memory longer than playing the game.

7. Limitations and Future Work

Only 30 participants were able to participate in the second part of our study, which included a total of 121 participants. In comparison to the large number of Tanzanian teenagers who use the internet and mobile devices, this is a small number. We advocate increasing the sample size in the future to represent the wider population and variability of the participants for more accurate comparisons. We also encourage employing smart gadgets such as JINS MEME eyewear to monitor participants' mental focus, discover characteristics that cause people to miss dangerous content, and improve their efforts in making the right decision. In future research, we recommend that the time spent playing the game be extended to allow participants to become accustomed to it and retain the knowledge they have gained for a longer period. Furthermore, rather than utilizing a survey questionnaire to assess participants' knowledge, we recommend that future research should investigate employing an experimental setup to examine participants' degree of comprehension in a real-world setting. This may have been accomplished, for example, by creating a testing environment in which participants were exposed to phishing scenarios from the real world by receiving a mix of malicious content. As a result, researchers would receive immediate feedback based on their activities, and participants' ability to detect phishing information in real time would be assessed. We also recommend using customized mobile games to teach cybersecurity concepts such as phishing, which is the most common attack nowadays in public places such as schools and workplaces, because mobile phones

and tablets are inexpensive, and teenagers are the most frequent users of the internet and mobile devices.

8. Conclusions

We conducted a survey of 121 teenagers to measure their phishing knowledge in the first part of the study. We noticed that the majority of the teenagers frequently use the internet and social networks, as well as mobile devices like cellphones, laptops, and tablets for communication.

Our findings further suggest that teenagers' awareness of phishing varies depending on their socioeconomic background and social culture. Teenagers who attend international and private schools and live in urban centers, for example, are more informed than those who attend public schools and reside in rural areas. Surprisingly, even those teenagers who were more knowledgeable about phishing demonstrated poor cybersecurity hygiene, such as sharing mobile phones, in the initial assessment of their phishing knowledge. Some respondents said they shared their social media accounts and passwords with their friends, and the majority said they are open and respond to suspicious emails, phone calls, and messages.

Therefore, we created a smartphone game to test teenagers' knowledge and see whether it could help them understand phishing better. Only 30 people took part in the second part of the study, which compared the outcomes of those who used the standard teaching technique to those who engaged in a customized mobile game to measure their phishing knowledge improvement. Performance evaluation indicates that those who played the game did better and retained more knowledge than those who simply read notes.

Author Contributions: Conceptualization, R.C.T.P. and J.D.N.; methodology, R.C.T.P.; software, R.C.T.P.; validation, R.C.T.P., J.D.N. and J.M.; formal analysis, R.C.T.P.; investigation, R.C.T.P. and J.D.N.; resources, R.C.T.P.; data curation, R.C.T.P.; writing—original draft preparation, R.C.T.P.; writing—review and editing, R.C.T.P. and J.D.N.; visualization, R.C.T.P. and J.D.N.; supervision, J.D.N. and J.M.; project administration, J.D.N.; funding acquisition, R.C.T.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Tanzania Ministry of Education, Science and Technology (MOEST) in Collaboration with Center for Development of Advanced Computing (CDAC), India; Fund Number 2001.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board of Kibong'oto Infectious Diseases Hospital–Nelson Mandela African Institution of Science and Technology–Center for Educational Development in Health, Arusha (KIDH-NM-AIST-CEDHA)-KNCHREC (The protocol code KNCHREC00062/12/2021 and approved on 24 January 2022).

Informed Consent Statement: Written informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy concerns and the need to be made anonymous on request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res. (IJISR)* **2016**, *6*, 660–666. [CrossRef]
2. 29 Must-know Cybersecurity Statistics for 2020: Cyber Observer. 2020. Available online: https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer (accessed on 18 June 2020).
3. Agency, C.I. *The World Factbook*; Central Intelligence Agency: Langley, VA, USA, 2018.

4. Authority TCR. Quartely Communications Statistics: Tanzania Communications Regulatory Authority. 2021. Available online: https://www.tcra.go.tz/uploads/text-editor/files/TelCom%20Statistics%20June%202021_1630483653.pdf (accessed on 20 June 2021).
5. Nicholson, J.; Javed, Y.; Dixon, M.; Coventry, L.; Ajayi, O.D.; Anderson, P. Investigating teenagers' ability to detect phishing messages. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 7–11 September 2020; pp. 140–149.
6. Kabali, H.K.; Irigoyen, M.M.; Nunez-Davis, R.; Budacki, J.G.; Mohanty, S.H.; Leister, K.P.; Bonner, R.L. Exposure and use of mobile media devices by young children. *Pediatrics* **2015**, *136*, 1044–1050. [CrossRef] [PubMed]
7. Robb, M. The Data on Children's Media Use 2018. Available online: https://doi.org/10.1177%2F0031721718762418 (accessed on 26 February 2018).
8. Onditi, H.Z. Tanzanian Adolescents in the Digital Age of Cell Phones and the Internet: Access, Use and Risks. Ph.D. Thesis, Dar es Salaam University College of Education (DUCE), University of Dar es Salaam, Dar es Salaam, Tanzania, 2018.
9. Porter, G.; Hampshire, K.; Abane, A.; Munthali, A.; Robson, E.; Mashiri, M.; Tanle, A. Youth, mobility and mobile phones in Africa: Findings from a three-country study. *Inf. Technol. Dev.* **2012**, *18*, 145–162. [CrossRef]
10. Vanderhoven, E.; Schellens, T.; Valcke, M.; Raes, A. How safe do teenagers behave on Facebook? An observational study. *PLoS ONE* **2014**, *9*, e104036. [CrossRef] [PubMed]
11. Cain, A.A.; Edwards, M.E.; Still, J.D. An exploratory study of cyber hygiene behaviors and knowledge. *J. Inf. Secur. Appl.* **2018**, *42*, 36–45. [CrossRef]
12. Lastdrager, E.; Gallardo, I.C.; Hartel, P.; Junger, M. How effective is anti-phishing training for children? In Proceedings of the Thirteenth Symposium on Usable Privacy and Security ([1] 2017), Santa Clara, CA, USA, 12–14 July 2017; pp. 229–239.
13. Orlando, J. Kids Need to Learn about Cybersecurity, but Teachers Only Have So Much Time in the Day: The Conversation. 2019. Available online: https://theconversation.com/kids-need-to-learn-about-cybersecurity-but-teachers-only-have-so-much-time-in-the-day-112136 (accessed on 27 February 2019).
14. APWG. Phishing Activity Trends Report. 2021. Available online: https://apwg.org/trendsreports/ (accessed on 8 June 2021).
15. Ndibwile, J.D.; Luhanga, E.T.; Fall, D.; Miyamoto, D.; Blanc, G.; Kadobayashi, Y. An empirical approach to phishing countermeasures through smart glasses and validation agents. *IEEE Access* **2019**, *7*, 130758–130771. [CrossRef]
16. APWG. Phishing Activity Trends Report. 2020. Available online: https://apwg.org/trendsreports/ (accessed on 24 November 2020).
17. Sampath, D. Not Just Phishing with A 'P' Anymore: Examining the A to Z of Social Engineering Attacks. *Forbes Technol. Council* **2020**. Available online: https://www.forbes.com/sites/forbestechcouncil/2020/08/11/not-just-phishing-with-a-p-anymore-examining-the-a-to-z-of-social-engineering-attacks/?sh=85a98c831687 (accessed on 11 August 2020).
18. Ventures, C. 2019 Official Annual Cybercrime Report. 2019. Available online: https://www.threathunting.se/wp-content/uploads/2020/05/Cybercrime-Ventures-2019-Official-Annual-Cybercrime-Report.pdf (accessed on 19 April 2022).
19. Maqsood, S. Evaluation of a persuasive digital literacy game for children. In Proceedings of the Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018; pp. 1–6.
20. Wen, Z.A.; Lin, Z.; Chen, R.; Andersen, E. What. hack: Engaging anti-phishing training through a role-playing phishing simulation game. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, UK, 4–9 May 2019; pp. 1–12.
21. Dixon, M.; Gamagedara Arachchilage, N.A.; Nicholson, J. Engaging users with educational games: The case of phishing. In Proceedings of the Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow Scotland, UK, 4–9 May 2019; pp. 1–6.
22. Weanquoi, P.; Johnson, J.; Zhang, J. Using a game to improve phishing awareness. *J. Cybersecur. Educ. Res. Pract.* **2018**, *2018*, 2.
23. Baslyman, M.; Chiasson, S. "Smells phishy?": An educational game about online phishing scams. In Proceedings of the 2016 APWG Symposium on Electronic Crime Research (eCrime), Toronto, ON, Canada, 1–3 June 2016; pp. 1–11.
24. Gavett, B.E.; Zhao, R.; John, S.E.; Bussell, C.A.; Roberts, J.R.; Yue, C. Phishing suspi- ciousness in older and younger adults: The role of executive functioning. *PLoS ONE* **2017**, *12*, e0171620. [CrossRef] [PubMed]
25. Katsantonis, M.N.; Fouliras, P.; Mavridis, I. Conceptualization of game based approaches for learning and training on cyber security. In Proceedings of the 21st Pan-Hellenic Conference on Informatics, Larissa, Greece, 28–30 September 2017; pp. 1–2.
26. Kumaraguru, P.; Cranshaw, J.; Acquisti, A.; Cranor, L.; Hong, J.; Blair, M.A.; Pham, T. School of phish: A real-world evaluation of anti-phishing training. In Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, CA, USA, 15–17 July 2009; pp. 1–12.
27. Olano, M.; Sherman, A.; Oliva, L.; Cox, R.; Firestone, D.; Kubik, O.; Patil, M.; Seymour, J.; Sohn, I.; Thomas, D. SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education. In Proceedings of the 2014 {USENIX} Summit on Gaming, Games, and Gamifcation in Security Education (3GSE 14), San Diego, CA, USA, 1 May 2014.
28. Sa˘lceanu, C. The Influence of Computer Games on Children's Development. Exploratory Study on the Attitudes of Parents. *Procedia-Soc. Behav. Sci.* **2014**, *149*, 837–841. [CrossRef]
29. Bailey, K.; West, R.; Anderson, C.A. A negative association between video game experience and proactive cognitive control. *Psychophysiology* **2010**, *47*, 34–42. [CrossRef] [PubMed]

30. Unchit, P.; Das, S.; Kim, A.; Camp, L.J. Quantifying susceptibility to spear phishing in a high school environment using signal detection theory. In *International Symposium on Human Aspects of Information Security and Assurance*; Springer: Cham, Switzerland, 2020; pp. 109–120.
31. Gehl, R.W.; Lawson, S.T. *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulativ e Communication*; MIT Press: Cambridge, MA, USA, 2022.
32. Burita, L.; Klaban, I.; Racil, T. Education and Training Against Threat of Phishing Emails. In Proceedings of the International Conference on Cyber Warfare and Security, Albany, NY, USA, 17–18 March 2022; Volume 17, pp. 7–18.
33. Kaspersky. Internet Safety for Kids: How to Protect Your Child from the Top 7 Dangers They Face Online 2019. Available online: https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online (accessed on 23 March 2020).
34. Department of Homeland Security. National Cybersecurity Awareness Campaign Kids Presentation. 2018. Available online: https://www.cisa.gov/sites/default/files/publications/Kids%20Cybersecurity%20Presentation.pdf (accessed on 18 June 2018).
35. Christofides, E.; Muise, A.; Desmarais, S. Risky disclosures on Facebook: The effect of having a bad experience on online behavior. *J. Adolesc. Res.* **2012**, *27*, 714–731. [CrossRef]
36. Kumaraguru, P.; Rhee, Y.; Acquisti, A.; Cranor, L.F.; Hong, J.; Nunge, E. Protecting people from phishing: The design and evaluation of an embedded training email system. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 28 April–3 May 2007; pp. 905–914.
37. Harrison, B.; Svetieva, E.; Vishwanath, A. Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Inf. Rev.* **2016**. Available online: https://www.semanticscholar.org/paper/Individual-processing-of-phishing-emails%3A-How-and-Harrison-Svetieva/0dbaf27103f808d8d0b3b7e9658c499fe127f206 (accessed on 19 April 2022). [CrossRef]
38. Hendrix, M.; Al-Sherbaz, A.; Victoria, B. Game based cyber security training: Are serious games suitable for cyber security training? *Int. J. Serious Games* **2016**, *3*. Available online: https://journal.seriousgamessociety.org/index.php/IJSG/article/view/107 (accessed on 1 January 2016). [CrossRef]
39. Arachchilage, N.A.G.; Hameed, M.A. Integrating self-efficacy into a gamified approach to thwart phishing attacks. *arXiv* **2017**, arXiv:1706.07748.
40. Tucker-Drob, E.M.; Briley, D.A. Socioeconomic status modifies interest-knowledge associ- ations among adolescents. *Personal. Individ. Differ.* **2012**, *53*, 9–15. [CrossRef] [PubMed]
41. King, H.M. A Popular Blue Gem That Is Only Produced Commercially in One Small Area of Tanzania. Available online: https://geology.com/ (accessed on 23 March 2022).
42. Sheng, S.; Magnien, B.; Kumaraguru, P.; Acquisti, A.; Cranor, L.F.; Hong, J.; Nunge, E. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 18–20 July 2007; pp. 88–99.
43. Minoi, J.L.; Mohamad, F.; Arnab, S.; Phoa, J.; Morini, L.; Beaufoy, J.; Lim, T.; Clarke, S. A Participatory Co-Creation Model to Drive Community Engagement in Rural Indigenous Schools: A Case Study in Sarawak. *Electron. J. e-Learn.* **2019**, *17*, 173–183. [CrossRef]
44. Jansen, J.; van Schaik, P. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *Int. J. Hum. Comput. Stud.* **2019**, *123*, 40–55. [CrossRef]