Scientific Research Publishing

Journal of Information Security, 2021, 12, 233-249
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Relevance of Cybersecurity Education at Pedagogy Levels in Schools

Eric Amankwa

Grand Canyon University, Arizona, Phoenix, USA
Email: amankwaeric@yahoo.com, EAmankwa@my.gcu.edu

How to cite this paper: Amankwa, E. (2021) Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, **12**, 233-249.
https://doi.org/10.4236/jis.2021.124013

Received: August 1, 2021
Accepted: September 6, 2021
Published: September 9, 2021

Abstract

Today, the internet extensively impacts people's lives through improved communications, interactions, and the exchange of information. Despite all these positive effects, it also causes in significant negative issues. Over the recent years, cases of online fraud, cyber-bullying, racial abuse, gambling, and pornography have increased due to the lack of self-control and overall awareness among internet users. Therefore, there is a need to create awareness and training on cybersecurity in schools to protect students from cyber-bullying, online fraud, and being targets of prejudice. Research reveals that the level of self-control and awareness among internet users is still moderate and low. To ensure cybersecurity awareness and knowledge among internet users, young people need to get educated on how to operate safely in cyberspace. This education will guarantee that they understand how to protect themselves from cybercrimes. To this extent, this research paper will explore the essence of cybersecurity education in schools and provide strategies that educators can utilize to promote cybersecurity education across learning institutions. This paper will thus conclude how cybersecurity training can be implemented in a learning institution.

Keywords

Cybersafety, Cybersecurity, Cyber Awareness, Cyber Education

1. Introduction

Many people today use the internet as a platform to provoke discussions, to expand their popularity, or to express their feelings. They also engage in citizen journalism where they gain satisfaction from being the first to share a given issue through increased attention from other users. Through various social media platforms such as Facebook, Instagram, Twitter, and YouTube, internet users

can post their videos, photos, and even comments regarding a given issue. In this way, people often keep in touch through the internet by posting their activities, interactions, and other aspects of their daily lives [1]. However, sometimes a problem arises when these internet users are quick to share information without concern for their safety, or the validity of the content [2].

In this era of rapid advancement in multimedia and technology, the internet is easily accessible to all people, adults or children. Therefore, knowledge and education on cybersecurity should be availed at a young age to cultivate a culture of cyber-safety awareness on a global scale. Educators should focus on the benefits of internet excessive use in addition to its adverse effects which include personal information exposure and addiction to gambling, gaming, and pornography [3]. These adverse effects have negatively influenced young people's mental health and behaviors particularly with regards to their social interactions in the real world [3].

Cybercrime against adolescents and children is a growing concern among parents and the society at large mostly because parents are unaware of the threats that cyberattacks pose to their children within their households. Typically, children avoid inform their parents of their internet activities, an aspect that makes it more difficult to detect the harm presented by cyberattacks. Research also reveals that cyberbullying has grown in popularity due to increasing internet use by young people and more so, school children suffer the most as they are easy targets to bullying [4]. More importantly, using the internet among children has exposed them to prejudiced targeting, intimidation, harassment, and sexual exploitation [4].

Research conducted by the New York Police revealed that almost 80% of sexual abuse cases in the nation had been linked to virtual friendships. The study also asserted that the victims of these attacks are primarily teenagers, therefore revealing the need to teach young people on the importance of cybersecurity knowledge early enough [5]. The internet also provides anonymity, an aspect that makes it harder to identify and arrest sexual predators who target underage youth. Grooming adolescents and children to become sexual abuse victims has worsened due to this anonymity, and the predators' methods consistently evolve to avoid detection by authorities [6].

Today, children have become skilled and efficient in using their smartphones, and this becomes a problem for parents wishing to protect their kids from cyberattacks or to even monitor their online activities. With positive intentions, parents provide children with unlimited access to internet gadgets as a measure towards monitoring their safety or ensuring their accessibility. However, with this freedom and unrestricted access, children's vulnerability to cyber threats has tremendously increased especially by exposing them to cybercrime [7].

As such, when children enjoy the various benefits of the internet, they must understand the associated threats through cybersecurity education in academic institutions. Cybersecurity knowledge will help to protect them from the potential risks associated with internet use, and to understand cyber ethics. In this re-

gard, educators should be responsible for disseminating cybersecurity threats to promote accountable internet use; this will help reduce the prevalence of cyber-attacks [8]. Children's use of various social media platforms has rapidly evolved due to considerable market, technological and societal innovation. A study on children's internet usage revealed that they spend most of their internet time watching mini-movies, cartoons, animations, and songs [9]. Younger children prefer cartoons and animations while older ones watch more mature content on various platforms including blogs, games, music videos, entertaining short videos, internet personalities and engaging in social media [9].

Therefore, with this background information, schools should play a crucial role in teaching digital literacy to protect children from potential cyber threats. They can also guide parents on managing and monitoring their internet usage at home to restrict easy access to mature content. More importantly, parents can be advised on how to regulate the amount of time their children spend online using simple strategies and activities such as engaging them in house chores or spending quality time with them. It is important to control a child's online activities since research shows that children who spend too much time online playing video games, and watching movies are likely to develop antisocial or aggressive behaviors [9] [10].

The primary objective of cybersecurity knowledge in schools is to educate young internet users on the potential risks of using various social media platforms. The different internet communication platforms such as chat, social media, email, instant messaging, and online gaming can expose users to cyberattacks such as insults and prejudicial attacks from other internet users [11]. These attacks are particularly problematic for people with low self-esteem who are at a higher risk of being affected by hateful comments, and this might lead to depression [12].

Objectives

Several previous studies have been conducted regarding the implication of cybersecurity knowledge in schools to shed light on the essence of this education in learning institutions. However, very few articles focus on the necessary measures to be implemented by schools in cultivating cybersecurity awareness. Therefore, the main objective of this research is to discuss the relevance of cybersecurity education in schools. It will give insight into the risks associated with excessive usage, the types of risks, and the key aspects that educators ought to highlight in providing quality education. Factors that hinder cybersecurity education will be discussed along with the significance of cybersecurity knowledge that teachers can utilize in schools in the context of the American education system.

2. Cybersecurity

Today, the emergence and advancement in technology allow people to enjoy dual realms, that is, the virtual world and the real world. For instance, people

have been known to create fake Instagram and Facebook posts that show lavish lifestyles while living in poverty. With applications and search engines such as YouTube, Yahoo, and Google, vital information is now readily available and accessible by all people with electronic gadgets such as computers and phones whereby users can manipulate the message to achieve their set goal or to entice their victims [13].

To add on, the physical market is slowly being replaced by the virtual marketplace through e-commerce, which proves to be a more efficient and cost-effective approach to conducting business. Depending on the website's policy, a buyer identifies the item he intends to buy, after which he pays before or after delivery. However, online business has dramatically contributed to online frauds and cybercrimes. For instance, a buyer can purchase an item that does not exist but is displayed in an online market and as such, the buyer often gets scammed off their money [4]. In other instances, the buyer might end up providing vital personal information that could be exploited for phishing or identity theft from uncredible websites.

The growing use of the internet also contributes to adverse effects including the development of addictions (gambling, gaming, and pornography) and cyberbullying. Such issues should be contained at an early stage to ensure they have limited implications on internet users. The best way to manage these internet threats is through incorporating cybersecurity education in learning institutions, where students learn early enough how to identify potential scams or threats and the ethics of interacting with others online. To this extent, cybersecurity knowledge is vital among internet users as it covers ways of reacting to cyber threats to ensure they have limited implications on people's lives [6].

Research also shows that cybercrimes can occur at any time, regardless of organizations, places, and individuals. Therefore, this calls for the implementation of cybersecurity knowledge across all levels of learning institutions [8]. *Cybersecurity* is the state of protection from unauthorized electronic data use and criminals' access [8]. It covers the measures taken in ensuring safety from cybercrimes. Incorporating this knowledge in schools will cultivate a culture that embraces ethical internet use from an early age, ultimately mitigating the negative effects that cyber-criminals have on younger populations particularly with regards to bullying [10].

The explosion and advancements of Information Communication Technology (ICT) lead to in drastic changes in daily lives. Communication is far more efficient regardless of geographical boundaries, and information is readily available to all. More importantly, the advancement in technology has helped develop a society that embraces innovation and inventions. Through the exchange of ideas, internet users can easily develop solutions to crucial problems and ultimately contribute to the establishment of a more positive community in the long term. However, criminals can exploit these advancements to devise new ways of executing cybercrimes while ensuring their anonymity and intrackability by authorities [13].

The World Wide Web has enabled organizations and individuals to easily display and share vital information across distances. However, sometimes this information can be utilized for damaging purposes, which negatively impacts people's lives. For instance, criminals develop ransomware and use it to target large corporations by threatening to expose vital data and information unless they receive some form of payment. In this case, the failure to pay the ransom may result in releasing critical information that may damage an individual or organization [1]. Therefore, cybersecurity knowledge can help curb this problem by securing data and information free from criminals.

Another important aspect to note is that mature content such as pornography easily accessible to children through the internet. While these websites are required to issue a warning indicating adult content, such warnings do very little to deter or blocking children from accessing their content. Viewing such content at an early age gives children a negative image of sex and could be detrimental to children's mental health. The increased access to pornography can also contribute to the prevalence of antisocial and violent behaviors with particular regard to sexual violence. Also, research conducted on New York schools revealed that unhealthy channels on the internet are to blame for the prevalence of teenage drop-outs in schools today [3].

Cybersecurity can also be described as the process, state, or activity in which communication systems and information are protected from modification, unauthorized access, or exploitation. Therefore, cybersecurity knowledge can help prevent people from cyber threats such as ransomware [14]. Children are often exposed to numerous threats such as adult content that they may encounter in games and videos; this content may negatively affect their mental health. To this extent, parents can also benefit from cybersecurity knowledge by ensuring that they help protect their children from harmful online content [9]. Parents can do this by installing parental controls in televisions and phones to restrict children from harmful content and also engaging their children in active conversations on their online activities and the associated risks.

On a more positive note, children can use the internet to access numerous books and journals vital for their education and ultimately expand their knowledge and expertise. For instance, YouTube is full of tutorial videos that can help people tackle common problems in their everyday life. More importantly, people need skills and knowledge in English to play games to understand the games' procedures and settings [2]. Therefore, playing games often encourage the advancement and development of speaking, writing, and reading in English. However, such games often encourage laziness among kids as they spend long hours trying to complete the various levels. Too much concentration on these gadgets and gameplay has proven detrimental to children as they may develop aggressive or antisocial behaviors in their adulthood [5]. More importantly, such games may affect their education as they often spend more time playing video games instead of reviewing their course contents and lessons [5].

Principles of Cybersecurity

Typically, cybersecurity principles guide how people and institutions can protect themselves from cyber threats that may be detrimental to their stored data and information. In this manner, the cybersecurity principles help protect vital data and information, and they are grouped into four main categories; protect, govern, respond and detect [4].

The governing principles are often involved in managing and identifying various security risks, which helps detect cyber threats. Additionally, the protection principles are designed to implement multiple security controls to help prevent and reduce vulnerability to cyber threats [10]. There are also response principles that are designed to recover from and respond to various cybercrime incidents. Therefore, this principle helps prevent a similar occurrence in the future. Finally, the detect tenets ensure cybersecurity incidents are detected, solved, and understood to avoid negative implications [8].

More importantly, these principles follow their separate guidelines (labelled G1 to G5) to ensure the security of given cyberspace is maintained. For instance, the G1 often involves a Chief Security Officer who provides oversight and leadership in cybersecurity programs. In this manner, they overlook various procedures to avoid any mistakes. The G2 is also critical as it helps identify faults in multiple systems, data, and applications. In this way, they are often documented to allow for future reference. The G3 is also vital as it helps in the integrity, availability, and confidentiality of applications, data, and various systems. Additionally, the G4 is also vital as it manages the cybersecurity processes embedded in different frameworks [14]. The G5 code is also critical as it helps document, manage, and identifies the applications and systems authorized for use [3].

The protect principles also have various categories. The first is the P1, a system designed to help deploy, maintain, and design applications according to confidentiality, value, availability, and integrity. The P2, on the other hand, is designed to support and deliver trusted suppliers to online users; this allows institutions to benefit from their innocence. Additionally, there is the P3 that is a system configured to help propagate and reduce the vulnerability of systems to cyberattacks. The P4 is also vital in ensuring that applications and systems are kept accountable, auditable, and secure. Lastly, the P5 is critical in ensuring that the various security vulnerabilities are identified and curbed [9].

The detect cybersecurity principles have proven essential in promoting cybersecurity among various institutions. For instance, it has the D1 code to help detect abnormal activities and security events in multiple systems and applications. More importantly, the D1 is significant in promptly correlating, analyzing, and collecting data on abnormal activity. The response principles are also vital in promoting cybersecurity as they have the R1 that identifies and reports cybersecurity events externally and internally to relevant bodies [1]. The R2 is also critical as it helps eradicate, contain, and recover from cyber-attacks promptly. Therefore, these systems can help institutions protect their data from cyber

threats. More importantly, they are often able to help institutions recovery from cyberattacks. Finally, the R3 usually ensures business continuity and creates development plans that help entities recover from cyber-attacks [8].

Educational institutions can take advantage of the various maturity modeling plans to help in ensuring that cybersecurity is upheld. The five maturity levels include; incomplete, initial, managing, developing, and optimizing. Initial means that the cybersecurity principles are utilized but poorly. The incomplete means that the codes are not implemented or partially implemented. The developing model means that the principles are well implemented. On the other hand, the managing principle means that the regulations were established as standard business policy and practice. Finally, the optimizing model implies a deliberate focus on continual improvement and optimization [2]. Therefore, cybersecurity is often ensured when these principles are upheld.

3. Need for Cybersecurity Knowledge

Research conducted by the Multimedia and Cyber Crime Investigation Division revealed that cyber-love scams concern the United States [11]. In such cases, scammers often find their victims over the internet and spend quality time ensuring trust is established before seeking financial help or personal information that could compromise the victims' security. These cases have been on the rise recently, as some most youths find it to be a lucrative way to earn money faster [11]. The number of cybercrimes in the United States has tremendously increased, with 814 cases reported in 2012 and 1095 cases reported the following year, and a relative increase in 2020 primarily due to the COVID-19 pandemic [15]. These cases have been rampant and have contributed to the loss of money from victims. More importantly, the downloading and uploading of international films and local music without the owner's consent increased. In such cases, fake internet profiles have made it impossible to make arrests and curb this problem. Although the US has various measures to curb internet fraud, the vice is still prevalent today targeting older and younger victims [7].

Furthermore, the fraudulent purchase of illegal goods over the internet is prevalent in the US, with the nation recording billions in losses involving housing, tourism, and the automobile sector [12]. Therefore, this calls for the incorporation of cybersecurity education in schools to prevent cybercrime among young people; this will also transpose into adulthood. A culture of cybersecurity knowledge will be cultivated among people. More importantly, cybersecurity knowledge and education are also crucial in preventing addiction to pornography and computer games available on the internet. This addiction often results in the development of antisocial behaviors [12].

As teenagers spend most of their time socializing and playing computer games, they often develop addiction towards the virtual world, and in most cases, they may lose touch with the real world. Addiction to computer games can be inevitable with time, and children's precious time may be consumed with their

gadgets. In this way, such kids could struggle with their education and interactions with friends. Therefore, the internet is responsible for having adverse effects on young people [1]. This can be prevented by implementing cybersecurity knowledge in schools.

More importantly, the excessive use of the internet is associated with an imbalance in sleeping patterns; children often spend their nighttime browsing the internet and playing video games. Typically, the imbalance in sleeping patterns is associated with health problems that may affect a child's life. Therefore, cyber threats come in various ways that affect people in numerous ways. For instance, excessive internet use has been linked to depression and trauma as some people hope to live the life they see on the internet. In such cases, internet users often post their luxurious lives that may be stressful to those struggling with life. However, research has revealed that some people post fake lives, causing unnecessary psychological damage to their colleagues [9].

Additionally, cybersecurity knowledge is vital among young internet users as some may not be aware that they are victims of cyberattacks. Also, some internet users have reported not being conscious as they attack other internet users. For instance, cyberbullying may be conducted by children wishing to have fun and tease their friends. In this regard, they may be unaware of the extent of damage caused to their friends [7]. Therefore, cybersecurity education will educate young internet users on various forms of cyberbullying; more importantly, it will help them prevent such attacks. For instance, research has revealed that internet users who turn off comments and notifications from their posts are likely to avoid cyberbullying [8].

3.1. Attacks and Vulnerabilities

A *cyber vulnerability* is a weakness in the implementation, design, internal control, and operation of various computer systems. Most of these vulnerabilities are documented and inputted by the Common Vulnerabilities and Exposures (CVE) database. Usually, vulnerabilities can be hunted, exploited, researched, and reverse-engineered using customized scripts or automated tools [5]. Therefore, to ensure the security of computer systems, it is vital first to comprehend the attacks that can be perpetrated towards a computer. Understanding these threats is crucial in developing measures to combat them and ensure safe use of the internet. The examples include:

3.1.1. Backdoor

The backdoor is an algorithm or cryptosystem that offers a secret method in bypassing authentications. Typically, these cyber threats provide a solution to passing security controls, often detrimental to internet users. Additionally, this cyber threat exists because of poor configuration and original design that may lead to such a cyber threat. Also, the danger can be employed by an authorized person in allowing legitimate access. However, cyber attackers may also take advantage of backdoors and use them for malicious purposes. In either way, re-

gardless of their use, they still pose vulnerabilities among internet users [1]. Usually, backdoors are hard to detect, and they often require IT experts to conduct a sweep on a given computer system.

3.1.2. A Denial-of-Service Attack (DoS)

A denial-of-service attack is often designed to disrupt a network or machine resource. In such cases, they often make these resources unavailable, which may be challenging to internet users. For instance, attackers, in this case, can deny internet users access to vital websites by simply inputting wrong passwords. In this way, the incorrect password is inserted severally until the account is blocked. Typically, these attacks are rampant where an attacker comes from a significant point, and it, therefore, becomes impossible to pinpoint their location. Also, these attacks are ordinarily common among zombie computers with a range of possible techniques that include; amplification and reflection attacks [3].

3.1.3. Direct-Access Attacks

Direct access attacks often involve cyber attackers gaining physical possession and access to a computer. Usually, these computers are often considered vital to a given entity and organization due to the information stored. Therefore, physical access to these computers could be detrimental to the victims [3]. Attackers, in this case, may make operating system changes and modifications that affect the data inside the computer. Additionally, attackers may install critical loggers and software worms that may ruin the data and information inside the computer. In such cases, even when security systems protect computers, attackers may find ways of bypassing them [13].

3.1.4. Eavesdropping

Eavesdropping has also been on the rise recently, with attackers aiming to listen to private conversations. Typically, these intimate conversations are often conducted over the internet, and attackers may access such discussions. For instance, in the US, NSA and FBI utilize software such as NarusInSight and Carnivore to monitor conversations across networks. Although there are various criticisms regarding the act, with researchers claiming it is a breach of confidentiality, the authorities have asserted that eavesdropping is vital for national security [2]. In this way, many criminals have been caught while making plans to perpetrate attacks.

3.1.5. Phishing

Phishing has been rampant today, and they are employed in acquiring sensitive data and information such as passwords, credit cards, and usernames that can be used in perpetrating attacks against internet users. This is typically done by deceiving internet users, often leaking their usernames and passwords. Typically, phishing is conducted through instant messaging and email spoofing to ensure that internet users trust the cyber attackers completely. Relatively, such attackers may create fake websites that ask for passwords and usernames [7].

3.1.6. Social Engineering

Social engineering is a cyberattack that aims to convince internet users to disclose personal information and secrets such as card numbers and passwords. Generally, social engineering involves gaining internet users' trust by posing as trustworthy institutions after which personal information is retrieved. Usually, attackers often impersonate banks, senior executives, customers, and contractors, which helps them gain access to personal information [1]. Emails are often sent to finance and accounting department personnel requesting illegal action [1].

Cybersecurity education in schools has also proven critical in ensuring young internet users understand the various cyber threats they are exposed to. For instance, internet users who use computers are often at risk of suffering a malware attack. *Malware* is a virus created and utilized for malicious intent. Typically, malware includes numerous software that is not limited to trojan horses, viruses, rootkits, crypto-jacking, worms, and spyware. Likewise, internet users can also suffer from ransomware attacks. Cyber-attacks are conducted on a computer system where the software encrypts crucial data and information in exchange for a ransom; this malware could paralyze a given organization [14]. To this extent, cybersecurity education could be essential for the future generation as it will lead to a society that acknowledges cybersecurity awareness. More importantly, children in schools could be empowered on the responsible and safe use of online platforms and resources to help establish a cyber safety culture [8].

4. Limitations of Cybersecurity Education

The most popular social media applications used in the US include Instagram, Facebook, YouTube, Twitter, and Linked. These applications have been responsible for ensuring friends keep in touch even when they are in different states. In this regard, these platforms have held communication going across the nation. More importantly, the media have profiles that provide news and meaningful information to people across the US. Thus, people can learn from the vast array of images, audio, and videos available in these social media applications. However, the problem arises where the explosion of this information results in various security and privacy risks [10].

The accuracy and authenticity of information on the internet have often been a subject of question. Researchers believe that it is impossible to verify this information since they are posted by people a million miles from us [5]. Therefore, people have to be extra careful, especially when sharing these videos and images. More importantly, children have to be protected from fake information as it may misguide their life. In this case, cybersecurity education would be vital in ensuring young internet users are equipped with the necessary knowledge to defend themselves against fake information. Also, they can learn to take responsibility for their actions over the internet [9].

Cybersecurity education, however, faces various challenges that often hinder its implementation in learning institutions. For instance, the main challenge is

ensuring that tutors are well trained with up-to-date information to promote their ability to understand various cyber threats today critically. More cyber threats frequently emerge today, posing a challenge to tutors as they have to learn how to combat such threats. Additionally, the other challenge is that it may be impossible for teachers to track the use of phones and computers by learners while at home [10]. Therefore, although cybersecurity education may be implemented in schools, learners are still exposed to cyber threats at home.

Parental control has also proven challenging, especially to those guardians that are always busy with work. Children often left at home are likely to misuse the internet through gadgets such as phones and computers. In such cases, parents may lose track of how their children use the internet, exposing them to various cyber threats. For instance, children left unattended may get addicted to pornography or video games that may have tremendous implications on their mental health. In such cases, these kids are at a greater risk of developing antisocial behaviors such as rape and molestation [4].

Additionally, the lack of expertise has proven challenging to the implementation of cybersecurity education in learning institutions. With the limited number of cybersecurity professionals, it becomes challenging to incorporate cybersecurity education in schools. More importantly, the implementation of the instruction requires money and resources that may be challenging to schools that are struggling with their finances [14]. In such cases, failure to secure funds and grants from the government could lead to the program's loss [1].

To add on, most teachers in schools lack the expertise and knowledge regarding cyberspace. Therefore, schools may be forced to hire IT professionals to help with cybersecurity awareness among children. In such cases, schools with limited resources may fail to hire IT professionals leading to the failure of such programs [12]. Government ministries should come in to assist schools in incorporating cybersecurity knowledge in learning institutions [6].

Today's speed of technological advancement poses risks and new challenges to schools wishing to implement cybersecurity education in their curriculum. Therefore, IT professionals may find it challenging to develop their skills and knowledge to the latest technology [9]. In such cases, ensuring the safety of children against cyber threats may be challenging. Therefore, implementing this program in schools calls for teachers to increase their sensitivity to technological advancement and change. Additionally, some teachers may lack access to specialized learning materials that may be challenging, significantly when expanding their technical know-how [13].

To mitigate these limitations, early training and exposure to cybersecurity should be conducted through cybersecurity seminars and symposiums [5]. More importantly, the implementation of this program requires the collaboration of both students, teachers, and parents in ensuring cybersecurity awareness is promoted among students. Parents should ensure they perform their role at home by providing parental control as their kids use the internet on phones and

computers [14]. People exposed to cybersecurity training are often expected to train others as they are the nation's future in cyber defense.

5. Methodology

This research paper is vital in highlighting the numerous studies conducted on cybersecurity awareness in schools. Therefore, the report utilizes various databases such as Google Scholar, Emerald, EBSCOhost, Sci, and Scopus in getting information regarding the importance of implementing cybersecurity education in learning institutions across the US. While exploring these databases, the keywords used included cyber awareness, cybersecurity, and cyber education. More importantly, the literature chosen was in English, widely used by most people in the US. Additionally, the research utilized research published between 2014 and 2021; out of the 100 studies discovered, only 14 were employed in this research paper. Finally, these studies were chosen based on their scope, context, and respondents.

Table 1 below summarizes the studies selected in terms of location, research focus, methodology, application, and research areas. Table 2 below outlines the process employed in choosing the studies.

Research Questions

1) What is the significance of cybersecurity education in learning institutions?

2) What are the challenges faced in the implementation of cybersecurity awareness in schools?

Table 1. Studies reviewed.

Methodology	Area	Research Focus	Location	Application of cybersecurity education
Quantitative (2)	Cybersecurity	Students	USA	Safety
Qualitative (3)	Cybercrime	Students	UK	Mobile Application
Concept Paper (3)	Reasoning	Educators	USA	Legislations
Case Study (3)	Conception/ Perception	Employees	Korea	Infrastructure
Quasi-experimental (3)	Awareness	Parents	USA	Security Training

Table 2. The process of selecting past studies.

Search Journals	Keywords such as cyber education, cyber awareness, and cybersecurity were used.
Select 14 Studies	The selected studies were based on the research objective and focus. They mainly focused on cybersecurity education in learning institutions.
Database Used	Google Scholar, Emerald, Sci, Scopus, and EBSCOhost.
Limit The Studies	English Language, cybersecurity education in schools, the importance of cybersecurity awareness among young internet users, published between 2014 and 2021.

3) How can stakeholders combat these challenges in implementing cybersecurity education?

4) How can a society that embraces cybersecurity awareness be established?

5) What is the importance of a nation that embraces cybersecurity awareness?

6. Discussions and Results

This research paper had findings that are structured according to the objectives and research questions.

6.1. The Significance of Cybersecurity Education in Learning Institutions

According to various research findings, learning institutions can significantly benefit from cybersecurity education. Researchers have revealed that most adults are often unwilling to spend time or money seeking cybersecurity knowledge in programs and seminars. In this case, such adults often fall victim to cyberattacks due to the lack of knowledge on shielding themselves from such attacks [8]. Therefore, schools have proven to be the best place to ensure adequate training on cybersecurity. This is because young people are often ready and willing to learn, and this skill can help them provide a cyber defense to the United States as a nation.

In schools, teachers and administrators can organize activities and programs that help train on cybersecurity. Additionally, schools in the US are provided with grants and financial allocation from the federal government to ensure they can cope with any financial constraints. In this regard, schools in the US, especially in New York, are better positioned to implement cybersecurity education in their curriculum [11]. More importantly, schools can organize symposiums and seminars where students bombard their heads on cybersecurity issues. This can help improve students' knowledge and skills on cybersecurity awareness. Government funding can help cover the expenses of these seminars [14].

Additionally, cybersecurity education has proven vital in changing the mindset of students. The advancement in technology and the internet has encouraged invention and innovation among young people. The videos and images on the internet can help improve creativity among young people. Therefore, cybersecurity awareness can help young internet users ensure that they benefit from the internet without falling victim to cyberattacks. Today, most people lack information on the effects and importance of cybersecurity awareness, an aspect that compromises cyber ethics within the community. Therefore, incorporating cybersecurity education in learning institutions can help increase awareness among internet users [3].

6.2. Strategies Stakeholders Can Utilize in Promoting Cybersecurity Awareness in Schools

Teachers of kindergarten schools have asserted that cartoons can be a vital resource in discussing cybersecurity awareness among kids. Additionally, primary

schools have also cited that animations go a long way in attracting students' attention. Therefore, animals that display the importance of cybersecurity awareness can be used to teach students. For instance, tutors have cited that the Ipin and Upin stories can be vital in teaching cybersecurity education among students [12]. Additionally, high schools and universities that offer Communication and Information technology courses can include cybersecurity awareness in their curriculum to ensure each student has a chance to learn the effects and importance of cybersecurity [12].

Additionally, the safety issues relating to cybersecurity can be taught through other courses and subjects. For instance, in English and Literature, students can be given assignments to write essays on cybersecurity awareness. More importantly, in other learning activities such as debates and mock parliaments, students can discuss various aspects of cybersecurity. Also, speech competitions can be organized where the central theme is cybersecurity; this can help train students on cybersecurity awareness. Cybersecurity weeks can also be organized in learning institutions where students learn the significance of cybersecurity [4].

The education programs meant for teachers and tutors can also incorporate cybersecurity courses in their curriculum to ensure teachers get full training on the subject. Additionally, teachers will offer proper guidance to students when they already taught in their education programs. More importantly, the teaching models should be adjusted to include cybersecurity topics. In this way, future generations can understand how to protect themselves from cyber threats. Additionally, the government should subsidize expenses incurred in implementing cybersecurity programs in schools to ensure most learning institutions are motivated to incorporate the program in their curriculum [1].

Additionally, through cybersecurity awareness, students can learn to protect themselves from various cyber threats. More importantly, young internet users can learn to keep themselves secure and safe on the internet. Despite the inadequate access and demography to technology, teachers do not possess the necessary cybersecurity knowledge to teach their students [2]. In this way, future generations can understand how to protect their information and data from unauthorized access. However, researchers have revealed that natives have problems accepting cybersecurity awareness training because they believe that nature would protect them from harm [9].

Providing vital knowledge to uplift and upgrade students' and teachers' comprehension of cybersecurity is critical to move towards a society protected from any cyber threats. More importantly, an area protected from cyber threats can help prevent the evolution of cybersecurity threats. Due to the advancement in technology, new and emerging issues arise every day, and therefore, a solution utilized yesterday may be ineffective today. Therefore, programs on cybersecurity must be frequently upgraded to ensure they are up to date; in this way, they can tackle new and emerging problems [7].

However, some critics doubt the significance of cybersecurity training and education in schools as they claim this will only cause extra expenses to struggle

schools. For instance, private schools that lack government funding may be skeptical about implementing cybersecurity education in schools as it would be expensive. The expenses include hiring IT consultants, training teachers, and purchase of computers [11]. Although it is costly, researchers have asserted that it is worth it because it helps protect internet users from cyber threats. Since education is often up to date, it can help address the emerging cybersecurity issues [5]. Moreover, schools that aim to promote cybersecurity awareness can be utilized to ensure students get a better understanding of cybersecurity. Although cybersecurity principles have evolved over the years, most Information Technology consultants are still largely ignored. Therefore, the development of information security programs often fails to acknowledge the various principles of cybersecurity awareness [1].

In the United States, a cybersecurity awareness program called the GenCyber was invented to help train people to promote cybersecurity [13]. The program is a summer camp for grade school teachers and students supported by the NSF/NSA. Since implementing this program, teachers and students have claimed that their cybersecurity has tremendously improved through the awareness program. More importantly, the awareness program has ensured that cybercrimes have been reduced by almost half, with most internet users surfing the internet safely [13].

Therefore, such programs should be implemented across the United States to ensure that students and teachers improve cybersecurity at school and home. Additionally, the program can be vital in promoting cybersecurity preparedness and awareness among the surrounding community. In addition to this program, schools can incorporate councils and clubs focused on promoting cybersecurity awareness. Students can compete and get exposure to cybersecurity through these clubs and promote it from an individual to a communal level [2]. Through these programs and seminars, students can get directions and guidance from their tutors regarding cybersecurity. In this manner, teachers will also be improving their skills and knowledge concerning cybersecurity. According to Straub (2014), teachers and students can benefit from these programs if they become devoted and objective [14]. In this way, the aims and objectives of these programs can be outlined to ensure all students and teachers are on the same page regarding cybersecurity. More importantly, these seminars will help increase the use of technology among students, leading to inventions and innovations that can improve their creativity in class [9].

Additionally, students need to comprehend the importance of cybersecurity in their lives; in this way, learners will have the self-drive to participate in cybersecurity awareness programs. Researchers have revealed that the most effective way of promoting comprehension and understanding among students is through active learning. At this age, students often use the learner-centered approach that allows them to track their learning process. Therefore, students can look on the internet at the various aspects of promoting cybersecurity. In this case, teachers are only there to supervise and guide the student-centered learn-

ing process [1].

Active learning also proves essential in encouraging the comprehension of the importance of cybersecurity awareness. Through active learning, students can develop an awareness of cybersecurity threats such as cyberbullying and help prevent such cybersecurity incidents. More importantly, teachers should limit self-protection and cyber-sex in such cases to ensure they stay aware of harmful sites. Researchers have revealed that these contaminated sites often ask for personal information frequently retrieved and used for malicious purposes [3]. Therefore, it is crucial for parents, the government, and teachers to be proactive in tutoring students about the various cybersecurity sectors and how to overcome the criticisms on sex education.

7. Conclusions

Based on the research finding, it is evident that there is a need for cybersecurity education in learning institutions. This is because it can help protect people from various cyber threats through increasing cybersecurity awareness. More importantly, internet users can understand their vulnerabilities when using multiple social media platforms such as Facebook, Instagram, YouTube, and Twitter through cybersecurity awareness. Also, internet users can learn to prevent some cyberattacks such as cyberbullying by simply understanding their negative implications on other internet users. Besides, cybersecurity awareness can help internet users understand the legislations associated with various cybercrimes [4].

However, the implementation of cybersecurity education faces various challenges that range from the lack of governmental support to insufficient resources. More importantly, teachers' lack of skills and expertise poses a challenge, especially when they are expected to train their students on cybersecurity [10]. Therefore, relevant parties such as the government, parents, teachers, and peers must develop the best solutions to protecting young internet users from cyberbullying and other various forms of cybercrimes. Finally, the media such as radio and television should help spread the word on the significance of cybersecurity through campaigns that may be interesting and interactive to children.

Acknowledgements

I want to thank my professor for giving me this golden opportunity to conduct this incredible research on the importance of implementing cybersecurity education in schools. This project has helped me understand the importance and implications of promoting cybersecurity awareness in learning institutions.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Pencheva, D., Joseph, H. and Awais, R. (2020) Bringing Cyber to School: Integrating

Cybersecurity into Secondary School Education. *IEEE Security & Privacy*, **18**, 68-74. https://doi.org/10.1109/MSEC.2020.2969409

[2] Park, H.-Ho. (2020) A Study on Cyber Crime Deterrence Recognition: The Influence of Recognition of Punishment for Cyber Crime on Intention to Report Crime. *Korean Criminal Psychology Research*, **16**, 85-98. https://doi.org/10.25277/KCPR.2020.16.4.85

[3] Goswami, A. (2018) Impact of Cyber Security in Different Application of E-Governance. *Journal of Advances and Scholarly Researches in Allied Education*, **15**, 65-70. https://doi.org/10.29070/15/57309

[4] Rademaker, M. (2016) Assessing Cyber Security 2015. *Information & Security: An International Journal*, **34**, 93-104. https://doi.org/10.11610/isij.3407

[5] Robins, A. (2015) The Ongoing Challenges of Computer Science Education Research. *Computer Science Education*, **25**, 115-119. https://doi.org/10.1080/08993408.2015.1034350

[6] Hart, S., Andrea, M., Federica, P. and Vladimiro, S. (2020) Risk: A Serious Game for Cyber Security Awareness And Education. *Computers & Security*, **95**, Article ID: 101827. https://doi.org/10.1016/j.cose.2020.101827

[7] Negi, S. and Sunita, M. (2019) Effectiveness of Cyber Bullying Sensitization Program (CBSP) to Reduce Cyber Bullying Behavior among Middle School Children. *International Journal of Cyber Research and Education*, **1**, Article No. 5. https://doi.org/10.4018/IJCRE.2019010105

[8] Trappe, W. and Straub, J. (2021) *Journal of Cybersecurity and Privacy*: A New Open Access Journal. *Journal of Cybersecurity and Privacy*, **1**, 1-3. https://doi.org/10.3390/cybersecurity1010001

[9] Keith, M. (2015) Cyber Security Education, Qualifications and Training. In: Holloway, R., Ed., *Engineering & Technology Reference*, Institution of Engineering and Technology, London, 1-11. https://doi.org/10.1049/etr.2014.0029

[10] Fichtner, L. (2018) What Kind of Cyber Security? Theorising Cyber Security and Mapping Approaches. *Internet Policy Review*, **7**, 1-19. https://doi.org/10.14763/2018.2.788

[11] Tarasyuk, A. (2020) Certain Aspects of the Social Factor In Providing Cybersecurity of Society. *Knowledge*, *Education*, *Law*, *Management*, **2**, 206-211. https://doi.org/10.51647/kelm.2020.3.2.37

[12] Horowitz, B.M. and Scott Lucero, D. (2016) System-Aware Cyber Security: A Systems Engineering Approach for Enhancing Cyber Security. *Insight*, **19**, 39-42. https://doi.org/10.1002/inst.12087

[13] Pawar, S.C., Mente, R.S. and Chendage, B.D. (2021) Cyber Crime, Cyber Space and Effects of Cyber Crime. *International Journal of Scientific Research in Computer Science*, *Engineering and Information Technology*, **7**, 210-214. https://doi.org/10.32628/CSEIT217139

[14] Straub, J. (2014) Assessment of Examinations in Computer Science Doctoral Education. *Computer Science Education*, **24**, 25-70. https://doi.org/10.1080/08993408.2014.890792

[15] Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P.C. and Glenn, T. (2021) Increasing Cybercrime since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, **23**, Article No. 18. https://doi.org/10.1007/s11920-021-01228-w