Official Cybersecurity Curriculum for High School Students

Rahilkumar Patel

School of Cyber Security, Old Dominion University

WCS 494 Entrepreneurship in Cybersecurity

Prof. Akeyla Porcher

December 2, 2022

Official Cybersecurity Curriculum for High School Students

Introduction

The widespread reliance humans place on digital applications and devices has significantly increased the significance of cybersecurity. The utilization of the traditional course has changed the view of users in the modern world. In the contemporary world, the internet has become a powerful component of everyone's life, enabling access to everything and fulfilling users' requirements. The emergence of the internet has given birth to the field of cybersecurity. Cybersecurity is protecting designed networks, technologies, programs, frameworks, devices, and information from the access of unauthorized personals. The youth's widespread use of the internet in education and entertainment has benefited society. It helps the child to succeed in the future. Nonetheless, it is the rule of probability in the spinning of a coin. When the coin is in the air, two predictions are available. The hope will be for positive results, but the good things do bring some adverse effects. The negative impact of the internet is making an enormous impact on the world's youth.

Children today are using electronic devices before knowing the proper use, and most of these devices are actively connected to the internet and retrieving content. Children around the world are increasingly targeted by cybercrime, which poses a threat to connected networks and devices. The threat can be severe and has the capability of destroying systems, and it could leave their personal data at risk. As a result, developing an official cybersecurity curriculum for high school students is essential, and researchers have placed a significant emphasis on raising cybersecurity awareness among all citizens of a nation (Peker, Ray, & Silva, 2018).

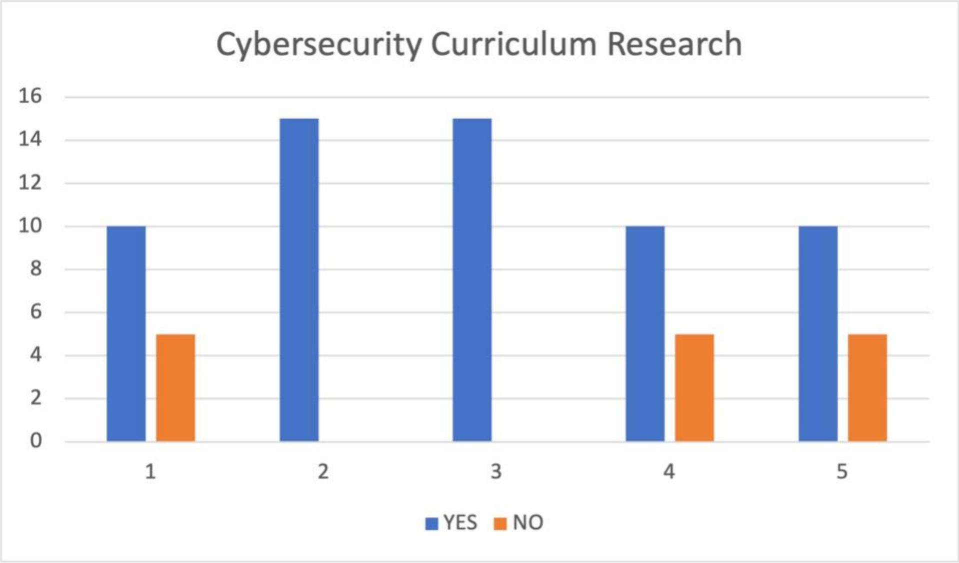
Keywords: Cybersecurity awareness, Cyberattacks, Cybercrimes, High School Students, Vulnerabilities

The research examines the definitions of cybersecurity, cyberattacks, cybersecurity awareness, cybercrimes, and vulnerabilities.

- *Cybersecurity* is the art of protecting sensitive information and digital systems from unauthorized digital attacks (Kemmerer, 2016).
- *Cyberattacks* are malicious and intentional attempts on networks and organizations to occupy sensitive information (Zhang & Chiasson, 2022).
- *Cybersecurity awareness* is the skills and knowledge to understand cybersecurity practices to prevent cyber threats to networks (Muhirwe & White, 2016).
- *Cybercrimes* are crimes committed in the digital environment to destroy or occupy the data of individuals or groups without authorization (Kemmerer, 2016).
- *Vulnerability* is the weakness in the digital devices or networks that an attacker can use to deliver a successful attack (Konstantinou, 2020).

Project Objective

Children's lack of awareness about cybersecurity leaves them as the most vulnerable components of society, and cybercriminals will easily target them. The use of the internet has skyrocketed in recent years. Moreover, now most electronic devices are designed to have the capability of connecting to the internet. The widespread availability of internet devices enables more options and easier access for cybercriminals to manipulate children. Providing cybersecurity education is one of the quickest ways to prevent the victims of cyberspace. It would require the collaboration of professors and family members to check children's progress to provide an excellent understanding of cybersecurity (AlShabibi & Al-Suqri, 2022).



We surveyed by asking questions to students of the age group 12-16 studying at either the middle school or high school. The survey was conducted with the collaboration of fifteen students. The answers were astonishing for a cyber professional, but it may seem all right to the general people. The first question was about cybersecurity knowledge and skills, and ten positive answers were found among fifteen students. The following two questions have received all fifteen positive responses do they use technology in their daily lives, and do they keep the same password for all their social media accounts? The answers determined that the lack of education on cybersecurity poses more risks to children. The next set of responses focused on whether they were victims of any cyberattack or had been taught in schools how to use the technology safely. The responses had ten positive answers, while five refused to answer because they needed an idea about the questions. The responses from students gave us a profound thought that we can develop a set of instructions for students to provide the necessary skills and knowledge of cybersecurity (Peker, Ray, & Silva, 2018).

Therefore, the official curriculum can instruct all high school students, regardless of their major. When high school students have the skills to prevent cybercrimes and the required awareness from spreading in the community, the number of cyberattacks will be reduced. Modules could be used to present the curriculum and create modules for a new subject. High school students can learn about cyber activities over the network through modules. After each module, students' readiness to prevent cyberattacks could be assessed through quizzes. The quizzes will access the understanding of skills gained by students, and they will empower them to pursue more cybersecurity knowledge. Therefore, the necessity of having an official curriculum for high school students has been a continuous debate among the education board, and the implementation of a successful program would increase the number of educated cyber professionals, prevent cyberattacks, and spread awareness in the community (Peker, Ray, & Silva, 2018).

Cybersecurity

The world heavily relies on cybersecurity because of the expansion of the internet, computer systems, and wireless networks. The growth of intelligent devices and the Internet of Things (IoT) have brought tremendous changes to human lives. The way of living has changed because of automation through the internet. Cybersecurity is an essential part of the internet, and it is impossible to maintain the security of systems without cyber skills and knowledge. According to research, "Society relies heavily on its networked physical infrastructure and information systems. Accurately assessing the vulnerability of these systems against disruptive events is vital for planning and risk management" (Dinh, Xuan, & Pardalos, 2012). The goal of cybersecurity is to provide a secure environment to protect users' privacy, data, and integrity. The failure to maintain the security of systems can leave systems vulnerable. It can allow cybercriminals to gain access to the devices unlawfully, and they can install malware, viruses, trojan horses, rootkits, and backdoors (Muhirwe & White, 2016).

Cybersecurity Awareness: An Official curriculum for High School Students

Nowadays, cybersecurity awareness is very crucial for students and internet users. "Bele et al. (2014) investigated the effect of raising cybersecurity awareness levels among middle adolescent children and highlighted children's need for knowledge and skills to mitigate cybercrimes' potential risk" (AlShabibi & Al-Suqri, 2022). Cybersecurity awareness can be crucial for networks and organizations to secure information distribution. According to previous studies, a lack of awareness and human error account for most security incidents over the internet. The greatest obstacle to cybersecurity awareness is the factor of human weakness. Several studies have been conducted to explain methods for raising cybersecurity awareness, and it would be essential to have an official cybersecurity curriculum for high school students. It will help prevent many cyberattacks on children and the education system. Moreover, it will help students to fight cyberattacks with the required knowledge and skills (AlShabibi & Al-Suqri, 2022).

Most industries and organizations are using digital platforms to complete their tasks, and they are producing enormous amounts of digital data and store it in the storage servers. Some of the data is directly connected to human lives as it has humans' information but is not completely secured on the internet. A system flaw or a bug can compromise the data. Therefore, it increases the rate of cyberattacks. Cybercriminals are more advanced than cyber professionals and need only a way to establish a connection between their system and the victims' systems. Moreover, they know that educational institutions are the prime target of cyberattacks as they lack awareness and data security to prevent disruptive events. It becomes essential to have cybersecurity education for high school students to decrease cyber threats and cyberattacks on children (Peker, Ray, & Silva, 2018).

Module Integration

The education will provide the necessary skills and knowledge to high school students with the help of modules. The skills and knowledge will integrate into the module by dividing the content into six chapters. The chapters are cyberattacks, cybercrimes, cyberbullying, cyberstalking, vulnerabilities, and third-party resources. The modules will have all the details of how it can prevent and keep cyberspace safe. It will provide the details of recent cybercrimes for study and research. Moreover, the modules will educate students to find vulnerabilities, flaws, unpatched drivers, and outdated systems so that preventive measures can be taken. Videos and images will be integrated into the modules to give a better understanding of cybersecurity. Quizzes will be taken at the end of the module to determine students' progress. Instructors will be able to see the progress of the curriculum and guide students in the right direction. The instructors will use the quiz grades to enhance students' skills, and they will not be used to provide an actual grade. There will not be any 'F' in the curriculum, but the students must complete all the assessments. There will not be any fear of failing the course for students, but it will encourage them to excel in the course (Peker, Ray, & Silva, 2018).

Moreover, modules will help students create a secure network for themselves and spread awareness in the community. Cyber skills and methods will help students to educate their parents and prevent cyberattacks. While studying official cybersecurity curriculum, students must gain and practice suitable cyber hygiene methods. Cyber hygiene is regularly maintaining the security and health of networks, devices, and users. It will help to find system flaws quickly, so malicious actors will not be able to make unauthorized access. Module integration will create a cyber chain to create more cyber professionals and make the cyber environment safe for everyone (Konstantinou, 2020).

Cyberattacks

In recent years, COVID-19 has made an enormous impact around the world. The global cycle was stopped for months to fight against the pandemic, so companies have allowed their workers to work from home. The government had imposed restrictions to reduce the spreading of the virus, but as a result, education was stopped. Many schools still need to adopt online platforms to educate children, but the sudden change in the guidelines has made schools educate children using online platforms. Online platforms are great, enabling children to educate themselves from any part of the world with internet access. As a result, children could access the educational material and connect to instructors using their smartphones, laptops, or desktops. Nonetheless, the sudden change in the infrastructure needed to be more focused on the security of devices, leaving many devices vulnerable to cybercriminals. The emergence of the pandemic started to bless cybercriminals because of the decision to adopt the online platform without accurate security measurements. Many devices were using outdated systems, drivers were not updated, and newer security patches were not installed, making them vulnerable to cybercriminals (Kemmerer, 2016).

Cybercrimes

Cybercrimes have emerged at an unexpected rate in recent times. Cybercriminals are looking for the weakest link in the system for hacking, staking, exploiting, bullying, and cheating. Research states, "Bullying is the most widespread type of cybercrime, and it covers 80% of schools among the students" (AlShabibi & Al-Suqri, 2022). Cyberbullying is taking advantage of someone without permission to abuse, prosecute, or intimidate individuals using cyberspace. Cyberbullying targets individuals in the form of electronic, physical, verbal, or social. The increase of cyberbullying on children has caused destructive damage to society. The main reason behind the attacks was the sudden implementation of online policies, which uploaded children's sensitive information on untrusted platforms. Also, the government was not ready to prevent vast amounts of cyberattacks on the education systems because cybercriminals were targeting groups and organizations to obtain personal information. According to a survey by the Cyberbullying Research Center, "almost 34 per cent of students in middle and high school had been cyberbullied in 2016 - the largest percentage reported since the organization began tracking cyberbullying ten years ago" (Dazeley, 2022). The growing number of cyberbullying can bring adverse effects on students. It could increase their anxiety level and put them under tremendous depression. It can impact the student's academic performance and may lead them to a wrong way of adapting and making the bad habit of drugs and alcohol. As a result, depression and bad habits are why students commit suicide at a young age. It will be the loss of family and community because young people are the drivers to lead the planet to a beautiful destination (Joshi, Ramani, Murali, Krishnan, & Mithra, 2013).

Vulnerabilities

It requires establishing a connection between two devices to send the data over the network so the data transfer process is completed with successful authentication. The versions of systems, drivers, and security patches play an essential role during the data transfer process, providing confidentiality, integrity, and availability. Nonetheless, when a system fails to maintain the required security standards, it becomes vulnerable to attackers. Vulnerabilities can be present in the software or hardware of systems. Attackers use different tools and methods to find vulnerabilities, allowing them to exploit systems. Therefore, it is a critical practice to keep systems secure over the network. It is essential to assess the network platforms, prioritize assets, and keep the information secure by necessary vulnerabilities scan on systems. Nonetheless, the sudden change in the education system has made many devices vulnerable. It was an excellent initiative by the government to educate children over the internet to continue education in the difficult time of the pandemic. Many students were using old computers, and some needed computer access. Many computers failed to maintain quality-of-service (QoS) on the network, resulting in malicious cyberattacks and dangerous events for the community. The identified vulnerabilities can be used to establish a backdoor connection to devices and occupy users' sensitive information. Therefore, the education board needs a robust design for vulnerability check-in of students' devices to maintain security and prevent cyberattacks on schools (Qayyum, Cruzes, & Jaccheri, 2021).

Overview of knowledge outside the major

Cybersecurity is an emerging field that has gained attention in recent years. Internet technologies have changed the structure of cybersecurity. It has provided ease in human lives by creating new devices. Nonetheless, education in cybersecurity is optional for many majors. The personal experience that among the general courses taken, most of the general courses' professors needed to gain more knowledge about cybersecurity. Moreover, some professors needed help adapting the technology to students and required skills and knowledge of cybersecurity to prevent attacks. Most instructors were the victims of cyberattacks. Cyberattacks can make a significant impact on the economy as they can destroy the economy. According to the research, "the estimated cost of cybercrimes in the United States is $3.5 billion a year, and each attack takes place at the approximation of 39 seconds" (Joshi, Ramani, Murali, Krishnan, & Mithra, 2013). Most of them happen because of a lack of human awareness, and it can compromise password security and allow cybercriminals to install malware on their devices. They are an essential component of cybersecurity and play a crucial role in preventing cyberattacks. Malware and password security are explained below for module integration and spread awareness outside the major.

Malware

Malware is malicious code designed to damage systems and networks to gain unauthorized access to someone else's devices. Worms, backdoors, shell scripting, trojan horses, viruses, and spyware are malware. Vulnerabilities in systems can allow cybercriminals to install malware to manipulate systems. Users often download free stuff from unknown web sources so that it could have a malicious script written on it and exploit the systems. The successful installation of malware can encrypt the user's data and demand money to decrypt the data. Moreover, it could damage an organization's infrastructure, resulting in the loss of wealth and reputation. Research states, "In May 2017, a global ransomware campaign adversely affected approximately 48 UK hospitals. Response to the WannaCry cyber-attack resulted in many hospital networks being taken offline, and non-emergency patients being refused care" (Boddy, Hurst, & Mackay, 2017). Nowadays, cybercriminals are targeting students to deploy malware on their devices because students are actively using the internet and would like to retrieve the content quickly. They may click on malicious advertisements while retrieving the content and provide access to third parties. Cybercriminals know that students still need to be involved in preventing malicious attacks. Therefore, it is essential to have cyber awareness for students, so students' privacy, sensitive information, and data will not be violated (Konstantinou, 2020).

Password Security

Password security is an essential component of the networks which enables robust security. However, it is also the central area of concern when users have weak passwords to protect their privacy. As a result, it brings the biggest threat to the networks. "Lack of encryption: most ICS protocols send all data in clear text; thus, an attacker can intercept the communication to read all packets and data sent" (IRMAK & Erkek, 2018). All the information will be shared when the attacker has found the vulnerability and established the connection between the victim and the attacker. If the user logs in using the web browser and opens the portal, the information shared in plaintext will be intercepted by the attacker. After occupying the login credentials, attackers can access the user's personal information, credit cards, and social security numbers (Qayyum, Cruzes, & Jaccheri, 2021).

According to the survey of fifteen students aged twelve to sixteen, all fifteen students mentioned that they use the same password for their social media accounts. The passwords were their names, family names, birth dates, and pet names without the combination of memorable characters and numbers. Moreover, many users keep the default passwords as their regular password because of the easy accessibility to the devices, but they do not know the outcome destroy systems and data. The combination of passwords was so easy that dictionary and brute force attacks could quickly crack. Therefore, it is required to have awareness about developing solid passwords and change it after some time (Dinh, Xuan, & Znati, 2012).

Effective Innovation

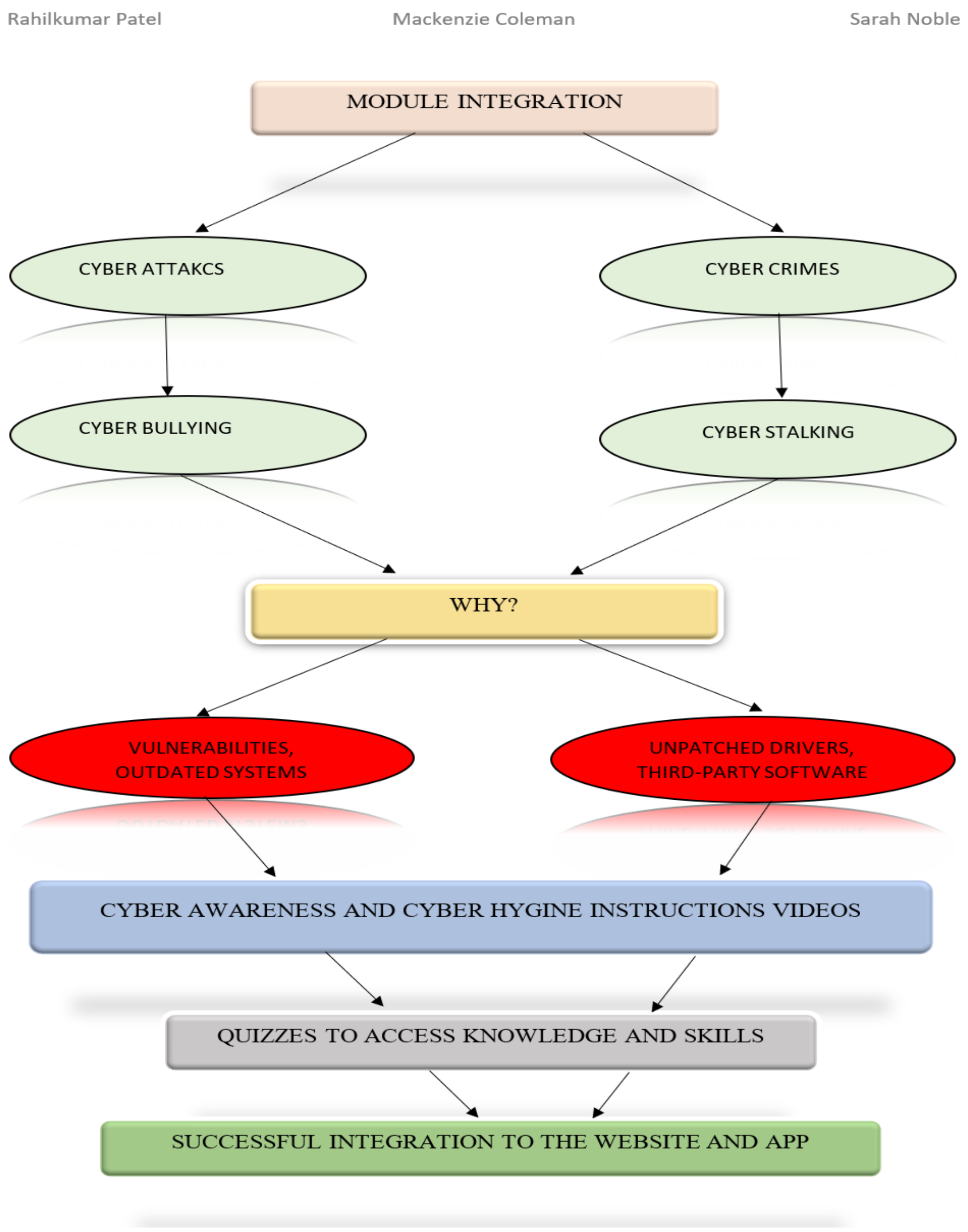
It is required to have an official cybersecurity curriculum for high school students. According to the survey, more than 50% of cyberattacks have increased in the educational environment. Moreover, over 60% of students were targeted by ransomware attacks. Students are the primary source of cybercriminals because they lack cybersecurity knowledge and skills. Therefore, Cyber professionals are looking at the consequences and actively working on reducing cyberattacks and keeping the environment safe for students. Technologies have changed the infrastructure of human lives, and it has benefited students to an extraordinary level.

Students can use online platforms to educate with the help of the internet. Instant access allows one to have entertainment and stay connected with friends and family. Moreover, collaboration allows students to work in groups, play games, complete tasks, and seek help from instructors (IRMAK & Erkek, 2018).

Fortnite and PubG are popular games that every student would like to play. They are available on the app stores, but most students download them from third-party websites, and they need to be verified and trusted websites. It could have scripts written in the games to install malicious software on students' devices. Moreover, games are advertising various vendors on their platforms to generate revenue, but the advertisement can have phishing links to steal students' data and information. Nonetheless, the official curriculum can teach skills and guide students, and it will educate them on using the website, gaming platforms, and group chats. Furthermore, training will be provided on downloading software from trusted sources and eliminating phishing links in students' emails, browsers, and games. The innovation will be very effective, and it will help to prevent cyberattacks in the educational environment. The increase in the skills of cyber students will increase the number of cyber professionals in the community (AlShabibi & Al-Suqri, 2022).

Bringing Innovation to Reality

It is crucial to have a robust idea to determine the situation and requirements. It is a process of creative and critical thinking aimed at the betterment and benefits of the community, and it addresses how it can be helpful to humans. A successful product requires a plan to visualize the process, and it will be followed by feedback from peers and community members to have a quality product. Therefore, we have designed a plan to make the official cybersecurity curriculum for high school students. The process has been explained on how it can be a successful innovation in the education environment (Peker, Ray, & Silva, 2018).


Rahilkumar Patel
Mackenzie Coleman
Sarah Noble
MODULE INTEGRATION
CYBER ATTAKCS
CYBER CRIMES
CYBER BULLYING
CYBER STALKING
WHY?
VULNERABILITIES, OUTDATED SYSTEMS
UNPATCHED DRIVERS, THIRD-PARTY SOFTWARE
CYBER AWARENESS AND CYBER HYGINE INSTRUCTIONS VIDEOS
QUIZZES TO ACCESS KNOWLEDGE AND SKILLS
SUCCESSFUL INTEGRATION TO THE WEBSITE AND APP

The plan has been divided into six phases, all addressed with real-life events, and students have taken feedback on how it can be a practical approach. Moreover, the implementation part requires the collaboration of the Virginia Education Association and the approval of the high school departments in every high school in Virginia. The team focuses on Virginia Education Association's mission: "To unite our members and local communities across the Commonwealth in fulfilling the promise of a high-quality public education that successfully prepares every single student to realize his or her full potential. We believe this can be accomplished by advocating for students, education professionals, and support professionals" (Virginia, 2022).

Moreover, the approval to integrate the curriculum into high school systems will enable us to provide the training and skills to high school instructors. The school board must have a minimum of two instructors to provide cyber education to students. Moreover, they will need to monitor students' progress actively to excel in the course, so it will require creating a website to provide easy access to students. Nowadays, the advancement in technology has allowed the education platform to educate students online, and students can accomplish their assigned tasks over the internet at their convenience. Therefore, the website will be integrated with the school's website to provide remote access to the course materials. It will enable students to complete tasks online and learn more cyber skills and knowledge. They will require active monitoring to identify vulnerabilities and security flaws to prevent cyberattacks on the website. Therefore, the instructors will be trained and provided with tools to perform necessary scans on their connected network. The scan reports will be reviewed, and the required actions and patches will be made to establish a secure cybersecurity environment for high school students (Peker, Ray, & Silva, 2018).

Summary of Next Steps

It is crucial to have innovations in the product to develop a new experience for the users. Users are always looking to find innovations in products, and it is essential to have upgrades to existing products. Sometimes, it will give a better experience to users, or it will increase the dominance in the market with the competitors. Therefore, we have planned to develop an App, provide hands-on exercise, and develop a game based on cyber skills and techniques. A survey released in 2015 by Pearson "found that 53 per cent of 4th and 5th graders, 66 percentage of middle schoolers, and 82 percentage of high school students regularly used a smartphone. In addition, 41 per cent of polled students reported using a smartphone at least twice a week to complete schoolwork, according to the survey conducted on about 2,300 elementary, middle, and high-school students" (Versel, 2018). It is vital to have an App that will enable remote access to the course content for students. It will only require an active network connection, but apart from that, they will be able to complete the assigned tasks and assignments using their smartphones (Versel, 2018).

The integrations of hands-on exercises will be based on real-world cyberattacks. A virtual environment will be created for students to enhance their cyber techniques and skills. The students will be provided with a real-world cyber scenario with the details, so students will need to find possible ways to overcome the situation. Students will be asked to perform actions in a secure virtual environment, which will not negatively impact systems. Furthermore, developing cyber games for students will enable them to learn and prevent cyberattacks. Nowadays, most students like to play different games to entertain themselves, so cyber games will entertain them while providing cyber education. It is proven that students can learn quickly by having a practical experience which will be remembered for a long time. Therefore, the hands-on exercises and cyber games will benefit students to excel in the course (Konstantinou, 2020).

Self-Reflection

Rahil Patel

Director

Advanced Technology Center

November 28, 2022

Self-Reflection Letter

Cybersecurity is an evolving and innovative field that keeps improving in the cyber world. Cyber professionals will never feel like they have explored everything in the field and will keep working on protecting humans' privacy, data, and information. Nonetheless, according to the research, approximately 2200 cyberattacks happen daily (IRMAK & Erkek, 2018). Most of them are aimed at students. Innocent students become victims of cyberattacks because of a lack of cyber skills and knowledge. Therefore, educating students and providing cyber skills and techniques to prevent cyberattacks is essential.

An official cyber security curriculum for high school students is a great initiative to educate students about cyber skills and methods early in life. The curriculum will be integrated into the existing curriculum, making it easy for students to accommodate. There will not be any pressure to pass the course, but it will excel them to strive in the course with active participation. Real-world cyberattacks will be presented in scenarios to understand and identify the situation, guiding students to take preventive measures using the internet. As a result, there will be fewer cyberattacks targeting students.

Thank you,

Rahil Patel

Conclusion

Digital devices and applications have increased the importance of cyber security because humans rely heavily on the internet. As a result, the number of cyberattacks has skyrocketed as not all digital applications are secured to connect to the internet. Cybercriminals identify students as their main target because they lack cyber skills and education. Nonetheless, an official cybersecurity curriculum for high school students can create awareness in the community, which will help prevent many cyberattacks in the future. Furthermore, it will create more cyber professionals by giving them a passion at the early stage to students.

References

AlShabibi, A., & Al-Suqri, M. (2022, January 17). *Cybersecurity awareness and its impact on protecting children in Cyberspace*. Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace. Retrieved October 18, 2022, from https://ieeexplore.ieee.org/abstract/document/9677117/

Dinh , T. N., Xaun , Y., & Znati, T. (2011, October 18). *On new approaches of assessing network vulnerability: Hardness and ...* On New Approaches of Assessing Network. Retrieved November 18, 2022, from https://ieeexplore.ieee.org/document/6051504

IRMAK , E., & ERKEK, I. (2018, July 5). *An overview of cyber-attack vectors on SCADA systems*. An Overview of Cyber-Attack Vectors on SCADA. Retrieved October 25, 2022, from https://ieeexplore.ieee.org/document/8355379

Joshi , A., Ramani, V., Murali, H., Krishnan, R., & Mithra, Z. (2013, May 31). *Student Centric Design for Cyber Security Knowledge Empowerment | IEEE ...* Student centric design for cyber security knowledge empowerment. Retrieved November 7, 2022, from https://ieeexplore.ieee.org/document/6208658

Kemmerer, R. (2016, May 28). *What is cybersecurity?* IBM. Retrieved November 18, 2022, from https://www.ibm.com/topics/cybersecurity

Konstantinou, C. (2020, January 1). *Cyber-physical systems security education through hands-on lab ...* Cyber–Physical Systems Security Education Through Hands-on Lab Exercises. Retrieved December 1, 2022, from https://ieeexplore.ieee.org/document/9130868/

Muhirwe, J., & White, N. (2016, March 18). *A review of the impact of training on cybersecurity awareness*. CYBERSECURITY AWARENESS AND PRACTICE OF NEXT GENERATION CORPORATE TECHNOLOGY USERS. Retrieved October 18, 2022, from https://www.researchgate.net/publication/336766330_A_REVIEW_OF_THE_IMPACT_OF_TRAINING_ON_CYBERSECURITY_AWARENESS

P, D. (2022, November 4). *Cyberbullying in school*. Accredited Schools Online. Retrieved November 27, 2022, from https://www.accreditedschoolsonline.org/resources/cyberbullying-prevention-and-support/

Peker, Y., Ray, L., & Silva, S. (2018, December 30). Online Cybersecurity Awareness Modules for College and High School Students. Retrieved December 1, 2022, from https://ieeexplore.ieee.org/Xplore/home.jsp

Quayyum, F., Cruzes, D., & Jaccheri, L. (2021, December 15). *International Journal of Child-Computer Interaction*. International Journal of Child-Computer Interaction | Review Articles in Child-Computer Interaction Research | ScienceDirect.com by Elsevier.

Retrieved October 18, 2022, from https://www.sciencedirect.com/journal/international-journal-of-child-computer-interaction/special-issue/10LRHCZP8MM

Versel, L. (2020, December 8). *As cell phones proliferate in K-12, schools search for smart policies*. Education Week. Retrieved November 29, 2022, from https://www.edweek.org/technology/as-cell-phones-proliferate-in-k-12-schools-search-for-smart-policies/2018/02

Virginia, A. (2019, August 16). *Advocating a high-quality public education: Virginia Education Association*. VEA Website. Retrieved October 18, 2022, from https://www.veanea.org/about/who-we-are/

Zhang, L., & Chiasson, S. (2022, January 2). *A systematic review of multimedia tools for cybersecurity awareness and Education*. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. Retrieved December 1, 2022, from https://www.researchgate.net/publication/348180029_A_Systematic_Review_of_Multimedia_Tools_for_Cybersecurity_Awareness_and_Education