Empowering K-12 STEM Educators: Enhancing Cybersecurity Awareness Through Professional Development

Gahangir Hossain
Dept of Information Science
University of North Texas
Denton, USA
Gahangir.Hossain@unt.edu
ORCID : 0000-0002-8205-4939

Mikyung Shin
Dept. of Education
West Texas A&M University
Canyon, USA
mikyung.shin@wtamu.edu
ORCID: 0000-0001-7907-9193

Mehnaz Afrose
Dept. of Computer Information Systems and Business Analytics
West Texas A&M University
Canyon, USA
mafrose1@buffs.wtamu.edu

***Abstract*— Given the increasing significance of promoting cybersecurity awareness within K-12 educational settings, it becomes imperative to provide teachers with appropriate professional development. This paper reports on a current workshop that aimed to assess the viability of cybersecurity online modules developed by researchers and to deliver cybersecurity training to high school STEM educators. The workshop sought to evaluate the level of cybersecurity awareness among teachers and enhance their comprehension of its importance. This evaluation was conducted through scales devised by researchers, aligned with standards set by the National Institute of Standards and Technology and the Computer Science Teachers Association. The training also aimed to fortify teachers' grasp of cybersecurity content, encompassing relevant standards, analysis of cyber threats, establishment of secure online environments, and other pivotal cybersecurity concepts. Acknowledging the comprehensive nature and adaptability of cybersecurity education, the workshop endeavored to distill essential ideas and recommended practices tailored for K-12 teachers. In this document, we outline the workshop's structure, in addition to presenting the initial survey and assessment outcomes. The findings demonstrate an enhancement in teachers' awareness of cybersecurity and affirm the social significance of their learning experiences, thereby equipping them for the forthcoming academic year.**

Keywords*— *Cybersecurity awareness, STEM education, Teacher training, NIST and CSTA standards, Online privacy

I. INTRODUCTION

As the educational world embraces transformative technology and online connectivity , the choice to shield confidential informations, make sure students are well supported, and can protect the authenticity of educational endeavors has emerged as an overarching priority [1]. The increasing usage of emerging technology brings about more exposure to cybersecurity concerns and makes attention to cybersecurity of utmost significance [2]. As well as teachers working in academic establishments face a pressing need to tackle and mitigate the multifarious dangers of the digital environment [3].

In the face of developing cybersecurity needs, a current record by the American Government Accountability Office highlights the extent of damage due to school cyberattacks, which includes lengthy disruptions, months of recovery efforts, financial losses up to million, and the alarming compromise of personal information, risking emotional, physiological, and financial damage [4]. K-12 graders from districts and schools have emerged as potential targets of private issues and crimes, regularly exacerbated via lack of cybersecurity practices, and that is why formal cybersecurity recognition emerges as a crucial defense against the vulnerabilities exploited by cybercriminals [5].

Ransomware, a widely recognized malicious software causing financial harm, has surged due to the evolving threat landscape; this type of malware, which locks computer files, via encryption and demands payment for decryption, presents a growing danger by preventing users from accessing their files, systems, or networks until a ransom is paid [6]. Because of the COVID-19 pandemic working and learning through digital connection has increased significantly, which has made the school network more vulnerable to ransomware attacks [7].

The severity of the situation is significant from the alarming statistics that reveal how big the problem is. In 2020, a record-breaking 408 cybersecurity incidents hit schools, affecting 377 districts in forty states – marking an 18% increase from the year before; these led to school closures and misused funds, and data breaches caused credit card fraud and identity theft, affecting various stakeholders [8].

Educators need to plan safe and enriching online experiences for students, which requires clear guidance on internet safety, but teachers could lack adequate information about their students' potential risky behaviors online [9]. Teacher training helps educators use computers for better learning, but some feel confident about safety; however, looking closely at their grasp of cyber ethics, online safety, and related areas, along with their confidence in teaching them, reveals they aren't fully prepared to teach these topics effectively [10].

All these references indicate that educational institutes are at great risk of cyber-attacks and becoming more vulnerable day by day. In this scenario, it is time to give emphasized attention to cybersecurity among teachers as they play a key role in spreading cybersecurity attention among their students. Aiming for this, we have organized a two-day workshop session for the STEM teachers to equip them with knowledge of cybersecurity which can help them to convey their awareness into the classroom.

II. METHOD

A. Recruitment of Participants

In contacting and recruiting high school teachers, the principal investigators have communicated with the education specialists, school administrators, and teachers in STEM (Science, technology, engineering, and mathematics) fields, including the career and technical education department. In the summer 2022, the research team invited teachers to a 1-hour led pre-workshop where teachers shared the importance of cybersecurity topics about phishing and spam emails, malware, ethics, privacy, policy, and assessment. With the continuous collaboration and partnership with schools in the Texas Panhandle, we invited high school STEM teachers to the current workshop upon the letter of support from the school or local Independent School Districts following the guidelines of Institutional Review Boards.

B. Participants

Eight high school general education or special education STEM teachers, working at seven different public high schools in Texas, participated in this cybersecurity training. The participants' ages range from 25 to 61. Table I shows that they have between 1 year and 25 years of teaching experience in the STEM fields. In the school, participants taught important disciplines, including mathematics, chemistry, physics, astronomy, CTE, and technology. We can tell that they are very knowledgeable in their subjects based on the number of years they have spent teaching.

TABLE I. PARTICIPANTS' DEMOGRAPHIC SUMMARY

Age	Gender	Race/Ethnicity	Role in school	Years of teaching
46	Male	White or Caucasian	Teacher of Chemistry, Physics, Astronomy, and Video Game Design	24 years
50	Female	White or Caucasian	Special Education Teacher	25 years
26	Female	White or Caucasian	CTE Teacher	1-3 years
43	Female	White or Caucasian	Technology	1-3 years
25	Female	White or Caucasian	Teacher	1-3 years
61	Female	Caucasian/ Hispanic	High School math teacher	23 years
34	Female	Hispanic	Teacher/Admin Assistant	1-3 years
41	Female	White or Caucasian	Teacher	11-20 years

C. Development of Cybersecurity Modules

Between May 30 and May 31, 2023, the workshop was held. There were two days of training, a total of 12 hours with six hours per day. Nine instructors from West Texas A&M University and the University of North Texas shared their expertise on various facets of cybersecurity.

The research team used a computing cybersecurity framework and curriculum based on both national and state-level standards, such as the National Institute of Standards and Technology (NIST) and Computer Science Teachers Association (CSTA) standards. Among the CSTA standards, we first identified the cybersecurity sub-concept under the Networks and the Internet concept. Reviewing cybersecurity components through previous literature (e.g., Coenraad et al., 2020; Ignaczak et al., 2021), the research team has developed the basic level module covering topics such as concepts and issues related to cyber ethics, privacy, forensics, cyber threats, and data security. The recorded videos and resources for the basic-level modules are publicly available at https://mshin77.github.io/perfect-basic.

TABLE II. MODULE CONTENT

#	Topics and Resources
1	Cyber ethics, privacy, forensics, and investigation [11]
2	Cyber threats analysis: Concept of cyber data [12][13][14]
3	Basic ethical hacking: What do hackers do through wireless/ mobile networks. [15] [16]
4	Cybersecurity through games-based learning [17]
5	Securing networks, internet, the web/cloud, and email accounts, detection, and protection with tools [18]
6	Social media security, and educational tools for kids learning cybersecurity. [19][20]
7	Blockchain, Encryption-Decryption, Authentication passwords, multi-factor, and single-sign on. [21][22]
8	Cybersecurity frameworks/ career, standards and Metaverse. [23][24][25]

D. Data Collection

The workshop was delivered in a flipped learning format. Participating teachers were invited to watch the recorded videos (20 to 30 min per topic) and access the workshop materials before joining the virtual face-to-face workshop. During the online workshop through Zoom, instructors provided reviews and emphasis on what should be taught per topic. The virtual meeting focused on hands-on activities and interactions among teachers and workshop presenters, extending the content. All teachers have experience using the virtual online platform; thus, we did not make any additional preparations and assistances to make them participate in the session. Table II shows the summary of each topic and resource.

The workshop began with an overview of the "PERFECT- Providing Environment and Resources for STEM 9th-12th Graders in Effective Cybersecurity Training" project. Then there was a discussion about cyber ethics, privacy, forensics, and investigation: why we need to care for our children. This was the first workshop session. In the second session, there was a detailed discussion of Cyber Threats Analysis: the concept of analyzing cyber data (e.g., malware, DoS, n/w packets, etc.) using Weka or other simple tools. This conversation led to the lunch break. Following the lunch break, there was an educational session on basic hacking: what do hackers use wireless/mobile networks? The day concluded with a lecture on Cybersecurity through Games Based Learning.

The workshop resumed the following day with a lecture on Securing networks, the internet, the web/cloud, and email accounts, detection, and protection (with tools such as Wireshark available). The second session of the second day focused on social media security and educational tools for youngsters studying cybersecurity. Following the lunch break, the speaker reviewed blockchain, encryption-decryption, and authentication (passwords, multi-factor authentication, and single sign-on). The workshop presented a detailed lecture on cybersecurity frameworks and Careers. The closing discussion focused on the metaverse. In a variety of settings, advanced technology, including the metaverse, can increase learners' motivation and learning chances. This technological development could, however, potentially present unforeseen security risks. Proactive steps must be taken in using and producing data while considering the restricted resources. Accessibility among underrepresented groups should be ensured to have a responsible technology implementation.

E. Procedures

The team shared handouts and exercises following each lesson to support attendees' active participation. One of the significant hands-on activities involved cyber data analysis using Weka, which involved looking at a dataset to identify different network assaults, the features that were used to detect them, and perhaps even developing a model to predict similar attacks in the future. Everyone was successfully able to accomplish the task.

Another intriguing activity was utilizing the scratch app to create a password-guessing game. Participants received individual support from each presenter while participating in hands-on activities. After the session, teachers could employ and review what they practiced at each session.

Other noteworthy activities included a crossword puzzle game on cybersecurity awareness, playing an internet safety Hangman game to discover frequently used cyber terms, and several quizzes. The quizzes heightened everybody's competitiveness as they wanted to submit accurate answers quickly.

Everyone received an optional case study assignment after the workshop. The task was to comprehend their cybersecurity frameworks and standards. Each participant demonstrated a good level of understanding while employing the cybersecurity framework and standards illustrated by the case study.

III. Results

A. Post-Workshop Survey

After the workshop, we gave the participants a survey to gauge how well it had increased their awareness of cybersecurity issues, the state of the school's cybersecurity system, and their desire to share what they had learned with their students.

There were 25 questions asked in the survey. We asked them: “Establishing cybersecurity roles and responsibilities for students is just as important as establishing roles and responsibilities for senior executives (teachers, senior teachers, principal) in my school” to determine how much they value their part in ensuring cybersecurity. Agreed strongly made up 62.5% of responses, agreement made up 25%, and disagreement made up 12.5%. In the response to the question “How our school properly manages remote access (e.g., virtual private network) to its information systems and assets", only 37.5% responded excellently, whereas 12.5% think the school management system is very poor.

When we asked, “What topics could we address in the future cybersecurity workshop to benefit you?” their responses were:

- Passkeys (FIDO authentication), detecting student exploits such as proxies to subvert school security
- Knowing which emails are legitimate and which to ignore/report.
- How to set up a classroom server and use it to practice cybersecurity

After analyzing the survey results, we discovered that the workshop increased the teachers' cybersecurity expertise and that they were very keen to share that knowledge with their students. They can spot the weaknesses in managing cybersecurity in schools. In terms of protecting the school's cyberspace, there is much to be done in collaboration with them.

B. Evaluation:

Before the workshop, the teachers knew about cybersecurity in general. But, after the workshop, they have the knowledge to measure the whole aspect according to the NIST and CSTA K-12 cybersecurity standards. They now have a clearer understanding of their roles in educating students about cybersecurity awareness in accordance with the NIST framework and CSTA K–12 cybersecurity standards, as well as their duty to protect the school's cyberspace. For instance, a significant portion of students enjoy playing video games online. The lesson "Game-Based Learning" gave a detailed explanation of how cyberattacks may affect not only kids but even adults. There was also a discussion of password-guessing online games, which, when used to teach cybersecurity without making the subject boring, may excite students about using strong and difficult passwords to secure their online accounts. This was the participants' point of view, and they asked for details so they could teach the same topic to their students in class. Responses from the case study analysis show that they thoroughly understand how to use the CSTA and NIST frameworks for cybersecurity. The participants loved the idea of Metaverse.

C. Narrative Description of Evaluation

Overall, teachers evaluated the usefulness of the cybersecurity training as 4.5 out of 5. 70% of them liked that the topics of the training were well designed. They decide upon more of these sorts of schooling workshops. Teachers feel that their school's management efficiency in managing remote access is 45% effective. Because the scale ranges from 1 to 5, at least one person believes the management system is poor. Their school's management efficiency in managing remote access is 45% effective. Because the scale ranges from 1 to 5, at least one person believes the management system is poor.

Participants showed satisfactory responses in general. In every session, they were inquisitive to comprehend better. The individuals engaged in the workshop processes through interactive games, specifically the quizzes. Teachers responded that they could apply a wealth of knowledge at the event to their teaching.

TABLE III. SUMMARY OF SURVEY RESPONSES

Topic	Avg.	Range
Overall workshop experiences	4.5	4-5
The importance of creating cybersecurity roles and responsibilities not just for students but also for instructors and school administration personnel.	4.375	2-5
Communicating cybersecurity roles, responsibilities, and risk management decisions to students.	4.5	3-5
The school’s management efficiency in managing the remote access to its information systems and assets.	3.625	1-5

IV. DISCUSSION

Our training initiative had the specific goal of equipping STEM educators with knowledge in cybersecurity. This knowledge would then be seamlessly integrated into their STEM lessons, fostering a heightened awareness of cybersecurity among their students. These instructional strategies underscore the importance of safeguarding online privacy, aligning with the K–12 NIST and CSTA guidelines. Teachers are tasked with incorporating cybersecurity practices into their teaching routines, both in the physical classroom and in virtual learning environments.

We have maintained ongoing communication with the teachers who participated in our program. As the subsequent school year commences, we intend to provide these educators with a comprehensive assessment of the NIST and CSTA K–12 requirements, along with the NASA task load index. This will enable a more thorough evaluation of various extensive aspects of cybersecurity. The aim is to construct and evaluate a cybersecurity awareness scale, leveraging the insights derived from this survey.

Informed by valuable teacher feedback, our research team will refine the content of our online modules. We will then seek input from participating teachers to ensure the accuracy of the updates. Our commitment extends to extending the current cybersecurity training regimen and disseminating resources throughout the community via ongoing workshops in the upcoming academic year. Furthermore, the college plans to involve STEM instructors from neighboring schools to guide secondary school students in grades nine through twelve. Our objective is to consistently enhance university students' grasp of cybersecurity, empowering them to comprehend, manage, and safeguard themselves against online threats. This cybersecurity program will equip students with practical skills in the digital realm.

CONCLUSION

Professional development opportunities in the field of cybersecurity for high school teachers in inclusive school environments are insufficient. This encompasses educators who work with students both with and without disabilities. Our approach adopts a flipped learning format, and all resources are openly accessible to facilitate the dissemination of information and extend the benefits to both practitioners and the public. In the future, researchers will have the opportunity to expand and generalize the current outreach initiative. This expansion could involve organizing cybersecurity awareness workshops for parents of schoolchildren. This comprehensive approach would enable the younger generation to gain a holistic understanding of their roles and responsibilities in cybersecurity, learning both from their schools and their parents at home.

ACKNOWLEDGMENT

The "PERFECT - Providing Environment and Resources for STEM 9th-12th Graders in Effective Cybersecurity Training" project was supported by the Office of Naval Research (ONR).

REFERENCES

[1] I. Goran, "Cyber security risks in public high schools," *CUNY Academic Works*, 2017. https://academicworks.cuny.edu/jj_etds/5

[2] R. K. M. Bharadwaj and B. García de Soto, “Cyber security challenges and vulnerability assessment in the construction industry,” In *Creative Construction Conference*, Budapest, Hungary, 2019, doi: 10.3311/CCC2019-005.

[3] D. Pencheva, J. Hallett, and A. Rashid, "Bringing cyber to school: Integrating cybersecurity into secondary school education," *IEEE Security & Privacy*, vol. 18, no. 2, pp. 68-74, Mar.-Apr. 2020. doi: 10.1109/MSEC.2020.2969409.

[4] *As cyberattacks increase on K-12 schools, here is what’s being done*, U.S. GAO, 2022. https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done

[5] M.D. Richardson, P.A. Lemoine, W.E. Stephens, and R.E. Waller, "Planning for Cyber Security in Schools: The Human Factor," *Educational Planning*, vol. 27, no. 2, pp. 23-39, 2020.

[6] E. Alhajjar and K. Lee, "The US Cyber Threat Landscape," in *European Conference on Cyber Warfare and Security*, vol. 21, no. 1, pp. 18-24, June 2022.

[7] J. G. Koomson, "Rise of Ransomware Attacks on the Education Sector During the COVID-19 Pandemic," *ISACA Journal*, vol. 5, pp. 1-4, 2021.

[8] E. Belastock, "Our Biggest Nightmare Is Here: Cyberattacks are targeting school districts. How can schools respond to keep data and systems secure?" *Education Next*, vol. 22, no. 2, pp. 44-50, 2022.

[9] C. Chou and H. Peng, "Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience," *The Internet and Higher Education*, vol. 14, no. 1, pp. 44-53, 2011.

[10] P. Pusey and W. A. Sadera, "Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference," *Journal of Digital Learning in Teacher Education*, vol. 28, no. 2, pp. 82-85, 2011.

[11] NRE US Navy: https://www.nre.navy.mil

[12] Weka : https://sourceforge.net/projects/weka/

[13] CodeMonkey: https://www.codemonkey.com/

[14] Curiosity Machine: https://www.curiositymachine.org/lessons/lesson/

[15] Anitvirus Kespersky: https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online

[16] Ethical Hacking: https://www.simplilearn.com/career-benefits-of-learning-ethical-hacking-

[17] Scratch: https://scratch.mit.edu/download

[18] Wireshark: https://www.wireshark.org/download.html

[19] Haveybeenpwned https://haveibeenpwned.com/

[20] Security awareness: https://securityawareness.usalearning.gov/cdse/multimedia/games/cybersecurity-crossword/index.html#

[21] Password Security: https://www.security.org/how-secure-is-my-password/

[22] Blockchain: https://101blockchains.com/explain-blockchain-to-a-child/

[23] NIST : https://www.nist.gov/cyberframework

[24] K12 standers: https://csteachers.org/k12standards/

[25] Metaverse: https://metaverse-standards.org/