ISSN: 2473-4901
v11 n6383

Beyond Awareness: Building Digital Resilience Through Comprehensive Cybersecurity Foundations for K-5 Students

Ellie Ebrahimi
ebrahimie@uncw.edu

Yasin Emre Gokce
gokcey@uncw.edu

Marjorie Pare
parem@uncw.edu

Jude Vargas
jrv4914@uncw.edu

Jacob Blount
jmb7970@uncw.edu

University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

This paper introduces Cybersecurity Practice and Awareness for Rising Kids (Cyber-PARK), an innovative cybersecurity education platform specifically designed for K–5 students. Cyber-PARK aims to empower teachers and parents by offering a comprehensive suite of interactive tools, including PowerPoint presentations, videos, worksheets, hands-on activities, and video games. These resources are designed to facilitate the seamless integration of digital safety lessons that align with state and federal guidelines. The platform fosters early digital literacy and builds resilience against online threats, preparing the next generation for a secure digital future. This paper will detail the Cyber-PARK curriculum, outlining its modules and lessons. Furthermore, it will present empirical evaluations from usability testing conducted with diverse groups, including K-5 students, high school students, K-5 STEM/Technology/Media teachers, and cybersecurity experts. The results of these experiments highlight the engagement and comprehension of the content by students, the usability and adaptability of the materials for teachers, and the expert validation of the curriculum's relevance and importance. The insights gained from these evaluations have been instrumental in refining the Cyber-PARK platform, ensuring its scientific soundness and practical effectiveness in addressing the critical need for early cybersecurity education.

Keywords: Cybersecurity, K-5 Education, Gamified Learning, Digital Literacy, Teacher Training, Usability Testing

ISSN: 2473-4901
v11 n6383

Beyond Awareness: Building Digital Resilience Through Comprehensive Cybersecurity Foundations for K-5 Students

Ellie Ebrahimi, Leo Gokce, Marjorie Pare, Jude Vargas, and Jacob Blount

1. INTRODUCTION

In an increasingly digital world, equipping young children with foundational cybersecurity knowledge and digital literacy skills is essential. Just as children learn to safely navigate physical environments, they must also learn to navigate the online world securely. The widespread engagement of K-5 students with online platforms, social media, and gaming exposes them to various risks, including cyberbullying, online predators, privacy breaches, and scams. Despite this heightened digital immersion, there remains a critical lack of foundational cybersecurity education for this age group, leading to a dangerous knowledge gap.

Cybersecurity Practice & Awareness for Rising Kids (Cyber-PARK) addresses this urgent need by providing a browser-based, gamified learning platform designed to instill essential cybersecurity knowledge and digital literacy in K-5 students. This initiative is crucial not only for protecting children from immediate online dangers but also for cultivating critical thinking skills, fostering responsible online behavior, and building an early pipeline for the rapidly growing cybersecurity workforce, thereby mitigating a significant national shortage. Additionally, early exposure to cybersecurity concepts can spark interest in STEM fields, opening doors to future technical careers and developing valuable problem-solving and analytical skills.

The Cyber-PARK education kit is designed with North Carolina Computer Science standards, NC Digital Learning Plan Initiatives, and industry certifications in mind. It aims to streamline the educational experience for teachers and parents by offering a single, comprehensive resource that includes classroom course material, interactive games, and a website for monitoring student progress. The curriculum covers vital topics such as data privacy, internet safety, and digital footprints, with each module aligning with NC K-12 computer Science standards (See Appendix A). The accompanying website serves as a knowledge hub, allowing parents and teachers to track student progress through carefully designed modules.

The current landscape of cybersecurity education for elementary schools faces several challenges:

- **Curriculum Priorities:** Schools often prioritize core subjects, viewing cybersecurity as secondary rather than essential.
- **Lack of Teacher Training:** Many educators lack the necessary cybersecurity knowledge or training, hindering effective instruction.
- **Limited Resources & Funding:** Budget constraints can prevent schools from investing in cybersecurity programs, software, or professional development.
- **Lack of Standardization:** Unlike established subjects, cybersecurity education lacks a widely accepted, standardized curriculum, leading to inconsistencies across schools.
- **Rapidly Evolving Threats:** The dynamic nature of cyber threats makes it challenging for educational materials to remain current.
- **Parental & Administrative Awareness:** A lack of full understanding regarding the importance of early cybersecurity education can lead to insufficient demand and support.

By equipping students with crucial online safety skills, Cyber-PARK helps bridge the digital divide, granting young students and their families greater access to valuable online resources and future employment opportunities. This initiative delivers significant societal benefits by reducing vulnerability to cyber threats while fostering digital inclusion. This paper will elaborate on the Cyber-PARK curriculum and present the empirical findings from usability testing conducted with students, teachers, and cybersecurity experts, providing insights into the effectiveness and relevance of the current approach.

2. LITERATURE REVIEW

Improving STEM (Science, Technology, Engineering, and Mathematics) skills is a current and future imperative for addressing the complex social and economic challenges society faces (English, 2016). STEM education is not merely about preparing students for specific technical careers; it is fundamentally about cultivating essential problem-solving, analytical, and critical thinking skills that are vital for success across all career paths and in daily life (National Research

Council, 2012). The urgency of this goal is highlighted by existing and projected shortages in the STEM workforce (Hopkins et al., 2014; Charette, 2015). The Committee on STEM Education of the National Science and Technology Council emphasizes that STEM competencies are crucial for overall life success, extending far beyond traditional STEM professions (Maclsaac, 2019).

A highly effective pedagogical approach for fostering these critical skills is Problem-Based Learning (PBL). Grounded in situated cognition theory, which posits that "knowing is doing" and that knowledge application is intrinsically linked to its context (Brown et al., 1989; Putnam and Borko, 2000), PBL requires students to engage with realistic problems. This methodology empowers students to take control of their learning, utilizing teachers as inquiry coaches while working collaboratively. PBL has consistently yielded positive outcomes for students in areas such as collaboration (Boaler, 2003; Penuel, 2006), student engagement (Belland et al., 2006; Brush and Saye, 2008), and crucially, the development of critical thinking and problem-solving skills (Mergendoller and Thomas, 2005). Research indicates that PBL can significantly increase long-term knowledge retention and improve both test scores and overall problem-solving abilities. Furthermore, PBL offers valuable learning scaffolds that enrich inquiry and enhance student engagement, making it an ideal framework for developing the foundational cognitive skills necessary for navigating complex fields like cybersecurity.

The Imperative of Early Cybersecurity Education

The importance of K-12 cybersecurity education cannot be overstated in today's digitally driven world. Children are increasingly engaged in online activities through school, social media, and gaming platforms, often from a very young age (Anderson and Juang, 2018). This pervasive digital immersion, while offering numerous benefits, also exposes them to a growing array of potential threats, including phishing scams, online predators, and privacy breaches. Cybersecurity education is therefore crucial for helping them identify and avoid these dangers (Quayyum et al., 2021). Teaching children to protect their personal information, such as names, addresses, and locations, is vital for preventing identity theft and reducing the risks of cyberbullying. Moreover, cybersecurity education fosters digital literacy, enabling children to comprehend the broader digital environment, including ethical technology use and the ramifications of their online actions.

Despite this critical need, there remains a noticeable scarcity of cybersecurity curricula specifically designed for students in grades K-5, largely due to perceptions about their developing computer skills and knowledge (Zepf and Arthur, 2013). However, early childhood is widely considered an optimal time for learning, suggesting that introducing cybersecurity or digital literacy in elementary schools could create significantly greater opportunities for future careers and safer digital habits. It is imperative to offer early exposure to cybersecurity principles to protect young children from "negative experiences" (Giannakas et al., 2019; National Science Foundation, 2020; Zepf and Arthur, 2013). Such early curricula can enhance student awareness of cyberattack dangers while proactively introducing them to cybersecurity-related topics before they encounter more complex threats.

Focusing on the grades K-5 demographic also allows researchers to mitigate developmental, behavioral, and technology-access issues often associated with older students. This early intervention provides a crucial opportunity to longitudinally assess the long-term impact of training on students' perceptions of cybersecurity as they reach middle school and beyond. Research indicates that students in middle and high school grades often begin to perceive their academic ability as a "fixed quality," which can lead them to withdraw from subjects where they lack confidence (Jethwani et al., 2016; Rhodewalt and Tragakis, 2002) or a sense of belonging (Jethwani et al., 2017; Margolis and Fisher, 2002). Introducing cybersecurity concepts at an earlier, more malleable stage can prevent these issues, fostering a positive disposition towards the field.

Designing Effective Curricula: Embracing Diverse Learning Styles and Methodologies

Effective teaching and learning are inherently intertwined, with learning occurring most naturally when instruction is optimal and aligns with the diverse learning styles of the learners (Proserpio and Gioia, 2007). Educators teaching the "virtual generation," who are native to digital environments, must leverage new technologies, such as internet-based tools and games, to increase participation and achieve learning objectives (Ambrose et al., 2010). Research has consistently demonstrated that virtual technologies can significantly enhance student

performance (Scoville and Buskirk, 2007; Han, 2020).

Consequently, game-based technology and strategies have gained substantial momentum in educational settings and have been shown to increase knowledge retention (Putz et al., 2020; Ortiz-Rojas et al., 2019; Kim et al., 2018). With game-based technologies, students can visualize abstract concepts and perform hands-on tasks, moving beyond mere imagination (Trindade et al., 2002; Christou, 2010). A growing body of research suggests that when students interact with and control events within extended reality environments, they become more actively involved in constructing knowledge through immersive experiences, as opposed to passive learning methods like lectures or reading (Roussou, 2004; Dewey, 2004). This active engagement is particularly vital for complex and abstract topics like cybersecurity, where practical application and experiential learning can solidify understanding.

Moreover, disparities in science education, particularly in rural, low-income areas, can exacerbate student engagement issues, especially for those with diverse learning needs. Traditional textbook-lecture formats often involve substantial independent analysis of expository writing and worksheet activities, which can be challenging for students rapidly introduced to new theories, facts, and vocabulary in an inconsistent manner. Many general education teachers also lack adequate training or experience in accommodating students with special needs. The proper integration of diverse technologies and pedagogical approaches, such as game-based learning and problem-based learning, into the curriculum has been shown to effectively overcome some of these obstacles, making education more accessible and engaging for all students.

Cybersecurity Education as a Pathway to Future Workforce Development

Cybersecurity workforce development is not merely an academic concern but a critical national and global need for addressing pressing societal, social, and economic challenges. Improving STEM skills is a current and future imperative (English, 2016), and the urgency of this goal is highlighted by existing and projected shortages in the STEM workforce (Hopkins et al., 2014; Charette, 2015). The cybersecurity sector, in particular, faces a severe talent gap, with hundreds of thousands of open positions globally (ISC2 Cybersecurity Workforce Study, 2023). This shortage poses significant risks to national security, economic stability, and individual privacy.

The Committee on STEM Education of the National Science and Technology Council emphasizes that STEM skills are vital not only for specialized STEM careers but for all career paths, as they contribute to overall life success (Maclsaac, 2019). Therefore, early exposure to cybersecurity education serves a dual purpose: it protects young individuals in their digital lives today and simultaneously cultivates the foundational knowledge and interest necessary to build the cybersecurity workforce of tomorrow. By introducing cybersecurity concepts at the elementary level, we can spark curiosity, demystify the field, and encourage a diverse range of students to consider careers in this critical domain. This proactive approach to education is essential for creating a robust pipeline of skilled professionals, addressing the current workforce deficit, and ensuring a more secure digital future for all.

3. CURRENT CYBERSECURITY EDUCATION SOLUTIONS

The critical need for early cybersecurity education for K-5 students is underscored by their increasing digital engagement and the prevalent online threats they face. Despite this growing exposure, current educational approaches largely fall into two categories: passive learning (e.g., videos, lectures) and active/gamified learning. While passive methods efficiently deliver foundational knowledge, they often lack the interactivity crucial for sustained engagement and deep comprehension in young learners. For instance, platforms like Tynker offer cybersecurity curriculum through videos and quizzes, but these often lack the interactive experiences necessary to solidify understanding. Similarly, Trend Micro Cyber Academy and MalwareBytes provide information-rich videos, yet they frequently lack interaction, may lose viewer attention, and crucially, do not provide opportunities for assessing knowledge retention without supplemental materials.

Existing active learning resources, though generally more engaging, often prove too complex or text-heavy for elementary students, or they do not offer comprehensive, measurable learning outcomes. For example, the PBS NOVA Labs - Cybersecurity Lab game, while interactive, requires lengthy tutorial and extensive reading, which can deter younger users. Cyber Sprinters also teaches through interactive elements but relies heavily on text and does not allow for active

practice of real-world techniques. Even resources from the Center for Development of Security Excellence, which include word searches, are often geared towards an adult audience and can be overly text dependent. Furthermore, a common deficiency across many existing activities is the absence of formal knowledge assessment, leaving educators and parents without clear indicators of a child's understanding and ability to apply the material. This collective absence of age-appropriate, truly interactive content, combined with a lack of measurable learning outcomes, highlights a significant and critical gap in effectively designed cybersecurity education activities for young audiences.

The Cyber-PARK project directly addresses these limitations. By developing a curriculum that integrates hands-on activities with gamified learning experiences (e.g., Password Chef, Two-Step Treasures, Potion Post), Cyber-PARK provides simplified, experiential learning opportunities. The Cyber-Park methodology prioritizes active participation and immediate feedback to enhance engagement and comprehension. Furthermore, the inclusion of built-in assessment mechanisms within the games and activities provides clear indicators of student understanding, a crucial feature often missing in current offerings. This approach ensures that Cyber-PARK not only introduces essential cybersecurity principles but also fosters digital resilience through practical application and measurable learning outcomes, effectively bridging the identified gaps in early cybersecurity education.

4. THE CYBER-PARK CURRICULUM

The Cyber-PARK curriculum is designed to provide K-5 students with essential cybersecurity knowledge and digital literacy through a structured, standards-aligned learning journey. It is built around four comprehensive modules, each comprising four dynamic lessons. These modules are equipped with clear objectives, relevant vocabulary, and hands-on materials included in the starter kits, providing educators with everything they need to deliver engaging instruction. Educators set up their classrooms by grade level, which automatically populates age-appropriate content. Although the core lessons are often consistent across all age groups, they are differentiated by adjusting the content's complexity, activities, and assessment methods. The lessons are designed to last at most 30 minutes for one lesson per week.

Here is a detailed breakdown of the Cyber-PARK modules and their respective lessons:

- *Module 1: Digital Foundations*
  - Devices: Students learn to understand basic digital elements.
  - Network & Internet: Introduces how various digital components connect.
  - Accounts & Passwords: Covers fundamental security concepts related to accounts and passwords.
  - Digital Footprints: Explores what information we leave behind online.

- *Module 2: Online Protections*
  - Password Building: Teaches strategies for creating strong, memorable passwords.
  - Social Etiquette: Focuses on positive online interactions.
  - Malicious Actors: Helps students understand who poses threats online.
  - Password Cracking (Basics): Demonstrates how weak passwords are vulnerable.

- *Module 3: Threat Identification*
  - Multi-Factor Authentication (MFA): Explains how to add layers of security to accounts.
  - Phishing: Teaches students to identify online scams.
  - Catching Misinformation: Focuses on critical evaluation of online content.
  - Cyberbullying: Covers identifying and reporting cyberbullying.

- *Module 4: Future & Responsibility*
  - How Technology Evolves: An introduction to concepts like Deepfakes & AI.
  - Careers in Cybersecurity: Explores pathways for future professionals in the cybersecurity field.
  - Safety in Numbers & Responsible Digital Citizenship: Emphasizes responsible online behavior.
  - Maintaining Digital Habits: Focuses on lifelong online safety practices.

Figure 1: Starter kit for in-class activities. The

ISSN: 2473-4901
v11 n6383

sharpie shows the relative size of the objects in the kit.

Each module utilizes specially designed starter kit to empower teachers with tangible tools. These kits include (Figure 1):

- 3D Printed Items: Physical models, such as device components, for tactile engagement.
- Multi-Purpose Cards: Versatile cards for activities like password creation, network simulations, and scenario role-playing.

Current Games in Cyber-PARK

The browser-based game platform, Cyber-PARK, is actively under development to provide K-5 students with essential cybersecurity knowledge, skills, and abilities through engaging, age-appropriate activities. It currently includes several proof-of-concept games covering topics such as two-factor authentication (2FA), strong password creation, social engineering, phishing, encryption, and malware injections. The platform is designed to be an engaging and immersive learning environment, allowing for the collection and storage of relevant data to track student progress and performance. The games are integrated into a large, interactive map where each section represents a unique themed area. Students navigate this map as caretakers or explorers, engaging with diverse challenges and objectives. Completing modules unlock virtual rewards like pets, tools, or resources specific to the map area. The modules combine problem-solving, critical thinking, and subject-specific skills, and students can personalize their rewards and map areas. Collaboration can also be incorporated to unlock special regions or solve larger challenges.

Currently, three games, Password Chef, Two-Step Treasures, and Potion Post, have been functionally tested by adult and student volunteers, and their design and performance are continuously being refined. The knowledge assessment components have been refined to measure the effectiveness of these games in conveying cybersecurity concepts.

Password Chef: Password Chef is a 2D point-and-click game designed to teach players about creating secure passwords by likening the process to cooking in a restaurant (Figure 2). Players create and memorize unique "dishes" (passwords) by combining virtual ingredients: vegetables (uppercase/lowercase letters), meats (numbers), and spices (special characters). The game requires players to meet specific criteria for password complexity and rewards them based on the strength of their creations. In later stages, players must recall previously created "dishes" for repeat customers, reinforcing memory and retention of strong password practices. This game assesses password growth and recalls overtime. The game provides simple touch controls, making it accessible even for players unfamiliar with games. The narrative encourages players to create memorable and secret "recipes" to prevent other "chefs" from guessing them. Challenges progressively increase in complexity, requiring specific character types or minimum lengths. The

Figure 2: Password Chef is a 2D point-and-click game that encourages learners to develop their password safety skills through cooking.

focus is on rewarding successes, empowering players. Password Chef is built using Unity Game Engine and can be deployed as a WebGL or desktop application (See Appendix A – Modules 1 and 2).

Two-Step Treasures: Two-Step Treasures is a 2D point-and-click game that introduces players to the concept of multi-factor authentication (MFA) (Figure 3). Initially, players learn about single authentication factors by creating simple image-based passwords related to personal preferences (e.g., favorite color, animal, or shape). Jigsaw pieces representing these factors are used to unlock treasure chests. After each successful attempt, tooltips provide information about authentication methods, preparing players for subsequent sections. Quiz questions about authentication factor facts are administered at the end of each stage to assess understanding.

As players advance, they are introduced to various authentication methods, including fingerprint scanners, one-time passwords, and facial recognition technology. Unlocking treasure chests then requires multiple jigsaw pieces, combining knowledge factors with possession or inheritance factors. For instance, players might

ISSN: 2473-4901
v11 n6383

use a fingerprint to unlock a device to retrieve a second key or use facial recognition for identity verification. The game progressively increases the complexity of authentication methods and quiz questions. Player assessment is based on quiz results and stage completion. This game is built using Unity Game Engine which aims to introduce 2FA in an easy-to-understand format, without time restrictions or consequences for incorrect guesses, allowing for experimentation and understanding of its protective benefits (See Appendix A – Module 3).

Figure 3: Learners will practice one-step authentication, and then, they will be introduced to two-step authentication.

Potion Post: Potion Post is a 2D educational game focused on teaching players to identify common internet scams, such as prize scams, phishing scams, and pyramid schemes (Figure 4). The game presents text-based interactions within the context of a small shop. Players respond to messages by stamping them green for legitimate or red for scams, while also providing requested items or information. Correctly identifying scams rewards players with virtual currency, while incorrect decisions result in financial losses, or loss of items, reinforcing the consequences of falling for scams. The game is broken into three stages, each introducing a new type of scam with progressively harder goals and more messages. Data collected includes click locations, time per stage, time per message, total game time, game score, game goal, and the proportion of messages correctly or incorrectly identified. This data is communicated to the server via HTTPS request. Built in Godot Engine, it can be deployed as a WebGL or desktop application. This design allows players to be entertained and challenged while developing their understanding of scam awareness, connecting their in-game actions to real-world impacts (See Appendix A – Module 3).

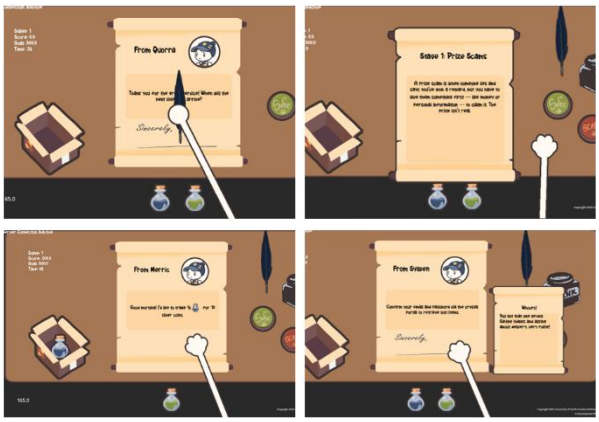

Figure 4: Potion Post allows players to practice identifying scams as potion merchants.

5. METHODOLOGY

To ensure the effectiveness and age appropriateness of the Cyber-PARK curriculum and its interactive components, three sets of usability testing and consultations with distinct target audiences and expert groups has been conducted. This empirical evaluation provided rich qualitative data to refine the materials. This study has been approved by the Institutional Review Board (IRB #03072025) of the University of North Carolina Wilmington. The evaluation involved the following groups:

- Students:
  - Two summer camp groups (25 and 31 students, ages 8-11).
  - 18 individual K-5 students from various grade levels.
  - 5 high school students (to gather general feedback on content and identify areas for additional K-5 content).
- Teachers:
  - 15 K-5 STEM/Technology/Media teachers.
- Cybersecurity Experts:
  - Over 20 experts, including university professors, researchers, and industry/IT

ISSN: 2473-4901
v11 n6383

Question	Pre-test Responses (N=20)	Post-test Responses (N=16)	Key Improvement
Q1: Familiarity	60% "No/IDK"	62.5% "Yes"	Significant increase in familiarity with the terms.
Q2: Two-Step Purpose	Vague, "extra safety"	More detailed, "harder for hackers", "proves it's you"	Better understanding of the mechanism of security.
Q3: Fingerprint vs. Password	Highlighted "uniqueness"	Repeated the same point, more confidently, and added that passwords can be "copied" or "repeated"	Reinforced understanding of why biometrics are more secure.
Q4: Examples of Factors	Limited examples (phone number, face ID)	Expanded examples across multiple factor types (know, have, are)	Broader and more comprehensive knowledge of security methods.

Table 1: Student improvement analysis on multifactor authentication

security professionals.

The testing protocol varied slightly for each group to best gather relevant feedback:

Student Testing: Students at the summer camps engaged in specific lessons, including those on devices, networks, and multi-factor authentication exercises. Their engagement was observed during PowerPoint presentations and hands-on activities. Pre- and post-assessments were administered to measure their comprehension. Individual K-5 students and high school students provided direct feedback on the age-appropriateness and relevance of the content.

Teacher Testing: Teachers participated in smaller groups. They reviewed PowerPoint presentations for each lesson, simulated student roles in hands-on activities, and examined activity sheets and assessment worksheets for feasibility across different K-5 age groups. Their feedback was crucial for identifying practical usability issues.

Cybersecurity Expert: Experts provided feedback on the overall curriculum content, material accuracy, and the importance of various concepts. They also advised on the modality for teacher and student training, emphasizing the broader goal of workforce development starting at the elementary school level.

6. RESULTS

Student Feedback: The two summer camps (grades 4 and 5) provided invaluable data on the lessons provided and step-by-step activities. Students were highly engaged during the PowerPoint presentations, actively participating in discussions and responding well to prompt questions. Their curiosity and engagement were evident through the insightful talking points and questions they raised. For the hands-on activities, students demonstrated significant enthusiasm, moving around and actively participating, a stark contrast to passively listening to instructions. They explicitly stated that "doing it" helped them understand the concepts better, indicating a strong preference for active learning. Pre- and post-assessments consistently showed improved comprehension of the concepts after the combination of PowerPoint presentations and group activities. The overall level of engagement was significantly higher during the interactive group activities (see table 1). For example, the data from the lesson on MFA suggests an overall improvement in the students' understanding of multifactor authentication, particularly in their ability to define and provide examples of different authentication factors. In the pre-test, many students were unfamiliar with terms like "two-step verification" or "multi-factor authentication," with 12 out of 20 saying they had never heard of them. However, in the post-test, a majority of students (10 out of 16) responded "yes" when asked if they knew the terms. This indicates a significant increase in their familiarity. Students also demonstrated a better grasp of the purpose and mechanics of these security measures. In the pre-test, responses to why two-step verification is used were often vague, mentioning general concepts like "extra security" or to ensure it's "the right person". By the post-test, their answers were more specific, explaining that it makes it harder for hackers to get in because they would need "two passwords" or the code from a

ISSN: 2473-4901
v11 n6383

"connected device". Furthermore, their ability to name different types of security factors expanded. Initially, examples were limited to passwords, phone numbers, and codes. In the later test, students provided a wider range of examples, including facial recognition, fingerprints, PIN numbers, and email, showing they now understood a broader spectrum of authentication methods (See table 1 for more information).

All students in the K-5 group tested the Password Chef game, and their passwords became significantly longer and stronger with variety of characters after only three attempts. In the next stage of the game, students will practice techniques to remember their passwords. Two-Step Treasure helped students to learn what the three factors are and identify them correctly after interacting with the game for an average of 30 minutes. Potion Post game only has been tested for its usability and game mechanics.

Teacher Feedback: The teacher groups were run in smaller sessions, which allowed for immediate feedback integration and content modification. This iterative, teacher-centered design process proved highly effective. Teachers identified several areas for improvement in the curriculum, including:

- **Age-Appropriate Language**: Adjusting vocabulary and phrasing to better suit different K-5 grade levels.
- **Missing Steps in Activities**: Clarifying instructions for activities, as some initial assumptions about teacher actions needed explicit detailing.
- **Typos and Errors**: Correcting minor errors in the materials.
- **Difficulty Level Adjustment**: Reallocating certain content between different grade levels based on observed difficulty.
- **Online Assessment**: Providing an option for online assessments instead of paper version for different lessons.
- **Internet Safety Standards**: Mapping the standards to the ISTE Computer Science and Cybersecurity standards instead of one state.

After each round of testing, the curriculum was promptly modified, and the revised content was then tested with the subsequent teacher group. This iterative refinement process ensured that the materials were highly usable and practical for classroom implementation by teachers.

Cybersecurity Expert Consultation: The consultations with over 20 cybersecurity experts, encompassing university professors, researchers, and industry/IT security professionals, validated the critical need for cybersecurity education at the K-5 level. Experts provided comprehensive feedback on the curriculum's content, emphasizing the importance of including foundational concepts and identifying key areas for future workforce development that should begin in elementary schools. Their insights were instrumental in shaping the overall materials for both students and teachers, ensuring the curriculum's relevance and alignment with current industry needs and future trends. They also provided guidance on effective modalities for delivering training to both teachers and students.

7. DISCUSSION

The empirical evaluations of the Cyber-PARK initiative, involving K-5 students, teachers, and cybersecurity experts, strongly demonstrates its efficacy and critical importance. Student responses highlighted the power of gamified and hands-on learning, with pre- and post-assessments confirming improved comprehension, aligning with the "knowing is doing" principle of situated cognition theory.

The iterative design process, heavily informed by K-5 teacher feedback, was crucial for developing a practical and user-friendly curriculum. This teacher-centered approach allowed for immediate adjustments to language, activity instructions, and content difficulty, ensuring the materials are highly usable and address the challenge of limited teacher training in cybersecurity.

Furthermore, strong endorsement from academic and industry cybersecurity experts validated the curriculum's content and its alignment with broader cybersecurity workforce development goals. Their input ensures Cyber-PARK is academically sound and relevant, contributing significantly to building a skilled talent pipeline by starting education at the elementary level.

Unlike many current passive or overly complex cybersecurity education offerings for young children, Cyber-PARK stands out by actively integrating gamified learning with comprehensive, standards-aligned content and built-in assessment opportunities. Detailed data from games like Potion Post, Password Chef, and Two-Step Treasures provides measurable outcomes, addressing a significant limitation in existing programs. Ultimately, Cyber-PARK directly combats educational inequality and promotes digital inclusion, fostering responsible digital citizenship and reducing vulnerability to

cyber threats on a societal scale.

8. CONCLUSIONS

Cybersecurity education is indispensable for empowering young learners to navigate the digital world safely and responsibly. The Cyber-PARK project directly addresses this need by providing an innovative, empirically validated platform for K-5 students, teachers, and parents. By reducing children's vulnerability to online threats such as fraud, scams, and identity theft, early cybersecurity education fosters a generation of informed and cautious digital citizens.

Through the development and refinement of engaging, interactive games and a comprehensive curriculum, we aim to make learning these critical concepts both accessible and enjoyable. The positive feedback and demonstrated comprehension from students, the iterative refinement based on teacher insights, and the expert validation of the content collectively affirm the strength and relevance of the Cyber-PARK approach. By combining research-driven educational methods with hands-on experiences, we strive to create a lasting impact, empowering children to build safe digital habits that will benefit them throughout their lives.

9. FUTURE WORK

The Cyber-PARK project is being piloted in New Hanover County public elementary schools. This large-scale pilot will provide a rich, longitudinal database encompassing all activities and content within the curriculum. This includes detailed data on PowerPoint presentations used by educators, in-class activities, student engagement with video games, assessment sheets, and take-home exercises. This extensive data collection will allow for a more robust empirical analysis of the curriculum's long-term impact on student learning, behavior, and interest in cybersecurity. The future work will focus on:

- *Longitudinal Impact Assessment:* Analyzing the data from the pilot program to understand the sustained effects of Cyber-PARK on students' cybersecurity knowledge, attitudes, and behaviors over time.
- *Curriculum Expansion and Refinement:* Continuously developing new interactive games and learning modules based on evolving cyber threats and educational needs, while further refining existing content through ongoing feedback loops.
- *Teacher Training and Support:* Developing scalable teacher training programs and support resources to facilitate widespread adoption and effective implementation of the Cyber-PARK curriculum.
- Integration with Existing Educational Frameworks: Ensuring seamless integration of Cyber-PARK with existing school curricula and educational technology infrastructures.
- Age-Related Content: Revisiting the lessons and student's activities and reevaluating their age appropriateness.

Through these ongoing efforts to establish Cyber-PARK as a leading solution for early cybersecurity education, contributing significantly to a more cyber-resilient and digitally literate future generation.

11. REFERENCES

Ambrose, S. A., Bridges, M. W., DiPietro, M., Lovett, M. C., & Norman, M. K. (2010). *How learning works: Seven research-based principles for smart teaching*. John Wiley & Sons.

Anderson, M., & Jiang, J. (2018). Teens, social media & technology 2018. *Pew research center*, *31*(2018), 1673-1689.

Belland, B. R., Ertmer, P. A., & Simons, K. D. (2006). Perceptions of the value of problem-based learning among students with special needs and their teachers. *Interdisciplinary Journal of Problem-Based Learning*, *1*(2), 1-18.https://doi.org/10.7771/1541-5015.1024

Boaler, J. (2003). Setting, social class and survival of the quickest. In *Mathematics Education* (pp. 205-228). Routledge. https://doi.org/10.4324/9780203465394

Brown, J. S., Collins, A., & Duguid, P. (1989). Situated cognition and the culture of learning. *1989*, *18*(1), 32-42.

Brush, T., & Saye, J. (2008). The effects of multimedia-supported problem-based inquiry on student engagement, empathy, and assumptions about history. *Interdisciplinary Journal of Problem-Based Learning*, *2*(1), 21-56.https://doi.org/10.7771/1541-5015.1052

Charette, R. N. (2015). STEM Sense and Nonsense. *Educational Leadership*, *72*(4), 79-83.

Christou, C. (2010). Virtual reality in education. In Affective, interactive and cognitive methods for e-learning design: creating an optimal education experience (pp. 228-243).

IGI Global Scientific Publishing. 10.4018/978-1-60566-940-3.ch012

Dewey, J. (2024). Democracy and education. Columbia University Press. https://doi.org/10.7312/dewe21010-003

English, L. D. (2016). STEM education K-12: Perspectives on integration. *International Journal of STEM education*, *3*(1), 3. https://doi.org/10.1186/s40594-016-0036-1

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. Information Security Journal: A Global Perspective, 28(3):81–106. https://doi.org/10.1080/19393555.2019.1657527

Han, I. (2020). Immersive virtual field trips in education: A mixed-methods study on elementary students' presence and perceived learning. British Journal of Educational Technology, 51(2), 420-435. https://doi.org/10.1111/bjet.12842

Hopkins, S., Forgasz, H., Corrigan, D., & Panizzon, D. (2014). The STEM issue in Australia: What it is and where is the evidence. In *STEM Conference. Vancouver, Canada (http://stem2014.ubc.ca)*

ISC2 Cybersecurity Workforce Study (2023). How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, https://cybergovernancealliance.org/wp-content/uploads/2024/01/ISC2_Cybersecurity_Workforce_Study_2023-1.pdf

Jethwani, M., Memon, N., Richer, A., and Seo, W. (2016). It's hard to be the only girl: Obstacles facing adolescent girls in computer science contexts. In Journal of The Colloquium for Information System Security Education, volume 4, pages 16–16. https://cisse.info/journal/index.php/cisse/article/view/52

Jethwani, M. M., Memon, N., Seo, W., and Richer, A. (2017). "I can actually be a super sleuth" promising practices for engaging adolescent girls in cybersecurity education. Journal of Educational Computing Research, 55(1):3–25. https://doi.org/10.1177/0735633116651971

Kim, S., Song, K., Lockee, B., & Burton, J. (2017). What is gamification in learning and education? In *Gamification in learning and education: Enjoy learning like gaming* (pp. 25-38). Cham: Springer International Publishing.

Margolis, J. and Fisher, A. (2002). Unlocking the clubhouse: Women in computing. MIT press.

MacIsaac, D. (Ed.). (2019). US government releases charting a course for success: America's strategy for STEM education, report guiding federal agencies that offer STEM funding opportunities. The Physics Teacher, 57(2), 126-126. https://doi.org/10.1119/1.5088484

Mergendoller, J. R., & Thomas, J. W. (2005). Managing project based learning: Principles from the field. *Retrieved June 14*, 2005.

National Research Council, Division of Behavioral, Social Sciences, Board on Science Education, & Committee on a Conceptual Framework for New K-12 Science Education Standards. (2012). *A framework for K-12 science education: Practices, crosscutting concepts, and core ideas*. National Academies Press.

National Science Foundation (2020). Cybersecurity education in the age of artificial intelligence. https://www.nsf.gov/pubs/2020/nsf20072/nsf20072.jsp.

Ortiz-Rojas, M., Chiluiza, K., & Valcke, M. (2019). Gamification through leaderboards: An empirical study in engineering education. *Computer Applications in Engineering Education*, *27*(4), 777-788. https://doi.org/10.1002/cae.12116

Penuel, W. R. (2006). Implementation and effects of one-to-one computing initiatives: A research synthesis. *Journal of research on technology in education*, *38*(3), 329-348. https://doi.org/10.1080/15391523.2006.10782463

Proserpio, L., & Gioia, D. A. (2007). Teaching the virtual generation. *Academy of Management Learning & Education*, *6*(1), 69-80. https://doi.org/10.5465/amle.2007.24401703

Putz, L.-M., Hofbauer, F., and Treiblmaier, H. (2020). Can gamification help to improve education? Findings from a longitudinal study. Computers in Human Behavior, page 106392. https://doi.org/10.1016/j.chb.2020.106392

ISSN: 2473-4901
v11 n6383

Putnam, R. T., & Borko, H. (2000). What do new views of knowledge and thinking have to say about research on teacher learning?. *Educational researcher*, *29*(1), 4-15. https://doi.org/10.3102/0013189X029001004

Quayyum, F., Cruzes, D. S., and Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, Volume 30:100343. https://doi.org/10.1016/j.ijcci.2021.100343

Rhodewalt, F., & Tragakis, M. W. (2014). Self-handicapping and the social self: The cost and rewards of interpersonal self-construction. In *The Social Self* (pp. 121-140). Psychology Press.

Roussou, M. (2004). Learning by doing and learning through play: an exploration of interactivity in virtual environments for children. Computers in Entertainment (CIE), 2(1), 10-10. https://doi.org/10.1145/973801.973818

Scoville, S. A., & Buskirk, T. D. (2007). Traditional and virtual microscopy compared experimentally in a classroom setting. *Clinical Anatomy: The Official Journal of the American Association of Clinical Anatomists and the British Association of Clinical Anatomists*, *20*(5), 565-570. https://doi.org/10.1002/ca.20440

Trindade, J., Fiolhais, C., & Almeida, L. (2002). Science learning in virtual environments: a descriptive study. British Journal of Educational Technology, 33(4), 471-488. https://doi.org/10.1111/1467-8535.00283

Zepf, I. and Arthur, L. (2013). Cyber-security curricula for basic users. Technical report, Naval Postgraduate School Monterey CA.

ISSN: 2473-4901
v11 n6383

Appendix A

Module 1: Digital Foundations

- ***Devices:*** Understand basic digital elements.
- ***Network & Internet:*** How things connect.
- ***Accounts & Passwords:*** Basic security concepts.
- ***Digital Footprints:*** What we leave behind online.

NC K-12 Computer Science Standards

- **K2-NI-01:** Illustrate how information is broken down into smaller pieces and can be reassembled.
- **K2-NI-02:** Apply knowledge of what passwords are and why we use strong passwords to protect devices and information from unauthorized access.
- **K2-NI-03:** Discover and understand what a digital footprint is, and how information can be obtained and protected.
- **K2-IC-04:** Model responsible login and logoff procedures on all devices
- **68-IC-09:** Compare tradeoffs between allowing information to be public and keeping information private and secure.

Computing Device	**K2-NI-02, K2-DA-02**: Physical items that use hardware and software to receive, process, and output information. Computing, inputting, networking, and peripheral are all examples of devices.
USB	A standard interface for connecting cables to PCs and consumer electronics devices. Users can connect a specially designed wire called the USB cable. USB cables may transmit both power and information
HDMI	A connection used for displaying digital video and audio from a source, such as a computer or TV, to a computer monitor, TV or projector.
Bluetooth	a short-range wireless connection of mobile phones, computers, and other electronic devices to exchange data.
Cell Tower	Cell towers are structures that house the equipment necessary for wireless communication between phones that allow us to make calls, exchange text messages, and access the internet on mobile devices.
Wifi and Hotspots	a wireless networking technology that uses radio waves to provide wireless high-speed Internet access.
Internet	**35-NI-01**: The large system of connected devices around the world that allows people to share information and communicate with each other.
Network	**35-NI-01, ICS-NI-01:** A collection of computers that are connected together so that they can share information.
Router	**ICS-NI-01:** A router is a unique electronic device that allows the network to be shared with people in a small area.

ISSN: 2473-4901
v11 n6383

Browser	A browser is an application on a device that connects to the internet and allows you to view and interact with the information on it.
Account	A user's access to a specific Internet platform. An account contains a variety of personal and private information used to interact with others online.
Password	**K2-NI-02**: A string of characters used for authenticating a user on a computer system. Most passwords are comprised of several characters, which can typically include letters, numbers, and most symbols, but not spaces.
Digital Footprint	**K2-NI-03, 35-NI-02:** A trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services. A "passive digital footprint" is a data trail you unintentionally leave online. (example IP address, browsing history, ...) An "active digital footprint" includes data that you intentionally submit online. (example email, social media post, ...)
Digital Citizenship	**35-IC-04:** The norms of appropriate, responsible behavior with regard to the use of technology. Digital citizenship topics include instruction on media balance, privacy and security, cyberbullying, news and media literacy, and digital identity and footprint.

Module 2: Online Protections

- ***Password Building:*** Strategies for strong, memorable passwords.
- ***Social Etiquette:*** Positive online interactions.
- ***Malicious Actors:*** Understanding who poses threats.
- ***Password Cracking (Basics):*** How weak passwords are vulnerable.

NC K-12 Computer Science Standards

- **68-NI-02:** Explain how physical and digital security measures protect electronic information
- **68-NI-03:** Explain permission and authorizations to access resources to computer systems online
- **K2-IC-03**: Work respectfully and responsibly with others online
- **35-IC-04:** Exhibit positive digital citizenship and social responsibility in online interactions
- **ICS-NI-02:** Identify examples to illustrate how sensitive data can be affected by malware and other attacks.

ISSN: 2473-4901
v11 n6383

Digital Citizenship	**35-IC-04:** The norms of appropriate, responsible behavior with regard to the use of technology. Digital citizenship topics include instruction on media balance, privacy and security, cyberbullying, news and media literacy, and digital identity and footprint.
Password Cracking	The process of guessing passwords protecting a computer system or account. Generally done through brute-force.
Netiquette	A set of guidelines in online communication that help to ensure positive interactions.
Malicious Actors	a person or a group of people that take part in an action that is intended to cause harm to the individuals or companies using: computers, devices, systems, or networks
Password	**K2-NI-02**: A string of characters used for authenticating a user on a computer system. Most passwords are comprised of several characters, which can typically include letters, numbers, and most symbols, but not spaces.
Netiquette	The set of rules and behaviors that people are expected to use when interacting with others on the internet.
Phishing	The practice of sending fraudulent communications that appear to come from a legitimate and reputable source, usually through email and text messaging.
Malware Ads	The use of malicious code in online ads and popups to spread malware or steal information. Scammers use them as a covert tactic to spread dangerous code across multiple websites.
Social Engineering	The tactic of manipulating, influencing, or deceiving someone to gain control over a computer system or to steal personal and financial information.

Module 3: Threat Identification

- ***Multi-Factor Authentication (MFA):*** Adding layers of security.
- ***Phishing: Identifying*** online scams.
- ***Catching Misinformation:*** Critical evaluation of online content.
- ***Cyberbullying:*** Identifying and reporting.

NC K-12 Computer Science Standards

- **68-NI-04:** Apply multiple methods of encryption to model the secure transmission of information.
- **68-NI-02:** Explain how physical and digital security measures protect electronic information.
- **35-IC-04:** Exhibit positive digital citizenship and social responsibility in online interactions.
- **68-IC-08:** Understand how online interactions make an impact on the social, emotional, and physical aspect of others.

ISSN: 2473-4901
v11 n6383

One-Time Password	an automatically generated password that is only valid for a single login session or transaction.
Multi-factor authentication	an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more distinct types of evidence (or factors) to an authentication mechanism.
Authentication Factor	a special category of security credential that is used to verify the identity and authorization of a user attempting to gain access, send communications, or request data from a secured network, system or application.
Phishing	Phishing is the practice of sending fake communications that appear to come from a legitimate and reputable source, usually through email and text messaging.
Electronic mail (email)	a communication method that uses electronic devices to deliver messages across computer networks. "Email" refers to both the delivery system and individual messages that are sent and received.
Chat Messaging	Chat messages are instant digital communications exchanged over the internet through various platforms like live chat, social media, and messaging applications.
Bias	a tendency to believe that some people, ideas, etc., are better than others, which often results in treating some people unfairly.
Cyberbullying	the use of technology to harass, threaten, embarrass, or target another person. Online threats and mean, aggressive, or rude texts, tweets, posts, or messages all count. So does posting personal information, pictures, or videos designed to hurt or embarrass someone else.
Misinformation	False or Incorrect information. It is usually done accidentally.
Disinformation	Intentionally incorrect information meant to mislead individuals or the general public.
CAARP method	A 5-step method used to identify misinformation. They are: - Currency: When was this made? Is it out of date? - Authority: Are they an expert on the topic? - Accuracy: Where did their information come from? - Relevance: Is the information useful to you? Purpose: What is the intention behind it?

Module 4: Future & Responsibility

- ***How Technology Evolves:*** Introduction to Deepfakes & AI.
- ***Careers in Cybersecurity:*** Pathways for future professionals.
- ***Safety in Numbers:*** Responsible Digital Citizenship.
- ***Maintaining Digital Habits:*** Lifelong online safety.

NC K-12 Computer Science Standards

ISSN: 2473-4901
v11 n6383

- **35-IC-01:** Compare computing technologies that have changed the world and how they both influence and are influenced by cultural practices.
- **ICS-NI-02:** Identify examples to illustrate how sensitive data can be affected by malware and other attacks.

Artificial Intelligence	Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
Machine Learning	A program that uses data and algorithms to train computers to make classifications, generate predictions, or uncover similarities or trends across large datasets.
Generative AI	Deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on.
Deepfake	an image, video, or audio that has been edited or generated using artificial intelligence.
Career	an occupation or profession, especially one requiring special training
Information Security Analyst	A career where individuals monitor and maintain networks, making sure company data stays safe and secure.
Digital Forensic Examiner	A professional who analyzes digital evidence in legal or criminal investigations.
Pen Tester	A cybersecurity professional who simulates cyberattacks on computer systems, networks, and applications to identify and exploit vulnerabilities.
Security Architect	A professional who designs, builds, and implements security systems within an organization's IT infrastructure. They are responsible for safeguarding networks, data, and information from cyber threats and ensuring compliance with security policies and standards.
Cryptography Engineer	A career where a professional designs, develops, implements, and analyzes cryptographic algorithms and systems to secure data and communication. They work with software and hardware to integrate these systems into various applications, devices, and networks.