Cybersecurity Early Education: A Review of Current Cybersecurity Education for Young Children

Elham Ebrahimi[a], Marjorie Pare, Geoff Stoker[b] and Shauna White
Compu , U.S.A.
ebrahimie@uncw.edu, parem@uncw.edu, stokerg@uncw.edu, whitest@uncw.edu

Keywords: Cybersecurity, Educational Games, Active Learning, k-12 Education.

Abstract: Cybersecurity education is critical for children growing up in a digital world where learning to navigate the internet safely is as important as learning to safely cross a busy street. Interacting with engaging games is an excellent way for children to learn complex cybersecurity concepts. Students are increasingly engaged in online activities at school, via social media, and on gaming platforms. Cybersecurity education helps them recognize and avoid potential threats, like phishing scams, online predators, and privacy breaches. Teaching children to protect their personal information (like names, addresses, and locations) can help prevent identity theft and reduce the risks of cyberbullying. Furthermore, cybersecurity education fosters digital literacy, enabling children to understand the broader digital environment, including the ethical use of technology and the consequences of their online actions. Early exposure to cybersecurity concepts also cultivates interest in STEM, which opens doors to future technical careers and builds valuable problem-solving and analytical skills. This article aims to provide an overview of available games on cybersecurity topics for primary and secondary school students and to describe the implementation of a browser-based game platform for primary school students.

1 INTRODUCTION

Games are highly effective for teaching complex concepts to younger age groups. They engage children in natural, enjoyable, and memorable ways, allowing them to explore, experiment, and build understanding at their own pace (Lamrani and Abdelwahed, 2020). More than that, games make learning enjoyable by incorporating elements of play. This not only sustains a child's attention during creative activities longer than traditional methods but also makes learning an exciting and interesting journey (Behnamnia et al., 2020).

This is especially beneficial when learning challenging or abstract topics, as children are more likely to stick with them. Games encourage hands-on interaction, allowing children to learn by doing rather than just observing or listening (Yannier et al., 2021). Complex concepts are often easier to understand when children can experiment and receive instant feedback on their actions, which helps them understand cause-and-effect relationships and learn from mistakes (Alam, 2022). This quick feedback loop enables children to self-correct and gain confidence in tackling complex ideas (Murtazaev and Shukrulloev, 2024).

Moreover, many educational games are designed to involve problem-solving and decision-making, which build critical thinking skills (Mao et al., 2022). For example, math-based puzzles or strategy games teach logical thinking, strategic planning, and persistence, which are foundational for understanding more advanced topics (Murtazaev and Shukrulloev, 2024). Games also often feature levels or stages that increase in difficulty, providing a scaffolded approach to learning. Children can start with simple tasks that gradually become more challenging, allowing them to build foundational knowledge before tackling advanced concepts (Janson et al., 2020). Additionally, games often involve visual, auditory, and sometimes even tactile interactions, engaging multiple senses. Multi-sensory learning has been shown to improve memory retention, making it more likely that children will remember complex information (Aaron, 2017). Gamification elements like points, badges, and rewards boost motivation by giving children a sense of accomplishment as they progress. This encourages children to continue learning and to push through

[a] https://orcid.org/0000-0001-9431-557X
[b] https://orcid.org/0009-0001-0495-3162

Ebrahimi, E., Pare, M., Stoker, G. and White, S.
Cybersecurity Early Education: A Review of Current Cybersecurity Education for Young Children.
DOI: 10.5220/0013501000003932

In *Proceedings of the 17th International Conference on Computer Supported Education (CSEDU 2025) - Volume 1*, pages 822-833
ISBN: 978-989-758-746-7; ISSN: 2184-5026

challenges, even when faced with complex topics (Alsawaier, 2018; Buckley and Doyle, 2016; Chapman and Rich, 2018). In this paper, we review some of the existing cybersecurity content and our game-based platform focused on cybersecurity themes for primary school students for early cybersecurity education and training.

2 LITERATURE REVIEW

Importance of k-12 Cybersecurity Education. Students are increasingly engaged in online activities at school, via social media, and on gaming platforms. Cybersecurity education helps them recognize and avoid potential threats like phishing scams, online predators, and privacy breaches. Teaching children to protect their personal information (like names, addresses, and locations) can help prevent identity theft and reduce the risks of cyberbullying. Furthermore, cybersecurity education fosters digital literacy, enabling children to understand the broader digital environment, including the ethical use of technology and the consequences of their online actions (Quayyum et al., 2021).

There is currently a paucity of cybersecurity curricula designed to teach students in grades 3-5, due to their basic computer skills and knowledge (Zepf and Arthur, 2013). Additionally, young children often learn better in early years so introducing cybersecurity in elementary schools can offer them greater opportunities for future careers. It is critical that we offer early exposure to cybersecurity principles to protect young children from "negative experiences" (Zepf and Arthur, 2013; National Science Foundation, 2020; Giannakas et al., 2019). Offering curricula earlier may improve student awareness of the dangers of cyberattacks while also introducing them to topics associated with cybersecurity. From an early age, students are exposed to and engaged in online practices. For instance, by age 11, 50% of children have their own social media accounts, 64% have access to the Internet via their own laptop or tablet, and 38% have access to the Internet via their phone (Influence Central, 2016).

There are three primary areas of vulnerability that children encounter online: content, contact, and conduct. Middle school youth are susceptible to all three and start to engage in inappropriate cyber activity such as bullying or hacking (Keeley and Little, 2017). The grades 3-5 population allows researchers to mitigate developmental and behavioral, and technology-access issues associated with older students, and to longitudinally assess the impact of the training on earlier students' perceptions of cybersecurity once they reach middle school. Research suggests that students begin to focus on their academic ability as a "fixed quality" in middle and high school grades, and therefore, withdraw from subjects for which they lack confidence (Jethwani et al., 2016; Rhodewalt and Tragakis, 2002), or sense of belonging (Margolis and Fisher, 2002; Jethwani et al., 2017). This effort creates the scaffolding to engage students earlier in critical STEM areas of cybersecurity and supports exploratory learning in later grades. Concurrently, this directly correlates to students' interests in cybersecurity: educators' lack of cybersecurity self-efficacy (Agamba and Keengwe, 2012; Ertmer et al., 2003). XR and Game-Based Learning (GBL) can serve to demystify cybersecurity and build self-efficacy for educators and students alike.

eXtended Reality and advantages of XR and Gamification. Teaching and learning have always been intertwined. Learning occurs more naturally when teaching is optimal and fits the learning style of the learners (Proserpio and Gioia, 2007). Thus, educators teaching the virtual generation should take advantage of new technologies, such as internet-based tools and games to increase participation and fulfill learning objectives. Research has shown that virtual technologies could enhance student's performance (Scoville and Buskirk, 2007; Han, 2020). Consequently, game-based technology and strategies have gained 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). Virtual technologies or eXtended Reality (XR) refers to the spectrum of experiences including Augmented Reality (AR), Mixed Reality (MR), and Virtual Reality (VR). In general, Extended Reality includes any human-machine interactions generated by computer technology and wearables. XR has wide-ranging applications that include a large training and education subset. Within XR, students can visualize abstract concepts and complete related hands-on tasks rather than imagining them (Trindade et al., 2002; Javidi, 1999; Christou, 2010). A growing body of research indicates that when students interact and control events in extended reality environments, they become more actively involved in constructing knowledge through an immersive experience rather than learning by lecture or reading expository text (Roussou, 2004; Dewey, 2004).

Cybersecurity Workforce Development. Improving STEM skills is a current and future need that must be addressed to solve the social and economic challenges our society faces (English, 2016). This goal's urgency is based on the shortages in the current and fu-

ture STEM workforce (Hopkins et al., 2014; Charette, 2015). According to the Committee on STEM Education of the National Science and Technology Council (2018) (on STEM Education, 2018), STEM skills are important not only for STEM careers, but all career paths in general as these skills can help people to be successful in their lives.

Elementary-High School Cybersecurity Education is more effective if it is grounded in situated cognition theory, which emphasizes "knowing is doing" and that how knowledge is applied is only as important as to how and where the knowledge will be applied (Brown et al., 1989; Putnam and Borko, 2000). *Problem-Based Learning* (PBL) has garnered positive outcomes for students in the areas of collaboration (Boaler, 1997; Penuel, 2006), student engagement (Belland et al., 2006; Brush and Saye, 2008), critical thinking, and problem-solving skills (Mergendoller et al., 2006). PBL requires students to solve realistic problems, gain control over learning, and use teachers as inquiry coaches, while working collaboratively (Darling-Hammond et al., 2015; Thomas, 2000). Research indicates that PBL can increase long-term retention and improve test scores and problem solving (Ravitz, 2009). Further, PBL can offer students learning scaffolds that enrich inquiry and increase student engagement (Brush and Saye, 2000; Ertmer and Simons, 2006; Jonassen, 2011; Mergendoller and Thomas, 2005; Tamim and Grant, 2013). The integration of technology into PBL assists teachers because it can promote self-discovery and independence (Grant, 2002; Krajcik et al., 2014).

Additionally, science education available to students in rural, low-income areas further aggravates student engagement, particularly for those with diverse learning needs (Potkonjak et al., 2016). For instance, instruction traditionally delivered in a textbook-lecture format frequently involves a substantial amount of independent, self-regulated analysis of expository writing and worksheet activities (Scruggs and Mastropieri, 1994a; Scruggs and Mastropieri, 1994b; Scruggs et al., 2010). Students often experience difficulty in a learning environment where they are rapidly introduced to new theories, facts, and vocabulary in an inconsistent and unpredictable manner (Downing et al., 2002) and many practicing general education teachers have little training or experience in identifying and accommodating the needs of students with special needs (Moon et al., 2012; McGinnis and Stefanich, 2007; Norman et al., 1998; Villanueva et al., 2012). Proper integration of technologies into the curriculum are shown to overcome some of these obstacles (Merchant et al., 2014; Hew and Cheung, 2010; Annetta et al., 2009; Simões et al., 2013; de Marcos et al., 2016; Potkonjak et al., 2016; Hsieh et al., 2008).

3 CURRENT CYBERSECURITY EDUCATION EXAMPLES

Young children often learn better in their early years, so early exposure to cybersecurity principles must be offered before they reach middle school to protect them from negative experiences. Most current cybersecurity education for children is predominantly passive, where students watch videos and follow along with minimal interaction, limiting engagement and retention of knowledge. Where interactive games do exist, they are often designed for older children and are too complex or inaccessible for younger learners. This creates a gap in educational tools for elementary-aged students who need simplified, hands-on experiences to grasp basic cybersecurity principles (e.g., online safety). Additionally, most activities fail to incorporate any form of knowledge assessment, leaving educators and parents without clear indicators of how well children understand and can apply the material. This lack of interactive, age-appropriate content combined with the absence of measurable learning outcomes highlights a critical need for better-designed cybersecurity education activities for young audiences.

There are two main categories of cybersecurity education for elementary school students, each with distinct approaches to teaching and engagement:

- **Passive Learning.** In this method, students receive information in a more traditional, one-directional manner, without significant interaction or hands-on participation. The focus is on absorbing knowledge through methods such as lecture-based learning, reading informational materials, and watching videos or demonstrations. While this approach is effective for conveying foundational concepts and theoretical knowledge, it may not fully engage younger learners or encourage deep understanding. However, it can serve as a useful introduction to cybersecurity topics before moving on to more interactive approaches.
- **Active or Gamified Learning.** This approach actively involves students in the learning process, encouraging critical thinking, problem-solving, and participation. It often incorporates game elements such as challenges, points, levels, and rewards to make learning more engaging and interactive. By immersing students in hands-on activities, puzzles, simulations, or cybersecurity-

themed games, this method fosters deeper understanding and retention of cybersecurity principles. Gamified learning also promotes collaboration, decision-making, and a proactive approach to online safety, making it particularly effective for younger audiences who benefit from experiential learning.

Both methods have their place in cybersecurity education. While passive learning provides essential knowledge and background information, active or gamified learning helps students internalize and apply cybersecurity concepts in a meaningful way. A balanced approach that incorporates both strategies can create an effective and engaging cybersecurity curriculum for elementary school students.

Here are some examples of passive and active/gamified methods used to teach cybersecurity to young audiences with a significant number of subscribers.

Tynker, a company dedicated to teaching K-12 student coding, provides an expansive website with a variety of activities and games focused on several different aspects of coding and software development. Tynker offers both a subscription-based website service and an app store product. Starting with premade coding blocks, players follow lessons to create graphics and learn code. The scaffolded learning approach allows individuals to complete goals at their own pace. As users improve, they are introduced to different coding languages, statistics, and data analytics, as well as more expansive art and design tools for creative coding (from BYJU'S, 2024). Users also get the freedom to create interactive games and tools outside of lessons. The site allows users to create projects and share them with the community, so students receive feedback from others and are not just graded based on completion.

Unfortunately, the curriculum relating to cybersecurity and internet safety is relegated to videos with quizzes based on the source material. These cartoons provide fantastical scenarios in which to introduce cybersecurity concepts and provide educational material that discusses them in a way that users can understand. These videos, while helpful, do not provide an enriching interactive experience. Going through the actions of what makes an individual's data secure could solidify the concept in the user's minds.

Trend Micro Cyber Academy is a collection of videos related to cybersecurity concepts such as password safety, scams, and privacy. This 12-episode series educates learners on the importance of internet safety and how to keep yourself protected (Micro, 2022). These videos are packed with information from start to finish, which allows them to provide a

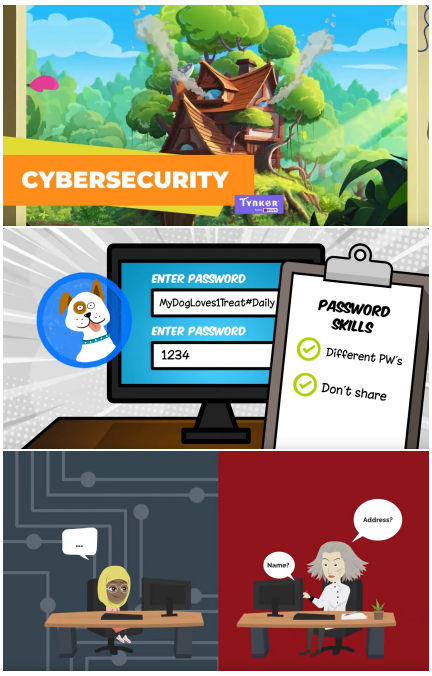

Figure 1: A collection of children's educational videos from Tynker, Trend Micro, and Malwarebytes, respectively. The colorful visuals and approachable material keep viewers engaged despite the passive learning style.

dense summary of the topics. However, the videos lack much narrative and can potentially lose viewer attention if the concepts are hard for an individual to grasp. The passive nature of videos lacks the opportunity to assess viewer retention as well, so parents and educators are unsure of what viewers have learned without supplemental material.

LearningMole is a website offering a variety of educational videos for young learners, ranging from history and geography to science and math. These videos break down topics for viewers in a cartoony, easy-to-digest format (Mole, 2024). The information relating to cybersecurity and password safety is limited to only a few videos, but they are simple and easy to understand. More experienced learners might not feel engaged with the material LearningMole provides, as each video provides an introductory overview of each topic.

MalwareBytes, the antivirus protection company, offers one video teaching young learners about cybersecurity. This video emphasizes the dangers of being unprotected by creating a scenario focused on the attacker's perspective. It provides a series of example situations that children are susceptible to, and demonstrate ways they can be exploited (Malwarebytes, 2021). Although helpful, this video lacks educational material explaining how to protect against these attacks. The solution suggested to create a

strong password lacks extra information on how to build strong passwords, and telling kids to ”avoid anything that looks weird” without showing examples could lead to some confusion in the future without additional guidance.

Smile and Learn is a company offering educational videos and interactive activities for children on a wide array of topics. Smile and Learn offers their material in 6 different languages, and allows for personalized goals to be set for each student (Smile and learn, 2021). This company offers some educational videos on cybersecurity and internet safety, with a focus on phone use and practicing good social habits. These videos offer recommendations and warnings in a fun way to encourage viewers to protect themselves online. These videos go over a wide array of situations involving cyberbullying and how to maintain your first mobile device, but lack information for a slightly younger audience.

The Center for Development of Security Excellence offers several crosswords and word searches related to cybersecurity (for Development of Security Excellence, 2024). The information presented is directed towards a more adult audience, and aims to encourage companies to use these games as a refresher for different cybersecurity and internet safety concepts. The word searches provide a definition of the word when discovered. There are also a few interactive games centered around identifying workplace vulnerabilities. The games require a lot of reading, which can lower engagement for individuals even at their target demographic. Additionally, they lack immediate auditory feedback and provide little incentive to play longer than a few minutes.

PBS NOVA Labs offers an interactive cybersecurity game called the Cybersecurity Lab (Labs, 2022). This game puts you into the role of a new mobile app developer that just launched his application without cybersecurity protocols in place. Now the player is tasked with keeping all the information secure by managing currency and working towards growing your business without compromising assets. The game lacks audio feedback and requires completion of a lengthy, non-interactive tutorial before getting into the missions. The game also requires a large amount of reading, which could lower user engagement. Despite this, the material offered in this game could be beneficial for students in a high school setting, to teach them more complex topics relating to application security while mixing in programming knowledge.

Google’s Interland is an interactive, browser based game meant to teach users about internet safety while exploring different lands. Each area showcases

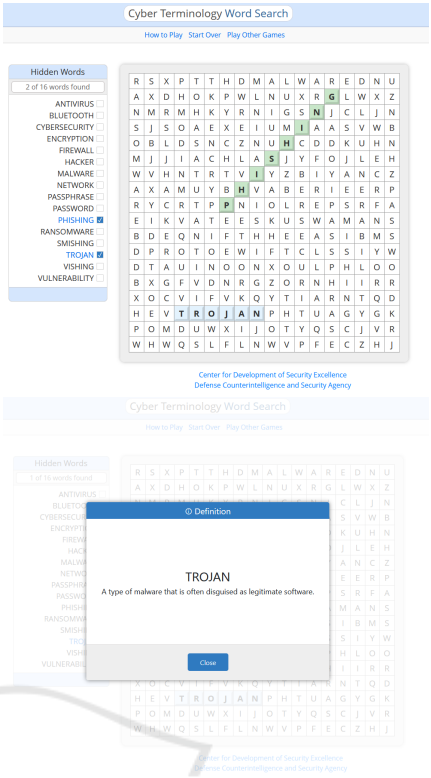

Figure 2: Cybersecurity Word searches allow players to learn and understand different definitions when terms are discovered.

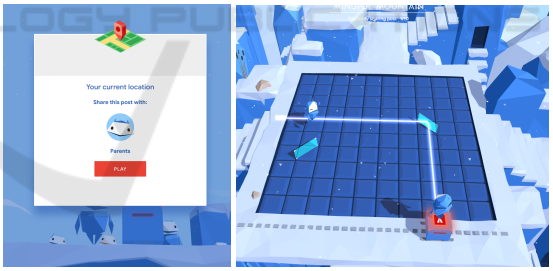

Figure 3: Google’s Interlands teaches privacy safety through this interactive mirror-based puzzle game. Players are given a category of people that is allowed to have this data and must only share it with them.

a different topic to discuss, such as when and how to share data, who to identify fake information, and how to practice proper password safety (Interland, 2024). The concepts shown are abstracted and shown in a way that is simple to understand and easy to perform, with plenty of opportunities to take breaks and learn from mistakes. Each section focuses on a specific area and allows for a high level of interactivity. All of the instructions are shown visually through text, as well as through voice over.

Gameplay varies from selecting the most secure

Figure 4: Cyber Sprinters provides quizzes in the form of yes or no questions to educate players on cybersecurity concepts.

password from a list, to mirror-based logic puzzles and endless runners. Overall, this interactive website offers a really engaging experience for young learners, and could benefit from being expanded into more complex topics. Each section ends with a quiz in order to assess the player's knowledge gained from the session. Points are awarded based on how well the user performs and are encouraged to get as high a score as possible. The game lacks a social and collaborative element to it, so users are not encouraged to replay after they are finished, but this material could be used as a refresher if topics are forgotten.

Cyber Sprinters, a game developed by the UK National Cyber Security Center, aims to teach learners about different cybersecurity topics by avoiding obstacles in the form of hackers and trojans (Centre, 2024). Players can also encounter bonus tokens. When collected, they prompt the user to answer a yes-or-no quiz question relating to any number of cybersecurity situations. Players are then given extra details when answering correctly, and provided guidelines on how to protect themselves from real-world scenarios. Additionally, users encounter major threats in the game that require minigames to defeat. These minigames range from creating strong passwords to ensuring devices are updated regularly. The information within this game is text-heavy but is informative and engaging for short gameplay sessions. The game is fun and interactive, but none of the actions allow players to actively practice techniques that would be performed in real-world situations. Many of the questions only offer two answers, allowing players to guess if they are not paying full attention to what is being asked of them. Despite this, the material offers a simple and engaging way to get introduced to cybersecurity topics.

Cyber Games UK offers a short, interactive game called Password Strength Meter on their website (UK, 2023). This game asks you to create a variety of passwords at different strengths while showing you what makes a password successful. This short experience gives players the freedom to practice creating their own password while seeing the points awarded for good password choices. The real-time feedback of this game while writing passwords easily helps players understand how to improve creating their own passwords, while giving them the creativity to experiment and play with different combinations. Despite its simplicity, this game can give young learners a firm understanding of secure password generation while maintaining a level of creative freedom.

noindent ***Summary of Pros and Cons of Passive and Active Learning.*** Passive learning offers a structured and comprehensive way to introduce cybersecurity concepts to young learners, making it easier to deliver dense information efficiently. Videos and readings provide a simple and accessible format, allowing students to learn at their own pace. However, the lack of interactivity in passive learning can reduce engagement and retention, especially for children who benefit from hands-on experiences. Additionally, these methods do not provide opportunities for students to actively apply what they have learned, making it difficult to reinforce cybersecurity concepts in real-world contexts. Another limitation is the minimal assessment and feedback, leaving educators and parents uncertain about how much students have truly absorbed.

In contrast, active learning engages students through interactive activities, games, and simulations that encourage critical thinking and problem-solving. By allowing learners to apply their knowledge in dynamic ways, active learning improves retention and helps students understand complex cybersecurity principles through experience. Immediate feedback and gamification elements can also make learning more enjoyable and motivating. However, some interactive activities may oversimplify real-world cybersecurity challenges, and the time investment required for these methods can be greater than passive alternatives. Furthermore, some games may lack social or collaborative elements, limiting their long-term engagement, while text-heavy formats or lengthy tutorials may discourage younger audiences from fully participating.

While both passive and active learning methods have their strengths and weaknesses, there is a pressing need for fundamental research to better understand their impact on young learners. More studies are required to examine how each approach influences knowledge retention, engagement, and skill development in cybersecurity education. Additionally, research can help determine the most effective way to balance passive and active methods, ensuring that young audiences receive a well-rounded

Figure 5: 2D point-and-click game that encourages learners to develop their password safety skills through cooking. Their password strength will be assessed throughout different levels of the game.

and impactful learning experience. By exploring the best ways to integrate these strategies, educators and researchers can develop optimized approaches that maximize both engagement and educational outcomes.

4 CyberFortress ACADEMY

Cybersecurity awareness will be used to teach children safety skills and promote critical thinking in fun and engaging ways. The goal of our technology is to teach children how to protect their passwords and personal information, how to recognize scams, phishing attempts, and cyberbullying, and teach them the role of trusted adults (parents/teachers) to keep their devices safe. Our approach ensures that cybersecurity education is age-appropriate, engaging, and impactful, giving children the foundation they need to be safe and responsible digital citizens. To ensure that students are absorbing the material effectively, we will implement regular assessments and simulated digital attacks. This approach not only makes cybersecurity education accessible and engaging but also lays a strong foundation for children to become safe and responsible digital citizens.

We are actively building CyberFortress Academy, a browser-based game platform designed to provide grades 2-5 students with essential cybersecurity knowledge, skills, and abilities through engaging, age-appropriate activities. Our technology currently includes 10 proof-of-concept games covering topics like two-factor authentication (2FA), strong password creation, social engineering, phishing, encryption, and malware injections.

The platform will serve as an engaging and immersive learning environment for students. The platform will be designed to allow the collection and storage of relevant data, enabling educators and parents to easily track student progress and performance. The games will be integrated into a large, interactive map, where each section represents a unique themed area. Students will navigate this map as part of their learning journey, taking on the role of caretakers or explorers within the virtual world. Each area of the map will offer distinct challenges and objectives, encouraging students to engage with a variety of subjects or skills. As students complete different modules within the games, they will unlock rewards such as virtual pets, tools, or resources that are specific to the map's area.

The modules themselves will be designed to be both fun and educational, combining problem-solving, critical thinking, and subject-specific skills. Each area of the map will have a unique focus. To further enhance engagement, students will have the opportunity to personalize their pets, tools, and areas of the map, making the experience uniquely theirs. Collaboration can also be incorporated by allowing students to team up to unlock special regions or solve larger challenges. The end result will not just be a completed website but a dynamic, evolving platform that grows with students' progress, creativity, and engagement.

Our games have been functionally tested by adult volunteers, and we are continuously working to enhance their design and performance. Currently, we are refining the knowledge assessment components to measure how effectively the games convey cybersecurity concepts. The first round of testing will use only three Cybersecurity games (Password Chef, Two-Step Treasure, and Pelican Phishing) involving second and third-grade students to ensure the content is age-appropriate and user-friendly. During this initial phase, students will engage with the games and training modules to develop their cybersecurity knowledge. Following this, they will take on a grand challenge designed to evaluate their ability to apply what they have learned through interactive activities.

Password Chef is an educational, 2D point-and-click game that encourages users to develop their password safety skills through cooking (Figure 5). Users are tasked with creating passwords using specific criteria that get more complex over time by creating unique recipes. Ingredients are labeled with different alphanumeric characters and symbols, with vegetables having the ability to be chopped in order to make letters lowercase. Other items, such as meats and spices, serve as both numbers and special char-

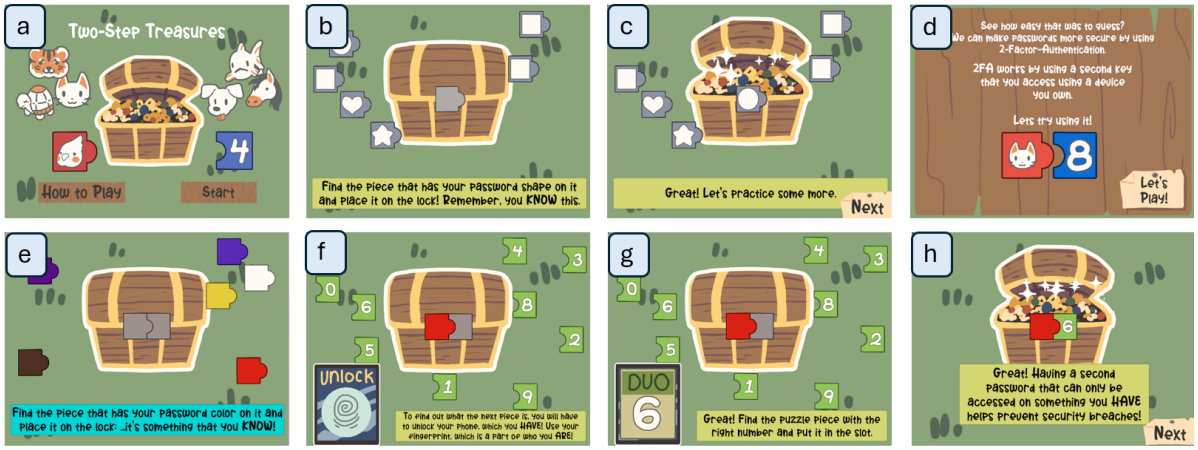

Figure 6: Images a-c show how one-step authentication that learners will go through. Learners will practice the one-step authentication, and then, they will be introduced to two-step authentication - images d-h. There are assessment phases in-between different phases.

acters, respectively. Users are encouraged to create long passwords, as that makes it harder for individuals to guess the exact combination used. Players interact with the game through simple touch controls, giving them the ability to drag and drop items onto different areas of the screen to add them to their password. This allows players unfamiliar with games to feel confident in their ability to participate.

Players are encouraged to create recipes that they can recall and keep secret, as narratively, it is important to prevent other chefs from guessing what they used. After players complete a tutorial explaining ways to make a secure password, they are given challenges to complete. These challenges range from using a specific character to creating a password with a minimum number of letters and symbols. When ready, a judge awards points to the dish based on the length, variability of the characters, and whether or not the challenge goal was met.

After a set number of challenges are completed, users are asked to recall one of them at random. This helps reiterate the need to remember these passwords so they are not forgotten later. Password Chef aims to assess players in their ability to create and recall strong passwords using length, character variability, and knowledge while maintaining secrecy. The player should feel excited and empowered when finishing the game, as the focus is on rewarding successes rather than delivering harsh punishments for lacking knowledge.

Two-Step Treasures is a 2D point-and-click game designed to introduce players to the concept of two-factor authentication (Figure 6). This game requires players to create a password from simple shapes, symbols, and colors and recall them to open treasure chests. After this knowledge is established, users are introduced to two-factor authentication concepts by requiring not only the initial password, but a secondary password on another device to fully unlock the new treasure chest.

Players are shown a collection of keys that contain a variety of different symbols on them. Players are then expected to choose the correct key to unlock the treasure in front of them. After this, the game asks the user to try and guess another individual's password and unlock their chest. This aims to introduce the idea that passwords are easy to bypass without proof of identity, showing that two-factor authentication can be one way to make access more secure. This introduces the second stage of gameplay, where users put in their own password key but are then shown a cellphone that requires a secondary form of identification to open, showing another level of security, before a second set of keys is generated in the play area (Figure 6.f). The player simply has to unlock their device, read the number shown on their phone screen, and find the respective key to open the chest (Figure 6.g).

This game has no time restriction or consequence for guessing incorrectly, as this game aims to introduce the concept of two-factor authentication in an easy to understand format. The game allows for more complexity by adding multiple checks, having users attempt to guess passwords without access to two-factor authentication, and similar methods to show how easy it is to protect yourself when using multiple forms of password safety.

Pelican Phishing is an educational game focused on teaching and enforcing concepts of identifying phishing attempts (Figure 7). The game does this by showing the player multiple text-based interactions that could or could not be phishing. This game is a 2d style game. The goal of the game is to teach

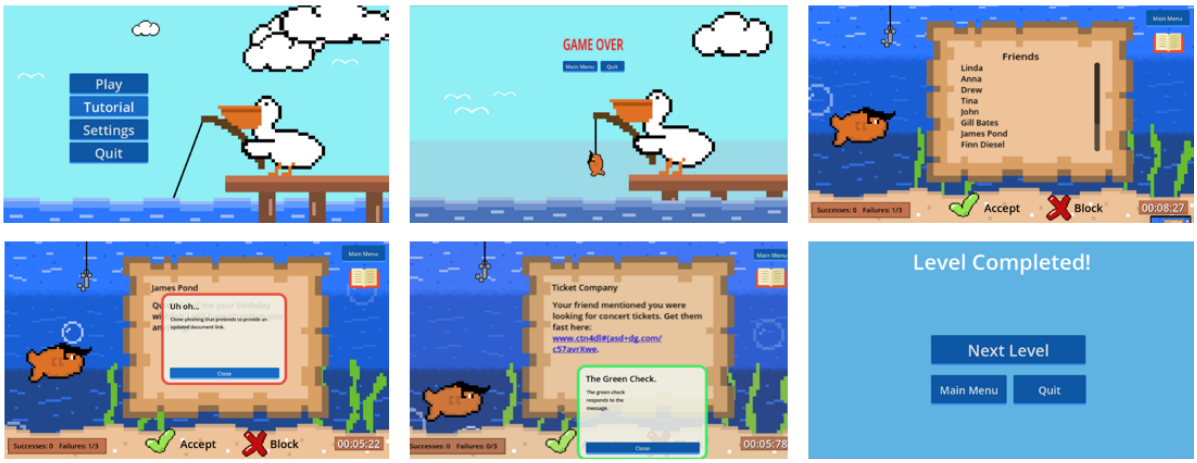

Figure 7: This game will be based on a simple text pop-up scene. Each pop-up is the text the player needs to review. The player will accept or deny communication with each pop-up. The pop-ups will vary in context and style to challenge the players understanding of phishing. The goal of the player is to not respond to phishing attempts.

the player simple concepts of phishing attempts in a fun and interactive way. In the Pelican Phishing game, the player's goal is to analyze text-based interactions and pop-ups and decide whether or not the presented scenarios are safe or potential phishing attempts. Through this gameplay, we aim to educate players in a fun and engaging way about the dangerous tactics used by phishers and scammers, as well as how to identify suspicious online behaviors in order to avoid them.

The game will focus on players who have zero to minimal internet or online social interactions but have some initial gaming experience. Pelican Phishing aims to provide a light introduction to essential cybersecurity concepts. Through a right-to-left scrolling mechanic, players will control a fish trying to "get to work", while a pelican overhead attempts to "catch" them using phishing tactics. The player's success depends on correctly identifying and responding to phishing attempts, allowing them to progress further in their journey. The core mission of Pelican Phishing is to empower young players with the information and skills needed to protect themselves online by recognizing suspicious links, understanding their data privacy, and resisting social engineering. As players advance through the game, the difficulty of the phishing scenarios increases, allowing the players to apply the lessons learned in the earlier stages to more complex situations. This progression is designed to create a sense of achievement and growth for the player while reinforcing gameplay goals. The vision behind Pelican Phishing is not only about making learning about phishing fun but also **building confidence in users as they navigate and enter the digital world.** By making the game progressively challenging, players will feel both entertained and capable of applying their new cybersecurity knowledge in real-world situations.

5 NEXT STEPS

We are currently conducting rigorous testing of three of our cybersecurity games, detailed in section 4, by implementing them in elementary school classrooms with both students and teachers. We are collaborating with three schools and will collect data from four second-grade classes, three third-grade classes, two fourth-grade classes, two fifth-grade classes, two technology classes at two elementary schools, and the Education Laboratory afterschool program at the Watson College of Education at UNCW, targeting over 200 students. This hands-on testing process allows us to gather valuable real-world feedback, helping us refine the games to enhance engagement, usability, and educational effectiveness. By observing how young learners interact with the games and assessing teacher feedback in the eight 30-session, we can make necessary improvements to ensure the content is both age-appropriate and impactful in teaching cybersecurity concepts.

In addition to refining our existing games, we are committed to expanding our efforts by developing more cybersecurity-focused educational tools. This includes creating new interactive games, engaging learning modules, and innovative assessment methods designed to simplify complex cybersecurity principles for young learners. Our goal is to make cybersecurity education more accessible, enjoyable, and effective by incorporating interactive elements

that encourage critical thinking and problem-solving. Through ongoing research, collaboration with educators, and iterative design improvements, we strive to build a comprehensive suite of resources that empower children to navigate the digital world safely and responsibly. The long-term goal for this project is to develop a fully functional, browser-based platform that integrates all the games and features a dynamic map for immersive gameplay. This platform hosts a comprehensive curriculum aligned with educational standards while fostering critical thinking and problem-solving skills.

This project offers profound societal benefits by addressing key gaps in cybersecurity education. This project allows elementary school students to gain essential knowledge to navigate the digital world safely, reducing their vulnerability to cybercrimes like fraud, scams, and identity theft. By building this foundational knowledge, the initiative not only mitigates the risks of online threats but also promotes digital inclusion. This work enhances research in child-focused cybersecurity education and effective teaching methods. A digitally literate population reduces internet crimes and fraud while supporting workforce development goals by inspiring students to pursue careers in cybersecurity, helping meet the growing demand for skilled professionals. In 2022, there were 14,228,545 grades 2-5 public school students in the US. This sizable audience highlights the potential for a significant opportunity to make a meaningful local and national impact by equipping young learners with essential online safety skills and fostering responsible digital behavior at an early age.

6 CONCLUSIONS

Cybersecurity education is essential in equipping young learners with the knowledge and skills needed to navigate the digital world safely and responsibly. By reducing their vulnerability to online threats such as fraud, scams, and identity theft, early cybersecurity education fosters a generation of more informed and cautious digital citizens. Additionally, promoting cybersecurity awareness helps bridge the digital divide, ensuring that underserved communities can safely access online opportunities. Through the development and refinement of engaging, interactive games, we aim to make learning these critical concepts both accessible and enjoyable. 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.

REFERENCES

Aaron, J. M. (2017). Auditory, visual, kinesthetic-tactile, and multi-sensory modalities: A quantitative study of how preferred modalities create more effective teaching and learning environments. *Journal of Neuroscience and Behavioral Health*, 9(1):1–9.

Agamba, J. J. and Keengwe, J. (2012). Pre-service teachers' perceptions of information assurance and cyber security. *International Journal of Information and Communication Technology Education (IJICTE)*, 8(2):94–101.

Alam, A. (2022). A digital game based learning approach for effective curriculum transaction for teaching-learning of artificial intelligence and machine learning. In *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, pages 69–74. IEEE.

Alsawaier, R. S. (2018). The effect of gamification on motivation and engagement. *The International Journal of Information and Learning Technology*, 35(1):56–79.

Annetta, L., Mangrum, J., Holmes, S., Collazo, K., and Cheng, M.-T. (2009). Bridging realty to virtual reality: Investigating gender effect and student engagement on learning through video game play in an elementary school classroom. *International Journal of Science Education*, 31(8):1091–1113.

Behnamnia, N., Kamsin, A., Ismail, M. A. B., and Hayati, A. (2020). The effective components of creativity in digital game-based learning among young children: A case study. *Children and Youth Services Review*, 116:105227.

Belland, B. R., Ertmer, P. A., and 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.

Boaler, J. (1997). Setting, social class and survival of the quickest. *British educational research journal*, 23(5):575–595.

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

Brush, T. and Saye, J. (2000). Implementation and evaluation of a student-centered learning unit: A case study. *Educational technology research and development*, 48(3):79–100.

Brush, T. and 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.

Buckley, P. and Doyle, E. (2016). Gamification and student motivation. *Interactive learning environments*, 24(6):1162–1175.

Centre, T. N. C. S. (2024). Cyber sprinter.

Chapman, J. R. and Rich, P. J. (2018). Does educational gamification improve students' motivation? if so, which game elements work best? *Journal of Education for Business*, 93(7):315–322.

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*, pages 228–243. IGI Global.

Darling-Hammond, L., Barron, B., Pearson, P. D., Schoenfeld, A. H., Stage, E. K., Zimmerman, T. D., Cervetti, G. N., and Tilson, J. L. (2015). *Powerful learning: What we know about teaching for understanding*. John Wiley & Sons.

de Marcos, L., Garcia-Lopez, E., and Garcia-Cabot, A. (2016). On the effectiveness of game-like and social approaches in learning: Comparing educational gaming, gamification & social networking. *Computers & Education*, 95:99–113.

Dewey, J. (2004). *Democracy and education*. Courier Corporation.

Downing, J. A., Bakken, J. P., and Whedon, C. K. (2002). Teaching text structure to improve reading comprehension. *Intervention in School and Clinic*, 37(4):229–233.

English, L. D. (2016). Stem education k-12: Perspectives on integration. *International Journal of STEM education*, 3(1):3.

Ertmer, P. A., Conklin, D., Lewandowski, J., Osika, E., Selo, M., and Wignall, E. (2003). Increasing preservice teachers' capacity for technology integration through the use of electronic models. *Teacher Education Quarterly*, 30(1):95–112.

Ertmer, P. A. and Simons, K. D. (2006). Jumping the pbl implementation hurdle: Supporting the efforts of k–12 teachers. *Interdisciplinary Journal of Problem-based learning*, 1(1):40–54.

for Development of Security Excellence, C. (2024). Security awareness games.

from BYJU'S, T. (2024). Cybersecurity - all about computers.

Giannakas, F., Papasalouros, A., Kambourakis, G., and Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective*, 28(3):81–106.

Grant, M. M. (2002). Getting a grip on project-based learning: Theory, cases and recommendations. *Meridian: A middle school computer technologies journal*, 5(1):83.

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.

Hew, K. F. and Cheung, W. S. (2010). Use of three-dimensional (3-d) immersive virtual worlds in k-12 and higher education settings: A review of the research. *British journal of educational technology*, 41(1):33–55.

Hopkins, S., Forgasz, H., Corrigan, D., and 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)*.

Hsieh, P., Cho, Y., Liu, M., and Schallert, D. L. (2008). Examining the interplay between middle school students' achievement goals and self-efficacy in a technology-enhanced learning environment. *American Secondary Education*, 36(3):33–50.

Influence Central (2016). Smartphones & the dramatic reshaping of american families. *http://blog.influencecentral.com/smartphones-the-dramatic-reshaping-of-american-families/*.

Interland, G. (2024). Interland.

Janson, A., Sollner, M., and Leimeister, J. M. (2020). Ladders for learning: is scaffolding the key to teaching problem-solving in technology-mediated learning contexts? *Academy of Management Learning & Education*, 19(4):439–468.

Javidi, G. (1999). Virtual reality and education.

Jethwani, M., Memon, N., Richer, A., and Seo, W. (2016). It's hard to be the only girl. In *Journal of The Colloquium for Information System Security Education*, volume 4, pages 16–16.

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.

Jonassen, D. H. (2011). Design problems for secondary students. *National Center for Engineering and Technology Education*.

Keeley, B. and Little, C. (2017). *The State of the Worlds Children 2017: Children in a Digital World.* ERIC.

Kim, S., Song, K., Lockee, B., and Burton, J. (2018). What is gamification in learning and education? In *Gamification in learning and education*, pages 25–38. Springer.

Krajcik, J., Codere, S., Dahsah, C., Bayer, R., and Mun, K. (2014). Planning instruction to meet the intent of the next generation science standards. *Journal of Science Teacher Education*, 25(2):157–175.

Labs, P. N. (2022). Corporation battle network.

Lamrani, R. and Abdelwahed, E. H. (2020). Game-based learning and gamification to improve skills in early years education. *Computer Science and Information Systems*, 17(1):339–356.

Malwarebytes (2021). Cybersecurity training for kids.

Mao, W., Cui, Y., Chiu, M. M., and Lei, H. (2022). Effects of game-based learning on students' critical thinking: A meta-analysis. *Journal of Educational Computing Research*, 59(8):1682–1708.

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

McGinnis, J. R. and Stefanich, G. P. (2007). Special needs and talents in science learning. *Handbook of research on science education*, pages 287–317.

Merchant, Z., Goetz, E. T., Cifuentes, L., Keeney-Kennicutt, W., and Davis, T. J. (2014). Effectiveness of virtual reality-based instruction on students' learning outcomes in k-12 and higher education: A meta-analysis. *Computers & Education*, 70:29–40.

Mergendoller, J. R., Maxwell, N. L., and Bellisimo, Y. (2006). The effectiveness of problem-based instruction: A comparative study of instructional methods and student characteristics. *Interdisciplinary Journal of Problem-based Learning*, 1(2):49–69.

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

Micro, T. (2022). Trend micro cyber academy.

Mole, L. (2024). Why is it important to create strong passwords?

Moon, N. W., Todd, R. L., Morton, D. L., and Ivey, E. (2012). Accommodating students with disabilities in science, technology, engineering, and mathematics (stem). *Atlanta, GA: Center for Assistive Technology and Environmental Access, Georgia Institute of Technology*, pages 8–21.

Murtazaev, M. and Shukrulloev, B. (2024). Unusual methods of teaching mathematics to elementary school students. *NRJ*, 1(3):929–940.

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

Norman, K., Caseau, D., and Stefanich, G. P. (1998). Teaching students with disabilities in inclusive science classrooms: Survey results. *Science Education*, 82(2):127–146.

on STEM Education, C. (2018). Charting a course for success: America's strategy for stem education. *National Science and Technology Council*, pages 1–48.

Ortiz-Rojas, M., Chiluiza, K., and Valcke, M. (2019). Gamification through leaderboards: An empirical study in engineering education. *Computer Applications in Engineering Education*, 27(4):777–788.

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.

Potkonjak, V., Gardner, M., Callaghan, V., Mattila, P., Guetl, C., Petrović, V. M., and Jovanović, K. (2016). Virtual laboratories for education in science, technology, and engineering: A review. *Computers & Education*, 95:309–327.

Proserpio, L. and Gioia, D. A. (2007). Teaching the virtual generation. *Academy of Management Learning & Education*, 6(1):69–80.

Putnam, R. T. and 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.

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.

Quayyum, F., Cruzes, D. S., and Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30:100343.

Ravitz, J. (2009). Introduction: Summarizing findings and looking ahead to a new generation of pbl research. *Interdisciplinary Journal of Problem-based Learning*, 3(1):4–11.

Rhodewalt, F. and Tragakis, M. (2002). Self-handicapping and the social self: The costs and rewards of interpersonal self-construction. *The social self: Cognitive, interpersonal, and intergroup perspectives*, pages 121–143.

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.

Scoville, S. A. and 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.

Scruggs, T. E. and Mastropieri, M. A. (1994a). The construction of scientific knowledge by students with mild disabilities. *The journal of special education*, 28(3):307–321.

Scruggs, T. E. and Mastropieri, M. A. (1994b). Successful mainstreaming in elementary science classes: A qualitative study of three reputational cases. *American Educational Research Journal*, 31(4):785–811.

Scruggs, T. E., Mastropieri, M. A., Berkeley, S., and Graetz, J. E. (2010). Do special education interventions improve learning of secondary content? a meta-analysis. *Remedial and Special Education*, 31(6):437–449.

Simões, J., Redondo, R. D., and Vilas, A. F. (2013). A social gamification framework for a k-6 learning platform. *Computers in Human Behavior*, 29(2):345–353.

Smile and learn (2021). Online privacy for kids - internet safety and security for kids.

Tamim, S. R. and Grant, M. M. (2013). Definitions and uses: Case study of teachers implementing project-based learning. *Interdisciplinary Journal of problem-based learning*, 7(2):3.

Thomas, J. W. (2000). A review of research on project-based learning.

Trindade, J., Fiolhais, C., and Almeida, L. (2002). Science learning in virtual environments: a descriptive study. *British Journal of Educational Technology*, 33(4):471–488.

UK, C. G. (2023). Password strength meter.

Villanueva, M. G., Taylor, J., Therrien, W., and Hand, B. (2012). Science education for students with special needs. *Studies in Science Education*, 48(2):187–215.

Yannier, N., Hudson, S. E., Koedinger, K. R., Hirsh-Pasek, K., Golinkoff, R. M., Munakata, Y., Doebel, S., Schwartz, D. L., Deslauriers, L., McCarty, L., et al. (2021). Active learning:"hands-on" meets "minds-on". *Science*, 374(6563):26–30.

Zepf, I. and Arthur, L. (2013). Cyber-security curricula for basic users. Technical report, NAVAL POSTGRADUATE SCHOOL MONTEREY CA.