A New Curriculum for Cybersecurity Education

Paper Written by: Mackenzie Coleman

Group Partners: Sarah Noble & Rahilkumar Patel

WCS 494: Entrepreneurship

Professor A. Porcher

12/2/2022

Introduction

We can never know everything that is going on behind our device screens, but we can better prepare ourselves to protect our information and our devices while still enjoying the benefits of technology. This is one of the many reasons cybersecurity is important now more than ever. But what good are the benefits of technology if kids, who are known to use the same devices as adults, do not understand the potential risks of using the internet? It is important to protect your information from being stolen and your devices from being hacked but it is important to know why this is important and the risks that are out there. Cybersecurity has become one of the most demanding jobs in the world, primarily due to the high volume of technology use. Over time, people have discovered ways to use technology for malicious intentions. Cyber-attacks are now one of the most common forms of crime today. From ransomware attacks to phishing emails, cyber-attacks happen every day.

The problem that will be addressed in this curriculum is the lack of cybersecurity knowledge and awareness in children and young adults while using the internet and their devices. We want to develop an official Cybersecurity Curriculum for middle schools and high schools that will start teaching the importance of cybersecurity along with the importance of internet safety. This curriculum would focus on the basics of device protection, effective password creation techniques, and different methods of cyber-attacks for example, phishing emails. In middle schools, the problems would be more simplified for the age group to understand at their level but still highlight the same topics. Other topics include cyberbullying reporting methods, how to spot an active cyber-attack on their devices, and internet safety. With the implementation of this Cybersecurity Curriculum, students will have more skills, knowledge, and an overall better understanding of technology and cybersecurity awareness altogether.

Review of Literature

According to the official NIST glossary, also known as the National Institute of Standards and Technology (NIST), cybersecurity has multiple definitions. In the first definition listed, NIST defines cybersecurity as the "prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." (nist.gov). Cybersecurity has become one of the most critical components of national security across the world. For instance, in the UK cyber policy has incorporated cybersecurity at all levels of education starting at the age of 11 (Catota, F. E., et al., 2019). The world has begun to recognize the importance and demand for this knowledge, now and for future generations. The United States has also made progress in cybersecurity education, for example, NIST has created the National Initiative for Cybersecurity Education known as the NICE framework. This framework is intended to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development (Newhouse, et al. 2017). This organization also has held an annual conference called *The NICE K12 Cybersecurity Education Conference* for K12 grade educators to have the opportunity to learn more about cybersecurity and tools for cybersecurity education in the classroom. The opportunities to grow and expand cybersecurity knowledge and awareness are here.

One important fact that is mentioned in multiple reviews of children and technology, is the obvious generational difference between how kids are growing up now, versus how the older generation grew up. The advanced technologies that children have available and have learned to become very comfortable with, were not in the lives of anyone that grew up before the later

2000s. This generational gap has led to parents and guardians not always being actively aware of the online activity their child is participating in, leaving them vulnerable to many online risks. Research from the World Internet Statistics Review showed that only 4 out of 10 parents admitted to being aware of their child's online presence (Sulaiman, N., et al., 2021). The security risks that children face over the internet and on these devices were not issues that older generations had to endure at that age, so this new understanding of technology has proven to be a learning curve for everyone.

Today, children across the world are using the internet and technology for a variety of reasons. From education to entertainment, technology has become a staple in many children's lives. In a study done by NPR, 53% of children in the United States have their smartphone by 11 years old (Kamenetz, 2019). Security risks and threats for children on the internet include cyberbullying through digital platforms and social media sites, possible exposure to inappropriate content, privacy issues, password security, and so much more (Quayyum, F., et al., 2021). In addition to these facts, researchers have also found that the younger the child, the more likely they are to be exposed to online risks such as stalking, grooming, and bullying (Al Shamsi, A., 2019). Cyberbullying is one of the most common cybercrimes among young users on the internet. Reports show that the most common age for cyberbullying is between 13 and 15 years old and 89% of reported cases of cyberbullying go without any action taken (Sulaiman, N., et al., 2021). Bullied children are also recognized to be at a higher risk of fraud and scams because they are actively seeking out friendships online (Sulaiman, N., et al., 2021).

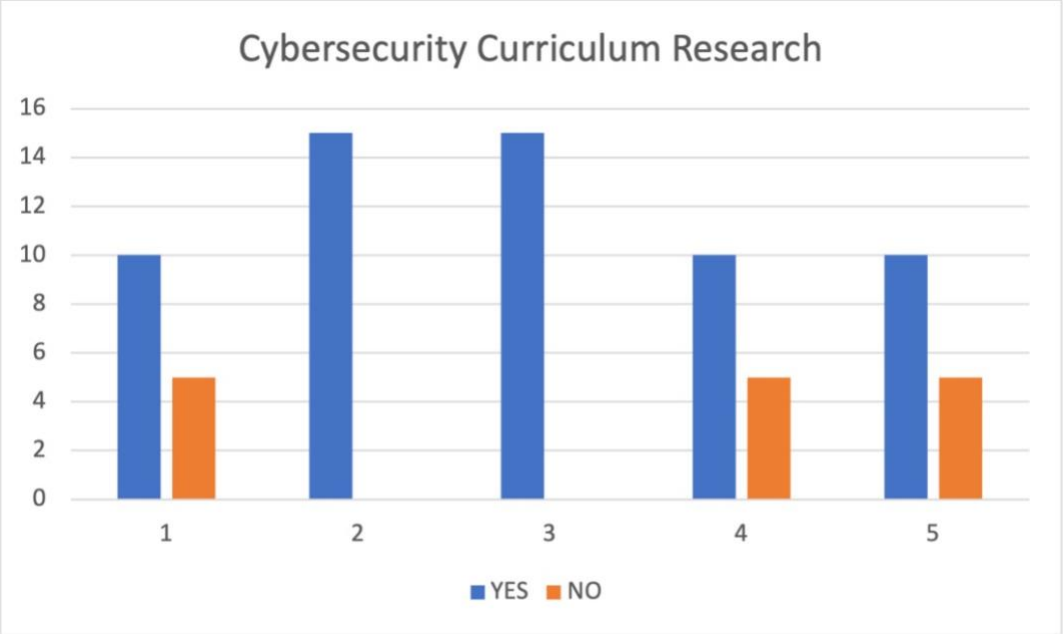
Earlier this year, in October, a cybersecurity attack occurred on a 16-year-old high school student in a local neighborhood. This student received a tempting message to a personal cellphone via Google Chat from an unknown account. As soon as the student clicked on the link,

a photo was captured of their face through their phone camera and sent back to the unknown user. A few moments later, this student received another message from the same account with the image of their face on an inappropriate photo with a message followed that said, “if you don’t send $700 to [a bank account] then this photo will be sent to all of your contacts.”

Within a 5-minute time period of the student clicking on the unknown link, this hacker was able to access their camera, their contacts, and possibly more contents within the phone, leaving this student a victim of their first cyberattack. Luckily, this student was willing and able to tell their parents and take the proper measures to re-secure their information and devices. However, the initial attack happened just after midnight and the student did not take any action until almost 5 hours later, leaving the hacker with more time to access more of the phone. Eventually, it was also found that in this 5-hour time frame, the attacker attempted to lock the student's PayPal account and steal more money than the original amount. This student quickly became aware of the true intentions of phishing messages and fell victim to not only a phishing message but also to cyber harassment as well as a ransomware attack. If this student had been previously educated on the common red flags of a scam message and that it is proper cybersecurity procedure to never open links from unknown senders, the student could have possibly avoided this situation.

After learning about this cybersecurity attack, our group quickly decided to use this incident as a learning opportunity. We came up with 5 questions related to cybersecurity and device protection to use in our research. We asked the questions to 15 middle school and high school students ranging from ages 12 to 16, who attend public schools in the Great Bridge area of Chesapeake, Virginia. The five questions included the following: (1) Do you know what cybersecurity is, (2) Do you use the same password for different social media accounts, (3) Do

you use technology daily while in school or for your schoolwork, (4) Have you ever been a victim of an account hack/scam email or know anyone who has, and (5) Have you been taught about technology safety in school on a regular basis? We found that the majority of the younger students, 12 and 13, were not as familiar with the concepts of cybersecurity and device protection as most of the older kids, 14 to 16. However, all of the students admitted to using technology and/or the internet in some way for their schoolwork or personal use. Many also said that internet safety is a regular discussion from some teachers, but not in an official learning capacity such as learning through modules and hands-on practice labs. We asked these questions to get a better understanding of where our local students might be in cybersecurity knowledge, awareness, and internet safety. The following graph is a visual of our findings from this survey.



Since the outbreak of COVID-19, everything in life was moved virtually resulting in the demand and requirement for technology as well as the internet to take off. Even though, in some ways, life has gone back to normal, internet and technology threats are still serious problems.

The internet and technology are being used now more than ever before and as a society, it is necessary to adapt to the changes that have been brought on.

In a reported study, the research found that humans are the top security weakness at an overwhelming 86% followed by technology security weaknesses at 63% (Nobles, C., 2018). Human-related errors are recognized as “Any action leading to an undesired result.” (Nobles, C., 2018). Although making mistakes is a natural part of being human, there are ways to grow and learn how to not make the same mistakes again. This can also be said with properly managing your information on the internet and various devices. Even though these statistics are taken from research concentrated on organizations’ and businesses' cybersecurity awareness, they can be relevant to everyone. Human-related errors in cybersecurity are primarily due to users' lack of knowledge and skills about how to use proper security protocols (Nobles, C., 2018). This lack of knowledge and awareness has the potential to be preventable with proper training and education, not only for kids in school but also for adults in the workforce. Cybersecurity awareness training has become an urgent necessity as cyber incidents caused by human-related errors take up the largest percentage of the reasons for cybersecurity incidents (Al Shamsi, A., 2019).

As stated previously, children and teens spend a vast amount of their time on the internet and their devices, either for schoolwork or entertainment. In a publication by Farzana Quayyum, they discuss the importance of cybersecurity education for children and how to promote knowledge and awareness through gamification. Gamification is a category of games used to educate users with the goal to promote more engagement from people by creating various experiences in everyday life events using game mechanics (Quayyum, F., 2020). Computer games have been around for a long time and have been developed into useful learning tools for children in subjects such as Math, English, and Science. There have been computer games

developed for children based on cybersecurity such as *Cybersecurity Lab*, which was designed to teach children and young adults basic cybersecurity skills, and another called *The Internet Safety*, a website-based game designed to teach topics about safety on the internet (Quayyum, F., 2020). One of the findings by Quayyum led to the understanding that these games are effective and do teach the target audience about cybersecurity awareness and skills, however, the games were found to often become unavailable to the public or just disappear altogether (Quayyum, F., 2020). Other issues found that researchers mention positive feedback of the games but are not evaluating the learning outcomes or presenting conclusive results on the benefit of the games (Quayyum, F., 2020). Although some of these games have had reports of success, there is still a need for a long-term solution to teaching young adults and children about cybersecurity awareness and internet safety.

In the U.S., the development of the NICE framework by the NIST has been a great step toward promoting cybersecurity education. The NICE framework, in addition to being useful to employees and employers, is a useful reference for educators to develop curriculums, degree programs, courses, and more that cover the necessary knowledge, skills, and abilities that are covered in the framework (Newhouse, et al. 2017). Knowledge, skills, and abilities, referred to as KSA, are defined as "the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training" (Newhouse, et al. 2017). In addition to the NIST framework, new computer security competitions called Capture the Flag (CTF) have also been designed to help users gain computer skills (Khan, M. et al., 2022). An example of a relatively successful cyber-education development is the CyberAware application designed for cybersecurity education. The CyberAware app has two main goals: (1) to define and explain to learners the fundamental cybersecurity technologies that are required to keep their

devices protected and keep their passwords safe against threats, and (2) to increase the awareness of learners on privacy issues related to their identity and protecting their personal information that is public on the web (Khan, M., et al., 2022).

Attempting to keep the attention of children for a long period of time is a challenging task. That is why it is important that through this Cybersecurity Curriculum we incorporate ways to keep the attention of students while also delivering important information. The Instructional Design Model (IDM) is a tool designed to translate principles of learning through instruction material, sources of information, learning objectives, and more (Khan, M., et al., 2022). Incorporating our Cybersecurity Curriculum with the IDM has the potential to be the long-term solution for educating young impressionable children on the importance of internet safety and device protection. In the Instructional Design Model, steps include creating the initial set of assumptions such as how the class is taught and how frequently, identifying the scope of instruction such as gathering the resources for the information like journals and publications, Identifying the learner's knowledge level of the topic, and formulating learning objectives (Khan, M.A. et al. (2022)). The IDM structure is similar to how the education system in the U.S. already structures most of the main curriculums, like math, science, etc. The concept of implementing this Cybersecurity Curriculum in high schools and middle schools is not too far out of reach.

Using the research found in different methods of instruction for cybersecurity education such as computer games, and hands-on lab activities, as well as the research and tools already offered such as the NICE framework, combined with this Cybersecurity Curriculum, has the potential to not only benefit the world but protect children from these newfound dangers brought with technology. A cybersecurity awareness program offered by the Ministry of Education in the UAE, a country in the Middle East, started this program to focus on training and educating

students ages 8-10 about online risks and how to properly respond to these risks (Al Shamsi, 2019). Those who participated in this program agreed the information was beneficial and effective. It is important to also recognize that without the repetition of safe cybersecurity practices or any learned skill, the knowledge goes away (Al Shamsi, 2019). This shows that this official Cybersecurity Curriculum has the potential to be the solution for developing the future generation on cybersecurity awareness as well as safe internet and technology use.

Relating to Courses Outside of Cybersecurity

Even though this official Cybersecurity Curriculum has the word 'cybersecurity' in the title, this curriculum can relate to many courses in different disciplines of education. Previously in the literature review, many points were outlining the different dangers and potential risks that the Internet and technology have on children using these devices. One of the most studied topics in education is the study of psychology and behavior. Maturity levels influence many of the behaviors and actions that people take online. For this reason, it is important to have research and information drawn from professionals in subjects such as psychology and childhood development to discover how children and developing adults learn and retain information. However, not only is some of the information that is needed for this curriculum from other subjects, but this curriculum can be relevant to many disciplines and relate to different courses.

This innovation relates to courses such as Website Design and Development, Cyber Law and Policies, Childhood Education, and Psychology. While developing this basis of our curriculum, it was necessary to look into topics outside of just course content and instruction methods such as development theories and legalities of developing educational content for a younger audience. "Cyber Hygiene" is a common term used to describe proper practices for users to maintain their security on the internet and technology. This term is another tool that can

be used to describe the proper behavior that users should follow while on the internet. The research behind the behavior of children as to the reasons why they act the way they do, what benefits their educational and social development, and what deters it. One of the more referred-to theories when talking about childhood education is Jean Piaget's Theory of Cognitive Development.

Piaget's Theory of Cognitive Development is a detailed theory explaining how intelligence changes and develops as children grow (McLeod, 2020). This theory is a great tool for our curriculum to use in order to ensure that we are giving children information that they can fully comprehend and apply in their lives. The theory is broken down into four main stages of development: (1) Sensorimotor stage, birth to 2 years old, (2) Preoperational stage, 2 to 7 years old, (3) Concrete operational stage, 7 to 11 years old, and finally (4) Formal operational stage, ages 12 and up (McLeod, 2020). While everyone does go through these same stages, everyone goes through them at different rates. For this curriculum, we will be focusing on Piaget's fourth stage of this theory, the formal operations stage, which is the age range of where our primary target group will be. In psychology courses, implementing these theories into everyday situations and breaking down the ethical reasoning behind the decisions and actions of people is very similar to cybersecurity. In cybersecurity, there is a constant cycle of assessments of online behavior and trends to better assess security measures.

In our initial problem, we address that there is a lack of cybersecurity awareness and knowledge among most internet users, especially children, and young adults. This topic is very interdisciplinary, deals with multiple areas of study, and can be applied to any professional field that requires technology. For example, right now I work as an office administrator for a facility maintenance company. From the title, one would not think that cybersecurity would relate but I

use technology every day and have to use troubleshooting techniques that I have learned in my networking classes and cyber operations classes to update systems used for payroll. From an interdisciplinary perspective, knowing standard operating procedures for everyday-used devices is why this curriculum could benefit more than students who are interested in technology. Much of the material covered in classes such as psychology and childhood development is a huge part of implementing into this curriculum to make it successful.

Determining Effectiveness

The primary objective of this curriculum is to spread cybersecurity knowledge and awareness as well as internet and technology safety to kids and young students. This official Cybersecurity Curriculum has the potential to not only lower human-related errors in cybersecurity but also could benefit kids' daily lives as well as prepare them for the inevitable technological advancements to come. Recently schools have focused primarily on the physical safety of children and while this is extremely important, so is the virtual safety of students. One way this official Cybersecurity Curriculum can be determined effectively is through annual national surveys sent to every public school using the curriculum. Using this research, we can use this information to see if students seem to be improving in their understanding of cybersecurity and internet safety. Many teachers use this method in schools to see where the weaker areas of knowledge are in their classes so they can make sure to spend more time on the topic. If the results found that students did not seem to be retaining any more information regarding cybersecurity and internet safety, then we can learn where we need to re-evaluate our information in the curriculum. However, as the research has shown, this curriculum is a necessity in providing students with information that will keep them safe while using technology. Ensuring students are provided with the education and resources to learn more about the internet and the

devices they use every day will inevitably make children safer from falling victim to cyber-attacks. Another way that we will see this Cybersecurity Curriculum is effective is by seeing the percentage of cyber-attacks caused by human-related errors decrease across the nation. This is a possibility because the main reason that human-related errors are the leading cause of cybersecurity attacks is the lack of knowledge regarding proper cybersecurity measures. With students beginning their education on these proper cybersecurity measures and going through them throughout their education career, there is a better chance of fewer human-related errors.

Making This Cybersecurity Curriculum A Reality

The long-term goal is to make this official Cybersecurity Curriculum for middle schools and high schools throughout the nation. For now, our first milestone is to implement this Cybersecurity Curriculum in the local state of Virginia. The Virginia Department of Education (VDOE) creates and administers SOL-based learning for Virginia Public Schools for various courses. SOL or the Standards of Learning is the set of expectations for student learning and achievement in Virginia (Education, V. D.). In addition to math, science, history, and health, the VDOE SOL also outlines a Computer Science Curriculum. Currently, on the VDOE website, there is an SOL guideline for Computer Science for grades K-8 with topics in Computer Science Foundations, Principles, and Programming (virginia.gov). This section of the SOL does not have a standard test affiliated, however, the outlines and documents are available as a resource.

In order to make our Cybersecurity Curriculum a reality for Virginia Public Schools, the best, and what seems to be the most efficient way, would be to have it implemented in the Virginia Department of Education SOL. Before this can happen, there are several steps to be taken. First, as we have already made abundantly clear, our reason for creating this Cybersecurity Curriculum is to educate middle school and high school students on the

importance of safe internet and device use as well as cybersecurity methods to protect their information and devices. Topics of learning include but are not limited to; the basics of device protection, password security, cyber-attacks such as phishing attacks, viruses, worms, ransomware, and any other topics deemed necessary to help educate young students on the importance of internet safety, cybersecurity, and other Information Technology (IT) devices.

Another important part of implicating this curriculum effectively is ensuring that the information is delivered to the students in ways that enhance their learning. Finding professionals in the cybersecurity field as well as having experience as an educator, has proven to be the more challenging part of creating this curriculum. A way to solve this issue is by instilling ways to ensure that cybersecurity education programs are offered to teachers and anyone else in order to grow national cybersecurity awareness among the citizens of the U.S. This could be a possible solution to the lack of cybersecurity educators because training teachers on how to effectively use the Cybersecurity Curriculum to educate young students would also help ensure the success of the curriculum.

From research regarding curriculum development, there have been many different ways that curriculums have been implemented in the past. The four main steps to follow include planning, organizing, implementing, and reviewing. Using these four steps as a guide we can ensure our Cybersecurity Curriculum will pass VDOE SOL. In our planning step, we would note our reason for creating this curriculum, as well as the information that will be included in each section of our curriculum. Step two, organizing, is when we would develop the instructional plan and the delivery method of how the information in the curriculum will be given to the students. This includes hiring teachers, creating modules, quizzes, hands-on labs, study guides, PowerPoints, lectures, and weekly lesson plans for teachers, as well as the expected level of

knowledge that the students will have after the curriculum is complete. In step three, we will implement these plans and modules in small schools to start educating middle school and high school students on cybersecurity. After the first school year of this Cybersecurity Curriculum, we would be able to move into step four. In step four, we can review the growth of cybersecurity knowledge and awareness by distributing surveys to the students who participated in the course. Using the information gathered in these surveys, we will be able to determine the effectiveness of this information on young students. If the reports show that students benefit from this education, then we will be able to use this to show that the implementation of our Cybersecurity Curriculum is effective and have it implemented in other schools across the nation.

Next Steps

Now that we have developed the outline, and the course structure and talked about the necessary training of teachers and staff, the next steps involve making this curriculum a sustainable solution for spreading cybersecurity awareness. In order to keep this curriculum up to date on relevant cybersecurity issues, there must be a way to ensure that the content of the curriculum is being maintained. One of the ways that this can happen is by ensuring that the schools have the proper resources that are available to them to properly update their course content. This can happen through a cybersecurity curriculum-based section on the VDOE site much like they already have their course structured now. It is important for education developers to also recognize the importance of having the proper team in place to develop this content for teachers. Much like the NIST Cybersecurity Education Conference, having an annual review of the curriculum to ensure the content is relevant to students is a great way to ensure that this curriculum will be sustainable in developing the next generation of technology users. Another way we want to continue our development is by creating an app for students to access outside of

school. Not only would this app be available on any mobile phone with an app store, but it would also be available for desktop and laptop download to make it accessible for all students. This app could be for both educational activities for teachers to assign for grades or could be for parents and children to learn from and expand their knowledge about cybersecurity and technology. There would be a setup for studying and learning that would have flashcards, practice quizzes, and real-life cybersecurity scenarios where the user has to decide what they would do in this situation. The implementation of hands-on labs in this app would also help students engage with even more advanced real-world scenarios such as coding techniques and Wireshark practice. This curriculum can be utilized in so many different ways to ensure that children and students are receiving the education they need to improve their technical knowledge and skills.

Self-Reflection

To Whom It May Concern:

In this innovation, we have developed an official cybersecurity curriculum for middle schools and high schools that we hope to have implemented in schools around the Hampton Roads area of Virginia and eventually lead to the implementation of this curriculum around the nation. In this curriculum, we will focus on educating young students on the importance of safe technology and internet use as well as increasing their cybersecurity knowledge, skills, and awareness. We have found research that suggests that the age of children in middle schools and high schools is their most crucial development time to learn life skills and techniques. Technology is the most important aspect of life today and is involved in everything that we do on a day-to-day basis including working, socializing, and learning. That is why teaching young, impressionable students the importance of technology safety and developing cybersecurity skills will help keep them safe now and in the future. Students will find value in this curriculum

because they will take away new skills and knowledge to possibly prevent them from being the next victim of a cyber-attack. As the team of developers for this curriculum, we are open to editing and adjusting the content or outline of this curriculum as higher education officials see fit. We also recognize that there is a noticeable funding shortage for curriculums across the curriculums, but with organized fundraisers and collected donations for our cybersecurity curriculum, much like schools do already for sports, clubs, and teams, this can be resolved. We have seen that this information is critical to teach students and hope that this curriculum will help be the sustainable, long-term solution to spread cybersecurity knowledge, internet safety, and proper device use. Thank you for taking the time to read this overview of our innovation for an official cybersecurity curriculum and hope that we have the opportunity to share this innovation with more officials to eventually have this developed into a reality.

Respectfully,

Mackenzie Coleman
Old Dominion University
Partners; Sarah Noble and Rahilkumar Patel

Acknowledgments

I would like to thank my group partners, Sarah Noble and Rahilkumar Patel for such diligent work this semester as we developed our innovation as well as the student who was willing to share their cyber-attack story with us to help our survey and project research.

References

A guide to curriculum development: Purposes, practices, procedures overview. (n.d.). Retrieved November 29, 2022, from https://portal.ct.gov/-/media/SDE/Health-Education/curguide_generic.pdf

Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud*, *3*(2), 8-29. https://www.researchgate.net/profile/Arwa-A-Al-Shamsi/publication/342887888_Effectiveness_of_Cyber_Security_Awareness_Program_for_young_children_A_Case_Study_in_UAE/links/5f0c14fa299bf1881619832d/Effectiveness-of-Cyber-Security-Awareness-Program-for-young-children-A-Case-Study-in-UAE.pdf

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian Environment. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz001

Editor, C. S. R. C. C. (n.d.). *Cybersecurity - glossary: CSRC*. CSRC Content Editor. Retrieved November 27, 2022, from https://csrc.nist.gov/glossary/term/cybersecurity

Education, V. D. of. (n.d.). *Virginia Department of Education*. VDOE :: Virginia Department of Education Home. Retrieved November 29, 2022, from https://doe.virginia.gov/

Kamenetz, A. (2019, October 31). *It's a smartphone life: More than half of U.S. children now have one*. NPR. Retrieved September 29, 2022, from https://www.npr.org/2019/10/31/774838891/its-a-smartphone-life-more-than-half-of-u-s-children-now-have-one

Khan, M.A., Merabet, A., Alkaabi, S. *et al.* Game-based learning platform to enhance cybersecurity education. *Educ Inf Technol* 27, 5153–5177 (2022). https://doi.org/10.1007/s10639-021-10807-6

Mcleod, S. (2020, December 7). *Jean Piaget's theory and stages of cognitive development*. Piaget's Theory and Stages of Cognitive Development. Retrieved December 2, 2022, from https://www.simplypsychology.org/piaget.html?campaignid=70161000000RNtB&vid=2120483

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. https://doi.org/10.6028/nist.sp.800-181

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Quayyum, F. (2020). Cyber Security Education for children through Gamification: Challenges and Research Perspectives. *Methodologies and Intelligent Systems for Technology Enhanced Learning, 10th International Conference. Workshops*, 258–263. https://doi.org/10.1007/978-3-030-52287-2_26

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

Sulaiman, N. S., Yacob, A., Aziz, N. S., Samsudin, N., Mohamed, W. A., Rahman, S. A., Hassan, W. N., Nasir, A., Wahab, S. F., & Othman, W. R. (2021). A review of Cyber Security Awareness (CSA) among Young Generation: Issue and countermeasure. *Proceedings of International Conference on Emerging Technologies and Intelligent Systems*, 957–967. https://doi.org/10.1007/978-3-030-85990-9_76