How has the U.S. contributed to the growth of cybersecurity education and knowledge and how does it continue to do so?

Mackenzie Coleman

IDS 300W: Interdisciplinary Theory and Concepts

Dr. Patricia Oliver

Abstract

Technology has undoubtedly taken the 21st century by storm in all aspects of life. Especially since COVID-19, technology has changed the way we think, act, learn, talk, develop relationships and so much more. These amazing advancements have especially been seen in the education system. With so many students required and still choosing to take classes online, the demand for technology, including devices and the internet, has increased dramatically. In recognition of this rapid use of technology, there have been many programs and courses dedicated to learning and understanding technology, for example, engineering and robotics. However, cybercriminals have found ways to use this technology to damage people's lives. The growth of cyber-attacks and the countless victims of these attacks, not only in the United States but all over the world, is one of the many reasons that cybersecurity is taken so seriously. Cybersecurity has become one of the most demanding fields over the past decade. This is because the lack of education and knowledge of the technology that people use every day is the norm. The objective of this paper is to highlight why cybersecurity is a crucial topic in the education system and to show what the United States has done to contribute to the expansion of cybersecurity knowledge and awareness in all schools and how different disciplines view cybersecurity education.

Keywords

Education Technology, cybersecurity, education, psychology, interdisciplinary, sociology, information technology

There is no question that over the last several decades, technology has taken over the world from cell phones, laptops, desktops, wireless headphones, and more. Although society has made amazing achievements with technology and the internet, there has also been a rise in cybercrime through various forms of cyber-attacks. From phishing emails and identity theft to different viruses and worms that end up leaking private information from accounts or destroying devices altogether. During a survey taken in 2013 by a non-profit organization called AARP, the research found that nearly 79% of Americans who use the Internet shared that they are scared or nervous about being victims of scams on the internet; however, many were found to avoid taking basic precautions for themselves and their devices (Sauer, 2014). This leaves the question of what is being done to promote cybersecurity education to expand the necessary knowledge of safe device and internet use. Cybersecurity education is not only necessary in schools across grade levels but has proven to be highly necessary for businesses and organizations as well. This paper will highlight concepts and theories from disciplines including, education technology, education, psychology, and sociology regarding cybersecurity education.

It is important to address this question from an interdisciplinary perspective because technology is not specific to any one discipline. Technology and the internet are used across professions in a variety of ways, which is why is it important for all users to know safe practices for device and internet use. To best address the necessary improvements in cybersecurity knowledge and awareness that are being implemented, it is necessary to have an interdisciplinary approach with various perspectives. Human-related errors are the leading factor in cyber-security-related incidences across the world. This is primarily due to the lack of proper cybersecurity awareness and knowledge. Cybersecurity training and education have become a top priority in attempting to mitigate these errors, but this requires a change in the way some users think and act while online which involved research in psychology and sociology development.

According to the Oxford dictionary, psychology is defined as the scientific study of the human mind and its functions, especially those affecting behavior in a given context. The study of psychology has proven to enhance the understanding of human behavior at all ages as well as brain development and comprehension. Psychology has also been used to understand online behavior and decisions and how users interact with devices as well as risks online. The Department of the Army recognizes three layers within the cyber domain: the physical layer, consisting of hardware and infrastructure supporting our networks, the logical layer, which includes any device with an internet protocol address, and the social layer, consisting of the human and cognitive aspects. (Dawson, J. & Thompson, R., 2018). The social layer is a key concept to understanding the cyber domain in real-world scenarios because this is where humans are interacting the most. “The complexity of human interactions across layers create the uniqueness of the cyber domain, and it is understanding these human interactions that create underlying vulnerabilities on the network” (Dawson, J. & Thompson, R., 2018). Psychology is critical in understanding cybersecurity and the potential risks and vulnerabilities of online behavior. A part of developing an effective cyber workforce is having a deep understanding of human behavior, both online and in real life (Dawson, J. & Thompson, R., 2018).

Not only can research from psychology benefit cybersecurity education in how students are taught but psychology can also help identify common behavior patterns of cybercriminals online. Psychology is a broad topic, with many areas of research that can be pertinent to “multi-faceted” issues such as cybersecurity (Taylor-Jackson, J., et al., 2020). Cyber-attacks, such as phishing emails as previously mentioned, can be classified as a form of psychological manipulation because the attacker is attempting to trick the user into clicking a persuasive, yet also false, link or attachment (Taylor-Jackson, J., et al., 2020). This form of cyber-attack is also relevant to the Protection Motivation Theory. The psychological theory explains the fear appeal that is being used to motivate a user into taking actions that put them at risk (Taylor-Jackson, J., et al., 2020). Some also refer to cybersecurity not just as a form of practice but as a mindset while using technology.

Society is constantly evolving and changing as the world progresses into new eras, such as this new age of technology. Sociology is the study of the development, structure, and functioning of human society. Cybercrime is now one of the more common forms of crime today. Hirschi's Social Bonding Theory explains that antisocial behavior is a result of an individual's weak ties to conventional society (Back, S. et al., 2018). This theory has been used to explain crimes committed by kids and young adults but also by grown adults as well. Researchers: Back, Soor, and LaPrade used a survey on middle school and high school students across eight countries and found that juvenile hackers from all countries seemed to have been influenced by similar factors or low self-esteem and attachment to parental supervision for their hacking behaviors (Back, S. et al., 2018) (Choi, K.-Shick, & Lee, C. S. (2018). Due to the increase in technology, the field of cybersecurity has increased exponentially in demand for cybersecurity professionals around the world. However, in society, this field is not diversified to promote more individuals to feel like individuals can be successful in this field. In 2018, the professionals hired included 24.9% women, 12.3% African Americans, and 6.8% Latinos (Mountrouidou, X., et el. 2019).

The science disciplines require teams made up of people with a variety of diverse backgrounds and experiences to gain insights and draw new ideas to solve solutions and as cybersecurity is considered, as well as many other disciplines, a science (Mountrouidou, X., et el. 2019). Diversity is important in society to not only promote different ideas and insights from various backgrounds but also to promote to younger generations that no matter their background or ethnicity, they too can be successful in not only pursuing a career in cybersecurity but would be encouraged to learn more about it in the present. Using the basis of cultural responsiveness, which includes all forms of diversity including gender and race, is a way to improve diversity in cybersecurity education (Mountrouidou, X., et el. 2019). One example of a possible reason for the under-representation of females in technology fields is that more middle school boys are already exposed to computing and technology experiences than girls (Mountrouidou, X., et el. 2019). In society, it is important to have a variety of representations to promote diversity among not only young students but also young adults who are new to the cybersecurity field.

Many educational theories have been developed based on psychological theories and ideas such as the cognitive theory of development and behaviorism. Recently, learning theories and models have been applied to include research into effective methods of cybersecurity education. The concept of combining learning as well as entertainment has appeared in recent years through new terms such as, “learning by playing, “Game-Based Learning”, and “Educational Entertainment” (Khan, M., et al. 2022). This is a popular form of learning that has been developing consistently over many different methods to increase education tools and resources. Game-based learning is the method of using a game as a part of the learning process (Khan, M., et al. 2022). Many game-based learning platforms have been used to teach users the importance of internet safety as well as cybersecurity awareness. One of the main objectives of game-based learning methodology is to give students the right tools to learn various cybersecurity challenges (Khan, M., et al. 2022). Dr. Te-Shaun Chou, an Associate Professor in the Department of Technology systems at East Carolina University developed a cybersecurity learning system that included a training program to educate students on cyber-attacks and prevention methods based on several learning techniques including game-based learning with hands-on virtual labs (Chou, 2019). In the research findings, it was proven that the students who fully completed all hands-on labs, students were able to advance their skills and understanding of cybersecurity (Chou, 2019). Education technology is a popular term defined by the Association for Educational Communications and Technology (AECT) as the study and ethical practice of facilitating learning and improving performance by creating, using, and managing appropriate technological processes and resources (Huang, R., et al., 2019). Education technology has become a crucial piece of education today. Students are able to use technology to advance their technical skills not only in school but in everyday life. The ARCS (Attention, Relevance, Confidence, and Satisfaction) Model of Motivational design, an education theory created by John Keller, is a problem-solving approach to designing the motivational aspects of learning environments to promote motivation for students to learn. (Huang, R. et al. 2019). Many cybersecurity educational games and game-based learning techniques are centralized around this ARCS model of motivation to ensure educators are keeping students engaged and responsive to the information given to them.

Cybersecurity has been recognized as an important topic for employees in the workforce and an important topic for students in all grades as well. Cybersecurity education is necessary regardless of individuals, organizations, or places because cybercrime can occur anywhere (Rahman N. A. A., et al 2020). Cybersecurity education does not only pertain to technical studies, such as malware analysis and network security but is not starting to require an understanding of traditional technology and non-traditional skills. (Jacob, J., et al., 2019). There have been steps in creating more opportunities for cybersecurity education. For instance, in the United States, the National Initiative for Cybersecurity Education (NICE) Framework was developed by the National Institute of Standards and Technology (NIST) as well as government, academia, and the private sector to promote cybersecurity education, training, and development (Brecht, 2021). Human error is one of the leading causes of cybersecurity-related incidents and attacks. Because of this, cybersecurity education involved psychology and sociology-related topics as much as cyber topics. Social psychology is a study of how a person's attitudes and behaviors are affected by others which gives cybersecurity professionals a better understanding of cybercriminal behavior online (Thackray, et al. 2016). Social psychology can be used as a tool to further research into detecting potential internet risks and cybercriminals for law enforcement as well as everyday users.

From a sociological perspective, cybersecurity education is seen as beneficial to not only members of society but also to preventing cyber-attacks on societal infrastructure in the nation. Education systems have begun incorporating technology programs into their facilities such as STEM (Science, Technology, Engineering, and Math) learning which also includes a computer science-based curriculum (Virginia Department of Education). However, cybersecurity has yet to have a specific curriculum implemented in all public schools in a formal learning capacity. Psychology theories and concepts of human behavior have also proven to be useful in cybersecurity education for the purpose of educating users about common cyber-attack techniques as well as detecting cybercrime prior to an attack. Cybersecurity education is truly an interdisciplinary study that requires the attention of not only the disciplines mentioned in this review but from more disciplines such as ethics, law, criminology, and any other discipline that can promote cybersecurity awareness, knowledge, techniques, and skills.

In conclusion, Cybersecurity education has been promoted and encouraged through different methods such as game-based learning, national initiatives, and research methods conducted as to why it is beneficial to both schools and businesses. NIST'S NICE Framework has been used as an interdisciplinary tool that has been developed for businesses, organizations, educational facilities, and individuals to access and use to learn the necessary skills for internet and device safety. From the research publications and reviews regarding cybersecurity education, there is a conscientious that because of the potential risks and threats the internet poses to everyone on a daily basis, proper cybersecurity training and education is a necessity. Cybersecurity education through game-based learning has proven to have a positive effect on students and their cybersecurity awareness and overall knowledge. Cybersecurity education is a necessity for the safety of users now as well as in future generations.

References

Back, S., Soor, S., & LaPrade, J. (2018). Juvenile hackers: An empirical test of self-control theory and social bonding theory. *The International Journal of Cybersecurity Intelligence and Cybercrime*, *1*(1), 40–55. https://doi.org/10.52306/01010518vmdc9371

Brecht, D. (2021, November 3). *What is the Nice Cybersecurity Workforce Framework?* Infosec Resources. Retrieved December 5, 2022, from https://resources.infosecinstitute.com/topic/what-is-the-nice-cybersecurity-workforce-framework/

Choi, K.-shick, & Lee, C. S. (2018). The present and future of cybercrime, cyberterrorism, and cybersecurity. *The International Journal of Cybersecurity Intelligence and Cybercrime*, *1*(1), 1–4. https://doi.org/10.52306/01010218yxgw4012

Chou, T.-S. (n.d.). Multi-learning techniques for enhancing student engagement in Cybersecurity Education. *2019 ASEE Annual Conference & Exposition Proceedings*. https://doi.org/10.18260/1-2--33127

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful Cyber Performance. *Frontiers in Psychology*, *9*. https://doi.org/10.3389/fpsyg.2018.00744

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/

Huang, R., Spector, J. M., & Yang, J. (2019). Educational Technology. *Lecture Notes in Educational Technology*. https://doi.org/10.1007/978-981-13-6643-7

Hwang, M. I., & Helser, S. (2021). Cybersecurity educational games: A theoretical framework. *Information & Computer Security*, *30*(2), 225–242. https://doi.org/10.1108/ics-10-2020-0173

Jacob, J., Peters, M., & Yang, T. A. (2019). Interdisciplinary cybersecurity: Rethinking the approach and the process. *Advances in Intelligent Systems and Computing*, 61–74. https://doi.org/10.1007/978-3-030-31239-8_6

Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-Based Learning Platform to enhance cybersecurity education. *Education and Information Technologies*, *27*(4), 5153–5177. https://doi.org/10.1007/s10639-021-10807-6

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T. (2019). Securing the human. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*. https://doi.org/10.1145/3344429.3372507

Rahman, N. A., Sairi, I. H., Zizi, N. A., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Sauer, J. (2014, March 1). *Caught in the scammer's net: AARP survey of American adults age 18 and...* AARP. Retrieved November 15, 2022, from https://www.aarp.org/research/topics/economics/info-2014/internet-fraud-victimization-attitudes-behavior-national.html

Taylor-Jackson, J., McAlaney, J., Foster, J. L., Bello, A., Maurushat, A., & Dale, J. (2020). Incorporating psychology into Cyber Security Education: A pedagogical approach. *Financial Cryptography and Data Security*, 207–217. https://doi.org/10.1007/978-3-030-54455-3_15

Thackray, H., McAlaney, J., Dogan, H. Z., Taylor, J., & Richardson, C. N. (2016). Social Psychology: An under-used tool in cybersecurity. *Electronic Workshops in Computing*. https://doi.org/10.14236/ewic/hci2016.64