The Importance of Cybersecurity Education for Half of Everyday User

Cristina Laing

Cybersecurity principles

CYSE 600

August 6, 2021

Dr. George Mikulski

Author Note

This is my own work and has been done solely by me. This paper has been written for the Old Dominion University’s CYSE 600 Cybersecurity Principles class and not used for any other purpose.

Cristina Laing

Abstract

This paper focuses on the importance of education about cybersecurity for the everyday user. More importantly, this paper focuses on the education of women and girls on the topic of cybersecurity. The reasons why there is a lack of females in computer science fields such as cybersecurity. The consequences of the lack of women in cybersecurity and how it has become a national security problem. This paper is also an analytical review of three different studies that aim to answer the questions (1) Where are all the girls? (2) Why so few girls? (3) what can we do to attract women and girls into the cybersecurity field. The paper title, The Importance of Cyber Education for Half of the Everyday Users, focuses on how females make up half the population in this country yet only make 11% of the workforce in areas such as cybersecurity.

The Importance of Cybersecurity Education for Half the Everyday Users

Introduction

The IT/cybersecurity department inside an organization works hard to keep the organization's, employee's, and customer's information safe. Nevertheless, researchers often say humans are the weakest link in the security chain (Ricci, Breitinger, & Baggili, 2019. Part of the problem is that users are responsible for adjusting their privacy settings, choosing strong passwords, and complying with security policies (Zhang-Kennedy and Chiasson, 2021). These decisions require informed decision-making, foresight, and tradeoffs based on users' existing knowledge about online risks and the technology they use (Zhang-Kennedy and Chiasson, 2021). Therefore, improving non-expert end-users knowledge and awareness is an essential step towards Cybersecurity (Zhang-Kennedy and Chiasson, 2021).

The importance of education is thought to be noticeable, but many times, we do not stop and put thought into the power education has to change lives. Many governments have realized that investing more in the education of their citizens gives their country a competitive edge in the global workforce. Some other areas where education helps:

1. Eliminating poverty
2. Safety and Security against crime
3. Prevention of Wars and terrorism
4. Commerce and Trade
5. Law and Order
6. Women Empowerment
7. Upliftment of economically weaker sections of society
8. Communication (The Asian School, 2021).

The global challenge for education is not just about providing access but also ensuring progress. In today's hyperconnected world, cybersecurity education is critical for governments, organizations, and individuals alike. We hear the term more and more these days. Still, only a few know what the term entails. According to the Cybersecurity and Infrastructure Security Agency or CISA, Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or unlawful use and the practice of ensuring confidentiality, integrity, and availability of information (CISA, 2009). Nowadays, it seems every component of everyday life has an aspect of itself in cyberspace; communication (e.g., email, smartphones, tablets), entertainment (e.g., interactive video games, social media, apps), transportation (e.g., navigation systems), shopping (e.g., online shopping, credit cards), medicine (e.g., medical equipment, medical records), and the list goes on (CISA, 2009). Information flow is constant either on personal computers, smartphones, tablets, or someone else's system beyond an individual user's control.

One key term in Cybersecurity is a risk. *Risk* is defined as the possibility of loss or injury (Merriam-Webster, n.d.). In the context of Cybersecurity, there are many risks, some more serious than others. For example, the risks to an individual user include "malware erasing your entire system, an attacker breaking into your system and altering files, an attacker using your computer to attack others, or an attacker stealing your credit card information and making unauthorized purchases" (CISA, 2009). Fortunately, there are steps users can take to minimize the risks of cyberattacks, better known as best practices:

- Keep software up to date. Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates (CISA, 2009).

- Run up-to-date antivirus software. A reputable antivirus software application is an essential protective measure against known malicious threats. It can automatically detect, quarantine, and remove various types of malware. Be sure to enable automatic virus definition updates to ensure maximum protection against the latest threats (CISA, 2009).
- Use strong passwords. Select passwords that will be difficult for attackers to guess and use different passwords for different programs and devices. It is best to use long, strong passphrases or passwords with at least 16 characters (CISA, 2009).
- Change default usernames and passwords. Default usernames and passwords are readily available to malicious actors. Change default passwords as soon as possible to a sufficiently strong and unique password (CISA, 2009).
- Implement multi-factor authentication. *Authentication* is a process used to validate a user's identity. Attackers commonly exploit weak authentication processes. Multi-factor authentication uses at least two identity components to authenticate a user's identity, minimizing the risk of a cyberattacker gaining access to an account if they know the username and password (CISA, 2009).
- Install a firewall. Firewalls may be able to prevent some types of attack vectors by blocking malicious traffic before entering a computer system and restricting unnecessary outbound communications. Some device operating systems include a firewall. Enable and properly configure the firewall as specified in the device or system owner's manual (CISA, 2009).
- Be suspicious of unexpected emails. Phishing emails are currently one of the most prevalent risks to the average user. The goal of a phishing email is to gain information

about the user, steal money from you, or install malware on your device. Be suspicious of all unexpected emails (CISA, 2009).

According to Cybersecurity Ventures, there are 3.5 million unfilled cybersecurity jobs globally (Cybercrimemag, 2020). This number might seem extreme however it is a troubling reality. There is a shortage of cybersecurity professionals and a workforce-skills gap in those already in the field. So much so that President Biden has made Cybersecurity, a critical element of the Department of Homeland Security's (DHS) mission, a top priority for the Biden-Harris Administration at all levels of government (DHS, 2021). In March of 2021, Secretary Mayorkas of DHS spoke at a conference and openly discussed challenges the government has had with cybercrime and the vision he has for the country's cybersecurity landscape. Below are the challenges spoke by the Secretary of DHS:

1. The US government cannot achieve the nation's cyber resilience alone (DHS, 2021).
2. The US government got hacked in 2020, and it was not noticed for months (DHS, 2021).
3. The US government seeks to speak with one voice but too often speaks through different channels, confusing and distracting those who need to take fast action (DHS, 2021).

Following the challenges, the Secretary of DHS described five principles essential to the cybersecurity efforts. The fifth and final principle focused on integrating diversity, equity, and inclusion: throughout every aspect of work, especially in Cybersecurity. First, Secretary Mayorkas stated that "developing sound public policy requires diverse perspectives from communities that represent America" (DHS, 2021). He followed by saying, "It requires equal access to professional development opportunities to fill the current half million cyber vacancies across our country and to prevent future shortages that threaten our ability to compete" (DHS, 2021).

In other words, the government of the United States acknowledges a lack of cybersecurity professionals that are needed to protect this great country's assets, and there is no better way to alleviate this issue than educating its citizens. However, the government also realizes that it is not enough to just educated its citizens but to focus on minorities, people of color, and women who make up half of the country's population. Therefore, the DHS has partnered up with schools such as Hampton University and with organizations such as the Girl Scouts of the USA to advance Cybersecurity education to the public and the most vulnerable demographic, women.

Literature Review

"I Can Actually Be a Super Sleuth": Promising practices for Engaging Adolescent Girls in Cybersecurity Education

Jethwani, Memon, Seo, and Richer, 2017, research conducted through a focus group of adolescent girls in a cybersecurity summer program, examine the following questions (1) How do adolescent girls perceive the cybersecurity field? And (2) What are the promising practices that engage girls in cybersecurity education? Guided by ecological and social role theories, findings reveal that single-sex collaborative settings with encouraging and supportive teachers and female mentors are practices that contribute to girls' increased interest in the field of Cybersecurity (Jethwani, Memon, Seo, and Richer, 2017). Findings also suggest that emphasizing creative and collaborative problem-solving processes and the real-world application inherent to Cybersecurity are likely to increase girls' engagement in the field (Jethwani et al., 2017). Results have implications for educators, researchers, and policymakers aiming to close gender gaps in computer science and build interest in Cybersecurity, an area of critical national need (Jethwani et al., 2017).

The authors open the paper by explaining how to immerse society is in information technology and how it plays an increasingly important role in our lives. However, they state that ubiquity and trustworthiness are what is becoming the norm. Moreover, as previously mentioned, the authors acknowledge the nation's acute shortage of cybersecurity professionals in the workforce. However, as in all areas of computer science, women are vastly underrepresented in the field (Jethwani et al., 2017). Jethwani et al. state that evidence suggests that girls are becoming disengaged with computers science in adolescence; even though girls are becoming increasingly more involved in other STEM-related subjects, they are less likely than boys to pursue computer science (Jethwani et al., 2017).

The unique set of challenges presented by Jethwani et al. are:

- Girls in computer science classes tend to express less confidence and rate their computer abilities lower than boys, even when actual achievement levels are similar Jethwani et al., 2017).
- Girls are less positive in their perceptions of computing careers than boys and perceive computer science fields as masculine and isolating (Jethwani et al., 2017).
- Girls also experience lower feelings of belonging in computer science courses than boys due to lower feelings of fitting in with computer science stereotypes.
- Limited access to female role models in computer contexts often confirms misperceptions about the field and further hinders girls' participation in the field (Jethwani et al., 2017).

Jethwani et al., the two-year study resulted in four promising principles that are likely to improve girls' interest in Cybersecurity.

1. Single-Sex Collaborative Settings. Promotes supportive peer relationships that encourage girls to build their confidence and skills in Cybersecurity (Jethwani et al., 2017).

2. Supportive Teachers That Emphasize the Process of Knowledge. Exposure to content through encouraging, available, and supportive teachers, girls felt confident that, with practice, they could build their understanding of how they might solve cybersecurity problems. Regardless of their prior skill level, knowing that they were accepted kept the girls from giving up. Understanding that their cybersecurity skills could be improved triggered a more profound interest in the material (Jethwani et al., 2017).
3. Presence of Female Mentors Challenges Stereotypes About the Field. Girls explained that cybersecurity women speakers and professionals were "powerful" and "inspiring" and "relatable" (Jethwani et al., 2017).
4. Emphasis on the Real-World Application and Creative Qualities of Cybersecurity. Findings suggest that the real-world application and perceived creative processes involved in Cybersecurity make the field socially relevant and particularly appealing to girls (Jethwani et al., 2017).

Cybersecurity needs women

In Winifred Poster's research of the underrepresentation of women in Cybersecurity, the author explains how even though women only represent 11% of cybersecurity professionals worldwide, it was not always the case. The author states that "Safeguarding our lives online requires skills and experiences that lie beyond masculine stereotypes of the hacker and soldier" (Poster, 2018). The Poster stresses the issue of computer hacking in today's society as being widespread and damaging. More worrisome, Poster states that cybercrime exacerbates inequalities (Poster, 2018). For example, a million more US women than men had their identities were stolen in 2014 (Poster, 2018). People of African American and Latino descent are, on average, two to three times more likely than white people to be victims of fraud related to debt or income (Poster, 2018). Moreover, women and girls are more likely than men to be targets of 'remote sexual abuse' - coerced into posing nude online or stalked through the Internet (Poster, 2018).

The Poster emphasizes that Cybersecurity's future depends on its ability to attract, retain, and promote women, who represent a highly skilled and under-tapped resource (Poster, 2018). The discipline also needs to learn about women's experiences as victims of cybercrime and the steps needed to address the imbalance of harm (Poster, 2018). The Poster study also found that the proportion of women in computer science grew until the mid-1980s until the personal computer came out for the public but was advertised towards men. Even so, the Poster highlights four-way in which the field of Cybersecurity should adapt in the present:

1. Acknowledge women's contributions. Women have been working in Cybersecurity for a century. However, many of their stories have been sidelined because of the secrecy of the work, its wartime contexts, or because male colleagues have been put in the limelight instead (Poster, 2018).
2. Recognize diverse expertise. Despite being few in number, female candidates for cybersecurity jobs tend to be more educated than their male counterparts. Women professionals are more likely to have a master's degree or higher (51% for women globally, compared with 45% of men). Women also tend to bring broader expertise (Poster, 2018).
3. Shed sexist image. The two fields most closely associated with Cybersecurity - IT and the military - are plagued by cultures that are hostile towards women.
4. Realize that women and girls are prime targets of cybercrime. Women in the United States were 26% more likely than men to experience identity theft in 2008, often

involving the fraudulent use of a bank account or credit card. Some cybercrimes, such as 'sextortion, are directed at women and girls (Poster, 2018).

Gender-based Investigation of Stereotypical Barriers in Management Information Systems Profession

Yagmur and Jaideep tackle the lack of women in management information systems (MIS) by examining the effects negative stereotypes have on degrees and careers in the computer science field. The study investigated students' stereotypical images of MIS professionals and compared male and female students' perceptions (Yagmur and Jaideep, 2018). It also examined whether the introductory level course played a role in altering female and male students' stereotypical image of MIS professionals (Yagmur and Jaideep, 2018). The findings carry several important implications for MIS programs and educators (Yagmur and Jaideep, 2018).

The authors note that "Negative stereotypes are assumed to be one of the significant barriers preventing students from pursuing Information Technology (IT) degrees and careers (Yagmur and Jaideep, 2018). Furthermore, a significant worldwide problem, the underrepresentation of women in IT, has also been linked to negative stereotypes (Yagmur and Jaideep, 2018). In today's information age, overcoming these stereotypes to attract more students to the IT field is extremely important for advancing our economy and society (Yagmur and Jaideep, 2018). Therefore, the authors propose that it is necessary to reduce the entry barriers and attract more students in general and more female students to pursue degrees in various computer science fields, such as Cybersecurity.

Stereotypes are beliefs and generalizations about the attributes of a particular group of people that are over-generalized and/or exaggerate assumptions and are not accurate reflections of reality (Yagmur and Jaideep, 2018). For example, the stereotype about computer scientists is that they are assumed to be male, heavily technology-oriented, intensely focused on computers, and socially awkward personalities lacking interpersonal skills (Yagmur and Jaideep, 2018). Other stereotypes include that being a computer scientist requires inborn brilliance and that computer science is an isolating profession that does not involve teamwork.

Yagmur and Jaideep's study specifically focused on male and female undergraduate students who enrolled in an introductory Management Information System career course to challenge negative stereotypes. The authors administrated surveys of students' perceptions of the information system field at the beginning and a survey of the students' perceptions at the end of the semester.

Beginning of the semester:

- Geeks: At the beginning of the semester, both female and male students were neutral about the geeky and nerdy features of MIS professionals. Even though the mean score for male students was slightly higher than the mean score for female students, the difference between the two groups was not statistically significant (Yagmur and Jaideep, 2018).
- Gender: At the beginning of the semester, female students believed that the MIS profession was dominated by men and MIS was a career pursued by men, not women. However, male students were neutral about the gendered view of the profession. Moreover, a comparison of the mean scores showed that the difference in perceptions between the two groups was statistically significant (Yagmur and Jaideep, 2018).
- Intelligence and Managerial: For the intelligence and managerial dimensions, both groups of respondents agreed that MIS professionals tend to be intelligent with good problem-solving skills and possess managerial skills, including people and communications skills.

The difference between the two groups was not statistically significant for either dimension at the beginning of the semester (Yagmur and Jaideep, 2018).

- Technical: Both female and male students agreed that MIS professionals tend to have a strong technical emphasis similar to that of a computer scientist, including a need for a robust math and science background along with programming skills. The difference between the two groups was statistically significant: with the mean score for female students being considerably higher than the mean score for male students. This indicates that female students placed greater emphasis on the need for a high level of technical skills (Yagmur and Jaideep, 2018).

End of the semester

- Geeks: At the end of the semester, both female and male students disagreed with the statements about MIS professionals being nerds and computer geeks. The difference between the two groups was not statistically significant (Yagmur and Jaideep, 2018).
- Gender: The findings state that neither female nor male students believed that men dominated the MIS profession at the end of the semester. Both groups of students were neutral about the gendered view of the profession. Accordingly, there was no significant difference between the two groups (Yagmur and Jaideep, 2018).
- Intelligence and Managerial: At the end of the semester, both groups agreed that MIS professionals tend to be intelligent and possess managerial skills. The mean score for female students was slightly higher than the mean score for male students for the intelligence dimension and slightly lower for the managerial dimension. However, the difference between the two groups was not statistically significant (Yagmur and Jaideep, 2018).

- Technical: At the end of the semester, male students were no longer concerned about the solid technical emphasis for MIS professionals; however, female students agreed on the statements about MIS professionals' possessing strong technical backgrounds and skills. The mean score for female students was considerably higher than the mean score for male students. The difference between the two groups was statistically significant (Yagmur and Jaideep, 2018).

Yagmur and Jaideep's study was an excellent example of why introductory courses are necessary and how students can be exposed to otherwise unknown career opportunities. Most of all, introductory courses can aid in closing the shortage of skilled workforce in the cybersecurity field by educating students in the reality of a career field and debunking stereotypes that might turn away half of the population, women and girls. "The impact of the introductory MIS course on female and male students' perceptions, we can see that the course has had a positive impact on both groups of students' perceptions" (Yagmur and Jaideep, 2018). Generally, the introductory course is students' first formal introduction to the MIS field, and the majority of students are in the early stages of deciding what major to pursue (Yagmur and Jaideep, 2018). Thus, making introductory courses more critical. Given this situation, introductory MIS courses can be used to dissipate any misconceptions students might have about this field (Yagmur and Jaideep, 2018). Yagmur and Jaideep suggest for introductory courses to be successful gateways to fields like cybersecurity programs and educators should:

- Educators need to create a stereotype threat-free environment in which students are exposed to different field features. Rather than just focusing on the technical concepts, they need to focus on the managerial aspects of MIS and help students understand that

MIS deals with people and technology in organizational contexts (Yagmur and Jaideep, 2018).

- Materials and the technologies used in the classroom should be state-of-the-art and, more importantly, relevant and exciting to both genders (Yagmur and Jaideep, 2018).
- The assignments, projects, case studies, etc., used in the course should be selected carefully to avoid any gender bias and incorporate material that appeals to both genders (Yagmur and Jaideep, 2018).
- The introductory course should expose students to different MIS career options that would be attractive to both male and female students and instill an understanding of the positive aspects of becoming an MIS professional (Yagmur and Jaideep, 2018)
- Connect female students with successful female MIS professionals through awareness campaigns, guest speakers, major and career fairs, and mentorship programs would prove helpful (Yagmur and Jaideep, 2018).
- Exposing students, especially to peers and recent alumni who have reaped the rewards of the MIS field, would be highly fruitful (Yagmur and Jaideep, 2018).
- The MIS course instructor should have the knowledge and skills in both the business and technology fields and serve as a role model to students (Yagmur and Jaideep, 2018).
- Assigning successful female faculty to teach the introductory course can prove particularly helpful in inspiring and attracting female students to the discipline (Yagmur and Jaideep, 2018).

Discussion

Who is entitled to participate? According to Jethwani et al.; Poster, and Yagmur, and Jaideep, all users should participate. However, women and girls are urgently needed in the cybersecurity field. Women's perspectives and experiences are needed to fight cybercriminals better. All three studies pointed out the negative impact stereotypes, gender biases, gender roles, and socialization patterns have on the field of Cybersecurity. All three studies acknowledge that women and children are more often targeted as victims yet are underrepresented in the rooms where security and privacy decisions are being made. The principles, steps, and suggestions proposed by all authors are far-reaching and anything but simple yet crucial to the country's cybersecurity efforts.

Summary

Cybersecurity is crucial for the security of our nation and the success of our country's commerce. Closer to home cybersecurity is vital to keep our children and loved ones safe. We cannot achieve safety, privacy, or keep a competitive edge in the world's commerce if there is a lack of female representation in tech. The lack of females in technology has created substantial blind spots in technology and security (Girl Scout Research Institute, 2020). Accessible, affordable, and available education is critical in solving the shortage of knowledge for everyday users and attracting a diverse workforce. Cybercriminals are not a homogenous group; cybercriminals come from various backgrounds and geographic locations and bring diverse skillsets and experiences (Girl Scout Research Institute, 2020). Hence the solution should be diverse and inclusive education for all. Cybersecurity's future depends on its ability to attract, retain, and promote women, who represent a highly skilled and under-tapped resource (Poster, 2018).

References

The Asian School. (2021). Importance of education in life: Salient features of education. Retrieved from https://www.theasianschool.net/blog/importance-of-education/#:~:text=%20Importance%20of%20Education%20in%20Our%20Society%20,%26%20secure%20life%2C%20one%20needs%20to...%20More%20

CISA. (2009). Security tip (st04-001). https://us-cert.cisa.gov/ncas/tips/ST04-001#:~:text=What%20is%20cybersecurity%3F%20Cybersecurity%20is%20the%20art%20of,of%20ensuring%20confidentiality%2C%20integrity%2C%20and%20availability%20of%20information.

Cybercrimemag. (2020). Cybersecurity talent crunch to Create 3.5 million unfilled Jobs globally by 2021. From https://cybersecurityventures.com/jobs/

The Girl Scout Research Institute. (2020). Breaking the Firewall to Girl's Cybersecurity Access. https://www.girlscouts.org/content/dam/girlscouts-gsusa/forms-and-documents/about-girl-scouts/research/20_GSRI_CybersecurityWhitePaper_Final.pdf

Jethwani, M., Memon, N., Seo, W., & Richer, A. (2017). I Can Actually Be a Super Sleuth. Journal of Educational Computing Research, 55(1), 3-25.

The Department of Homeland Security (DHS). (2021). Cybersecurity. From https://www.dhs.gov/topic/cybersecurity#

Poster, W. (2018). Cybersecurity needs women. Nature (London), 555(7698), 577-580.

Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. Education and Information Technologies, 24(1), 231-249.

Yagmur A., & Jaideep M. (2018). Gender based Investigation of Stereotypical Barriers in Management Information Systems Profession. Advances in Management (Indore, India), 11(4), 1-8.

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. ACM Computing Surveys, 54(1), 1-39.