Valparaiso University
ValpoScholar

Cyber Security Capstone Research Project Reports

Department of Computing and Information Sciences

1-28-2018

Cybersecurity in the Classroom: Bridging the Gap Between Computer Access and Online Safety

Andrew Malecki
Valparaiso University, andy.malecki@valpo.edu

Valparaiso University

Cybersecurity in the Classroom:
Bridging the Gap Between Computer Access and Online Safety

Andrew Malecki

CYB 692 : Independent Research in Cybersecurity

Dr. Nicholas Rosasco

January 28, 2018

Abstract

According to ISACA, there will be a global shortage of 2 million cybersecurity professionals worldwide by 2019. Additionally, according to Experian Data Breach Resolution, as much as 80% of all network breaches can be traced to employee negligence. These problems will not solve themselves, and they likewise won't improve without drastic action. An effort needs to be made to help direct interested and qualified individuals to the field of cybersecurity to move toward closing this gap. Moreover, steps need to be made to better inform the public of general safety measures while online, including the safeguarding of sensitive information.

A large issue with solving the problems at hand is that there seems to be no comprehensive curriculum for cybersecurity education to teach these basic principles. In my paper, I review and compare several after- and in-school programs that attempt to address this problem. I've also interviewed teachers from Montgomery County Public Schools, a relatively ethnically diverse school district outside of Washington, D.C.

These issues need to be addressed, and while private organizations and local schools are attempting to tackle the problem, wider action may need to be taken at a national level to come to a resolution.

Introduction

A commonly held assumption about cybersecurity is that many of the skills encompassed require a high level of education to grasp, study, and put into practice. While this is certainly true for subjects such as enterprise network configuration, penetration testing, and memory forensics, there are myriad other skills that are not only appropriate for younger students, but also include conceptual topics such as the CIA (Confidentiality, Integrity, and Availability) triad, “strong” password creation, and basic online etiquette and safety. These topics are not exclusively the realm of highly trained experts, but they are also not “common sense,” nor are they universally taught in schools.

In a world where most Americans have been the victim of a major data breach, trust in public institutions to protect their personal information wanes. And yet, the majority of Americans fail to follow cybersecurity best practices when safeguarding their own information online. For example, a report by the Pew Research Center found that 65% of Americans rely primarily on memorization to keep track of their online passwords. An additional 18% rely heavily on writing their passwords down on a piece of paper (Olmstead and Smith, 2017). The survey also found that just over two-thirds of Americans polled (69%) admitted that password security is not a concern (2017). It is difficult to tell whether these numbers are due to genuine apathy, or ignorance of the importance of proper password skills, including “strong” password formulation and robust password management.

One way to improve awareness and proficiency in protecting one’s personally identifiable information (PII) is by introducing the relevant skills early in education, and in a formal setting. Cybersecurity education is no longer the exclusive domain of highly trained Subject Matter Experts (SME’s), and should be more universally taught throughout primary and secondary education.

Early Exposure To Computers

There is no universally agreed-upon rubric for teaching cybersecurity to young students. Cybersecurity is still so entrenched in the IT profession — and so separate from the education system — that neither security professionals nor educators have a good grasp of which skills are important to pass on to young children. Moreover, teachers often lack the cybersecurity expertise and time to properly prepare their students for the technology and scenarios they will face.

Though the U.S. Department of Education (ED) “does not mandate or prescribe particular curricula or lesson plans,” it shouldn’t be a stretch to expect that the Department would make mention of the importance of cybersecurity education, especially in light of recent breaches in the ED. But the ED itself is largely silent on the subject of cybersecurity education. The only mention on the Department web page is a National Cybersecurity Awareness Month page listing “7 Ways to Keep Kids Safe Online.” (Cybersecurity) In the absence of rigorous guidance, teachers are creating their own materials as they are capable.

One organization with the goal of providing educators with cybersecurity safety materials is Common Sense Media, which has developed lessons on Digital Citizenship. Their Digital Citizenship curriculum consists of over 70 lessons for students from kindergarten to grade 12, covering domains such as Internet Safety, Privacy and Security, Cyberbullying and Digital Drama, Information Literacy, and Digital Footprints and Reputation. As a nonprofit, however, adoption of their materials is limited to individual educators’ prerogative.

A good example of this practice is taking place in the Montgomery County Public School System (MCPS) in Montgomery County, MD. MCPS students have regular access to Internet-connected classroom computers as early as Kindergarten. By third grade, each student is issued his or her own Chromebook for use in the classroom. Students are issued their own usernames and passwords, and therefore have private account access to academic resources. Proper safety guidelines commensurate to even this meager level of access, however, is not regularly afforded to these students. In most cases, Internet, intranet, and computer safety is left up to students’ parents or teachers without any sort of standardized curriculum (Treichler, personal communication, July 9, 2017).

MCPS reasonably reflects the demographics of students nationally with 30% percent of students reported as Hispanic, 29% as White, Non-Hispanic, 22% Black, and 14% Asian (mcpsmd.org). This compares to 29% Hispanic, 45% White, 15% Black, and 6% Asian nationwide as reported by the National Center for Education Statistics (NCES). Additionally, according to MCPS statistics, approximately 45.8% of students in the district receive meal assistance through Maryland’s FARMS (Free and Reduced Price Meals) program.

Basic computer and local network access is a large responsibility for a young child. It also presents a fantastic opportunity for a series of cybersecurity learning points while other rudimentary tasks are being taught. For example, individualized usernames and passwords allow students to access personalized account information across an enterprise network. It also allows them the freedom to change basic desktop settings and familiarize themselves with a computerized environment that they can call their own.

Yet personalized usernames and passwords also present a challenge. Password safety is an integral part of general online safety. In the case of Glenallen Elementary, usernames and passwords are issued on cards and passwords are not changed after initial login (Treichler, personal communication, July 9, 2017). Therefore, if cards are not properly secured, students’ accounts can be compromised. Sure enough, teachers report cases where children have acquired their classmates’ usernames and passwords, logged into their accounts, and changed personal settings. Fortunately, the changes made are relatively innocuous. Nonetheless, this scenario provides excellent background for a follow up lesson: Why is it important to change one’s password? And just as importantly, why is it important to choose a “strong” password? What constitutes a strong password? All of these questions should be addressed, and should be answerable in some form by students given the responsibility of personalized login credentials.

There are outside organizations that are trying to address this sort of opportunity. The SANS Institute, for example, has published a Computer and Internet Safety presentation called “You, Me & Everyone Else.” Though very basic, the document introduces the Internet to children and explains how it connects to devices with which children might already be familiar, such as tablets, smartphones and certain home appliances. Subsequent slides introduce the concept of interfacing with other individuals online (SANS). The safety measures presented on these slides heavily reflect the steps used to help children deal with strangers in the real world. These measures include identifying personal information, not giving personal information to unfamiliar (untrusted) individuals, and understanding when it is appropriate to seek the help of a trusted adult.

These lessons are fundamental to secure usage of the Internet, and teach skills that are integral to safeguarding one’s identity. While some of these lessons may seem too complicated for younger children, this is mainly by virtue of the vocabulary used and not because of the complexity of the concepts presented.

What Is Age-Appropriate?

It is clear that computers are an integral part of many students’ education well before computer education appears in current school curriculums. There may be any number of reasons for this. Perhaps funding for computers and networking is more plentiful or easier to justify than money for additional educators. It could also be the case that school real estate is at a premium, and integrating computer learning increases the education density of the classroom. The point is that students are learning with computers several grade levels before they learn more formally about computers, and there are critical mismatches here that should not exist.

There are programs that exist to aid schools in building cybersecurity curriculums. The University of Rhode Island Computer Science for All in Rhode Island (CS4RI) program was developed to fill this gap between computers in education and computer education. The program was developed to promote the availability of and enrollment in Computer Science courses in Rhode Island public high schools (CS4RI).

The CS4RI program focuses heavily on high school computer education, but does offer support for elementary and middle school programs. A major drawback with adapting the CS4RI lesson suggestions geared toward elementary and middle school students for a Cybersecurity lesson plan is that they lean heavily on coding for younger students (CS4RI).

Nonetheless, coding is an important skill, and interpreting code in various programming languages is invaluable to all cybersecurity disciplines. Coding also offers near immediate rewards. Think of a basic “Hello World!” script. The instant feedback earned through coding is prime for young learners who may have shorter attention spans than older students, and the visual aspect of HTML, CSS, or other web-heavy languages may be easier to present than the more in-depth subjects of IT law or systems auditing.

Other cybersecurity curriculum programs likewise focus heavily on beginning formal computer and Cybersecurity training with high school students. King William County Public Schools (KWCPS), just east of Richmond, VA, has a fairly well thought out cybersecurity curriculum. The first semester of their program prepares students for the Comp TIA A+ certification exam.

This course, an industry-recognized and respected certification, presents an opportunity for students to learn about the inner workings of a device on which they are already spending a considerable amount of time. A+ certification is intended to introduce participants to how computers work, their components, and basic troubleshooting procedures. The main purpose of the course is to serve as an introduction certification to further Information Technology learning, and eventual professional certifications. The subject matter also covers concepts essential to understanding the technical aspects of cybersecurity.

While some of the more technical details are best left to high school classrooms, conceptually there seems to be no reason not to formally cover this course material even sooner in students’ academic careers. Why not allow kids to indulge their curiosity and pull apart old desktop computers, perhaps donated from local businesses that have just gone through an upgrade? The beauty of this sort of program is that, although the computer industry has made great strides in computing and transfer speed as well as storage capacity, the basic makings of a “desktop computer” have not changed significantly in decades. CPUs still reside on motherboards, as do RAM and hard drives, and network interface cards still connect them to other networked devices. It doesn’t much matter whether the computer is three months old or 30 years old — all the same parts are there in one shape or form.

Further courses in the KWCPS curriculum prepare students for the Linux+ certification. Again, waiting until high school to teach all of these concepts may not be necessary. MCPS students use Google Chromebooks from the third grade. The Chrome OS running on these laptops is based on the Linux kernel. Though third graders may not need to learn Linux command line or BASH scripting, there may be lessons there that would be appropriate for slightly older elementary school students. These lessons could be taught on hardware that the students already access regularly, and that will remain crucial to their future education.

Familiarity and success with the Linux framework are basic skills for current cybersecurity professionals, and their importance is only expected to grow in the next generation. As ubiquitous as Windows and Mac Operating Systems are, Linux systems are nearly as common in most IT security environments. Moreover, most Linux distributions are free or “pay what you want,” and modern distributions are as easy or easier to use than a Microsoft or Apple OS. This combination of usefulness and frugality make learning Linux command line and BASH scripting a winning combination for cybersecurity education as well as for school administrators.

As young as cybersecurity is as a discipline, there already seem to be some well-entrenched assumptions about when students should be exposed to certain concepts. The timeframe for introducing most cybersecurity-related topics seems to be centered on high school, and this is later than optimal. Given that students may be exposed to computing devices before they even enter formal schooling, waiting until they are 14 years old to teach them how to responsibly use those devices, let alone secure them and identify potential threats, seems woefully overdue.

Why Bother?

As mentioned earlier, the discipline of cybersecurity is no longer solely the realm of highly trained experts. Network and end-point security on a national and global scale are still squarely in the hands of individual users. The Internet Security Threat Report

(ISTR), published by Symantec in April 2017, shows that while spam and phishing rates have been decreasing over the past several years (2014-2016), the email malware rate has increased to one infected email in 131. According to the same report, the United States is at the top of the lists for both number of data breaches in 2016 (1,023) and total identities stolen in 2016 (791,820,040) (ISTR22).

These numbers lead to two important conclusions. First, the United States is a huge target for attacks leading to massive data breaches. While the U.S. suffered 1,023 breaches, the second highest country on Symantec's list was the United Kingdom, with a mere 38 breaches. This gap shows how preferable our networks are to those hosted in or owned by other countries. The risk/reward ratio for attacking U.S. networks is relatively low, and the return on investment is high (ISTR22).

Second, these discrepancies suggest normal Internet users in the U.S. are unaware of the threats posed to our networks, and therefore to their personal information. Moreover, day-to-day Internet users are untrained in identifying these threats, as well as what to do once they are identified.

Deployment of custom intrusion sets and sophisticated scanning and monitoring tools to gain access to networks is not the culprit in most major data breaches. Rather, the culprit is the intruders' careful use of tried-and-true non-technical techniques to gain access, coupled with users' lack of education on how spam, phishing, and social engineering help to facilitate these attacks.

It could take a hacker group weeks or months of planning and reconnaissance to identify a target, characterize it, and gain access. After this, the target's movements on the network are restricted so as to avoid detection by IDS or savvy system administrators. The hackers can avoid such difficult work simply by exploiting a single employee with proper network access.

The Internet is permissive by nature. Its protocols and architecture were designed for ease of use first and foremost, and the prioritization of connectivity and resource availability ensured users could request and access information with few impediments. This model also has a downside though, and we are still struggling with its effects.

Education against these basic and ubiquitous threats can and should start early in life, and as previously mentioned can be easily integrated with similar lessons that teach safety in the physical world.

The term “Herd Immunity” is used often in discussions of vaccinations. According to the U.S. Department of Health and Human Services:

> When a critical portion of a community is immunized against a contagious disease, most members of the community are protected against that disease because there is little opportunity for an outbreak. Even those who are not eligible for certain vaccines—such as infants, pregnant women, or immunocompromised individuals—get some protection because the spread of contagious disease is contained. This is known as "community immunity (Vaccines.gov)."

The collective population is less susceptible to infection because there are fewer potential vectors of infection. This increases the overall health of the population, while having the added benefit of specifically protecting its most vulnerable members.

The same concept can be applied to cybersecurity education. According to the 2017 Symantec Internet Security Threat Report and the 2016 Managing Insider Risk Through Training & Culture report, 55-60% of all organizational security incidents or data breaches can be attributable to employee actions. According to Experian Data Breach Resolution, as much as 80% of all network breaches can be traced to employee negligence (Experian, 2017).

Clearly there is a knowledge gap that must be addressed. More and more companies are getting on board with employee education regarding network security risks. Through early cybersecurity education, there is an opportunity to drive home the principles of proper defensive Internet usage before people even enter the workplace.

Cybersecurity As Life Skills

Sure, training and expertise are needed to defend critical infrastructure and large corporate networks, but there are local and personal applications for cybersecurity skills as well. Many schools incorporate “mandatory electives” such as health class that essentially teach students basic maintenance of their bodies as well as help explain and manage adolescence.

A well-outlined cybersecurity curriculum could serve a similar purpose to prepare children for the situations they could be exposed to on the Internet. This could include aforementioned lessons on phishing, but also on how actions taken online can affect the real world. Topics such as what to do if a stranger asks to meet in person, asks for personal information, or even cyberbullying, could be covered in such a class.

These lessons could purposefully stay away from the more technical aspects of cybersecurity, such as networking protocols and cryptography. They should, however, integrate the general theory of these topics and more as needed to understand personal, public, and Internet safety. For example, students should have a basic working knowledge of how IP addresses, ports, and sockets work. This knowledge would help to inform not just a general sense of how the Internet works, but also how to configure home networking devices such as routers and Wi-Fi access points to better secure their homes. Such lessons could be taught using slides and lectures for older students, or games and hands-on activities for younger students. Frankly, hands-on games and activities could be beneficial for all age groups when trying to teach these concepts from scratch.

Cryptography is another concept that is ubiquitous enough in daily life that rudimentary knowledge of it may be beneficial at an early age, and over a broad spectrum of the population. Lessons may cover what cryptography is, the history of cryptography, and various types of cryptography in use today. Sample lessons could explain, in mathematical terms, how cryptography works. Advanced lessons might invite students to develop their own ciphers and algorithms, to illustrate how they work.

Practical lessons on any subject, however, should focus less on how the technology works, and more on how it affects students’ daily lives (Mutafian, personal communication, July 24, 2017). That is what will help keep the topics relevant and therefore more interesting. For example, practical lessons on cryptography can explain how ciphers are used to obfuscate and encrypt sensitive information. Used in conjunction with lessons on PII and types of sensitive information, it will be easier to drive home the point that proper use of robust crypto techniques is essential to students' online personal safety, not to mention the safety of those around them.

After School Programs

Programs teaching these principles are few and far between, and largely consist of after school or private programs. There are obvious weaknesses in this model. Among them, participants, and therefore the knowledge itself, is limited to students whose families can afford to send their children to classes. Out-of-pocket costs can, hypothetically, be covered by grants or from some other source in order to provide access to disadvantaged students. The remaining issue is that of logistics, such as transportation. If a student simply cannot get a ride, they are unlikely to participate. Incorporation into the existing school day would ameliorate these issues.

There are as many barriers to including cybersecurity principles in school programming as there are schools. Access to computer infrastructure, unreliable funding, too few adults to support participating youth, and even the assumption that all children now are "digital natives" (CyberGirlz) all make it difficult to get such programs off the ground, let alone sustain, develop, and expand them. Moreover, in-school cybersecurity programs may not be agile enough to keep up with evolving technologies and emerging threats. Therefore, despite the aforementioned challenges, independently contracted after school programs could be the answer.

CyberGirlz is a STEM (Science, Technology, Engineering, and Math) program developed in the Spring of 2015 at San Jose State University. The program is aimed at engaging middle school-aged girls in cybersecurity topics specifically, and at developing an interest in STEM generally. CyberGirlz curricula vary from location to location (groups can be found in California, Wisconsin, Virginia, and elsewhere), but they generally offer a survey of topics such as cryptography, coding, and network configuration.

As they are geared toward building middle school-aged girls' interest in STEM fields, CyberGirlz also invites female professionals in those sectors to visit and speak to students. The organization likewise devotes time to exploring jobs in cybersecurity in the hopes of attracting young women to the field professionally.

According to the Global Information Security Workforce Study (GISWS) sponsored by International Information System Security Certification Consortium (ISC)2, women only make up 11% of the current Information Technology workforce. This could be because these career paths are not widely advertised to them, as 69% of women say they have not pursued careers in IT because they were unaware of the potential (GISWS). CyberGirlz is clearly geared toward mitigating these discrepancies and directing young girls toward career paths they otherwise might not have known to exist.

In June 2017, Girl Scouts of the USA (GSUSA) announced the creation of 18 cybersecurity badges (Zarya). The badges were created in conjunction with Palo Alto Networks, Inc., a network and enterprise security company in Santa Clara, CA. Like CyberGirlz, this partnership was developed to expose girls to STEM fields. One stated goal of the program is to narrow the projected deficit of 3.5 million qualified cybersecurity professionals by 2021 (McAtee Cerbin).

GSUSA has a membership of approximately 2.6 million (McAtee Cerbin). There is no telling exactly how many of these Scouts will pursue any of the available cybersecurity badges, but the organization is capable of helping to whittle down the aforementioned 69% of women who have not pursued IT careers due to lack of exposure to the underlying concepts. By their own admission, “This national effort is a huge step toward eliminating traditional barriers to industry access, such as gender and geography” (Girl Scouts).

In-School Curriculums

Schools by and large have yet to dive in to general cybersecurity education. That has not kept other organizations from developing materials for schools and educators to adopt for their own use. National organizations such as the K-12 Computer Science (K12CS), the National Cyber Security Alliance, and the National Institute for Standards and Technology (NIST) have published cybersecurity frameworks to be used with targeted age groups.

One of the benefits of utilizing such a framework is that the concepts taught can be more easily reinforced in students' daily lives. Use of such frameworks would not only provide children the knowledge needed to be responsible digital citizens, but also allow them to utilize cybersecurity concepts in a supervised environment.

K12CS.org is one organization whose goal is to help children "better understand the role of computing in the world around them," and "critically engage in public discussion on computer science topics" ("Framework", 2016).

The K12CS Framework integrates Computer Science topics as early as Kindergarten (hence the name). By introducing children to concepts such as Authentication, online safety, and strong passwords at an early age, students are treated as true digital natives.

By fifth grade, K12CS recommends teaching the importance of backing up data, and ways to monitor for and mitigate the effects of viruses and malware. The concept of "Confidentiality" is also introduced to this age group, suggesting that lessons revolving around the CIA Triad (Confidentiality, Integrity, Accessibility) in general may also be appropriate.

Through the K12CS Framework, middle school and high school students are exposed to topics such as encryption, two-factor authentication, and biometrics. Additionally, potential security problems such as viruses, denial of service attacks, and ransomware can be introduced ("Framework", 2016). Students at this age are also old enough to discuss and debate the merits/faults of both familiar and novel concepts pertaining to cybersecurity. When they are constantly exposed to cybersecurity topics throughout their education, students will be better prepared to understand how these concepts affect their daily lives as well as the world around them.

SafeOnline.org, developed by the National Cyber Security Alliance, is another resource to help teachers present cybersecurity concepts to their students. In addition to lessons about how passwords work and the importance of securing personal information, SafeOnline also provides lessons on risk mitigation and remediation. Lessons such as "Should I Report Cybercrime?" and "Who To Contact?" help reinforce not only the nature of threats children will face while online, but also the fact that they aren’t helpless and there are steps that can be taken to minimize their exposure to harm (SafeOnline).

The NIST National Initiative for Cybersecurity Education (NICE) states its mission as “…[promoting] a robust network and an ecosystem of Cybersecurity education, training, and workforce development” (NIST). NICE does not see K-12 cybersecurity education as an isolated program; rather, the Initiative frames K-12 education as part of a larger effort to develop the cybersecurity workforce. The NICE K-12 Roadmap asserts that the way to accomplish this is to:

1. Increase Career Awareness
2. Infuse Cybersecurity Across the Education Portfolio
3. Stimulate Innovative Educational Approaches
4. Identify Academic and Career Pathways

(Implementation Plan)

Other programs such as K12CS, SafeOnline, and CS4RI are devoted to teaching school-aged children the importance of cybersecurity and its relevance to the world beyond the classroom. Yet NICE’s K-12 program is uniquely incorporated into a holistic cybersecurity education framework that includes workforce development. NICE’s “ecosystem of cybersecurity education” requires adults and children alike to participate in order to ensure a safe online environment for all.

Conclusion

Despite the technical complexities of cybersecurity as a discipline, there is considerably more that educators and curriculum developers can do immediately to improve student safety online. It is also clear this issue needs to be addressed in a more organized fashion than it has been to date.

By boiling down cybersecurity topics to basic concepts, complex ideas can be made more accessible to younger students as they are introduced to them in practice. Doing so will help build a foundation of cybersecurity awareness, best practices, and could also lead to addressing increasingly advanced topics.

There are existing frameworks aimed both at extracurricular and in-school programs that can be put into practice at once. However, these may only be a stop-gap until a more comprehensive national initiative could be put into effect. In February 2017, Representative Sheila Jackson Lee (D-TX, 18th District) introduced HR 935: The Cyber Security Education and Federal Workforce Enhancement Act to tackle exactly this problem (Jackson Lee, 2017). As of January 2018, the Act is still couched with the Subcommittee on Research and Technology.

In order to build the practical and professional skills needed to protect the country and world from these threats, the next generation will need a strong foundation of cybersecurity awareness and education. Current cybersecurity professionals have an opportunity to help ensure that the next generation is well informed, curious, and prepared for the challenges that await us.

Bibliography

"2016 Managing Insider Risk Whitepaper." 2017. Accessed July 23, 2017. http://www.experian.com/data-breach/2016-ponemon-insider-risk.html?WT.srch=2016_insider_risk_pr.

"Community Immunity ('Herd Immunity') | Vaccines.Gov." 2017. Accessed July 22, 2017. https://www.vaccines.gov/basics/protection/index.html.

"The Condition of Education - Participation in Education - Elementary/Secondary - Racial/Ethnic Enrollment in Public Schools - Indicator May (2017)." 2017. *Racial/Ethnic Enrollment in Public Schools*. May. https://nces.ed.gov/programs/coe/indicator_cge.asp.

Csec2017_v0.75_PRCrelease061517.Docx - 895bd2_e3443415db4c432da8a66b59d076e151.Pdf." 2017. Accessed July 19, 2017.https://docs.wixstatic.com/ugd/895bd2_e3443415db4c432da8a66b59d076e151.pdf.

"Cybersecurity: 7 Ways to Keep Kids Safe Online." 2017. Accessed January 28, 2018. https://www2.ed.gov/free/features/cybersecurity.html.

"Cyber Security Planning Guide - FCC Cybersecurity Planning Guide_1.Pdf." 2017. Accessed July 2, 2017. https://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide_1.pdf.

"Demographics - Montgomery County Public Schools, Rockville, MD." 2016. *Update on Student Enrollment and Facilities*. October 10, 2017. http://www.montgomeryschoolsmd.org/departments/planning/demographics.aspx.

"Home." 2017. *CS4RI*. Accessed July 27, 2017. https://www.cs4ri.org/.

"Information Security Awareness | Cybersecurity Awareness | Kids | SANS." 2017. Accessed July 13. https://securingthehuman.sans.org/resources/kids.

"ISTR22_Main-FINAL-JUN8.Pdf." 2017. Accessed July 22, 2017. https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_.

Jackson Lee. 2017. "All Info - H.R.935 - 115th Congress (2017-2018): Cyber Security Education and Federal Workforce Enhancement Act." Webpage. April 25. https://www.congress.gov/bill/115th-congress/house-bill/935/all-info.

"Framework Statements by Grade Band." 2017. *K12cs.Org*. Accessed August 11, 2017. https://k12cs.org/framework-statements-by-grade-band/.

McAtee Cerbin, Carolyn. 2017. “Hackers, Beware! Girl Scouts to Offer Cybersecurity Badges.” News. *USA TODAY*. Accessed July 27, 2017. https://www.usatoday.com/story/tech/nation-now/2017/06/22/girl-scouts-offer-cybersecurity-badges/418443001/.

“National K-12 Cybersecurity Education Implementation Plan.” 2017. *National Initiative for Cybersecurity Education.* Accessed July 27, 2017. https://www.nist.gov/sites/default/files/documents/2017/04/26/nice_k12_implementation_plan.pdf.

Olmstead, Kenneth, and Aaron Smith. 2017. “Americans and Cyber Security.” *Pew Research Center: Internet, Science & Tech*. January 26. http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

“Phishing.” 2017. *Security Through Education*. Accessed July 4, 2017. https://www.social-engineer.org/framework/attack-vectors/phishing-attacks-2/.

Zarya, Valentina. 2017. “Why Girl Scouts Make Great Cybersecurity Hackers.” *Fortune*. Accessed July 29, 2017. http://fortune.com/2017/06/16/girl-scouts-cybersecurity/.