5-2016

Cybersecurity Awareness Shrewsbury Public Schools

Brittany Crompton
Clark University, bcrompton@clarku.edu

David Thompson
Clark University, dthompson@clarku.edu

Manuel Reyes
Clark University, mareyes@clarku.edu

Xueyan Zhao
Clark University, xuezhao@clarku.edu

Xueke Zou
Clark University, xuzou@clarku.edu

CYBERSECURITY AWARENESS

Shrewsbury Public Schools

ABSTRACT

In the 21st Century, technology reaches every aspect of our lives. As "digital citizens" we must be aware of the dangers both to our technological equipment and our personal information stored, transmitted, and processed on this equipment. The Cybersecurity Awareness curriculum developed for the Shrewsbury Public School district is designed to meet this need, as well as foster an interest in technology and ethical computer use.

Brittany Crompton, David Thompson, Manuel Reyes, Xueyan Zhao, Xueke Zou

MSIT-3999 / MSPC-3330 : Capstone

Table of Contents

Acknowledgements

Team Acknowledgements

The team would like to acknowledge the contributions of Brian L'Heureux, the Director of Information Technology, and Shawna Powers, the Director of Instructional Technology and Media Services, at the Shrewsbury Public School district. Working with them to fully identify the requirements of the school district enabled the team to effectively tailor the recommendations to the school population, and provide additional advice in managing the cybersecurity curriculum in the future.

In addition to the Shrewsbury Public School district, the team would also like to acknowledge the contributions of the Capstone Advisors and other professors at Clark University. These educators have instructed and guided the team members, and provided the tools to successfully complete this capstone project. While the graduate degree shows the level of education that the students have completed, the capstone project is a demonstration and application of that learning.

Each team member would also like to acknowledge the contributions and support of people in their lives.

Brittany Crompton

It is due to the encouragement and support given to me by my parents and boyfriend that I have been able to continue my graduate studies and work towards completion of my degree. Their unwavering faith in my abilities has helped me to understand the power and strength of having loved ones by your side, in both good and bad times. It is my parents' that inspired me to begin my educational journey towards this degree, and my boyfriend who is helping me see it through to its completion.

David Thompson

I would like to acknowledge the support of my wife over the many years I have been in school. Without her support and unselfish attention to our children, our home, and our families; with everything else going on in our lives; she has managed to give me the time and support to not only attend classes and complete the necessary work, but excel at these endeavors. Although I will receive a piece of paper with my name on it, I couldn't have done it without you, and we will have earned this degree together.

Manuel Reyes

I want to acknowledge each and every individual in our group for working very hard to put in their amount of valuable work into this project despite dedicating time to other classes, full-time jobs, and their personal lives. Although I was often times crammed with my 9-to-5 job and other classes, my group members still made me feel part of the team and complimented as well as provided their constructive criticism on the research that I brought to the project. I would also like to acknowledge Shawna Powers, the Director of Instructional Technology and Media Services, and Brian L'Heureux, the Director of Information Technology, from Shrewsbury High School. They got us familiar with Shrewsbury High and their current computer system, Schoology. Last but not least, I would like to acknowledge Professor Chetro-Szivos for giving me and my group the proper tools to begin our research and plan for our capstone. Although we did not see him from time to time due to his busy schedule, he was always quick with responding to our emails and the documents that he uploaded on Moodle have tremendously aided us in understanding how to properly do this capstone.

Xueyan Zhao

I would like to acknowledge the help of our Capstone advisor and other professors who taught us all the knowledges through the graduate level study. With them guiding us where to go, we completed this project with less difficulties. I also want to acknowledge Brian L'Heureux, the Director of Information Technology, and Shawna Powers, the Director of Instructional Technology and Media Services, from Shrewsbury High School. They have provided us a lot of useful information and background so we could know our client better and develop a specific curriculum. Last but not least, I want to acknowledge our group members. Although many of them have other classes and work, they all made great effort this project.

Xueke Zou

I would like to acknowledge our team members for their invaluable contribution to the project. I would also like to acknowledge Shawna Powers, the Director of Instructional Technology and Media Services, and Brian L'Heureux, the Director of Information Technology, from Shrewsbury High School. They provided profound background information and helped us to understand the requirement of the project. Last but not least, I would like to acknowledge the MSIT capstone adviser, Professor Cohen, for nonstop support for the project.

Executive Summary

Understanding cybersecurity is crucial to simply existing in the modern era, especially as more and more information is stored and exchanged electronically. The past generation focused on ensuring students graduated from high school receiving not only the basic academic foundation, but also learning the essential "life skills" of the time such as balancing a checkbook, or cooking a nutritious meal. While those life skills are important, understanding cybersecurity needs to be added to the list of essential life skills. This project aimed to address this need in a local school system with a track record of embracing and capitalizing on technology.

The dual-program graduate team from Clark University analyzed current trends in both the information technology industry and the education industry. The team used this analysis to strategically frame the development of a curriculum that would not only provide the most relevant and applicable information, but also be relatable to the target audience of high school teenagers. Using information from various government agencies, studies conducted by IT giants such as Google, and curriculum suggestions from IT education pioneers such as Code.org, the team put together recommendations for the Shrewsbury Public Schools to implement a comprehensive, yet optional, cybersecurity training curriculum, spanning all levels of expertise.

The overall architecture recommended by the team, was a three-tiered approach, with the first tier focused on providing the foundational understanding of cybersecurity, which can be applied not just to specific scenarios, but to develop a way of thinking. This tier is designed to be delivered to all students in the high school in short, independent modules during their homeroom period. The second tier is designed to build upon information from the first, and begin to develop the concept of "digital citizenship" in the students. The final tier is designed to

provide higher-level information, in a trusted environment, about cybersecurity and ethical hacking.

Because most students will only complete the first tier, the second and third are targeted toward those students with an interest in computer science, or involved in IT clubs or the Student Innovation Team, which provides first-line help desk support for the school district's iPad program. Beyond the three-tier architecture, the team made additional recommendations of continual assessment and improvement of the program, collaborating with local IT companies, and using the curriculum to develop similar programs for the primary schools in the district.

Ultimately, the Shrewsbury Public School district is responsible for physical development and implementation of any cybersecurity program, however the Clark University graduate team has put together a recommendation that provides a roadmap to delivery. The recommendations can be taken in whole, or in part, but overall provide a solid framework for ensuring all graduates of the Shrewsbury school system are prepared for the digital age, to keep themselves and their information safe.

Chapter 1: Introduction

Background

What do Home Depot, Target, the Internal Revenue Service (IRS), and Sony Pictures Entertainment all have in common? They have all been the victim of major cybersecurity attacks within the last three years. When news of security breaches of the magnitude that these companies suffered reaches the general public, it highlights the importance of cybersecurity and how is plays a part in everyone's life.

The recent increase in internet-related crimes and sophistication of hacker techniques has shown the importance of introducing topics such as cybersecurity and internet safety to children prior to leaving high school. A topic previously reserved for elective choices in college, cybersecurity has become a fast-growing industry and no longer can its importance be ignored. Then why has it not been made a part of every public school in the nation's core curriculum? This issue has been brought to the forefront of the nation's attention, with President Obama putting cybersecurity as a top priority for the country, given the number of security breaches in recent years. Schools across the nation are now beginning to see the merits of working cybersecurity into the curriculum to give students a better foundation in what risks are out there, how to spot them, and most importantly, how to stop them.

But what is "cybersecurity"? The term cybersecurity, as defined by the National Initiative for Cybersecurity Careers and Studies (a Dept of Homeland Security sponsored site), is:

> *The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected*

from and/or defended against damage, unauthorized use or modification, or exploitation." (U.S. Dept of Homeland Security, 2016)

This highly-technical explanation can be rephrased for applicability to the general public, and the focus of our project. For the purpose of educating the public, through the use of secondary school educational programming, cybersecurity could be defined as "ensuring information is protected from electronic theft or exploitation." It is this definition that we aim to apply to the curriculum for the Shrewsbury Public School system.

Statement of Problem

As classrooms across the country continue to integrate more technology into the learning process, it becomes apparent that schools have an obligation to ensure the online safety of their students. To do this, it is imperative that students are given a solid foundation in cybersecurity and how to protect their own information. One such school district that has begun to integrate technology not only into their classroom on a regular basis, but into the curriculum is the Shrewsbury Public School District in Shrewsbury, MA. A new initiative discussed on the district's website is their 1:1 Technology Program, which runs in grades 5-12, integrating iPad technology with the learning process in the classroom.

While Shrewsbury High School currently offers a few computer/technology classes, none focus on cybersecurity or network protection. Ms. Shawna Powers, Shrewsbury School District Director of Instructional Technology and Media Services (ITAMS), overseas and administers the instructional technology, and provides guidance to the teachers. Students have approached Ms. Powers asking for a technology-related independent study or if any additional computer training is available through the school. At this time, neither the high school, nor the district, have the time or resources to put together a cybersecurity curriculum. Shrewsbury became aware of just

how important a cybersecurity program could be when last year a student at the high school was able to bring down the school's network briefly, by using only their smartphone.

Acting in a consulting role, Clark University graduate students in the Master of Science in Information Technology (MSIT) and Master of Science in Professional Communications (MSPC) programs, worked with our client, the Shrewsbury Public School District, to develop a cybersecurity curriculum for the district which will address the need for high school graduates to learn basic cybersecurity skills to protect themselves, as well as to become good "digital citizens".

In order to accomplish this task, it was necessary for students in the MSIT and MSPC graduate programs to work in tandem to solve Shrewsbury High School's curriculum gap. MSIT group members, David Thompson and Xueke Zou, brought their expertise in the field of cybersecurity and curriculum knowledge. They were charged with defining what the most important concepts of cybersecurity are that every student graduating high school should know, and designing the curriculum modules.

MSPC group members Brittany Crompton, Xueyan Zhao, and Manuel Reyes aided in the design, but also proposed module delivery ideas and researched cybersecurity as an industry and how it effects education. The curriculum designed would be completed by Shrewsbury High Schools students on a purely voluntary basis. Due to the voluntary completion requirement, it was necessary for our group to find a way to convince students and teachers of the importance of the curriculum and become motivated to obtain this practical knowledge.

Purpose of Capstone

School systems are beginning to integrate cybersecurity courses into the curriculum as young as the fourth grade because of their importance in daily life. The advantage of starting

early is to help students become more comfortable with the technology being used in the classroom and helping them to become more conscientious digital citizens. Shrewsbury Public Schools District adopted "a set of strategic priorities that included having all students in grades 5-12 being educated in 1:1 learning environments by 2016" (Shrewsbury Public Schools, 2015). The technology initiative has since been achieved with all students in Shrewsbury High School using iPads in interactive and innovative ways.

However, it would be irresponsible to integrate iPads into the classroom for students in grades 5-12, and not teach them about the care and responsibility that comes along with technology. Developing digital citizenship skills is what leads students to have more confidence in their own online ability, as well as act responsibly with technology. The curriculum requested by Shrewsbury Public Schools District was meant to supplement the courses they already offer, and provide ad-hoc modules which students and faculty could complete. Introducing students to the concept of digital citizenship also provides them with a perspective in responsible online behavior, hopefully preventing them from becoming involved in malicious activities for which "hackers", "cyber bullies", and "cyber thieves" are notorious.

The purpose of the cybersecurity curriculum for Shrewsbury Public Schools is to further develop their technology program and give them relevant material that could later be built upon and extended in future years. The current technology trend is helping to create the classroom of the future, where cybersecurity is an absolute necessity.

Significance of Capstone Project

Since President Barack Obama has named cybersecurity as "one of the most important challenges we face as a Nation" (The White House, 2009), the issue can no longer be ignored. With over 13 million identity fraud victims in 2015 and $15 billion stolen as a result of

cybercrimes (Javelin Strategy & Research, 2016), it is imperative that drastic steps be taken to reduce risks of these numbers continuing to climb, especially with the popularity of online and mobile banking. As technology is an inexorable part of our lives, it has become increasingly important to include cybersecurity into grade school education. Though we are still in the beginning stages of creating digital classrooms, the technology is already being used extensively and trends are being created.

There are many arguments for the addition of cybersecurity to the K-12 curriculum. The National Cybersecurity Institute at Excelsior College works to conduct research and trainings for organizations on the topic of cybersecurity. In the post "Should cybersecurity become a part of K-12 curricula?" the Institute discusses the benefits and importance of the curriculum addition.

> According to the Occupational Outlook Handbook, the field of cybersecurity is expected to grow by 37 percent in the next 10 years. This means that when the children who are currently in elementary and middle school begin to look for careers, they will have a great opportunity to obtain jobs in information security. By beginning cybersecurity training at a young age, there is a chance to create a stronger, more prepared cyber defense force. (National Cybersecurity Institute at Excelsior College, 2015)

If cybersecurity were to be added to the curriculum of all schools, students would also be learning how to be better digital citizens.

Cyber threats are daily risks that students face not only in their online lives, but can spill over into their offline lives. Cyberbullying, a term used to describe bullying that takes place through the use of electronic devices, has gained national attention due to its increasing

prevalence. Teaching students about cybersecurity and digital citizenship not only helps them recognize cyberbullying and how to end it, but also not to perpetuate it.

Subsequent Chapters

In the following chapters, the team will discuss the trends in the industry as identified through research, methods used to identify the requirements, constraints, and opportunities, the findings of research and analysis of data, and finally the detailed recommendations for the Shrewsbury Public Schools district. Each chapter provides detailed information on the process used to arrive at the recommendations, so that the client can understand how the team worked through the various industry trends, recommendations in security and education, and what is of utmost importance to provide an up-to-date cybersecurity curriculum.

Chapter 2: Trends in the Industry

Cyber-Education

With so many instances of data security breaches in companies, personal information loss and even cyber terrorism, it's easy to see why cybersecurity has become such an important topic for today's society. Though there is a plethora of information available to anyone with access to the internet, not all of it is reliable and it can become difficult to distinguish truth from the hype. To make a topic as all-encompassing as cybersecurity easier to understand, it must be broken down into smaller and more manageable subsections, such as education or government involvement. One of the largest trends emerging from the cybersecurity field is its effect on education.

Within the last five years, educators, parents and students have begun to give more consideration to STEM courses, especially computer science and related subjects. Numbers of K-12 school systems are exploring the benefits of providing cyber courses after receiving requests from students and parents. Schools that adopt a strong cyber program into their curriculum become part of a growing industry. According to Gallup, a research and analytics company, the general trend in schools is to work more computer science options into the curriculum. In a nationwide 2014 poll of schools who are part of this trend, the following courses were found to be the most likely to be offered: Computer Graphics, Creating Websites, Computer Programing & Coding, and Robotics/Artificial Intelligence (Google/Gallup, 2015).

Making computer science and cybersecurity courses a part of a school's curriculum requires a substantial amount of support from an IT Department. With most IT departments resources stretched as far as possible, it is not uncommon for schools to turn to external organizations for assistance with curriculum development. Two such organizations are the

National Integrated Cyber Education Research Center (NICERC) and Code.org, both non-profits that work with schools to create a system or give advice on a set of programs already in place. Understanding that our workforce already suffers from a dearth of cyber professionals, NICERC wants to help develop and cultivate interest in the subject in children grades K-12 (National Integrated Cyber Education Research Center, 2015). Code.org wants to increase the involvement of women and minorities in the field of computer science through programing in schools. They work to establish "diversity in computer science" (Code.org, 2015).

Though both of these organizations work with schools to develop computer science and cybersecurity curriculums, they do so in different ways. The efforts of both organizations have earned them recognition not only in schools, but with government groups such as the Department of Homeland Security.

The NICERC has worked with the Department of Homeland Security (DHS) for the last four years to bring to fruition the goal of putting more technology into K-12 schools and providing teachers with the training they need to utilize to its full potential. The massive undertaking, which included 15,000+ teachers and 820,000 students in 42 states, was achieved at no cost to the schools, because of a generous grant (U.S. Dept of Homeland Security, 2016). When looking for resources on what is available for cyber curriculum development to schools that don't have a pre-established system, the DHS website is a great place to begin any search. In addition to the many wonderful groups they have partnered with since coming into existence, such as the NICERC, they are a repository for information about the future of the cybersecurity workforce. The DHS wants to help schools create strong cybersecurity leaders and "standardize roles" to ensure all those entering technology jobs were taught the same material (U.S. Dept of Homeland Security, 2016).

For schools that have decided to work with an organization to increase classroom technology and development of a cyber curriculum, the NICERC is an example of one such organization. Their website explains how they work with schools to develop a curricula that will work for them and "showcases a system-level understanding of real-world applications of science, technology, engineering, and mathematics" (National Integrated Cyber Education Research Center, 2015). By putting their curriculum topics, such as Cyber Society- Law or Ethics and Cyber Business- Protection of Data on their website (2015), it allows schools who do not have the ability to use NICERC's services to gain insight into what a cybersecurity curriculum should include.

Another organization advocating for the addition of computer science to the core curriculum of students everywhere is Code.org. They are a relatively new non-profit organization, having been around since 2013, that focuses more on making computer science available to all, with a goal of reaching out specifically to women, unrepresented minorities and lower income populations (Code.org, 2015). Code.org does not just work to help get more computer science classes into schools, but sponsors events that can be held anywhere. One of the most well-known programs globally is the Hour of Code. This program, which has been held in over 180 countries, is "a one-hour introduction to computer science, designed to demystify code and show how anyone can learn the basics" (Code.org, 2015). Programing that builds self-confidence as well as a particular skill set is a model that many schools strive to emulate. With Code.org's Hour of Code program that can be held by any school, community group or workplace, awareness is raised in regards to computer science education and those who may have never seen themselves going into a career in computers experience a new field.

Adding to the information from Code.org on their website, there are a number of other resources that are broken down into grade levels. For the high school level, some organizations that offer further coding or computer science courses for free include Beauty & Joy of Coding, Codecademy, ScratchEd and TEALS (Code.org, 2015). Code.org is committed to the idea that even if your school does not work directly with them, they want to provide the public with as many realistic, user-friendly resources as possible to make computer science a standard for all grade levels.

The National Cyberwatch Center is an organization that is also interested in solutions to strengthening the cybersecurity workforce. They achieve this through collaborations with universities and institutions, businesses and government agencies (National Cyberwatch Center, 2016). Cyberwatch has even caught the eye of the President in 2012 when he was giving a speech at Northern Virginia Community College and praised the work the organization had done at the college level helping to prepare students for a career in the cyber field (Cimons, 2012). Though Cyberwatch mainly collaborates and works with colleges and universities, it has begun expanding its reach, "including a program for K-12 students with a curriculum track for high schoolers, summer camps, after school programs, students' contests and workshops" (Cimons, 2012). The willingness of organizations that shape the future of cyber education to create useable and effective programs for students younger than college proves the importance of the issue. The National Science Foundation that helps fund Cyberwatch intended for it to be a vessel by which to bring more training and education in the field of cybersecurity to as many people as possible (National Cyberwatch Center, 2016). More information about the National Cyberwatch Center can be found on their website.

With the future of the cybersecurity workforce being determined by the resources students are provided during their K-12 years, the DHS created the National Initiative for Cybersecurity Careers and Studies (NICCS). Their focus lies in expanding resources for teachers to train in cyber skills and increase awareness of what a career in cybersecurity would mean for those who choose to pursue these skills (U.S. Dept of Homeland Security, 2016). The promotion of the inclusion of cybersecurity and computer science in the K-12 classroom has become essential because of the workforce issue. Many arguments used for squeezing computer science into school's already tight curriculum is that students will gain practical skills with real-world applications that, should they choose to continue studying in the field, lead to a wealth of job opportunities. The NICCS sees that and through programing and curriculum development works towards making that a reality for all students.

Digital Citizenship

Any discussion on cybersecurity must also include the idea of digital citizenship, a topic which schools and organizations across the globe have taken notice of and are beginning to work into the curriculum of the 21st century. Though digital citizenship does include general standards and 'rules of behavior' for online usage, there is still comparatively a very small amount of societal laws governing what takes place online. Digital citizenship is not just 'digital etiquette', while it encompasses the rules of digital behavior, it is so much more. It is for this reason that schools are beginning to teach students as early as possible what is acceptable and what their online responsibilities are, so they will be less likely to become victims of cybersecurity attacks.

A common theme throughout most research and literature discussing the topic is that students learn best through active engagement with computers and mobile devices. Therefore, the first step in teaching digital citizenship is to equip classrooms with technology which allows

for an interactive experience. The Making Learning Mobile Project, through the Project Tomorrow organization, took place over a three-year period, exploring student and teacher usage of technology in the classroom when each individual is given an Internet-connected tablet (Project Tomorrow, 2014). This study explored the effect of mobile learning on teacher effectiveness and performance as well as if students are motivated to extend learning beyond the classroom. The project focused on how mobility affects education, finding that students only became comfortable with the technology once teachers were confident incorporating it in their lessons on a regular basis. Though the information online does not give specific details about curriculum, the report does directly address students' introduction to the development of skills necessary to become responsible digital citizens, done in the safety of the classroom with instruction (Project Tomorrow, 2014). While the exploration of digital citizenship in the classroom has become more prevalent, it is important to understand what it actually means for both students and teachers.

While there is a wealth of information on the "digital revolution", there is surprisingly little when it comes to the actual elements of digital technology. The site Digital Citizenship: Using Technology Appropriately (Ribble, 2016) was put together by Mike Ribble who has taught a variety of educational levels in both the public and private sector. His ideas include nine themes or elements of digital citizenship which covers all aspects of what it means to be a participating member of an online community. What makes this site important is not just the information Ribble brings to us, but his ability to take highly technical concepts and explain them in such a way that they have relevance for everyday users. The nine elements of digital citizenship are: digital access, commerce, communication, literacy, etiquette, law, rights &

responsibilities, health & wellness, and security (Ribble, 2016). Each of these elements work together to give a picture of how we, as individuals, interact with each other in the digital age.

In addition to Ribble's nine elements, he co-authored an article with Lotta Larson and Teresa Miller on considerations for administrators implementing new technology into their educational institution (2009-10). The article "5 Considerations for Digital Age Leaders" asserts that administrators and teachers need to take the lead on technology integration in the classroom and changes in technology implementation. They cannot rely solely on support staff, as it is educational leaders who are responsible for bringing classrooms and schools into the digital age (Larson, Miller, & Ribble, 2009). With the proliferation of new technology available to schools, educators and scholars have begun to realize that digital learning is the future of the educational experience. In a Huffington Post blog article "Technology for Schools and Teachers: 5 Reasons Digital Learning Matters" from March 2013 (Steinberg, 2013), it is said that schools are rapidly changing from what they used to be, to incorporate a technology-driven curriculum structure. It is important because 'digital learning' allows for personalization, accessibility, cultural relevance, efficiency and performance (Steinberg, 2013). Once again, the importance of active creation within a digital forum is stressed.

Student engagement with curriculum material digitally is referenced in material from organizations such as Creative Educator, Getting Smart, Educause and even PBS, furthering the idea of the importance of digital citizenship in new learning mediums. Creative Educator (Tech4Learning, 2016) and an article on Getting Smart written by Megan Mead (Mead, 2016) both stress the role the creative process plays in digital citizenship, allowing students to take ownership of their work and become more confident. Creative Educator discusses four ways for teachers to engage their students in material by using a new digital platform. Tapping into

students' passions and connecting to their world on their level gives students an ownership of material and increases their awareness of the new potential open to their educational experience (Tech4Learning, 2016). The article written by Mead on the Getting Smart site, "Interaction with Digital Content: 5 Actions to Look for in Your Students' Online Experience" reaffirms the idea that if students are actively engaging with the material in ways that allow them to show what they have observed, create something, see a new perspective, this shows they are getting the material (Mead, 2016). Ultimately, curriculums that do that are successful in producing highly aware digital citizens.

Looking at digital citizenship and technology in the classroom from an educational background, a new paradigm beginning to show presents a significant shift in the pedagogy of teachers. The value of this shift has been explored and reported by organizations such as Educause and the International Society for Technology in Education (ISTE). Educause is a "non-profit association and the foremost community of IT leaders and professionals committed to advancing higher education" (Educause, 2016) Malcolm Brown, Joanne Dehoney and Nancy Millichap authored The Next Generation Digital Learning Environment (Brown, Dehoney, & Millichap, 2015) under Educause's learning initiative. Their paper discussed learning management systems and how those can be layered within digital learning environments. Also discussed is how the classroom has been affected by the introduction of technology as a 'norm'. Rather than dismissing digital learning as a phase, Brown, Dehoney and Millichap are integrating the notion of it into the pedagogy of learning (Brown, Dehoney, & Millichap, 2015). How this ties into digital citizenship is explained in ISTE's article by Andra Brichacek, Infographic: Citizenship in the Digital Age (Brichacek, 2014). In it, Brichacek explains how parents and teachers are calling for digital citizenship to be added to the curriculum because of

all the difficult issues students today now face. Those issues include social media, cyberbullying, cybercrime, internet addiction and online privacy concerns (Brichacek, 2014). We can see from previous articles and explored that proper digital citizenship curriculums address each of these concerns, and can be tailored for different age groups.

The Center for Digital Education shares an article on their news page about using data analytics to keep schools safe. In a 2015 article, Managing School Safety in the Digital Age (Industry Perspective) (Ware & Boatman, 2015), authors Bryan Ware and John Boatman explain how administrators are expected to work with local law enforcement to keep schools safe. Though there are many threats made to schools online, there are new initiatives such as data analytics on-site and cloud collaboration (Ware & Boatman, 2015). It is because of the threats made to schools that it is important to teach with digital technology available in the classroom, but to show students its capabilities and what a responsibility it is.

Another organization exploring how digital media has become ubiquitous in the classroom is the Public Broadcast System (PBS) who produced a special Digital Media: New Learners of the 21st Century (Digital Media - New Learners of the 21st Century, 2013) produced by Mobile Digital Arts and Twin Cities Public Television. In the documentary, digital media is called an "educational revolution" and talks about "digital afterschool programs and their potential relationship to in-school practices" (2013). Through this, we learn how technology is allowing students the freedom to direct their own learning and communicate with peers on a global scale (2013). The first part in a multi-series program about the growing and evolving face of education lends credence to the idea of technology helping shape students values; both on and offline. Being introduced to digital citizenship before leaving high school gives way to a higher appreciation for the skills necessary for effective communication in the 21st century.

Communication Theory

Looking at how students are being prepared in schools for digital citizenship also sheds light on how schools function as organizational structures, and their methods of communicating with students and teachers. Before looking at that, it is important to first have an understanding of what type of communication is being used. The interaction school administrators have with students and teachers can be understood by looking at organizational communication. BusinessDictionary.com defines organizational communication as "A process by which activities of a society are collected and coordinated to reach the goals of both individuals and the collective group" (WebFinance, Inc.). Looking through the lens of communication theory, we can see a school community made up of students, teachers, staff, and administrators, all working towards the goal of furthering education. In his book Organizational Communication, Gerard M. Goldhaber (Goldhaber, 1990) cites how research proves that high performing organizations are those that understand and use effective communication throughout (Goldhaber, p. 5). The specifics of how an organization communicates with its employees makes all the difference. With the knowledge that we live and work in the digital age, most organizations have made the move to electronic correspondence as the fastest and most effective mode of communication. Yet emails are not the only way companies, organizations and school districts can reach those they work with.

As social networks have become an almost inescapable part of communication theory, it is not surprising that so many scholarly articles, research studies, and books have been written on the matter. Books such as Brian V. Carolan's "Social Network Analysis and Education: Theory, Methods & Applications" and Alan J. Daly's "Social Network Theory and Educational Change" (Daly, 2010) explains what this theory can tell us about the world of education and the

interactions within. Daly's work tells us, "Social network research suggests that informal webs of relationships are often the chief determinants of how well and quickly change efforts take hold, diffuse, and sustain". While it may seem instinctive to think of social network theory as a result of the prevalence of online social networks in society, it is actually the direct opposite. Social networking sites such as Facebook, Twitter, and Instagram gained popularity from the utilization of the principles of social network theory. The definition of the theory is, "the study of how people, organizations or groups interact with others inside their network" (Claywell). Social networks have made it easier and more convenient to get in contact with another party but it has also left users' personal information exposed to cybercriminals and potential malicious software. Any person's sensitive information such as address or debit/credit card number could be seen and used against them if it is shared through an unreliable site and to an unreliable source. However, does this theory have anything to do with the educational experience? As it turns out, social network theory as well as networking sites play quite a part in the communication plan of a school district.

In addition to the traditional communication methods such as emails, memos, website announcements and Facebook or Twitter account posts, Shrewsbury Public Schools uses Schoology in and out of the classroom. This system is the hub of where all course work takes place and mimics the look and feel of Facebook, which is so popular with the students who use it. Shrewsbury School District uses Schoology to communicate with students and of the familiarity they will have with the format.

When looking at cybersecurity from an industry perspective, the importance of it is now at an all-time high as more adolescents utilize the internet for almost all of their needs, from entertainment to assistance with everyday tasks. Many groups and initiatives have been created

for the prevention of cyber-attacks, but the one of the most prevalent is the Team for Research in Ubiquitous Security Technology (TRUST), which "…focuses on the development of cybersecurity, science, and technology" (Heidenreich & Gray, 2013, p. 22). What is different about this organization is that instead of regular forms of cyber protection functioning by reaction of a threat, "TRUST believes today's security should be proactive which is possible through developing systems in a principled way" (Heidenreich & Gray, p. 22). This will be done by trying to find ways to expose threats. Heindenreich and Gray's statement of the United States being both aware and prepared within our cyber environment and our Nation's information infrastructure (Heidenreich & Gray, p. 25) is extremely accurate as it relays the importance of cybersecurity as more people log on to the internet.

The topic of cybersecurity continues with the patterns of cybercriminals described by Hamid Salim (Salim, 2014). He states the sophisticated methods of cybercriminals work such as using malware and other engineering to gain personal information, using big companies such as TJX and Marshalls as examples of real-life attacks done by hackers (Salim, pp. 103-104). He even goes as far as questioning the safety of the now-common cloud computing and use of Web 2.0, in which the user doesn't even know where their confidential information is stored or how safe and/or secure it is (Salim, p. 16). Although his paper talks more about cybercrime towards big businesses, it still serves as a harsh reminder of what cybercriminals are capable of towards individual citizens, since any personal information that is shared with businesses could possibly be accessible to criminals. Also, he delves in how these methods of cybercrime make it difficult to measure the cost put on a business.

One business that has made its way into almost daily headlines for its stance on cybersecurity of its customers is Apple. When tech giant Apple refused to create a 'hack' for the

United States Federal Bureau of Investigation (FBI) to gain access into the iPhone of the San Bernadino shooter, they cited the rationale as being too dangerous to allow that kind of software to exist. "Apple executives have said creating one skeleton key to break into iPhones opens a portal to all - including cyberterrorists. Penetrating software released to law enforcement could fall into the wrong hands, too" (Allen, 2016). An article in the Worcester Telegram and Gazette on March 19, 2016 states Worcester Police have also petitioned to Apple for help unlocking iPhones, but to no avail (Allen, 2016). Both Apple and the police department say they are trying to protect the public- one from terrorism, one from invasion of privacy.

Technology is forever advancing and improving, both for cybersecurity and cybercriminals. The literature reviewed here proves the precarious nature of online adolescent behavior. If students are taught about cybersecurity from an early age, they may be encouraged to learn and apply cybersecurity practices to their current activities, as well as develop those practices into adulthood.

Chapter 3: Methods

Design

The team met with the Shrewsbury Public Schools Director of ITAMS (Instructional Technology and Media Services), Shawna Powers, and Director of Information Technology, Brian L'Heureux, to not only discuss the scope of the project, but also get a sense of the environment in which the curriculum would be completed. During the requirements gathering process, the MSIT group members evaluated the constraints inherent in the environment, in order to appropriately address these in the design of the course materials. The four major constraints identified were; (1) the 1:1 technology program's use of iPads in the classroom as the primary means of completing the learning, (2) the school's use of the Schoology platform to host the digital learning curricula, (3) the voluntary basis upon which students will be asked to complete the learning, and (4) the homeroom period time constraint for each module.

If students encounter errors or technical difficulties while attempting the modules, due to the lack of other incentives for completion, they may abandon the curriculum altogether. In addressing the constraint of iPads and the iOS operating system not supporting flash media, the MSIT team members decided that purely HTML5 interactions would be preferable. HTML5 is natively supported by all operating systems and browsers, with a few exceptions to specific tags and methods. This will ensure an error-free experience to for the students of the school district as they are completing the modules, increasing the likelihood of completion.

To address the constraint of the Schoology platform and the potential for not being able to use encapsulated webpages and/or JavaScript interactions, the MSIT team members first tested basic HTML webpages in a "dummy" course setup by the district. While the Schoology platform does not block HTML pages, it doesn't inherently provide the URI file & folder

structure as a website would when uploading web resources via FTP. After testing several of the functions available in Schoology, the team discovered that when uploading a .zip archive directly, the files within the archive would not be available and linked to one another. The team learned that by adding the .zip archive as a "Package" in Schoology, and selecting the option for "Web Content", the files and resources would be linked together and work properly. It is of note that the Package uploaded seems to have a 10GB maximum file size, however it is unexpected that any of our modules will come close to that limit.

In addressing the constraint of "dangling the carrot" to entice the students to complete the training, the team evaluated the trends in the industry (schools implementing IT and cybersecurity into their curricula). The PBS Nova Labs Cybersecurity Lab provided solid "proof of concept" ideas for the team. Games, such as the ones used by the PBS Nova Labs, Cybersecurity Lab (PBS/WGBH - Nova Labs, 2016) are ideal for encouraging high school student participation.

In order to utilize the trends in the industry and demonstrate the real-world applicability and importance to the students, the team drew upon the recommendations of the National Initiative for Cybersecurity Careers and Studies (U.S. Dept of Homeland Security, 2016), where many other web resources are made available. Each of these resources focuses on a different segment of the population, ranging from the very young (elementary school age) to adults. By drawing upon the techniques presented by each, the team was able to determine how best to target this information to high school age students.

Finally, the team had to address the constraint of making the modules self-directed, and concise enough that they may be completed within the 10-15 minute homeroom period. Because of union requirements and fairness to teachers that have not been trained in the subject matter,

they cannot be asked to teach a new curriculum without any prior training. Additionally, the district does not want to impose additional graduation requirements upon the students. Based upon client recommendation, it was decided that individual modules, which can be completed within the 10-15 minute homeroom period was ideal. This would allow the modules to be completed by the students at any point in which the homeroom period was not being used for other content.

In order to provide adaptability, so that modules can be completed in any sequence, it was decided to avoid making any content based upon other modules. This allows the faculty to take advantage of real-world occurrences and ask students to complete a module related to that occurrence. This does not bar the development of intermediate and advanced level modules that can build upon the core foundational modules.

Materials

While the primary delivery method for the curriculum will be the students' iPad devices, the content can be accessed from a Windows, Linux, or Android device. The only requirement will be access to an internet connection, as the Schoology platform itself is online. Some of the modules include videos that are hosted online, often at federal agency websites, which also require an internet connection. No experience with computer science is necessary to complete the training curriculum. Though the modules are designed expressly for students with minimal or no knowledge of computer science, suggestions for intermediate level modules are provided for the client.

In addition to the core content of the curriculum, promotional items are suggested, in order to obtain student "buy-in" to the curriculum, and foster interest throughout the school. The group is recommending an introductory video, relating the concepts of cybersecurity to the

students, and explaining the real-world importance of the subject matter. Some graphical posters can be used to instill a sense of relevancy around the school as well.

In order to encourage participation, the group is recommending utilizing the built-in functionality of the Schoology platform to provide "badges" to students that complete certain modules. The curricula administrators can provide badges for students that complete:

- 1 module – Cyber Security "White Belt"

- 3 modules – Cyber Security "Yellow Belt"

- All 5 basic modules – Cyber Security "Green Belt"

- 2 Intermediate modules – Cyber Security "Red Belt"

- 5 Intermediate modules – Cyber Security "Brown Belt"

- 2 Advanced modules – Cyber Security "Black Belt"

Ethical Concerns

The Children's Online Privacy Protection Act (COPPA) is designed to protect children under the age of 13. As the high school students all are above 13 years of age, there are not concerns regarding the age restriction imposed by COPPA. Additionally, all students are already provided an Apple ID by virtue of their enrollment at the school. There are no additional requirements for privacy with the curriculum, as no personal information is collected. To the contrary, the curriculum is designed to teach the students how to protect themselves online.

The Americans with Disabilities Act (ADA) (U.S. Dept of Justice, 2007) requires that equal educational opportunity be provided to all students. While Section 508 of the Rehabilitation Act of 1973 (as amended) pertains to federal agencies, Section 504 imposes similar requirements of accessibility for educational opportunities (U.S. Dept of Education, 2015). Section 508 may be used to inform decisions about accessibility for digital content, to meet the requirements for both the ADA and Section 504 (U.S. General Services Administration, 2016).

The internet and web development community has long stayed ahead of the federal regulations, in an effort to provide a positive user experience to all people. As a result, federal regulations are based upon the standards and guidelines set by the World Wide Web Consortium (W3C) (World Wide Web Consortium, 2016); specifically the Web Content Accessibility Guidelines (WCAG) (World Wide Web Consortium, 2016). By following the generally accepted web standards already incorporated into HTML5, and the WCAG 2.0 standards, the curriculum will inherently be compliant with federal regulations and accessible to students with disabilities.

In addition to the content within the curriculum being accessible, the team also reviewed support articles from Schoology, to determine if Schoology itself is accessible. The support articles indicate that it is designed to meet the requirements of ADA and other accessibility guidelines (Schoology, 2015). The articles indicate that Schoology works with the major screen reader software, and support is available if needs are not met (Schoology, 2015). The team researched other legal requirements and ethical guidelines, and found that all other aspects of the curriculum seem to be in compliance with, and support recommended practices.

Chapter 4: Findings & Data Analysis

Overview

Computer science education is popping up in schools throughout the country, including Massachusetts. By comparing findings on the national level with those from the state of Massachusetts, we can see where strides have been made, and also were we can do far more for cyber education. Also included are ideas which came out of an interview with staff of Shrewsbury Public Schools to see what their specific needs for a cybersecurity curriculum are. These findings have aided in directing us in development of the modular cybersecurity curriculum designed for Shrewsbury High School.

Data Analysis

In 2014, Google asked Gallup, a research business, to help collect data relating to computer usage in the classrooms, across the United States, and how those numbers change (if at all) when factoring in the grade level or race of the student. The research also included collecting the priorities and opinions of school leaders towards computer education. It was discovered that the higher the grade level, the more likely students are to use computers every day in class, going from 31% in 7^{th}-8^{th} grade to 50% in the 11^{th}-12^{th} grade. There was also a disparity found amongst different ethnicities. Hispanic and Black students were less likely to have access to a computer at home or a parent/guardian that works in a computer-related field (Google/Gallup, 2015).

Though both parents and students who participated in the study expressed their support and desire for there to be more computer programming offered in schools, most administrators said the opposite. “Despite the value students, parents, teachers, and school administrators place

on computer science, teachers' principals and superintendents are unlikely to say computer science education is a top priority for their school or district, and less than half say their school board thinks it is important to offer computer science education" (Google/Gallup, 2015). In summation, the study done by Gallup showed a nation that does not currently give wide-spread, daily in-class access to computers for all students, and most administrators do not consider this a top priority to fix.

STUDENTS

			GRADE LEVEL		
		Total	*7th or 8th*	*9th or 10th*	*11th or 12th*
Are there classes where ONLY computer science is taught in your school?	*Yes*	58%	45%	61%	69%
	No	37%	53%	31%	25%
	Don't know	5%	2%	7%	5%
Is computer science taught as part of OTHER classes at your school?	*Yes*	52%	46%	54%	57%
	No	42%	49%	38%	39%
	Don't know	5%	5%	8%	3%
As far as you know, are there any groups or clubs that meet at your school where students learn computer science?	*Yes*	43%	37%	43%	48%
	No	51%	60%	48%	46%
	Don't know	6%	4%	9%	6%

Figure 1: Computer Science Learning Opportunities by Grade

(Source:"Searching for Computer Science: Access and Barriers in U.S. K-12 Education," 2015)

For a more fine-tuned look at an area more specific to our client, it was necessary to investigate the state of computer science education in Massachusetts. According to The Massachusetts Department of Elementary and Secondary Education (ESE) 2015-16 school year profile, Massachusetts is home to 315 middle/junior high schools and 396 secondary public high schools (Massachusetts Dept of Elementary & Secondary Education). Code.org reports that "9 in 10 parents want their children to learn computer science, but only 1 in 4 schools teach it" (Code.org, 2015). This is supported by further data from Code.org that in the 2014-2015 academic year, a mere 137 Massachusetts schools offered the Advanced Placement Computer course (Code.org, 2015). Although the rate for now is not great, the trend of students paying

attention to computer science is growing. In 2015 there were 25% more students participating in Computer Science Advanced Placement Program (AP) exam than in 2014, while the rate of schools offering the Computer Science AP exam grew by 15% from the 2014 figures through the country (The College Board).

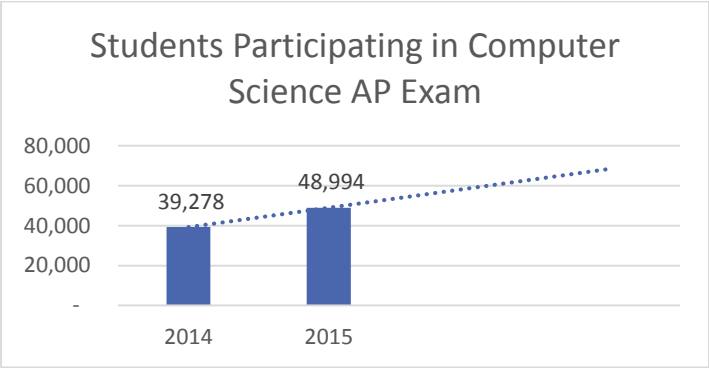

Figure 2: Student Participation in Computer Science AP Exam

One of the areas which has stunted the growth of a more vibrant cyber technology program is the lack of state-wide computer science standards. Suggestions made by Code.org include a standard that is, "focused on both the creation and use of software and computing technologies at all levels," ("Support K-12 Computer Science Education in Massachusetts", Code.org). Without a united standard, high schools in Massachusetts could find developing a computer science program difficult. Different schools will determine what they consider to be the most important aspects of technology, with no professional guidance. Without course standards based on scientific research, curriculums created by each school might not fit what students really needs, doing them a disservice. Courses must be designed at appropriate levels, to give students the best chance for success.

Code.org also suggest that making computer science a core graduation requirement, Massachusetts could see a 50% enrollment increase in AP Computer Science courses as other states did. It also served to increase science courses, as other states did, and increases underrepresented minority populations (Code.org, 2015). If Massachusetts were to add computer science as a core graduation requirement, it would do more than just exposing those who may have never taken a computer class to a

new world of possibilities. It also shows the Department of Education (DOE) supports and is actively engaged in increasing student technology participation. The support and approval of the DOE raises the profile of the importance of cyber instruction in Massachusetts schools.

Interview with SPS District Employees

An interview was conducted by the Capstone Group with Shrewsbury Public School employs Brian L'Heureux, Director of Information Technology, and Shawna Powers, Director of Instructional Technology & Media Services. From the interview, we learned there are already computer science courses such as Java Programming, Multi Media, and Web Design offered at Shrewsbury High School. They use Schoology (https://app.schoology.com/home), an e-learning, online system for course selection and curriculum instruction. Currently they have no curriculum that would function as an independent study for students are hoping to learn more about computer science. They have requested a cybersecurity course in an independent instruction modular format.

The course modules need to be self-directed and will be voluntary, non-graded, and fit in the 15-minute homeroom time. The initial discussion of the curriculum included the requirements of real-world relevance, interactive, short and appropriate degree of difficulty. To make the course work best for the Schoology platform, we will use independent modules for different cybersecurity topics, limiting each module to 10-12 minutes in length. There was also some discussion of the possibility of creating two different versions of the curriculum: “lite” or “basic” for all students, and an accelerated version for students who are interested in more in-depth material.

During the interview, we were given an opportunity to see the Schoology platform we would be using for the modular courses. As the system itself looks similar to the layout of the popular social networking site Facebook, we were encouraged to take advantage of the use of

"badges" and "class cup" to encourage students participate. Other possible ideas brought up during the interview to incorporate the badges were quick videos to establish the real-world relevance of the topic and quiz games.

Salient Issues

The more research done, the more inherent issues were found on the topic of cybersecurity that must be taken into consideration.

- Since cybersecurity is still relatively new, authoritative resources are limited. Some concepts in the field do not have clear, universal definitions, leading to different organizations giving their own interpretation. When it comes to the curriculum for cybersecurity used for schools, because there is no standard, schools are likely to put together a curriculum that teaches only what they feel is relevant to their schools. Not only does this potentially miss a wealth of other important information not considered, it robs students of the opportunity to experience a new field fully.
- Cybersecurity is more than just a technology issue; it also includes social issues. The personal information people put online puts them at a higher risk for theft or identity fraud, but social media is also a risk. Millions of people are on various social media platforms every day, whether for entertainment or professional purposes. Though these sites were originally created as tools, they have been turned, for some, into platforms to cultivate and coordinate messages and plans of hate and harm.
- When considering the curriculum for Shrewsbury High School, there were time constraints to consider. Students only have homeroom twice a week for 15 minutes. It was determined that though the time was minimal, it was the most appropriate schedule allotment for the program.

- Public schools have certain required class for graduating, also known as “core classes”. Trying to fit technology electives into schedules is difficult. Since this cybersecurity program is not a required course, it makes how it is presented to students critical to its success.
- Cybersecurity is a constantly evolving field of technology, where information can become obsolete very quickly. In one hand, it is difficult to stay aligned with the latest progress in the cyber security field, since changes happen so frequently. As new threats keep appearing, the curriculum must be updated with the corresponding solution. Yet, when new cybersecurity threats evolve, the solution is not always available immediately, therefore creating a gap in the curriculum between problem and solution. Not only does the curriculum need constant reviewing for accuracy and relevancy, but the method of delivery also needs to be taken into account. In general, the curriculum needs to be revised every time before it is used, which require time and resources.
- The complexity of the cybersecurity applications may become an obstacle for students to form the concept of the cybersecurity system. Some cybersecurity applications only have one function; some consist of a group of functions. There will be functions overlapping between applications. As the cybersecurity solution evolves, there will be different versions of an application. The open-source software is not guaranteed to maintain customer service, and may even stop updating in some cases. Another source of software and simulator may add stress to the budget. Students need easy-to-use, up-to-date training tools, so that they can focus on learning the principles.
- Union contracts present a barrier to teacher participation in our program. Teachers are not contractually obligated to participate, nor can they be asked to teach more than what

their contract specifies. It is possible that low teacher support for the project could have a negative impact on participation rates among the students. However, there are some teachers that have responded positively and with enthusiasm to the addition of technology in the classroom and Ms. Powers feels will likely be supportive of the cybersecurity curriculum we create.

Chapter 5: Recommendations

Overview

During the initial meeting with the Shrewsbury Public Schools personnel, the team discussed the district's ideas for the curriculum, the technology available, constraints on content delivery, and possible methods of obtaining student "buy-in". The team determined that the most critical requirements of the project are:

- 4-5 modules delivering a cybersecurity curriculum
- The modules can be delivered on an ad hoc basis
- The modules can be completed during homeroom sessions (10-12 minutes)
- They do not contain any requirements for administration or testing
- They are self-contained modules, without reliance upon other resources or tools
- They do not require prior knowledge of cybersecurity or completion of other modules

The team submitted a Datasheet and Project Plan to the school district, to confirm the requirements identified, and obtain approval of the selected module subject matter. The project was completed with these requirements set as a priority, with additional recommendations and information provided where possible. The recommendation of the team is to implement the following curriculum architecture; which will provide a robust and flexible cybersecurity curriculum, serving the many needs of the district.

Curriculum Architecture

The recommended curriculum architecture consists of 3 tiers of education. The first tier is targeted towards all students, with the goal of providing a basic cybersecurity foundation for all graduates of the Shrewsbury Public School system. In the current digital age, where almost everything involves technology, it is critical to prepare students for the "connectedness" of the world. The second tier will

provide additional learning opportunities, for students interested in going beyond the minimum, as well as a launching point for information technology clubs. This tier will also focus on digital citizenship, and teaching students how to not only keep themselves safe from cyber-attacks, but also how to act responsibly in the digital world.

In addition to information technology clubs, students participating in the Student Innovation Team (SIT) will also benefit from additional cybersecurity training beyond the basic foundation, when they are asked to provide frontline technical support for students and faculty as part of the 1:1 Technology program. Finally, the third tier of education will be focused on delivering cybersecurity topics that can be used as discussion points for computer science courses, information technology clubs, and act as a "primer" for students expecting to continue into collegiate level information technology studies.

The recommended 3-tier approach would consist of:

(1) Basic Foundational Modules

(2) Intermediate Digital Citizen Modules

(3) Advanced Ethical Hacking Modules

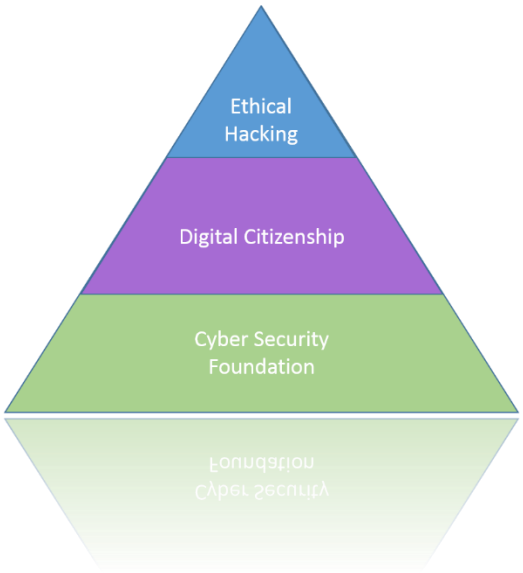

Figure 3: Three-Tiered Curriculum

While the 3rd tier title includes the term "hacking", it should be understood that proper use of the term does not apply strictly to malicious computer actions. Instead; "hacking" refers to using personal expertise to drive a system to perform in ways that are not originally intended. "Ethical Hacking" then imparts the mindset that while innovation and experimentation are the hallmark of information technology; technological innovation and experimentation should not be conducted without regard to ethical implications of those actions.

In addition to the basic foundational modules, an introductory video should be presented to the students during the first homeroom session. This video should be designed to encourage participation in the cybersecurity curriculum, by relating the subject matter to the "real world" of the students, and demonstrate the importance of understanding how to stay safe in a digital world. The introductory video should be presented as part of an official launch of the curriculum, after using promotional posters and other publicity to foster "buzz" about the curriculum.

The following sections outline the details of each of the basic foundational modules, as well as additional recommendations for the curriculum. The 5 basic foundational modules are:

- Phishing and Spam Emails
- Social Engineering
- Internet Browsing Security
- Wireless Attacks
- Malware Introduction

General Module Completion Use Case

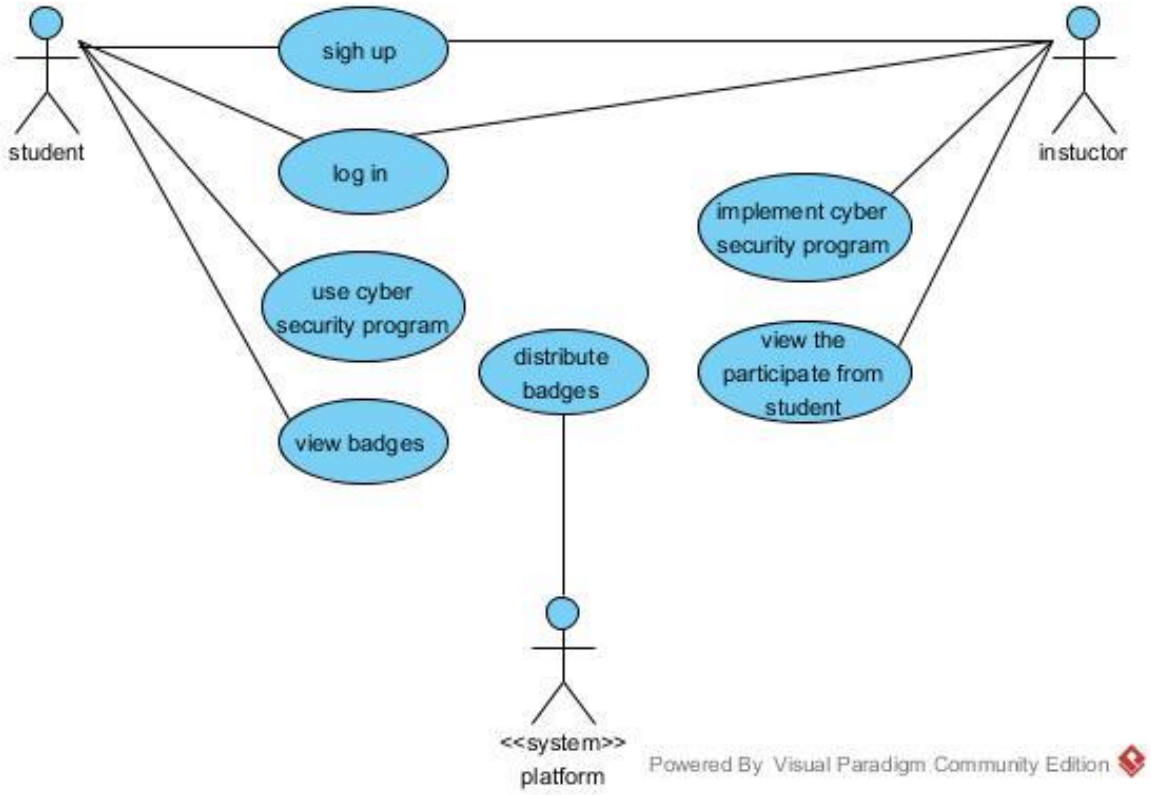

Figure 4: Module Completion Use Case Diagram

Basic Foundational Modules

Introductory Video

As mentioned in the overview, an introductory video should be used to generate interest, awareness, and "buy-in" from students. Nova Labs from PBS has developed a video (3:52) that perfectly explains how the internet has become such a dangerous place, and why it is so important for everyone to understand cybersecurity: https://www.youtube.com/watch?v=sdpxddDzXfE. (NOVA PBS, 2014) Additionally, the Federal Trade Commission has developed a video (3:32) that broadly covers personal computer security: https://youtu.be/yeepZr64XjU. (Federal Trade Commission, 2013) These two should be presented in sequence, and combined they will explain why cybersecurity awareness is important, and provide quick tips to all students as a primer for the rest of the curriculum.

Module 1 – Phishing and Spam Emails

General Information

Module 1 will focus on teaching students how to identify phishing attempts, specifically those conducted via email. While spam filters at multiple levels are built into all email systems, including free ones, these filters do not always succeed at blocking phishing attempts. This is especially true when sender spoofing is used. An example of a phishing email; would be an email that claims to be from the recipient's banking institution, and says that they need to click a hyperlink in the email to go to the bank's webpage where they will verify their SSN. The hyperlink then points to a false webpage, made to look like the bank's webpage, and collects the personal information for later use in identity theft.

Topics to Cover

- Don't trust the display name (spoofing)
- Hover over any links first (check actual URL)
- Look for and be aware of spelling mistakes (most orgs have multiple QA checks)
- Check the salutation (general or specific; equivalent of "Current Resident")
- Never give personal information via email (this includes legitimate emails)
- Be strongly wary of urgent or threatening language (nothing urgent is done via email)
- Review the signature line (legitimate businesses usually provide contact info)
- Don't open attachments you don't expect (if it's unexpected; it's likely malware)
- Don't trust the "from" header (67% of spoofs also fake the origin email address)
- Pictures can be reused by anyone (just because an email has a logo doesn't make it real)

Structure/Scenario

Users will receive an introductory explanation of what phishing and spam emails are, and telling them that they need to be wary of messages that they receive, which may or may not be legitimate messages. After going through the introductory explanation; users will be given an exercise where they are provided a set of 4 email messages to review. They will be told that only one of the messages is legitimate, and asked to pick the correct one. After the user chooses an email, they will be told which of the messages was the legitimate one. They will then be able to re-review each phishing message and be shown the items on each that should have served as clues to their deception. The system will remind the user before closing the module, that in the real world, they will not be told how many of their messages are fake.

Prototype Module Components

A prototype of one of the four emails suggested for the scenario has been created and uploaded to the Schoology platform, within the SPS Cybersecurity Awareness Course. This demonstrates the viability of the suggested scenario, as well as providing a visual guide for development. The prototype was developed exclusively in HTML, CSS, and JavaScript; to demonstrate that no additional e-learning tools are required. Although there are several e-learning curriculum development tools that could greatly enhance and expedite the course development. The SPS Cybersecurity Awareness Course in Schoology can be accessed at: https://lms.shrewsbury.k12.ma.us/

Because only SPS District personnel and the Project Team can access the course in Schoology, two images are provided in this document. A live demonstration of accessing the course, and the functionality of the email examples, will be provided during the client presentation and capstone defense. While these can be reused in development of the course, and

are now the property of the Shrewsbury Public School district, they are provided only as a "proof-of-concept".

Activity Diagram, Use Case, and Images

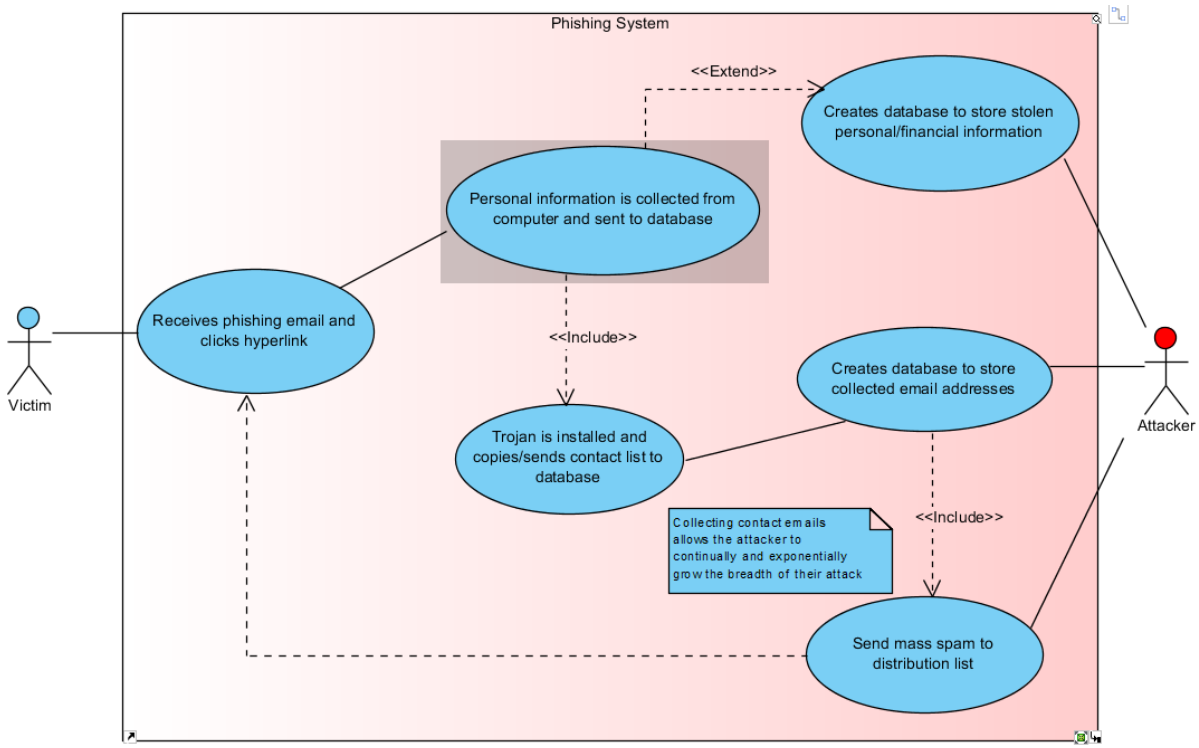

Figure 5: Use Case of a Phishing Attack via Email

From: American Bank of the U.S. <amercanbank@americanbank.com>
To: John Doe <john.doe@personalemail.net>
Subject: **Suspected Fraudulent Activity**
Date: Mon, 26 Oct 2015 15:51:13 +0100

Dear Banking Customer,

A recent transaction in a foreign country with your ATM card has been flagged as suspected fraudulent activity.

Please click here to log into your account, and verify the charges. Immediately after logging into your account, you will be provided a summary of the transaction, and the opportunity to dispute the charges.

It is critical that you complete this action within 10 days. Otherwise, we will assume the transaction is correct and you will waive your rights to dispute the transaction.

If you encounter any problems logging into our system to verify the transaction; you can send an email to the below address, including the following information, and one of our specialists will contact you via telephone:

Name as listed on the card
ATM Debit/Credit Card number
Expiration Date
CVV (found on the back of your card)
Billing Zip Code
Contact phone number at which you may be reached

Contact us at: fraudalert@americanbank.com

Figure 6: Example Email 1, pre-selection

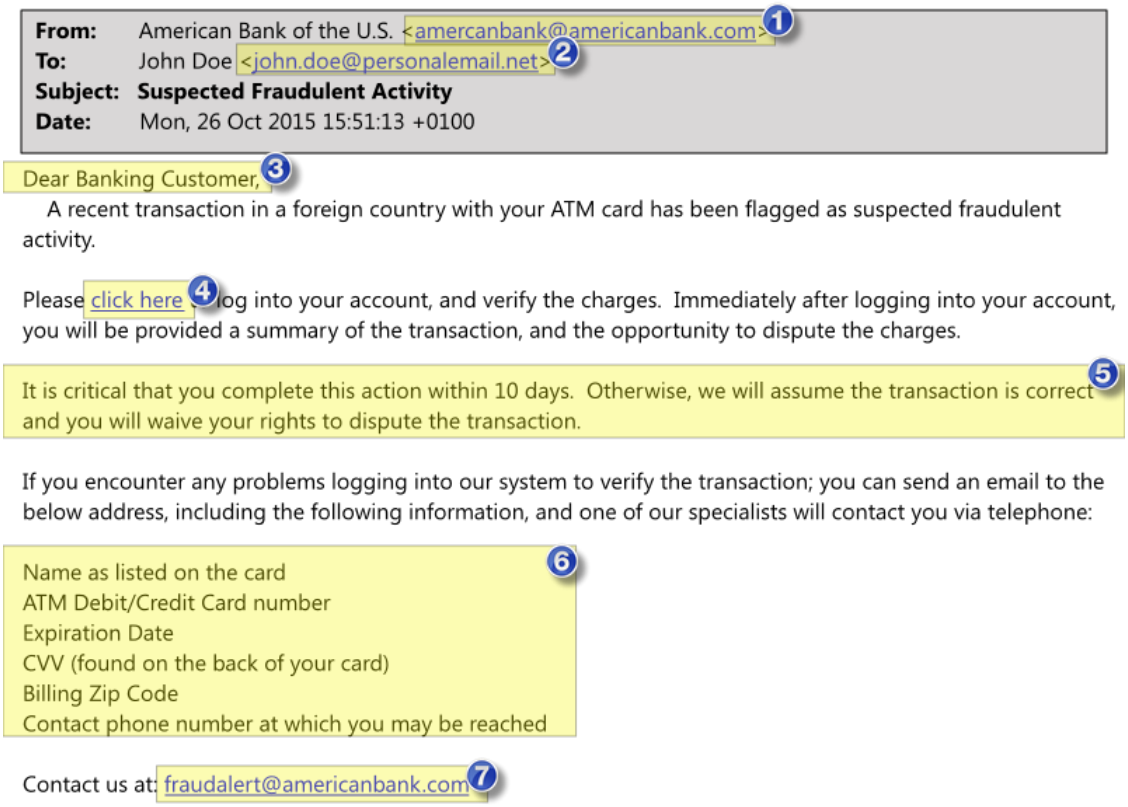

Figure 7: Example Email 1, post-selection

Additional Sources of Information:

- https://blog.returnpath.com/10-tips-on-how-to-identify-a-phishing-or-spoofing-email-v2/
- https://www.consumer.ftc.gov/media/game-0011-phishing-scams
- https://www.consumer.ftc.gov/media/video-0104-hacked-email-what-do

Module 2 – Social Engineering

General Information

Even when trained in cybersecurity and information assurance, people do not always remember the "safe practices" they're taught in mind when not actively working with technology. Social engineering aims to use social interactions (in person, on the phone, etc.) to obtain sensitive information from an individual, which can be used for cyber-attacks, identity theft, or further information gathering leading up to these attacks. Module 2 focuses on teaching students how to be aware of these threats, even when not actively using technology. The techniques learned in this module can be applied beyond technology, as they pertain to using caution with any personal interaction.

Topics to Cover

- Maintain "healthy skepticism"
- Remember who called who
- How do I know you are who you say you are?
- Do not give out personal information over the phone
- Remember that an attacker could be using you to get someone else's information
- Think about how someone could use information that you're about to give out
- Ask yourself; do they really need exactly this information, or will something else suffice?
- Legitimate organizations will respect your concerns for privacy and your skepticism

Structure/Scenario

The user will be presented with a description of social engineering, and how an attacker takes advantage of the social nature of people. The victim is often unprepared, as the attacker often attempts to gain information through offline means. Even the most security-minded person

on a computer, may not think about information security in an offline scenario, such as receiving a phone call. After being presented with an explanation of social engineering; the user will be presented with a video of an interview with one or more victims of social engineering. The module will wrap up with a reminder to the user, that an attacker may be trying to get information about someone else, and not necessarily the person they are talking to.

An example video to use is the Social Engineering Personal Story shared by AT&T ThreatTraq: https://www.youtube.com/watch?v=LgCax4xQIw4 (AT&T ThreatTraq)

Example Diagrams and Images

Figure 8: Tailgating Warning at Apple Corp.

Figure 9: Weakest Link Human Factor

Additional Sources of Information:

- http://www.social-engineer.org/
- http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering
- http://lifehacker.com/why-social-engineering-should-be-your-biggest-security-1630321227
- https://youtu.be/opRMrEfAIiI

Module 3 – Internet Browsing Security

General Information

An immeasurable amount of information is available on the web, and people rely upon this information to complete work products, college assignments, and personal tasks. In fact, the vast majority of financial transactions in the U.S. are now conducted online or electronically in some way. Unfortunately, the open nature of the internet also makes it inherently untrustworthy. This unreliability also exists in not just the content on the internet, but applications used to access the internet should also be used with caution. Module 3 teaches students to maintain a healthy level of skepticism with both online content, and the applications used to access online content.

Topics to Cover

- Use HTTPS (and look for lock icon)
- Log out every time you finish using a website
- Do not store your passwords in your web browser
- Avoid using password saving applications
- Don’t click on pop up ads or ads displayed on websites
- Limit the use of Cookies (and what are cookies)
- Introduce Featured security function of several web browsers
    - "undercover" private surfing
    - Google Chrome "sandboxing" feature

Structure/Scenario

The user will experience a two-part structure to the module. The first part will walk through the various hazards on the internet. The second part will use a browser setting screen

simulation. There will be pop-up labels when the user's mouse hovers over certain settings, which will explain how the setting works and what would be the risk if set to a different level/setting.

Example Diagrams and Images

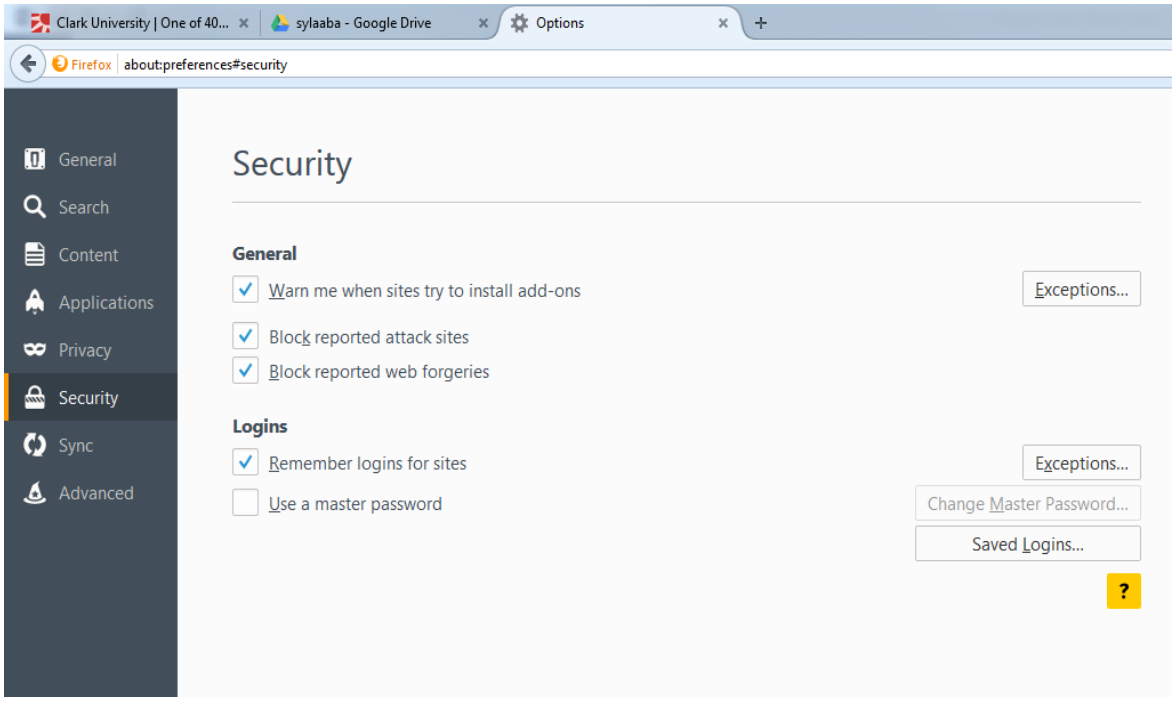

Figure 10: Firefox Browser Security Settings

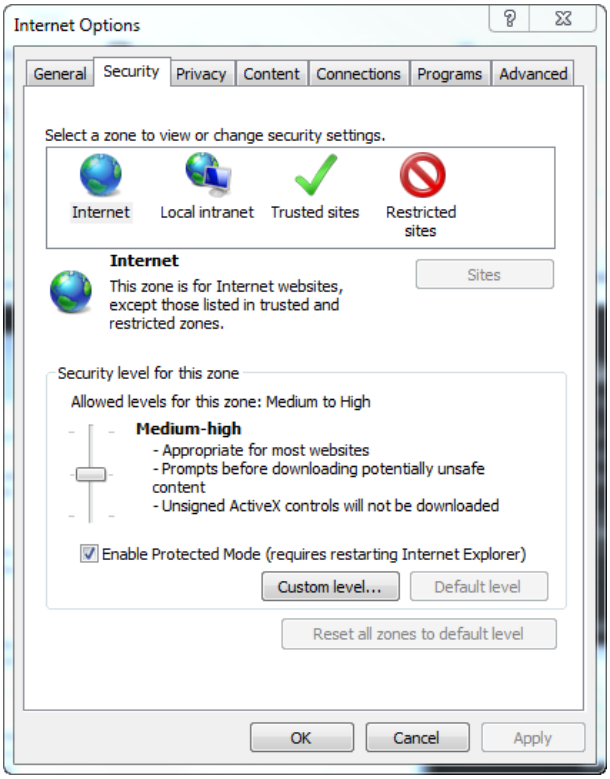

Figure 11: Internet Explorer Security Settings

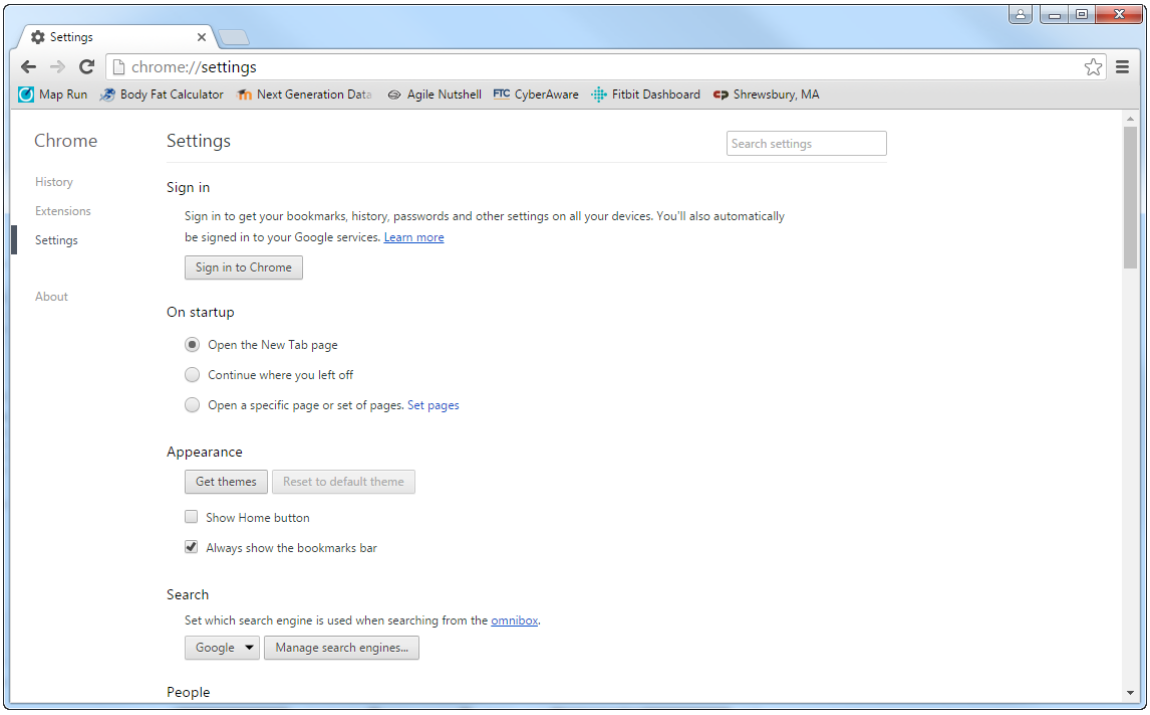

Figure 12: Chrome Browser Security Settings

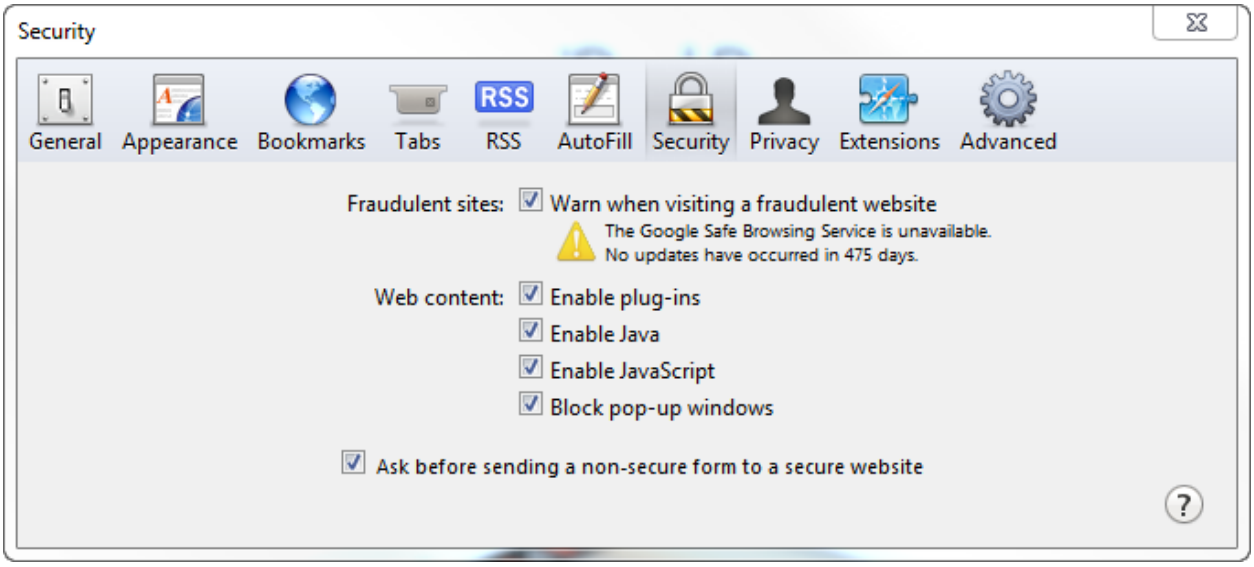

Figure 13: Safari Browser Security Settings

Additional Sources of Information:

- http://www.gcflearnfree.org/internetsafety/5
- http://www.pcworld.com/article/170518/article.html
- http://www.entrepreneur.com/article/228241
- https://www.consumer.ftc.gov/media/video-0082-online-shopping-tips
- https://youtu.be/_u8Rss3W4Wg

Module 4 – Wireless Attacks

General Information

Due to the cost of mobile internet data plans, and the ever-increasing demand for internet access, many businesses and organizations offer free/public Wi-Fi access. These access points are often referred to as "hot spots" and while convenient, should never be trusted. Users do not realize that they should never conduct any online activity through these connections. They should ensure their personal data is not shared through a public connection. Module 4 teaches students how to take advantage of these "hot spots", while ensuring their personal information remains secure.

Topics to Cover

- Configuring your client device to request approval before connecting gives you greater control over your connections.
- Disable sharing: Your Wi-Fi-enabled devices may automatically enable themselves to sharing / connecting with other devices when connecting to a wireless network
- Connect only to known, and secured Wi-Fi access points
- If you must use a public Wi-Fi "hot spot", avoid high-risk activities, or use a Virtual Private Network (VPN) connection
- Encryption types:
    - WEP - WEP is a weak security standard from 1999, which was outdated in 2003 by WPA

- WPA - WPA was a quick alternative to improve security over WEP, but is insufficient for today's standards
- WPA2 - WPA2 uses an encryption (AES) that encrypts the network with a 256-bit key; the longer key length improves security over WEP or WPA
  - Authentication types:
    - WPA2-PSK: pre-shared key (useful for home networks)
    - WPA2-802.1x: uses EAP authentication method, often Active Directory or certificate authentication (useful for many devices, enterprise settings)

- Consider using your cell phone network for inputting any sensitive information if you are in a hotel or other public "hot spot"

Structure/Scenario

The user will first watch a brief video about the security of public Wi-Fi connections, and the dangers. After the video, the user will have an exercise where they are asked to choose the safest Wi-Fi access point from four different ones shown in an image. If the user chooses the wrong access point, there will be an explanation as to why the one chosen was incorrect. The exercise can be followed up with the standard Windows prompt when connecting to a new Wi-Fi access point, which asks the user to choose what type of network connection (public, work, or home) to use. The module can show how the option chosen changes the file and printer sharing settings that Windows provides through the network.

Example Diagrams and Images

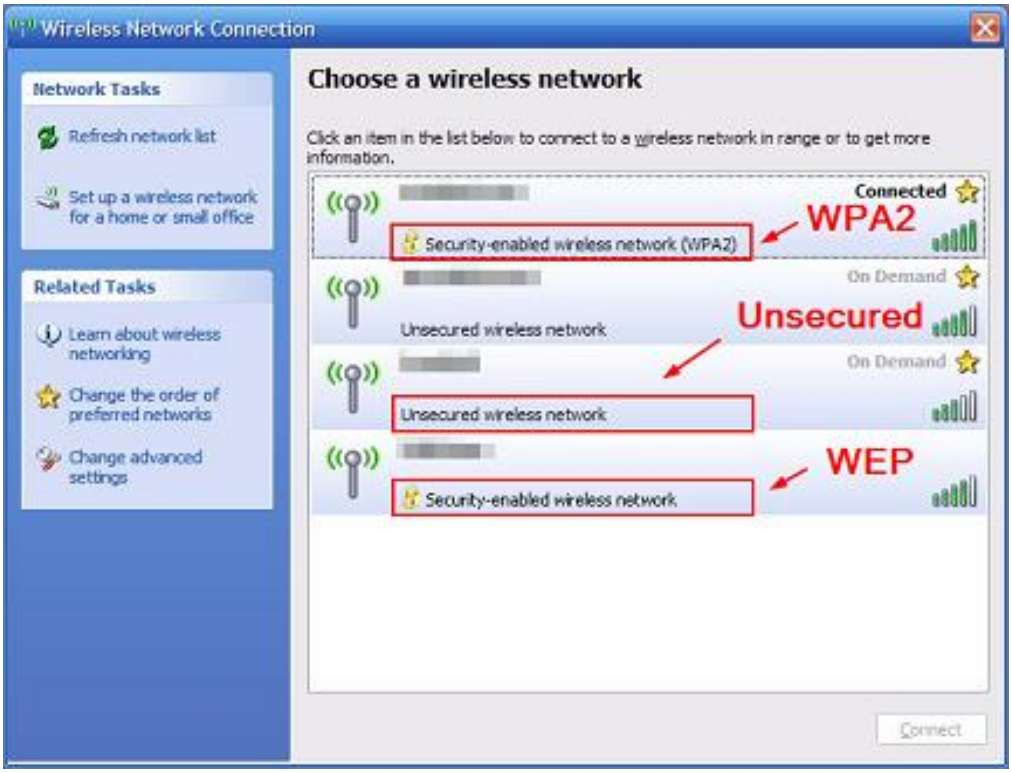

Figure 14: Windows Wireless Network Selection Screen

Figure 15: Windows Network Location Selection Screen

Additional Sources of Information:

- http://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/
- https://en.wikipedia.org/wiki/Wireless_security
- http://youtu.be/bzoEy-t8Y-8

Module 5 – Malware Introduction

General Information

While most people have heard of computer viruses and are aware of the threat they pose, many do not understand that viruses are actually the least of their concern as an average user. Module 5 introduces students to the terms malware, spyware, adware, Trojans, worms, and other cyber threats, while defining each so the student can learn to identify them. Students will learn what types of threats exist with each information system they use, and will begin to appreciate how the various anti-malware protections are used.

Topics to Cover

- Introduces students to the terms malware, spyware, adware, Trojans, worms, and other cyber threats
    - Spyware is a software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.
    - Malware is a catch-all term for malicious software; and typically what people mean when they say “virus”
    - Adware is software that automatically displays or downloads advertising material (often unwanted) when a user is online.
    - A Trojan is a program designed to breach the security of a computer system while ostensibly performing some innocuous function. (there is a legitimate function, part of the software – like a browser search bar add-on)
    - A virus is a standalone program, designed to replicate itself within a given storage medium, and carries a malicious payload

    - A computer worm is a standalone computer program that replicates itself in order to spread to other computers through a network, and carries a malicious "payload". (similar to a virus, but spreading through a network instead of a single drive)

- How to protect
    - Only transfer files from a well-known source
    - Run anti-virus (and anti-malware) on unknown sources, drives, and files
    - Maintain/update anti-virus/malware definition files
    - Install real-time protection agents (IPS: intrusion protection systems)
    - Use a non-administrator account for routine tasks

Structure/Scenario

The user will get an explanation of each type of malware, along with a graphic representation of the type of "baddie". An animated/cartoon version of a representative biological "germ" could be used for each, and bear similarity to the name of the malware type. The visual representation, while entirely made-up, will help reinforce the concepts and help the students remember each of them, and their distinct nature.

The Kaspersky Labs video, while self-promoting, presents how malware comes from many sources and many types: https://youtu.be/XFfm-88_gYk (Kaspersky Lab, 2013)

Vince Valenti has created a more descriptive video explaining the common types of malware, and while pretty basic, provides some fun animations to go with them: https://youtu.be/UFPCEVgTq38 (Valenti, 2013)

Example Diagrams and Images

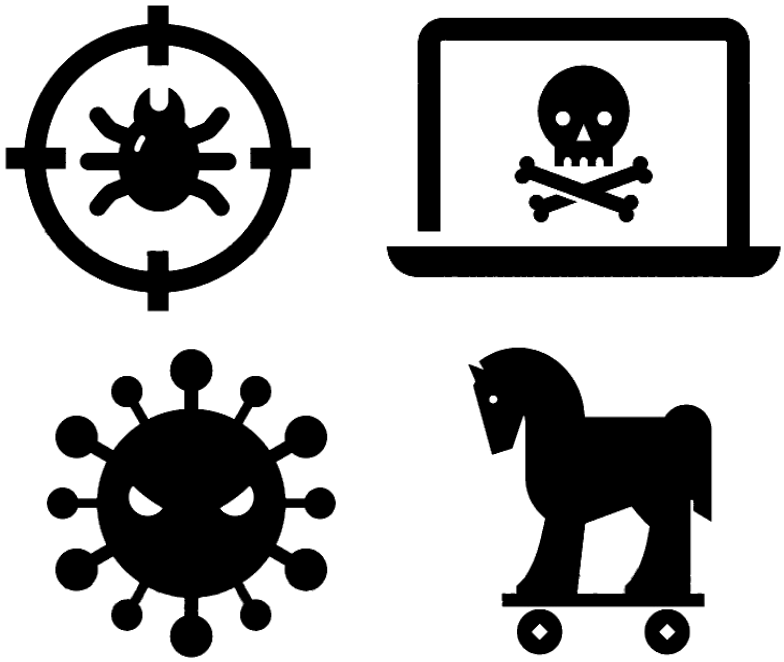

Figure 16: Images/Icons Representing Types of Malware

Additional Sources of Information:

- http://us.norton.com/security_response/malware.jsp
- http://youtu.be/XU8PHihT_P4
- https://www.consumer.ftc.gov/media/game-0002-beware-spyware

Intermediate Modules

Overview

Intermediate modules should be created to provide interested students the opportunity to continue learning about cybersecurity in this trusted environment. These modules could be used to enhance the knowledge of the Student Innovation Team (SIT), as any deskside support should have a working knowledge of cyber threats. Beyond the SIT, teachers of computer science can use these modules to convey the concepts of digital citizenship in the classroom.

Topics suggested:

Some suggested intermediate level topics for development are:

- Social Media Security
    - http://www.adweek.com/socialtimes/5-social-media-threats/493325
- Mobile Device Security
    - https://staysafeonline.org/stay-safe-online/mobile-and-on-the-go/mobile-devices
- Physical Security of Hardware
    - https://www.consumer.ftc.gov/media/game-0008-mission-laptop-security
- Malware Infection Recovery Methods
    - https://www.consumer.ftc.gov/media/video-0103-hijacked-computer-what-do
- Home Network Security
    - https://www.consumer.ftc.gov/media/game-0006-invasion-wireless-hackers
- Peer-to-Peer P2P Networks (file sharing networks)
    - http://netsecurity.about.com/od/newsandeditorial1/a/p2psecurity.htm

Advanced Modules

Overview

Finally, advanced modules should be developed to provide the next step in learning, for those students with an affinity for information technology, and an interest in continuing their computer science studies at the collegiate level. Students with these natural abilities and interests should be introduced to the concepts of ethical hacking early, as they are prime candidates for high-demand, "white hat" careers in the industry.

Topics suggested:

Additional topics suggested for advanced modules are:

- Ethical Hacking
    - http://www.pcworld.com/article/250045/how_to_become_an_ethical_hacker.html
- International Travel and Cybersecurity
    - https://www.onguardonline.gov/media/game-0013-case-cyber-criminal
    - https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers
- Digital Forensics
    - http://www.digitalforensicsmagazine.com/

Additional Recommendations

Industry Pace-matching

Information technology and cybersecurity are a fast-changing, and fluid field of study. A commonly known concept in the field of Information Technology is Moore's Law; which broadly states that computing power, specifically processor speeds, double every 18 months (Schaller, 1996). In general, the advance of technology has kept this same pace (electronic storage capacity, RAM capacity, etc.…). Due to these facets of information technology, it is extremely important for cybersecurity education to keep up with these changes.

Due to this need for curriculum currency, the team recommends the curriculum be reviewed on a cyclic and continuing basis, in order to ensure that the material presented keeps pace with the changes in the industry. This recommendation is not only to add or remove detailed content as technology changes, but also to periodically review the entire program, to ensure that the highest priority content is included in the appropriate tier.

Partnering Computer Science Courses

During the initial meeting with the district personnel, the team learned that the high school offers some computer-science oriented courses in the high school, but that the breadth of coverage of these courses is very limited. Specifically, it seemed that there was student interest, but a lack of ready-made curricula for instructors to use, as well as diversity of experience and knowledge in the field. In order to leverage the local community and area, the school district could reach out to local technology companies for partnering opportunities.

Local technology companies can benefit from increased technological innovation, by having a more competent and knowledgeable employment base; and the school can benefit from the high-level expertise and resources of the companies. Additionally; local colleges

specializing in information technology, such as Worcester Polytechnic Institute (http://www.wpi.edu/); and non-profits such as Technocopia (http://technocopia.org/), could also work with the school district to enhance learning in the computer science field. The National Initiative for Cybersecurity Careers and Studies has an entire section related to education and promoting cybersecurity education: https://niccs.us-cert.gov/education/promoting-education.

Elementary and Middle School Curricula

A final recommendation of the team, is to utilize the computer science interest of the high school students, to develop content oriented toward the middle and elementary school level. Many high schools utilize students in education oriented toward early childhood education. These same programs and methods can be applied to develop and "cascade down" the technology focus to the middle school and elementary school levels.

External resources and non-profits such as Code.org (www.code.org) and the Association for Computing Machinery (www.acm.org) provide tools that can be used, or roadmaps for implementing a more robust computer science curriculum in K-12 schools. When computer science concepts are learned early in school, they are more readily expanded upon later in secondary and post-secondary education. This directly supports the school's mission to "provide students with the skills and knowledge for the 21st century".

Chapter 6: Conclusion

In 2015 alone, over 25 million people's personal information was compromised by the U.S. Office of Personnel Management. The 2014 estimate of the U.S. population is about 318.9 million people, which makes the data breach almost 8% of the U.S. population! This is just one instance of a data breach showing that the need for cybersecurity education is all too obvious.

As recently reported in the Telegram & Gazette, high school students at the Advanced Math and Science Academy of Marlboro have created and setup a "Hackathon"; one of the first on the east coast, where high school students will have the opportunity to meet with technology companies as big as Microsoft. (Klaft, 2016) Incorporating a robust information technology and cybersecurity curriculum will ensure that Shrewsbury meets its Strategic Priorities of:

- Increasing Value to the Community
- Engaging and Challenging All Students
- Enhancing Learning Through Technology
- Promoting Health and Wellbeing

The curriculum that the Clark MSIT and MSPC team have put together will help all Shrewsbury Public Schools graduates understand how to protect themselves, their personal information, and their computers. As digital citizens, they will learn how to consider the ethical implications of their actions online, and make appropriate decisions with information technology.

Shrewsbury's dedication to the use of technology to enhance learning is evident in the 1:1 Technology Program. After success in the Sherwood and Oak Middle Schools, the district expanded the program into the high school, with a full implementation to approximately 1700 students in the high school for the 2015-2016 school year. Shrewsbury should continue to set the

standard across the state, and rather than simply making use of technology to enhance learning, incorporate technology into the subject matter being taught. Due to the pervasiveness of technology in our world, it is only fitting that the school implement a program to instruct students on the security of technology.

References

Allen, S. (2016, March 19). Worcester police feel repercussions of IPhone encryption. *Telegram & Gazette*. Worcester, MA. Retrieved April 2016, from http://www.telegram.com/article/20160319/NEWS/160319118

AT&T ThreatTraq. (n.d.). Social Engineering: A Personal Story - AT&T ThreatTraq: Episode 100 (Part 6 of 7). *AT&T Tech Channel (YouTube)*. Retrieved March 31, 2016, from https://www.youtube.com/watch?v=LgCax4xQIw4

Brichacek, A. (2014, October 22). Infographic: Citizenship in the digital age. International Society for Technology in Education (ISTE). Retrieved April 2016, from https://www.iste.org/explore/articledetail?articleid=192

Brown, M., Dehoney, J., & Millichap, N. (2015, April). The Next Generation Digital Learning Environment. Retrieved April 2016, from https://net.educause.edu/ir/library/pdf/eli3035.pdf

Cimons, M. (2012, May 29). Cybersecurity: Training Students. *U.S. News & World Report*. Retrieved March 7, 2016, from http://www.usnews.com/science/articles/2012/05/29/cybersecurity--training-students

Claywell, C. R. (n.d.). What is Social Network Theory? LoveToKnow. Retrieved from http://socialnetworking.lovetoknow.com/What_is_Social_Network_Theory

Code.org. (2015). 3rd Party Educator Resources. Retrieved March 16, 2016, from https://code.org/educate/curriculum/3rd-party

Code.org. (2015). About Us. Retrieved March 12, 2016, from https://code.org/about/

Code.org. (2015). Support K-12 Computer Science Education in Massachusetts. Retrieved March 12, 2016, from https://code.org/advocacy/state-facts/MA.pdf

Code.org. (2015, July 29). What is the Hour of Code? Retrieved March 16, 2016, from https://support.code.org/hc/en-us/articles/203524386-What-is-the-Hour-of-Code-

Daly, A. J. (2010). *Social Network Theory and Educational Change.* Cambridge, MA: Harvard Education Press.

Digital Media - New Learners of the 21st Century (2013). [Motion Picture]. Public Broadcasting Service (PBS). Retrieved March 2016, from http://www.pbs.org/program/digital-media/

Educause. (2016). About Educause. Retrieved April 2016, from http://www.educause.edu/about

Federal Trade Commission. (2013, February 13). Computer Security. *Federal Trade Commission (YouTube)*. Retrieved February 23, 2016, from https://youtu.be/yeepZr64XjU

Goldhaber, G. M. (1990). *Organizational Communication* (5th ed.). Buffalo: Wm. C. Brown Publishers. Retrieved from http://www2.uvawise.edu/pww8y/Supplement/OCSup/00%20Readings%20OC/101%20Goldhaber%20OrgCommo%20WhatIsOrgCom.pdf

Google/Gallup. (2015). Searching for Computer Science: Access and Barriers in U.S. K-12 Education. Retrieved April 1, 2016, from http://services.google.com/fh/files/misc/searching-for-computer-science_report.pdf

Heidenreich, B., & Gray, D. H. (2013). Cyber-Security: The Threat of the Internet. *Global Security Studies, 4*(3). Retrieved 2016, from http://globalsecuritystudies.com/Heidenreich%20Cyber-Security%20-%20AG.pdf

Javelin Strategy & Research. (2016, February 2). 13.1 Million Identity Fraud Victims but Less Stolen in 2015, According to Javelin. Retrieved March 14, 2016, from https://www.javelinstrategy.com/press-release/131-million-identity-fraud-victims-less-stolen-2015-according-javelin

Kaspersky Lab. (2013, May 23). Max and the Encounter with the Mobile Malware Monsters. *Kaspersky Lab (YouTube)*. Retrieved April 1, 2016, from https://youtu.be/XFfm-88_gYk

Klaft, L. (2016, April 3). Marlboro students gonna hack around the clock in problem-solving marathon. *Telegram & Gazette (telegram.com)*. Marlboro, MA. Retrieved April 3, 2016, from http://www.telegram.com/article/20160402/NEWS/160409763/101370

Larson, L., Miller, T., & Ribble, M. (2009). 5 Considerations for Digital Age Leaders. International Society for Technology in Education. Retrieved March 2016, from http://www.digitalcitizenship.net/uploads/LLDecArticle.pdf

Massachusetts Dept of Elementary & Secondary Education. (n.d.). State Profile 2015-16 School Year. Retrieved February 28, 2016, from http://profiles.doe.mass.edu/profiles/general.aspx?topNavId=1&orgcode=00000000&orgtypecode=0&

Mead, M. (2016, February 26). Interaction With Digital Content: 5 Actions to Look For In Your Students' Online Experience. GettingSmart.com. Retrieved April 2016, from http://gettingsmart.com/2016/02/5-actionstolookforinyourstudentsonlineexperience/

Moore, G. E. (n.d.). *Moore's Law*. Retrieved from Moore's Law: http://www.mooreslaw.org

National Cybersecurity Institute at Excelsior College. (2015, October 14). Should cybersecurity become a part of K-12 curricula? *Editorials by NCI at Excelsior*. Albany, NY. Retrieved March 18, 2016, from http://www.nationalcybersecurityinstitute.org/editorials/should-cybersecurity-become-a-part-of-k-12-curricula-2/

National Cyberwatch Center. (2016). About. Retrieved March 18, 2016, from http://www.nationalcyberwatch.org/about/

National Integrated Cyber Education Research Center. (2015). About. Bossier City, LA. Retrieved March 18, 2016, from http://nicerc.org/about/

National Integrated Cyber Education Research Center. (2015). Curricula. Bossier City, LA. Retrieved March 18, 2016, from http://nicerc.org/curricula/

NOVA PBS. (2014, September 15). Cybersecurity 101. *Nova PBS (YouTube)*. Retrieved February 23, 2016, from https://www.youtube.com/watch?v=sdpxddDzXfE

PBS/WGBH - Nova Labs. (2016). *Cybersecurity Lab*. Retrieved from PBS/WGBH Nova Labs: http://www.pbs.org/wgbh/nova/labs/lab/cyber/

Project Tomorrow. (2014). Making Learning Mobile. Irvine, CA. Retrieved March 21, 2016, from http://www.tomorrow.org/publications/MakingLearningMobile.html

Ribble, M. (2016). Digital Citizenship: Using Technology Appropriately. Retrieved March 2016, from http://www.digitalcitizenship.net/

Salim, H. (2014, May). Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks. Cambridge, MA: Massachusetts Institute of Technology. Retrieved April 2016, from http://ic3.mit.edu/ResearchSamples/2014-07.pdf

Schaller, B. (1996, September 26). The Origin, Nature, and Implications of "Moore's Law". *The Benchmark of Progress in Semiconductor Electronics*. Retrieved March 19, 2016, from http://research.microsoft.com/en-us/um/people/gray/moore_law.html

Schoology. (2015). *Support Article 203068668*. Retrieved from Schoology Support: https://support.schoology.com/hc/en-us/community/posts/203068668-Does-Schoology-have-an-accessibility-ADA-compliance-statement-

Schoology. (2015). *Support Article 205255958*. Retrieved from Schoology Support: https://support.schoology.com/hc/en-us/community/posts/205255958-What-is-the-accessibility-options-for-Visually-Impaired-students-using-Schoology-on-the-iPad-

Shrewsbury Public Schools. (2015). Shrewsbury's Digital Conversion - 1:1 Technology Program. Shrewsbury, MA. Retrieved February 2, 2016, from http://schools.shrewsburyma.gov/it/11-technology-program.cfm

Steinberg, S. (2013, March 8). Technology for Schools and Teachers: 5 Reasons Digital Learning Matters. Huffington Post. Retrieved March 2016, from http://www.huffingtonpost.com/scott-steinberg/technology-for-schools-an_b_2805201.html

Tech4Learning. (2016). The Creative Educator. Retrieved March 2016, from http://www.thecreativeeducator.com/

The College Board. (n.d.). Program Summary Report 2015. *AP Program Participation and Performance Data 2015*. Retrieved March 20, 2016, from https://secure-media.collegeboard.org/digitalServices/pdf/research/2015/Program-Summary-Report-2015.pdf

The White House. (2009, May 29). Remarks by the President on Securing Our Nation's Cyber Infrastructure. Retrieved February 21, 2016, from https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

U.S. Dept of Education. (2015, October 16). *Frequently Asked Questions About Section 504 and the Education of Children with Disabilities*. Retrieved from Protecting Students With Disabilities: http://www2.ed.gov/about/offices/list/ocr/504faq.html

U.S. Dept of Homeland Security. (2016, February 17). *Curriculum Resources - Teaching Tools for Educators*. Retrieved from National Initiative for Cybersecurity Careers and Studies: https://niccs.us-cert.gov/education/curriculum-resources

U.S. Dept of Homeland Security. (2016, March 3). Cybersecurity Education & Career Development. Retrieved March 18, 2016, from https://www.dhs.gov/topic/cybersecurity-education-career-development

U.S. Dept of Homeland Security. (2016). *Explore Terms: A Glossary of Common Cybersecurity Terminology*. Retrieved April 13, 2016, from National Initiative for Cybersecurity Careers and Studies: https://niccs.us-cert.gov/glossary#cybersecurity

U.S. Dept of Justice. (2007, May 7). *Chapter 5 - Website Accessibility Under Title II of the ADA*. Retrieved from ADA Best Practices Tool Kit for State and Local Governments: http://www.ada.gov/pcatoolkit/chap5toolkit.htm

U.S. General Services Administration. (2016). *Section 508 Homepage*. Retrieved from Section508.gov: http://www.section508.gov/

Valenti, V. (2013, November 14). What is Malware? - Types, Prevention & Treatment. *VinceValentiDM (YouTube)*. Retrieved April 1, 2016, from https://youtu.be/UFPCEVgTq38

Ware, B., & Boatman, J. (2015, November 24). Managing School Safety in the Digital Age (Industry Perspective). Center for Digital Education. Retrieved March 2016, from http://www.centerdigitaled.com/higher-ed/Managing-School-Safety-in-the-Digital-Age.html

WebFinance, Inc. (n.d.). Organizational Communication. *BusinessDictionary.com*. Retrieved from http://www.businessdictionary.com/definition/organizational-communication.html

World Wide Web Consortium. (2016). *Accessibility*. Retrieved from W3C: https://www.w3.org/standards/webdesign/accessibility

World Wide Web Consortium. (2016). *HTML & CSS*. Retrieved from W3C: https://www.w3.org/standards/webdesign/htmlcss

Appendix 1: Module 1 Activity Diagram & Mind Map

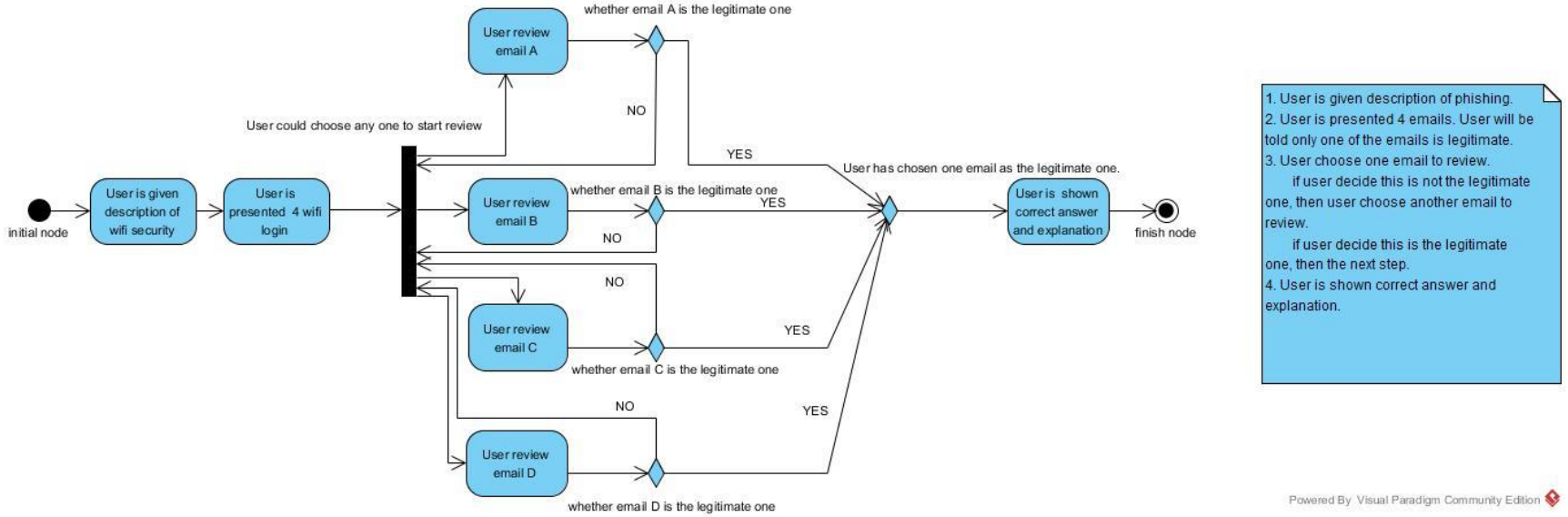

Figure 17: Phishing & Spam Module Activity Diagram

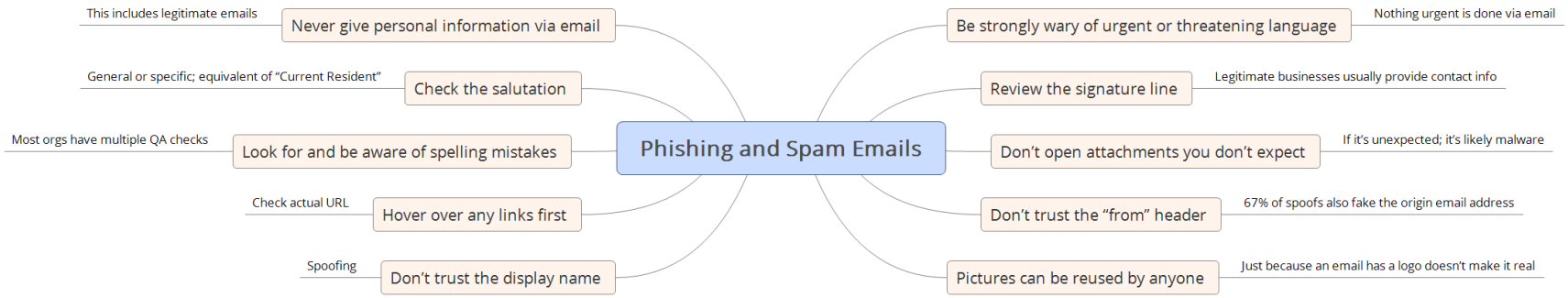

Figure 18: Phishing & Spam Email Mind Map

Appendix 2: Module 2 Activity Diagram & Mind Map

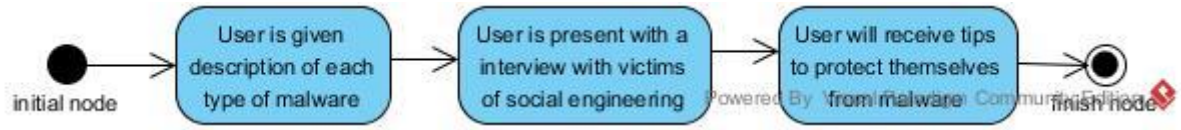

Figure 19: Social Engineering Module Activity Diagram

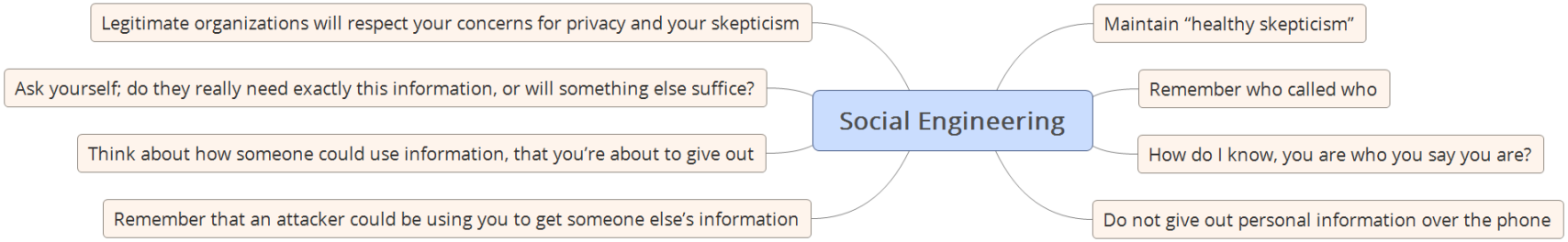

Figure 20: Social Engineering Mind Map

Appendix 3: Module 3 Activity Diagram & Mind Map

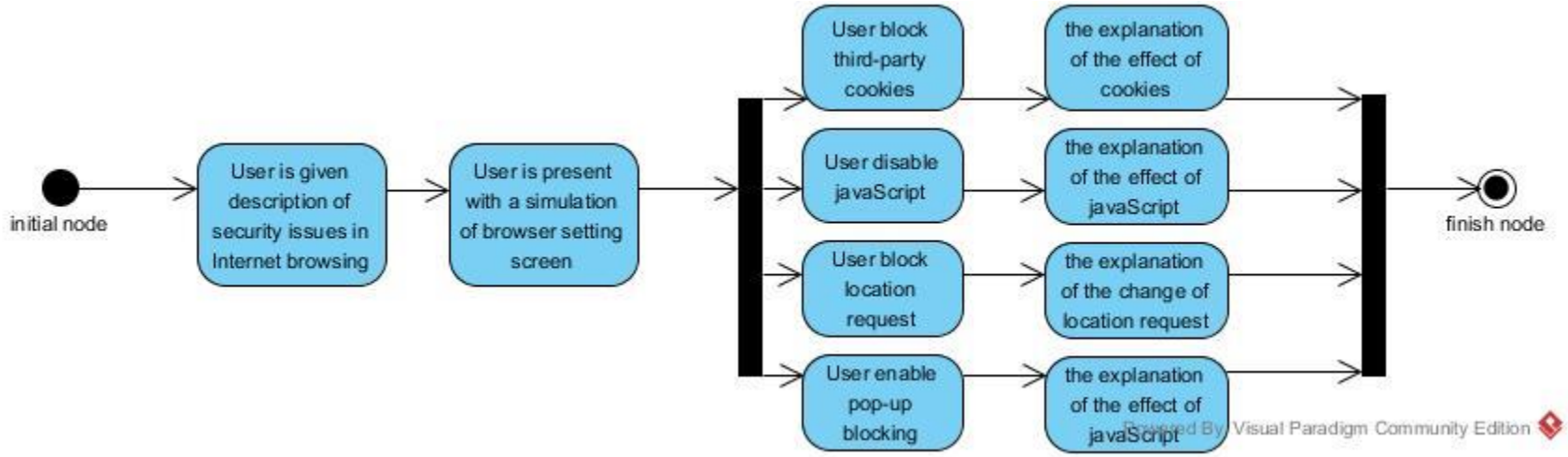

Figure 21: Internet Browsing Security Module Activity Diagram

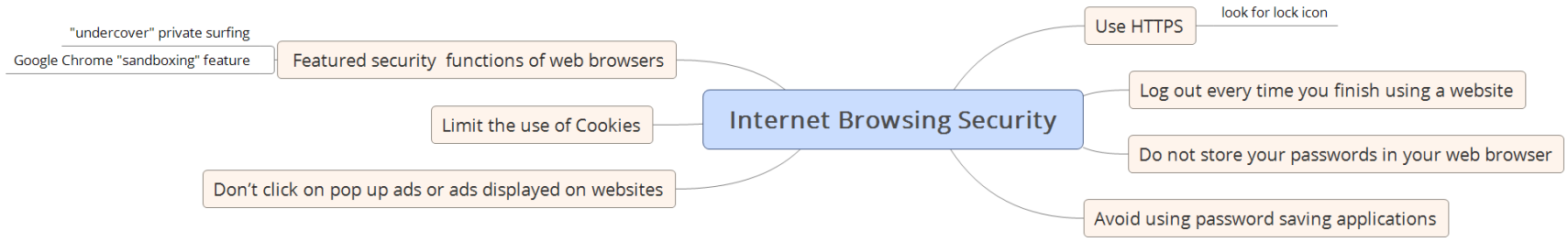

Figure 22: Internet Browsing Security Mind Map

Appendix 4: Module 4 Activity Diagram & Mind Map

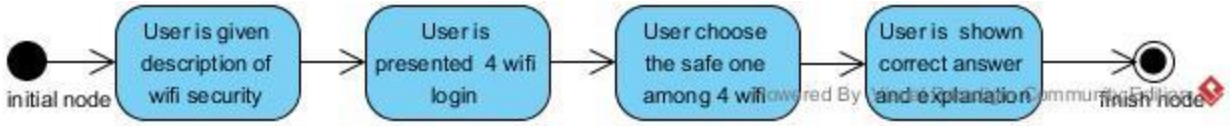

Figure 23: Wireless Attacks Module Activity Diagram

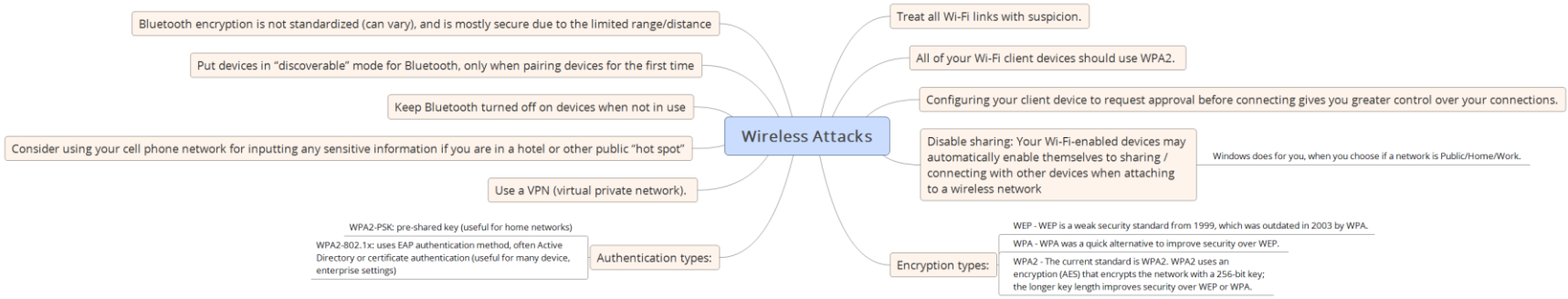

Figure 24: Wireless Attacks Mind Map

Appendix 5: Module 5 Activity Diagram & Mind Map

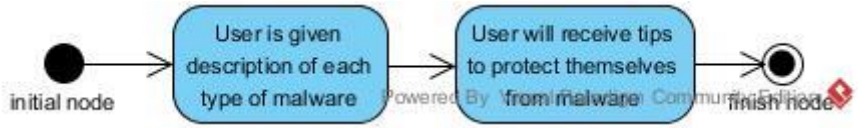

Figure 25: Malware Introduction Module Activity Diagram

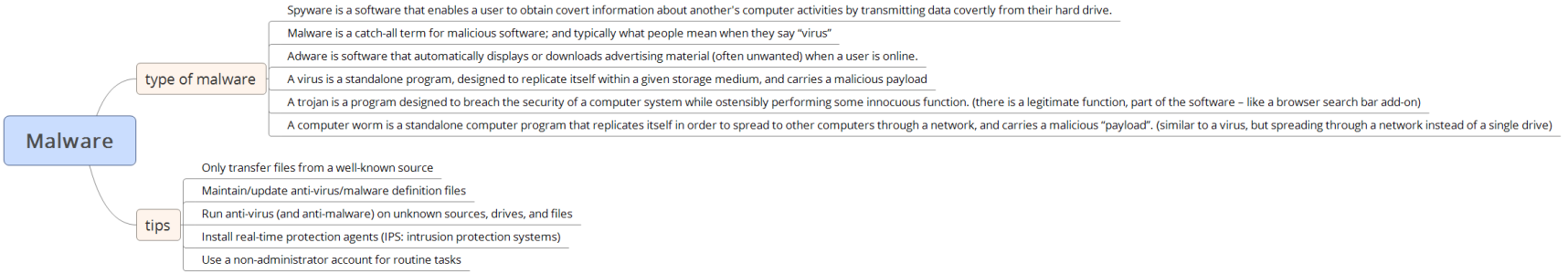

Figure 26: Malware Introduction Mind Map

Appendix 6: Table of Figures