

Introduction

Today, it appears virtually irrefutable that people across the globe are expanding and integrating technology into their daily lives. Similarly, not only are individuals becoming more involved in the use of technology, it also appears that our world as a whole is running off of critical infrastructures, including governments, healthcare systems, transportation systems, banking systems, etc., that depend on technology. As with any new advancement, new challenges are inevitable, and a challenge facing our world today due to the advancement of technology is maintaining cyber security.

The popularization of the internet, smart phones, online banking, social media, and email are but a few of the many frequently used cyber services that leave countless people worldwide at risk for fraud and theft if proper awareness and precautions are not taken. With this issue in mind, this paper will both address the pressing issue of lack of online security awareness and propose a solution for how websites can take responsibility in ensuring that their users are understanding the posed risks and necessary precautions when using their websites and others.

Rationale

With the continuing rise of the digital era, the risks associated with using tools such as the internet also continue to rise. In 2015, there were over one million cyber-attacks against internet users each day (Symantec, 2016). These attacks included database breaches, malware, worms, and other attempts to damage or steal information from other people. The number of digital transactions also continues to rise showing how more and more people and companies are relying on digital systems in order to operate (Agarwal, 2017). The lack of online security awareness seems to be present in most age groups, including adults and even professionals in

computing fields. It seems people are either simply unaware of potential security issues, or simply do not see them as a serious enough threat.

A survey by CompTIA looked at HR professional and found that only a third of U.S. organization requires some sort of cyber security awareness training program (Downers, 2016). In addition, only half of that third makes it mandatory to all employees. Even tech savvy professionals are not safe from being tricked into giving away crucial information or downloading a malicious program. It is important to make sure that awareness is made as wide spread throughout the company as possible. A survey by Trench Micro Security revealed that less than 1 in 10 Asianic/Pacific companies fully understand how cyber-attacks are even performed (Trend Micro, 2016)!

However, this issue may not even come from a person's lack of cyber awareness persay, but their lack of interest to actually adjust their behavior in order to operate online safely. Even the simpler forms of cyber protection that most people are aware of are not properly followed, such as using unique passwords across sites. According to Ofcom's Adult Media Use and Attributes 2013 Report, a little more than half of adults aged 16 and older use the same password for most - if not all - of their online accounts (Cluley, 2013). The severity of the issue does not seem to be reaching out as much as it should be.

Another important aspect of cyber security is how much cyber threats continue to grow. In the early ages of the internet, viruses and malware were usually created for pranking or breaking others computers, and would be as obtrusive and obvious as possible. With the rise more personal information being stored on the web and computers, cyber criminals started to make these viruses less in your face with intent to mess with your computer, and more silent and

intent on stealing information. Nowadays, access to information on how to create these ransomware, spyware, and keyloggers is available to anyone who wants to look them up. In fact, countries like Brazil even offer tutorials and things like courses to want-to-be cyber criminals for a price (Gamer 2016).

Due to the increasing rise of cyber criminal activity, it has become important to make sure people are not only educated with cyber security practices and threats, but also actively work to prevent them in any way they can. This is a problem that will continue to become more important as technology advances, but there has been an interesting trend in recent years with millennials becoming more familiar with cyber security due to increased exposure in the news (Raytheon, 2016).

Problem Analysis

The Department of Homeland Security (2017) has defined cyber security as, “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.” They also have extended this definition to specify the areas that can be at risk at a global level of communication and information infrastructure, including, “computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions,” (Department of Homeland Security, 2017). While these definitions explain cybersecurity, this issue is one that often goes undefined in day to day life and that can unfortunately be noted by individuals when they have felt the first hand effects of a security breach. Thus, it is important to also look at how this issue

relates to individuals and how lack of awareness among users is one of the factors that continues cyber security issues.

Information security threats have gradually shifted from hackers who are highly skilled in technology that using hacking to demonstrate their expertise to more organized and established hackers who are using hacking for financial gain (Hinde, 2004). Both academic and commercial communities have begun to understand the importance of focusing on cyber security issues and increasing awareness (Talib, Clarke, & Furnell, 2010). For organizations, the development of strategies to promote awareness in their companies has become more popularized as they have understood the importance of the information of their companies (Talib, Clarke, & Furnell, 2010). There has been much research done to help promote the awareness of cyber security, included but not limited to, developing various learning mechanisms, like in person training seminars, email messages, training via the web, video game, and poster campaigns (Talib, Clarke, & Furnell, 2010). The Computer Security Institute (CSI) survey reported that 68% of the organizations measure the effectiveness of their awareness training (Richardson, 2008).

While it is important for businesses and organizations to develop programs to aid in cyber security, it is also becoming increasingly important for people not in work settings to be educated on how they could be affected security problems. Those who use technology and are thus at risk from lack of cyber security awareness are referred to as users. Personal internet users have further classified into two groups: Home users and non-home users (Kritzinger & Solms, 2017). Non-home users are the users that utilize technology in non-home work stations in work environments, including areas like the government, industry, academia, etc. (Kritzinger & Solms, 2017). This group of users often has access to more resources to equip them for cyber security

awareness than do home-users, which refer to the users that use Information Communication Technologies for their own personal use outside of a work environment, primarily through computers in a home environment (Kritzinger & Solms, 2017). This group has been recognized as particularly vulnerable to cyber security threats because there is not an organization above them that would seek to ensure that they are using their technology and their personal information safely and properly (Kritzinger & Solms, 2017). However, with the popularization of mobile phones, a third and prominent group of users has appeared: smartphone users.

Smartphones have become highly popularized in certain areas of the world today. 72% of phones users in the United States are reported to be smartphone users, which ranks behind other countries in the world like Israel with 74% smartphone users and South Korea with 88% users (Baer, 2016). With these new innovations have also come new challenges with cyber security. Today, smartphone users are also at a heightened level of vulnerability, noted as a new and large target for cyber attacks. The login credentials, private data, and account information that is readily able to be saved in smart phones are common reasons for why these particular users suffer cyber attack (Imgraben, Engelbrecht, & Choo, 2014). Smartphone users are also cited to be put organizations and corporate networks at risk in addition to themselves through the wide range of capabilities that their phone offers (Imgraben, Engelbrecht, & Choo, 2014). For example, VanDerwerken and Ubell (2014) said that the biggest cyber-security threat for businesses occur when employees click on invasive files that are embedded in messages from beyond the company firewalls, and the researchers further noted that mobile devices greatly increased that particular risk. biggest threat to security is negligent employees who are “clicking

on invasive files embedded in messages from beyond company firewalls.” It says that mobile devices of employees also increases this risk. (p. 49)

Large organizations and sectors can not sit by passively while their users continue being at risk without being informed. Cyberspace has been labeled the “nervous system of our economy,” and it is thus important for businesses, governments, and organizations to help ensure that our economy is functioning in a healthy and safe way (Information Technology Industrial Council, 2011). This problem affects individuals, but organizations and sectors that have the resources and power to help or halt the problem can and should take responsibility for raising awareness among their users. Bank of America and Merrill Lynch are two businesses that exemplify this kind of responsibility that businesses should take. Vice President of Securities from these two companies voiced their concern for this subject, stating, “As cyber criminals continue to expand and gain access to even more financial information, we continue to evolve our capabilities and expertise to ensure that our customers are protected,” (VanDerwerken & Ubell, 2011). Other businesses and organizations should continue to follow the examples of companies like Bank of America and Merrill Lynch, however, the educational system is another sector in which raising cyber awareness is a necessity.

In schools, adolescents face their own kinds of issues in relation to technology and cyber security. Teens in school have been noted for facing risks such as content risks, for example hate messages, contact risks, like cyber bullying, sexual solicitation of minors, etc., and commercial risks, such as tracking user behavior to target advertising or commercial misuse of personal information (Vanderhoven, Schellen, & Valcke, 2014). These kinds of cyber dangers are often the first that adolescents encounter, only to further to other kind of risks later on that could pose

more financial and security risks. Thus, this problem is one that begins as soon as adolescents gain access to technology and will likely only to continue to progress until active intervention is taken.

Criteria

In any case, whether with a government, school system, business, or home, effort to combat cyber security issues must focus on awareness to understand the risks and importance of addressing these risks (Information Technology Industrial Council, 2011). In evaluating solutions for this problem, we are looking to how well the proposed solution would create deep awareness of cyber security among a group of users. More specifically, it is important to look to factors including the group of people affected by the solution, the perceived effectiveness of the solution, the depth of awareness raised, and the sustainability of the solution.

Regarding the group of people targeted, it is important for a solution to be proposed to groups that would be able to readily understand the problem and be influential in the implementation of the solution. Regarding perceived effectiveness, it is important to select solutions that would likely be effective in capturing the attention of users and educating them on cyber security. Regarding the depth of awareness raised, it is important to propose a solution that would help users have a deep understanding of cyber security that would lead to change, instead of a surface level awareness. Regarding sustainability of the solution, it is also important to select a solution that could continue to be implemented rather than a one time event or solution. These criteria would lead to an effective solutions, because they ensure that the solution would effectively raise awareness of cyber security to a group people and would continue to advance along with the continuing advancement of technology.

Considered Solutions

There were many proposed solutions to combat the lack of cyber security among users, but all but one were ruled out through careful evaluation of the possibilities.

Proposed Solution: *Presenting Cyber Attack Averages*

One proposed solution was to have pamphlets or flyers that present students with the averages of cyber attack and security among different domains and with certain demographics. This solution was proposed due to prior knowledge from a psychology class where it was found that presenting averages of certain behaviors were found to be effective in reducing people's activity in a certain aversive behavior. The example mentioned in class was in regard to college students and binge drinking, and the data showed that when college students were presented with the averages of how much people actually drank, students who drank more than the average were highly likely to modify their own behavior. Thus, through this form of raising awareness, we had thought that people might also reduce behaviors with technology and the internet that would put them at risk. While this solution would be cheap and relatively easy to do by compiling data and printing it on paper, we opted against this option for three main reasons. One was that another finding of that psychology of behavior modification is that a trend has also been shown that people who do things below the averages sometimes engage in the behavior more. More major concerns were that it would be difficult to determine locations that would reach the attention of a large group of people and that the flyers or posters might not be effective in really grabbing people's attention and raising awareness.

Proposed Solution: *Online Risk Warnings*

Creating online risk warnings was a considered solution for our problem. This idea would be pitched to different social media sites, for example Twitter. Facebook is a good example of a media site that is already doing so. Facebook uses security warnings and facts presented in a time-hop form, which is shown as soon as you login. Upon the user opening the web console while visiting facebook, they will be greeted with the message,

“This is a browser feature intended for developers. If someone told you to copy-paste something here to enable a Facebook feature or “hack” someone’s account, it is a scam and will give them access to your Facebook account” (www.facebook.com).

This makes users aware of what can happen to their social media accounts, this was considered a pro for our group. The downside of this solution is that it would be hard to pitch an idea to a substantially large amount of websites and convincing them to implement similar warnings and solutions.

Proposed Solution: *College Orientation Events*

Capitalizing on orientation events on college campuses was another proposed solution. Master plan is large orientation event at WKU that was mentioned as a possible idea for a solution. The size of this event was a major pro to our group. We thought we could have an informational session or have a booth of some kind at master plan. That is the only pro that we could think of because of a big number of college students that are freshman attend the event. The ultimate reason why we decided that this was not a good solution for our problem was because it is not a mandatory college event which even further limiting the scope of the people

affected. The people affected would fall from college student to college student also attending the event.

Proposed Solution: *College Class*

To build more on the event solution above, another solution proposed was to incorporate cyber security topics into coursework and have a non-Computer Science course that people can take. Colleges are a prime target to cyberattacks due to the open network containing hundreds of student with their own devices. BitSight Technology analyzed external data to identify and the top schools' security ratings ranging from 500 to 900. They found the best score to be 661 and the worst at 588 (Wang, 2014). As can be seen, the scores are less than adequate for a problem of this scale and reach. Making a course as opposed to an event would be more forceful in making sure the information is not only known to students, but applied to some extent.

However, the limitations of this course of action were too great. Forcing college students to have more workload than they already have would reduce the effectiveness of making sure they retain and apply the knowledge they gain. This solution would also have a more narrow audience than would be preferred; limited to college student who elect to take the course. Lastly, the obvious cost of having the class was considered and assessed to be too much. Overall, while this solution may have a decent level of effectiveness, the negatives of audience and cost weighed too heavy. The most limiting factor, as with the above solution, was the relatively narrow reach.

Proposed Solution: *E-mail Education of Cyber Security*

Email tricking is a clever way to get people's attention and the point of this solution is to ultimately educate people and bring awareness. For this solution to work, you will need to have a

master list of emails to send the “fake” email. The fake emails are not uncommon and it would be more likely that people would see it. The difference is that instead of sending the computer user to a website that would give them a virus or worm, we would send them to one telling them what just happened and how to tell the difference. The downside is that it’s easy to ignore emails and just delete them without assessing their content. In addition the solution would only cover a small aspect of cyber security, and those who are tricked into seeing the webpage of information would likely not even read it.

Proposed Solution: *Community Events*

Another proposed solution was to create events that could help raise awareness of the issue of cyber security. 5ks and dance marathons were two mentioned possibilities that are commonly used for different organizations and that often involve a good number of people. We also mentioned that these events could occur during cyber-security awareness month in October.

The pros of the idea of creating events was that it appears more exciting and engaging than say a class or a pamphlet, at times creating more publicity and participation. However, it was also mentioned that these kinds of events require lots of volunteers, time, energy, and resources in order to make them happen. Having an event to raise awareness will need a sponsor to provide enough money to fund the event, this idea is normally used for fundraising and a non-profit event. Additionally, the strongest con that led us to ruling out this idea was that it might not be as effective of raising the kind of awareness necessary to help change the problem. We discussed that many of the organizations that use 5k runs or dance marathons do so to raise funding, such as foundations for medical conditions or hospitals that need more money for a certain kind of research. In our case, raising awareness and educating users was the priority,

rather than supporting a certain organization or kind of research, and we felt that hosting an event would not be the most effective in engaging users about the issue.

Chosen Solution

In order to achieve an effective and long term solution to the lack of cyber security awareness among users, we propose that implementing programs in secondary education environments will help reach the coming generation and leaders of technology users. Various researchers have found that the educational environment is particularly effective in educating users about cyber security because it is already a place of learning, targets a large demographic at one time, and offers heightened peer support (Vanderhoven, Schellen, & Valcke, 2014). In addition, research has shown that both education of the threats and proper training are very effective methods for improving both awareness and initiative with cyber security awareness (McCrohan, Engel, & Harvey, 2010). In the context of the United States, high schools, rather than a higher education, would be more effective and wide reaching given that public education is compulsory. Wong (2016) noted that high school graduation for high school seniors as 82% in 2016. This was an increase from the high school graduation rate from the year before of 81% and a step towards the goal of the coalition of organizations that keeps the data for the National Center for Educational Statistics that has been in place for the past decade (Wong, 2015).

Furthermore, not only are high school graduation rates increasing in the US, hitting record levels, they are surpassing college admission rates, which have continued to decrease with 1.7% less in 2015 than the year prior (National Student Clearinghouse Research Center, 2015). Thus, targeting high schoolers as the group to raise cyber-security awareness would likely offer the largest number of students. Various programs for schools are available, with varying prices

and commitment levels for schools, however we are proposing that a four year high school program with required elective classes that cover cyber security would be most effective in raising deep awareness about this issue that will result in lasting change.

For this particular solution, the age group and setting that accompanies secondary was very influential in choosing this particular solution. Firstly, the current generation of high school students were born into a world very different from their parents--a world where cell phones, computers, and the internet were ubiquitous. This years graduating seniors in America, born between 1999-2000 would have never lived a life without the internet, created in 1989, worldwide Wi-Fi, created in 1997, and would have never attended school without the existence of Wikipedia, created in 2001 (Woodford, 2017). In recent years, this age group has also been increasingly cited for their dependence on such devices. In recent studies by the Pew Research Center (2015), 24 % of teens from ages 13 to 17 reported their internet use to be “almost constantly,” which is noted to be facilitated by the wide use of smartphones. While this age group is distinguished for their connection with technology, they are also at a pivotal point in their lives to be made aware about cyber security issues. High schoolers are at a point where they transitioning to more independent adults and making more of their own purchases online. Additionally, they are also beginning the transition to college or the career force, two areas in which cyber security is also increasingly important. Thus, by engaging high school age students, this solution would be targeting the generation that will be the next group of college students, parents, and employees.

Aside from choosing high school age students because of their school attendance and involvement with technology, we also chose to propose this solution to a secondary education

setting because it would be a logical way to raise awareness through education that is already being undertaken. We are proposing that this solution be made a required elective class to serve the biggest benefit of high schoolers. By making it a required elective, students will be sure to have been made aware of cyber security, and by having a class dedicated to the subject, it can also be assured that this topic can be covered in depth and will be addressed in an ongoing fashion, fulfilling our criteria of depth of awareness. Once established in a high school, this program would also be sustainable because the same class could be offered year after year, with the materials already in place.

Implementation Plan

In order to implement this solution, we are proposing the use of the advanced four-year cyber security track created by the The Institute for Cyber Education. This program would cost around \$1,500, however this cost would be for a program that covers four years of a student's high school, occurring in a specific sequence that strategically educate high schoolers to offer them job ready skills by the time that they graduate (Morga, 2016). More specifically, the overall \$1,462 cost covers the textbooks used in the course use for all four years, video lectures, virtual labs, practice exams, exams, and certification exam at the end of the fourth year (Institute for Cyber Security, 2015).

A freshmen enrolled in this program would gain knowledge of computer systems technology, gaining a basis for the knowledge that will later aid with cyber security (Institute for Cyber Security, 2015). Their sophomore year will center around Network Software Operations, where they be able to, "describe the major networking technologies, systems, skills, and tools in use in modern networks" (Institute for Cyber Security, 2015). With the sophomore year courses,

cyber security is hit thoroughly, covering how to monitor security on networks, applications, and operating system and how to respond in instances of security breaches, and concluding at the end with the CompTIA Security+ and TestOut's Security Pro certification exam (Institute for Cyber Security, 2015). The junior year would introduce Programming and Advanced Computer Network Software Operations, where security issues are again discussed (Institute for Cyber Security, 2015). A student in their senior year would complete the program, doing an internship or alternate senior project as well as an advanced programming class, where they will learn advanced programming techniques used by Cyber Security professionals; through this class, students will acquire in depth knowledge and practical experience working with important security systems as well as become a Council Certified Ethical Hacker (Institute for Cyber Security, 2015). This certification means that students have had the unique opportunity to learn about security through penetration testing, by scanning, testing, and penetrating their own security systems (Institute for Cyber Security, 2015). Thus, this four year program would offer a much more in-depth look into cyber security and knowledge about computer technology that would not only aid students in their personal security with technology, but would also equip them with valuable skills for today's technological college and career force.

Suggested senior projects that students could take could also help engage those who are not directly affected by the class themselves. Creating programs to educate middle school students on cyber security could be a way to extend the reach of this awareness. Another idea would be that students could create some sort of program to present the relevant cyber security knowledge that they have learned to a parent or guardian to reach another generation that could be made more aware of cyber security. It could be left up to the student as to how they would go

about creating these specific projects, however the overall idea could be to help diffuse the responsibility of raising cyber security awareness to those who are also being educated about cyber security, as to promote the furthering of this solution. It is hoped that through this 4 year program, students themselves would not only be positively affected by being made aware of cyber security, but that they would also be given the tools to pursue careers and degrees in which they can further the efforts of cyber security.

Limitations

Although we are optimistic about the implementation of our program, we are not so naive to think that there it comes without certain limitations. Unfortunately, some schools may not have qualified instructors to administer the program. Though this program is largely implemented online, having an instructor or facilitator for this particular solution we are suggesting would be a necessary component that might not be possible for certain schools. In addition, some school districts may not have the appropriate resources or funding to cover the course cost. Also, while some schools might be able to cover the costs and have the staff, they might be unwilling to make this a required elective course. These issues are problematic, however there are alternatives that can be proposed that are possible for any high school.

One option, in regard to the lack of teachers and available funding is to provide students with the free online resources that are created for secondary education. One example is the ISECOM institute that created the Hacker High school project, which is a set of free, interactive lessons that are designed for high school aged students to learn about cyber security and related internet skills (Morgan, 2016). It is a full program that has teaching materials in multiple languages, with books, lessons,a and support for high school teachers and home-schooling

parents (Morgan, 2016). If a high school is noted for having a large minority population, this particular solution would also be a great alternative or substitute for the four year required elective. In that case, ESL or minority students could be allowed to be exempt from the 4 year program to participate in the ISECOM program.

Another option for a school that has the resources for the 4 year program but who does not want to make it a required elective could make the computer classes a general elective for the school. In order to encourage participation, the school could offer certain incentives such as the certification already included in the program or making it an avenue through which students could receive an advanced diploma at graduation.

Conclusion

In conclusion, cyber security is a relevant and complex issue in today's society that will require creative and purposeful intervention to raise awareness. As the use of technology continues to develop, the need for cyber security will consequently follow. After looking at the necessity for cyber awareness, the analysis of the problem, and the criteria and options for a solution, it has been determined that the best way to help raise awareness of cyber security is through secondary education, by capitalizing on the setting and implementing sustainable education of cyber security.

While we understand that this solution would only directly affect high school students, we believe that targeting this group would be the best way to implement a sustainable change that would affect generations to come. While our group has determined that this solution is the most effective way to raise awareness, we are not saying that this is the only solution that should be taken to confront a lack of online security awareness. Further research and efforts should be

undertaken in order to help share responsibility for this problem on a global scale. Citizens of our world can not avoid the dangers of cyber security if they are not first aware of its presence and educational systems in various countries should follow in this model, making their own alterations for what would be appropriate for their setting.

Bibliography

Agarwal, Simon. (2016) *Volume of digital transactions climbed to 84 percent in 2015-16.*

Retrieved from <https://thetechportal.com/2016/12/30/digital-transactions-climb-rbi/>

Baer, Drake. (2016) *This map shows the percentage of people around the world who own smartphones.* Retrieved from

<http://www.businessinsider.com/how-many-people-own-smartphones-around-the-world-2016-2>

Budd, Christopher. (2016) *The deck is stacked against APAC: Lack of cyber security awareness preludes potential problems.* Retrieved from

<http://blog.trendmicro.com/the-deck-is-stacked-against-apac-lack-of-cyber-security-awareness-preludes-potential-problems/>

Cluley, Graham, (2013). *55% of net users use the same password for most, if not all, websites.*

When will they learn? Retrieved from

<https://nakedsecurity.sophos.com/2013/04/23/users-same-password-most-websites/>

Raytheon (2016). *Cyber Survey Survey.* Retrieved from

http://www.raytheoncyber.com/news/feature/2016_cyber_survey.html

Department of Homeland Security (2017). *Cyber safety tips.* Retrieved from

https://www.tn.gov/assets/entities/safety/attachments/Cyber_Safety_Tips_14_OCT_13.pdf

Downers, Grove. (2016). *Comptia shares new cybersecure training course with premier*

- members free of charge*. Retrieved from <https://www.comptia.org/about-us/newsroom/press-releases/2016/01/13/comptia-share-s-new-cybersecure-training-course-with-premier-members-free-of-charge>
- Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73-80.
- Gamer, Noah. (2016) *The rise of the Brazilian underground*. Retrieved from <http://blog.trendmicro.com/the-rise-of-the-brazilian-underground/>
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. *Computer Security Journal*, 21(3), 1.
- Imgraben, J., Engelbrecht, A., & Choo, K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile users. *Behaviour & Information Technology*, 33(12), 1347-1360. doi:10.1080/0144929X.2014.934286
- Information Technology Industrial Council (2011). *The IT industry's cybersecurity principles for industry and government*. Retrieved from <http://www.itic.org/dotAsset/31bcabf8-514e-498e-a0af-7ed37e3a92ef.pdf>
- Institute for Cyber Security (2015). 2015-2016 iForce CTE STEM cyber security track. Retrieved from <http://cybersecurityed.org/scope-sequence/>
- Institute for Cyber Security (2015). iForce advanced cybersecurity training budget. Retrieved from <http://cybersecurityed.org/getting-started/>
- Kritzing, E. & Solms, V. (2017). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840-847.
-

- McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of internet Commerce*, 9(1), 23-41.
- Morgan, S. (2016). Hacker High School teaches cyber security skills to teens. Retrieved from <https://www.forbes.com/sites/stevemorgan/2016/03/20/hacker-high-school-teaches-cyber-security-skills-to-teens/#1cf2e0b04d50>
- National Student Clearinghouse Research Center (2015). *Term enrollment estimates: Fall 2015* [Data file]. Retrieved from <https://nscresearchcenter.org/wp-content/uploads/CurrentTermEnrollment-Fall2015.pdf>
- Pew Research Center. (2015). *Teens, social media & technology overview 2015*. Washington, DC: Lenhart, A.
- Prichard, J. J., MacDonald, L. E., & Hunt, L. (2004). Cyber terrorism: A study of the extent of coverage in computer security textbooks. *Journal Of Information Technology Education*, 3279-289.
- R. Richardson, "2008 CSI Computer Crime & Security Survey," CSI, 2008. - Open Access Library. N.p., n.d. Web. 16 Apr. 2017.
- Symantec. (2016). *Internet security threat report, 21*. Mountain View, CA: Symantec Corporation.
- Talib, S., Clarke, N. L., & Furnell, S. M. (2010) "An Analysis of Information Security Awareness Within Home and Work Environments." *Advanced Computer Science Applications and Technologies (ACSAT) 2015 4th International Conference on*, pp. 256-260, 2015.
-

- Trend micro survey reveals less than 1 in 10 APAC companies fully understand how cyber attacks are performed.* (2016). Retrieved from <http://newsroom.trendmicro.com/press-release/commercial/trend-micro-survey-reveals-less-1-10-apac-companies-fully-understand-how-cy>
- Vanderhoven, E., Schellen, T., & Valcke, M. (2014). Educating teens about the risks of social network sites: An intervention study in secondary education. *Comunicar*, 22(43), 123-131. Doi: 10.3916/C43-2014-12
- VanDerwerken, J. & Ubell, R. (2011). Training on the cyber security frontlines. *T+D*, 65(6), 46-50.
- Wang, Abigail. (2014). *College Campuses Get An "F" In Cybersecurity*. Retrieved from <http://securitywatch.pcmag.com/security/326921-college-campuses-get-an-f-in-cybersecurity>
- Wong, A. (2015). Where dropping out is going up. Retrieved from <https://www.theatlantic.com/education/archive/2015/05/where-dropping-out-is-going-up/393398/>
- Wong, A. (2016). Where are all the high school grads going? Retrieved from <https://www.theatlantic.com/education/archive/2016/01/where-are-all-the-high-school-grads-going/423285/>
- Woodford, C. (2017). Technology timeline. Retrieved from www.explainthatstuff.com/timeline.html