https://doi.org/10.48009/1_iis_2019_186-194

Issues in Information Systems
Volume 20, Issue 1, pp. 186-194, 2019

YOU'VE BEEN HACKED: A TECHNIQUE FOR RAISING CYBER SECURITY AWARENESS

David T. Smith, Indiana University of Pennsylvania, dtsmith@iup.edu
Azad I. Ali, Indiana University of Pennsylvania, azadali@iup.edu

ABSTRACT

In today's interconnected world, cyber security is a major concern affecting all corners of cyber space. This ranges from major corporations and governments having sensitive data compromised to casual home users encountering ransomware demanding payments to restore their system. While stories of cyber-attacks and commercials for anti-malware products are readily appear in mainstream media, few realize that the threat is right there at the router's door. National initiatives such declaration of National Cyber Security Awareness Month, STOP.THINK.CONNECT, and GenCyber summer camps for school students are aimed at promoting cyber security as "everyone's responsibility". Yet these initiatives for the most part do not bring the threat into full focus. This paper presents a technique for school students and others to experience the ease to which malicious parties may access sensitive information and attack a system. The technique leverages young person's interest in gaming, which in itself is a major surface of attack. The technique has been used as a session in cyber security camps and as a covert lecture in computer science courses. Results have been very positive.
Keywords: Cyber security threats, cyber security awareness, GenCyber workshop

INTRODUCTION

> *Although it may seem that malware attacks and cybercrime live in the adult world, cyber thieves regularly target children and teens where they're most active – chat rooms, social media, video streaming sites and online video games. Children are good targets because they may have high levels of trust in people and low levels of knowledge in cybersecurity. (Corron, 2017, p. 2).*

Cyber security threats have been affecting youth as many unknowingly download viruses and other malicious functions and suffer consequences. This has been going on for years and likely increase in the future. Youth are targeted from different sites where they frequent, like social media, YouTube and gaming web sites. For the gaming web sites, it was noted that a lot of these sites offer games which covertly and deliberately contain viruses and malicious functions (BBC, 2012).

To respond to these threats, several cyber security awareness programs and workshops have been organized to educate young people about the potential threats of unwisely browsing the web (Bada and Sasse, 2014, GenCyber web site, 2018, Kritzinger et al., 2017). But these information security awareness programs do not guarantee the audience will understand the threats and exercise due caution from the lessons learned (Khan, Alghathbar, Nabi, & Khan, 2011). Beda and Sasses (2014) further noted that these workshops often do not achieve the intended results because they did not address the behavioral and specific characteristics that lead the students being hacked. At the same time, others suggested that more is needed to be done to combat cyber security threats and to educate the public about these threats (Defranco, 2011). Kritzinger, Bada and Nurse (2017) offer a list of over fifteen recommendations to improve cyber security awareness education for youth that includes recommendations for teachers and parents.

This paper presents a technique we have developed for raising cyber security awareness in school students, college students and others. This technique has been used as a session in cyber security camps and in freshman college courses.

The remainder of this paper is divided into the following sections:

- A literature review of cyber security threats
- Cyber security awareness efforts
- Theoretical models to promote behavioral change
- Technique to raise cyber security awareness
- Results and discussion
- A summary and notes on further work

LITERATURE REVIEW – CYBER SECURITY THREATS

This section presents literature review on cyber security threats and on threats where youth are a target. Included is a review of specific cyber security threats when downloading games from the internet.

The Potential Cyber Threats

Khan, Alghathbar, Nabi, and Khan (2011) explained that the potential losses of cyber-attacks could include loss of income, loss of customer trust and may be legal action. This is of high concern in the business world (like losing customers) and government (impact to security) but may also impact virtually all who use computers in their daily lives. Possible attacks include:

- Stealing sensitive information
- Corrupting viruses
- Hold data hostage as in ransomware

Stealing of sensitive information is a prime target in computer hacking. The objective here is to obtain sensitive information like social security number, account number, birth date, employee number and others. Once these are obtained by the hackers, the risk can increase as this information can be shared with other criminals and they continue to cause damage. They can buy a car, apply for a mortgage or just use credit cards.

Corrupting viruses can cause damage to the computer by impacting performance, causing crashes, and denying access by affecting authorization. Furthermore, it can enable hackers to gain control of a computer and use a compromised computer as a vehicle to attack other computers. Once a hacker is able to gain control, a hacker can not only steal sensitive information, but can corrupt data and information on the system to causing harm to business and persons (Pzor, 2005).

Ali (2017) noted that a new type of infection is on the rise where cyber criminals demand money for returning data files. In this case, if a computer is hacked with this kind of malware, it encrypts the files and do not allow use of the file until a ransom is paid. When the ransom is paid, then the files are decrypted and allowed access to them.

Youth a Prime Target

Although hackers can target any person or business, they often target youth for the following reasons:

- Youth lack emotional maturity combined with a lack of caution (Defranco, 2011)
- The social and cognitive immaturity of youth offers less protection compared to adults (Straker et al., 2009)
- Lack of knowledge from the youth may push them to act spontaneously while browsing the web (Handeli, 2018).
- Children and youth have high levels of trust for others (Corron, 2018)
- Low motivation to follow security guidelines (Gjertsen et al., 2017)

Kritzinger, Bada and Nurse (2017) suggested that the Internet became more attractive to online predators. They noted further that young children are unaware of the various threats online, they are immediately at an increased risk and highly susceptible to attack. The lack of emotional maturity combined with the ease and abundance of access to the Internet make it easier for hackers to target youth. Through emotional maturity, individuals learn that there are consequences for certain radical behavior on the web. Liam (2010) introduced the "cyber security maturity" that

specifies the steps that it takes to develop a maturity over the web. Without this emotional maturity, the individuals are at risk -they get the hook easily.

Social and cognitive immaturity is proven to be another problem for dealing with these issues. Social maturity teaches a lot and a person who is socially mature is much better to handle cybersecurity risks that others who are not. Through social interaction, individual may learn about viruses and about the loss of data and others. When social maturity is lacking so are the lessons that come with it and among them the lessons about hacking from the cyber space.

Lack of knowledge is another source that may cause the youth to download the viruses (Gjertsen et al., 2017). Most are not aware of the risks associated with their unwise use of the web, they download viruses and get their computers hacked without awareness that it is taking place (Jabee & Alam, 2016).

Gjesrsten and others (2017) suggested that most hacking takes place because the individuals have low motivation to follow guidelines. In children and youth, this could be a factor because some of these guidelines are not well established and are not very clear. It takes experience and it takes certain level of maturity to understand.

Methods to Attack Youth

Although youth can be targeted from many places on the web, there are certain places on the web that where they are attacks are more prone to occur including:

- Social media web sites (Jabeen & Alam (2016)
- Video Streaming Web Sites (Corron, 2018)
- Computer gaming web sites (Avast, 2012)

Jabee and Alam (2016) explained that social networking web sites are platforms for cyber criminals and cybercrimes. As they browse through different web sites, youth face not only the contents that are supposedly to see but also additional people and content, like predator's cyber bully's and other contents (O'Keefe, 2011).

For video streaming web sites, the threat does not come from the videos that are posted on the web, instead they could from other contents posted on the cite. This can include clicking on a link a comments section or a video description or a popup screen that could get their computer hacked and install viruses (Corron, 2018). Giles (2018) noted that some of that hackers follow an art of crafting convincing messages that leads to luring children to click on them and then get hacked.

Computer gaming is another attack surface where youth may inadvertently download viruses and other malicious functions embedded within a game (BBC, 2012). Avast (2012) explained that computer gaming web sites are not risk free. Avast noted further that they searched computer gaming web sites and found more than 60 of them contain viruses which can be easily be transferred to the computer when they visit these gaming web sites. Youth indeed have strong interest in playing computer games (Boyle et al., 2011). It is, however the excitement that the game brings which helps to distract youth from noticing the potential threats (Payne, Abegaz and Antonio, 2016).

CYBER SECURITY AWARENESS EFFORTS

To counter the cyber security risks, many cyber security camps have been organized to promote awareness among youth and promote safe browsing of the web. The timing and the content of the program could be different from one program to another, but they in general share a common purpose for the camps. Bada and Sasse (2014) noted the primary purpose of security awareness is to "influence the adoption of secure behaviors (p. 5)". Jian, Tian and Hu (2017) indicated that cyber security training camps allow students to learn cyber security concepts and principles by applying conceptual knowledge to real-world situations

Given that the primary purpose of the program is to promote the secure behavior, faculty who teach in these camps organize lessons that may contribute to this goal from different perspectives including:

- Game-based training that helps make it more interesting to participate and influence their learning (Jin et al., 2017)
- Challenge-based learning in teaching cyber security awareness is an effective method for delivering the message (Cheung et al., 2018)

- Hands on computer lab lessons that promotes not only the concept but also the practical application (Jian, Tian and Hu, 2017)

GenCyber Program

The National Science Foundation (NSF) and National Security Agency (NSA) have started several initiatives to raise awareness among middle school and high school students. One of these initiatives is the GenCyber program which sponsors summer camps across the United States to promote cyber security awareness and attract students toward a career in cyber security. These camps started in 2014 and has been going every summer since then. Payne, Abegaz and Antonia (2016) explained more about this camp

> The GenCyber program is jointly sponsored by the National Security Agency (NSA) and the National Science Foundation (NSF) to help faculty and cybersecurity experts provide summer cybersecurity camp experiences for K-12 students and teachers. The main objective of the program is to attract, educate, and motivate a new generation of young men and women to help address the nationwide shortage of trained cybersecurity professionals. The curriculum is flexible and centers on ten cybersecurity first principles. Currently, GenCyber provides cyber camp options for three types of audiences: students, teachers, and a combination of both teachers and students (P. 1).

GenCyber programs emphasized the hands-on, active learning and sound pedagogical practice approach for the program (Jin et al., 2017). They are typically organized as a multiday workshop where each day is composed of 50-minute-long sessions. Each session covers a different subject which may range from safe use of social media, reacting to cyberbullying, computer network lab, security protocols, and use of drones to more technical topics such as database exploits lab, robot programing, and game programming. The overall goal of the camps is to promote cyber security knowledge among the participants (Jian, He and Tian, 2017). As a guideline for the program the curriculum is to emphasize a set of "cyber security first" principles, which are:

1- Process isolation	4- Information hiding	7- Least privilege
2- Domain separation	5- Minimization	8- Layering
3- Resource encapsulation	6- Simplicity of design	9- Modularization

The GenCyber program provides grants to universities to pay a nominal stipend to the organizers, cost of materials for running the camp, stipend and travel expenses for teachers attending the camps, prizes, and a small electronic gift (raspberry pi, drone, Arduino, etc.), thereby resulting in no costs to the attendees. Universities receiving grants then promote the program at middle/high schools with goal of attracting 50 or more attendees including teachers at each camp.

Shortfalls of Cyber Security Campaigns

While the security campaigns have many good outcomes, not all are successful in influencing secure behavior. Khan, Alghathbar, Nabi, and Khan (2011) note that educational campaigns are often structured as transfer of knowledge ignoring the motives behind human behavior. Thus, while information is gained it does not result in a change in behavior and awareness. A report from the Information Security Forum (2014) provides other reasons why these campaigns may not achieve the intended goal:

- Solutions are not aligned to business risks
- Neither progress nor value are measured
- Incorrect assumptions are made about people and their motivations
- Unrealistic expectations are set
- The correct skills are not deployed
- Awareness is just background noise

Bada and Sasse (2014) in reviewing existing cyber security campaigns note that fear is often used to influence behavior, however fear invocations by themselves have proved insufficient. A change in behavior will not be effective without combining fear, threat, and efficacy.

THEORETICAL MODELS TO PROMOTE BEHAVIORAL CHANGE

Khan, Alghathbar, and Khan (2011) look to the information motivation behavior (IMB) skills model in their proposed alternate approach to an information security awareness campaign. IMB has been successful in health care and environmental safety domain. By considering motivation and behavior factors in addition to information, they propose a comprehensive security awareness model. Bada and Sasse (2014) in their analysis into why cyber security awareness campaigns fail state that to change behavior there needs to be change in attitudes and intentions. They highlight several psychological models on behavior including theory of reasoned action, theory of planned behavior, protection motivation theory, self-efficacy, and expected utility hypothesis. Of these we believe the protection motivation theory (Rogers, 1975) to be the best applicable model as it considers threat and coping assessments in terms of severity, vulnerability, efficacy, and self-efficacy as a method to motivate change in behavior. Given this, we provide a further explanation of protection motivation theory.

Protection Motivation Theory (PMT)

The protection motivation theory is intended to study what motivates individuals to act in a certain way in the face of threats (Rogers, 1975). It is organized around two appraisals each of which is dependent on evaluating two variables. The first considers threat assessment. It takes into account the severity of a threat, being the degree of potential harm, and vulnerability, being perceived probability that the threat may occur. The second considers the effectiveness of recommended behaviors and practices to cope with the threat, termed efficacy, and a self-evaluation of abiding by the recommended practice, termed self-efficacy. These appraisals when taking together will provide the motivation to adopt the recommended behavior and practice. Figure 1 provides a depiction of the protection motivation model.

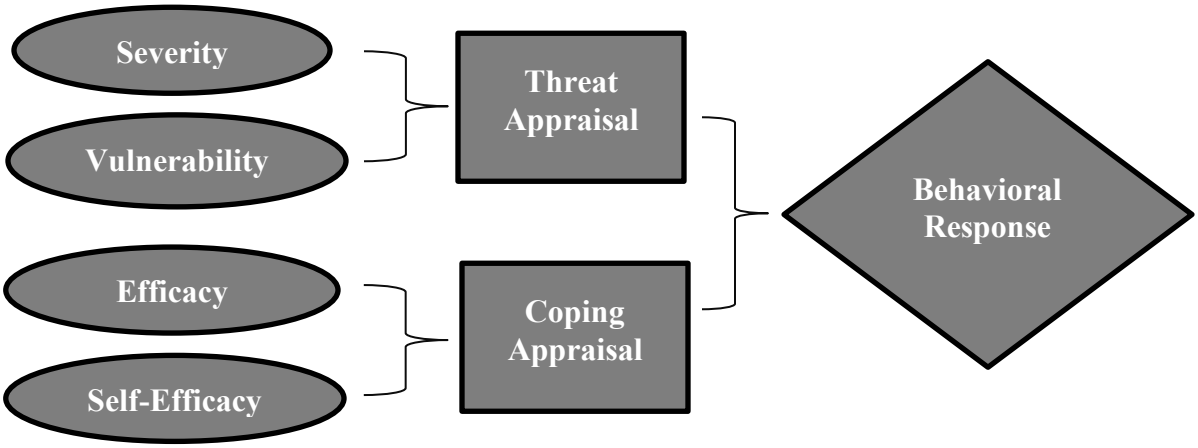

Figure 1. Model of Protection Motivation Theory

THE TECHNIQUE

In this section we present our technique to raise cyber security awareness. It involves a forty to sixty-minute lab/lecture providing a hands-on activity to engage those in attendance. It is promoted as a session in game programing. That is, to introduce students to the basics of object-oriented programming and how it can be used to develop computer games. The real intent of cyber security awareness is kept hidden and is not exposed until near the end of the lab/lecture. In doing so, attendees will directly feel the impact of cyber security threats.

The lab/lecture involves a series of simple yet interesting computer games with which students will see source code, make minor modifications, and play the games. Under the guidance of the instructor, students will make modification to source code to change attributes to game pieces within the games and add new pieces and functions into the games. This activity builds to seeing a complete helicopter attack game with which the students are now eager to play.

In addition to the game programs a short presentation on game programming is included. It presents an overview of object-oriented programming and how it relates to game programing. The presentation contributes to the deception that the session is on gaming.

The Steps

As noted, the intent of this session, although hidden, is to raise cyber surety awareness and to motivate a change in behavior. The steps to achieve this goal are as follows:

Step 1 – Setting the Stage. Here students are told that they will be doing game programming and to prepare for this task they copy a workspace containing all the source code for the games to the desktop of their computer from a network drive. They are also asked to create a word document in which they will list the names of their secret players (anything from sports players to cartoon characters) for their team in a game and a text file to contain a key to use to activate their games. They are asked to save these files on the desktop each under any file name they choose.

Step 2 – The Distraction. At this step the presentation on object-oriented game programming is given. While the presentation does have merit in introducing students on the basics of object-oriented programming and how it relates to gaming, the covert intent is to provide a distraction from the fact that they have just created files on their computer which represent sensitive information. After all, they are told that the names of their players should be secret. Furthermore, the key file is to be used to activate their game and thus should be guarded.

Step 3 – The Draw. Following the presentation, students are guided to open the workspace containing the source code to the games. Under controlled direction students open each of the games and are instructed to make a few changes. Students will change attributes of pieces and add new objects such as soccer balls, obstacles, and bouncing heads. The sequence proceeds from simple static display, to animation of many objects, to a complete helicopter attack game with which all students are enticed to play.

Step 4 – The Hack. While the students are playing the helicopter game, the instructor logs into a remote computer in another office which has a program running that is the backend to the covert activity. Unknown to the students the helicopter game has on a separate hidden thread of execution found the two documents they created on the desktop at the start of the lab and has sent them to the remote computer. The instructor checks the computer has received the files from students.

Step 5 – The Announcement. At this point the instructor gets the attention of the students and makes the announcement "You've been Hacked" and proceeds to show them the file directory on the remote computer. By having the students place the original files on their desktop, the user ids of are part of the hack that are seen as part of the directory structure on the remote system. Copies of their files from their desktop appear in a subdirectory under their user id. A few of the files of the team documents are then opened (with students consent) on the remote computer. This is done to emphasize the files have indeed been stolen.

Step 6 – The discussion. After the announcement several important points are made. While the game program here restricted itself to finding and sending the documents on the student's desktop it could have easily found files of any type anywhere on the computer including bank statements, employment data, and tax returns. While files were sent to a remote computer in a nearby office, they could have been sent to anyplace in the world such as Europe and Asia. The key file is used to emphasize storing of passwords in files could be extremely dangerous as such files could once sent somewhere could allow malicious parties full access to computer systems, bank accounts, credit card accounts, shopping services, etc. While the hack was only used to steal sensitive information, it could have installed a virus or performed other malicious activity. An additional point is made that the vulnerability demonstrated is not restricted to game programs, but to any software that is downloaded and executed on a system. Lastly, prevention techniques such as confirming the source is trustworthy, use of anti-malware products, installation of firewalls, account management, and limiting capabilities are discussed.

RESULTS AND DISCUSSION

The lecture/lab has been presented to various audiences including middle school students, high school students, school teachers, and freshman college students. The first three groups were in the context of a cyber security summer camps

which include GenCyber. The college students were in a lab session of an introduction to computer science course and in an introductory lecture/lab of an object-oriented programming course.
In general, a gasp is expressed by most upon hearing the announcement and seeing the files have been stolen and sent to a remote system. This is most profound in the freshman college students who use computers as an integral part of their lives. Likewise, teachers get what has taken place as the realization that sensitive life impacting data on their computers could be stolen with relative ease. While still effective to some degree, the group having the least impact are the middle school students. They are intrigued that the files have been stolen, however they do not yet have full appreciation that disclosure of sensitive information can have life impacting consequences. Nevertheless, we consider the technique to be effective in demonstrating cyber security threats to the various groups.

We claim the technique is effective in the context of protection motivation theory (PMT). While the two documents stolen in the technique are of no real value, students readily comprehend that information stored on their systems could be highly sensitive therefore demonstrating high severity in the event such information was stolen. The ease by which the information was stolen demonstrates they are far more vulnerable than they are aware. Given high severity and high vulnerability the threat appraisal significantly raises awareness of cyber security threats. It is generally recognized by attendees that recommended practices are effective in coping with the threats. Attendees are thus faced with a self-evaluation with respect to their capability to adhere to those practices. We trust this will result in greater attention to proper cyber security practices thereby resulting in a change in behavior.

With respect to the GenCyber cyber security first principles, the technique speaks to process isolation, resource encapsulation, and least privilege. All software, especially software that has been downloaded, should be run in isolation from other tasks. Sensitive information is a resource that should be encapsulated from external access. Programs should be executed with least privilege to ensure malicious activity is not successful. These would be recommended practices to be adopted.

SUMMARY, FURTHER WORK, AND SOLICITATION FOR COLLABORATION

In this paper we have presented the background on the need for raising cyber security awareness, the shortcomings of cyber security campaigns, and the specific threat facing youth as they download and play games from the internet. Given the strong interest in gaming, we developed a technique for youth and others to feel the reality of potential threats. Overall, we feel the technique is very effective in raising cyber security awareness. We trust that it has stimulated those in attendance to give careful thought when downloading and running software (especially games). We also emphasized the importance of correct configuration of network and anti-malware software, and to operate their computers in a safe manner.
We would like to develop a new set of games and an updated polished presentation that is package for distribution and use by cyber camp instructors, high school teachers, college professors and others. Our plan is to develop another study that builds on this one using the package.

The results presented here are subjective. We would like to develop empirical methods to assess its effectiveness and to gather data from a broader base. Here to we would welcome feedback and collaboration from professors and professionals in the field.

REFERENCES

Ali, A. (2017). Ransomware: a research and a personal case study of dealing with this nasty malware. *Issues in Informing Science and Information Technology*, *14*, 087-099.

Avast (2012). Avast Software: Online games sites can be cute, pink, and infected. Retrieved February 12, 2019 from https://press.avast.com/avast-software-online-game-sites-can-be-cute-pink-and-infected.

Bada, M & Sasse, A., (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?, *Global Cyber Security Capacity Centre*, University of Oxford: Oxford, UK

BBC (2012, March 8). Hackers spread malware via children's gaming websites. *BBC News Technology*. Retrieved February 12, 2019 from https://www.bbc.com/news/technology-16576542

Boyle, E. Connolly, T. M., Hainey, T. (2012). The role of psychology in understanding the impact of computer games*, Entertaining Computing*, *2*(2), 69-74.

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Corron, L. (2018, January). Social Cyber Threats Facing Children and Teens in 2018. Retrieved from November 5th, 2018 from https://staysafeonline.org/blog/social-cyber-threats-facing-children-teens-2018/ .

DeFranco, J., F. (2018). Teaching Internet Security, Safety in our Classrooms. Techniques, May 11, 52-55.

GenCyber website, INSPIRING THE NEXT GENERATION OF CYBER STARS Retrieved January 31, 2019 from https://www.gen-cyber.com/about/.

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., & Flores, W. R. (2017). Gamification of Information Security Awareness and Training. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy,* Porto, Portugal, 19-21

Giles, M. (2018). Six cyber threats to really worry about in 2018. *Technology Review*.

Handeli, K. (2018, March). A Cybersecurity High School Curriculum Course. In *Society for Information Technology & Teacher Education International Conference* (pp. 864-869). Association for the Advancement of Computing in Education (AACE).

Jabee, R. & Alam, M, A (2016, June). Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). *International Journal of Computer Applications, 144 (3), , 36-40.*

Jiang, P., Tian, X., Xin, C., & He, W. (2017, June). Teaching Hands-On Cyber Defense Labs to Middle School and High School Students: Our Experience from GenCyber Camps. In *EdMedia+ Innovate Learning* (pp. 640-644). Association for the Advancement of Computing in Education (AACE).

Jin G., Tu M., Kim T., Heffron J. & White J., (2018). Game based Cybersecurity Training for High School Students. P*roceedings of the 49th ACM Technical Symposium on Computer Science Education,* Baltimore, MD, USA, 68-73.

Information Security Forum (ISF). From Promoting Awareness to Embedding Behaviors, Secure by choice not by chance, February 2014. Retrieved from: https://www.securityforum.org/shop/p-71-170

Khan, B., Alghathbar, K. S., & Khan, M. K. (2011). Information Security Awareness Campaign: An Alternate Approach. *Communications in Computer and Information Science*, *5*(26), 10862-10868.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Managemen*t, *200*, 10862-10868.

Kritzinger, E., Bada, M., & Nurse, J. R. (2017, May). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In *IFIP World Conference on Information Security Education* (pp. 110-120). Springer, Cham.

Liam, M. M., Bahr, G. S., Carey, D. B., Matthew, G. B., Ford, R., Kevin, L. F., ... & Wayne, B. S. (2010, October). A hybrid cognitive-neurophysiological approach to resilient cyber security. In *Military Communications Conference MILCOM 2010* (pp. 942-947). IEEE.

O'Keeffe, G. S., & Clarke-Pearson, K. (2011). Clinical report—the impact of social media on children, adolescents, and families. *Pediatrics*, peds-2011.

Payne, B. R., Abegaz, T., & Antonia, K. (2016). Planning and Implementing a Successful NSA-NSF GenCyber Summer Cyber Academy. *Journal of Cybersecurity Education, Research and Practice*, *2016*(2), 3.

Pzor, P. (2005), *The Art of Computer Virus Research and Defense*, Symantec Corporation

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Straker, L., Pollock, C., & Maslen, B. (2009). Principles for the wise use of computers by children. *Ergonomics*, *52*(11), 1386-1401.