Toni Hunt

Cyber Security Awareness in Higher Education

Central Washington University

Abstract

With technology advancing every day our society is becoming more connected than we have ever been before. While these advances are making our daily lives easier they are also adding extra risks to our personal information. Most people do not think about their identities getting stolen when they make an online purchase, check their email, or use social media. However, each time that you put your personal information on the Internet you are at risk of that information getting stolen. This is especially true for students, who spend so much time online doing school activities. Every time that they login to do school work, they are putting themselves at risk. There are many simple ways that these risks can be reduced, but it starts with cyber security awareness.

The purpose of this research paper is to discuss the security challenges that are associated with the digital age. The topic of cyber security is one that should be talked about more often in today's society. This paper points out the importance of cyber security awareness and protection. It touches on the major ideas of why our academic community and corporations are currently in a predicament. Lastly, the paper ends with four proposed solutions on what can be done to address cyber security challenges in higher education.

Keywords: cyber, security, awareness, protection, Internet, students, higher education

Introduction

What is cyber security and why should we care? Cyber security has become a new concept in the last decade. With technology advancing every day our society is becoming more connected than we have ever been before. While these advances are making our daily lives easier they are also adding extra risks to our personal information. Most people do not think about their identities getting stolen when they make an online purchase, check their email, or use social media. However, each time that you put your personal information on the Internet you are at risk of that information getting stolen. This is especially true for students, who spend so much time online doing school activities. Every time that they login to do school work, they are putting themselves at risk. There are many simple ways that these risks can be reduced, but it starts with cyber security awareness.

Cyber Security

The internet is not a secured space. It is an area where there currently are not many regulations. It is where anyone can put up, take down, or gather as much information as they want (Hall, 2012). It is open for anyone to place any information that they want online. Cyber security is becoming an increasingly talked about topic. With more and more people making their personal information available online than ever before, it is becoming a hacker's paradise. There are multiple different schemes that have been happening recently that are associated with Internet usage. Some of these scams involve hackers cracking passwords to get access to personal information and criminals using phishing techniques to gather information that they can use to steal individual’s identities. Lastly, some schemes include phishing techniques used to con people out of money (Jansson & von Solms, 2013).

However, most individuals do not know about all of these scams and are unaware when they are happening to them. Because of this, people do not know how to protect themselves and how to stop being a target. It is important that we, as a nation, focus on making these individuals aware of the potential risks associated with the Internet. Cyber security needs to be more common knowledge and education needs to be more readily available. It is important for us to help educate individuals on what they can do to stop and prevent potential cyber security attacks. It is also especially important that our students to be able to recognize potential threats. Therefore, cyber security, awareness, and education needs to be taught at the higher education level.

Awareness

We log into our email account, bank account, or social media account and we do not even think about the process. These are the types of activities that hacker’s make a living off of. The majority of people are not only unaware that cyber threats are real, but are also unaware of what to do about them. Most people just hope or assume that identity theft and phishing attacks are not going to happen to them. Ignorance is bliss after all. But, making society aware that even the smallest tasks can pose potential threats is crucial for their safety.

Awareness is the first step in reducing the number of identity thefts and personal information threats. The majority of individuals understand that by having their personal information online that they are taking a risk of that information being compromised. However, they do not possess the knowledge to know how to protect themselves. These people also understand that they should not include very sensitive information online, such as their social security numbers. Yet, they do not realize that even accessing your email could be just as detrimental to their safety.

Individuals believe that if they have a unique password then they are protecting themselves enough that they do not have to worry about cyber security threats (McCrohan, Engel, & Harvey, 2010). While this is a good first step, and it is strongly recommended to create unique passwords, it still simply is not enough to keep information private. Most hackers have the technology and knowledge to know how to decrypt these passwords or bypass them completely. Each day that our technology is improving is another day that hackers are figuring out how to crack that technology. “There is no argument whatsoever that the proliferation of devices and information are empowering. Technology is today far more democratically available than it was yesterday and less than it will be tomorrow” (Geer, 2015).

Likewise, much of the population believes that installing virus protection or spy software onto their computers is enough. They think that this software is going to save them from ever being hacked or having their information stolen (McCrohan, Engel, & Harvey, 2010). This is also simply not true. We need to change this way of thinking by helping society recognize the signs of the potential threats and risks. We then need to hand them the information that they need to keep themselves safe and protected. Some of the signs that users need to be aware of that usually indicate a phishing attempt are: words being misspelled, a certain degree of urgency or “deadlines”, fake names and web links, and a request for personal information (Lungu & Tăbuşcă, 2010).

Higher Education

While cyber security awareness is an important topic for anyone to discuss, it is especially important for students involved in higher education. College students are becoming a target for phishing attacks at increasingly high rates. Due to the amount of time spent on the Internet, college student's information is at a greater risk. This is especially true for the students that are enrolled in online programs and classes. Since they spend a lot of time using the Internet for research, communicating with other students, and participating in class activities, they are a perfect target to hackers.

Because of this, the topic of cyber security awareness is becoming more critical than ever to discuss in higher education environments. There is currently a lack of awareness amongst students due to the absence of education that is readily available to them. In fact, a study that was conducted by the National Cyber Security Alliance (NCSA) and sponsored by the Microsoft Corporation found "that schools are ill prepared to teach students the basics of online safety, security and ethics, skills that are necessary in today's digital times" (U.S. Schools Not Preparing Kids for Digital Age, 2013). This is because we are not talking about the importance of cyber security as much as we should be in the United States. We have not set up our academic requirements to include this critical education. We must make cyber security awareness a priority in our education systems.

There are so many phishing schemes out there aiming to steal the identity of individuals or aiming to con people out of money. So, it is important for us to not only be aware of the threats, but to also know what to do about them. Just like math or science is a college degree prerequisite, it should be required that students learn the basics of cyber security before they are able to graduate. In the United States, our education system is not making this a priority or a concern for our students.

"America's schools have not caught up with the realities of the modern economy. Teachers are not getting adequate training in online safety topics, and schools have yet to adopt a comprehensive approach to online safety, security and ethics as part of a primary education. In the 21st Century, these topics are as important as reading, writing and math" (Geer, 2015). With technology changing every day, potential risks are changing as well, and it is critical that protection education be made more available. "It is our job to teach students how to stay ahead of the technology race" (Geer, 2015). Teaching the next generation how important Internet safety and security is should be something that the Department of Education is focusing on and making a priority.

In current studies on the topic, it has been shown that with the proper education and training, students can learn to change their Internet behavior. Students have shown that they are able to comprehend the importance of cyber security protection. "From the data and findings..., it may reasonably be concluded that users can learn and positively adapt their e-mail behaviour – as a result of simulated phishing exercises – together with embedded training" (Jansson & von Solms, 2013). From this study it shows that with the proper education and training students are able to learn some of the basic fundamentals of cyber security and identity protection. With this training, students were more aware of the threats and were able to understand how protection can make a huge difference.

Therefore, with the proper training and education our students can be more prepared for these digital threats. "Therefore, it may be deduced that simulating phishing attacks together with embedded training can, indeed, contribute towards cultivating users' resistance to phishing attacks" (Jansson & von Solms, 2013). Giving the students the skills and knowledge on how to protect against cyber threats and phishing attempts has proven to be successful. It enables them to have the knowledge and power to know what they should do and what does not work. This shows that having classes and degrees in Universities that focus on cyber security awareness and education is worth it.

Mobile Awareness

Cyber security threats are not only common with computers. These threats are becoming increasingly popular on mobile devices. This is something that everyone, including students need to become aware of as well. With just as much information, if not more, on our cell phones as on our computers, hackers are starting to utilize the same technics that they do for computer phishing as they are now using for mobile device phishing. This threat is also something that students also need to recognize and become aware of. Behaviors need to change with both computer and mobile device usage. Just because your phone is almost always in your possession does not mean that the information in it is secured.

Education needs to become more available for both computer security and mobile device security as well. Many corporations are at risk because their employees are not knowledgeable on internet protection. This problem is one that needs to be addressed at the higher education level with college students (Patten & Harris, 2013). Many of the same security threats that are associated with computers are also associated with mobile devices. However, mobile devices pose more threats and challenges when it comes to protecting your information. This is because your cell phone usually holds more personal data than your computer does. Also, with mobile devices constantly moving in and out of Wi-Fi networks, many of which are unsecured, it makes stealing data easier for hackers. Another problem with mobile device security is the amount of malware being downloaded from App downloads. Malware on mobile devices is now higher than it is for PCs (Patten & Harris, 2013).

Creating a Safer Future

Teaching cyber security awareness and protection to students is not only important for their personal safety, but it is also setting us up for a safer future. Many of the threats that companies face could have been prevented if their employees were more educated on the subject of cyber security. “The state cyber-security in the United States is suffering from a lack of attention from industry and academia” (Pappalardo, 2004). This is leaving large corporations unprotected because their employees are not trained in this field. This is also leaving many of their client’s personal information unsafe and unsecured. It is the responsibility of The Department of Education to address attention to this major issue.

In fact, this issue is becoming “a matter of local and global importance” (U.S. Schools Not Preparing Kids for Digital Age, 2013). The workplace is filled with challenges associated with the digital age. Students in the United States are coming out of college not prepared to handles these challenges. This is making it difficult for employers who are looking for an IT professional that can help them with their cyber security needs. Since employers are not able to find these professionals who are both trained in general IT and security, it is leaving the employers and their company vulnerable. “Not only must students know how to stay safer online at school and at home, but they also must be equipped to deal with the workplace challenges of the digital age” (U.S. Schools Not Preparing Kids for Digital Age, 2013).

Technology is continuing to change and therefore curriculum needs to be changing along with it. “Cybersecurity is perhaps the most difficult intellectual profession on the planet” (Geer, 2015). Employers are realizing that they need more employees that have technology and security knowledge, but are finding it difficult to find students with the right combination of knowledge and expertise (Patten & Harris, 2013). They are finding that students are usually trained in specific areas of IT, but not with knowledge of cyber security practices. Colleges and Universities should be steering students towards degrees and careers that focus on cyber security and IT practices for the future safety of US organizations (Peterson, 2014).

Proposed Solutions

So what is to be done about this ever increasing dilemma? Well, there are a few options. The first option is to make everyone aware of the problem and get them excited about learning about cyber security. President Obama has taken the first step in making this come to life. He has declared that October will be National Cyber Security Awareness Month (Homeland Security, 2016). NCSAM is all about getting both the public and private sectors aware that the internet affect's all of our daily lives, whether we realize it or not. The month is filled with events that are aimed at making the community aware of the threats associated with the internet. In addition to NCSAM, January 28th has been declared National Data Privacy Day (StaySafeOnline.org). On this day the National Cyber Security Alliance holds an event to promote cyber security awareness. They encourage users to STOP. THINK. CONNECT. All of these events are a great way to get information out to the public. However, for it to sink in for users and to make a difference we need this information to be important all year long, not just in October or on January 28th. These events are great for awareness and for getting the public excited about cyber security, but the end goal is for this information to be important year round.

The second option to solving this problem is starting cyber security education at younger ages. This topic should be just as important as history and gym. We need to start education in the middle school and high school levels. If we education students when they are younger, then there is a chance that we can get them excited about cyber security. We can create passion in students and they will then continue with that passion into college and their future careers. "Kids and teens have embraced the digital world with great intensity, spending as many as eight hours a day online by some estimates” (U.S. Schools Not Preparing Kids for Digital Age, 2013). This option will work because kids are already interested in the digital world, now we need to get them interested in how to protect themselves. We need to create a generation of cyber security enthusiasts.

The third option is to better educate our teachers. A major reason that our students are not educated on the affects cyber security is because our teachers are not educated on the subject either. “Yet, few …educators are teaching topics that would prepare students to be cyber-capable employees or cybersecurity-aware college students” (U.S. Schools Not Preparing Kids for Digital Age, 2013). The only way that we can expect student’s behavior to change is if we teach them the proper way to handle these situations. Therefore, students who are now enrolled in teaching programs should be required to take cyber security courses. And current teachers should focus on online safety and cyber security awareness when taking continuing education courses and professional development training.

Lastly, the fourth option is for the academic community and corporations to team up (Pappalardo, 2004). We need to know what these corporations are looking for in an IT professional when they come out of college. We need to know what their company’s needs are. Then the academic community will be able to come up with curriculum that meets and exceeds those needs. We need to start producing college graduates that possess the knowledge, skills, and capabilities to handle the new challenges that are associated with the digital age and cyber security.

Conclusion

Cyber security awareness is more important now than it has ever been before. Threats to personal information is increasing and identities are getting stolen every day. Making individuals aware of this is the first step. The second step is giving individuals the tools and knowledge that they need to protect themselves. Focusing more on higher education curriculum is a key factor for the safety of our students and for the safety of our future. Why The Department of Education has not made cyber security awareness and education a prerequisite is a mystery. The importance of educating our students can-not be expressed enough. This is becoming a pressing issue for The United States. We are now aware that this is an issue, it is our responsibility to make society aware as well.

References

Geer, D. (2015). Six Key Areas of Investment for the Science of Cyber Security. *Futurist, 49*(1), 10-15.

Hall, C. (2012). Security of the Internet and the Known Unknowns. *Communications of the ACM*, *55*(6), 35-37. doi:10.1145/2184319.2184332

Homeland Security. (2016, March 24). Retrieved March 24, 2016, from https://www.dhs.gov/national-cyber-security-awareness-month

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584-593. doi:10.1080/0144929X.2011.632650

Lungu, I., & Tăbuşcă, A. (2010). Optimizing Anti-Phishing Solutions Based on User Awareness, Education and the Use of the Latest Web Security Solutions.*Informatica Economica*, *14*(2), 27-36.

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. doi:10.1080/15332861.2010.487415

National Cyber Security Alliance | StaySafeOnline.org. (n.d.). Retrieved April 11, 2016, from https://staysafeonline.org/

Pappalardo, J. (2004). Cyber-security Hampered by Lack of Attention. *National Defense,89*(610), 11.

Patten, K. P., & Harris, M. A. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. *Journal Of Information Systems Education*, *24*(1), 41-52

Peterson, J. (2014). America's Cyber-Star Search. *U.S. News Digital Weekly*, *6*(27), 13. http://ezp.lib.cwu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=96928025&site=ehost-live

U.S. Schools not preparing kids for digital age. (cover story). (2011). *Computer Security Update*, *12*(6), 1-5.