Raising Cybersecurity Awareness among College Students

Yesem Kurt Peker, Lydia Ray, Stephanie Da Silva, Nathaniel Gibson, Christopher Lamberson

Cybersecurity is of increasing importance due to the rise in reliance on digital equipment and programs to manage our daily lives, including the transmission and storage of personal information. Research studies establish that an effective security awareness program is one of the most important steps towards increasing cybersecurity. In this project we set out to understand the current level of security awareness among college students and develop a module that will help raise their awareness. The main features of our module are interactivity and the presentation of shocking consequences of careless cyber habits of common Internet / technology users. We designed a survey that includes pre and post-tests to fulfill the goals of our project and administered it to students on our campus. Our survey results indicate that the module has been effective particularly among non-Computer Science majors. It has raised their level of awareness not only for the specific topics that the module addresses but overall in cybersecurity.

1. INTRODUCTION

Monday morning Cindy realizes she forgot to e-mail that essay on the process of cell division and regeneration. She opens her email and filters through her files to attach her document. She quickly sees a message from her school telling her that her password expired. Thinking this might slow her process for the day's activities, she opens the e-mail and fills the form to reset her password. She does not realize that she, like hundreds of others, just fell victim to a phishing attack. Her password information is now in the hands of malicious attackers who, with that single password, can compromise the entire network of her school.

Cindy's story represents a common ignorance of people in managing and protecting their information in cyber space, and accessing information from the

Internet. As a result of this ignorance, threats of cybercrime are continuously in rise. Security threats to Internet users are exposed through stories of web cams being hacked to access personal videos, Internet traffic being redirected to fake websites for extraction of passwords, social media being stalked to steal identities. And individual users are not the only ones at risk; companies, institutions, and governments are at risk every day. There are reports of Russia and China using cyber-attacks to gather information from agencies in other countries (Adams, 2015); a popular general merchandise store, Target, experienced one of the most high-profile credit card breaches in 2013, exposing credit card information for millions of customers (Newman, 2015). Cyber criminals are now targeting hospitals, and locking down hospital systems for ransom, thereby exposing many patients to serious life risks (Zetter, 2016). Remarkably, in all these recent incidents, the underlying cause of security breach was ignorant human behavior.

Cyber security is of increasing importance due to the rise in reliance on digital equipment and programs to manage our daily lives, including the transmission and storage of personal information. This digital world provides many conveniences, but also poses new risks that often go unknown or unnoticed. The pace of growth of the Internet exceeded expectations and predictions by early Internet developers (Chouchri, Madnick, and Ferwerda, 2014). Perhaps it is this unexpectedly rapid growth of the Internet that has left users in the dark about cyber security issues. We (society) did not plan, create, and disseminate education about cyberspace quickly enough to match the increased use of cyberspace. As a result, common users of the Internet / technology (including current college students, most of whom were raised in a cyber world) are ignorant of risks to their safety and personal information through the use of electronics in unsecure ways. Kim (2013) argues that, counterintuitively, it is the heavy users of digital devices who are usually the least knowledgeable and aware of cyber security issues and prevention. Although concern over protection of one's physical body, property, and space is natural for most people, concern about protecting one's information and property in cyber space is not natural.

As stated by Ludwig (2003) "There are numerous controls IT professionals can implement to safeguard electronic information from unauthorized users. But it's the authorized end users that possess the IDs and passwords to access that data giving them the ability to print it, share it, alter it or delete it. If they are careless with or choose weak passwords, casually discard confidential printed reports in the trash, prop open doors to secured areas, fail to scan new files for viruses, or leave back-ups of data unsecured, then that information remains at risk."

Researchers have observed the consequence of lack of security awareness of people a decade ago (CSI, 2007). Recently Aurigemma and Panko (2012) pointed out that software and hardware security mechanisms can successfully minimize risks for information security only if users of the specific system consistently follow a secure policy. These studies establish the fact that an effective security awareness program is one of the most important steps towards increasing cybersecurity. As the society is becoming increasingly dependent on technology, the need for creating a culture of safe cyber behavior is growing significantly.

Per NIST 800-50, an awareness program, unlike a security training program, specifically intends to change behavior and culture. It aims to provide information that impacts daily actions. That requires a drastically different approach than just providing information. While employees in some organizations get specific security training, for a vast majority of technology users (common people including college students and school kids), security awareness is limited to some tips for security available in some websites. This is why most security awareness programs fail. The increasing number of data breaches and other cyber-attacks clearly demonstrate that these tips are not enough to raise public security awareness to a level required to create a secure cyber culture.

A security awareness program is difficult to implement (Manke & Winkler, 2013). According to Manke and Winkler the measures that create the greatest likelihood of security awareness success include the use of creativity in disseminating materials and participatory experiences.

We hypothesized that an adequately interactive security awareness module that demonstrates the shocking consequences of careless cyber habits of common Internet / technology users will effectively increase awareness at a large scale and will eventually help build a safer cyber culture. Based on this hypothesis, we created the project "Campus Security Awareness Online Module" that aimed at creating an interactive e-learning module to improve college students' awareness of cyber security. Using a combination of educational strategies, as recommended by Abawajy (2014), the online module contains elements of text, video, and game-playing to convey information about cyber security. Multiple exercises within the module contain probes to make users aware of limits and / growth in their understanding of cyber security risks, thereby facilitating awareness. Building on the work of McCrohan, Engel, and Harvey (2010), we used a pretest-posttest design to assess changes in cyber security awareness. A pilot study was conducted on a group of college students. The results show that the learning module not only increased cybersecurity awareness on the specific topics it addressed, but also helped the participants gain an insight about cybersecurity in general.

This paper describes the project and the results of the pilot study that has been done. We have organized the paper in the following way. In next section, we describe related work on this topic. In section 3, we describe the project in details. In section 4 results of the pilot study are discussed. Finally, we draw the conclusion from our study and state our direction for future research on this topic.

2. RELATED WORK

The importance of public security awareness has been studied by researchers a decade ago. CSI (2007) determined lack of security awareness of people as one of the most critical computer security issues in coming years. Kim (2013)'s study shows that, counterintuitively, it is the heavy users of digital devices who are usually the least knowledgeable and least aware of cyber security issues and prevention.

Attempts to educate people about cyber security risks have surged in the past 5 years (e.g., Power & Forte, 2006; Vacca, 2012). See Franke and Bryneilsson (2014) and Tsohou, Kokolakis, Karyda, and Kiountouzis (2008) for reviews of programs developed to improve cyber security awareness. Also note that governments and institutions worldwide have created programs, such as CyberWatch and US-CERT, to increase awareness and responsiveness to cyber security threats. National Cyber Security Division (NCSD) within the Department of Homeland Security and the National Cyber Security Alliance (NCSA) declared the month of October as Cyber Security Awareness Month in 2004 citing the importance of making the public aware of cyber security issues. Since then many schools, organizations, and businesses adopted it. Kim (2013) argued that cyber security training is imperative for college students and that survey data can help determine whether problems with security are due to lack of concern or lack of skill (in navigating devices' security settings).

3. DESCRIPTION OF THE PROJECT

The project involves the development of a cybersecurity awareness module that will help raise the level of security awareness in using the Internet and the technology associated with it among college students. The main attributes of our module that distinguishes it from some other cybersecuirty awareness modules are interactivity and the presentation of shocking consequences of careless cyber habits of common Internet / technology users. We believe these attributes will effectively increase awareness at a large scale and will eventually help build a safer cyber culture. The goal of our project is two-fold:

1) To observe the pattern of security awareness of college students before completing the module.

2) To assess the effectiveness of the module in raising awareness among college students.

We have targeted college students as our audience because of the following reasons:

- College students use technology and the Internet for the two major activities: education and socializing.

- The culture of BYOD potentially weakens the security of university networks and poses major risk of data breach (DiFilipo, 2013).

- College students are the future workforce, future teachers, and parents. The impact of their security aware behavior will be significant and far reaching for the society.

Salient features of our project are:

- The project focuses on the three most common vulnerabilities of people's cyber habits:
    - weak / default passwords
    - lack of awareness about social engineering
    - risky browsing habits that can interfere with privacy
- The awareness module combines interactive exercises and videos together to demonstrate disastrous effects of careless cyber behavior.
- The project carefully administers a survey with pre and post-tests to assess the impact of the program.

3.1 Description of the Module Exercises

The e-learning module contains three units titled Password Security, Social Engineering and You, and Browser Security. Each unit is designed to provide the user with information about the topic and engage them in the topic by providing interactive exercises such as entering passwords, watching short videos of news clips of incidents related to the topic, and / or checking out interesting websites relevant to the topic. Below are the descriptions for the exercises in the module.

3.1.1 Password Security

Weak passwords remain to be the biggest threat to one's privacy as was noted by Tozzi (2016). People still tend to rely on weak passwords that can easily be broken leading to data theft and other vulnerabilities for the user (Hern, 2016). This unit includes three exercises on passwords:

a. Password Strength: This exercise first explains the user what makes a good password. Then it asks the user to enter a possible password; analyzes it; and presents the user a table with information on what components for a strong password it has and what it is missing as well as an estimation of how long it would take to break the password depending on the set of characters used in it.
b. Password Cracking: Continuing the first exercise, this exercise briefly describes how dictionary and brute-force attacks work and allows the user to enter a password (composed of no more than 5 lower-case letters for the sake of time) and provides the timings of how long it takes to crack the password using either of the methods.
c. Default Passwords: After describing that some devices come with a default password for easy set-up and accessibility, this exercise provides the user with a video of a news clip warning them about using the default password on a webcam. The exercise also provides a link to a website that lists default passwords for many devices including webcams and routers.

3.1.2 Social Engineering

This unit focuses on phishing, the art of tricking people to handing over their credentials to protected systems. The number of people who fall for phishing attacks is staggering. The Verizon Data Breach Investigations Report (2015) reports that a study of 150,000 phishing emails by Verizon partners found that 23 percent of recipients open phishing messages and 11 percent open attachments.

This unit in our module includes two exercises:

a. Phishing and You: This exercise starts with the definition for phishing and warning signs in an email for a phishing attack. It then demonstrates a technique used by attackers where the URL displayed for a link and the URL that the browser connects to when that link is clicked are two different sites.

b. Fake Websites: This exercise demonstrates a technique used by attackers where an innocent looking link takes the user to a website that looks very much like the website mentioned in the link but in fact is a completely different site purposely replicating the legitimate site. This could be a malicious site asking for user credentials!

3.1.3 Browser Security

For many the internet browsers are the windows that connect them to the cyberworld. People do most of their activities on the Internet through web browsers yet they don't take control of their browser; they often accept the default settings and are not aware that they can change these settings. This exercise provides brief descriptions of common browser functionalities that may pose concerns for security such as cookies, scripts in codes, and plugins. It also provides the user simple instructions to get to the security settings on common browsers including Chrome, Firefox, and Internet Explorer. Then users are informed of official support sites of these browsers where in depth explanations of the various options in their security settings are provided.

3.2 Description of the Survey

The pretest-posttest was a self-devised survey of 20 items assessing users' concern and awareness related to cybersecurity. The items mainly asked users to rank their awareness level in setting up passwords, browsing the internet, clicking on links, etc. In the post-test, users also completed a short survey to provide feedback about elements of the module that were enjoyed or not enjoyed, and to provide suggestions for improvement(s). The comparison of the pretest-posttest results yielded information on the effectiveness of the module.

4. RESULTS

Scores on the Cybersecurity Awareness Survey (CAS) were computed for each participant. Responses to each item were coded from 1-4, where 4 represents the most concern or awareness and a 1 represents the least concern or awareness. Higher scores, then, indicate more concern. Total scores on the survey were computed by calculating the mean of participants' answers across all 20 items.

There was a significant increase in CAS scores from pretest (M=2.93) to posttest (M=3.36) according to a paired-samples t test, t (25) = 4.478, p<.001, comparing changes in awareness for the entire sample (n=28). More telling, perhaps, is the differences in findings obtained for the participants / students who are majoring in Computer Science and participants / students who are majoring in other disciplines. Figure 1 contains a summary of CAS pretest and posttest scores for participants grouped by major. An independent-samples t test revealed that the mean CAS score of Computer Science majors (M=3.43) was significantly higher (p=.002) than the mean CAS pretest score for other majors (M=2.70). Completion of the module increased the CAS scores of participants who are not Computer Science majors to the point that their mean CAS posttest score (M=3.34) was not different (p=.80) from the Computer Science majors' CAS posttest score (M=3.40). It appears from these data that the module effectively improved cybersecurity awareness of participants who are not Computer Science majors (even to the point they are as concerned about security as Computer Science majors).

Table 1 contains the mean score for each item on the CAS on the pretest and posttest for Computer Science majors and students who are majoring in other disciplines. Paired-samples t test were used to compare pretest and posttest responses on each item individually. Responses to zero items changed significantly for Computer Science majors (as noted by the absence of any asterisks in the table indicating significance of items for Computer Science majors). For participants who are not Computer Science majors responses to most items on the CAS increased (as indicated by the asterisks), indicating their awareness or concern about that topic increased after completing the learning module. On all 20 items, CAS scores increased by 24% (a significant amount, p<.001) for non-Computer-Science majors after completing the learning module.

A final analysis of the data involved comparing pretest-posttest scores on items that were addressed explicitly by the learning module (i.e., Items 1-10) and pretest-posttest scores on items that were not addressed explicitly in the learning module (i.e., Items 11-20). Interestingly, posttest scores were significantly higher than pretest scores on both sets of items (p<.001) This indicates that the learning module not only increased cybersecurity awareness on the specific topics it addressed, but also helped participants gain an insight about cybersecurity in general.

Survey Item		Comp. Science		Other		
		Pretest	Posttest	Pretest	Posttest	
		Score	Score	Score	Score	
1	How important is cyber security to you?	3.63	3.63	3.28	3.56	
2	How concerned are you that cyber security could affect your personal safety?	3.50	3.75	2.78	3.39	★
3	How important do you think it is to renew or update your passwords?	3.38	3.38	2.67	3.50	★
4	How concerned are you about the strength of your passwords?	3.25	3.13	2.61	3.22	★
5	How likely are you to change the default password on an electronic gadget (for example, a web cam) you use?	3.63	3.50	2.44	3.39	★

Survey Item		Comp. Science		Other		
		Pretest	Posttest	Pretest	Posttest	
		Score	Score	Score	Score	
6	How concerned are you that your personal information may be compromised when you use the Internet?	3.50	3.00	3.22	3.56	
7	How aware are you of the security implications of *https:* versus *http:* in website addresses?	3.38	3.38	1.44	3.33	★
8	How careful are you when opening e-mails from unfamiliar senders / addresses?	3.50	3.50	2.61	3.22	★
9	How aware are you of phishing attacks and their dangers?	3.25	3.50	1.89	3.33	★
10	How likely are you to click on an unknown link provided to you in an e-mail?	2.63	2.50	3.50	3.33	

Survey Item		Comp. Science		Other		
		Pretest	Posttest	Pretest	Posttest	
		Score	Score	Score	Score	
11	How concerned are you about using a credit card for shopping online?	3.50	3.50	2.67	3.33	⋆
12	How concerned are you about your identity or privacy when using social media?	3.38	3.38	2.89	3.44	⋆
13	How careful are you when posting your location or photos on social media?	3.50	3.63	3.28	3.67	
14	How concerned are you that your smartphone can get a virus?	3.25	3.25	2.78	3.17	
15	How careful are you when installing apps to your phone?	3.38	3.38	2.56	2.94	
16	How careful are you when opening e-mails from unfamiliar senders / addresses?	3.75	3.63	3.17	3.83	⋆

Survey Item		Comp. Science		Other		
		Pretest	Posttest	Pretest	Posttest	
		Score	Score	Score	Score	
17	How aware are you about potential viruses / malware on your computer?	3.63	3.63	2.33	3.22	★
18	How concerned are you about connecting to an open WI-FI?	3.25	3.25	2.28	2.89	★
19	How careful are you when downloading files from the Internet?	3.50	3.50	2.78	3.22	★
20	How important do you think it is to keep your computer up to date?	3.75	3.63	2.89	3.22	★

Mean Score on First 10 Items (topics in Module)	3.37	3.33	2.64	3.38	★
Mean Score on Last 10 Items (topics not in Module)	3.49	3.48	2.76	3.29	★
Mean Score on All 20 Items	3.43	3.40	2.70	3.34	★

Survey Item	Comp. Science		Other		
	Pretest	Posttest	Pretest	Posttest	
	Score	Score	Score	Score	
Note: Asterisk (*) indicates significant change from pretest to posttest, where p < .05.					

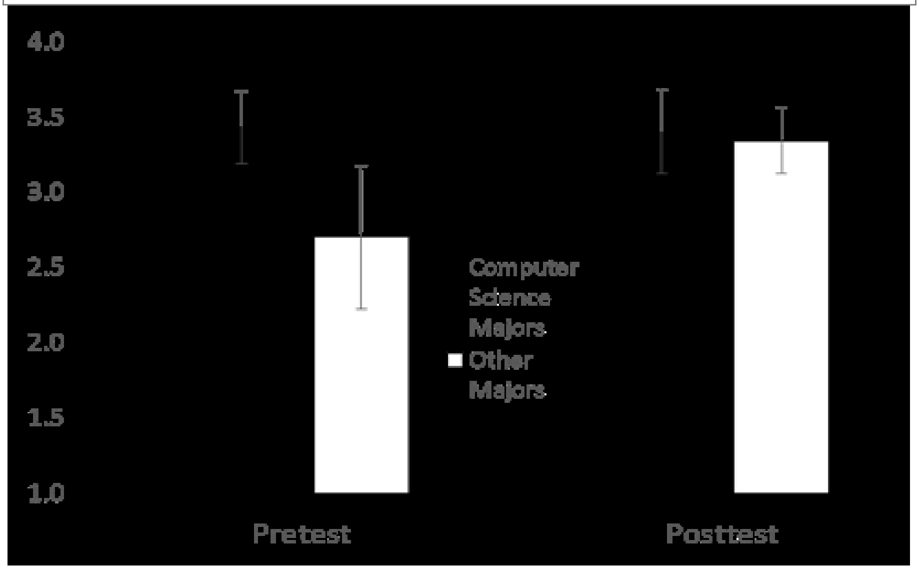

Figure 1. Mean pretest and posttest scores on all 20 items of the Cybersecurity Awareness Survey (CAS) for participants who are Computer Science majors and participants who are majoring in other disciplines. The error bars represent 1 ±SD, and the asterisk indicates a significant difference found in CAS pretest scores between Computer Science majors and other participants (p<.05).

5. CONCLUSIONS AND FUTURE WORK

In this project we set out to understand the current level of security awareness among college students and develop a module that will help raise their awareness. Our survey results indicate that the module has been effective particularly among non-Computer Science (CS) majors. It has raised their level of awareness not only for the specific topics that the module addressed but overall in cybersecurity. The pre-test data indicates that CS majors started with a high level of awareness in the first place and the module did not result in a significant change. This may be attributed to the fact that CS students are often more aware and knowledgeable about computer technology and related issues.

We are encouraged by the results of our study and plan to develop more exercises for the module particularly in the areas of smartphone security, online shopping, and privacy issues in social media. We also plan to collect more diversified data with respect to age and gender. In addition to more students we plan to include the faculty and staff on our campus as users in our study.

REFERENCES

[1] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 236-247.

[2] Adams, R. (2015). Cyber Review – Cybergeddon? Military Technology, 39(11), 67-69.

[3] Aurigemma S, Panko R (2012). A composite framework for behavioral compliance with information security policies. Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS). pp. 3248–3257.

[4] CSI (2007). Computer crime and security survey 2007. Computer Security Institute, retrieved April 1,2016 from http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

[5] Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. Information Technology for Development, 20(2), 96-121.

[6] DiFilipo, S. (2013). The Policy of BYOD: Considerations for Higher Education. EDUCAUSE, retrieved April 14, 2016 from http://er.educause.edu/articles/2013/4/the-policy-of-byod-considerations-for-higher-education

[7] Franke, U. & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. Computers & Security, 46, 18-31.

[8] García-Rodicio, H. (2015). Questioning as an Instructional Strategy in Multimedia Environments: Does Having to Answer Make a Difference? Journal of Educational Computing Research, 52(3), 365-380.

[9] Hern, A. (2016). As easy as 123456: the 25 worst passwords revealed. The Guardian, retrieved April 14, 2016 from https://www.theguardian.com/technology/2016/jan/20/123456-worst-passwords-revealed

[10] Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. Information Security Journal: A Global Perspective, 22(4), 171-179.

[11] Ludwig, K. (2003). Security Awareness: Preventing a Lack in Security Consciousness, GIAC, retrieved April 14, 2016 from https://www.giac.org/paper/gsec/792/security-awareness-preventing-lack-security-consciousness/101700

[12] Manke, S. &Winkler, I. (2013). The Habits of Highly Successful Security Awareness Programs: A Cross-Company Comparison. Securementem, retrieved April 12, 2016 from http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf

[13] 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

[14] Newman, J. (Dec, 2015). The Target credit card breach: What you should know. TIME.com. Retrieved April 5, 2016 from http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/

[15] Power, R., & Forte, D. (2006). Case study: A bold new approach to awareness and education, and how it met an ignoble fate. Computer Fraud & Security, 7-10.

[16] Tozzi, C. (2016). Are Weak Passwords the Biggest Threat to Data Security and Privacy? The Var Guy, retrieved April 11,2016 from http://thevarguy.com/secure-cloud-data-storage-news-and-information/are-weak-passwords-biggest-threat-data-security-and-p

[17] Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. Information Security Journal: A Global Perspective, 17, 207-227.

[18] Vacca, W. A. (2012). Military Culture and Cyber Security. Survival (00396338), 53(6), 159-176. doi:10.1080/00396338.2011.636520

[19] Verizon (2015). 2015 Data Breach Investigation Report. Verizon, retrieved April 14, 2016 from http://www.verizonenterprise.com/DBIR/2015/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2015

[20] Zetter, K. (2016). Why hospitals Are the Perfect Targets for Ransomware. Wired, retrieved April 14, 2016 from http://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/