INTERNET SECURITY AND PRIVACY THREATS, AS PERCEIVED BY AMERICAN AND INTERNATIONAL BUSINESS STUDENTS

James Frost, Idaho State University
Alan Hamlin, Southern Utah University

ABSTRACT

The authors collected responses from American and International business students concerning their attitudes towards internet security and privacy. The students answered questions about password usage, their knowledge of online scams, their conduct while participating in e-Commerce, social media issues, cell phone security, and their awareness and/or training about personal identifiable information. The responses indicate a lack of basic understanding about internet security, and steps to acquire a background or knowledge base in these key areas to protect themselves from external threats. This was especially evident with their use of social media.

We compared the responses to multiple questions about security issues for American and non-American (international) students. Usually, both groups had similar response in their understanding of critical issues, except in a few areas. We believe, based on the data, that security and privacy awareness and training are not being emphasized enough for business students (and probably all students) in academia.

***Keywords**: MSR model, privacy, security, passwords, social media, personally identifiable information (PII), training, education, awareness, network centric.*

INTRODUCTION

Over the past several years, the authors have collected information from business students attending both domestic and foreign colleges and universities about their respective attitudes about the dangers to personal privacy and security from various technologies. This paper provides an analysis of a survey given to 259 students in 34 nations about their perceptions of risk to their personal security and information from internet predators, hackers, and other technology-driven sources, and what they are personally doing (or not doing) to minimize or eliminate such risks . Comparisons of the responses from domestic and foreign students illustrate the relative differences of the groups regarding perceptions of the significance of the problem, and what tools each are using (including such things as the use of special characters in passwords, the length and variation of passwords, the likelihood of opening an attachment to an email from an unknown source, etc.). It is hoped that, with the results of this paper, faculty and administrators who are involved in teaching and advising such students will be provided helpful information regarding cultural differences which might affect how their students can be trained and protected from risks, particularly online risks, to which they are exposed daily from their use of high-tech products.

This paper is organized into four parts. The first describes why the problem of internet security is important, examining the extent of the problem and describing approaches to control it.

The second is a review of the literature. The third is an analysis of our primary research and the tool used to conduct it. The last section provides concluding remarks based on the research, and assesses the implications for further study in the field.

WHY THIS PROBLEM IS IMPORTANT

While the root cause of personal information risk is the subject of much debate, anecdotal evidence suggests multiple factors, including the lack of rigorous law enforcement; lack of consistent ethics training across cultures; peer pressure for increased monetary gain, and changing societal norms about what specifically constitutes unethical behavior. There is evidence that hacking itself is only a minor threat, and that negligent insiders, outsourced data, malicious insiders and social engineering are actually the most serious threats to our personal information security. Even still, the amount of data loss to hacking is staggering. From Edward Snowden hacking government records to recent hostile actions involving political parties and even religious groups, the problem of keeping records safe seems to grow each year. There have been many recent examples of predators from countries like China and Russia successfully accessing private consumer data from major domestic and foreign companies, including JP Morgan Chase Bank, Target and many other firms, accessing the private records of millions of Americans (Riley & Robertson, 2014). Home Depot was recently attacked by cyber-terrorists, who accessed as many as 40 million payment cards (Reuters, 2014). A hacker collective from Germany broke into the servers of 300 banks, corporations and governments for 12 years, stealing sensitive and confidential personal data without being caught (Sky News, 2014).

In their zeal to gain access to private records, even health care service companies are being attacked. Two years ago, the Utah Department of Health server was breached, allegedly by Eastern European predators, and 780,000 individuals were impacted (McNeil, 2014). In June, 2014 the Montana Health Department confirmed a server breach impacting up to 1.3 million individuals (ibid). In July 2014 the State of Vermont confirmed that a server used in the state's health insurance exchange was attacked by Romanians over 15 times (ibid). In March 2014 Chinese hackers broke into the computer networks of the US government and gained access to personal information on US government employees who had applied for top-secret security clearances (Schmidt, Sanger & Perlroth, 2014).

No matter the source of the threat, the risk in total to the safety and security of personal information is substantial, especially to young students who may not be aware of the significance of the problem. Many do not realize that these predators hijack usernames and passwords; steal money from bank and credit card accounts; ruin credit; request new credit cards; make purchases, add themselves or an alias as an authorized user to the victim's credit; obtain cash advances, use and abuse the victim's Social Security number; and sell information to others (Webroot, 2014). Predators use various methods to access personal data, including footprinting, scanning, enumeration, penetration, advance and cover tracks, etc. (Encyclopedia.com, 2002).

This paper will illustrate student perceptions of this very current and significant issue, and what they can and should do to minimize the threat to their personal information and security.

REVIEW OF THE LITERATURE

It was noted that "most social media platforms are used by college students not only for social interactions or entertainment purposes, but also for information seeking in the academic context (Kim, Sin, & He, 2013)." Social media use expanded with the reduction of monthly cost for smartphones and their expanded use with the marketing of unlimited minutes, texting and internet access. This also provided access to social media by users throughout the world. This has expanded to photo sharing through services like Flickr. Researchers found that users were somewhat unconcerned for the potential exposure via photo sharing and posting (Ahern, Eckles, Good, King, Naaman & Nair, 2007). However they also acknowledge that tremendous risks are also involved with posting of pictures.

Multiple ages of students are using social media. Rivero (2013) reported that 75% of seventh through twelfth graders have at least one social media profile. It is safe to assume that most college students use social media in one form or another. Many of the studies focus on the educational potential of social media (Educational Information Technology, 2011) and the cultural issues of social media in education (Ahn, 2011). Our study did not dwell on the impact of social media in education; instead we investigated the attitudes of students when using social media and their personal information. When considering virtual worlds and social media; researchers identified the importance of the security triad of confidentiality, integrity and availability (Gogolin, Gogolin & Kam, 2014). While there is some data that is appropriate to keep completely confidential, it is critical to maintain the integrity of all data. In the end, it is up to each individual to determine the level of availability of data to other individuals (for example, their close friends, friends of their friends, or the general public).

Social engineering refers to the "selection of techniques that exploit human weaknesses and manipulate people into breaking normal security procedures" and engineering as a preferred method to bypass computer and physical security over technical controls (Bakhshi, Papadaki & Furnell, 2008)." Many of the techniques used by social engineers can be diminished by awareness and training efforts of the corporation. In two studies, social engineering is even effective on individuals participating in cyber competitions who think they cannot be affected by such actions (Kvedar, Nettis & Fulton, 2010). These researchers found strong success by using a well planned and executed event. Social engineering requires information gathering to be successful and social media sites are packed with personally identifiable information (PII). If social engineering works on individuals that are trained to avoid seductive requests, it is understandable that novices would fall to the influences of well-prepared social engineers.

In one experiment, one fourth of the staff fell to the lure of social engineering attacks (Bakhshi, Papadaki & Furnell, 2008). As it is natural to wish to assist and when provided with authentic appearing credentials, it is understandable why social engineering of social media attacks are successful. To deal with the vulnerabilities posed by social media it is prudent to provide training, education and awareness. The importance of awareness, training and education is emphasized in several articles including McCallister, Grance & Scarfone, (2010) and McCumber, (2004).

ANALYSIS OF PRIMARY RESEARCH

Data Analysis

Data was collected from multiple international business classes over the past two years. Two hundred fifty nine students participated in a multi-question survey to identify their personal actions towards different issues involving information assurance and privacy. These students were international undergraduate students from across the world, who enrolled in a business class taught by an American at various universities in Europe. The survey was conducted in hard copy with the students circling their selected choices and writing responses to the open question that dealt with their personal attitude/view of information assurance issues. We chose to use hard copies as some of the students did not have access to computers to enter responses on-line and the motivation to complete the survey would have been reduced if not done during class time. The surveys were entered into an Excel worksheet and reviewed for accuracy. This involved hand checking each entry for accuracy combined with a computer analysis for error checking. We did not collect gender information since identifying the gender, when combined with other variables, can reduce the response rate. The statistics package JMP Pro 12 was also used.

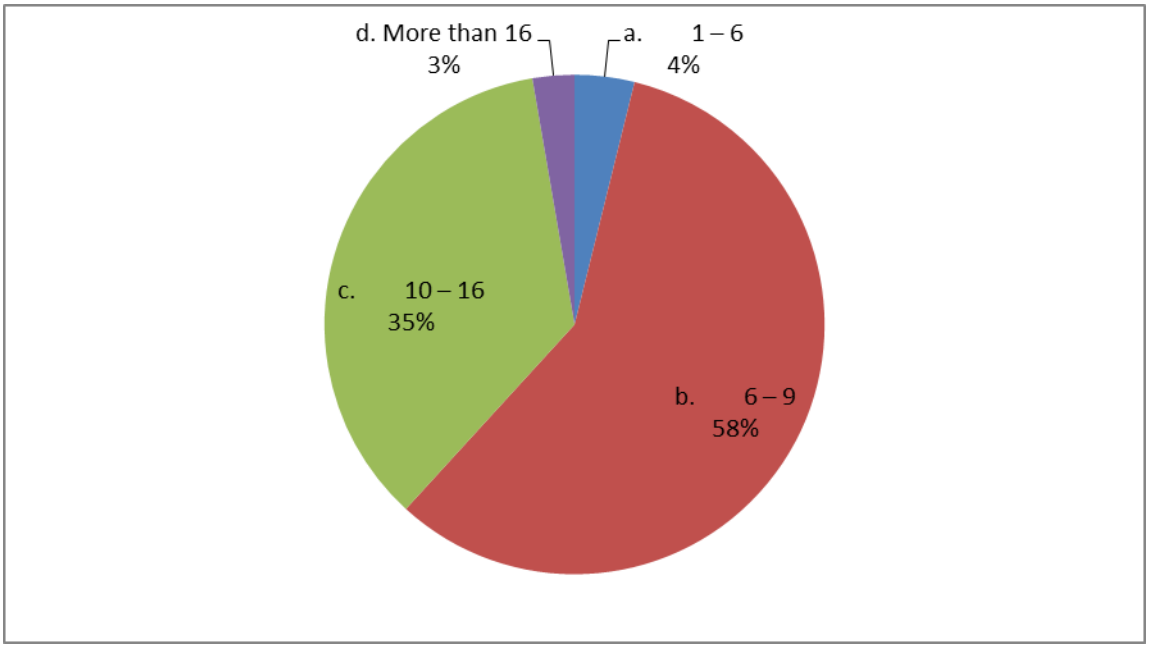
Table 1
Number of American vs. International Students

American	122
International	136

The students' majors were quite varied, especially beyond the "traditional" business categories. Approximately half of all the students (135) were "traditional" business majors of management, marketing, accounting, and CIS while the rest showed a variety of interests.

When asked about the student's preferences for password length for computer accounts ("Usually my passwords are at least _____ characters in length"), the students responded as shown in Figure 1 below:

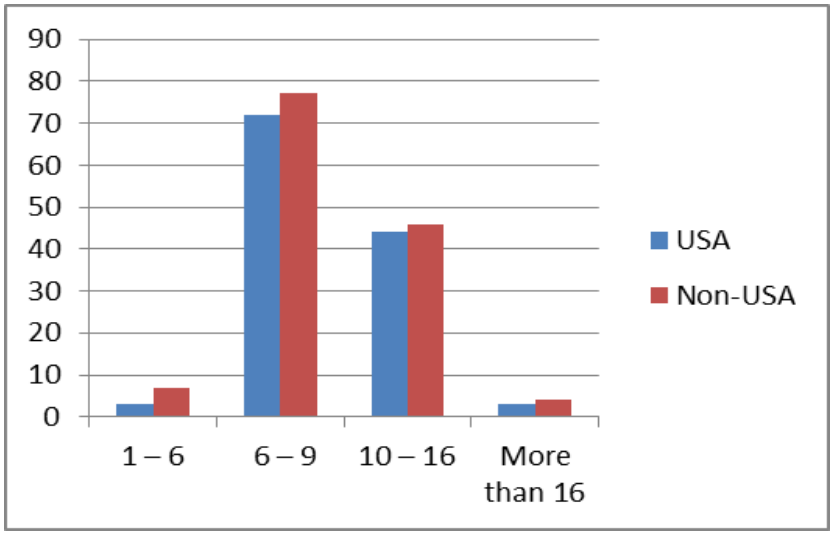
Figure 1: Length of Password



Password length is a positive information assurance activity as length is a critical aspect in maintaining computer security. The majority of the students are using passwords that are six characters or longer. Over one-third are using passwords of ten or more characters. Only four percent of the students report using passwords that are less than six characters. The password lengths may be affected by minimum requirements for "n" characters of the security system. When comparing international students, there did not seem to be a vast difference in the groupings of password lengths. The bar chart of figure 2 displays a continuum of values without any groupings of observations in any area for either group.

However, even though password length contributes to the information assurance posture of an individual, it is more important to be able to remember the password. The inclusion of cryptic characters to confuse the hacker that is attempting to "crack" your password is not a major advantage to the student. Many professionals still portray that a password is "stronger" with the inclusion of special character, number and uppercase letters. However, special characters are just another character that is difficult for the human to remember which numbers and/or special characters are substituted for the alphabet. It is important for users to remember that the computer is a tireless worker and can crack any password, given enough time. Therefore, it is important to maintain usability with length over cryptic numbers and/or symbols using difficult to remember special characters.

Figure 2: American v. International Password Lengths



As an example, suppose we use a passphrase like: horsepucky with some substitutions and symbols. It could become "#or3e9ucky14." It would only ONE DAY for a brute force attack to crack this password (https://passfault.appspot.com/password_strength.html#menu).

Using a password that a user can remember, "baseballworldseriesyogiberra" we see the subsequent time to crack – 2,374,525,075 centuries.

Many sources and sites verify the benefits of having longer passwords, and the time it takes for hackers to crack them. Some of these also show the expansion of time required to crack a longer password. Table 2 gives information from another password cracking site that shows similar times to crack (Gibson Research: https://www.grc.com/haystack.htm).

Table 2
Time Required to Crack a Specific Password

Type of attack	Time involved
Online Attack Scenario: (Assuming one thousand guesses per second)	3.76 billion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	37.58 centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	3.76 years

The authors support a philosophy that it is a superior technique to use a password that is long, yet retrievable and easier to memorize, instead of a difficult and shorter password. Often computer

users believe that a hacker will poke at the website with a hacking tool until they succeed in discovering your password. This is not the case. The hacker will download the password file after compromising the site and then run the tool on the file at his location so safeguards to prevent multiple attempts are not present. Password length is critically important for information assurance.

When queried as to the inclusion of special characters in my password(s) like *, &, ~; only 30% of the students responded yes (Figure 2). We feel safe in assuming that the exclusion is for simplicity in typing in a password. That observed, nearly one third are including special and obscure characters, probably because they believe that these unique characters will make the password more secure from hackers.

When we look at a breakout between the Ameican students and international students, there does not appear to be a dramatic difference in the use of special characters (Figure 3).

Figure 3: Percentage of students using "special" characters

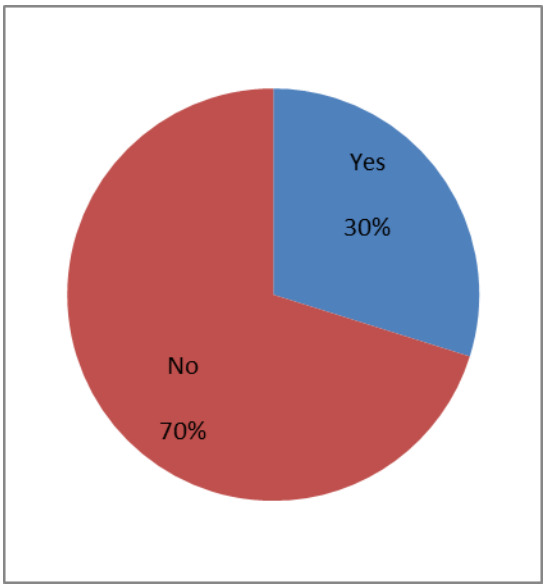
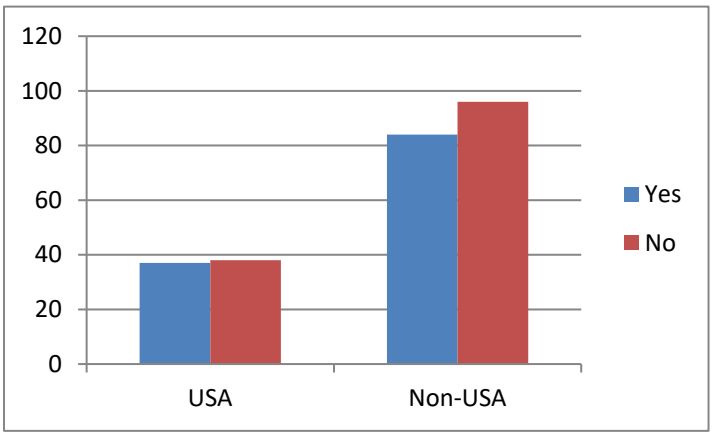


Figure 4 shows the same data however it is divided into American versus international students. There does not appear to be a dramatic difference between these two groups for the use of special characters.

Figure 4: Use of special characters



Do the students have multiple passwords or just one password for all their on-line accounts? Table 3 shows (sorted by percentage of total descending):

Table 2
Number of passwords for each student

# of Passwords	Percent of total
3	32.56%
4	19.38%
2	13.95%
5	10.47%
6	4.65%
1	2.71%
10	2.71%
7	1.55%
8	1.16%
12	0.78%
0	0.78%
9	0.78%
13	0.39%
15	0.39%
30	0.39%

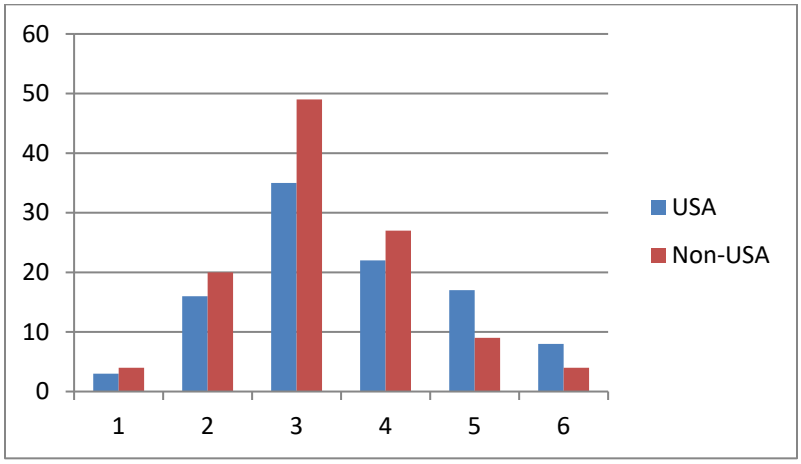
Seventy one percent of the students responding to the survey have four or less passwords for their accounts that are online. Nearly one-third had three passwords for their online accounts and the less than six percent have ten or more passwords for their online accounts. This is a potential security issue because if one of their passwords is compromised, then the hacker would have access to other accounts. This is a target of phishing attacks and "requirements" to establish

a login for something "free." The hacker is hoping that the user has a limited number of passwords and the subject will use one of them to establish an account on their system. Then they can social engineer other sites to access your online resources. A superior posture for the student is to have independent, long passwords for each web site and do not reuse your passwords.

Keeping track of more than ten passwords can be troublesome; however there are strong and reliable password management systems that are available at low or no cost. These systems keep your passwords under a single password that can be very long and the system can be on your local machine or it can reside in the cloud. Most of the password management systems also offer a mobile version for smartphones as well. It is important to avoid having one/few passwords for critical accounts as if one account is compromised; the user does not want all of their online accounts vulnerable.

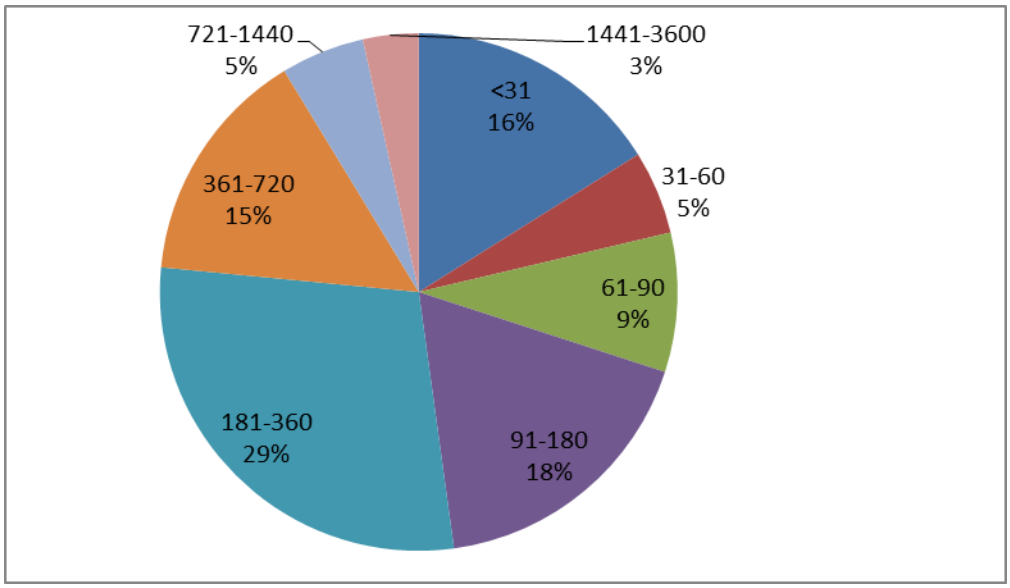
There does not seem to be a difference between the two groups of this study as shown in Figure 5. Each bar represents the number of passwords the students uses (passwords 1 – 6) and represents 85% of the students.

Figure 5: Use of multiple passwords



A follow-up question involved the issue of how often the student changes their password. As expected, the students reported that they do not change their passwords very often. Figure 6 shows that 23% of the students wait to change their password on an annual basis or longer (up to every three years). Another 29% change their passwords every six months to one year. The students report that they change their passwords no sooner than six months to as much as three years.

Figure 6: Time elapsed before student changes their password (in days)



It is important for computer users to change passwords more often than annually as hackers often do not immediately use a compromised password. They may wait and see if the user has changed their password as time passes. They will also create a supervisor account for themselves to use later.

Figure 7 shows a noticeable difference with two responses. More international students respond that they never change their password (zero) or wait to change their password annually (360). We do not have an explanation for this response rate, however the international students seem more reluctant to change their passwords.

Figure 7: Days until password is changed

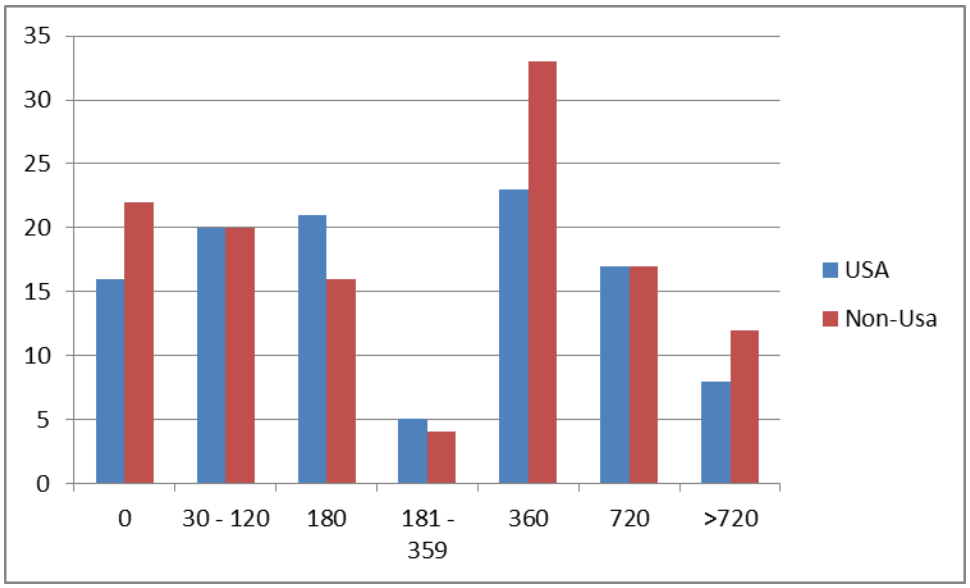
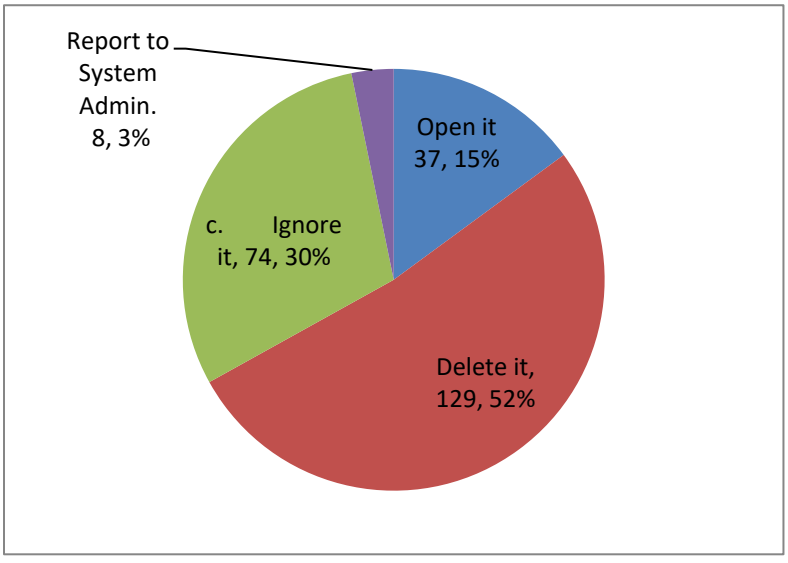


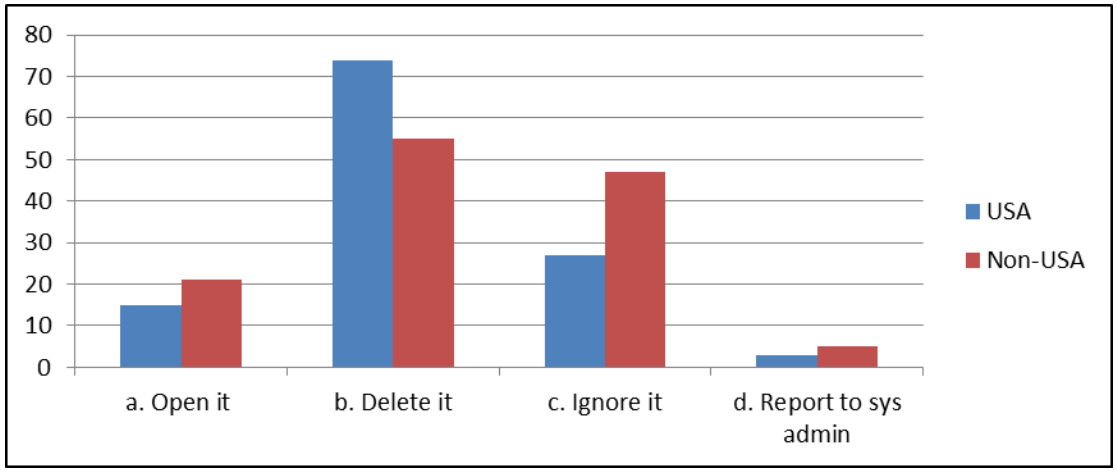
Figure 8 shows the student responses to a query on what to do if an email has an attachment. Half of the students indicate that they would delete it; however, a disturbing number of the students say they would open an attached executable file. Usually it is advisable to leave any attached executable alone and not open it as this would possibly launch malware that would compromise their system.

Figure 8: Action for an executable file attached to an email



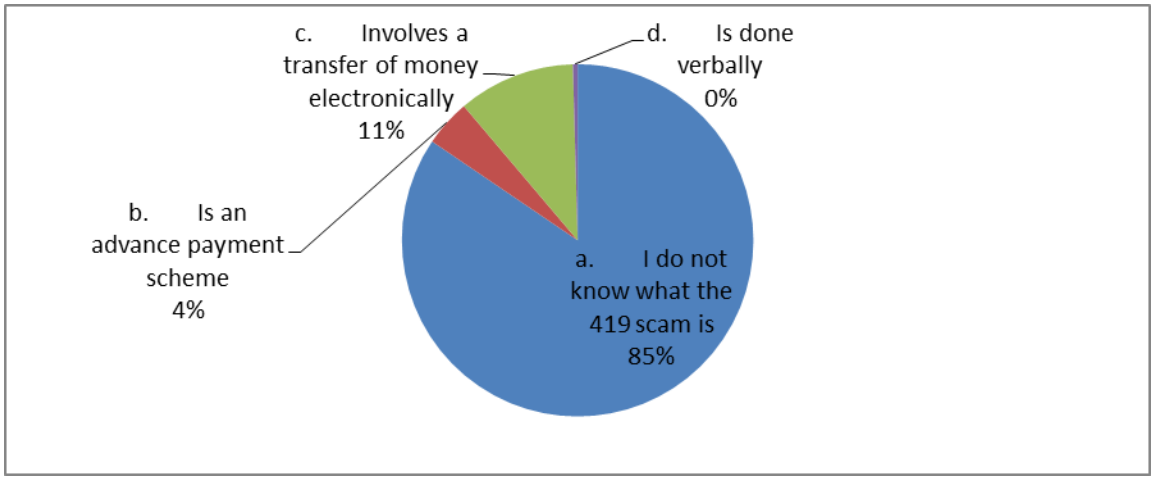
When comparing the American students to the international contingent, there are a couple of differences when dealing with an attached executable (Figure 9). Comparatively, more American students would delete it while more international students would ignore it. However, not many of either cohort would report it to a network supervisor.

Figure 8: Comparison of responses on an attached executable file



The next survey question dealt with the student's knowledge of a specific, yet famous scam, the Nigerian 419 (Advanced Payment) scheme. Figure 10 queries their knowledge of this scam. Eighty five percent of both American and international students did not know what this program was and how it could affect them. This advanced payment scheme (known by the 419 criminal code in Nigeria) is a powerful "get rich quick scheme" that has taken cash from many internet and non-internet users. Internet users and individuals should be aware of the dangers of this and other criminal vehicles that are just too good to be true.

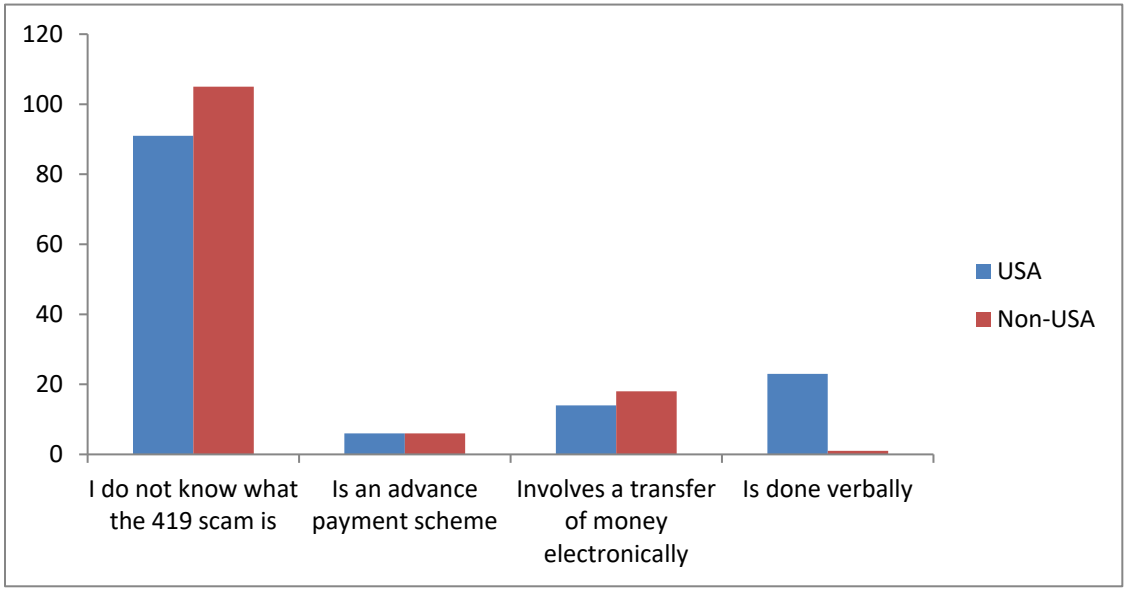
Figure 9: Student knowledge of Nigerian 419 scheme



As a society we are becoming net-centric in our activities. We stream movies via Netflix, purchase commercial goods via Amazon.com and we roam through the flea market of eBay with little concern for our personal security. We conduct online banking and monitor the stock market via online connections. As students participate in online activities, which of their actions could expand vulnerabilities?

There is not much difference between the American students and international students as shown in Figure 11. An exception is on the question of the Nigerian scheme being done verbally. The American students supported this concept, possibly guessing.

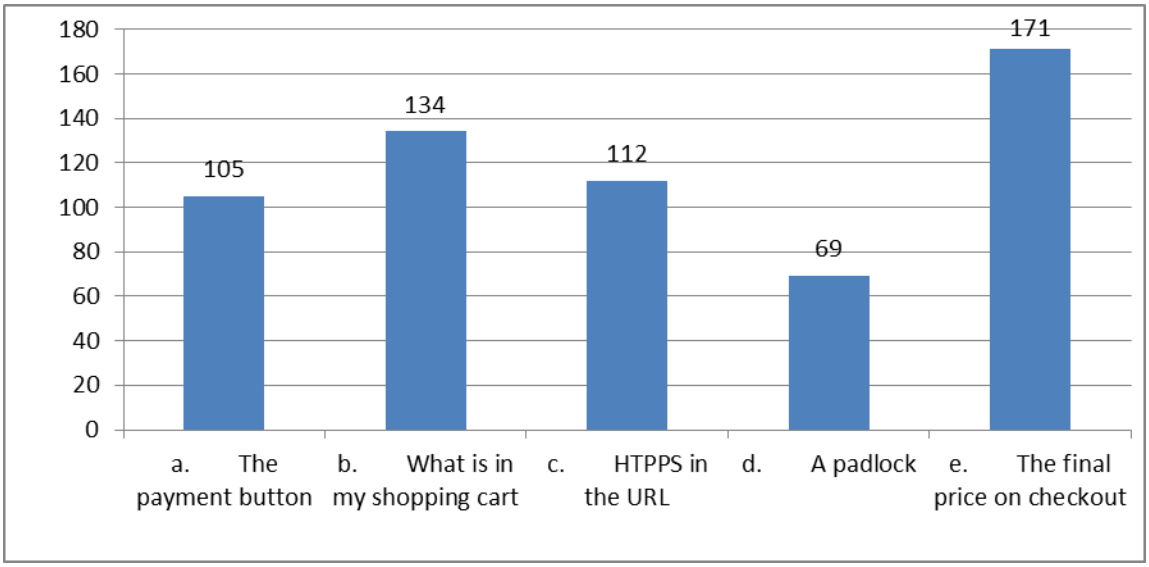
Figure 10: Nigerian Scam



Although one third of the students are "very to extremely concerned" about their social media web site, only 25% felt it was "likely to extremely likely" that their site would be hacked.

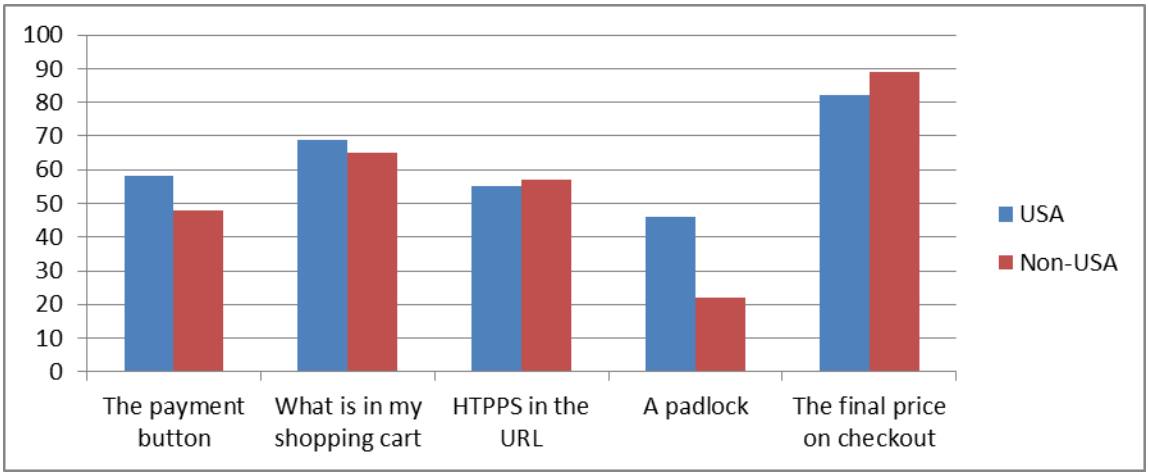
Figure 12 shows that nearly one fourth of the students check on what is in their shopping cart when they purchase an item online. The international students are more concerned about the final price and where the payment button is, rather than if the transaction is secure as indicated by a padlock or htpps in the url.

Figure 11: Things monitored when participating in e-Commerce



When comparing American students to the international students (Figure 13), the most dramatic difference is that fewer international students look for a padlock. Perhaps this is a unique word in their understanding of the English language.

Figure 12: American v. International things monitored in e-Commerce



This is a security concern as half of the students are looking at the price and what is in the shopping cart, not if they are at a secure site. It is imperative to raise the awareness of students when they are involved in e-Commerce. The students were allowed multiple selections on this question. The international students primarily selected the final price on checkout. This is interesting as we rarely find it in error in the price as a computer is calculating the price based on

the buyer's choices. The second most selected item is what is in their shopping cart. The choice of finding the payment and checking for a HTPPS in the URL could be a security issue.

The students' privacy concern at a social media site is interesting. Here is a visible difference between the American students and the international set. The international students are very concerned about the security of their social media web site while the USA students indicate less concern as shown in figure 14.

Figure 13: Social media site security

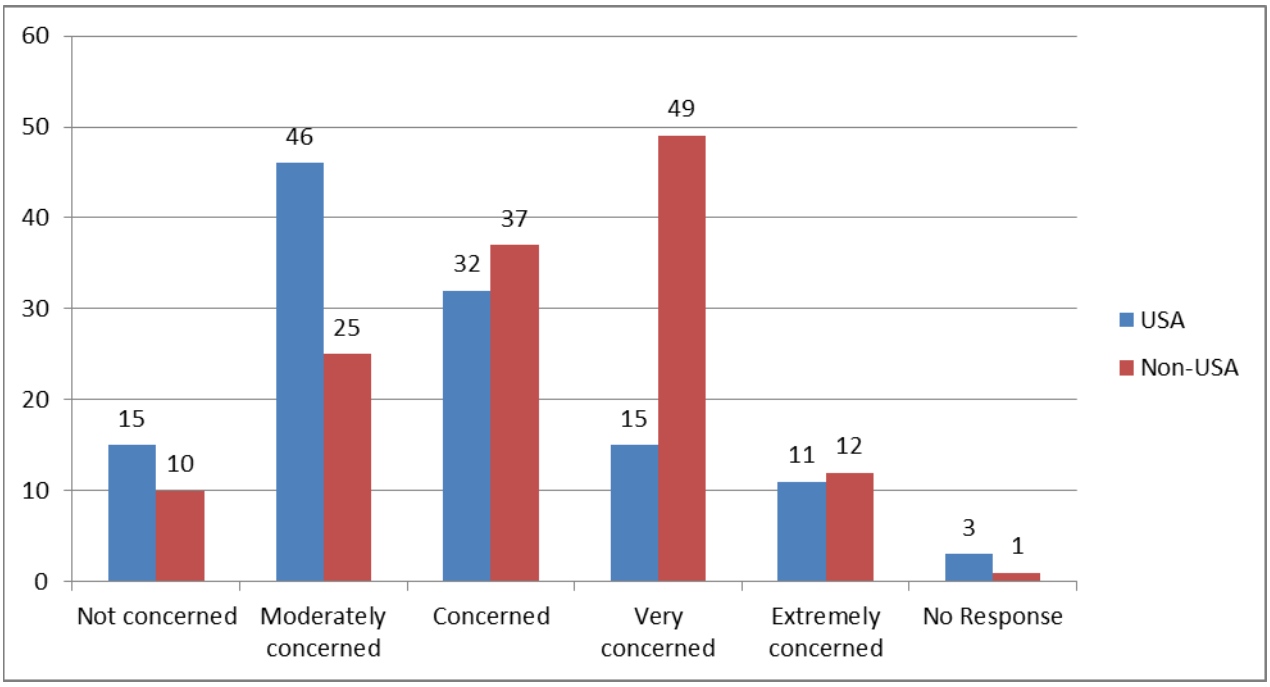
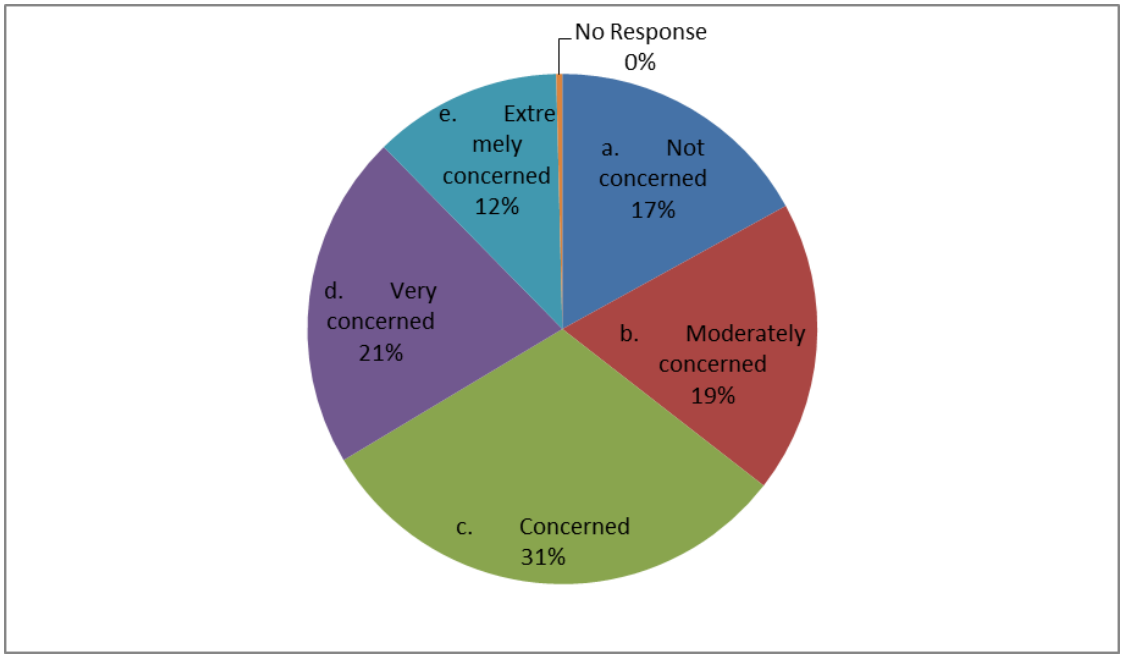


Figure 15 looks further at the student's concern for privacy when using Google. This is a security problem as government agencies are challenged when using facial recognition; however it is not un-Constitutional for a non-government agency to perform facial recognition. A corporation with the resources of Google may have more influence than many governmental agencies. If the populace does not raise a concern about this type of illegal search of a person, it will probably continue unabated.

Figure 14: Students selecting concerns the issue of facial recognition at Google



Again, the international students show more concern for their privacy at social media sites. Figure 16 shows the American students less concerned over facial recognition at these sites.

Figure 15: - Use of facial recognition at social media site

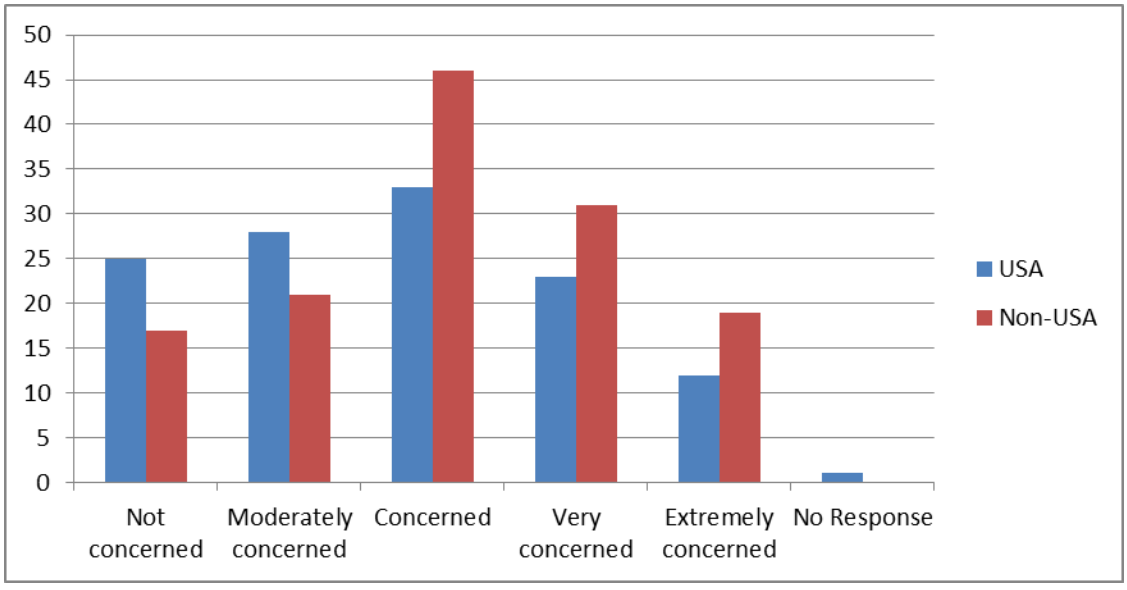
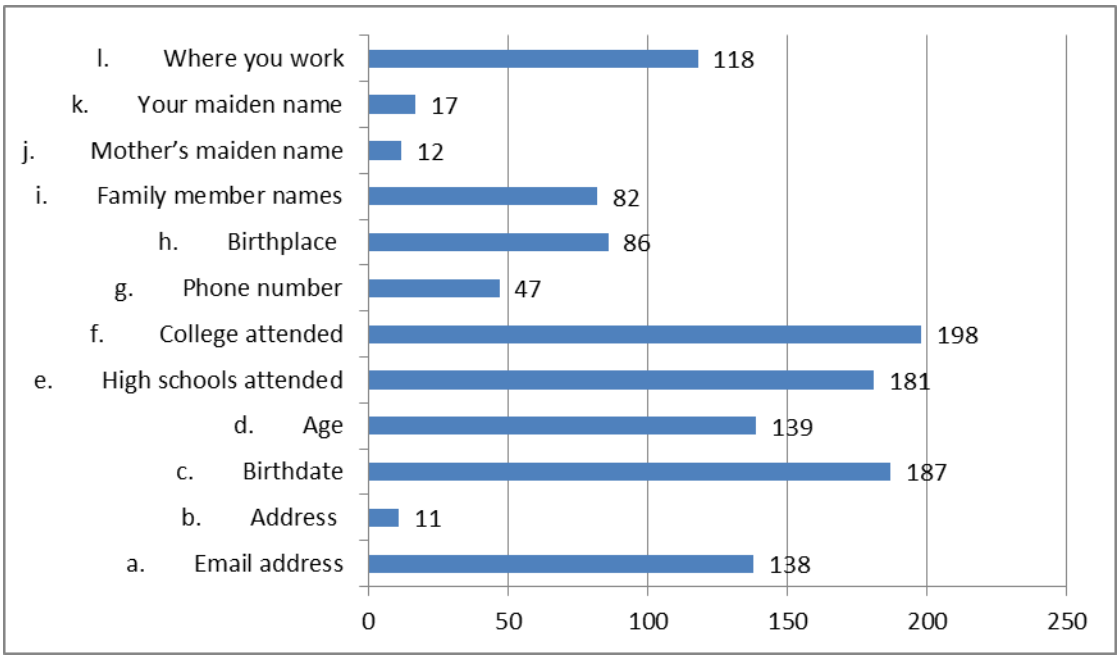


Figure 17 shows what personally identifiable information (PII) students are including in their social media sites. Students appear to be including a large amount of personal information about themselves on their social media sites.

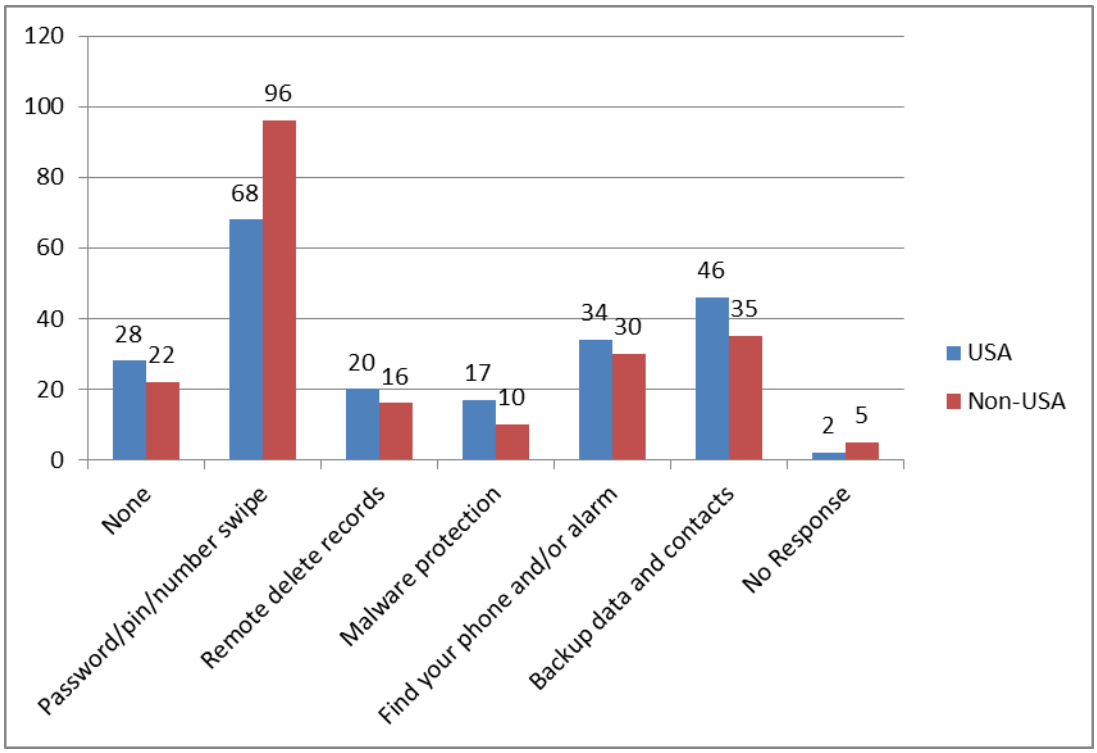
Figure 16: Social media web site information



The inclusion of birthdate and birthplace as well as family member names should be avoided. In addition, the inclusion of their maiden name and mother's maiden name on a web site must be avoided. Individuals enjoy creating a history for others to pursue; however, this is a gold mine for social engineers, thieves and hackers. It is time to raise the awareness of our students on this issue. When looking at a comparison of American and international students, comparatively more international students included their e-mail address, birthdate and birthplace. More American students included family member names at their social media site.

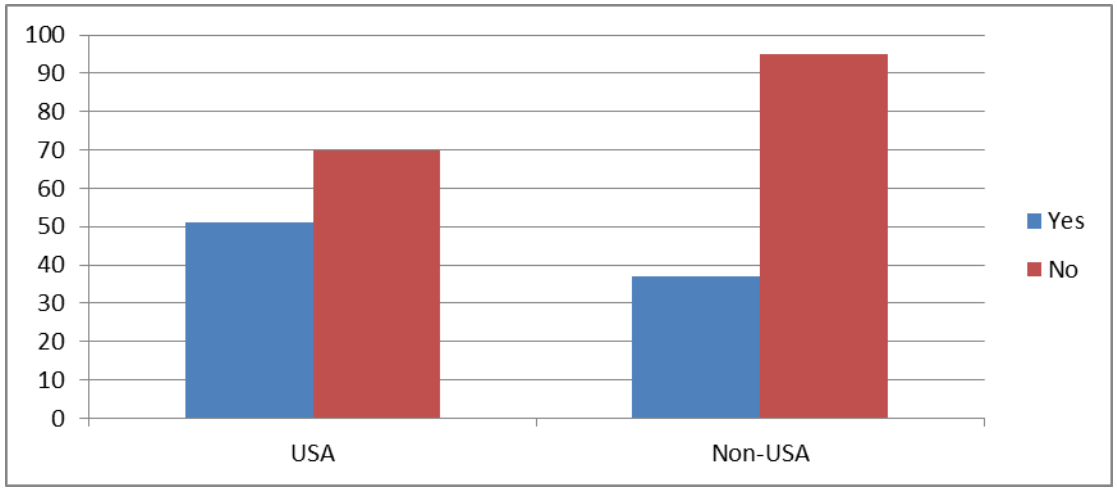
When questioned about security measures, 164 reported that they do use a password/pin/security swipe to limit access to their device (Figure 18). This is comforting; however only 25 have malware protection. Also, it appears that more international students adopt password/pin/swipe protection than there American counterparts. The students have a powerful, network-centric device in their hand and many are conducting mobile commerce and banking regularly. They need a stronger defense to protect this access node. It is interesting that 79% of these students report they have malware protection on their personal computer, yet far fewer have the corollary for their cell phone.

Figure 17: Cell phone security



These responses are not surprising as only 35% have had training on internet privacy issues and/or protection for your personal information. The comparison of American and international students (Figure 19) shows the international students trailing in this exposure issue. This is a rapidly developing field and the students are involved daily and are actively exposing their PII to all individuals and corporations. The basics of computer security should be included in several classes and more network-centric security classes should be offered.

Figure 18: PII Training



CONCLUSIONS AND RECOMMENDATIONS

We consider it imperative that any individual that participates in activities on the internet enhance their knowledge (through training, education and awareness) of the risks and countermeasures to protect their identities and assets. This needs to be an international issue for awareness and training, especially for students who are young and vulnerable. We are taught in kindergarten to not trust a stranger; however, we practice a different set of standards for the internet. Some may feel insulated from the effects of thieves and hackers because they are conducting the transaction in a virtual world. It is time for all to realize that the risks are large and we continually add new vulnerabilities with each of our most recent virtual interfaces and tools.

There is a need to embrace strong (i.e. long) passwords that are not necessarily cryptic as it is important that humans can remember them. Individuals using social media should use caution to not put any data on the web that could be embarrassing or used to assume their personality. It is also important to always be diligent in protecting our PII.

Students are generally deeply involved in social media, and often do not realize the risks to their PII and assets. They need to adopt countermeasures such as the McCumber cube (McCumber, 2004) and also consider expanding protection as in the Maconachy/Schou/Ragsdale (MSR) model (Maconachy, Schou, Ragsdale & Welch, 2001). They must use more enhanced security technologies including long passwords; locking devices when not in active use; checking for encrypted transmissions (https); and use of anti-virus software. Also, they should expand their education and training by study and classes in information assurance. The use of a password manager will assist in providing a vault for numerous and/or complex passwords.

The authors plan to mature this survey with specific changes to focus on the changing environment. We would like more follow-up questions on data included at social media sites and their information assurance awareness. Information assurance is a personal issue and requires diligence from the individual. This attitude must be encouraged and supported at multiple levels to provide a positive experience in our network-centric world.

REFERENCES

Ahern, S., Eckles, D., Good, N., King, S., Naaman, M., & Nair, R. (2007). Over-exposed? Privacy patterns and considerations in online and mobile photo sharing. *Human Computer Interface*, 1 -10.

Ahn, J. (2011). Digital divides and social network sites: Which students participate in social media? *Educational Computing Research,* 147-163.

Bakhshi, T., Papadaki, M., & Furnell, S. M. (2008). A practical assessment of social engineering. *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance.*

Educational Information Technology (2011). How are campus students using social media to support their studies?

Encyclopedia.com. (2002). *Hacking*. Retrieved September 15, 2014, from Encyclopedia.com : http://www.encyclopedia.com/topic/Hacking.aspx

Gogolin, G., Gogolin, E., & Kam, H.-J. (2014). Virtual worlds and social media: Security and privacy concerns, implications, and practices. *International Journal of Artificial Life Research*, 30-42.

Kim, K.S., Sin, S.C., & He, Y. (2013). Information seeking through social media: Impact of user characteristics on social media use. *Proceedings of the Association for Information Science and Technology.*

Kvedar, D., Nettis, M., & Fulton, S. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. *Journal of Computing Sciences in Colleges*, 80-87.

Maconachy, W., Schou, C. D., Ragsdale , D., & Welch , D. (2001, June 5 & 6). *A Model for Information Assurance:An Integrated Approach.* Retrieved September 22, 2014, from BYU Lectures: http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf.

McCallister, E., Grance, T., & Scarfone, K. (2010). *NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* Gaithersburg: National Institute of Standards and Technology.

McCumber, J. (2004). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology* . Auerbach Publications.

McNeil, A. (2014). Why hackers are targeting health data. Retrieved July 7, 2014, from *Data Breach Today*: http://www.databreachtoday.com/hackers-are-targeting-health-data-a-7024

Riley, M., & Robertson, J. (2014, August 27). FBI examining whether Russia is tied to JPMorgan hacking. Retrieved August 27, 2014, from *Bloomburg Tech*: http://www.bloomberg.com/news/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking.html

Reuters. (2014, September 9). States probe Home Depot breach; Senators seek FTC inquiry. Retrieved September 11, 2014, from *Moneynews*: http://www.moneynews.com/Economy/States-Home-Depot-Breach/2014/09/09/id/593647/

Rivero, V. (2013, December). What's new in the social media sphere. Retrieved September 5, 2014, from *Tools for Learning:* www.internetatschools.com

Schmidt, M., Sanger, D., & Perlroth, N. (2014, July 9). Chinese hackers pursue key data on US workers. *New York Times*.

Sky News, H. (2014, September 17). Hackers 'swooped' on biological warfare study. Retrieved September 17, 2014, from *SkyNews:* http://news.sky.com/story/1337337/hackers-swooped-on-biological-warfare-study

WEBROOT. (2014). Computer hackers and predators. Retrieved July 9, 2014, from *WEBROOT:* http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-hackers