Do Students and Instructors See Cybersecurity the Same? A Comparison of Perceptions About Selected Cybersecurity Topics

Mark Ciampa, Ray Blankenship
Western Kentucky University
USA

Abstract

Cybersecurity attacks continue to increase. This is particularly true for attacks based on social engineering or relying on the weaknesses of individuals as a means of gathering information or crafting an attack. Along with an increase in attacks there is likewise an increase in the number of calls for educating users about attacks and equipping them with the knowledge and skills for warding off attacks. Many entities advocate that institutions of higher education should be responsible for providing practical, applied security awareness instruction. This study compared student and instructor attitudes towards security to determine if there is an apathy on the part of students regarding security or if they are concerned about selected security topics, and if instructors perceive that practical, applied security instruction is a necessary component to their courses, or if security instruction belongs elsewhere. The relationship of student attitudes towards security was compared with those of instructors over six current security topics. When comparing students to instructors to students there was no significant difference between them on the topics of using anti-virus software, using a firewall, securing wireless networks, and using spam filters. The results seem to indicate that there is a significant difference between the perceptions of students and instructors regarding the security topics of protection from phishing and how to create a strong password.

Keywords: cybersecurity; higher education; instructors; students; phishing; passwords

1. Introduction

Cybersecurity attacks have grown to the point that they are dramatically reshaping the lives of users. Virtually all technology devices today, from computers to mobile devices to wearables, must all be first viewed in the context of security. “Locking down” devices so that they are initially secure and continue to remain secure is essential. All user practices must likewise be performed with a keen eye on the security implications: Is downloading this app safe? Can I reply to this email? Should I view this attachment? Cybersecurity has dramatically changed how users interact with all forms of technology.

Just as cybersecurity has changed how users interact with technology, so too has modern cybersecurity changed how these attacks can be thwarted. At one time protecting users and their data was seen as the role of the information technology staff, who would build a secure “fence” made up of an impenetrable local area network that would ward off attackers while keeping internal users safe. This is no longer the case. Defending against attacks has shifted so that a single technology solution is not available. And defending against attacks is the role of every user on a system, from the most tech-savvy to the tech-newbie.

The job of instructing users of the correct cybersecurity defense techniques has unfortunately not found a permanent home. Whose job is it to provide users with the knowledge and skills to prevent attacks? Is it the employer? Is it secondary education? Is it the community at large? Or should users just figure it out for themselves?

One of the entities that is often verbally tasked with cybersecurity training is that of higher education. For many years a loud chorus of voices has advocated that colleges and universities should instruct their students on how to remain secure so that they may practice secure skills at home and on the job.

Yet how do students in colleges and universities view the importance of learning and practicing cybersecurity? And equally important, how to instructors view the importance? Do they see this as their roles? Or should this be something already completed by the time these students set foot on a college campus?

This study examines how students and faculty perceive cybersecurity to determine if they share an equal understanding of its importance. It explores the relationship of student attitudes towards security was compared with those of instructors over six current security topics.

2. Literature Review

The relentless volume of cybersecurity attacks has numbed most users to the latest attacks and required defenses. In just the first six months of 2017 more data was lost or stolen (1.9 billion records) than in the entire year of 2016 (Dean, 2018). That dwarfs the estimated 234,919,393 data records lost or stolen in all of 2015, which, if spread over the entire period, would equate to 56,611 records stolen every hour (Gemalto, 2015). In February 2015 unknown attackers compromised the Bangladesh Central Bank and tried to transfer almost $1 billion. Even though their fraudulent transactions were cancelled—only after a typographic error raised concerns about one of the transactions--nevertheless the attackers managed to transfer $81 million (Bright, 2016). Between 2013 and 2015 attackers gained access to secure information from over 100 financial institutions around the world by using malware to infiltrate the computer systems to harvest personal customer data. By impersonating online staff, the attackers were able to authorize fraudulent transfers, and even ordered automated teller machines (ATMs) to dispense cash without a valid bank card. Estimates of the funds stolen range has high as $920 million (Elson, 2017).

According to the National Security Agency's director of Tailored Access Operations most attacks are not directed at uncovering unknown or "zero day" technical vulnerabilities (Zetter, 2016). Instead, attackers are focusing on tricking users to perform insecure actions. Humans have consistently been found to be the weakest link in the chain of security (Mitnick & Simon, 2001), posing serious risks to enterprises (Ranjeev & Lawless, 2015). Estimates range as high as 95 percent of security incidences are the result of employee insider human error (IBM 2015 Cyber Security Intelligence Index , 2015). Human threats to critical infrastructures and services predominately come from careless work behaviors and ignorance of basic cyber security practices, including irregular software patching, installation of malicious software, careless communication of sensitive information, and connections to insecure Internet networks or Wi-Fi (Gyunka & Christiana, 2017).

These attacks directed at users are typically known as social engineering attacks and rely on the weaknesses of individuals as a means of gathering information or crafting an attack. One of the most common forms of social engineering is phishing. Phishing is sending an email or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information. Users are asked to respond to an email or are directed to a website where they are requested to update personal information, such as passwords, credit card numbers, Social Security numbers, bank account numbers, or other information. However, the email or website is actually an imposter and is set up to steal what information the user enters (Ciampa, 2018).

Phishing attacks continue to increase. In the last three months of 2015 over 14 million new samples of phishing malware were observed (Group, 2016). The average 10,000-employee company spends $3.7 million annually dealing with phishing attacks (Korolov, 2015). The overwhelming number of phishing attacks (77 percent) are directed at targets located in the United States, yet over the past three years the percentage of phishing attacks targeting US companies has only grown 9 percent. However, this is not the result of increased defenses to ward off these phishing attacks. Rather, it is likely because U.S. companies have been so saturated by the phishing market that there is little room for additional growth (Phishlabs, 2016). The most popular attack by phishers at tricking victims to open and respond to a phishing attack is an email that purports to contain an important invoice. Other popular phishing attacks include emails that contain scanned documents sent from office printers or copies, email delivery failure notices, order and payment confirmation messages, and airline flight confirmations (Crowe, 2017).

Because phishing attacks are based on tricking the user through social engineering, it is not possible to defend against phishing through a purely technical solution. One widely implemented strategy that has been used to attempt to minimize successful phishing attacks is to warn users about the threat. Different warning technologies have been proposed.

An early warning technology was a website authentication indicator that used a padlock icon on the toolbar of the web browser. This signaled the presence or absence of a secure sockets layer (SSL) connection between the browser and the web site (Cranor, 2006). However, SSL does not ensure that the website is necessarily trustworthy. This is because certificate authorities issue domain validated certificates to anyone who can demonstrate domain ownership by only receiving emails addressed to that domain name (Jackson, Simon, Tan, & Barth, 2007) and thus does not make any implications regarding the validity of the web site. In response to these weaknesses, the certificate authority industry developed extended validation SSL (EV SSL) certificates. In addition to displaying a padlock, EV SSL also turns the web browser's address bar green and displays the name of the extended validation certificate owner. This indicates that the transaction is encrypted and that the organization has been authenticated according to higher standards.

Another example of warning users of phishing is having the web browser proactively warn users. A yellow button labeled 'Suspicious Website' in the web browser address bar indicates that the user may be viewing a suspected phishing site, while a red status bar indicates the user is visiting a known phishing site (Tulloch, Northrup, & Honeycutt, 2007). The Uniform Resource Locator (URL) the user enters is compared to a blacklist of known phishing sites maintained by the browser's vendor. Wu, Miller and Garfinkel (2006) list five additional vendor-security toolbar indicators, while Dhamija and Tygar (2005) along with others have created their own web browser add-ons that can warn users.

However, these different phishing warning technologies have consistently shown to be marginally effective. Usability studies testing the effectiveness of the SSL padlock by Dhamija, Tygar, and Hearst (2006), Downs et al. (2006), Schechter, Dhamija, Ozment, and Fischer (2007),Whalen and Inkpen (2005), Wu et al. (2006), and others have demonstrated that this standard security indicator is limited in its effect, while usability studies by Jackson et al. (2007) illustrated the ineffectiveness of EV SSL. Dhamija et al. (2006) concludes that “standard security indicators are not effective” (p. 581) while Cranor (2006) states that “a growing body of literature has found the effectiveness of many of these indicators to be rather disappointing” (p. 45).

The ineffectiveness of phishing warnings illustrates a broader issue: users lack both a fundamental knowledge and skill set of applied, practical security awareness as well as a desire to practice security. Bada and Sasse (2015) note that "changing behavior requires more than giving information about risks and correct behaviors--firstly, the people must be able to understand and apply the advice, and secondly, they must be willing to do--and the latter requires changes to attitudes and intentions” (p. 4).

Many researchers highlight the basic understanding of security risks and the application of defenses as important. User education and training is the key to counteract phishing, according to Dhamija, Tygar and Hearst (2006), Downs, Holbrook, and Cranor (2006), Jackson, Simon, Tan and Barth (2007), and Kumaraguru et al. (2007). Information security training and awareness are two of the most effective offsets to mitigate the human risk posed to information security (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Training is emphasized by Long (1999), Mangus (2002), Tobin and Ware (2005), Werner (2005), Witson (2003), and Yang (2001) among others. Observations ranged from a mild statement of “certain user practices contribute to information systems vulnerabilities” (Mangus, 2002, p. 5) to a sharp rebuke of “the average home user is clueless about security and should be required to obtain a license to log on to the internet” (Werner, 2005, p. 96). Long (1999) maintained that the need for organizations to develop appropriate policies requires all decision makers to have a certain level of awareness of standards for security. Training should apply to end users and even to federal government agencies (Macmanus, 2013) and the U.S. Department of Defense workforce of military, civilians, and contractors (McDaniel, 2013).

Educating general users on security also has additional benefits. First, it can provide future users with the critical thinking and basic skills to collaborate with vendors and IT professionals who provide security tools (Werner, 2005). Another benefit is that security training can change employee attitudes (Berry & Houston, 1993). In time, this becomes the way things are done and inculcates a positive information security culture (Da Veiga & Eloff, 2010). Effective training and awareness both result in behavioral change in organizations and are critical in embedding information security principles at the employee level (Da Veiga, 2015).

As noted by Bada and Sasse (2015), changing behavior requires changes to attitudes and intentions, and the antecedents of behavior change are key indices of a user’s mental readiness for action. These are found in several different psychological models of behavior. The Theory of Reasoned Action (TRA) was formulated by Ajzen and Fishbein (1980) as they tried to estimate the discrepancy between behavior and attitude. When behavior appeared to be completely involuntary and not under control, (Ajzen I. , 1988) then proposed the Theory of Planned Behavior (TpB) which attempted to predict deliberate behavior. Prentice and Rogers (1986) promoted the protection motivation theory that was originally developed to explain the influence of fear invocations on attitudes and health behaviors. Bandura (1977) endorsed the theory of self-efficacy, which was the adoption of a preventive health behavior that depended upon the three factors of the realization that the person is at risk, the expectation that behavior change will reduce this risk and the expectation that the person is capable enough to adopt preventive behavior or to refrain from risky health behavior. Bernoulli proposed in the year 1734 the concept of expected utility, in which behavioral change can be explained due to a person's perception of it as a "useful" decision. In the presence of risky outcomes, a decision maker could use the expected value criterion as a rule of choice so that higher expected value investments are the preferred ones (Fishburn, 1988).

Although Long (1999) advocated that security instruction should begin as early as kindergarten, most researchers stated that institutions of higher education should be responsible for providing security awareness instruction, including Crowley (2003), Mangus (2002), Null (2004), Tobin and Ware (2005), Valentine (2005), Werner (2005), and Yang (2001). This instruction and training is important not only to meet the current demands of securing systems but also to prepare students for employment in their respective fields. Werner (2005) said that as employees, new college graduates will have access to critical data to perform their jobs, yet they could be the weakest link in a secure computer system primarily because of inadequate education, negligence, and inexperience. Support for making institutions of higher education the primary source for security awareness training comes from several different sources. The Action and Recommendation 3-4 of the NASA Shared Services Center (NSSC) calls upon colleges and universities to model user awareness programs and materials (Valentine, 2005). Frincke and Bishop (2004) summarized several of the major groups and efforts currently involved in computer security education with institutions of higher education.

The location of security awareness instruction and training in a college curriculum should not be isolated in upper-level courses for IT majors, according to Tobin and Ware (2005) and Werner (2005). This instruction should be taught to all graduates as a 'security awareness' course (Valentine, 2005) along with integrating it across through the curriculum (Yang, 2001).

Institutions of higher education have used different techniques to provide security awareness instruction. Several schools hold annual cyber security training fairs to promote a secure culture within the campus, provide information-security education and training to all constituents, provide hands on peer-to-peer mentoring about security, teach users how to protect data through the deployment of common security practices, and to evaluate the cybersecurity awareness levels of the student population (Larson, 2015). Gaming has also been promoted as a technique to teach security awareness (Hendrix, Al-Sherbaz, & Bloom, 2016). Huang (2015) notes that an issue with existing cyber security training is that it relies mostly on lecture-style instructions without much hand-on experience. He advocates a training solution that provides a realistic, human-in-the-loop environment for exploration, collaboration, and interaction to promote effective learning and calls the approach Cyber Situation Awareness (CSA).

3. Methodology

Because attacks continue to increase, particularly phishing attacks, and because of the calls for institutions of higher education to be responsible for providing security awareness instruction, what are student and instructor attitudes towards security? Does there exist, as is sometimes postulated, an apathy on the part of students regarding security? Or are students concerned about security topics? Do instructors perceive that practical, applied security instruction is a necessary component to their courses, or do they perceive that security instruction belongs elsewhere?

In short, do students and instructors share the same concern over specific security topics, or do the two groups view security in a different light? This current study explored the relationship of student attitudes towards security compared with those of instructors over six current security topics: anti-virus software, using firewalls, securing wireless networks, using spam filters, protection from phishing, and how to create strong passwords.

The primary research hypotheses were as follows:

$H_0$1 – The means of student and instructor responses are equal and there is no difference between the perceptions of the importance of using anti-virus software.

$H_1$1– The means of student and instructor responses are different and there is a significant difference between the perceptions of the importance of using anti-virus software.

$H_0$2 – The means of student and instructor responses are equal and there is no difference between the perceptions of the importance of using a firewall.

$H_1$2– The means of student and instructor responses are different and there is a significant difference between the perceptions of the importance of using a firewall.

$H_0$3 – The means of student and instructor responses are equal and there is no difference between the perceptions of the importance of securing wireless networks.

$H_1$3– The means of student and instructor responses are different and there is a significant difference between the perceptions of the importance of securing wireless networks.

$H_0$4 – The means of student and instructor responses are equal and there is no difference between the perceptions of the importance of using spam filters.

$H_1$4– The means of student and instructor responses are different and there is a significant difference between the perceptions of the importance of using spam filters.

$H_0$5 – The means of student and instructor responses are equal and there is no difference between the perceptions of the importance of protecting yourself from phishing.

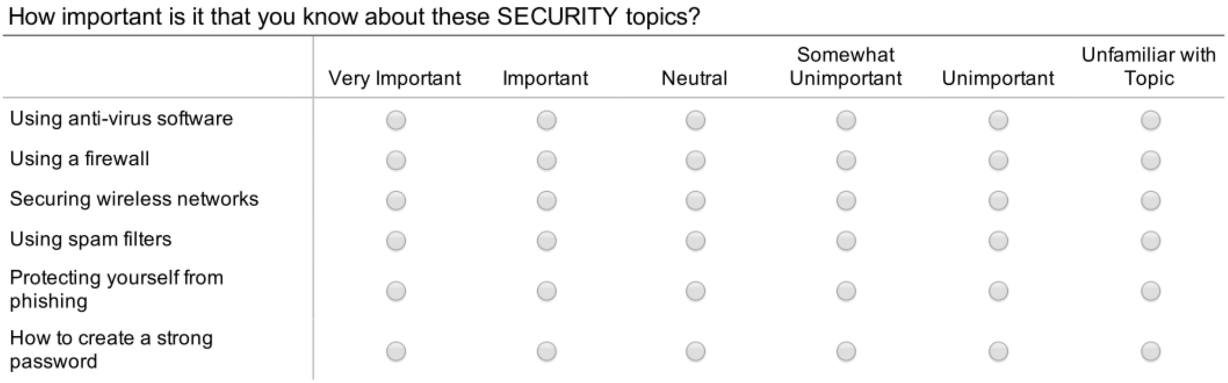
$H_1$5– The means of student and instructor responses are different and there is a significant difference between the perceptions of the importance of protecting yourself from phishing.

$H_0$6 – The means of student and instructor responses are equal and there is no difference between the perceptions of the importance of how to create a strong password.

$H_1$6– The means of student and instructor responses are different and there is a significant difference between the perceptions of the importance of how to create a strong password.

In this current study 1,057 students who had enrolled in a computer literacy course at a regional university in the mid-South were asked the first week of class regarding their perceived importance of a variety of common computer literacy topics. These topics include general computer topics, computer applications, and security. Students were then asked to rate themselves regarding their use and knowledge of technology. Due to the changes in technology students also were asked regarding their personal ownership of technology devices, along with gender, age, and employment status.

The security questions posed to students asked their perceived level of importance on the following security topics: using anti-virus software; using a firewall; securing wireless networks; using spam filters; protection from phishing; and how to create a strong password (*Figure 1*). The same security questions were asked of 95 instructors from different colleges located in the mid-South regarding their perceived importance of the same common computer literacy topics.



How important is it that you know about these SECURITY topics?

	Very Important	Important	Neutral	Somewhat Unimportant	Unimportant	Unfamiliar with Topic
Using anti-virus software	○	○	○	○	○	○
Using a firewall	○	○	○	○	○	○
Securing wireless networks	○	○	○	○	○	○
Using spam filters	○	○	○	○	○	○
Protecting yourself from phishing	○	○	○	○	○	○
How to create a strong password	○	○	○	○	○	○

Figure 1. Security questions

4. Results

The results of the student responses to the security questions are seen in *Figure 2* and *Table 1* and *Table 2*.

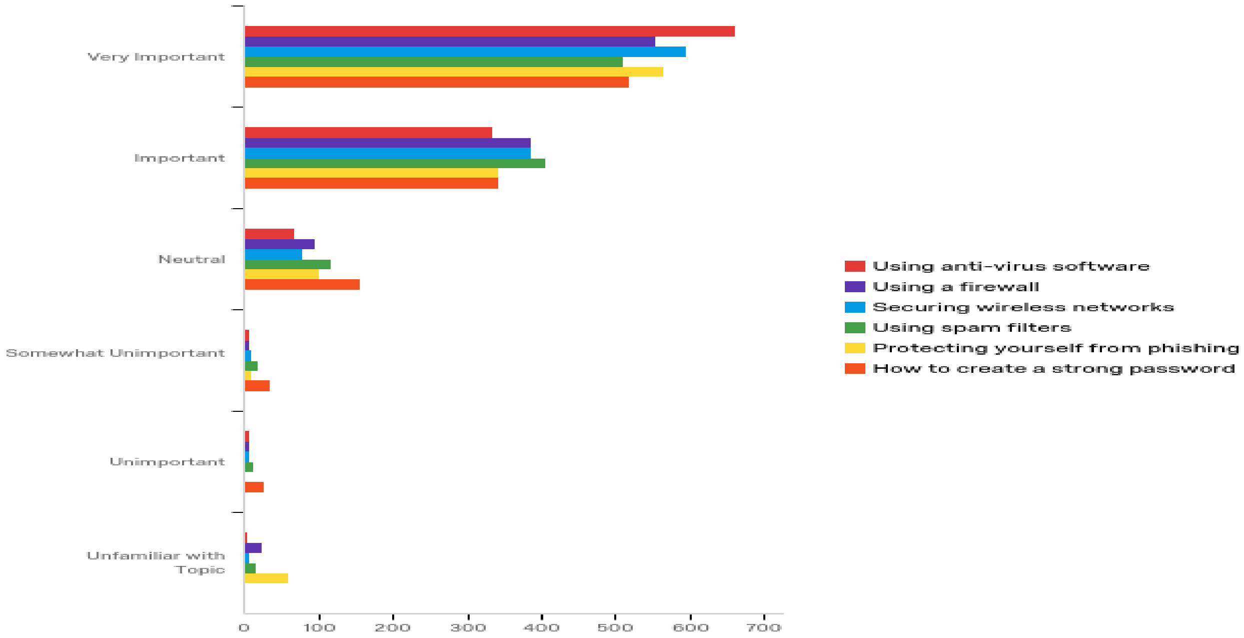


Figure 2. Students - How important is it that you know about these SECURITY topics?

Table 1. Basic statistics of student responses

Question	Minimum	Maximum	Mean	SD	Variance	Count
A. Using anti-virus software	1.00	6.00	1.49	0.73	0.54	1079
B. Using a firewall	1.00	6.00	1.69	0.98	0.95	1073
C. Securing wireless networks	1.00	6.00	1.58	0.79	0.62	1080
D. Using spam filters	1.00	6.00	1.76	0.96	0.93	1077
E. Protecting self from phishing	1.00	6.00	1.81	1.22	1.49	1078
F. How create strong password	1.00	6.00	1.81	0.99	0.97	1080

Table 2. Count and percentage of student responses

Q	1	#	2	#	3	#	4	#	5	#	6	#
A	61.26%	661	30.95%	334	6.30%	68	0.65%	7	0.56%	6	0.28%	3
B	51.72%	555	35.88%	385	8.95%	96	0.56%	6	0.65%	7	2.24%	24
C	55.00%	594	35.65%	385	7.31%	79	0.93%	10	0.56%	6	0.56%	6
D	47.26%	509	37.60%	405	10.86%	117	1.67%	18	1.11%	12	1.49%	16
E	52.41%	565	31.82%	343	9.28%	100	0.93%	10	0.19%	2	5.38%	58
F	48.06%	519	31.57%	341	14.44%	156	3.24%	35	2.50%	27	0.19%	2

1=Very important; 2=Important; 3=Neutral; 4=Somewhat unimportant; 5=Unimportant; 6=Unfamiliar with topic

The results of the instructor responses to the security questions are seen in *Figure 3* and *Table 3* and *Table 4*.

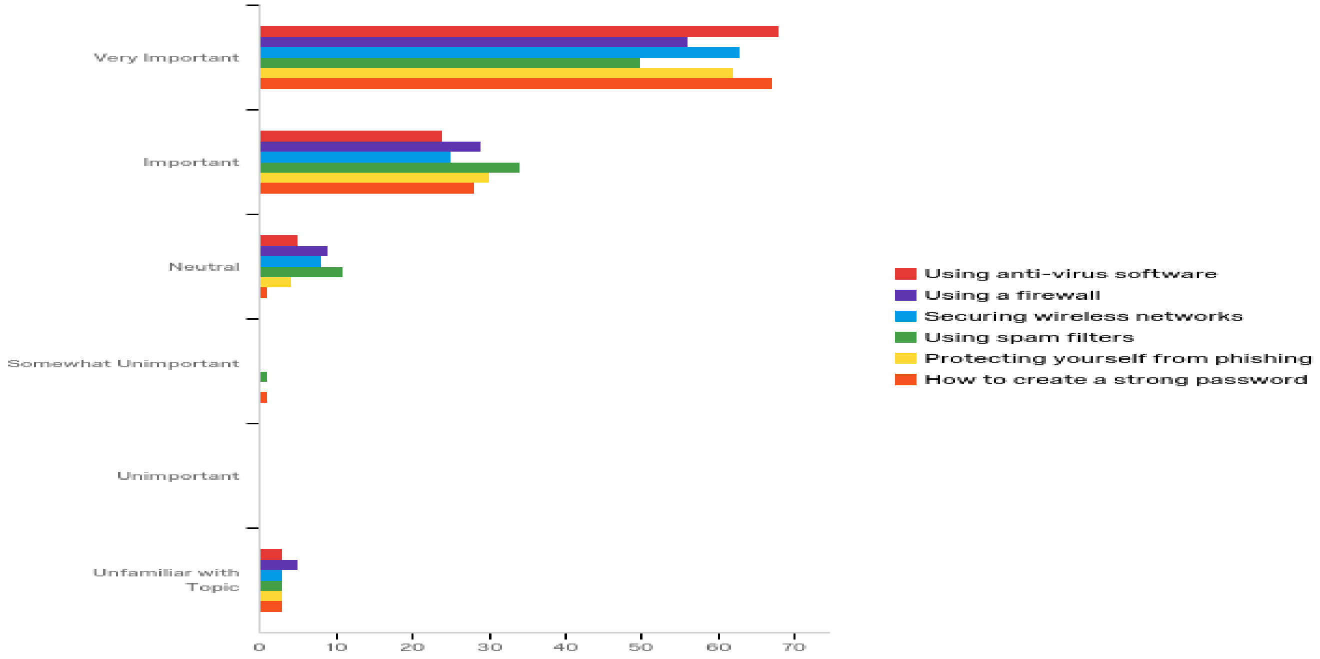


Figure 3. Instructors - How important is it that you know about these SECURITY topics?

Table 3. Basic statistics of instructor responses

Question	Minimum	Maximum	Mean	SD	Variance	Count
A. Using anti-virus software	1.00	6.00	1.49	0.97	0.95	100
B. Using a firewall	1.00	6.00	1.73	1.18	1.39	99
C. Securing wireless networks	1.00	6.00	1.57	1.01	1.01	99
D. Using spam filters	1.00	6.00	1.75	1.04	1.08	99
E. Protecting self from phishing	1.00	6.00	1.48	0.96	0.93	100
F. How create strong password	1.00	6.00	1.43	0.87	.76	100

Table 4. Count and percentage of instructor responses

Q	**1**	**#**	**2**	**#**	**3**	**#**	**4**	**#**	**5**	**#**	**6**	**#**
A	68.00%	68	24.00%	24	5.00%	5	0.00%	0	0.00%	0	3.00%	3
B	56.57%	56	29.29%	29	9.09%	9	0.00%	0	0.00%	0	5.05%	5
C	63.64%	63	25.25%	25	8.08%	8	0.00%	0	0.00%	0	3.00%	3
D	50.51%	50	34.34%	34	11.11%	11	1.01%	1	0.00%	0	3.00%	3
E	62.63%	62	30.30%	30	4.04%	4	0.00%	0	0.00%	0	3.00%	3
F	67.00%	67	28.00%	28	1.00%	1	1.01%	1	0.00%	0	3.00%	3

1=Very important; 2=Important; 3=Neutral; 4=Somewhat unimportant; 5=Unimportant; 6=Unfamiliar with topic

When comparing instructors to students there was no significant difference between instructors and students on the topics of using anti-virus software, using a firewall, securing wireless networks, and using spam filters. The cumulative percentage of instructors who found the topic of using antivirus software important or very important is 92.6% while the cumulative percentage of students who found the topic of using antivirus software important or very important is 92.1%. The cumulative percentage of instructors who found the topic of using a firewall important or very important is 86.3% and the cumulative percentage of students who found the topic of using a firewall important or very important is 87.6%. The cumulative percentage of instructors who found the topic of securing wireless networks important or very important is 89.5%. The cumulative percentage of students who found the topic of securing wireless networks important or very important is 90.5%. The cumulative percentage of instructors who found the topic of using spam filters important or very important is 85.3% while the cumulative percentage of students who found the topic of using spam filters important or very important is 84.8%.

There was a significant difference between instructors and students for the topics of protecting yourself from phishing and how to create a strong password. This was confirmed at the p<=.05 level using the Mann-Whitney U test (*Tables 4-6*). The cumulative percentage of instructors who found the topic of protecting yourself from phishing as important or very important is 93.7% and the cumulative percentage of students who found the topic of protecting yourself from phishing as important or very important is 84.4%. The cumulative percentage of instructors who found the topic of how to create a strong password as important or very important is 95.8%. The cumulative percentage of students who found the topic of how to create a strong password as important or very important is 79.8%.

Table 4. Ranking

Question	Group Number	N	Mean Rank	Sum of Ranks
A. Anti-virus	1	95	542.71	51557.50
	2	1057	579.54	612570.50
	Total	*1152*		
B. Firewall	1	95	555.53	52775.00
	2	1051	575.12	604456.00
	Total	*1146*		
C. Wireless Net	1	95	537.50	51062.50
	2	1058	582.55	614218.50
	Total	*1153*		
D. Spam Filters	1	95	556.74	52890.00
	2	1055	577.19	608935.00
	Total	*1150*		
E. Phishing	1	95	506.10	48079.50
	2	1056	582.29	614896.50
	Total	*1151*		
F. Password	1	95	449.88	42738.50
	2	1058	588.41	622542.50
	Total	*1153*		

1=Instructors; 2=Students

Table 5. Mann-Whitney Test for Questions A-E

	A. Anti-virus	B. Firewall	C. Wireless Net	D. Spam Filters	E. Phishing
Mann-Whitney U	46997.500	48215.000	46502.500	48330.000	43519.500
Wilcoxon W	51557.500	52775.000	51062.500	52890.000	48079.500
Z	-1.207	-.613	-1.364	-.628	-2.371
Asymp. Sig. (2-tailed)	.228	.540	.173	.530	0.18

Table 6. Mann-Whitney Test for Question F

	Password
Mann-Whitney U	38178.500
Wilcoxon W	42738.500
Z	-4.229
Asymp. Sig. (2-tailed)	.000

Additional comparisons were made between male and female students. There were 518 males and

533 females who participated in this study. Significant differences between male and female students were found for using anti-virus software, securing wireless networks, using spam filters, and how to create a strong password. Viewing the cumulative percentage for *Very Important* and *Important* results can be seen in *Table 7*.

Table 7. Cumulative Frequency Response for Very Important and Important

	A. Anti-virus*	B. Firewall	C. Wireless Net*	D. Spam Filters*	E. Phishing	F. Passwords*
Male	90.50%	87.40%	89.80%	83.30%	85.10%	76.50%
Female	93.80%	87.70%	91.40%	86.70%	84.00%	83.10%

*Significant at the p<=.05

In contrast, instructors overwhelmingly ranked higher the importance of these six security topics than students. In fact, only a total of two responses from all 95 instructors were ranked only somewhat important or unimportant (using spam filters and how to create a strong password). Ninety-two percent of instructors ranked phishing as very important or important.

5. Conclusion

The results from this study seem to indicate that there is no significant difference between the perceptions of students and instructors regarding the security topics of using anti-virus software, using a firewall, securing wireless networks, and using spam filters; both groups indicated a high level of concern for these topics. Thus, hypothesis $H_1$1, $H_1$2, $H_1$3, and $H_1$4 are to be rejected. The results seem to indicate that there is a significant difference between the perceptions of students and instructors regarding the security topics of protection from phishing and how to create a strong password. Thus, hypothesis $H_1$5 and $H_1$6 are to be accepted.

It is noteworthy that whereas among students protecting yourself from phishing had the third-highest response of being very important (52.41% or 565 responses), this same question resulted in the highest number of responses of not being familiar with the topic (5.38% or 58 responses). This may suggest that confusion remains regarding exactly what phishing entails. Future research may examine how clearly students understand the definitions of phishing and other types of attacks.

It is likewise significant that there was a significant difference between the perceptions of students and instructors regarding how to create a strong password. This question had the second-lowest response by students of being very important (48.06% or 519 responses), only ten responses higher than the lowest response of using spam filters (47.26%). With the continued number of successful attacks directed at compromising passwords the reason for this response may be an indication that many students erroneously believe that their passwords are strong when indeed they are not. Future research may look for additional underlying reasons for this perception.

Significant differences between male and female students were found for using anti-virus software, securing wireless networks, using spam filters, and how to create a strong password. Additional future research may examine why there are these differences between genders. This may prove to be beneficial in crafting training specifically directed between male and female.

6. References

Ajzen, I. &. (1980). *Understanding attitudes and predicting social behavior.* Inglewood Cliffs, NJ: Prentice-Hall.

Ajzen, I. (1988). *Attitudes, personality, and behavior.* Chicago: Dorsey Press.

Bada, M., & Sasse, A. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *First International Conference on Cyber Security for Sustainable Society 2015* (pp. 1-38). Coventry: Coventry University. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-awareness-campaigns-why-do-they-fail-change-behaviour

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215. doi:http://dx.doi.org/10.1037/0033-295X.84.2.191

Berry, M., & Houston, J. (1993). *Psychology at work.* New York: Brown and Benchmark.

Bright, P. (2016, April 25). *Billion dollar Bangladesh hack: SWIFT software hacked, no firewalls, $10 switches*. Retrieved from ArsTechnica: http://arstechnica.com/security/2016/04/billion-dollar-bangladesh-hack-swift-software-hacked-no-firewalls-10-switches/

Ciampa, M. (2018). *Security+ Guide to Network Security Fundamentals* (6th ed.). Boston: Cengage Learning.

Cisco. (n.d.). *Cisco Security Reports.* Retrieved from Cisco: http://www.cisco.com/c/en/us/products/security/annual_security_report.html

Cranor, L. (2006). What do they "indicate?" Evaluating security and privacy indicators. *Interations*, 45-47.

Crowe, J. (2017, July). *Must-know phishing statistics 2017*. Retrieved from Barkly: https://blog.barkly.com/phishing-statistics-2017

Crowley, E. (2003). Information systems security curricular development. *Conference on Information Technology Education* (pp. 249-255). Lafayette, IN: ACM.

Da Veiga, A. (2015). An information security training and awareness approach (istaap) to instil an information security-positive culture. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)* (pp. 95-107). Lesvos, Greece: International Symposium on Human Aspects of Information Security & Assurance.

Da Veiga, A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers and Security, 29,* 196-207.

Dean, J. (2018, January 18). *Conversations around digital security*. Retrieved from Gemalto: https://blog.gemalto.com/security/2018/01/18/2017-year-ransomware/

Dhamija, R., & Tygar, J. (2005). The battle against phishing: Dynamic security skins. *Proceedings of the 2005 Symposium on Usable Privacy and Security* (pp. 77-88). Pittsburgh: ACM.

Dhamija, R., Tygar, J., & Hearst, M. (2006). Why phishing works. *Conference on Human Factors In Computing Systems* (pp. 1-10). Montreal: ACM.

Downs, J., Holbrook, M., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security* (pp. 79-90). Pittsburgh: ACM.

Elson, D. (2017, July 31). *Attack of the hack*. Retrieved from The Sun: https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/

Fishburn, P. (1988). Expected utility: An anniversary and a new era. *Journal of Risk and Uncertainty*, 267-283. Retrieved from https://link.springer.com/article/10.1007/BF00056138

Frincke, D., & Bishop, M. (2004). oining the security education community. *IEEE Security and Privacy*, 61-63.

Gemalto. (2015, August 15). *http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf*. Retrieved from http://www.gemalto.com: http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf

Group, A.-P. W. (2016, March 22). *APWG news*. Retrieved from APWG: http://www.antiphishing.org/apwg-news-center/

Gyunka, B., & Christiana, A. (2017). Analysis of human factors in cyber security: A case study of anonymous attack on Hbgary. *Computing and Information Systems Journal, 21*(2), 10-18.

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games, 3*(1), 53-61.

Huang, Z. (2015). *Human-centric training and assessment for cyber situation awareness.* Ann Arbor, MI: ProQuest.

IBM 2015 Cyber Security Intelligence Index . (2015). Retrieved from Essextec: https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf

Jackson, C., Simon, D., Tan, D., & Barth, A. (2007). *An evaluation of extended validation and picture-in-picture phishing attacks.* Trinidad/Tobago: Commercenet.

Korolov, M. (2015, August 25). *Phishing is a $3.7-million annual cost for average large company*. Retrieved from CSO: http://www.csoonline.com/article/2975807/cyber-attacks-espionage/phishing-is-a-37-million-annual-cost-for-average-large-company.html

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: the design and evaluation of an embedded training e-mail system. *CHI 2007 Procedeedings* (pp. 905-914). San Jose: ACM.

Larson, S. (2015). The cyber security fair: An effective method for training users to improve their cyber security behaviors? *Information Security Education Journal, 2*(1), 11-19.

Long, C. (1999). A socio-technical perspective on information security knowledge and attitudes. *Doctoral dissertation, The University of Texas at Austin*. Austin, TX, USA: Dissertation Abstracts International.

Macmanus, S. A. (2013). Cybersecurity at the local government level: balancing demands for. *ournal Of Urban Affairs, 35*(4), 451-470.

Mangus, T. (2002). Perspectives and culture. A study of first-year community college students and proposed responsible computing guide. *Doctoral dissertation, Union Institute and University*. Cincinnati, OH, USA: Dissertation Abstracts International.

McDaniel, E. A. (2013). Securing the information and communications technology global supply chain from exploitation:. *Issues In Informing Science and Information Technology*, 313-324.

McFarland, C., Paget, F., & Samani, R. (2016). *McAfee Resources.* Retrieved from McAfee: http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf

Mitnick, K., & Simon, L. (2001). *The art of deception: controlling the human element of security.* Indianapolis: John Wiley & Sons.

Null, L. (2004). Integrating security across a computer science curriculum. *Journal of Competing Science In Colleges*, 170-178.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers and Security, 42*, 165-176.

Phishlabs. (2016). *2016 phishing trends & intelligence report: hacking the human* . Retrieved from Phishlabs: https://pages.phishlabs.com/2016-Phishing-Trends-and-Intelligence-Report-Hacking-the-Human_PTI.html

Prentice-Dunn, S., & Rogers, R. (1986, September). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research, 1*(3), 153-161. doi:https://doi.org/10.1093/her/1.3.153

Ranjeev, M., & Lawless, W. (2015). The human factor in cybersecurity and the role for AI. *AAAI Spring Symposium* (pp. 39-43). Palo Alto: AAAI. Retrieved from https://aaai.org/Symposia/Spring/sss15.php

Schechter, S., D. R., Ozment, A., & Fischer, I. (2007). The Emperor's new security indicators: an evaluation of website authentication and the effect of role-playing on usability studies. *2007 IEEE Symposium On Security and Privacy* (pp. 51-65). Oakland: IEEE.

Straub. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 45-55.

Straub, D. W., Carlson, P., & Jones, E. (1993). Deterring cheating by student programmers: A field experiment in computer science. *ournal of Management*, 33-48.

Tobin, D., & Ware, M. (2005). Using a windows attack intRusion emulator (AWARE) to teach computer security awareness. *10th Annual SIGSCE Conference on Innovation and Technology in Computer Signs Education* (pp. 213-217). Caparica, Portugal: SIGSCE.

Tulloch, M., Northrup, T., & Honeycutt, J. (2007). *Windows vista resource kit.* Redmond: Microsoft Press.

Valentine, D. (2005). Practical computer security: A new service course based upon the national strategy to secure cyberspace. *Conference on Information Technology Education*, 185-189.

Werner, L. (2005). Redefining computer literacy in the age of ubiquitous computing. *Conference on Information Technology Education* (pp. 95-99). Newark: ACM.

Whalen, T., & Inkpen, K. (2005). Gathering evidence: use individual security cues in web browsers. *Proceedings of Graphics Interface 2005* (pp. 137-144). Victoria, British Columbia: ACM.

Whitson, G. (2003). Computer security: Theory, process and management. *Journal of Computing Sciences in Colleges*, 57-66.

Wu, M., Miller, R., & Garfinkel, S. (2006). Do security toolbars actually prevent phishing attacks? *Conference on Human Factors in Computing Systems* (pp. 1-10). Montreal: ACM.

Yang, T. (2001). Computer security: An impact on computer science education. *Journal of Computing Sciences in Colleges*, 233-246.

Zetter, K. (2016, January 28). *NSA hacker chief explains how to keep him out of your system*. Retrieved from Wired: https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/

Copyright Disclaimer