OC10077

INFORMATION SECURITY ACTIVITIES OF COLLEGE STUDENTS: AN EXPLORATORY STUDY

Scott Mensch, Indiana University of Pennsylvania

LeAnn Wilkie, Indiana University of Pennsylvania

ABSTRACT

Academic institutions prepare students for their professional field of study, but student awareness of Information Technology (IT) security issues continues to be poor (McQuade, 2007; Livermore, 2006). Most college students communicate via email and social networking sites, such as Twitter, MySpace, and Facebook. However, students are at risk for identity theft through fraudulent emails, stolen passwords, unsecured systems, and inadequate network practices (Harwood, 2008). This exploratory study identifies key findings and recommendations regarding security attitudes, behaviors and tools used by college students along with suggestions for improving information security-awareness at academic institutions.

INTRODUCTION

Increasingly, a large portion of communication (Salas & Alexander, 2008) in higher education, as well as instruction (Allen & Seaman, 2010), is conducted through technology-mediated communication, such as email (Jones, 2008; Jones, Johnson-Yale, Perez & Schuler, 2007; Weiss & Hanson-Baldauf, 2008), learning management systems (Green, 2007; Hawkins & Rudy, 2007; Jacob & Issac, 2008), blogging (Nackerud & Scaletta, 2008), and social media (Allen & Seaman, 2009; Ashraf, 2009; Ellison, 2007; Gilroy, 2010; Rosen & Nelson, 2008; Saeed, Yang, & Sinnappan, 2009). College students use Internet technologies to take classes, register for courses, and communicate with other students, faculty, and administrators (Chueng & Huang, 2005; Jones, Johnson-Yale, Perez & Schuler, 2007). The need to develop an IT security awareness plan is crucial to ensure the security of student, faculty, and academic data (The Campus Computing Project, 2007). This paper explores relevant factors to educational institutions to enable a better understanding of the end-user perspective with regard to information security and the inherent dangers in the virtual world.

While academic institutions prepare students for professional careers Cheung & Huang, 2005), effective information security awareness training has taken a back seat as prospective employers are expected to take on responsibility for training of college graduate hires Okenyi & Owens, 2007; Turner, 2007). However, this approach is ineffective as sound IT security practices continue to fall through the cracks. Regardless of a student's vocational goals, universities and colleges must take a proactive approach to educate students about the potential risks associated with the Internet usage and message security, as reported dollar losses from Internet crime have reached new highs (Internet Crime Complaint Center, 2009).

Traditional data centers and corporate networks are specific about the types of data and methods used to access data that is permitted on their networks. Hackers and cyber criminals often bypass the security set up on computer networks, as these sites and programs use the same port as the users Web browser. Thus, many corporate networks ban users from accessing private email accounts, using instant messenger programs, and accessing social networking sites, such as Twitter, MySpace, and Facebook (Brodkin, 2008). High school networks also commonly block access to these sites and filter email for malware and other unwanted content. Because academic institutions openly share a substantial amount of information and data, web sites are rarely banned and message content is not filtered increasing the likelihood that students will encounter hackers or identity thieves while using institutional networks (Allison & Deblois, 2008; Ziobron, 2003). The present study explores security attitudes and behaviors of college students, along with their use of security tools, and highlights end-user security awareness practices that institutions can employ to help students better protect personal information and data.

LITERATURE REVIEW

While university campuses release yearly crime statistics on crimes such as aggravated assault, burglary, driving under the influence, theft, vandalism, and public drunkenness, one particularly vexing crime is unreported in university crime statistics. Cybercrime is one of the most common criminal activities affecting college students that is not tracked by the Clery Act (The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act, 1990). Yet, cyber thieves do an incredible amount of damage to individuals across all spectrums of society (Internet Crime Complaint Center, 2009) and cybercrime is considered to be a 24/7/365 threat (Computer Security Institute, 2009). Campus safety programs often cover the crimes covered by the Clery Act, but institutions of higher education should more proactively address end-user electronic data security and identity protection, particularly as it pertains to college students in the ubiquitous online world.

Information Security Threats

Many ever-evolving human-caused security threats lurk in virtual spaces. Social engineering is a common tactic used by attackers and involves persuading people that the perpetrator is someone other than who he/she really is (Mitnick, 2002). Social engineers use deceit to convince people to release information or perform actions. In addition to threats from viruses and worms (Luo & Liao, 2007), a survey by the Computer Security Institute (2009) of the most common attacks cites malware (64.9% of attacks), bots and zombies (23%), phishing messages (34%), denial of service attacks (29.2%), password sniffing (17.3%), browser exploitation (11%), social network profile exploitation (9%), and financial fraud (19.5%). Spyware, another worrisome threat, is client-side software that monitors and tracks computer activity and sends collected data secretly to remote machines. Spyware is often found in free downloadable software and may use the CPU and storage for tasks unknown to the end-user (Luo & Liao, 2007). Users running Windows operating systems are targets of most spyware, but Macintosh operating systems may also be vulnerable (InfoWorld, 2010). Offline threats also exist which include shoulder surfing, dumpster diving (Okenyi & Owens, 2007), and laptop/mobile device theft, which is currently a major threat to organizations and individuals (Computer Security Institute, 2009; Young, 2009).

Another threat often associated with cybercrime is identity theft, which involves someone gaining access to personal data without a person's knowledge often for purposes of committing identity fraud (Javelin Strategy & Research, 2009). It can be both a financial crime and a non-financial crime, such as criminal, government, and medical identity theft (Identity Theft Resource Center, 2009). A 2009 report by the Identity Theft Resource Center cites credit card fraud as the most common source of identity theft (17%), followed by governmental/benefit fraud (16%), which includes tax return and employment fraud, or a combination of the three. Two other sources of identity theft are phone/utilities fraud (15%) and employment fraud (13%). The total cost to consumers was more than $1.7 billion. Data breaches and the Internet as sources of identity theft are also rising, up 5.3% from 2003 (Identity Theft Resource Center, 2008). The greatest percentage of identity theft victims by age were 18-29 year-olds (17%), 30-39 year-olds (26%), 50-60 year olds (26%), and 40-49 year olds (22%) (Identity Theft Resource Center, 2009). While 56% victims know the thief, 43% of victims do not know the thief (Identity Theft Resource Center, 2009). The time it takes for victims discover the loss ranges from 3 months to two years and costs include "lost wages or vacation time, diminished work performance and morale, increased medical problems," along with financial and other costs (Identity Theft Resource Center, 2009, p. 18). Victims spend 58 hours on average repairing the damage over several months. In terms of dollar costs, fraud committed on an existing account averaged $739 in 2008 and $951 for new accounts. Almost 20% of victims required 2 years or more to clear their names and were also "secondarily wounded" by denial of or inability to get credit, increased insurance or credit card rates, and repeated contacts by collection agencies (Identity Theft Resource Center, 2009).

Security Behaviors of College Students

As the interests and practices of Internet users evolve, institutions much ensure that students are continually educated about online risks. A popular online venue, social networking sites are Web sites that provide people with the opportunity to create an online profile to share with others (Barnes, 2006) and even create a fictitious lives (Gorge, 2007). Social networking sites are "now visited by over two-thirds (67%) of the global online population (which includes both social networks and blogs) and is the fourth most popular online category ahead of personal email. Social networking is growing twice as fast as any of the other four largest sectors which include search, portals, PC software, and email (Nielsen/NetRatings, 2009).

Fogel & Nehmad (2008) found that 77.6% of college students used social networking sites and 79-95% of college students have Facebook accounts (Ellison, 2007). Half of the participants in Fogel & Nehmad's (2008) research included instant messenger names on personal profiles and 65% included a personal email address. Also, 74% allowed anyone to view their profiles, 10% provided a phone number, and 10% provided their home address. This scenario is a major concern as malware and viruses are sent through email and instant messenger programs.

Social networking sites are also subject to hijacking and fake log-in pages and password management is lacking since people often use the same password and username for various sites; therefore, once an a user's Facebook credentials are known, it is easy to gain access to a bank account with the same username and password (Mansfield-Devine, 2008). Many social network users are also not aware that the applications endorsed by a social network are not supplied by the site and there is no assurance of who wrote the software or where it's hosted (Mansfield-Devine, 2008).

Personal data from social networks can also be mined for purposes of conducting phishing attacks. Jagatic, Johnson, Jakobsson & Menczer (2007) conducted a study where 72% of the social network group clicked on the phishing link. Phishing success rates were highest among sophomores (26%) and those classified as "other" (50%) for the control group (receivers of a phishing email from an unknown person with a university address), and highest among freshmen (76%) and "other" (76%) for the social network group. Phishing success rates also were highest among education majors (50%) in the control group, and science (80%) and business (72%) majors in the social network group. Students in technology-related majors had the lowest phishing success rates (0% control; 36% social network). Jagatic, et al. (2007) also spoofed an email message as forwarded from a friend to a group of friends and, even though the experiment contained a coding flaw, 53% of the sample still clicked on the phishing link.). The Computer Security Institute reported that social network profile attacks were added to its 2009 survey for the first time. Many of these attacks are hatched as a result of successful social engineering efforts by attackers, including bots and zombies that originate from the infected computers of end-users.

End-user Security Software

A variety of security software is available to end-users including, firewalls, anti-virus software (Mitnick, 2006), and anti-spyware software. Browser-based tools, such as pop-up blockers and phishing filters, are also available. The question is whether end-users employ these tools and how diligent users are about updating security software (Jokela & Karlsudd, 2007). Also, students may not know if anti-virus is installed on their computers and may not know how to remove a virus once it's discovered (Jokela & Karlsudd, 2007).

The C.I.A. triad

The basis for information security models because in 1994 when the National Security Telecommunications and Information Systems Security Committee (NSTISSC) derived the Comprehensive Model for Information Systems Security, also known as the C.I.A. triad (Whitman & Mattord, 2009) and the McCumber Cube (McCumber, 1991). In the model, information systems security concerns "three critical characteristics of information: confidentiality, integrity, and availability" (NSTISSC, 1994). Confidentiality, the heart of any security policy, encompasses a set of rules that determine access to objects and involves access control of data by users (or groups). An important facet of confidentiality is "the assurance that access controls are enforced" (NSTISSC, "Critical Information Characteristics", para. 2.). The confidentiality construct was further defined by Bell & LaPadula (1973) and the U.S. Department of Defense (Trusted Computer System Evaluation Criteria, 1983). The second characteristic is integrity, which Pfleeger defined as "'assets' (which) can only be modified by authorized parties" (1989). Integrity relates to the "quality of information that identifies how closely the data represent reality" (NSTISSC, "Critical Information Characteristics", para. 5). The construct was further defined by Graham & Denning (1972), Biba (1977), and Clark & Wilson (1987). The third characteristic, availability, "ensures the information is provided to authorized users when it's requested or needed" and serves as a "check-and-balance constraint" on the model (NSTISSC, "Critical Information Characteristics", para. 7). Two additional concepts have been added to the CIA triad by most security practitioners. Authenticity involves verifying the authenticity of the user and ensures that inputs to a system are from a trusted source (Stallings & Brown, 2008). Finally, accountability requires an entity's actions to be traced uniquely to that entity (Stallings & Brown, 2008).

Security Training and Awareness

Training and security awareness are also important elements to assure information security. Training and awareness reduce risks to organizations and is essential to prevent hacking success rates at both the individual and organizational levels (Okenyi & Owens, 2007*).* Hall (2005) asserts that people are the largest component of the triad and the most susceptible to attacks. Thus, a successful security awareness program must shift the paradigm from "ad hoc secure behavior to a continuous secure behavior" (Okenyi & Owens, 2007, p. 306).

Faculty and administrators at colleges and universities may think that because students are technologically-savvy in using information technology (Kirkwood & Price, 2005), they also inherently understand and take appropriate measures to protect personal information and data from hackers and thieves. This may prove to be an unwise assumption.

The purpose of this study is to explore whether college students adopt the security attitudes, behaviors and tools necessary to effectively achieve end-user data and information security. The following research questions were generated:

1. Do security attitudes of college students significantly differ based on factors such as age, gender, ethnicity, classification level, academic major, identity theft victimization, installation of PC anti-virus software, or PC anti-spyware software?
2. Do security attitudes of college students significantly differ based on factors such as age, gender, ethnicity, classification level, academic major, identity theft victimization, installation of PC anti-virus software, or PC anti-spyware software?
3. Do college students' use of security tools, such as anti-virus and anti-spyware software, significantly differ based on age, gender, ethnicity, classification level, academic major,

identity theft victimization, installation of PC anti-virus software, or PC anti-spyware software?

For purposes of this study, our survey of security attitudes includes elements such as:

- Online account password management
- Anti-virus software installation and use
- Anti-spyware software installation and use
- Propensity to click on links inside email or instant messages
- Wireless computing behaviors
- Identity theft victimization
- Offline security measures (credit report monitoring, document shredding, etc.)

METHODOLOGY

This exploratory study investigates whether undergraduate and graduate students adopt the security attitudes, behaviors and tools necessary to achieve end-user data and information security.

Participant Population and Site of Study

The population sample for the study consisted of 2,000 undergraduate and graduate students from a mid-sized eastern university. While the authors desired to survey the entire student body, IUP University policies restricted the use of emails to 2,000 addresses. These emails were randomly picked by the IUP graduate research office and sent to full time students in all degree programs enrolled at the university. An email was sent by the IUP graduate research office to the 2,000 students noted above as notification of and to encourage participation in the study. A link to the survey was provided through the email notification to Survey Monkey, participation was voluntary. The informed consent form was used for students. Participants were identified by a unique identification number to maintain confidentiality. The data was then downloaded into the Statistical Package for the Social Sciences 14.0 (SPSS) where all analysis and statistical tests were performed.

Instruments

Based on a review of the literature and theoretical standpoints, the researchers developed and pilot tested a 6-item Likert scale consisting of 21 items to determine the security awareness of undergraduate and graduate students the previous academic year using an informal sampling of several classes that included students from several discipline areas across campus. Likert scaling is designed to measure people's attitudes and awareness (Nachmias & Nachmias, 1987). The survey used in the present study was administered via a web-based system to all current undergraduate and graduate students. Survey research has its advantages and disadvantages. Advantages include lower costs, relatively small biasing error, greater anonymity, and accessibility Disadvantages include "a low response rate, opportunity for probing, and the lack of control over who fills out the questionnaire" (Frankfort-Nachmias and Nachmias, 1996, p. 248).

Research Design

The study followed a descriptive research design using survey methods with statistical treatments. The design was a cross-sectional survey. Cross-sectional design is the most frequently used study design (Babbie, 1990, p. 65). Descriptive statistics, such as frequency distributions, means, and standard deviations, were utilized to analyze student demographic characteristics, and correlation tests were performed to determine if significant relationships exist between dependent variables. T-tests of independent samples and analyses of variance (ANOVA) were also conducted to compare differences in security attitude scores and sub-scale scores among the groups. Post hoc multiple comparison tests (Gabriel, 1987) were conducted to determine where differences between means existed. Statistical significance was set at the 95% level ($p > 0.05$).

Variables

The study featured one independent variable consisting of total scores derived from the 21-item security attitudes survey. To provide additional analysis, the Likert scale was divided into four subscales, categorized as follows: security behaviors (7-item subscale), use of security tools (5-item subscale), wireless security (5-item subscale), and data privacy (4-item subscale). Results from the data privacy and wireless security subscales will be discussed in subsequent articles.

Several dependent variables were included in the study. Age was categorized into four groups (1 = 18 to 23 years of age; 2 = 24 to 30 years of age; 3 = 31 to 36 years of age; 4 = 37+ years of age). Gender was categorized as male or female. Ethnicity was categorized into six groups (1 = White, 2 = Hispanic, 3 = African-American, 4 = Asian, 5 = Native American, 6 = Other [race not specified or non-resident alien]). Major was categorized into nine groups (1= Education, 2= Humanities & Social Sciences, 3= Health & Human Services, 4= Business, 5 = Fine Arts, 6 = Criminology, 7 = Natural Science, 8 = Information Technology, 9 = Other). Classification was categorized into six groups (1 = Freshman, 2 = Sophomore, 3 = Junior, 4 = Senior, 5 = Graduate, 6 = Other). Additional dependent variables included identity theft victimization with responses classified into three response groups (1 = Yes, 2 = No, 3 = Don't know). Participants were also asked if antivirus was installed on their personal computers. Responses were classified into four groups (1 = Yes, 2 = No, 3 = Yes, but not updated, and 4 = Don't know). Participants were asked if anti-spyware was installed on their personal computers. Responses were classified into four groups (1 = Yes, 2 = No, 3 = Yes, but it expired, and 4 = Don't know). Participants who affirmatively answered that they had a home wireless network were also asked if they changed the wireless router's default administrator password. Responses were classified into four groups (1 = Yes, 2 = No, 3 = Don't know).

Reliability analysis

Internal consistency reliability analysis was performed on the Likert subscales of the measure to provide a reliability measurement. Results revealed an internal consistency of α = .69 for the total scale computed from the raw scores of 21 Likert items. Tukey's test for additivity was significant ($F = 130.083$, $p = .000$, $\alpha = .05$) indicating that several scale items may be related. Exploratory factor analysis was conducted to determine if the instrument accurately measured the study's variables and to serve as an estimate to identify unobserved or latent variables that may account for the true variance of the observations. Eigenvalues of 1.0 indicate that a factor is significant (Gorsuch, 1983). Results revealed that 64.9% of the variance could be explained by the first seven factors with eigenvalues of 1.0 or more. Fifteen percent of the variance is explained by a single factor, 11.7% of the variance is explained by a second factor, 11.6% of the variance is explained by a third factor, 8% of the variance is explained by a fourth factor, 7% of the variance is explained by a fifth factor, 6.6% of the variance is explained by a sixth factor, and 5% of the variance is explained by a seventh factor. As indicated in Table 1, scale items 7 through 11 loaded high on factor 1 (security and browser tools). Items 5 and 6 loaded high positive on factor 2 and item 12 loaded high negative on factor 2 (security behaviors- communication tools). Items 14 through 17 loaded high on factor 3 (wireless security). Items 18 through 20 loaded high on factor 4 (data privacy). Items 1, 2 and 21 are loaded high on factor 5 (security behaviors – personal identification/passwords). Items 3 and 13 loaded high on factor 6 (security behaviors – public spaces). Item 4 loaded high on factor 7 (financial security – electronic data privacy).

Table 1

Primary Factor Loadings, Means and Standard Deviations for Security Attitudes.

Security Attitudes	**Primary factor loadings**	***M***	***SD***
Factor 1: Security tools/browser tools			
Running anti-spyware software	.869	3.91	1.57
Updating anti-spyware software	.843	3.89	1.62
Running anti-virus software	.801	4.35	1.34

Clearing internet history/data	.545	3.53	1.22
Running anti-virus on a USB memory stick	.526	2.66	1.22
Factor 2: Security behaviors – communication tools			
Clicking on IM web links+	.956	4.88	1.06
Clicking on email links+	.624	4.02	.882
Backing up data	-.956	3.12	1.06
Factor 3: Wireless security			
Hiding home network from outsiders	.828	4.51	1.88
Using wireless encryption	.762	3.48	2.25
Using MAC address filtering	.736	2.60	1.94
Check to ensure connecting to correct wireless network	.600	4.55	1.24

SSN			
Factor 5: Security behaviors – personal identification/passwords			
Allowing a PC to remember passwords	.783	4.17	1.328
Placing outgoing mail in unsecured mailbox+	.480	4.51	1.34
check email /log-in to financial institution's web site from hotel/other public computer	-.518	4.74	.928
Factor 6: Security behaviors – public spaces			
Allowing a public PC to remember passwords	.817	5.85	.473
Connecting to a wireless hotspot	.406	4.06	1.76
Factor 7: financial security – electronic data privacy			
Closing browser after visiting a financial web site	.742	5.13	1.136

Security Attitudes	**Primary factor loadings**	***M***	***SD***
Factor 4: Data privacy - Mixed electronic and non-electronic			
monitor credit reports	.768	4.02	1.75
Shredding documents	.664	4.90	1.38
Asking purpose for use of	.594	4.50	1.50

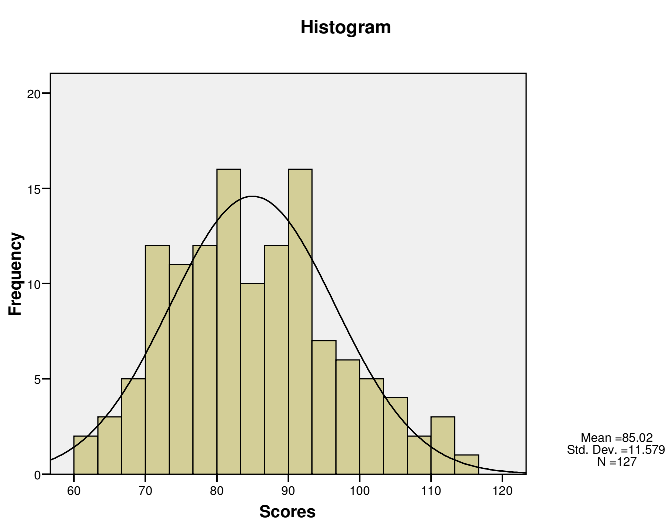
RESULTS

Descriptive Statistical Analysis

Descriptive statistics were used to analyze demographic data and Likert scale results. Correlation tests were also performed to determine if significant relationships exist between the dependent variables. Initially receiving 134 responses, the researchers eliminated incomplete responses, yielding a final sample size of *N* = 127 participants. Participants were mostly freshman and sophomores (45.6%) or graduate students (21.3%); female (63%), Caucasian (81.9%), and 18 to 23 years of age (71.7%). Most majored in Education (18.9%), Humanities & Social Sciences (17.3%), Business (16.5%), or Healthcare (12.6%). The majority of participants have not been a victim of identity theft (85.8%), have anti-virus software installed (80.3%), and have anti-spyware software installed on their PCs (74.8%).

Due to the way the questions were structured, five survey items were reverse coded prior to analysis. Security attitude score ranges were classified as: Very Low = 0-21; Low = 22-42; Moderately Low = 43-63; Moderately High = 64-84; High = 85-105; Very High = 106-126. Only 6% of participants recorded very high scores (*n* = 8) and 44% recorded high scores (*n* = 56). Another 48% recorded moderately high scores (*n* =61) and 1.5% recorded moderately low scores (*n* = 2). Mean security attitude scores overall were 85.02 (*SD* = 1.027). Participant scores ranged from 63 to 116 (Figure 1).

Figure 1: Distribution of Scores



This figure shows the distribution of total scores of the security attitudes survey.

Security attitudes survey and sub-scales

Table 2 summarizes mean security attitude survey scores and the two sub-scale scores by dependent variable.

Security attitude survey. The lowest mean scores, 24-30 year olds, were 6+ points lower than the 18-23 year-old group. On average, male security attitude scores were 4+ points higher than female scores. In terms of ethnicity, scores of Hispanics averaged 20+ points lower than those self-classified as "other" which was the highest scoring ethnic group. The lowest scores by classification were among juniors and graduate students, who scored 10+ points lower than the highest scoring groups, sophomores and those self-classified as "other". Attitude scores of information technology majors were 16+ points higher than healthcare majors, the lowest scoring group by major. Attitude scores of identity theft victims averaged 8+ points higher than the lowest scoring participants (those that didn't know if they were an identity theft victim). Participant attitude scores regarding anti-virus software installation averaged 6+ points higher than those that were unsure if anti-virus software is installed, and attitude scores regarding anti-spyware software installation averaged 13+ points higher than those that were unsure if anti-spyware software is installed.

Correlation tests conducted on security attitudes survey by dependent variables revealed significant positive relationships between age and classification (R = .421, p = .000, α = .05, two-tailed), and a significant negative relationship between age and ID theft victimization (R = -.185, p = .037, α = .05, two-tailed). A significant negative relationship exists between gender and classification (R = -.236, p = .008, α = .05, two-tailed) and a significant positive relationship exists between installation of PC anti-virus software and installation of PC anti-spyware software (R = .273, p = .002, α = .05, two-tailed).

Security behaviors subscale. Scores on the 7-item security behaviors scale ranged from 6 to 42. Security behavior scores among 24-30 year olds were slightly higher than the other groups. In terms of academic major, scores of fine arts majors and information technology majors were 3 points higher on average than scores of criminology majors. Mean scores for males and females were comparable. In terms of ethnicity, scores of those self-classified as "other" were 6+ points higher on average than scores of Hispanics, the lowest scoring group. In terms of academic classification, scores of participants self-classified as "other" were 3 points higher on average than the lowest scoring groups, juniors, freshmen and graduate students. Scores on the identity theft item were comparable. Scores of participants that don't know if anti-virus software is installed were 3 points higher on average than the lowest scoring group, those with anti-virus software installed, but not updated. Scores by anti-spyware installation averaged 3 points higher among those that don't have anti-spyware installed compared to the lowest scoring group, those that have anti-spyware installed, but not updated.

Security tools subscale. Scores on the 5-item subscale ranged from 6 to 30. The highest subscale scores by age group were among those aged 37+ years and those aged 18-23 years; 24-30 year-olds recorded the lowest mean subscale scores. Scores of information technology and criminology majors were 6 to 7 points higher than mean scores of "other" majors and natural science majors, the lowest scoring groups by major. Scores for males averaged 4% higher than female scores. With regard to ethnicity, scores for Asians and African-Americans averaged 4 to 5 points higher than Hispanics, the lowest scoring group. Scores for sophomores and those self-classified as "other" averaged 4 to 5 points higher than the lowest scoring groups, juniors and seniors. Scores for identity theft victims were 5 points higher than the lowest scoring group, those who did not know if they were identity theft victims. Scores for those with anti-virus software installed were 8 points higher than the lowest scoring group of participants, those that said it was not installed. Scores for those with anti-spyware software installed were 7 points higher than the lowest scoring group of participants, those that said it was not installed.

Table 2

Means and Standard Deviations – Security Attitudes scale and sub-scales.

		Security Attitudes Scale		Security Behaviors Sub-scale		Security Tools Sub-scale	
Variable	**Category**	***M***	***SD***	***M***	***SD***	***M***	***SD***
Age	18to23	85.97	11.278	32.27	3.222	18.35	4.895
	24to30	79.94	8.095	33.25	2.082	15.50	4.336
	31to36	85.17	16.469	31.75	3.696	16.92	6.082
	37+	84.13	11.813	31.88	3.834	19.63	5.449
Gender	Male	87.74	11.648	32.62	2.747	18.40	4.911
	Female	83.41	11.304	32.15	3.409	17.66	5.124
Ethnicity	White	84.70	11.542	32.37	3.220	17.81	5.076
	Hispanic	75.67	3.055	28.33	1.155	15.00	5.292
	African-American	85.88	12.856	33.13	1.458	19.38	4.502
	Asian	85.20	10.035	30.40	1.817	20.60	6.580
	Native American	83.50	14.849	31.50	.707	18.50	2.121
	Other	96.20	10.756	34.80	4.147	17.20	4.658
Classification	Freshman	83.57	11.976	31.93	3.290	18.53	4.974
	Sophomore	90.11	11.416	32.18	3.232	19.57	4.887
	Junior	80.68	10.149	31.79	2.347	15.53	4.247
	Senior	85.67	10.459	33.60	3.869	16.67	5.150
	Graduate	82.22	9.764	31.96	3.287	17.56	5.228
	Other+	91.13	15.533	34.38	1.408	19.38	5.208
Major	Education	85.79	13.309	32.33	3.088	18.71	4.796
	Humanities/soc sci.	82.82	8.198	32.27	3.089	17.14	4.622
	Healthcare	81.75	13.424	31.38	3.538	17.88	6.141
	Business	86.29	10.937	32.00	3.619	18.14	4.757
	Fine arts	90.60	11.546	33.60	2.966	18.40	5.367
	Criminology	82.63	9.870	30.63	2.825	19.88	4.086

	Natural science	82.62	10.211	33.46	2.696	16.46	5.010
	Information tech	98.50	7.609	33.50	2.429	22.00	4.050
	Other	84.75	13.011	33.00	3.247	15.67	5.549
Victim of ID theft?	Yes	89.55	13.765	32.09	3.590	20.09	5.108
	No	84.81	11.568	32.36	3.128	17.89	5.065
	Don't know	81.14	5.900	32.14	3.761	15.29	3.352
PC anti-virus installed?	Yes	85.85	11.884	32.39	3.090	19.04	4.620
	No	85.33	10.727	32.83	3.430	11.00	1.789
	Yes, not updated	80.92	10.501	30.67	4.008	14.83	3.689
	Don't know	79.57	7.721	33.71	1.976	13.14	5.610
PC anti-spyware installed?	Yes	87.57	11.283	32.61	3.102	19.52	4.458
	No	84.38	8.123	33.63	2.200	12.50	2.673
	Yes, expired	77.75	8.812	30.63	2.134	15.38	3.249
	Don't know	73.81	7.600	30.81	3.834	12.56	3.829

+participants earning enrolled in post-baccalaureate courses

**This table shows of mean survey and sub-scale scores by dependent variables*

Research Questions

Statistical analysis was performed on the data collected. The significance level was set at the 95% level (p > .05).

1. **Do security attitudes of college students significantly differ based on factors such as age, gender, ethnicity, classification level, academic major, identity theft victimization, installation of PC anti-virus software, or PC anti-spyware software?**

ANOVA tests were conducted to compare security attitude scores by the dependent variables of age, gender, major, ethnicity, ID theft victimization, and installation of anti-virus or anti-spyware programs, along with interaction effects between age and classification, age and identity theft victimization, gender and classification, and PC anti-virus and PC anti-spyware installation. No statistically significant interaction effects in security attitude scores were found between the dependent variables, age and classification $F(9,109)$ 1.663, p = .107, α = .05; age and identity theft victimization $F(4,117)$ .698, p = .595, α = .05; gender and ethnicity

$F(5,115)$ .890, p =.490, α = .05; or PC anti-virus installation and PC anti-spyware installation $F(6,114)$ .970, p = .449, α = .05.

Gender. Statistically significant differences in security attitude scores exist by gender, t (125) = 2.062, p = .041 (two-tailed), α = .05, 95% CI [.174, 8.49]. Male scores (M = 87.74, SD = 11.648) were significantly higher than female scores (M = 83.41, SD = 11.304).

Classification. Statistically significant differences in security attitude scores exist by classification $F(5,121)$ 2.639, p = .027, α = .05, R^2 = .167. Multiple comparison tests revealed no significant differences in mean scores by classification group.

Anti-spyware installation. Statistically significant differences in security attitude scores exist by installation of PC anti-spyware software $F(3,123)$ 9.044, p = .000, α = .01, R^2 = .18. Multiple comparison tests (Gabriel, 1987) revealed statistically significant differences in mean scores between participants that answered "Yes" to having anti-spyware installed and those that answered "Yes, but Expired" (MD = 9.818, p = .029, α = .05, 95% CI [.68, 18.96], and between those that answered "Yes" and those that answered "Don't know" (MD = 13.756, p = .000, α = .01, 95% CI [6.69, 20.82]. Participants that answered "Yes" to having anti-spyware installed scored significantly higher (M = 87.57, SD = 11.283) than those that answered "Yes, but expired" (M = 77.75, SD = 8.812), or "Don't know" (MD = 73.81, SD = 7.600).

No significant differences in security attitude scores exist by age $F(3,123)$ 1.255, p = .293, α = .05, major $F(8,118)$ 1.644, p = .120, α = .05, ethnicity $F(5,115)$ .894, p = .488, α = .05, identity theft $F(2,117)$ 1.669, p = .193, α = .05, or installation of PC anti-virus software $F(3,114)$ .361, p = .782, α = .05.

2. Do security behaviors of college students significantly differ based on based on age, gender, ethnicity, classification level, academic major, identity theft victimization, installation of PC anti-virus software, or PC anti-spyware software?

ANOVA tests were conducted to compare security behaviors sub-scale scores by the dependent variables of age, gender, major, ethnicity, identity theft victimization, and installation of anti-virus or anti-spyware programs, along with interaction effects by age and classification, age and identity theft victimization, gender and ethnicity, and PC anti-virus and anti-spyware software installation. No significant interaction effects exist between the age and classification $F(9,109)$ 1.124, p = .352, α = .05; age and identity theft victimization, $F(4,117)$ .242, p = .914, α = .05; gender and ethnicity, $F(5,115)$ .685, p = .635, α = .05; or PC anti-virus and anti-spyware software installation, $F(6,114)$ .370, p =.897, α = .05.

Anti-spyware installation. Statistically significant differences in security behaviors sub-scale scores exist by PC anti-spyware software installation $F(3,123)$ 2.788, p = .043, α = .05, R^2 = .064. Multiple comparison tests yielded no statistically significant mean differences between the groups.

No significant differences in security behaviors sub-scale scores exist by age $F(3,123)$ .639, p = .592, α = .05, gender t (125) = .799, p = .426 (two-tailed), α = .05, ethnicity $F(5,121)$ 2.146, p = .064, α = .05, classification $F(5,121)$ 1.456, p = .209, α = .05, major $F(8,118)$ .970, p = .463, α = .05, PC anti-virus software installation $F(3,123)$ 1.626, p = .187, α = .05, or identity theft victimization $F(2,124)$ .046, p = .955, α = .05.

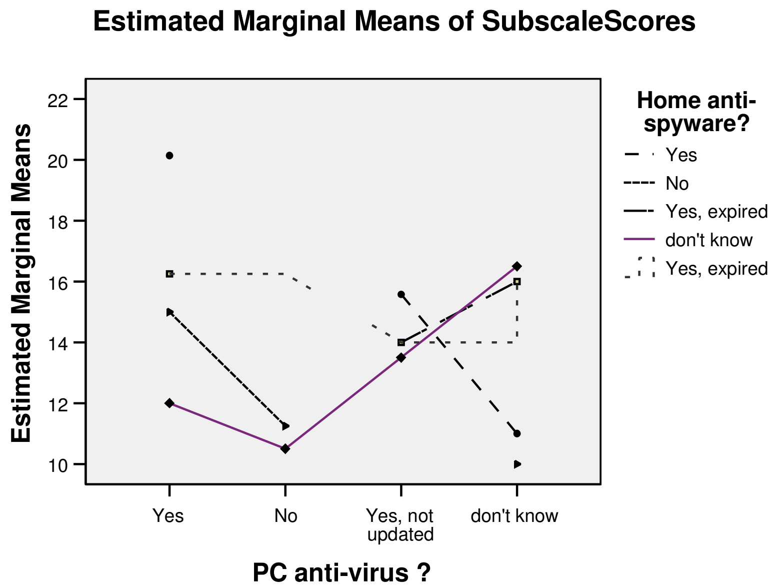
3. Do college students' use of security tools, such as anti-virus and anti-spyware software, significantly differ based on age, gender, ethnicity, classification level, academic major, identity theft victimization, installation of PC anti-virus software, or PC anti-spyware software?

ANOVA tests were conducted to compare security behaviors sub-scale scores by the dependent variables of age, gender, major, ethnicity, identity theft victimization, and installation of anti-virus or anti-spyware programs, along with interaction effects by age and classification, gender and ethnicity, and anti-virus software and anti-spyware software installation. No significant interaction effects exist between age and classification $F(9,109)$ 1.284, p = .254, α = .05, gender and ethnicity $F(5,115)$ .548, p = .740, α = .05.

OC10077

Anti-virus software and anti-spyware software installation. Statistically significant interaction effects exist between anti-virus and anti-spyware software installation $F(6,114)$ 2.543, $p = .024$, $\alpha = .05$, $R^2 = .118$ (Figure 2).

Figure 2: Interaction Plot



No significant differences in security tools sub-scale scores exist by age $F(3,123)$ 1.960, $p = .124$, $\alpha = .05$, gender $t(125) = .800$, $p = .425$ (two-tailed), $\alpha = .05$, ethnicity $F(5,121)$ .644, $p = .666$, $\alpha = .05$, classification $F(5,121)$ 1.967, $p = .088$, $\alpha = .05$, major $F(8,118)$ 1.248, $p = .277$, $\alpha = .05$, or identity theft victimization $F(2,124)$ 2.010, $p = .138$, $\alpha = .05$.

‘

DISCUSSION

The present study explores security attitudes and behaviors of college students, along with their use of security tools, and highlights end-user security awareness practices that institutions can employ to help students better protect personal information and data.

Security attitudes

The study revealed several interesting results in security attitude scores by each of the dependent variables.

Age. The highest security attitude scores by age were among the youngest participants, 18-23 year-olds ($M = 85.97$), while the lowest security attitude scores were among 24-30 year olds ($M = 79.94$). Of 18-23 year olds, those classified as "other" and sophomores achieved the highest scores ($M = 92.80$ and $M = 88.60$, respectively). Sophomores also comprised 27% of 18-23 year olds ($n = 91$). Graduate students comprised half of all 24-30 year olds ($n = 16$).

In terms of academic major, as would be expected, scores of information technology majors were among the highest (Jagatic, Johnson, Jakobsson & Menczer, 2007; Weber, Safonov, & Schmidt, 2008), but mean scores of fine arts majors were also among the highest in the present study. By contrast, healthcare majors reported the lowest mean attitude scores and mean scores of criminology majors were also among the lowest. Low attitude scores among criminology majors is a surprising result given that these students are destined for law enforcement and security-related careers that require security-conscious individuals. Low attitude scores for students destined for the healthcare industry are particularly troubling given the fact that this group will ultimately be responsible for protecting patient confidentiality and complying with healthcare laws, policies, and regulations, such as the *Health Insurance Portability and Accountability Act of 1996* (McClanahan, 2008). The results of the present study appear to indicate a possible need for security awareness training of college students in majoring in criminology and healthcare disciplines.

Male security attitude scores ($M = 87.74$, $SD = 11.648$) were significantly higher than female scores ($M = 83.41$, $SD = 11.304$). This finding appears to support prior research that there is a digital divide with regard to gender (Cooper, 2006; Jones, Johnson-Yale & Millermaier, 2009) and a lack of self-confidence in dealing with computer security issues (Jackson, 2007; Jackson, Ervin, Gardner, & Schmitt, 2001; Jokela & Karlsudd, 2007). In terms of ethnic minority groups, this study also found that the lowest mean security attitude scores by ethnicity were among Hispanics and Native Americans, but not African-Americans. This outcome appears to indicate that Hispanics are less security aware and supports Norum & Weagley's (2006) research findings that Hispanics were less likely to buy from a secure site than other ethnicities. The present study's findings appear to contrast survey results that found Hispanics to be more concerned about unauthorized access or misuse of personal information than whites or African-Americans (Unisys Security Index, 2010). In terms of academic classification, there appears to be a wide disparity of results as the lowest mean scores were among juniors and graduate students, while the highest scores were among sophomores, seniors, and those self-classified as "other" [5 of $n = 8$ were > age 30]. Freshmen mean scores were slightly below average mean attitude scores for the sample ($M = 85.02$). As one might expect, identity theft victims had the highest mean security attitude scores compared to non-victim participants or those who don't know if they are an identity theft victim.

Participants that have active anti-spyware software installed appear to be more security-conscious than those that either let their anti-spyware license expire or don't know if anti-spyware software is installed. However, 4 participants reported having no anti-virus or anti-spyware software installed. Perhaps this provides a partial explanation for the millions of PCs that are infected with viruses and/or malware worldwide (Young, 2009). Also, all participants that had anti-spyware installed on their computers usually had anti-virus software installed. A significant interaction effect exists between PC anti-virus installation and PC anti-spyware installation. Thus, PC anti-virus software installation goes hand-in-hand with PC anti-spyware software installation.

Security Behaviors and Security Tools

The security attitude scale was analyzed further by two of its subscales: security behaviors and security tools.

Age. The highest security behavior subscale scores by age were among those aged 24-30 year-olds (*M* = 33.25) and 18-23 year olds (*M* = 32.27), while 31-36 year-olds and 37+ year olds recorded the lowest mean security behavior subscale scores (*M* = 31.75 and *M* = 31.88, respectively). Interestingly, mean security tools subscale scores were highest among those aged 37+ (*M* = 19.63) and 18-23 year olds (*M* = 18.35). Security tools scores were lowest among 24-30 year-olds (*M* = 15.50) and 31-36 year olds (*M* = 16.92). While one would expect that maturity and experience would generally result in more security-conscious behaviors, the results of this study do not support that assumption; it appears that age does not necessarily portend wisdom when it comes to security behaviors, such as clearing Internet history/data, updating anti-virus and anti-spyware software, logging out of financial institution web sites, or installing and using security tools, especially with regard to the 31-36 year old age group. Also, while 24-30 year-olds more effectively exhibit security behaviors, the failure to complement those behaviors with the use of security tools may give this age group a false sense of security when it comes to protecting personal information and data. Future studies should be conducted to delve more deeply into behavioral profiles by age to determine if these results more widely occur through the general end-user population and to discover additional underlying factors that may contribute to these types of results.

Gender. While the differences in mean security behavior scores and security tools scores by gender were not statistically different, mean scores for males were higher than females on both subscales. This result is again in line with research by Jones, Johnson-Yale & Millermaier (2009) and Jokela & Karlsudd (2007) on gender differences with regard to security measures.

Ethnicity. With regard to ethnicity, African-Americans seem to be more security-conscious and utilize security tools more readily than Hispanics, a group that scored consistently lower than other groups on the two security subscales reported on herein.

Classification. In terms of academic classification, security behavior scores varied. The lowest security behavior subscale scores by classification were among juniors, freshmen and graduate students, while the highest scores were among those classified as "other" and seniors. With regard to the security tools subscale, the lowest mean scores by academic classification were among juniors and seniors, while the highest scores were among sophomores and those classified as "other." Since juniors recorded low mean scores for both the security behavior and security tools subscales, future studies should investigate contributing factors to this finding and determine if targeted security awareness training would improve this group's security behaviors.

Major. In terms of academic major, one would expect criminology majors to be among the most security-conscious of all college students; however, mean security behavior scores of this group were among the lowest by major. Security behavior scores for healthcare majors were also low, another a troubling finding. With regard to the use of security tools, mean subscale scores were highest for criminology majors. As with the prior findings on security behaviors and age, use of security tools may give criminology majors a false sense of security when it comes to protecting personal information and data. Not surprisingly, information technology majors routinely received some of the highest scores on both the security behavior and security tools subscales, supporting similar research findings (Jagatic, Johnson, Jakobsson & Menczer (2007); however, fine arts majors also recorded high security tools scores. Future research studies should investigate the factors attributed to security behaviors, as well as installation and use of security tools by academic discipline.

Identity theft victimization. Another surprising result was that identity theft victims recorded the lowest mean security behavior scores. It is puzzling that mean scores for victims of identity theft are not the highest group given that security-conscious behaviors might prevent loss of financial and personal information from occurring in the future. This finding may indicate a need for targeted security awareness training for identity theft victims. By contrast, the highest security tools subscale scores were among identity theft victims. As with the findings on security behaviors of 24-30 year olds and academic majors, the installation and use of security tools may give identity theft victims a false sense of security when it comes to protecting personal information and data.

Anti-virus software. In the present study, 80.3% of participants have anti-virus installed, slightly lower than the 88% of participants in Jokela & Karlsudd's (2007) study. Jokela & Karlsudd's (2007) study also reported that "quite a few students (5%)" do not know whether antivirus software is installed or updated. In the present study, a much higher percentage of students don't know if anti-virus software is installed or updated (14.1%) and another 15% of participants in the present study do not have anti-virus installed at all. Also, almost 15% of participants hardly ever or never run anti-virus software on their computers (n = 19) and only 44% do so always or most of the time. Further, 70.9% of participants hardly ever or never run anti-virus software on USB memory devices (n = 90) and only 11% do so always or most of the time. Perhaps this explains why corporate IT managers often restrict use of USB and other devices on corporate networks (Goodchild, 2008) and the concerns express about end-users by security professionals (Young, 2009).

Anti-spyware software. In this study, 74.8% of participants have anti-spyware installed, 6% of participants don't have anti-spyware installed, or do not know if it is installed (13%), and 6% have it installed, but it is expired. Also, almost 23.6% of participants hardly ever or never update anti-spyware software (n = 29), 22.8% hardly ever or never run anti-spyware software on their computers (n = 29), and only 40.2% update anti-spyware software always or most of the time, while 40.1% run anti-spyware always or most of the time. These findings clearly indicate a need for end-user training on the installation and use of security tools to better protect personal information and data.

On both the security behavior and security tools subscales, the highest mean scores were among those with anti-virus and anti-spyware installed (M = 19.04 and M = 19.52, respectively); the lowest mean scores were among those that don't have anti-virus or anti-spyware software installed (M = 11.00 and M = 12.50, respectively), or don't know if anti-virus software or anti-spyware software is installed (M = 13.14 and M = 12.56, respectively). Because, significant interaction effects between the PC anti-virus software installation and PC anti-spyware software installation variables exist indicating that the two security tools are closely-related constructs. Future studies should investigate additional factors that contribute to ineffective or non-existent user of security tools by college students.

CONCLUSION

The results of this study reveal a troubling disconnect among many college students with regard to effective security behaviors and application of security tools. The researchers agree with Okenyi & Owens' (2007) that a paradigm shift is needed towards continuous secure behavior. What actions should end-users and organizations take to protect personal information and data? For individuals, a multi-pronged approach is recommended to ensure secure Internet-related communication and access, including measures such as (Heinrichs, 2007; Luo & Liao, 2007; Mitnick, 2006):

- Installing and enabling a personal firewall;
- Regularly scanning computers, storage devices and email with updated anti-virus software;
- Regularly scanning computers and storage devices with updated anti-spyware software; and
- Using browser-enabled pop-up blockers and other built-in browser technologies.

The results of this study lend credence to Schneier's (1999) statement that "security it not a product, it's a process" (para. 6). Organizations should provide security awareness training (Allison & Deblois, 2008; Jagatic, 2007; Turner, 2007) to end-users about sound behavioral practices (Jones, 2008) to protect the confidentiality, integrity, and availability of personal and organizational data. These practices include end-user training on topics such as (Agee & Chang, 2009; Goodchild, 2009; Gorge, 2007; Luo & Liao, 2007; Mansfield-Devine, 2008; Mitnick, 2002):

- Social engineering methods and tools used by attackers;
- Spotting suspicious email messages and the risks of opening email attachments from unknown senders;
- Understanding risks of peer-to-peer file sharing networks and downloading unknown programs or files;
- Understanding risks of unsecure or unknown web sites and measures to identify and avoid these sites;
- Understanding risks of clicking on unknown email links, as well as risks associated with social networking sites and methods to protect personal information and data;
- Understanding the importance of regular data backups and data storage using external drives, CD/DVD's, or through virtualization technologies; and
- Understanding the importance applying software patches and security updates on a regular basis.

Network users should be trained how to identify email message threats before clicking on links or attachments (U.S. Department of Justice, n.d.), including examination of email headers and message source code to differentiate a suspicious message from a legitimate one (Goldsborough, 2008; TechRepublic, 2006), and to open a browser and manually navigate to the web site address rather than clicking on a messaged hyperlink. Network user training should also include strong password construction techniques, including the following elements (Thomas, 2005; Weber, Guster, Safonov, & Schmidt, 2008):

- 8 or more characters in length;
- Combination of letters, numbers, and symbols; and
- Mixed uppercase and lowercase letters, numbers, and symbols.

Organizations should also take proactive steps to reduce the likelihood of identity theft and personal data loss (Allison & Deblois, 2008). First, written password management guidelines should be adopted and widely dispersed, and regular training sessions should be conducted regarding the routine use of these guidelines at school and at home. Suggested password guidelines include (Mansfield-Devine, 2008; McDowell, Rafail, & Hernan, 2009):

- Change passwords often;
- Use different passwords for each account (especially financial institutions);
- Don't share passwords with others;
- Don't store passwords in the computer memory/history;
- Don't use words that can be found in a language dictionary;
- Use a mnemonic to remember a complex password;
- Never email passwords or reply to emails with passwords or other sensitive data; and
- Store password lists in a secure place.

Second, end-users should be taught how to construct a passphrase as a more secure alternative to passwords (Charoen, Raman, & Olfman, 2008; Weber, Guster, Safonov, & Schmidt, 2008**)**. A passphrase combines the first letters of a phrase coupled with numbers which substitute for words.

Third, training should also be provided to configure phishing filters and privacy settings in browsers and email clients, and to help users determine if a web site is legitimate, especially those using Secure Sockets Layer (SSL) or with bad SSL certifications (Goodchild, 2009; Krebs, 2006).

Lastly, educational institutions should also update privacy and security policies to include all IT resources (Allison & Deblois, 2008), while balancing the academic environment's need for openness with the need for individual privacy and data security (Agee & Yang, 2009). Institutions should also update end-user conduct policies to address standards of conduct on social networking sites (Gorge, 2007; Mitrano, 2006; Timm & Duven, 2008) without limiting students' freedom of expression. While computer usage policies are an integral part of computer security, a reliance on end-users to read policies may prove to be unreliable (Foltz, Schwager, & Anderson, 2008).

Despite training efforts, organizations cannot guarantee that end-users will practice the security measures after training (Welander, 2007). McMillan (2006) reported that 512 West Point cadets were sent a fake email that looked like it came from a colonel. The message stated that "there was a problem with your last grade report" and requested that the recipient click on a Web link and "follow instructions to make sure your information is correct" (para. 2). Even after hours of training, 80% of those students still clicked on the link. The "bad guys" are also getting more sophisticated in their use of social media to target individuals for fraud and identity theft (Collins, 2009). In response, social media companies are working to improve security and privacy of users. Recently, Facebook has taken steps to protect its users, such as (Zuckerberg, 2010). However, end-users must still proactively implement and monitor security procedures at social networking sites.

The results of this study bolster Mitnick's (2002) assertion that "the human factor is truly security's weakest link" (p. 3). When considering information security, no matter how sophisticated the technological solutions, the end-user must learn to accept responsibility and take proactive measures to stay educated about available security tools and procedures to protect personal data and information in both online and offline venues. People and systems must work together to minimize vulnerabilities (Welander, 2007). Educational institutions are the first line of defense to provide training to the end-user student population to begin to stem the tide of compromised computers that are be used by thieves and hackers to steal identities and wreak havoc on the Internet.

Limitations of the study

This study was exploratory in nature, is limited to the college student population (undergraduate and graduate students), and does not extend to those in the same age groups that are not enrolled in a 4-year college or in post-graduate studies. Also, additional factors may contribute to the results of the study to further explain attitudes and behaviors of undergraduate and graduate students.

Future research

While $\alpha = .69$ is acceptable for purposes of internal consistency and reliability, the security attitudes scale should be refined to increase internal consistency and reliability. Future studies should be conducted with larger sample sizes and expanded populations outside of an academic setting in comparable groups, and including university staff and faculty, to determine if this study's results can be replicated. Also, future research should investigate age, gender and ethnic differences with regard to security attitudes and behaviors, as well as end-users' use of additional security tools, such as pop-up blockers, browser-based filters, social network and IM privacy settings, and email junk mail filtering.

REFERENCES

The College Board. (2010). *College Search,* Retrieved May 24, 2010 from http://collegesearch.collegeboard.com

Agee, A.S. & Yang, C. (2009, July/August). Top 10 IT issues 2009. *Educause Review*, 46-58.

Allen, I.E. & Seaman, J. (2009). Learning on demand: Online education in the United States. *The Sloan Consortium*. Retrieved May29, 2010, from http://www.sloan-c.org/publications/survey/index

Allison, D.H., & DeBlois, P.B. (2008, May/June). Top 10 IT issues 2008. *Educause Review, 43*(3), 1622-1629.

Ashraf, B. (2009). Teaching the Google-eyed YouTube generation. *Education + Training, 51(5/6),* 343-352

OC10077

Babbie, E. (1990). *Survey research methods* (2nd ed.). Belmont, CA: Wadsworth Publishing

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday (Online)*, *11*(9), p. 1. Retrieved from OmniFile Full Text Mega database.

Bell, D.E. (1973, December). Secure Computer Systems: A Refinement of the Mathematical Model, MTR- 2547, Vol. III, *The MITRE Corporation*. Bedford, MA (ESD-TR-73- 278-III).

Biba, K.J. (1977). Integrity Considerations for Secure Computer Systems. *The MITRE Corporation*. Bedford, MA.

Brodkin, J. (2008, July). One in four firms block Facebook. *NetworkWorld*, p. 20.

Charoen, D., Raman, M., & Olfman, L. (2008). Improving end user behaviour in password utilization An action research initiative. *Systemic Practice and Action Research*, *21*(1), 55-72.

Chueng, W. & Huang, W. (2005). Proposing a framework to assess Internet usage in university education: An empirical investigation from a student's perspective. *British Journal of Educational Technology*. *36*(2), 237–253

Clark, D.D., & Wilson, D.R. (1987). A comparison of commercial and military computer security policies, pp. , 184-194.. *Proceedings of the 1987 IEEE Symposium on Security and Privacy, Oakland, California, USA, April 1987*. Los Alamitos, CA: IEEE Computer Society Press.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Collins, H. (2009, December). 2010 Cyber-threat forecast sees hacks growing in sophistication and reach. *Government Technology,* Retrieved January 6, 2010 from http://www.govtech.com/gt/articles/735777

Computer Security Institute. (2009). *14th annual CSI/FBI computer crime and security survey* (S. Peters, In Ed.), Retrieved May 20, 2010 at http://gocsi.com/survey

Cooper, J. (2006).The digital divide: The special case of gender. *Journal of Computer Assisted Learning*, 22, 320–334

Ellison, Nicole. (2007). *Facebook Use on Campus: A Social Capital Perspective on Social Network Sites*. Paper presented at the ECAR Symposium, Boca Raton, FL, December 5-7, 2007. Retrieved from http://www.educause.edu/ecar

Federal Trade Commission. (2010, February). *Consumer sentinel network data book*. Retrieved May 20, 2010, from www.ftc.gov

Fogel, J. & Nehmad, E. (2008). Internet Social Networking Communities: Risk Taking, Trust, and Privacy Concerns. *Computers in Human Behavior*, 25, 153-160

Foltz, C.B., Schwager, P.H., & Anderson, J.E. (2008). Why users (fail to) read computer usage policies. *Industrial Management & Data Systems*, *8*(6), 701-712.

Gabriel, K.R. (1987). A simple method of multiple comparisons of means. *Journal of the American Statistical Association*, 73, 724-729.

Gilroy, M. (2010). Higher Education Migrates to YouTube and Social Networks. *Education Digest: Essential Readings Condensed for Quick Review*, *75*(7), 18-22. Retrieved from ERIC database.

Goldsborough, R. (2008). Deciphering email headers. *Tech Directions*, *67*(8), p. 7.

Goodchild, J. (2009, April). 5 security flubs users makers when browsing the web. *Computer Security Officer*. Retrieved June 1, 2010 from http://www.csoonline.com/article/print/489738

Goodchild, J. (2008, August). Web 2.0 Applications and sites (and security concerns). *Computer Security Officer*. Retrieved October 7, 2008, from http://www.csoonline.com/article/print/442215

Gorge, M. (2007). Security for third level organizations and other educational bodies. *Computer Fraud & Security*, 7, 6-9.

Gorsuch, R. L. (1983). *Factor Analysis*. Hillsdale, NJ: Lawrence Erlbaum.

Graham, G.S., and Denning, P.J. (1972). Protection-principles and practice. *AFIPS Conference Proceedings*, Vol. 40. Montvale, N.J.: SJCC, AFIPS Press, 417-429.

Green, K. (2007). The 2007 campus computing survey. *The Campus Computing Project*. Retrieved May 22, 2010, from http://www.campuscomputing.net/sites/www.campuscomputing.net/files/2007-CCP_0.pdf

Hall, M. (2005). Secure the people. *Computerworld.* Retrieved May 20, 2010, from http://www.computerworld.com/securitytopics/security/story/0,10801,100448,00. Html

Harwood, M. (2008, May). Academic culture, understaffing blamed for higher ed IT insecurity. *Security Management.* Retrieved November 20, 2008, from www.securitymanagement.com/

Hawkins, B.L., & Rudy, J.A. (2008). *EDUCAUSE Core Data Service: Fiscal Year 2007 Summary Report.*. Retrieved May 22, 2010, from http:// net.educause.edu/apps/coredata/reports/2007/

Heinrichs, A.M. (2007, Feb.). Computer dangers that lurk within. *Pittsburgh Tribune-Review*, p. J5.

Identity Theft Resource Center. (2009). Identity theft: The Aftermath 2008. May 26, 2010, from http://www.idtheftcenter.org/artman2/publish/m_press/Identity_Theft_The_Aftermath_2008.shtml

InfoWorld. (2010, June). Macs under attack by high-risk spyware. *Infoworld Tech Watch*. Retrieved June 3, 2010, from http://www.infoworld.com/print/125698

Internet Crime Complaint Center (National White Collar Crime Center and The Federal Bureau of Investigation). (2009). *Internet Crime Report*. Retrieved March 13, 2010 from www.ic3.gov

Jackson, L. A., Ervin, K. S., Gardner, P. D., Schmitt, N. (2001a). Gender and the Internet: Women communicating and men searching. *Sex Roles*, 44, 363–379.

Jackson, M. (2007). Exploring gender, feminism and technology from a communication perspective: An introduction and commentary. *Women's Studies in Communication*, *30*(2), 149–156.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., & Menczer, F. (2007, October). Social phishing. *Communications of the ACM, 50*(10), 94-100.

Javelin Strategy & Research. (2009, February). *2009 Identity Fraud Report: Consumer Version*, Retrieved May 20, 2010 from www.javelinstrategy.com

Jokela, P., & Karlsudd, P. (2007). Learning with security. *Journal of Information Technology Education*, 6, 291-309.

Jones, J.G. (2008). Issues and concerns of directors of postsecondary distance learning programs regarding online methods and technologies. *The American Journal of Distance Education*, 22, 46–56.

Jones, S., Johnson-Yale, C., Perez, F.S., & Schuler, J. (2007). The internet landscape in college. *Yearbook for the National Society for the Study of Education, 106*(2), 39-51.

Kirkwood, A., & Price, L. (2005). Learners and learning in the twenty-first century: What do we know about students' attitudes toward and experiences of information and communication technologies that will help us design courses? *Studies in Higher Education*, 30, 257–274.

Krebs, B. (2006, Feb.) It's 10 p.m. Do you know where your identity is? *Popular Mechanics*. p. 54.

Lieberman Research Group. (2010). *Unisys Security Index: United States 31 March 2010*. Retrieved May 20, 2010 from http://www.unisyssecurityindex.com/us/

Livermore, A. (2006, July). College students at increased risk of identity theft; survey shows computer security habits are lacking. *BusinessWire*, Retrieved August 1, 2006, from LexisNexis Academic.

Luo, X. & Liao, Q. (2007**)**. Awareness education as the key to ransomware prevention. *Information Systems Security,* 16, 195–202.

Mansfield-Devine, S. (2008, November). Anti-social networking: Exploiting the trusting environment of Web 2.0. *Network Security,* 4-7.

McClanahan, K. (2008). Balancing good intentions: Protecting the privacy of electronic health information. *Bulletin of Science, Technology & Society*, *28*(1), 69-79.

McCumber, J. (1991). Information Systems Security: A Comprehensive Model. *Proceedings of the 14th National Computer Security Conference, 1991*. Retrieved June 1, 2010, from: www-static.cc.gatech.edu/classes/AY2008/.../InfoSystemsSecurityModel.ppt

McDowell, M., Rafail, J., & Hernan, S. (2009). National Cyber Alert System **-** Cyber Security Tip ST04-002. *United State Computer Emergency Readiness Team. Carnegie Mellon University*. Retrieved May 22, 2010, from http://www.us-cert.gov/cas/tips/ST04-002.html

McMillan, R. (2006, November). Security group ranks human error as top security worry. *NetworkWorld.* Retrieved October 7, 2007, from http://www.networkworld.com/news/2006/111506-security-group-ranks-human-error.html

McQuade, S. C. (2007). We must educate young people about cybercrime before they start college. *Chronicle of Higher Education*, *53*(18), B29-B31.

Mitnick, K. (2006, June). *Mitigating malware in userland*. Retrieved January 12, 2009, from http://www.appsense.com/files/documentation/AppSense-White-Paper-Mitnick.pdf

Mitnick, K. (2002). *The Art of Deception*. Hoboken, NJ: John Wiley & Sons.

Mitrano, T. (2006, Nov.,/Dec.). A wider world: Youth privacy, and social networking technologies. *EDUCAUSE Review,* 16–28.

Nachmias, D. and Nachmias, C. (1987). Research methods in the Social Sciences. New York: St. Martins Press.

Nackerud, S. & Scaletta, K. (2008). Blogging in the academy. *New Directions For Student Services*, 124, 71-87.

National Security Telecommunications And Information Systems Security Committee. (1994, June). National *Training Standard For Information Systems Security (Infosec) Professionals (No. 4011)*. Retrieved May 20, 2010, from http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

Nielsen/NetRatings (2009). *Social Networks & Blogs Now 4th Most Popular Online Activity, Ahead of Personal Email.* Retrieved June 15, 2009, from http://enus.nielsen.com/main/news/news_releases/2009/march/ social_networks

Norum, P. S. &Weagley, R. O. (2006–2007). College students, Internet use, and protection from online identity theft. *Journal of Educational Technology Systems*, 35, 45–59.

Okenyi, P.O., & Owens, T.J. (2007). On the anatomy of human hacking. *Information Systems Security,* 16, 302–314.

Pfleeger, C.P. (1989). *Security in Computing*. Upper Saddle River, NJ: Prentice-Hall.

Rosen, D. & Nelson, C. (2008). Web 2.0: A new generation of learners and education. *Computers in the Schools*, *25*(3–4), 211-224.

Salas, G. & Alexander, J.S. (2008). Technology for institutional enrollment, communication and student success. *New Directions for Student Services,* 124, 103-116.

Schneier, B. (1999, Dec. 15). *Crypto-Gram Newsletter*. Retrieved May 20, 2010, from http://www.schneier.com/ crypto-gram-9912.html#1

Stallings, W., & Brown, L. (2008). *Computer Security: Principles and Practice*. Upper Saddle River, NJ: Prentice Hall.

Jacob, S.M., & Issac, B. (2008, January). Mobile technologies and its impact – An analysis in higher education context. *International Journal of Interactive Mobile Technologies*. *2*(1), 10-18.

TechRepublic. (2006). *Examine e-mail headers to determine their real origin*. Retrieved May 1, 2006, from http://techrepublic.com.com/5102-1009-6056367.html

The Campus Computing Project (October, 2007). *The Campus Computing Report*. Retrieved May 22, 2010, from www.campuscomputing.net\

The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act. 20 U.S.C.A. § 1092(f). (1990).

Thomas, B. (2005). Simple formula for strong passwords (SFSP) tutorial. SANS Institute, Retrieved May 20, 2010, from http://www.sans.org/reading_room/whitepapers/authentication/simple-formula-strong-passwords-sfsp-tutorial_1636

Timm, D.M., &. Duven, C.J. (2008). Privacy and social networking sites. *New Directions for Student Services*, 124, 89-102.

Turner, M.L. (2007, September). Training your staff to protect SIS data. *University Business*, 61-64.

U.S. Department of Defense. (1983). *Trusted Computer System Evaluation Criteria*. DoD 5200.28-STD. Retrieved May 28, 2010, from http://csrc.nist.gov/publications/history/dod85.pdf

U.S. Department of Justice. (n.d.). *Special report on "phishing"*. Retrieved January 12, 2009, from http://www.usdoj.gov/criminal/fraud/docs/phishing.pdf

Weber, J.E., Guster, D., Safonov, P., & Schmidt, M.B. (2008). Weak password security: An empirical study. *Information Security Journal: A Global Perspective*, 17, 45-54.

Welander, P. (2007, November). Cybersecurity: The human factor. *Supplement to Control Engineering*, 2-3.

Weiss, M. & Hanson-Baldauf, D. (2008). Email in academia: Expectations, use and instructional impact. *Educause Quarterly*, 1, 42-50.

Whitman, M.E., Mattord, H.J. (2009). *Principles of Information Security* (3rd ed.). Boston, MA: Thomson Course Technology.

Young, J. (2009, May). Top 10 threats to computer systems include professors and students. *Education Digest, 74*(9), 24-27.

Ziobron, B. (2003, July). Keeping campus networks safe and secure. *Cabling Installation & Maintenance*, 27-30.

Zuckerberg, M. (2010, May). *Making Control Simple.* Message posted to http://blog.facebook.com/blog.php?post=391922327130

ORDERED THROUGH Interlibrary loan:

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476-490. doi:10.1016/j.cose.2009.01.003.

OC10077