POST-SECONDARY EDUCATION NETWORK SECURITY: RESULTS OF ADDRESSING THE END USER CHALLENGE

David Andersson, Karl Reimers, Charmaine Barreto

Dept. of Information Technology, American Public University System (UNITED STATES)
Tillman School of Business, University of Mount Olive (UNITED STATES)
Farquhar College of Arts and Sciences, Nova Southeastern University (UNITED STATES)

Abstract

Today, irrespective of what career field a college graduate enters, personal computer literacy is a given requirement. Personal computer security literacy is rapidly becoming as important as office application software literacy for today's typical employee. Coping with technology security issues is not something that can be simply accomplished through personal experiences. Currently, research of young adults and students indicates that 7 out of 10 frequently ignore IT policies, and 3 of 5 believe they are not responsible for protecting information and devices. In the past, fallout from poor IT habits was buffered by the IT department's iron control over the infrastructure. There were no smartphones, or applications such as Facebook, Twitter or Google to become a security hole as there are today. Schools have a vested interest in "biting the bullet" by assigning some resources to the issue and ensuring that their students receive a minimum of personal computer security training just as they should ensure their graduates are computer literate in the use of business application software for word processing, spreadsheets, presentations and database access. This is because: a) the students are effectively part of the institutions networks as end-users with needs that must be addressed, b) preparing students for life after college is an implied and accepted part of the role of the educational institution, and c) students are the schools' "product" and represent the school to everyone they interact with after graduation. Just as business organizations are increasingly requiring their members to undergo annual or semi-annual PC-based ethical and security awareness training, educational institutions may wish to consider emulating this for their staff, faculty and students on the topic of personal computer end user security best practices. The MIS program at the University of Mount Olive is addressing the challenge of technology/business computer security literacy by implementing a new e-learning solution. A customized, self-paced, web-based end user digital security awareness tutorial was created. This learning activity reinforces student retention of the material presented by providing questions at the end of each learning module to reinforce learning. As students become proficient at using security best practices, their proficiency, confidence, and student engagement in the class material increases. Since more classes require the use of computing technology in completing assignments, students enhance their progress throughout their undergraduate program and increasing the probability of program completion. The course instructor is able to shift their time and energy from "putting out fires" to focusing on higher-level feedback on assignments and administrative functions. Since more classes require the use of digital technology, both hardware and software, in completing assignments, students take these digital best practices for safety and security to other situations and courses, enhancing their progress throughout their undergraduate program and increasing the probability of program completion. A survey was developed to study and quantify the student's perception of the usefulness of an online PC security end-user tutorial. Results of this study suggest that regular exposure to a PC security tutorial can positively impact student success and program completion - a key aspect of program quality. As programs come under increasing scrutiny in terms of measuring learning outcomes, completion rates, and student success, faculty may wish to consider the advantages of regular exposure to PC security tutorials for their students.

Keywords: education, information technology, organizational change, program quality, professional development, network security, workplace competencies.

1 INTRODUCTION

Recent research finds that seven out of ten young employees frequently ignore IT policies, and one in four is a victim of identity theft before the age of 30. The students that will comprise the next generation of employees will be expected to easily understand network access, mobile device freedom, social media, and different work lifestyles. This behavior heightens personal and organizational risk amid a complex threat landscape [1]. The desire for on-demand access to
information is so ingrained in the incoming generation of employees that many young students/professionals will take extreme measures to access the Internet, even if it compromises their company or their own security. Such behavior includes secretly using neighbors’ wireless connections, sitting in front of a business to access free Wi-Fi networks, and borrowing other people's devices without permission [1].

Effective personal computer security is rapidly becoming as important as office application software literacy for the average employee. It is increasingly not something that can be simply “picked up somehow”. Colleges and Universities have a vested interest in “biting the bullet” and ensuring that their students receive a minimum of personal computer security training just as they should ensure their graduates are computer literate in the use of business application software for word processing, spreadsheets, presentations and database access. This is because: a) the students are effectively part of the institution’s networks as end-users, and b) preparing students for life after college is an implied and accepted part of the role of the educational institution.

1.1 Significance of the problem

The explosion of the Internet, though it has benefited society a lot, has brought along with it newer ways to commit frauds, scams, robberies, and so forth. Network fraud has grown as the Internet has become popular. As one CSI survey found [2], such crime peaked to record highs in 2001 to $3,149,000 per respondent, before everyone realized the importance of network security. Network related fraud, though, has come down sharply to $269,000 per respondent in 2008 [2] due to various measures being taken; however, it still causes substantial losses to various organizations. The CSI survey [2] also found an increase in unauthorized access of networks from 25% in 2007 to 29% in 2008 despite a drop in all other types of incidents. The Internet Crime Compliant Center (IC3) in their 2009 Internet Crime Report [3] found that the increase in complaints from 2008 to 2009 was 23%. The IC3 report [3] indicates that of the top five categories of offenses reported to law enforcement during 2009, non-delivered merchandise and/or payment occurred 19.9% of the time; identity theft, 14.1%; credit card fraud, 10.4%; online auction fraud, 10.3%; and computer fraud (destruction/damage/vandalism of property), 7.9%.

1.2 Student end user computer security concerns

Every person should care about computer security because an attacker can not only access the documents stored in the computer but also can use the computer to send forged messages and launch attacks on other computers. Arian [4] defines computer security as the process of preventing and/or detecting unauthorized use of your computer. With increasing software complexities it has become difficult to completely secure computer systems against vulnerabilities. An attacker can use these vulnerabilities to get into a computer and launch an attack. Unless taught, the typical end user has limited awareness of how to protect themselves; they do not know how to use proper settings (or “least privileged user account”) for the software programs so that an attacker can not use them to access their computer [5].

In order to create awareness and prevent computer related crime the FBI has published guidelines on protecting computers [6]. These guidelines give some key steps to protecting one’s computer, and include the following suggestions:

- Keep the firewall always on
- Install and keep antivirus software updated
- Install and keep antispyware software updated
- Keep the operating system updated
- Be careful of what is being downloaded
- Turn off your computer when not in use

Substantiating that students do not simply “pick up” good PC end user habits before they enter college, Cisco’s 2011 Annual Security Report found that about one in four college students and employees experiences identity theft before the age of 30. The following findings provide insight into the frequency of identity theft among this generation [1]:

- Adhering to IT policies. Seventy percent of employees admitted to breaking policy with varying regularity. This included the belief that they (employees) were not doing anything wrong, a
perceived need to access unauthorized programs and applications to get their job done, a perception that the policies are not enforced, they do not have time to think about policies when they are working, adhering to the policies is not convenient, they forget to do so, or their bosses aren't watching them. A staggering sixty-one percent reported believing they are not responsible for protecting information and devices, believing instead that IT and/or service providers are accountable.

- Risky behavior. Fifty-six percent of employees surveyed reported they have allowed others including family, friends, coworkers, and people they did not know to use their computers without supervision. Eighty-six percent of college students were more likely than young employees to engage in risky online behavior such as allowing others to use their computer unsupervised, leaving personal belongings and devices unattended in public while getting something to eat or drink at a cafe or going to the restroom, asking a neighbor for access to a computer or the Internet or accessing a neighbor's wireless connection without permission.

- Security and online privacy. Thirty-three percent of college students don’t think about privacy and do not mind sharing personal information online.

1.3 The digital generation gap: student end user computer security concerns

The digital generation gap is also an issue for post secondary IT management. Today’s college students have not only grown up using computers and other digital devices, they consider access to the Web and social networking services a basic right. According to Cisco's annual survey [1], which included 2,800 young adults, students, and employed white collar employees across 14 countries, 7 out of 10 young employees frequently ignore IT policies, and 3 of 5 employees believe they are not responsible for protecting information and devices, believing instead that IT and service providers are accountable.

Of those who were aware of IT policies, 7 of every 10 employees worldwide admitted to breaking policy with varying regularity. Among many reasons the most common was the belief that employees were not doing anything wrong (33 percent); 1 in 5 cited the need to access unauthorized programs and applications to get their job done, while 19 percent admitted the policies are not enforced [1]. Generation X and Y students and employees may have been careless about following rules in the past, but fallout from those attitudes was buffered by the organizations IT department’s tight control over the infrastructure. Previously, Facebook, Google+, smartphones, and Twitter were not present to become a security hole. Dan Lichter, Director of Systems and Networks Infrastructure at Saint Xavier University, reports that college student immediately begin deploying ad hoc, unapproved network devices in the college dorms with no regard for the implications of what they are doing; yet, they complain loudly and frequently until the problems caused by their actions are fixed, representing a major drain on his resources [7].

Further, we are seeing modes of attack on corporate networks shifting away from mass probing of large numbers of computers to social engineering thrusts targeted at particular individuals. An employee or student who is active on social networking sites can carelessly divulge where they work or what they know and will be noticed and targeted. Hackers can use them to gain entry into the system and work their way up to more senior people and parts of the network containing sensitive information [8].

2 PROPOSED SOLUTION

Several regional focus groups consisting of major employers from New Bern, Greenville, and Wilmington, North Carolina [9] disclosed that students needed more training with MS Office productivity tools as well as having an overall awareness of technology and its appropriate use in the workplace. In addition, the authors of this paper attended many Tillman School of Business meetings whereby student deficiencies or misconduct (e.g., not knowing how to use basic application software, the lack of knowledge in end-user computer security, using the internet to plagiarize, etc.) were discussed. Further, the IT Department at the University of Mount Olive was engaged regularly in alerting faculty, staff, and students via email, about compromising passwords and phishing schemes.

Just as business organizations are increasingly requiring their members to undergo annual or semi-annual PC-based ethical and security awareness training, educational institutions may wish to consider emulating this for their staff, faculty and students on the topic of personal computer end user security best practices. The MIS program at the University of Mount Olive addressed the challenge of
technology/business computer security literacy by implementing a new e-learning solution to augment a traditional course on the topic of computer security. The e-learning solution consists of a customized, self-paced, web-based end user digital security awareness tutorial.

2.1 Solution process

The computer security tutorial was updated and worked upon until it reflected current computer security issues and skills. Content and pedagogy expertise helped insure that the fundamental end-user computer security tutorial was well designed; and, all three of the authors instruct undergraduate computer security courses. Furthermore, two of the authors hold professional certifications (i.e., CompTIA’s Security + and CIW Security Professional which are international, vendor-neutral certifications that demonstrate competency in network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control and identity management, and cryptography) in end-user computer security. Similar to the office applications tutorial which was designed in 2013 [10], a customized case study utilizing a project management framework combined with the SDLC was integrated into a CIS capstone class [11]. In the former study, the project consisted of three teams - two teams working on separate projects and an Information/Technology (IT) team that fulfilled a support function and who acted as a liaison between the project managers and the instructor. This type of operational teamwork is highly effective in producing a successful capstone experience [12]. However, in modernizing the computer security tutorial, a more traditional approach using only project managers was employed. Regardless of the inclusion of an IT team, a good capstone course is one that captures both the business school course foundations while achieving a lasting/meaningful solution to a real-world problem. Thus, students have increased motivation to achieve a successful project using a real problem and the results of the project could be used by them to enhance their resumes.

2.2 Potential constraints

All students are required to have Internet access; they are mandated by administration to have Internet access because of email accounts and online course supplements (i.e. Moodle course shells). UMO computer labs have broadband access at all locations (i.e., Raleigh, New Bern, Mount Olive, Wilmington, and Jacksonville). In addition, the Mount Olive location has military students at Seymour Johnson Air Force Base who are often get deployed around the world. All students are required to have access to personal computers. This is mandated to ensure a common learning platform for the entire class. Moreover, because the tutorial acts as aggregator for other non-copyrighted web-based tutorials, maintenance of the external hyperlinks is a crucial to a favorable user experience. Browser compatibility with any web-based tutorial can be problematic because of frequent browser updating and the expansion of new mobile operating systems (e.g., Android Jellybean, iOS6, etc.). Currently, the tutorial is compatible with all major PC browsers. Fig. 1 [13] and Fig 2 [13] display the market share of the browsers for PCs and for mobile computing.

![Fig. 1: December 2013 market share of major browsers for PC’s. [12]](image-url)
3 DATA ANALYSIS

3.1 Demographics

A voluntary exit survey was completed by students to determine their perceived efficacy of the online security tutorial on computer security topics. 85 respondents participated in the survey study. The sample was fairly evenly split across males and females. Furthermore, more than half of the sample consisted of traditional students in the 18-22 age bracket. Finally, roughly half of the sample respondents identified as White whereas a quarter of the sample respondents identified as Black or African American. The sample was representative of the larger population of typical college students in a four-year degree programs. Table 1 below provided more details of the sample demographics.

<table>
<thead>
<tr>
<th>Gender</th>
<th>#</th>
<th>%</th>
<th>Age</th>
<th>#</th>
<th>%</th>
<th>Race</th>
<th>#</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>36</td>
<td>42.35%</td>
<td>18-20</td>
<td>44</td>
<td>51.76%</td>
<td>American Indian/Alaska Native</td>
<td>1</td>
<td>1.18%</td>
</tr>
<tr>
<td>Male</td>
<td>47</td>
<td>55.29%</td>
<td>21-22</td>
<td>9</td>
<td>10.59%</td>
<td>Hawaiian/Other Pacific Islander</td>
<td>1</td>
<td>1.18%</td>
</tr>
<tr>
<td>Undisclosed</td>
<td>2</td>
<td>2.35%</td>
<td>23-29</td>
<td>9</td>
<td>10.59%</td>
<td>Asian or Asian American</td>
<td>3</td>
<td>3.53%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>30-39</td>
<td>11</td>
<td>12.94%</td>
<td>Black or African American</td>
<td>20</td>
<td>23.53%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>40-49</td>
<td>5</td>
<td>5.88%</td>
<td>Hispanic or Latino</td>
<td>9</td>
<td>10.59%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50+</td>
<td>4</td>
<td>4.71%</td>
<td>Non-Hispanic White</td>
<td>42</td>
<td>49.41%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Blanks</td>
<td>3</td>
<td>3.53%</td>
<td>Prefer not to answer</td>
<td>9</td>
<td>10.59%</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100.00%</td>
<td></td>
<td></td>
<td>100.00%</td>
</tr>
</tbody>
</table>

4 RESULTS

The survey results indicate that a quarter of the respondents never used the computer security tutorial and were excluded from this analysis. This brought the usable sample size down to 63 respondents. For future studies, it would be useful to develop an alternate questionnaire to probe further into why students chose not to use the tutorial. This will help with developing a more efficacious security tutorial in the future. The survey results show that more than three quarters of the respondents used the security tutorial 1-2 times whereas a fifth of the respondents used the security tutorial three or more times. See Fig. 3 below for details.
Fig. 3: How many times did the students use the computer security tutorial?

Furthermore, over half of the respondents reported using the security tutorial for anywhere from 15 minutes to 90 minutes. Together, one might conclude that most students were not only intrigued enough to use the security tutorial, but they appeared to be spending a decent amount of time using the security tutorial.

Fig. 4: How long were the sessions when the students used the computer security tutorial?

Finally, about three quarters of the respondents perceived the tutorial to be easy to use. This may explain why so many were incentivized to keep on using the security tutorial beyond the first use. Fig. 5 shows student perception of the ease of the computer security tutorial.

Fig. 5: Students' perception of the ease of use of the computer security tutorial.
4.1 Overall Usefulness of Security Tutorial

Students appeared to find the security tutorial useful and helpful for the purpose of assimilating content on computer security. This is evidenced by over 70% agreeing or strongly agreeing that the security tutorial helped them better understand computer security as well as agreeing that the computer security tutorial as a whole, was helpful. See Fig. 6 and 7.

![The computer security tutorial helped gain a better understanding of computer security](image1)

![The computer security tutorial is helpful](image2)

Fig. 6: The computer security tutorial; helped gain a better understanding of computer security.

Fig. 7: How helpful the students perceived the computer security tutorial.

Furthermore, over half of the respondents perceived the security tutorial to have helped them complete their course assignments in a safe manner. This finding is especially important because it lends credibility to the assertion that the contents of tutorial (one of which is computer safety) was being assimilated and applied in real time. See Fig. 8.
Finally, the fact that approximately 70% of the respondents would recommend the computer security tutorial to their peers helps ascertain that the tutorial was well received and perceived to be useful. See Fig. 9.

4.2 Perceived usefulness of security tutorial on computer security topics

As reported earlier in this paper, respondents were asked to judge how well the computer security tutorial helped them increase their proficiency in a computer security sub-topic. Specifically, these subtopics included password proficiency, windows update, social networking, firewalls, ethics of security, spam, antivirus, wireless networking, and mobile computing. At least 50% of the respondents found that the computer security tutorial helped increase their proficiency in all ten subtopics. For instance, approximately 55% of the respondents agreed or strongly agreed that they perceived an increase in knowledge about social networking as a result of having used the security tutorial. Similarly, about 60% of the respondents agreed or strongly agreed that they perceived an increase in knowledge about wireless networking as a result of having used the security tutorial. Fig. 10 provides details of the percentages of respondents who agreed or strongly agreed that the computer security tutorial helped them increase their proficiency on the subtopic.
4.3 Correlations between increase in proficiency on a topic and usefulness of the tutorial on the same topic

In the survey, respondents were asked to reflect on their usage of the computer security tutorial along two dimensions. They were first asked if the security tutorial had increased their proficiency in a specific computer security subtopic such as passwords or conducting backups. For the same subtopic, they were also asked to reflect on whether they found the security tutorial component on that subtopic to be helpful. For example, using a Likert scale of 1 – 6 where 1 indicated that the respondent strongly disagreed with the statement whereas a 6 indicated that the respondent strongly agreed with the statement, a respondent was asked if “Using the Computer Security tutorial increased my proficiency with passwords” as well as if “Overall, I found the Password section of the Computer Security tutorial to be helpful.”

Our intent was also to ascertain if respondents who perceived the security tutorial to be helpful (useful) on a subtopic also perceived an improvement in their proficiency on the subtopic. This is our proxy measure to ascertain the efficacy of the security tutorial. The study shows this to be true as evidenced by very high correlations (Pearson r values) between the proficiency measure and the helpfulness measure for the same subtopic. For instance, the correlation between perceived increase in proficiency in ethics due to the security tutorial and perceived helpfulness of the ethics section of the security tutorial was $r = 0.95$. Similarly, the correlation between perceived increase in proficiency in firewalls due to the security tutorial and perceived helpfulness of the firewalls section of the security tutorial was $r = 0.89$.

5 CONCLUSION

The majority of respondents found the End-User Computer Security tutorial to be helpful (97.9%) and would recommend using the End-User Computer Security tutorial in future sections of the class (95.7%). As noted previously, student engagement in the learning process is a key indicator of quality. Engagement quality is one that contributes to enriching learning experiences for students that positively affect their growth and development [12]. The authors do not know at this point whether the knowledge garnered from the tutorial has made the students more effective at using secure computing...
technology at the work place and in their personal lives. Further research is necessary to answer the question and this research would likely be longitudinal where a study measures how prepared students are for the workforce as it pertains to computer security.

REFERENCES


