Computer Security Awareness of Accounting Students

Chlotia P. Garrison
Winthrop University
Computer Science & Quantitative Methods Department
Rock Hill SC 29733
803-323-2470 Fax: 803-323-3960
garrisonc@winthrop.edu

O. Guy Posey
Alabama A&M University, School of Business, Normal, AL 35762
256-372-4811 Fax: 256-372-5492
guy.posey@email.aamu.edu

ABSTRACT

Accountants store personal and financial data of clients on computers. The loss or exposure of this data can have devastating consequences for the client and the business. Are students preparing to work in a field that often has access to an individual’s social security number, bank account routing numbers, and company financial records, prepared to keep that data secure through common computer security practices? This paper analyzes the responses of a group of accounting students to a computer security survey. The survey was developed to investigate the security awareness and practices of college students. The results of this study indicate that accounting students may not be sufficiently prepared to help safeguard sensitive data and resources as they become practicing accountants.

INTRODUCTION

Computers are a part of almost every profession in some way and an integral part of an accounting profession. Accountants use special purpose software to perform various tasks and data used by accountants is stored on computers and separate storage devices. The education process is intended to prepare students to succeed in their chosen field. Position Statement No. One of the Accounting Education Change Commission declared that accounting graduates need the capability to locate, obtain, organize, report, and use information from electronic sources (American Accounting Association, 1990). The Association to Advance Collegiate Schools of Business (AACSB) Standards for Accounting Accreditation lists the “Design and application of technology to financial and non-financial information management” as a normal learning experience (2005). Many professors have designed their classes to satisfy these goals. The need to be educated in the area of computer security is equally critical. The American Institute of Certified Public Accountants includes in its Personal Competencies the need to address “privacy,
intellectual property rights and security issues related to electronic communications” as an element of Leverage Technology to Develop and Enhance Personal Competencies (2005).

Accountants often have access to personal and financial data of clients stored on computers. The loss or exposure of this data can have devastating consequences for clients, employees, and the business. Access to an individual’s personal information can lead to identify theft, one of the fastest growing crimes in America. Victims of identify theft can spend months and years trying to repair a damaged credit history, or recover stolen money. Victims may lose job opportunities, be refused loans, education, housing, cars, or even be arrested for crimes they did not commit (Federal Trade Commission, 2005). Computer incidents can cause reputation damage, loss of clients, or even liability for the business. It can be time-consuming or impossible to recover loss computer data. A study by the National Archives and Records Administration in Washington D.C. shows 50% of companies that lose data access for 10 or more days file for bankruptcy almost immediately following the loss (Datacentrick, n.d.). Lack of access to computers can lead to lost revenue and idle employees. The Internet Security Alliance estimates that businesses lose several billions of dollars each week to various forms of cyber attacks (2004).

Universities across the country have experienced network problems caused by students connecting infected machines to the school’s network. The classroom computers at the author’s institution were infected with the Sasser worm at the beginning of the 2004 fall semester. Instructors were unable to use classroom computers for the first week of classes. Student computers were identified as the source of the worm. A computer virus infected 2200 computers and slowed e-mail networks on the University of Wisconsin-Madison campus. Several businesses and the state’s legislature that remotely access the university’s network were also affected (Nathans and Welch, 2003). The University of North Texas in Denton reported that 70% of computers owned by resident students reporting for the fall term were infected with some type of virus (Krebs, 2003; Nathans and Welch, 2003). Students at all levels may have poor computer security habits. This became evident to network administrators at George Mason University. The administrators cut Internet access for all 3,600 students living on campus when an insufficient number of students signed a document confirming that their computers were updated with all the needed security upgrades (Krebs, 2003). To help protect the campus network, some universities impose certain measures such as requiring antivirus software on student machines before they can connect to the network.

Dr. Eugene Schultz, Principal Computer Engineer, University of California-Berkeley Lab and editor-in-chief of Computers & Security has said that universities are among the least secure places in the universe relative to computers (Foster, 2004). Are students preparing to work in a field that often has access to an individual’s social security number, bank account routing numbers, and company financial records, ready to keep that data secure through common security practices? This paper will investigate the computer security awareness of a group of accounting students. Results are based on an anonymous survey. The survey consisted of twenty-four questions designed to explore how aware and compliant students are of widely recommended security precautions. The results will be analyzed to determine if this particular group of students is prepared to help safeguard sensitive data and resources as they become practicing accountants.
RECOMMENDED SECURITY PRACTICES

A computer incident is an adverse event that interrupts normal operating procedures. Viruses are just one source of computer incidents. Good computer security practices by the computer user are an integral part of preventing computer incidents. A single negligent user can cripple a strong computer security program. Students as computer users should be aware of the following essential security practices.

**Passwords**

Computer users should never reveal their passwords because this compromises network security. There is never a reason for users to provide their password even to system personnel unless they initiated the communication. Authorized personnel can access accounts without user input. If the system does not provide generated passwords then the user should be aware of the characteristics of a good password. These include using a combination of upper and lower case letters, numbers and special characters. Passwords should be at least 6 to 8 characters, should never be a dictionary word, and should not consist of information that can be identified with the user, such as date of birth. In addition, passwords should be changed periodically, for example every six months.

**Patches and Updates**

When security vulnerabilities are identified, software vendors will often provide patches (a fix to a software defect) or updates (a newer version of existing software) to remove the vulnerability. These patches and updates should be applied as quickly as possible following the publication of a new vulnerability because attackers begin immediately to try to take advantage of the vulnerability. Users should also consider utilizing the automatic update feature of software.

**E-mail and Antivirus software**

The common caution is not to open e-mail from people you do not know. However, attackers have the ability to send out messages from a compromised machine to everyone in that person’s address book. Computer users should suspect any e-mail with an attachment they are not expecting, e-mails with intriguing subject lines, and e-mails containing filenames or messages that do not make sense, even if they are from known addresses. Before opening such a message, users should contact the sender to verify that they sent the message. Otherwise, delete the message without opening it. Once the user has decided to open an e-mail, attachments should first be scanned with antivirus software. Antivirus software attempts to detect and remove computer viruses. Antivirus software definitions should be updated at least weekly. Downloaded files should also be scanned with antivirus software before they are opened.

**Firewall, Spyware, and Popups**

A firewall helps prevent attackers from examining a machine and using existing vulnerabilities to facilitate their attacks. Software firewalls should be installed and configured to allow the least amount of access while still allowing legitimate use. Spyware and popup blocking software also
help protect a computer. Spyware is software that surreptitiously monitors the user. The term has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party (Wikipedia, n.d.). Popups are a form of online advertising. In addition to being irritating, attackers use popups to facilitate phishing. Phishing is an attempt to gain sensitive information such as passwords and credit card information by masquerading as a legitimate business in an official looking electronic communication.

**Backups**

Viruses, hard drive crashes, corrupted media, accidental deletion, and power failures are all potential threats to saved data. Creating a backup means making a copy to a second medium. Every computer user that saves files should perform backups regularly. Important files should be backed up whenever they are changed. Multiple backups are needed for onsite and offsite storage and to guard against corrupted backup media.

**Physical Security**

Users should be aware of password protected screensavers to prevent unauthorized access. An uninterruptible power supply (UPS) helps protect against data loss due to power outages or surges.

**SURVEY METHOD AND PARTICIPANTS**

A computer security survey was developed to assess the computer security awareness and practices of college students. The survey consisted of twenty-four questions addressing passwords, software updates, antivirus software, firewall, backups, spyware blocking software, popup blocking software, UPS, knowledge of the university’s security policies, and various demographic data. The anonymous survey was administered to students at four universities. Students were of all classifications, freshman through senior with a variety of majors. The results presented in this paper are of the computer security awareness and practices of the accounting students. Thirty-three (33) accounting students participated in the survey, 28 were seniors, two freshmen, one sophomore, one junior, and one did not specify.

**SURVEY RESULTS**

**Passwords**

Students were asked multiple questions about their passwords. In response to *Is your password easy to guess (for example a proper name, a dictionary word, your telephone number)*? 62.5% selected *No*. Seventy-two percent, 72%, indicated they did not write down their password. Students were provided several options for the question, *How often do you change your password?*. Only one student selected a frequency of six months or less. Seventy-five percent, 75%, indicated they never change their passwords. Figure 1 displays the selections relative to passwords.
The majority of students, 70%, selected No or Don’t Know when asked if the software on their computer was updated and patched against the latest security threats. Forty-eight percent, 48%, of students indicated they performed automatic updates of the software on their computer if available. Figure 2 displays the results for the two questions that addressed software patches and updates.

Students were most aware of antivirus software. Twenty-five or 75% of the students said they had antivirus software installed. Of the students with antivirus software installed, 18 or 72% knew the antivirus product name. Those students who identified the product being used were also the students that had a current subscription. Fourteen students indicted they had a current antivirus subscription, all but one of these provided the antivirus product name. Sixteen of the students who knew the product name also indicted the product was set to perform automatic updates. Three students without a current subscription indicated the product is set to receive automatic updates. Unfortunately, because the subscriptions are not current these students are not protected against the latest threats. Table 1 lists the responses by frequency to questions related to antivirus software.
Figure 2: Responses by percentage of participants to updated and patched software

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Don't Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed</td>
<td>25</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Current subscription</td>
<td>14</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>Automatic Updates</td>
<td>18</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 1: Frequency of responses to Antivirus Software questions

Participants were asked: *When do you scan e-mail attachments before opening? Always, If not expected, If suspicious looking, Occasionally, Never, Other (specify).* The most frequently selected response was *Always,* 48%, followed by *Never,* 29%. Table 2 shows the percentage and frequency of responses.
Table 2: E-mail attachments scanned before opening

Firewall, Spyware, and Popups

Thirteen students, or 39%, indicated they had a firewall. Almost the same number of students had spyware blocking software as had a firewall, 12 students. They were not necessarily the same students however. Only five students provided a spyware blocking product name. Fifty-eight percent, 18 of 31 participants, had pop-up blocking software. Only six of these provided a name of the software and one of these was actually spyware protection software. Table 3 lists the frequency and percentage of responses for these three security measures.

Table 3: Frequency (percent) of responses by product

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Don't Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>13 (39%)</td>
<td>12 (36%)</td>
<td>8 (24%)</td>
</tr>
<tr>
<td>Spyware</td>
<td>12 (39%)</td>
<td>14 (45%)</td>
<td>5 (16%)</td>
</tr>
<tr>
<td>Popup</td>
<td>18 (58%)</td>
<td>7 (23%)</td>
<td>6 (19%)</td>
</tr>
</tbody>
</table>

Backups

Most students were not following recommendations for backups. Just twelve students, 36%, indicated they have a current backup of their files. Three of these students indicated they did not perform backups either regularly, occasionally or when important changes are made. Fifty-eight percent, 58%, of students indicated they never backup their files. Figure 3 shows current backup and backup frequency by percentage of students.

UPS

Only 10% of students specified they have a UPS. The majority, 57%, did not know if they had a UPS.
CONCLUSION

The results of this study indicate that accounting students may not be sufficiently prepared to help safeguard sensitive data and resources as they become practicing accountants. Though some results are positive, security is an area that requires safeguards from multiple directions to be effective. The damage caused by viruses has received much media attention. The need to protect against viruses seems to be well known; 75% of the students indicated they had antivirus software and 68% did some e-mail scans prior to opening an attachment. However, all the students with antivirus software did not have a current subscription or perform automatic updates. Interestingly the majority of the students that indicated they never scan e-mail attachments before opening them have antivirus software. This could mean the antivirus product is set to do automatic scans or the students with antivirus software have a false sense of security. Results for passwords were also mixed. Sixty-two percent, 62.5%, said their password was not easy to guess and 72% indicated they did not write them down. However, an overwhelming 75% said they never change their password. In the critical area of software patches and updates, just 30% of students were current. Only 36% of students had a current backup of their files. These results reveal that the computer security practices of these students needs to improve.

Results also expose weaknesses in the computer security knowledge of the students. In five different areas the percentage of students that selected Don’t Know was at least 15%:

- 57% - UPS
- 42% - software updated and patched against the latest security threat
• 24% - firewall
• 19% - popup blocking software
• 16% - spyware blocking software
• 15% - software automatically updated if available

As universities focus on preparing accountants to succeed in using technology, the area of computer security should not be ignored. Forced compliance measures that help protect the campus network do not ensure students are conversant in computer security. The potential damage to clients and businesses only continues to increase as attackers devise new ways to take advantage of vulnerabilities that exist in software and people. In addition to concerns about identity theft, viruses, and loss data, Richmond (2004) reports that Symantec identified an average of over 10,000 programs a day that allow an attacker to remotely control a victim’s PC. The person who is capable of using technology must also be security conscious.

REFERENCES


