

5-2008

Student Survey on Computer Security Awareness And Responsiveness

Mark Rounds

University of Idaho, mrounds@uidaho.edu

Richard Pendegraft

University of Idaho

Norman Pendegraft

University of Idaho

Robert Stone

University of Idaho

Follow this and additional works at: <http://aisel.aisnet.org/confirm2008>

Recommended Citation

Rounds, Mark; Pendegraft, Richard; Pendegraft, Norman; and Stone, Robert, "Student Survey on Computer Security Awareness And Responsiveness" (2008). *CONF-IRM 2008 Proceedings*. 48.

<http://aisel.aisnet.org/confirm2008/48>

This material is brought to you by the International Conference on Information Resources Management (CONF-IRM) at AIS Electronic Library (AISEL). It has been accepted for inclusion in CONF-IRM 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISEL). For more information, please contact elibrary@aisnet.org.

71F. Student Survey on Computer Security Awareness And Responsiveness

Mark Rounds
University of Idaho
mrounds@uidaho.edu

Richard Pendegraft
University of Idaho

Norman Pendegraft
University of Idaho

Robert Stone
University of Idaho

Abstract

University students are very knowledgeable internet users, yet there seems to be disconnect between their actions and the security of their computer systems. This paper reports the results of an on-line survey of students' awareness of security threats on-line and their preparation to meet those threats.

Keywords

Network Security, User Modeling

1. Introduction

This research examines the attitudes of university students toward information system (IS) security, their behavior regarding security, and their use of their computers. University students are among the most computer literate members of our society. One would suppose that they are also the most aware of the threats they will confront using systems on-line. Surveys of professionals show that many users are not informed and not motivated to security aware but few if any have been done on student populations (Kankanhalli et. al. 2003, Stanton et. al., 2005, Khalfan, 2004). Foltz, Cronan, and Jones (2005) found that most students don't read their University's computer use handbooks. Adams and Sasse (1999) report that most users don't know a great deal about security. Siponen (2001) add that most users are also unaware of the damage they can do through ill considered responses to security situations.

These issues are important because fear of computer crime and the lack of awareness of computer security are major hindrances to growth of e-commerce is the (Udo 2001). There is a body of literature focusing on how to teach computer security awareness to students (Bishop, 1999, (2000, Yurcik and Doss (2001, Davis and Dark,2003). However, very few researchers have attempted to measure the effectiveness of security awareness training. Ferguson (2005) conducted an interesting experiment where randomly chosen cadets at West Point were sent an e-mail with a faked link that was discussed as inappropriate computer use in the class four hours prior to the experiment. Most of the students clicked on it anyway. This experiment was very interesting but limited to only one security practice.

In an attempt to more broadly understand the relationship between security awareness and security practice, we surveyed students at a western land grant university regarding security and security practices. This is a preliminary effort to gauge the size and complexity of the security awareness problem as it relates to modeling user attacker responses to increased security. We

have modeled these interactions in previous work (Pendegraft & Rounds, 2006, 2007) and have presented the theory that human interaction accounts for a larger share of the computer security problem than has been previously considered (Rounds, Pendegraft, & Taylor, 2007).

This work is based on the technology acceptance model or TAM (Davis, 1989) and the IS Success Model (ISM) (DeLone and McLean, 1992, 2003). TAM suggests that there is a link between ease of use and user acceptance. It is clear that security can reduce ease of use, hence our interest in evaluating attitudes toward security. ISM suggests that system and information quality leads to increased user satisfaction and increased use which in turn leads to net benefits. Security can also affect these factors. Wixom and Todd (2005) combine these models system and data quality and the one hand and system usage on the other. Clearly, systems usage increases system value and is bounded by the level that security intrudes upon the user.

2. Methodology

The first goal of the survey was to determine how the subject population perceives the current importance of computer security. The second goal was to look at which security practices they actually employ and compare the two to see if there is a dissonance. We examined two classes of behavior that we looked at. The first includes behavior and activities on line. The second is security practices designed for keeping your system secure. Security products usage questions were asked using a simple yes/no grid. Space was provided to respond with any other product that we may not have listed. The more qualitative questions were asked with a five point Likert scale.

The questionnaire contains twenty two questions (listed in results). Three questions looked at security awareness, eleven measured on-line behaviors and five measured specific security features such as software fixes and passwords.

The survey itself was administered on-line using Web Surveyor over a three week period. Two thousand initial requests were sent out. Two reminders were sent as the time period elapsed. We received 159 completed surveys for a 7.95% response rate.

2.1 Limitations

Since this survey was administered on-line, the respondents self selected. It was also limited to students of a single University. These results are representative of the state of awareness and security practices in certain populations of users at this University. While self-selecting web surveys do lack randomness, there are benefits to this approach. Schwartz et. al. (1995, 1996) suggests that the absence of an interviewer can elicit a more honest response.

3. Results

Table 1 summarizes the results.

Question	Results
Do you set your operating system to automatically download and apply updates?	69.81%
Do you use any of the following security software? avast! Antivirus	1.89%
Do you use any of the following security software? AVG Antivirus	25.79%
Do you use any of the following security software? BitDefender Antivirus	0%
Do you use any of the following security software? CA Antivirus	0.63%

Do you use any of the following security software? F-Secure Antivirus	1.26%
Do you use any of the following security software? Kaspersky Antivirus	0%
Do you use any of the following security software? Lavasoft Ad-Aware	9.43%
Do you use any of the following security software? MacAfee VirusScan	26.42%
Do you use any of the following security software? Norton Antivirus	37.11%
Do you use any of the following security software? Panda Antivirus	0.63%
Do you use any of the following security software? Spybot- Search and Destroy	18.87%
Do you use any of the following security software? Symantec Antivirus Corporate Edition	22.01%
Do you use any of the following security software? Trend Micro "PC-cillin" Internet security	5.03%
Do you use any of the following security software? Webroot Spy Sweeper	2.52%
Do you use any of the following security software? Windows Defender	7.55%
Do you use any of the following security software? Windows Live OneCare	0%
Do you use any of the following security software? ZoneAlarm Internet Security Suite	5.66%
Do you use any of the following security software? Other	9.43%
Approximately how often do you update the definition files for your antivirus program(s) (at least once a week)	60.38%
I often download from the web. (Agree or strongly agree)	61.01%
How many web sites do you visit that require passwords? Less than 4/(4-10)/(More than 10)	10.7%/67.3%/22%
For these web sites, about how many different passwords do you use? Average/median	4.22/3
Approximately how often do you change your University email account password? (once a semester or less)	96.7%
Do you share any of your passwords with other people? (Yes)	21.38%
Do you set your web browser to save passwords for you? (Yes)	31.45%
It is important to worry about computer security? (Agree or strongly agree)	87.42%
Keeping my computer secure helps keep other computers secure. (Agree or strongly agree)	81.13%
I am very careful about downloading from the web. (Agree or strongly agree)	77.99%
I am very careful about opening attachments or links in email. (Agree or strongly agree)	79.87%
Commercial sites such as Amazon.com. (Willing or Very Willing to use)	57.86%
Computer support sites such as Microsoft.com. (Willing or Very Willing to use)	78.62%
Social Networking sites such as FaceBook.com. (Willing or Very Willing to use)	17.61%
Blogs. (Willing or Very Willing to use)	3.77%
Sites with sexual content. (Willing or Very Willing to use)	5.03%
Sites associated with computer hackers. (Willing or Very Willing to use)	3.14%
Have you heard about the University Computer Security Awareness day? (Yes)	46.54%
Would you attend a free 2-hour course on computer security if one were offered? (Yes)	20.75%

Table 1: Summary of Results

3.1 Security Awareness

The bulk of our students agree that there is a security problem, in fact, 87.4% agree or strongly. Most students (81.1%) also agree that keeping their computers secure helps increase overall security. However, only 46.5% have heard about the University's Computer Security Awareness Day in spite of the fact that they all received e-mail on the subject and there were numerous posters around campus.

3.2 Web Practices

When we looked at web practices, we saw that many students are obviously aware of the suggestions for safe web usage and follow those that require passive acceptance. For example, 78% of students say they are very careful about downloading from the web and 79.9% of students say that they are very careful about opening e-mail attachments. When we looked at the types of web sites that students view, 78.6% of students say that they are willing to use on-line support sites and 57.9% say they are willing to use commercial sites such as Amazon.

However, when the focus of the questions turned to some sites with a less reliable track record the student's responses were significantly less positive. Only 17.6% are willing to use social networking sites such as Facebook and only 3.8% are willing to use blogs. When we asked about sites that had a potentially illegal or objectionable content, the number of positive responses are even lower, with only 5.03% willing to use sites with sexual content and only 3.14% willing to use sites associated with hackers.

However, when dealing with on-line security issues that require a positive action, the students are more likely to avoid the action. For example, when using passwords on-line, it is clear that many are using the same password for several sites as 67.3% visit between 4-10 websites that require passwords and another 22% visit more than 10 sites that require passwords, however, the average number of passwords that these same students have is 4.22 with a median of 3. Further, 21.4% share their passwords with others and 31.5% set their browsers to save passwords. In general, those with a higher number of passwords tended to let their browser store the passwords and those who had many passwords were more likely to share them.

3.3 Security Practices

When we start evaluating security practices where compliance requires some positive action, the information was more mixed. Most computers these days come with some form of anti-virus protection and so most have some form of security software. Only 5% of the respondents have no computer security software and 12.58% have no antivirus software. However, when the security measure requires an active response, more are likely to forego many security measures, for example while only 5% of respondents have no anti-virus program, only 61% of students with antivirus software update it at least once a week.

When it comes to optional security software, there was very little used. The most common security software was designed to stop agents from being implanted such as Ad-Aware. The percentage that had this software was 30.82% with very little overlap. Very few used any form of security management or integrating software and none used any other form of intrusion alert software.

As most systems are defaulted for auto update, it is surprising that only 69% allow Microsoft to auto-update their operating systems and other Microsoft products. Finally, only 20.8% would be willing to take a free two hour computer security class in spite of the fact that most don't follow good security practices such as frequent password renewal, sharing of passwords, using the same password on multiple sites and admit that it is a problem.

3.4 Factor Analysis

Using these responses to the questionnaire, a principle components factor analysis, using PC SAS version 9.1, was performed. The prior communities were set equal to one. The initial factors were rotated orthogonally using varimax rotation. Seven meaningful rotated factors were identified. One factor related to the respondents' attitudes towards computer security and was composed of two items ("It is important to worry about computer security" and "Keeping my computer secure helps keep other computers secure"). This factor is labeled as "Attitudes Towards Security." The other six factors were behaviors related to computer and Internet use and security. Each of these is discussed and labeled below. One factor, labeled "Visit Commercial and Support Sites" was composed of two items (On the Internet, I visit "Commercial sites such as Amazon.com" and "Computer support sites such as Microsoft.com"). Another factor, labeled "Using Social Networks and Blogs" was also composed of two items (On the Internet, I visit "social networking sites such as FaceBook.com" and "Blogs"). A factor labeled "Concern for Opening Files from the Internet" was made from two questionnaire items ("I am careful about downloading from the web" and "I am very careful about opening attachments and links in email").

The next factor is labeled "Visit Adult Sites" and was formed from two questionnaire items (On the Internet, I visit "Sites with sexual content" and "Sites associated with computer hackers"). The next factor is labeled "Passwords" and is made from two items ("How many websites do you visit that require passwords?" and "For these websites how many different passwords do you have?"). The final factor is labeled "Antivirus" and is composed from two questionnaire items ("Do you have your operating system to automatically download and apply updates?" and "Approximately, how often do you update the definition files for your antivirus program(s)?").

The items composing each factor were summed into the seven composite measures. These summed measures were then correlated to examine any potential interrelationships. These correlations were computed as the standard Pearson correlation coefficients and are reported in Table 2.

There are some cautious interpretations that can be made from these correlations. Respondents who are concerned about opening files from the Internet also have positive attitudes towards computer security. It appears that respondents who visit commercial and support sites on the Internet also use social networks and blogs. Furthermore, those respondents who visit social networks and blogs also tend to visit adult sites (i.e., ones with sexual content and computer hacker sites) and have reduced concern for open files distributed via the Internet. Finally, the respondents who expressed concern for opening files from the Internet also display increased number of sites visited requiring passwords and greater numbers of different passwords on these sites.

	Attitudes Towards Security	Visit Commercial and Support Sites	Using Social Networks and Blogs	Concern for Opening Files from the Internet	Visit Adult Sites	Passwords	Antivirus
Attitudes Towards Security	1.00						
Visit Commercial and Support Sites	-0.04	1.00					
Using Social Networks and Blogs	-0.12	0.23**	1.00				
Concern for Opening Files from the Internet	0.31**	0.01	-0.30**	1.00			
Visit Adult sites	0.07	0.17	0.23**	-0.15	1.00		
Passwords	0.07	0.11	-0.06	0.19*	0.10	1.00	
Antivirus	0.20*	0.01	-0.01	0.14	-0.05	0.10	1.00

Table 2: The Correlations Among the Factors

* Correlation significantly different from zero at a 5% level in a two-tail test.

** Correlation significantly different from zero at a 1% level in a two-tail test.

4. Conclusion

Many individuals seem similar to our students in that while they are aware of issues like the effect of obesity on health, or the importance of locking one's doors, they aren't willing to exert much effort to comply. While not really surprising, it is none the less a useful insight for systems administrators when developing security policies. Those methods that require active participation from the users would, based on this research, be less effective than those that were handled automatically or by the administrator. Password control in particular seems to be the area where students at this University pay the least heed even though they have heard the message in multiple contexts.

5. Future Research

This work has been exploratory, and its results suggest at least two potential lines of future research. It would be useful to follow this survey up with repeat surveys at other institutions as well as non university environments to determine whether our results can be generalized.

Longitudinal studies linked to security training would also be interesting. Secondly, it calls for a sound theoretical model of the relationship between the attitudes and behaviors of IS users. We are currently engaged in this work.

References

- Adams A., and Sasse M., "Users are not the enemy.", *Communications of the ACM*, Volume 42, Number 12, 40-46, 1999.
- Bishop, M., "What Do We Mean by "Computer Security Education"?" 22nd National Information Systems Security Conference, Proceedings October 1999.
- Bishop, M., "Education in Information Security", *IEEE Concurrency*, 4-8, December, 2000.
- Davis, F., "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", *MISQ*13(3) 319-340, 1999.
- Davis, J., and Dark, M., "Defining a Curriculum Framework in Information Assurance and Security" 2003 ASEE Annual Conference & Exposition: Staying in Tune with Engineering Education, Nashville, 22-25 June 2003.
- DeLone, W.H. and McLean, E.R., "Information System Success: The Quest for the dependent Variable.", *ISR* 3(1), 60-95, 1992.
- DeLone, W.H. and McLean, E.R., "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update.", *JMIS* 19(4), 9-30, 2003.
- Ferguson, A., "Fostering E-Mail Security Awareness: The West Point Carronade", *Educause Quarterly*, Volume 28, Number 1, 54-57, 2005.
- Foltz, C., Cronan, T., and Jones, T., "Have you met your organization's computer usage policy?", *Industrial Management & Data Systems*, Volume 105, Issue 2, 137-146, 2005.
- Kankanhalli, A., Teo, H., Tan, B., and Wei K., "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Volume 23, Issue 2, 139-154, April 2003.
- Khalfan, A., "Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors", *International Journal of Information Management*, Volume 24, Issue 1, 29-42, February 2004.
- Pendegraft, N., and Rounds, M., "A Simulation of IS Security with Variable Attacker Populations", *INFORMS Annual Meeting*, November 5-8, 2006, Pittsburg, PA.
- Pendegraft, N., and Rounds, M., "A Simulation Model Of IS Security", *International Journal of Information Security and Privacy*, Vol. 1, Issue 4, 62-74, July/September 2007.
- Rounds, M., Pendegraft, N., and Taylor C., "Human-Centric Approach to Simulation of IS Security Dynamics", presented at the 18th Annual Information Resources Management Association International Conference May 19-23, 2007, Vancouver, British Columbia, Canada.
- Siponen, M., "Five dimensions of information security awareness", *ACM SIGCAS Computers and Society*, Volume 31, Issue 2, 24 – 29, June 2001.
- J., Stam, K., Mastrangelo, P., and Jolton J., "Analysis of end user security behaviors", *Computers & Security*, Volume 24, Issue 2, 124-133, March 2005.
- Udo, G., "Privacy and security concerns as major barriers for e-commerce: a survey study.", *Information Management & Computer Security*, Volume 9 Issue 4, 165-174, 2001.
- Yurcik, W. and Doss, D., "Different Approaches in the Teaching of Information Systems Security," *Information Systems Education Conference (ISECON)*, 2001, Cincinnati, OH

Wixom, Barbara and Todd, Peter, A., "A Theoretical Integration of User Satisfaction and Technology Acceptance." *ISR*16(1), 85-102, 2005.