Security Practices of Students

James Morgan
Jim.morgan@nau.edu

Jo-Mae Maris
Jo-mae.maris@nau.edu

Alden C. Lorents
alden.lorents@nau.edu
Franke College of Business
Northern Arizona University
Flagstaff, AZ 86011

Abstract

This paper presents results of a survey of the security practices of introductory IS and MIS students that was conducted with the intent both to enliven classroom discussion of security topics and to provide an understanding of the state of student knowledge of security issues which can serve to guide curriculum development in this area. Survey results suggest that students, almost without exception, have anti-virus and personal firewall security software installed on their personal computers. Students are also found to be rather conscientious with regard to protecting their PCs and avoiding viruses and scams. However, significant numbers of students, particularly introductory students, tend to view tight network security rules as being overly stringent. Introductory students may not yet have the level of awareness of network security requirements that will be required when they enter the workplace.

Keywords: PC security, network security

1. SECURITY PRACTICES OF STUDENTS

This paper presents summary data from a survey that has been conducted in the required junior level MIS course in a business college over the past year and in a freshman level, liberal studies, introductory (intro) IS course in the Fall of 2006. The survey was conducted in part as a means of engaging students. Survey results are reported to each class and have served as an effective means of engaging students in discussions of security practices and security risks. Survey results are also used by the faculty as a means to assess where student capabilities are inadequate and security education needs to be strengthened. Finally, the survey results are, we believe of broader research interest as indicators of the current state of security awareness of a fairly typical set of university students.

This paper focuses on this latter aspect. There is no shortage of articles in the popular press describing the accelerating incidence and complexity of malware, phishing attacks, and denial of service schemes (see, for instance, Gaudin [2007], Giles [2007], Heyman [2007], Hecht [2007], and Seltzer [2007]). In recognition of the need for additional security coverage in the general business curriculum, supplementary texts focusing on security have been developed for use in the MIS course (Ciampa, [2004] and Rothke [2004]) and many introductory com-

puting and MIS texts have added sections or full chapters focusing on security issues (see, for instance, Norton [2006], Oz [2007], Parsons [2007] and Shelly, Cashman, and vermaat [2008]). However, there is little systematic information about the computer security practices of students. There have been a number of recent studies of general computing skills and practices of students (see, for instance, Hakkarainen et. al. [2000], Pask and Saunders [2004], and Hardy, Heeler, and Brooks [2006]), but none of these studies have focused on security practices of the student population.

The survey described below includes responses from the Introduction to IS and Junior level MIS courses. The survey was conducted online using the survey component of a popular course management package and was administered just prior to classroom coverage of security related topics. Students were given a small amount of credit for completing the survey to encourage them to respond. There were 50 students in the Introduction to IS course where the survey was administered, while 65 students were enrolled in the two sections of the MIS course where the survey was used. Response rates vary somewhat across the questions. However, the rate of response is over 80 percent for each of the questions.

Students were asked a variety of questions about their security practices when using their own personal computers and when using shared computers. In addition the students were asked to evaluate the appropriateness of various forms of access control to networked computer systems that might be imposed by system administrators. In the sections, that follow we will first look at the security related practices of the students and then look at their responses to alternative proposed access control measures on networked computer systems. Overall percentage results will be presented, as well as, raw numbers for the responses of students at both the intro and MIS levels. Separation of the responses of these groups also allows the use of a standard Chi-Squared test to evaluate whether introductory and MIS students differ significantly in their responses.

2. PC SECURITY PRACTICES

Tables 1A thru 1C deal with ownership and maintenance of PC security software on the students' home PCs. Table 1A shows that over 85 percent of students have anti-virus software and are confident that their software is being automatically updated. Installation of personal firewall software is also nearly universal (Table 1B) and over two-thirds of students have pop-up blocking software installed on their systems (Table 1C).

Table 1A PC Security Software Use

	My PC has current, on-line updated anti-virus, software		
	Intro. Studs.	MIS Studs.	Overall Pct.
Yes	36	55	85.80%
No	3	5	7.50%
Not Sure	2	5	6.60%
Chi-Sq. Prob.	*0.19*		
Chi-Sq. Prob.	*0.53*		

Table 1C PC Security Software Use

	My PC has software to block pop-up ads		
	Intro. Studs.	MIS Studs.	Overall Pct.
Yes	32	40	67.90%
No	2	11	12.30%
Not Sure	7	14	19.80%
Chi-Sq. Prob.	*0.12*		

Tables 2A thru 2C deal with the experience students have had with e-mail attachments. Table 2A shows that over 80 percent of students have received an e-mail from an unknown source containing an attachment that they were asked to open, and more than a third of students have had this experience 3 times or more in the past year. Most students do not open such attachments. However, only about a 20 percent of the students have ever reported a suspicious e-mail to a network administrator or service provider (Table 2B). MIS students are somewhat more likely than intro students to have reported a suspicious e-mail and the differences between the two groups are statistically significant for that question.

Table 2A E-mail Attachments: Have you received E-Mail from an unknown source asking you to open an attachment

	Intro. Studs.	MIS Studs.	Overall Pct.
Yes, 3+ times in the past year	18	23	36.90%
Yes, at least once	17	32	44.10%
No	11	10	18.90%
Chi-Square prob.	*0.36*		

Table 2B E-mail Attachments: Have you reported the Receipt of a suspicious looking E-Mail

	Intro. Studs.	MIS Studs.	Overall Pct.
Yes, 3+ times in the past year	5	3	7.20%
Yes, at least once	2	14	14.40%
No	39	48	78.40%
Chi-Square prob.	*0.03**		

Table 2C E-mail Attachments: Have you opened an attachment from an e-mail source you didn't recognize

	Intro. Studs.	MIS Studs.	Overall Pct.
Yes, 3+ times in the past year	2	4	5.40%
Yes, at least once	5	15	18.00%
No	39	46	76.60%
Chi-Square prob.	*0.21*		

Tables 3A thru 3C indicate that just over half of the students have received social engineering e-mails requesting that they divulge confidential information due to a "problem" with their account. Interestingly, very few students, less than 25 percent, report having received similar social engineering attempts via telephone. Table 3C shows the prevalence of students writing down a password. Overall, over two-thirds of students have written down a password. For this question, responses of intro students differ significantly from those of MIS students. The MIS students are more likely to have written down one or more passwords, perhaps because they have access to a greater variety of networks requiring passwords.

Students were also asked about their practices with respect to opening e-mail attachments (Table 4A –See remaining tables that the end of the paper). Students are generally quite cautious with respect to e-mail attachments from unknown sources (less than 10 percent would open such an attachment without checking it for viruses), but are substantially less cautious with attachments from sources they know (only 20 percent always check attachments for viruses before opening them). This may represent a significant vulnerability given recent and emerging forms of viruses.

Table 3A Social engineering: Have you received e-mail asking for personal information

	Intro. Studs.	MIS Studs.	Overall Pct.
Yes, 3+ times in the past year	8	10	16.22%
Yes, at least once	17	24	36.94%
No	21	31	46.85%
Chi-Square prob.	*0.96*		

Table 3B Social engineering: Have you received a phone call asking for personal info.

	Intro. Studs.	MIS Studs.	Overall Pct.
Yes, 3+ times in the past year	4	1	4.50%
Yes, at least once	6	14	18.02%
No	36	50	77.48%
Chi-Square prob.	*0.13*		

Table 3C Social engineering: Have you written down a user ID and password

	Intro. Studs.	MIS Studs.	Overall Pct.
Yes, 3+ times in the past year	7	9	14.41%
Yes, at least once	17	44	54.95%
No	22	12	30.63%
Chi-Square prob.	*0.01**		

Students were next asked to indicate their habits with respect to logging off of their home PCs and shared PCs (Table 4B). Not surprisingly, most students are much less concerned about logging off of home PCs than shared PCs. Table 4B indicates that the majority of students do not log off of their personal PCs unless they have concluded a session of work and don't expect to use the computer again for several hours. However, when using shared lab computers, nearly two-thirds of the students log off when they plan to be physically away from the computer for any period of time.

3. NETWORK ACCESS CONTROL MEASURES

The next set of questions students responded to dealt with their feelings about the appropriateness of various types and levels of access control measures, imposed by system administrators, on shared computer networks.

Tables 5A and 5B present alternative password complexity and password change rules that are typical of requirements set by system administrators on many shared systems. The majority of students felt that passwords with a minimum length of 5 characters and a requirement to use both letters and numbers in the password were appropriate, but felt that longer or more complex passwords might impose more burden than necessary on users. Very few students, less than 15 percent, felt that any of the password schemes were inadequate to provide appropriate control. With respect to password change rules, nearly 40 percent of students felt that a requirement to change passwords even once a year might be overly burdensome, while over 60 percent felt that a requirement to change every 6 months and not reuse a password for 2 years was at least somewhat excessive. In this area there are significant differences between Intro and MIS students with the MIS students being more accepting of password change requirements.

Table 5C deals with rules that terminate a user's session on a networked system after a given period of idleness. Systems terminating sessions after 5 minutes were felt, by most students, to be unnecessarily burdensome. The median response to termination was that an hour was clearly appropriate, while termination after 15 minutes of idleness was seen as somewhat excessive by about two-thirds of the students. There were significant differences between Intro and MIS students across this section. In general, MIS students were more accepting of network terminations than their Intro student counterparts.

4. SUMMARY

This paper has reported on the security practices and opinions of a rather typical set of university students at both the freshman and junior levels. The survey described here has been used as an effective means of generating student interest and engagement in security related topics in both the introductory IS and MIS classes and an aid to help plan curriculum improvement.

The survey results suggest that the vast majority of students are aware of and use basic security oriented software products such as anti-virus software, personal firewalls and pop-up blockers. Since most students have a number of security related software products on their own PCs, it should be possible to get them interested in the basics of how these products work, and the settings that can be used to adjust their performance.

Most students are also aware of malware threats associated with e-mail attachments, although few of them report suspicious software to service providers or network administrators. Just over half of the students reported having received an e-mail seeking to get them to divulge personal information, and about 70 percent of students reported having written down a password on at least one occasion.

The survey also asked students their opinions about various network security policies relating to passwords and termination of idle session. The vast majority of students accept the use of passwords of at least 5 characters, the requirement for both character and numbers, and a requirement to change passwords annually as an appropriate set of password policies. Policies more stringent than these were seen as at least somewhat

excessively burdensome. With regard to termination of idle session, a strong majority of students feel that termination after an hour of idle time is appropriate, while a slight majority of students felt that termination after 15 minutes was somewhat excessive. In this area Intro students tended to be less tolerant than the MIS students of tighter network policies. This suggests that student perceptions evolve as they gain more experience with network systems and have more valued resources stored on these systems.

Overall, the results of this survey suggest that students posses fundamental security related software and have broad knowledge of the nature of security threats. What appears to be lacking is a full appreciation of how serious these threats can be and of the importance of implementing effective security measures to protect against them both on their personal systems and on networked computers. Thus, it is important for IS security curriculum to focus on making the risks of security breaches real to students and on providing instruction focusing on practical security measures – behavioral habits and proper tuning of software – that students can apply to their personal use of computer systems.

5. BIBLIOGRAPHY

Ciampa, M. Security Awareness: Applying Practical Security in Your World, Thomson/Course Technology, Boston, 2004.

Gaudin, S., "Storm turns into a Hurricane; Is a Botnet Attack Brewing;" Information Week, Issue 1129, p. 38, 2007.

Giles, J., "The street Crime of the Internet," New Scientist, Vol. 194, Issue 2607, pp. 30-31, 2007.

Hakkarainen, K. L. Ilomaki, L. Lipponen, H. Muukkonen, M. Rahikainen, T. tuominen, M. Lakkala, and E. Lehitinen, "Students' skills and Practices of using ICT: results of a national assessment in Finland," Computers and Education, Vol. 34, pp. 103-117, 2000.

Hardy, C., P. Heeler, and D. Brooks, "Are high school graduates technologically ready for post-secondary education?', Journal of Computing Sciences in Colleges, Vol. 21 No. 4, pp. 52-60, 2006.

Hecht, J., "When web browsers turn bad," New Scientist, Vol. 194, No. 2602, p. 60, 2007.

Heyman, K. "New Attack Tricks Antivirus Software," Computer, Vol. 40, No. 5, pp. 18-21, 2007.

Norton, P., Intro to Computers 6/e, McGraw-Hill, 688 pages, 2006.

Oz, E., Management Information Systems, 5th Edition, McGraw-Hill, 560 pages, 2006.

Parsons, J., Computer Concepts-Illustrated Complete, 6th Edition, Course Technology, 464 pages, 2006.

Pask, J. and E. Saunders, "Differentiating Information Skills and Comp[uter Skills: A Factor Analytic Approach," Libraries and the Academy, Vol. 4, No. 1, pp. 61-73, 2004.

Rothke, B., Computer Security, McGraw-Hill, 46 pages, 2004.

Seltzer, L., "Windows Hacktivation," PC Magazine, Vol. 26, No. 14, p. 92, 2007.

Shelly, G., T. Cashman and M. Vermaat, Discovering Computers 2008, Complete, Course Technology, 904 pages, 2008.

TABLES 4 and 5

Table 4A PC Related Security Practices - Email Behavior

Which of the following best describes your behavior with respect to e-mail attachments	Intro	MIS	Overall
I never open e-mail attachments without checking the attachment for viruses.	9	13	19.57%
I never open e-mail attachments from sources I don't know	28	36	60.87%
I never open e-mail attachments from sources I don't know without checking for viruses	6	10	13.04%
I sometimes open e-mail attachments from sources I don't know if the message doesn't look suspicious.	2	5	4.35%
I open e-mail attachments that seem interesting without concern for viruses	1	1	2.17%
Chi-Square Probability	*0.94*		

Table 4B PC Related Security Practices - Log Off Behavior

Which of the following best describes your behavior with respect to logging/off of:	Your home PC			Shared / Lab PCs		
	Intro	MIS	Overall	Intro	MIS	Overall
I frequently do not logoff at the conclusion of a session	9	10	17.90%	2	2	3.80%
I only logoff when I do not expect to use the PC again for several hours	20	30	47.20%	14	10	22.60%
I logoff when I will be physically away from the PC for 30 minutes or more	5	12	16.00%	4	10	13.20%
I logoff of my PC anytime I am physically away from the PC	7	13	18.90%	21	43	60.40%
Chi-Square Probability	*0.71*			*0.13*		

Table 5A Opinions of Netwaork Security Policies

Password Complexity	What is your opinion of rules requiring passwords that are:								
	Lengthy and complex administrator assigned			User set 5 characters + with letters and			User set 9 characters + with numbers and		
	Intro	MIS	Overall	Intro	MIS	Overall	Intro	MIS	Overall
Inadequate for control	0	4	3.48%	8	6	12.17%	0	0	0.00%
Clearly appropriate	24	16	34.78%	36	50	74.48%	6	19	21.71%
May impose unnecessary burden	25	28	46.09%	5	4	7.79%	24	24	41.68%
Probably excessively restrictive	1	9	8.70%	1	4	4.33%	13	16	25.18%
Clearly excessively restrictive	0	8	6.96%	0	1	0.87%	7	6	11.29%
Chi-Square probability	0.01*			0.47			0.15		

Table 5B Opinions of Network Security Policies

Password Change Rules	What is your opinion of rules requiring that you								
	Change passwords every year			Change passwords every 6 months & no reuse for 2 years			Change passwords monthly with no reuse		
	Intro	MIS	Overall	Intro	MIS	Overall	Intro	MIS	Overall
Inadequate for control	4	14	15.65%	2	7	7.83%	6	1	6.36%
Clearly appropriate	24	26	43.48%	9	26	30.43%	5	8	11.82%
May impose unnecessary burden	15	18	28.70%	17	12	25.22%	12	20	29.09%
Probably excessively restrictive	4	6	8.70%	16	14	26.09%	16	16	29.09%
Clearly excessively restrictive	3	1	3.48%	6	6	10.43%	6	20	23.64%
Chi-Square probability	*0.24*			*0.04**			*0.06*		

Table 5C Opinions of Network Security Policies

Idle Session Termination	What is your opinion of rules that log you off of a network if you have been idle for:								
	1 Hour			15 Minutes			5 Minutes		
	Intro	MIS	All	Intro	MIS	All	Intro	MIS	All
Inadequate for control	4	21	22.12%	2	5	6.19%	6	1	6.19%
Clearly appropriate	26	28	47.79%	14	30	38.94%	4	21	22.12%
May impose unnecessary burden	11	11	19.47%	19	14	29.20%	7	25	28.32%
Probably excessively restrictive	5	3	7.08%	10	5	13.27%	13	7	17.70%
Clearly excessively restrictive	2	2	3.54%	3	11	12.39%	18	11	25.66%
Chi-Square probability	*0.04**			*0.02**			*0.01**		