AN EMPIRICAL STUDY OF CYBER SECURITY PERCEPTIONS, AWARENESS AND PRACTICE

Chen Zhang, Bryant University, czhang@bryant.edu
Janet J. Prichard, Bryant University, prichard@bryant.edu

ABSTRACT

This paper examines the perceptions, knowledge, and experience of security practices of users. A survey instrument was developed and administered to undergraduate students at a small private university. The results of this survey are presented, and the implications of these result discussed.

Keywords: Security, User Awareness, Survey

INTRODUCTION

With the growth of the Internet (a.k.a. cyberspace) users and Internet applications including communication, E-commerce, searching, and entertainment, Internet security incidents have also shown a rapid rate of increase. The total number of incidents received by cert.org increased from 1,334 in 1993 to 137,529 in 2003 (publication of the total incident reports number was deprecated after 2003), which was an increase of over 103 times in ten years [1]. Other research has surveyed U.S. organizations' practices and found that although financial losses had been falling since 2002, this trend has turned and respondents reported significant upswing in 2006 to $350,424 per respondent from $168,000 in 2005 (CSI 2007) and remains at $350,000 in 2007 (CSI 2008).

Other research reveals some related statistics about reported vulnerabilities in 2007 and found that the number of reported high severity vulnerabilities increased by 28% in comparison with 2006. Of all the vulnerabilities disclosed in 2007, only 50% can be corrected through vendor patches; and nearly 90% of 2007 vulnerabilities could be remotely exploited.

As for the intention of the Internet threats, it appears that profit is the new motive. The pride of one-upmanship—which used to inspire many cyber attacks—is giving way to calculated criminal intent according to Symantec [8]. Other research on cyberspace crime reveals the trend of the formation and the maturing of a cybercrime economy [2] where malicious software is distributed via the affiliate model (someone pays others to infect users with spyware and Trojans). This has become more prevalent in 2007 [4].

When we take all of these trends together, especially for the year of 2007, the outlook is not very optimistic. Public awareness of cyber security issues can definitely make a difference. The rise of security concerns since 2002 (after September 11, 2001) has resulted in the joint efforts by numerous organizations including the IT security industry and the US government to improve the application of defense tools. This achieved a fall in the organizational financial losses due to the cyber security attacks between 2001 and 2005. However, whether the upsurge of the cyber security threats has raised the awareness of today's Internet users is questionable.

The remainder of this paper is organized as the following: in section two is a review of the existing literature; section three is a discussion of the survey methodology; section four presents and discusses the survey results. Finally, a summary of the research findings is presented.

LITERATURE REVIEW

In the existing literature, the Computer Security Institute (CSI) has been surveying U.S. organizations in various industrial sectors for thirteen contiguous years (www.gocsi.com). The CSI survey questions cover IT security budgeting issues, security incidents/ losses, and security policies/technologies/training. The EU survey (European Commission Information Society and Media Directorate General, Emerging Technologies & Infrastructures Security) focuses on the observed types of security threats and the responding computer security legislation/policies and services [3]. It has a general set of questions about the user perceptions about security risks.

Internet user's perceptions and practices of security have been reported in Teer's survey [9] on college students' security perceptions/practices. This survey includes questions about general security perceptions, the students' security practices including usage of antivirus software and firewalls, as well as general password, security patches and email security habits.

Internet user's security perceptions and trust have strong impacts on their online shopping intention

[10]. Other works also studied the correlation between online users' security perceptions with technical factors such as authentication technologies [6] and non-technical factors such as brand name [7] and how the security system interacts with the users, such as how to phrase the security warnings [5].

RESEARCH METHODOLOGY

We developed a three page survey with refined questions related to Internet users' security perceptions, knowledge, experiences, and practices. Through this more refined design of the survey, we try to understand Internet users' behaviors in order to suggest better practices of the IT industry and education. In our survey design, we attempt to avoid high-tech jargon such as "firewall of wired/wireless residential gateway routers" in the survey and substitute it plain term of "firewall to my home network" to better match students' background IT knowledge.

This survey was then distributed to students in introductory information systems classes at an east coast university and received 90 usable responses. The survey was anonymous. The demographic information of the respondents is provided in Table 1.

The primary limitation of the survey is that the respondents are primarily college freshman and sophomores; and as such the results may not be generalized to users with other demographic profiles (such as older users).

RESULTS AND DISCUSSION

Internet Users' Security Perceptions, Knowledge, and Experiences

The users generally agree that security education is important to both business and home users with more importance leaning towards business users. Here we used a rubric system from 0 to 4 and does not count into the score for a "Not Sure" response.

We refined the user's perceptions on the most popular Internet services to try to find out users' security concerns about each of them. We used a weighted score system to facilitate the comparison of different services and in order to clarify the polarization we define Very Secure as +4, Somewhat Secure as +2, Somewhat Insecure as -2, Very Insecure as -4 and ignore Not Sure by setting it to 0.

Table 1. Demographic Information of Respondents

Demographic Attribute	Responses
Male	50
Female	40
Majors	
Accounting	24
Actuarial Math	3
Computer Information Systems	2
Communications	5
Finance	8
International Business	17
Information Technology	2
Management	9
Marketing	7
Political Science	1
Undeclared	12
Average Age	19.4
Average Years of Computer Experience	9.3
Average Computer Expertise Self Rating (out of 5)	3.5

Table 2. Perception of Importance of Internet Security Education

Importance of Internet Security Education to	Home Users	Business Users
Very Important (4)	54.4%	63.3%
Somewhat important (3)	38.9%	27.8%
Not very important (2)	6.7%	6.7%
Unimportant (1)	0.0%	0.0%
Not Sure (0)	0.0%	0.0%
Weighted Average (0-4)	3.48	3.50

As shown in Table 3, the users' perceptions generally meet our expectation of their security concerns and generally lean towards the secure side. Software Download is ranked as the most insecure service with a slight negative. This is probably because of the awareness that it has become a most direct way of distributing malware.

However, the trust of users' communications software such as Email and Instant Messenger are just slightly lower than Shopping Online. This is probably an over-optimistic view from a technical standpoint since they Email and Instant Messenger are mostly done as clear-text transmission subject to the risk of interception attack. Both allow files to be attached or transmitted and hyperlinks to be sent which makes them popular carriers of worm, spam and phishing attacks. This is supposed to be in strong

contrast with Shopping Online which is typically protected by 128-bit strong encryption, such as SSL, against interception attacks, and Certificate Authority (CA) services such as VeriSign which potentially protect against phishing attacks. Another possibility is that the users' overall security concern has affected the consumers' confidence online, especially when the users are unfamiliar with the technical factors of the security of a certain Internet service.

Table 3. Perceptions of the Security of Various Internet Services

Perception of the Service Security	OS†	ES‡	IM*	SD**
Very Secure (4)	10.0%	17.8%	18.9%	1.1%
Somewhat Secure (2)	72.2%	62.2%	53.3%	44.4%
Somewhat Insecure (-2)	15.6%	10.0%	18.9%	36.7%
Very Insecure (-4)	1.1%	8.9%	5.6%	14.4%
Not Sure (0)	1.1%	0.0%	2.2%	1.1%
Weighted Average (±4)	1.5	1.4	1.2	-0.4

† Online Shopping
‡ Email Service
* Instant Messenger Service
** Software Download

Another set of questions were designed to find out the users' experiences with spam and phishing emails (Table 4). Most of the users did not report a high frequency of email spam and are satisfied with their email service and spam filter. Only 10% of the users reported receiving phishing email, which sounds a bit low to the authors, but this could be due to the fact that some users don't really know what constitutes such an email. We also surveyed the users' preference regarding email and instant messenger services.

Table 4. Users' Spam and Phishing Email Experiences and Service Preferences

On average, how often do you receive spam (junk) email messages?	
None	37.8%
A few times a week	33.3%
Almost daily	12.2%
Least one per a day	7.8%
Many per day	8.9%
Have you ever received phishing email?	
Yes	10.0%
No	80.0%
Not Sure	10.0%
How well is your spam (junk) email filter working?	
Great	48.9%
Fine	35.6%
Poorly	15.6%
Not at all	0.0%
Spam/junk/phishing is affecting my email usage:	
Yes	22.2%
No	77.8%
Which email account do you use the most?	
School/Work	73.3%
Yahoo!	13.3%
MSN/Hotmail/Windows	10.0%
AOL	7.8%
Gmail	6.7%
ISP Providers	3.3%
Netscape	1.1%
Which instant messaging software do you use the most?	
AIM	81.1%
AOL	14.4%
MSN	4.4%

Identity theft is a cyber crime that has potential of high danger to the victim due to the potential financial and credit loss. In order to understand the Internet users' knowledge/experience and protection actions against it, we designed the following questions and the results are presented in Table 5. It shows that although just about one quarter of the users experienced or heard of someone experiencing identity theft, three quarters of the users are noticing the existence of the new insurance protective services (provided by financial institutes with insurance companies) and these services are acknowledged by more than half of them (63.2%) and some of them are already using such services (14.7%).

Table 5. Identity Theft Knowledge/Experience and Protection

Have you or someone you know experienced identity theft?	
Yes	24.4%
No	75.6%
Have you heard of identity theft protection services or identity theft insurance?	
Yes (people heard of it)	75.6%

Do you personally use one of these services?	
Yes (out of people heard of it)	14.7%
Do you think they are worthwhile and trustworthy?	
Yes (out of people heard of it)	63.2%

Internet Users' Security Practices

We surveyed the Internet users' security practices such as software updates (Table 6), firewall usage (Table 7) and the anti-virus/anti-adware/anti-spyware practices (Table 8).

Manual/automatic update operations for operating system and application software are what the current software industry relies intensively on to distribute security patches for known vulnerabilities. We first checked the frequency of users' software updates that they personally perform (manual update operations). We found that 45.6% of them either never update their operating systems manually or at a very low frequency (yearly) and 55.5% of them never or at a very low frequency (yearly) update application software manually.

The software industry is conscious of the users' general tardiness in downloading and installing patches and hence many modern software systems come with residential auto-updater programs that run periodically to check for updates, download and install them automatically when the user is online. We found that although 68.9% of the users enable the auto-update features when installing software, only 45.6% believe that it is helpful, with 34.4% of the remaining users staying neutral and 17.8% of the users responding negatively to these features. This perhaps reflects the fact that the current auto-update process might be too time-consuming and annoying to some users.

This passive attitude of many of the users' should draw attention to the software industry since the current users have shown high awareness for the importance of security issues, reflected by their high ranking of the importance of security education. We can tell from this contrast that the high reliance on patch distributions after a major software release is taken on passively by many users. So software companies must improve their software engineering from the beginning to develop high quality secure software to reduce this reliance and improve the customer satisfactory in the long term. This also implies the importance of secure programming and software engineering skills in CS/IT/MIS education to ensure students' qualification as developers of more secure future generations of software.

Table 6. Users' Software Update Practices

How often do you update/patch your operating system (such as Microsoft Windows, Linux)?	
Never	15.6%
Yearly	30.0%
Monthly	38.9%
Weekly	10.0%
More often than weekly	3.3%
How often do you update/patch software (such as Microsoft Office, Internet Explorer, Acrobat Reader)?	
Never	13.3%
Yearly	42.2%
Monthly	30.0%
Weekly	8.9%
More often than Weekly	2.2%
Do you enable the auto-update feature when installing?	
Yes	68.9%
No	31.1%
Do you find the auto-update features of operating system and software to be?	
Helpful	45.6%
A waste of time	17.8%
Neutral/Indifferent	34.4%

The Internet users' practice of applying software firewalls on their PC and on their home networks are 71.1% and 68.9% respectively (Table 7). Although the percentages themselves may look high, in consideration of the importance of such network utilities in the defense of automated scanning/backdoor/compromise attacking tools, the remaining Internet users leave their networks/PCs directly exposed which raise serious security concerns. This provides even novice cyber attackers an opportunity to easily compromise large amount of home/personal PCs for identity theft or recruit them as zombies for DDoS (Distributed Denial of Service) attacks.

Table 7. Users' Firewalls Usage Practices

I use/enable firewall on my computer.	
Yes	71.1%
No	11.1%
Not Sure	16.7%
I use/enable firewall to my home network.	

Yes	68.9%
No	11.1%
Not Sure	17.8%

We also surveyed the users' practice of software protection of their PCs (Table 8). Even though some of the users weren't sure if they use such software, they did recognize specific product names (Norton/Symantec, MacAfee, Ad-aware, Spybot, Spyware Doctor or Other), so we count them as protective software users. We found that the majority of the users (90.0% for antivirus and 88.9% for anti-spyware/anti-adware) are aware of the usage of these defensive tools to protect against malware. Most of the users (70.0% for antivirus and 72.2% for anti-spyware/anti-adware) scan their system frequently (at least monthly). Some of the users (30.0% for both antivirus and anti-spyware/anti-adware) are not aware of the importance of updating the malware definitions. This is an indicator that some protective software users (about one third) are not aware that these 'blacklist' malware defense tools rely highly on up-to-date malware signature databases to effectively recognize and remove fast evolving malwares.

Table 8. Users' Malware Protection Practices

I use antivirus software.	
Yes	86.7%
No	1.1%
Not Sure	12.2%
How often does the antivirus software scan your computer?	
Never	3.3%
Yearly	3.3%
Monthly	30.0%
Weekly	32.2%
More often than weekly	17.8%
How often do you update the virus definitions?	
Never	11.1%
Yearly	18.9%
Monthly	28.9%
Weekly	18.9%
More often than weekly	7.8%
Which type of antivirus software do you use?	
Norton/Symantec	68.9%
MacAfee	20.0%
Other	1.1%
I use anti-spyware/anti-adware software	
Yes	73.3%
No	5.6%
Not Sure	17.8%
How often does the anti-spyware/anti-adware software scan your computer?	
Never	4.4%
Yearly	2.2%
Monthly	30.0%
Weekly	27.8%
More often than weekly	14.4%
How often do you update the spyware/adware definitions?	
Never	10.0%
Yearly	20.0%
Monthly	26.7%
Weekly	13.3%
More often than weekly	6.7%
Which type of anti-spyware/anti-adware software do you use?	
Ad-aware	36.7%
Spybot	38.9%
Spyware Doctor	11.1%
Other	2.2%

SUMMARY OF FINDINGS

From the survey results, we can draw the following findings. First, the current Internet users' general awareness of the importance of cyberspace security education is relatively high. This relatively high awareness is probably the consequence of the combination of media efforts (including new media such as the Web and traditional media such as TV and newspaper) and personal experiences (such as experiencing malware infection, identity theft or system compromise). This perception of the importance of being educated about cyberspace security is a positive power to improve security defense practice. However, this has not led to immediate best practice defense for most users, reflected by the unawareness of patching software vulnerabilities frequently, applying defense tools universally (including firewalls, antivirus and anti-spyware/anti-adware software) and keeping them effective (such as frequent update of the malware definitions). This probably is due to the fact that most users are not familiar with the venues of such security threats and therefore cannot fully understand the roles of different defense strategies and defense utilities in enhancing cyber security.

Therefore, cyber security education for Internet users through different media needs urgent improvement. This includes more systematic Internet security education in higher education with a discussion of the larger cyber security picture with various security threats, attack venues, defense strategies and defense tools. Since college students will be future professional employees in organizations, this effort is important for better cyber-security practices of organizations.

Meanwhile, secondary schools also need to improve cyber security education. The current college student began using computers (mostly with Internet access) at an average age of 10 years old (from Table 1, average age and years of computer usage). Therefore, they have been active Internet users for many years before entering college. This population constructs a significant portion of the current Internet users. And this trend is on the rise with the computer hardware/software becoming more affordable and universal broadband Internet access expanding in households. Poorly protected home computers not only construct security threats to their owners, but also potential threats to other Internet users since they can be easily compromised and recruited as 'zombies' in Botnet for DDoS to other servers on the Internet. Moreover, easy compromises also help to fuel the quickly maturing cybercrime economy.

The public media could also play a more active role in raising cyber security awareness. The high awareness of cyber identity theft risks and the recognition of identity theft insurance is a proof of the public media's effectiveness in improving the general public's cyber security knowledge and practices.

Second, The Internet users' tardiness for manual software updates and passive attitudes towards automatic updates should draw the attention of the software industry. The current users have shown high awareness for the importance of security issues while the current high reliance on patch distributions after major software releases is taken passively by users. Software vendors must improve secure programming and software security engineering in the development lifecycle to deliver higher quality secure software in order to reduce vulnerabilities and improve the customer satisfactory in the long term. This also implies the importance of teaching secure programming and software security engineering in CS/IT/MIS curriculum to improve students' qualifications as developers of more secure future generations of software.

Finally, the complexity of the current defense system seems to be overwhelming to regular users. This is reflected in the failure of significant amount of users in activating firewalls, installing (or tolerating automatic updates) software or malware definition updates, and be cautious enough when using Internet services without strong built-in security. This raises the issue of how to make the future generation of defense systems more fool-proof and upgrading the built-in security of the existing Internet services such as Email and Instant Messenger. The new Windows Vista security center is an effort of making the defense system a one stop check point of defense tools. However, many organizations and individuals have not made the transition to Vista because of concerns of software compatibility issues and certain new security features such as UAC (User Account Control) does cause some legacy software to fail.

REFERENCES

1. CERT. (2008). *Full Statistics of cert.org.* Available from http://www.cert.org/stats/fullstats.html [accessed 11/01/2008].
2. Espiner, T. (2008). *Cracking Open the Cybercrime Economy*. Available from http://www.news.com/Cracking-open-the-cybercrime-economy/2100-7349_3-6222896.html [accessed 11/01/2008].
3. Galetsas, A. (2007). *Statistical Data on Network Security*. Available from ftp://ftp.cordis.europa.eu/pub/ist/docs/trust-security/statistics-network-security-050307_en.pdf [accessed 11/01/2008].
4. Gutmann, P. (2008). *The Commercial Malware Industry*. Available from http://www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf [accessed 11/01/2008].
5. Hardee, J. B., West, R., & Mayhorn, C. B. (2006). *To Download or Not to Download: An Examination of Computer Security Decision Making*, ACM Interactions, 13(3), 32-37.
6. Jones, L. A. Antón, A. I., & Earp J. B. (2007). *Towards understanding user perceptions of authentication technologies*, Proceedings of the 2007 ACM workshop on Privacy in electronic society, Alexandria, VA, USA, 91-98.
7. Nowak, M., Rao, S., Nass, C., Lewenstein, J., Meyer, A., & Richman, J. (2009). *Toward an experimental methodology for studying persuasion-based online security*, Proceedings of the 27th international conference extended abstracts on Human factors in computing systems, Boston, MA, 4033-4038.

8. Symantec. (2006). *Cybercrime: A Disturbing Trend*. Available from http://www.symantec.com/norton/products/library/article.jsp?aid=cybercrime_a_disturbing_trend [accessed 11/01/2008].
9. Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). *Empirical Study of Students' Computer Security Practices/Perceptions*, Journal of Computer Information Systems, 47(3), 105-110.
10. Van Slyke, C., Belanger, F., & Comunale, C. L. (2004). *Factors Influencing the Adoption of Web-Based Shopping: The Impact of Trust*, ACM SIGMIS Database, 35(2), 32-49.