

HOME COMPUTER SECURITY AWARENESS

Sponsoring faculty: Dr Rose Shumba

Students: Melissa A Karolewski, Alicia Coon, Sara Raffensperger, Louisa Ehinlaiye Ometere Computer Science Department
Indiana University of Pennsylvania

Shumba@iup.edu, M.A.Karolewski@iup.edu, A.A.Coon@iup.edu, hjrl@iup.edu, tmtj@iup.edu

ABSTRACT

Home computer security is often a neglected area of security. In the Fall of 2004, with funding from the ACM CREU (Collaborative Research Experience for Undergraduates in Science and Engineering) program, a project on home computer security was started. The goal of the project was to enhance the public's understanding and acceptance of information security issues through awareness and education. The project consisted of three phases: the identification of currently used practices for computer security, an evaluation of the practices and then a public¹ awareness and education outreach program on the importance and relevance of computer security. Through a questionnaire survey, currently used practices for home security were collected and analyzed. The target population was the IUP student community. During the identification phase, a questionnaire was administered to random IUP classes. From the results of the survey, a list of the best of breed security tools were identified and reviewed. During the last phase, the research was presented to three groups of high school students during the 2005 Natural Science's Science Festival.

KEY WORDS

Computer Security, Home Computer, Survey Results.

1. Introduction

The general public is often isolated from awareness and training opportunities in information security, yet the security of the cyberspace rests on the security of all its components. Although there is a reasonable number of websites with tips on protecting home computers [16, 18], these often have some technical vocabulary or are not known by the public, hence are seldom visited. Many computer owners don't realize the need to pay attention to computer security. No matter how a computer is connected to the Internet, intruders' attacks are

often successful. Security issues for home users are just as real as security for business users, perhaps more so because home users don't have enough resources to ensure proper security.

In the Fall of 2004, with sponsorship from the ACM CREU program, a research project on home computer security was started. The goal of the project was to enhance the public's understanding and acceptance of information security issues through awareness and education. The project consisted of the following three phases:

1. The identification of currently used practices for computer security.
2. An evaluation of practices identified in 1 above, and
3. Public awareness and education on the importance, and practices for home security.

This paper is based on phase 1 of the project; the identification of currently used practices for computer security. In order to identify the commonly used practices and tools for computer security, a questionnaire survey research was carried out at IUP in the Fall of 2004. This paper describes the methodology, findings from the questionnaire survey research, and the future work on the project.

2. Methodology

As stated in the introduction, the project was divided into three phases. The first phase of the project was completed in March 2005. A questionnaire survey was administered to the 350 multi-disciplinary IUP students. The aim of the survey was to capture as much data on current practices for computer security. The questionnaire was based on techniques to secure a home computer as given by the CERT Coordination Center [16], and the United States Home computer Emergency Readiness Team [17]. The techniques include good password management, email security, use of anti-virus

¹ The public in this case is the IUP community.

and anti-spyware software, use of firewalls, care in installing programs, use of encryption, backing up of files, care in sharing files, and securing wireless networks. Students from all disciplines participated. Target classes were picked at random. Questionnaires were administered at the start of a targeted class session. The questionnaire had 24 questions which included multiple choice, numeric open end and text open end. A sample of the questionnaire is attached. Participants were given 15 minutes to complete the questionnaire.

2. Analysis of Collected Data

The collected data was input analyzed using Excel. The following paragraphs provide an analysis of the data.

78% of the participants understood the difference between anti-virus and anti-spyware programs. McAfee, with a 47% usage rate, was the most commonly used anti-virus programs, followed by Norton with 34%. The rest of the participants used nothing or other software not listed. Of the participants who used anti-virus programs, 27% claimed updated program(s) on a weekly basis, 14% updated program(s) on a daily basis and 20% updated program(s) on a monthly basis. The rest of the participants (39%) did not know if they updated, didn't know how to update, or never updated.

Ad-ware and Spyware-Eliminator are the most popular, with usages rates of 50% and 17% respectively. 12% of the participants used other various programs. 21% of the participants either had no anti-spyware or were unaware if they had any anti-spyware program. Of those who used anti-spyware software, 30% updated programs weekly, 19% updated daily and 51% either never updated or didn't know how to do the update.

The most popular firewall was Microsoft (windows) Firewall at 23% usage. The followed by McAfee Personal Firewall at 21%, then ZoneAlarm at 11%. The majority of the participants did not know if they had a firewall or not.

Survey data shows that 71% of the participants did not use the same passwords for different

logins. 51% did not use unique² passwords. 33% of the participants never changed passwords and 40% only changed when necessary. 5% changed passwords 9-12 times/year, 3% changed passwords 5-8 times/year, and 19% changed passwords 1-4 times/year. 74% of the participants remembered passwords without writing them down. 22% used passwords that had something to do with them, i.e. child's name, type of car, an interest, etc. These were easy to remember. The rest of the participants did not remember their passwords, and hence had to write them down.

70% of the participants shared the use of home computer with others. Of the 70%, 44% shared with 1-2 other users, 47% shared with 3-4 other users, and 9% shared with 5-8 other users. Of those who shared computers, 58% restricted access to certain files, the rest did not. 31% used a file-sharing, 12% were unsure, and 57% did not.

58% of the participants had a wireless network in their home. Of those with a wireless network, only 8% had the network secured.

38% of the participants had encryption software. The rest either did not have it or did not know if they had it. Of those with encryption software, only 6% encrypted their files and emails.

51% of the participants took time to learn much about programs before installing. Only 32% purchased program, 48% got programs from a national chain, and 20% obtained programs from elsewhere.

45% of participants always scanned attachments. Of the 45%, only 9% always scanned, and 11% scanned sometimes. The rest scanned when they felt like. When attachments came from friends, 5% always scanned, 20% almost always, 20% scan sometimes, and 55% never scanned.

26% of the participants backed up files once a month, only 6% backed up everyday, and 8% backed up monthly. The remaining 60% either didn't know how to back up or never bothered.

Patches for the OS was either downloaded manually for those with knowledge about it, and for others the OS automatically updated itself.

² A unique password is a combination of letters, numbers and/or punctuation marks.

These patches were downloaded weekly, monthly and yearly; even though some did state that they had no idea if patches were downloaded or not. 16% of the participants updated patches with 21% doing it automatically.

3. Conclusion & Future Work

From the results of the survey, there is no doubt need to bring home computer security awareness to the public. The researchers organized a number of computer security awareness seminars for the IUP community. The researchers presented their presentation to high school students during the 2005 IUP Natural Science Festival. These seminars stressed the importance of an anti-virus and anti-spyware program on a computer, difference between anti-virus program(s) and anti-spyware program(s) functionalities, importance of updating computer security software, ways of restricting access to personal files, how to secure a wireless network, the need to read learn as much about a program before installation, the necessity of scanning all email attachments, regardless of who send the email, importance of backing up important files and folders, importance of good password management and the importance of having a firewall on a home computer.

References:

1. <http://www.chartwellsystems.com/sscalc.htm#ssneeded>.
2. http://www.cc.gatech.edu/classes/cs6751_97_winter/Topics/quest-design/.
3. http://www.cert.org/tech_tips/home_net_works.html
4. <http://www.tuketu.com/dsl/information-security/Securing%20DSL.htm>
5. <http://www.members.aol.com/gaf5200/myhomepage>.
6. <http://www.seattlepi.nwsourc.com/business/hack221.shtml>
7. <http://www.tech-forums.net/computer/topic/701.html>
8. http://www.3com.com/corpinfo/en_US/technology/tech_paper
9. <http://www.sarc.com>
10. <http://www.agnitum.com>
11. http://www.linuxsecurity.com/resources/host_security-1.html
12. <http://www.nic.com/~dave/SecurityAdminGuide/SecurityAdminGuide-4.html>
13. http://www.digitalsecurityconcepts.com/host_security.htm
14. <http://www.bb-zone.com/SLGFG/chapter24.html>
15. Garfinkel, S. Spafford, G, Schwartz, A; Practical Unix and Internet Security; O'Reilly; Third edition; 2003.
16. <http://www.cert.org/homeusers/HomeComputerSecurity/>
17. <http://www.us-cert.gov/>
18. [http://www.staysafeonline.info/enroll.adp](http://www.staysafeonline.info/enroll.asp)

Questionnaire

We are carrying out a research on what practices you are using to secure your home computer. Please answer the following question about you home computer.

1. Do you understand the difference between Anti-Virus Programs and Anti-spyware programs?
___Yes___No

2. What Anti-Virus Program do you use?
 - a. McAfee Anti-Virus
 - b. Microsoft (Windows) Anti-Virus
 - c. Norton Anti-Virus
 - d. Linux Anti-Virus
 - e. Mac Anti-Virus
 - f. Other _____
 - g. Don't know
 - h. Don't have Anti-Virus

If you do not use anti-virus software, why don't you?

 - a. I don't use the internet.
 - b. I don't understand anti-virus software.
 - c. Other: _____

3. How often do you update your Anti-Virus software?
 - a. Daily
 - b. Weekly
 - c. Monthly
 - d. Never
 - e. Don't know
 - f. Don't know how

4. Do you use an Anti-Spyware Program?
 - a. Ad-aware
 - b. Spy Killer
 - c. XoftSpy
 - d. Spyware Eliminator
 - d. None
 - f. Don't know
 - g. Other _____

5. How often do you run the Anti-spyware?
 - a. Daily
 - b. Weekly
 - c. Monthly
 - d. Never
 - e. Don't know
 - f. Don't know how

6. How often do you update your Anti-spyware program?
 - a. Daily
 - b. Weekly
 - c. Monthly
 - d. Never
 - e. Don't know
 - f. Don't know how

7. What kind of firewall is installed on your computer?
 - a. McAfee Personal Firewall
 - b. Zone Alarm Firewall
 - c. Microsoft (Windows) Firewall
 - d. Norton Firewall from Symantec
 - e. Linux Firewall / Linux Network Firewalls
 - f. Apple Quicktime Firewall
 - g. Don't know
 - h. Don't have Firewall
 - i. Other _____

8. Do you use the passwords over and over again for different logins? (e.g. Programs, network login, e-mail.)___Yes ___No

9. Do you use unique passwords? (i.e. a combination of letters, numbers or punctuation marks) ___Yes ___No ___Sometimes

10. How often do you change your passwords?
 - a. 1-4 times/year
 - b. 5-8 times/year
 - c. 9-12 times/year
 - d. never
 - e. Only when I must

11. Do you remember the passwords that you create?
 - a. Yes
 - b. Yes, because they are something that is about me, i.e. child's name, spouse's name, type of car you drive, an interest, etc.
 - c. No, but I have them written down.
 - d. No, I can never remember them.

12. Are you the only user of your home computer? ___Yes ___No
 If No, how many other people use it with you? _____
 Have you limited access of certain files and folders to certain users?
 ___Yes ___No ___Don't know

13. Do you use file sharing networks? _____Yes _____No _____ Don't know

14. Do you have an Encryption software on your home computer?
 _____Yes _____No ___Don't know
 If yes, what kind is it? _____

15. How often do you update your Encryption software?
 - a. Never/Don't know/Don't have Encryption software
 - b. Every night
 - c. Once a week
 - d. Three or more times in a month
 - e. Every other month

16. Do you encrypt your important files and folders? ___ Yes ___ No

17. Before you buy and install a program to your home computer, do you learn as much about the program as you can? ___Yes ___No

18. When you buy a program where do you mainly purchase them from?
 - a. A local store
 - b. A national chain
 - c. Other _____

19. Do you scan attachments from unknown e-mail sources?
 - a. always
 - b. almost always
 - c. sometimes
 - d. almost never
 - e. never
 - f. Don't know

20. Do you scan attachments from known e-mail sources? (such as friends and family)
 - a. always
 - b. almost always
 - c. sometimes
 - d. almost never
 - e. never
 - f. Don't know

21. How often do you backup important files on your home computer?
 - a. Once a month
 - b. Every week
 - c. Every day
 - d. Never/don't know

22. How often do you update/download patches for you operating system?

- a. Weekly
- b. Monthly
- c. Yearly
- d. The OS automatically updates itself
- e. Never/Don't know

23. Do you have a wireless network in your home? ____Yes ____No ____Don't Know

24. If yes, is it secured? ____Yes ____No ____Don't Know