# Computer Security: Just How Secure Is Your Computer?

Edward A. Schmalz

*Forensic Technology Group, Inc.*

## Abstract

Security has become a matter of utmost importance since the aftermath of September 11th, especially in the area of computer systems. There are many options that a health educator can do as an individual to help secure the computer system at their worksite and in their home. This article is a brief overview of some of the precautions that should be taken on a daily basis to protect your computer systems, files, data, and other pertinent information.


*Keywords: metadata, firewall, spyware, virus*

## Introduction

Do you know how safe your computer system is at work or for that matter at home? According to the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) Computer Crime and Security Survey, 99% of companies use antivirus software, but 82% of them were still hit by viruses and worms (Computer Security Institute & Federal Bureau of Investigation, 2003). One of the reasons is that that they do not have a worm protection program also in place. A worm is "a program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down" (Webopedia, 2005).

Since the aftermath of September 11th, national security, in particular security with computer systems has become a priority in this country. Computer systems are prime targets for terrorists because they can disrupt the economy by tampering with the records of financial institutions, create havoc in health education organizations by inserting a virus to disable the entire system and the population in general by upsetting our everyday lives. Health educators and other professionals have come to rely on the computer for an assortment of things in our daily lives. Examples are: we send e-mails both at work and at home; we do our banking and other transactions online; we store important data on our computers at work which may contain lists of clients, patient information, billing records and other statistical information. With this awareness, ask yourself these questions, "Is my personal or work information safe?" "Are my documents safe?" "Am I using a wireless Internet connection that can be accessed from a remote location?"

Throughout this article, I make suggestions for health educators, regardless of their worksite, to improve the security of the important data listed above.

Let's discuss your computer at work. When you first started at your place of employment did the Human Resource (HR) or Information Technology (IT) person ask you to sign a document explaining what you could or couldn't do on the computer while you were working? These documents have different names such as Internet Protocols or Netiquette Agreements, which state that if you violate any of the provisions of the agreement you can be terminated from your position. Some of these provisions outline what can be downloaded from the Internet. According to statistics, 80 percent of companies reported that employees had abused their Internet privileges by downloading pornography or pirated software (CSI & FBI, 2003). Be careful what you download, and what you write in an email or other documents stored

on your computer because your files may be audited and potentially be used in some form of litigation.

**Password Protection**

At your worksite, were you provided with a username and password for the computer? Most organizations keep track of when a person is logged on to their computer, the e-mails that were sent or received, access to other computers on the network or Internet sites visited. You should be cognizant that someone is tracking every move you make on the computer. If you are not provided with a password, you need to create one. Passwords are one way in which you can keep the information stored on your computer safe. Passwords should be kept secure from everyone. Never give your password to anyone and do not write your password down on a piece of paper and leave it in the top drawer of your desk or on a Post-it® taped to the side of your monitor. Use a password that will not be easily discovered by someone else. It is highly recommended that you use a series of letters, numbers or symbols, both upper and lowercase. For example, a password could be 34y&GH8. Some of the commonly used passwords are birth dates, children's or husband's names, social security numbers, telephone numbers or other information that is relevant to the individual. A good practice is to change your password at least once a month. Do not walk away from your computer while you are still logged on because this allows someone else to obtain data from your computer and you will ultimately be held responsible for it. Some places of employment have a system whereby if you are away from your desk or haven't entered any keystrokes in a specific amount of time, you will be automatically logged out of the system, requiring you to log back on with your password. Remember to log out of your computer or shut it down completely when leaving work. There is a possibility that there are other workers in the office after hours and if your computer is still running that they could extract important information from your machine.

**Virus Protection**

If your computer is connected to a network or the Internet, there is a likelihood that you might contract a computer virus. A computer virus is defined as "a piece of code that is loaded onto your computer without your knowledge and is designed to attach itself to other code and replicate it. It replicates when an infected file is executed or launched" (Solomon, Barrett, & Broom, 2005, p. 272). Computer viruses can be spread in many different ways such as through a network, by inserting a floppy disk, CD-ROM, zip disk or a flash or jump drive (a flash or jump drive is a small portable hard drive that plugs into the Universal Serial Bus [USB] port) in your computer that contains the virus, and more recently by the World Wide Web, through emails and by sharing files. The most common target of a virus is the executable files that contain application software or parts of the operating system. Computer viruses can be prevented or at least kept to a minimum by using various means of software programs and hardware in tandem. Since email is one of the easiest ways to spread or receive a virus, I have included a simple test that might help you prevent getting a virus on your computer system; it is called the KRESV test. Below are the KRESV steps to follow for any email that contains an attachment:

1. The Know test: Is the email from someone that you know?
2. The Received test: Have you received email from this sender before?
3. The Expect test: Were you expecting email with an attachment from this sender?
4. The Sense test: Does email from the sender with the contents as described in the Subject line and the name of the attachment(s) make sense? For example, would you expect the sender – let's say your Mother – to send you an email message with the Subject line "Here you have, ;o)" that contains a message with attachment – let's say *AnnaKournikova.jpg.vbs?* A message like that probably doesn't make sense. In fact, it happens to be an instance of the Anna Kournikova worm, and reading it can damage your system.

5. The Virus test: Does this email contain a virus? To determine this, you need to install and use an anti-virus program. (Rogers, 2005)

There are several manufacturers that can provide software programs that block viruses from entering your computer. Norton AntiVirusTM by Symantec Corp. and Virus Scan by McAfee are two of the biggest on the market. These programs should run continuously when the computer is in use; virus definitions should be updated on a weekly basis. Then, if a new computer virus has surfaced, it will be detected in the shortest amount of time. There is also hardware and software available in the form of firewalls. A firewall is a system that prevents unauthorized access to or from a private network (Webopedia, 2005). One of the key functions of firewalls is to prevent people using the Internet from accessing other networks that are connected to the Internet. The network will contain specific security features that monitor each message that is being transmitted or received. Only messages that meet these security features will be allowed to enter or leave the network. However, there may be conflicts with different software programs. For example, if you are running Microsoft Windows XP Professional with Service Pack 2 (SP2), you should not run the Norton Firewall. Microsoft Windows XP Pro with SP2 comes with a firewall built into the program and is incompatible with the Norton Firewall software. It is also important to have anti-worm protection on your system if it is not part of your antivirus program.

**Spyware**

Spyware is computer software that gathers and reports information about a computer user without the user's knowledge or consent (Webopedia, 2005). If you are on the Internet and you get a pop-up (unsolicited advertisement) while you are working, this is a form of spyware (Solomon, Barrett, & Broom, 2005). Spyware can include other programs namely malware. Malware is a software program intended to cause harm to a computer in the form of a virus, worm, logic bomb or trojan horse (Solomon, Barrett, & Broom, 2005). The number of malicious code attacks with backdoors, which are often used to steal confidential data, rose nearly 50% in the last year (Symantec, 2003). There are several anti-spyware programs available at no cost on the Internet. Spybot Search and Destroy (available at http://www.safer-networking.org) and AdAware (available at http://www.lavasoftusa.com) are two valuable programs to have on your computer. The programs should be run frequently to check for various types of spyware and viruses. Some spam (unsolicited bulk e-mails used for the purpose of advertising) may contain a virus. There are software and hardware solutions to reduce or eliminate spam or pop-ups. In my opinion, one hardware device that works very well is the Barracuda Spyware Firewall from Optrics Engineering. It blocks spam, spyware and viruses. When we install computer systems in different organizations, we suggest that they install this hardware. In one of our small corporate office networks that we monitor, it has the Barracuda Spyware Firewall and in just one 24 hour period, it prevented over 1500 pieces of spam and 65 viruses from entering the network.

Metadata

Metadata is defined as “definitional data that provides information about or documentation of other data managed within an application or environment” (Webopedia, 2005). In its simplest form, it is “data about data.” Your organization must be aware of metadata in regards to the use of the Internet for the transmission of documents to clients, patients, to other people within your organization or to other agencies. Metadata can include, but is not limited to: author’s name, author’s initials, author’s company or organization, the creation date of the file, the last modification date of a file, who made the modification and when, how many times the document has been revised and hidden text. The metadata may be pertinent if the file is used in litigation. This information might be confidential and you do not want this metadata to accompany the file or reveal confidential information about your clients. Metadata is present in programs such as Corel WordPerfect and Microsoft Office, which includes; Word, Excel, and PowerPoint. If you

are using Microsoft Word, some of the above information is available by selecting the "file" option from the toolbar menu. Under that heading select "properties." Under "Properties" many of the above pieces of information can be observed. Remember, when you send a file to someone, either through the Internet or some other type of media (a floppy diskette or CD-ROM for example) all of the above information becomes available to that person. There are also software programs available to view metadata. These viewers record the last ten authors of a document, who the document was routed to through e-mail, how many revisions were made, changes made to the text, who made the changes and when they were made. They can also include the author's comments, hidden text and possibly sensitive information.

If you are using Microsoft Word as your word processing program, Microsoft Corporation has made available, through its website, a patch (update) that will permanently remove hidden data and collaboration data, such as change tracking and comments, from Microsoft Word documents (Solomon, Barrett & Broom, 2005). See the following link for more information. (http://www.microsoft.com/downloads/details.aspx?FamilyID=144E54ED-D43E42CA-BC7B-5446D34E5360&dispalylang=en).

Wireless Internet Connections

Does your office or home computer use a wireless network to connect to the Internet? How secure are these connections? It is not uncommon that people from outside your work or home can access your computer. There are encryption programs available that block the transmission of your signal to outside people. One is known as Wired Equivalent Privacy (WEP). This provides security by encrypting the data over the radio waves so that it is protected from one point to another (Webopedia, 2005). Another method that is used is Wi-Fi Protected Access (WPA), which is more secure than the WEP method. WPA has improved on the encryption method by using a hashing algorithm and by using an extensible authentication protocol (EAP), which uses a more secure public-key encryption that only allows authorized network users to use the network (Webopedia, 2005). It is recommended for you to invest in one of the two programs listed above.

**Summary**

In conclusion, I have mentioned various methods that you can use to safeguard your computer and the valuable information that it contains. Remain vigilant when you are working with your computer and do not allow unauthorized access to your personal or organizational files. If your organization does not employ some of the above mentioned security devices it might be a good time to mention it to someone who has the authority to make changes. The loss of information can be devastating and could possibly ruin an organization.

**References**

Computer Security Institute & Federal Bureau of Investigation. (2003). Computer crime and security survey. Retrieved August 30, 2005, from http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf

Rogers, L. (2005). Use care when reading email with attachments. Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute. Retrieved August 30, 2005, from http://www.cert.org/homeusers/email-attachments.html

Solomon, M. G., Barrett, D., & Broom, N. (2005). Computer forensics: Jump start. Alameda, CA: SYBEX, Inc.

Symantec Corporation. (2005). Trojan.Hotword.B. Retrieved June 17, 2005, from http://securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.b.html

Webopedia.com. (2005). Webopedia – online encyclopedia for computer technology homepage. Retrieved August 30, 2005, from http://webopedia.com/

Author Information
Edward A. Schmalz, Ed.D.
Certified Computer Examiner (CCE)
Forensic Technology Group, Inc.
Westwood, New Jersey