Global Information Assurance Certification Paper

A USERS GUIDE TO SECURITY THREATS ON THE DESKTOP

Richard D. Hagen

SANS Security Essentials Course
GSEC Practical Assignment
Version 1.2e

July 22, 2001

Table of Contents:

INTRODUCTION

Everyone who uses a computer has heard of Internet security issues such as viruses, e-mail scams, and hacker attacks. Many computer users don't see the need for security or feel helpless in the face of hacker attacks. Both of these assumptions are false as will be discussed in this paper. This paper is written for non-technical computer users who need to know the security risks of the Internet and how to protect their important digital information.

WHY COMPUTER USERS SHOULD BE CONCERNED ABOUT SECURITY

Evidence of the need for security protection is everywhere. There is new of a new attack on someone's computer system or a new computer virus such as 'I love you' or 'Melisa' almost weekly. As this paper was being written a Knight Rider Newspaper news article came across my desk reporting two new viruses called Magistr.A and Funlov.4099. These new viruses spread very rapidly and use both e-mail and networks to spread. This is an increase in the lethalness of these viruses.

According to the 2000 ICSA Computer Virus Survey, 14 out of every 1,000 computers encounters a virus monthly. An FBI and Computer Security Institute, March 2001 survey of 538 Security Managers, 85% reported breaches of their security, which more than doubles the 42% that reported attacks in 1999. Every computer needs protection!

All this concern about information and computer security comes from the sad fact that there are individuals, called 'hackers', who use the Internet to vandalize computers and commit crimes. Criminals use modern technology such as the telephone, and mail system. The Internet is just the latest technology available to the criminal.

Hackers' use their programming skills in various ways. They create viruses, illegally access computer systems, and tie up computer networks with useless information. Another group called scam artists uses the Internet for financial gain by illegally getting credit card numbers, and other private information.

WHAT CAN BE DONE TO PROTECT THE COMPUTER AND INFORMATION

The average computer user is far from defenseless. There are many things that can be done to improve the security of the desktop computer and the information it contains. There are three major areas to be concerned with in the security arena.

- **Confidentiality of Information** – This refers to information on a computer being used only by the people for whom the information is intended. The computer system needs to know who is authorized to use information and who to keep out.

- **Integrity of Information** – This refers to being able to trust that the information is true and accurate. Information should only be added or modified by authorized people and

programs.

- **Availability of Information** – This refers to information and data being available when needed. The computer hardware and software must be up and running or it is useless.

There are several important actions that the average user can take to help assure the confidentiality, integrity and availability of computer systems and information. The areas of security a user has direct impact on and which will be discuss in this paper are:

- **Follow good password practices**
- **Monitor and manage e-mail accounts**
- **Provide virus protection on the desktop PC**

The home user should also consider a personal firewall, particularly if connected by cable or DSL. These connections are always on and often have static or permanent IP addresses. Attackers can see your computer whenever the computer is turned on. Personal firewalls will be discussed briefly at the end of this paper.

GOOD PASSWORD SECURITY PRACTICES

Standard practice on most computer systems is to use a two-part user identification system. The first part is the user identification name (user-id). The user-id identifies what computer systems, accounts, and databases a person has a right to use. The second part is a secret password known only to the user and the computer system. This is how the computer verifies that the person identified by the user-id is really the person sitting at the keyboard.

When asked to create a secret password follow the directions stated in your company's security policy. If there are no specific directions on how to create a secure password, here are some generally accepted guidelines.

A 'good' password for most users is one they can remember, such as the cat's name, or a favorite hobby or sport. These types of passwords are very easy to guess. A good and secure password should be very difficult to guess and therefore may be more difficult to remember. Hackers have special cracker programs that will automatically try every word in the dictionary as well as common names. These programs can break or 'crack' a single dictionary word password in a matter of minutes.

A good secure password follows these guidelines:

- A good password should be 8 or more characters long.
- The password should use a combination of letters, numbers and special characters.
- Do not use actual words in the password. Don't ever use 'password' as a password. .

- Passwords and user-ids are case sensitive, so remember if you used upper or lower case letters.

The concern of most computer users is how will they remember their password. One suggestion is to create a password using numbers and letters that mean something only to you. You might use the first letter of your children's and/or pet's names with the date of some special event and then place a special character, such as % ^ or $, in the middle.

The following three passwords meet the test. They have 8 characters, a mixture of numbers, letter, and special characters but because of the mixture of upper and lower case they are considered totally different passwords by the computer program. This password could have been created as follows: 'R' for first letter of the car they own, '3' for number of cats they own, ^ just because, 'B' for baseball, '82' year they bought their house, 'TWP' the children's middle initials.

R3^B82TWP
R3^b82twp
r3^b82TWP

It is also important to keep the password safe. Try to remember the password and NOT write it down. If you must right it down keep it in a very secure place such as a locked drawer. Also, don't put your User-id and password in the same place.

Do NOT save passwords on the hard drive. Windows will ask if you want to save the password to make it easier to log-on next time. Always say NO to this request. This means you will have to put in your password every time you log-on to the system. This will prevent someone from just sitting at your computer, clicking on an icon, and going directly into your programs. If a hacker gets control of the PC they will have access to all your e-mail and databases.

One final word on passwords. Many security organizations recommend that passwords be changed at least every 90 days if not more often. This means that even if a hacker gets a password it will only be good for a short time and then they will have to try to 'crack' it again.

UNDERSTANDING AND MANAGING E-MAIL SECURITY

Computer e-mail is the most used service on most business networks and home Internet accounts. E-mail has quickly become an important means of communicating second only to the telephone. Like the telephone, criminals and hackers have found ways to use e-mail for illegal purposes.

E-mail is now the number one method of transmitting viruses. According to ICSA Labs Computer Virus Prevalence Survey 2000, in 1999 and early 2000, 87% of all viruses were transmitted via e-mail. By comparison in 1996 only 9% of the viruses reported were transmitted via e-mail and 64% of the viruses were transmitted by infected diskettes. In the year 2000 only a scant 6% of the viruses were transmitted by diskette.

Defending the e-mail system is the responsibility of both the e-mail administrators and the e-mail user. What are the treats from e-mail? What can the average user can do to help defend against attack? The threats from e-mail that users need to be concerned with can be broken down into the following groups.

Virus attacks – Viruses are small pieces of computer programming code that are written by unscrupulous computer programmers called hackers. Viruses do two things. First thing a virus is programmed to do is duplicate itself and spread from computer to computer. This happens either when computer users exchange diskettes, by e-mail, from a web-site or via an operating system. As mentioned above E-mail is currently the number one way that viruses spread.

Second, when the virus program actually runs (executes), the program does whatever the programmer programmed it to do. This can be anything from an annoying message on the screen, to destroying all the information on a computer hard drive.

Spamming – This is the Internet's version of junk mail. Spam is a nickname derived from the meat product of the same name. It refers to the practice of flooding e-mail in-boxes with the same message perhaps hundreds of times. This is not only annoying but it can overload the network and mail server. When servers overload they slow down or stop completely. This denies users access to the network and/or e-mail, this is called a denial of service attack.

Another form of Spam is the old fashion chain letter that asks you to pass it on to others in your e-mail list. Never pass on a chain letter. It may have a virus attached but in any case they clog up the network connections and slow down response times.

Scams and cons - These are e-mails that are asking for information to use for illegal purposes. The e-mail may be asking for credit card information, passwords, or other personal information. Often these e-mails have false 'From:' addresses to make it look like a legitimate request. Never answer an e-mail asking for passwords or credit card information. No legitimate business will ever ask you for your account password. You should only give out your credit card information on a secure web site that can be trusted.

WHAT THE USER CAN DO TO DEFEND AGAINST E-MAIL ATTACKS

All e-mail must come from some computer or e-mail server somewhere. This means there is an 'e-mail geek' more politely called the Mail Administrator or Postmaster somewhere. In a large business this will be an employee or contractor paid by the company. If you are using an Internet service provider (ISP) such as AOL or MSN then there is an e-mail Administrator who is responsible for protecting and delivering your e-mail.

Your first defense against malicious e-mail is to find out who the technicians are who are responsible for managing the e-mail and keeping it secure. These Administrator(s) have probably installed software and possibly hardware to help prevent viruses and attacks. You should contact

the e-mail Administrator and find out what measures he/she is taking to protect your e-mail.

It is important to understand the e-mail user is the primary defense against e-mail attacks. The network e-mail defenses can scan e-mail for some malicious code but must let most e-mail through or risk blocking legitimate and important business e-mail.

The rest of this section gives you specific advice on what can be done to help protect your computer and information.

REVIEWING THE INBOX

The first line of defense is the listing of incoming messages that is presented when you first open the e-mail. When the inbox listing appears DO NOT start opening e-mail immediately. First study the information presented in the listing of e-mails in the inbox. Usually the following pieces of information are available:

From – The person who MAY have sent the message
To – This should be your name or e-mail
Subject – A brief description of what the message is about.
Date received – The date that the e-mail service provider received the message
Time received – The time of day the message was received

Using these pieces of information it is time to become a detective. Look for things that don't seem right or make sense. Here are some questions to ask yourself while looking over the Inbox.

Are there several e-mails with the same subject line possibly from different people?

Discussion: This could be Spam.

Suggestion: Notify the e-mail System Administrator. Follow the company's security policy. Do not delete all the e-mail, save one for the security folks they may want to see a copy and use it to help find the origin of the e-mail. You may want to contact law enforcement if a lot of e-mail is received.

Do you know the person who is listed on the From: line?

Discussion: The e-mail could have come from the person listed on the "From:" line OR it could have come from some one using that person's e-mail address. Using someone else's e-mail name and address is called 'spoofing'.

Suggestion: Even if you do recognize the person's name, do not open the e-mail yet. Check the Subject, date and time lines before opening.

Does the Subject of the e-mail make sense when related to the sender?

Discussion: Does the subject fit with what you would expect this person to send? An e-mail from the boss with a subject: 'I love you' would probably be very suspicious.

Suggestion: If you are suspicious do NOT open the e-mail. Contact the sender via phone or a separate e-mail and ask if they really sent this e-mail. If they didn't send it then delete the e-mail unopened.

Does the Sender, Subject, Date, and Time make sense when considered together?

Discussion: If you know the sender and some of his/her habits, check the date and time. Does it make sense to receive an e-mail from your mother at 2:00 AM or from the Boss over a weekend?

Suggestion: If you are suspicious, do NOT open the e-mail. Again contact the sender via phone or a separate e-mail and ask if they really sent this e-mail. Delete the e-mail unopened if there is suspicion.

Does the subject sound very generic or demand to be opened?

Discussion: E-mails with subjects like. "This is perfect for you" or "Open this for a great opportunity" or "Open immediately" may be a harmless form letter or hacker e-mail containing malicious code.

Suggestion: Compare the subject with the sender and see if it makes sense. Your friends and business associates may use lines like this but be suspicious.

Was this e-mail forwarded? Note: This information may be listed on the first line of the actual message.

Discussion: E-mail that is forwarded and has a strange subject or more importantly an attachment. This email may have actually come from the person you know BUT that person may not know what they are forwarding.

Suggestion: If you are suspicious do NOT open the e-mail. Contact the sender via phone or a separate e-mail and ask if they really sent this e-mail. The solution may be to delete the e-mail unopened.

OPENING AN E-MAIL

A typical e-mail is made up of three main sections. The header information described above, the actual text message or body, and optional attachments. Below are some things to check in the body of the e-mail, attachments with be covered in a later section.

Does the message ask for personal information? Is this an Internet scam?

Discussion: Before you open attachments or click on internet links, read the e-mail carefully. If the e-mail is asking you to do something out of the ordinary or give personal information be cautious. E-mails should never ask for your passwords or for credit card information. On July 8, 2001, The Allentown Morning Call, among other papers, reported that America On Line (AOL) customers received one of five bogus e-mails asking for passwords, credit cards, social security numbers, mothers maiden name, birthdays and everything else needed to assume a person's Internet identity. This e-mail LOOKED like it came from an AOL Administrator but of course it did not. It cost innocent users lots of money and time to straighten out the credit card mess.

Suggestion: Do NOT answer this type of e-mail! Do not send personal information by return e-mail. Report this type of e-mail to your Internet Service Provider and local law enforcement. Also, contact the Federal Trade Commission or the Fraud Internet Complaint Center, as listed in the References and Resources section. Also call the company or agency whose e-mail address is listed on the From: line and let them know of the problem.

Does the e-mail ask you to do something that seems out of the ordinary?

Discussion: Does the e-mail promise money or investment opportunity? For example: if the e-mail asks you to call an unknown phone number for a special message or to click on a special web site be cautious. There is a report of a scam in which people are asked to call a number to a normal looking area code that turns out to be in the Bahamas. The number works like a 900 number and charges your phones number hundreds even thousands of dollars for the call. Since it is outside the United States it is hard to prosecute the individuals responsible.

Suggestion: Delete this kind of email unless it is something you specifically requested. Don't call any phone numbers unless you check the area code or are familiar with the person or company asking you to call.

Are there any 'scripts' imbedded in the e-mail?

Discussion: Over the years, simple text e-mail messages have gotten more and more intricate and sophisticated. E-mails come with pictures, graphics, sound, and moving images. The moving images in web sites and e-mails use programming code called 'scripts'. Script code can be fun but they can also be used by hackers to run unwanted computer code. A hacker can use the script to unleash a virus or gain access to your passwords.

Microsoft's Outlook e-mail package is particularly susceptible to these scripts automatically running. This is because Outlook is set to automatically run scripts using a Windows service called Windows Scripting Host (WSH). This service is tuned ON when Windows is installed.

Suggestion: In order to prevent scripts from running automatically turn off the Visual

Basic Script (VBS) and Java Script features. You may need some help from the IT shop or a techie friend on this one. Here is how to keep these scripts from running automatically in Windows:

In order to turn off Windows Scripting Host (WSH) do the following:
- Click on 'Control Panel'
- Click on 'Add/Remove Programs'
- Click on the 'Windows Setup' tab at the top of the screen
- Click on 'Accessories'
- Scroll down to the bottom of the list
- Click OFF the service called 'Windows Scripting Host'
- Close the window by clicking on 'OK'

Are there any embedded URL links in the e-mail?

Discussion: Check to see if there are any Internet links in the e-mail. You need to decide if you trust the web link and if it is something you are really interested in checking out. Clicking on an unknown web link can expose your web browser to maliciously coded programming scripts.

Suggestion: If you are not interested just ignore the link. To open a link in your e-mail first copy the link, then open the web browse and past it directly into the URL line. This process uses the web browser only and does not pass information through the mail server. In addition the link will probably work better. Also it is a good idea to turn off scripts in the web browser, this is briefly discussed in a later section.

ATTACHMENTS

Attachments to e-mails are one of the greatest threats when it comes to spreading viruses. E-mail has become the favorite method for exchanging files. These files can contain everything from pictures of the grand kids to a copy of the national budget. It is important understand how to handle attachments.

The basic rule with all attachments is to either delete them without opening the file or save the file to your hard drive before opening. After saving the file to the hard drive be sure to run the virus scan program.. This will give your virus program a chance to scan the file for malicious virus code and warn you if there is a problem. Here are some questions to help evaluate attachments

Do you really want or need to view the attachment?

Discussion: Most people get so much e-mail they can't really read it all, particularly all the attachments. After reading the cover e-mail, decide if you really need or want to view the attachment.

Suggestion: Delete the e-mail and attachments if it is something you don't really want to

view, especially if it is a an executable program with a .com .exe or .vbs file extension

How to save the attachments you want to view

Discussion: Each e-mail package is a little different but generally when you 'click' on the attachment, you are asked to choose either to "Open it" or "Save it to disk". Always choose "Save it to Disk". In Lotus Notes mail the option to save a file is called "Detach". The next choice is where to save the file. Save the files in a special directory on the C: drive so they are isolated from other files and easier to locate.

Suggestion: Create a directory on the hard drive to use only for saving and virus checking e-mail attachments. Save all e-mail attachments to this directory before actually opening them. Start your virus program and scan the saved files. This may happen automatically depending on how the virus program is set-up.

THE NEED FOR DESKTOP VIRUS PROTECTION

Virus protection is the third area of security that the average user has in his/her control. The user has a tool called a Virus Checker or Scanner to look through files for malicious code. Virus protection is a two-pronged defense. The System Administrators will take care of virus protection on servers and network devises but every desktop computer needs the protection of a virus program. The home computer is even more vulnerable to viruses than the office computer. The home computer is often used by many family members and is usually not protected by a firewall.

Do you have a virus protection package installed on your PC?

Discussion: There are several very good virus protection packages available. The two most popular are McAfee VirusScan and Norton AntiVirus. Both received high rating from reviewers such as PC Magazine. In the June 26, 2001 issue of PC Magazine the reviewers rated Norton Antivirus 2001 slightly higher than McAfee based on ease of use, automatic update of signature files and the small drain it puts on system resources.

Suggestion: The action here is to be sure a virus-scanning program is installed on each desktop. In most companies a virus program is installed on each desktop by the IT staff. At home a virus program will need to be purchased and installed.

Is the virus scan program active at all times?

Discussion: Virus programs have several options on when to do the virus scan. They can be run only when you choose to run them or they can be set to watch the computer system all the time. It is best to have the virus program active at all times unless this causes a problem with another program.

Suggestion: Check to see if the icon for your virus program is at the bottom right corner

of the Windows screen. If the automatic scan is not turned on then open the virus program and turn on the automatic scanning option. Exactly how turn on the automatic scan option depends on the virus program. Check the program documentation, help screens, and the software developers web site.

Do the virus signature files get updated regularly?

Discussion: Virus protection software works by scanning the lines of code in each file and comparing them to the code from known viruses. This specific virus code is called the virus's 'signature'. There are thousands of identified viruses with more coming on the scene every day. In order to keep up with all the new virus codes being created, the virus protection software companies must constantly add new 'signatures' to the virus scanning database. It is essential that the 'virus signature' database on the desktop be kept up to date. Suggestion: In order to update the signature file, access the software developers web site and request a download. The new Norton Antivirus updates automatically every time the computer logs on to the Internet. Some software vendors give a warning that the signature file is out dated and needs to be updated. Signature file update should be done at least once per month but it is better to update more often.

Is the anti-virus software on the computer setup for the best protection?

Discussion: Anti–virus software has several different set-up or configuration options for different levels of virus protection. Virus software use computer resources, as do all software packages. You must strike a balance between configuring your software for maximum protection and how this effects the performance of your system. The best configuration for your desktop will depend on factors like, how much memory the computer has, how many programs you open at one time, and how many resources the virus program requires.

Suggestion: Virus protection software allows you to pick which type of files are to be checked and when these files should be scanned. A minimum configuration would be scan all new files that are opened by a program, created by a program or downloaded from the internet. In addition it is a very good idea to have the software scan all files on the hard drive when the computer is first started.

ADDITIONAL SECURITY CONSIDERATIONS

The primary focus of this paper has been on the security of passwords, e-mail and viruses. There are two other Security considerations of which the average computer user should be aware. They are web browser scripts and personal firewalls.

Web Browser scripts

As was mentioned earlier, scripting languages provide flash and interest to e-mails and web sites but they are dangerous from a security perspective. The primary scripting languages are Visual Basic Script, Java Script and Active X components. All of these scripts can be turned off in your

web browser. This will help protect the computer from malicious code coming from web sites. Turning these scripts off will also limit some of the interactions with web sites. At this time web delivered malicious code is not as big a problem as e-mail delivered viruses but who knows what hackers will do in the future.

If you are interested in how to turn off these scripts in your web browser one place to look for help is at the CERT web site:

www.cert.org/tech_tips/malicious_code_FAQ.htm

Personal Firewalls

A firewall is a piece of hardware and/or software that monitors any attempts by an outsider to enter the computer or computer network. The firewall looks at each request for access and based on a pre-defined set of access rules decides whether or not to let the request enter the system. The access rules are set by the Firewall Administrator or, in the case of a personal firewall, by the user.

All firewalls come with set of default rules that can be changed as conditions change. The home user may find the default rules are enough protection. The home user should strongly consider setting up a personal firewall particularly if using an always-on (persistent) connection such as a cable modem or a DSL line. Even a dial-up modem can be hacked so a firewall is a good idea.

There are several personnel firewalls on the market and there is even a free firewall from Zone Alarm, which available at the following URL:

http://www.zonelabs.com/

Additional information on personal firewalls may be found at the following site:

www.faqs.org/faqs/firewalls-faq/

CONCLUSION

Good computer and information security requires the involvement of many people including, network and system administrators, e-mail administrators, law enforcement, and especially the computer user. The computer user is the reason computers exist and is also a major player in defending against hacker attacks.

There are security tools and resources available to the user including virus protection programs, firewall software, computer professionals and the most important resource, knowledge. The computer user should make it a point to keep up with news on computer security issues by following news reports and checking web sites of computer security agencies such as CERT, SANS and ICSA to mention a few.

REFERENCES:

ICSA Labs Computer Virus Prevalence Survey 2000, by Lawrence M. Bridwell and Petter Tippett, copyright 2000, by ICSA.net, Reston, VA
www.icsa.net

"Antivirus" Utilities report, PC Magazine, June 26, 2001
www.pcmag.com

"No More Letter Bombs" by Les Feed, PC Magazine, June 12, 2001
www.pcmag.com

"FAQ: Prepare Now for the Next E-mail Virus" by Maurene Grey, June 22, 2000. Gartner Tutorial, Note Number: QA-11-2415
www.gartner.com

"Sophisticated new viruses strike through use of e-mail or networks" by Heather Newman, Knight Ridder Newspapers as reported in The Virginian Pilot, July, 16, 2001.

"Home Network Security", June 26, 2001 revision CERT Coordination Center, copyright Carnegie Mellon University, 2001

"Frequently Asked Questions About Malicious Web Scripts Redirected by Web Sites" February 2, 2000, release CERT Coordination Center, Copyright 2000 Carnegie Mellon University.
www.cert.org/tech_tips/malicious_code_FAQ.html

"Computer Virus FAQ for New Users" July 18, 1999 at www.faq.org

"AOL users victim of identity theft" by Tony Bridges of the Tallahassee Democrat as report in the Allentown PA. Morning Call, July 8, 2001

Resources for further research:

SANS (System Administration, Networking, and Security) Institute – a Cooperative Education and Research Organization
www.sans.org

CERT Coordination Center, Carnegie Mellon University
www.cert.org

ICSA Labs – A Division of True Secure Incorporated
www.icsalabs.com

Federal Trade Commission

www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Fraud Internet Complaint Center
www.ifccfbi.gov

Julia Scheeres, "Wait! Don't Forward That E-mail",
www.wired.com/news/technology 2/5/2001

Julia Scheeres, "Friends Don't E-mail Friends HTML",
www.wired.com/news/technology 2/6/2001

Cert Coordination Center, "Cert Advisory CA-2000-02 malicious HTML Tags Embedded in Client Web Requests"
http://www.cert.org/ Feb 3, 2000

Jim Wolf, "Number One Snoop",
http://www.abcnews.go.com/ , 9/22/2000

Cert Coordination Center, "Spoofed/Forged E-mail"
http://www.cert.org/ , 3/20/2000