The End Users Security Primer

January 1, 2002

Russell J. Poole III

The End Users Security Primer

Abstract

Security professionals pay a great deal of attention to hackers, their methods, the exploits and techniques they use, as well as the best ways to defend against them. Network and system administrators spend a great deal of time working to secure their network. However, there is very little attention focused on educating the *END USER* on how they can assist the network and systems administrators in making sure their network is secure. As security professionals, we know that our network and systems are most vulnerable to internal security threats. The wiley hacker knows this as well and will very often attack the weakest link. This weakest link, very often, is an un-informed end user.

This document has been created for the *END USER* – the individual that can either make or break a security plan. The end user must be informed, and continually informed, about the threats that face the network. This document makes a first attempt to do this. Included are 10 areas where the end user can make an impact on the security of the network and their systems. Every organization should have an *End User Security Primer* that is distributed to current and new users. Further, it should be continually updated so that end users are current on the best practices on how they can assist the network and system administrators in the battle against the wiley hacker.

The End Users Security Primer

This document has been created for you, the end user, as a "how to" manual on keeping your computer systems secure. You can assist your network and system administrator in keeping your and your co-workers' data secure by following the best practices mentioned in this document. This document is a security primer designed to help you assist in the fight against the wiley hacker.

Background:

For you, the end user, a computer is a tool. Every morning you sit down at the computer, create documents, check email, surf the web, create spreadsheets, and perform many other useful tasks that need to be carried out in the day-to-day business of your organization. To the wiley hacker, however, your computer is a treasure trove of information and access.

The hacker lives to learn. That is his motto. He wants to learn as much as he can about you, your habits, your computer, the information on your computer, and the access your computer has to sensitive information. Giving up one piece of information, by itself, may not be a significant threat, but many pieces of information can. By collecting lots of small pieces of information, the hacker can begin to devise a scheme to gain access to you and your organization's computers and data.

For example, if a burglar determines that you live in a brick house, this does not help him find your home. If he learns that you live in a red brick house, he begins to form a picture of the type of home you live in. If he then finds out that you live on Elm Street, although he does not have your address, he can narrow down your home to the red-brick homes on Elm. Then, if he learns that you drive a blue Mercedes, chances are, he will be able to zero in on which home is yours. It is simply the red-brick home on Elm Street that has a blue Mercedes parked outside.

This is exactly what the wiley hacker does with regard to your network and computer system. He patiently collects information that, when pieced together, gives him a complete picture of your network and computer system. This gives him a huge advantage in gaining access to your system and data.

Your effort, then, should be to make this information-gathering as difficult as possible. You should work with your network and systems administrator to ensure that the wiley hacker is not successful in gaining information about your system, or worse, gaining *access* to your system.

The following are ten areas of concern that you as an end user can address to help ensure that your computer is secure. Performing the suggested actions will not guarantee that your system is one hundred percent secure, but it will make it much more difficult for the hacker to gain access.

1. Social Engineering

In beginning to address the issue of network and system security, you need a keen understanding of the social threat that faces your organization.

Social Engineering is defined in this context as a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. Some have defined Social Engineering as an attempt to make people give up their passwords or even phone scams that pit your knowledge against the wits of another humans. Social Engineering is this and much more. (Searchsecurity.com)

Social Engineers use people's kind and trusting nature in an attempt to gain access to, or information about, a user's system. An example of this would be a wiley hacker making an attempt to gain physical access to your building by asking you to "hold the door" while he carries in a heavy object. Another may be as simple as following you into the office without letting the door close behind you. These are examples of Social Engineering where the good nature of an individual is used against them in gaining access.

Other attempts may be much more subtle. Sitting around a party chatting about your company's network and computer security measures is a great place for the wiley hacker to learn about your network. Simply letting out small pieces of information about the computers in your work environment gives the hacker those little nuggets of knowledge he needs to construct the big picture, which aids in the hacking of your system.

Another classic example is the direct attempt to learn an end user's password. This can be as subtle as looking around your desk for a password that has been written down because you did not want to forget it, or as direct as a phone call in which the hacker poses as a systems administrator and asks you for your password for some systems re-build or reset.

Social Engineers will go as far as searching dumpsters, memorizing passwords and access codes by looking over someone's shoulder (shoulder surfing), and taking advantage of people's natural inclination to choose passwords that are meaningful to them.

"HOW TO" deter the threat of social engineering:

- Never assume that someone you don't know has authorization to access secure areas. If they do, they should have proper identification as well as their OWN pass cards or keys to gain entry. Insist they use their own credentials.
- Protect passwords. Don't EVER, under ANY circumstances, give any computer password to ANYONE. There is NEVER a reason that you, or any end user, should give out passwords.
- If an administrator needs to work on your account, they should have access as administrators. If they do not have access, then they are NOT authorized.
- Be aware of shoulder surfing. Don't allow someone to sit over your shoulder and view confidential information, especially access codes and passwords.

- Don't give out information about your organization's network and computers; even at casual non-business events.
- Don't throw away anything sensitive. Shred it.
- Trust no one when it comes to the security of your data. Do what YOU can to make sure it is secure.

2. Physical Connection

If your computer is not part of a network, then the security threat to your computer is greatly diminished. With a stand-alone computer, the primary security threat comes from someone physically gaining access to your computer and attempting to gain access from your office. Once a computer is connected to a network, however, the security threat grows much greater.

Each computer that is connected to a network must have a physical connection to that network. The physical connection can be in the form of a wired connection in which the computer is plugged into a wall plate or it can be in the form of wireless connectivity in which the connection is made via wireless signal.

Any person that can gain access to the local area network (LAN) stands a much-improved chance of performing surveillance on the network and can gain those nuggets of knowledge needed to break into your systems. If you let another connect to the network using a connection available in your office, you give that person access to the LAN. From this connection, the person can perform surveillance, launch an attack against the network, or release viruses across the network.

Many networks have security measures in place that prevent access to the physical network unless some proof of identification is performed. However, these efforts are not full-proof, so as the end-user you need to help ensure the physical connections in your office are used by only those authorized.

How to ensure someone does not gain an unauthorized physical connection:

- Ensure that those who use your wall plates are authorized. You know your organization and should know who is allowed to access the network.
- Keep your office locked when gone.
- Don't leave unauthorized people in your office.
- If you have a network or system administrator, check with them if you are uncertain about letting someone have access to the physical connection.

3. Operating System

In today's organizations, most companies have standardized the end-users' desktop on Microsoft's operating systems. The flavors of Microsoft operating systems include Windows-95, Windows-98, Windows Millennium, Windows –NT, Windows-2000, Windows-XP, and the latest, Windows Vista. Other operating systems such as Linux and Macintosh OS X are

beginning to make in-roads onto the technical employees' desktop, but Microsoft still commands the market in this regard.

You, as an end user, need to ensure that certain issues are addressed with relation to your operating system to ensure that your data is secure.

Windows-95, Windows-98, Millennium, NT and 2000 are no longer supported by Microsoft and do not offer adequate local workstation security. What this means is that a computer running one of these operating systems is quite vulnerable to someone just sitting down at your machine, and immediately having access to the local workstation or easily gaining access over the network. It is recommended that you use Windows XP Pro, or Vista.

To lock these systems, all you have to do is press and hold down the "CONTROL" key, then press and hold the "ALT" key, and finally press the "DELETE" key. The task list appears and you have the option to lock your workstation. Only you or an administrator can unlock the workstation. (As you may already know, this key sequence in older versions of Microsoft's operating systems was the "three finger salute" or the key string that rebooted the machine. Not so in the newer operating systems.) You can also invoke a native Windows screen-saver with a password protect option that will automatically lock your machine for you after a specified period of time. This is useful as an added backup to ensure your machine is secure when not present. The screen saver is enabled by right clicking on the desktop and selecting "Properties". Under the properties window, choose the "Screen Saver" tab.

Windows XP Pro, and Vista allow for "file level security". This means that you can restrict access to individual files based on the username. To do this, you must have NTFS, Microsoft's secure file system, configured on your machine. If you have sensitive data on your local machine, it is important that you have NTFS security so that you can secure your data properly. Ask your system administrator if you are uncertain about the need for NTFS and how to secure your system at the file level.

All of Microsoft's operating systems generally need patches applied as they become available. Patches are fixes to the operating systems and other applications. These patches may address security issues as well as operational matters. You should consult your systems administrator before you apply any patch to any operating system or application as the patch itself can create security risks. If you do not have a network or system administrator, verify through research the integrity of the patches applied.

How to make sure you are properly secured in relation to your operating system:

- In secure environments in which Microsoft operating systems are used, ask for Windows XP Pro, or Vista.
- Use the workstation locking ability of your operating system when not present at your machine to ensure no unauthorized access occurs.
- Uses a native Windows screen-saver with the password protect option enabled.

- For secure environments in which a network or system administrator makes the decisions concerning your operating system, ask for a secure file system, especially if you have sensitive information on your local machine.
- Ask your system administrators to verify that all security patches have been properly applied. If you do not have a network or system administrator, verify through research the integrity and need of the patches before you apply them.

4. User Accounts and Passwords

In most organizations, users are assigned user accounts and passwords. This user account and password is what grants you access to the appropriate resources throughout the network. You are responsible for your account and the activities that occur from this account. For this reason, it is important that no one else have access to your account.

In an ideal world, no one would know the name of your user account or your password. If a wiley hacker knows your user account, he is half way into your system and needs only the password to gain access. So it is generally a good idea to keep your user account secret. Your password is the second part of the authentication process. Give up the password and you give up your account as well as any data the hacker wishes to take or destroy.

Passwords can be stolen through the afore-mentioned social engineering, from brute force programs that use dictionaries to guess combinations of words, from smart hackers who guess weak passwords, from trashcans where users have thrown away small pieces of paper upon which the password was written, and from users who freely give it away. The password is a hacker's gold mine. With it, he can gain the same access that the user has.

Although account names are often assigned, passwords are not. So the more difficult the password is to guess, the harder for the hacker to gain access. Never make your password too short. The preferred length of the password is at least six characters. Don't choose passwords like your spouses name, your birthday, your kids' names, or anything that's easy for the hacker to guess. Remember, the hacker has been gaining information about your system as well as *you*, so don't be surprised if the hacker guesses that your password is "sugar", the name of your cat.

Often, system administrators require users to change passwords on a regular basis. This can occur every month in very high-secure areas to every six months in less-secure areas. The reason for this is to minimize the damage that can occur from a stolen password. If a hacker guesses a password, but all the passwords are changed every month, the hacker has only a maximum time of one month to use the system. Granted, this is too much time, but it is an added security measure that some administrators will take.

How to ensure the security of your accounts and passwords

- Passwords should be at LEAST 8 characters long
- A good password is difficult to guess. It will contain alpha, numeric and shift characters, not be found in the dictionary, and not be any part or any form of a word that is easily

identified with you including your name, user id, birthday, address, phone number, social security number, etc.
- Do not write passwords down or store them online
- NEVER share passwords with anyone
- Change passwords often, at least every 3 months

5. Application Installation

As an end user, you may find it necessary to install an application. After all, applications are what make a computer useful. Without them, a computer would not provide much value. Hackers know this as well, and have been known to imbed "trojans", or hidden programs, in installation routines. You may think you are getting a new exciting screen saver when in fact you are getting a screen saver as well as a hidden program that sends information about your web surfing activities to a hacker who then sells that information to a marketing firm. Worse, you may get viruses or other programs that destroy data.

A popular hacker program that installs behind the scenes, a true trojan, is one that gives complete access to your computer from a remote machine. The software allows a hacker to do things to your computer as if he was sitting at the console. He could move your mouse, record your keystrokes, steal bank account records, and learn your credit card numbers, all because you installed a simple application that you believed to be harmless.

Free applications are plentiful off of the Internet. You can browse to one of thousands of sites that offer programs that range from simple screen-savers and calculator programs to full-blown imaging programs. To successfully install these applications without the risk of viruses or trojans, you need to verify the vendor and ensure that no viruses are in the installation routine.

For this reason, it is imperative that you check with your network or system administrator before you install any applications. What you believe may be a harmless program may in fact be the next virus that brings your corporate network to its knees.

How to make sure you don't install viruses, trojans, or other hacker programs from other applications.

- NEVER install an application from a non-reputable vendor.
- If attached to a network, always check with your network or system administrator before installing any applications.

6. E-mail and Viruses

E-mail is today's preferred medium for quick and easy communication. It is also a very easy way for users to transfer files. Hackers know this and use e-mail as a tool to eavesdrop, send Trojans throughout the Internet, or simply deliver a machine-killing payload. As an end user, you can help to deter the hacker's master plan.

Eavesdropping: Efficient hackers can "sniff" the traffic moving across the Internet and intercept e-mail messages. Since most e-mail is sent across the Internet in un-encoded text, a hacker could intercept and read your e-mail fairly easily. For this reason, you should never send any sensitive information via e-mail. Corporate documents and confidential data should never be sent over e-mail unless it is encrypted.

Sending Payload: Payload is used here as a term for an attached file containing a Trojan or a virus. E-mails can be sent with an attachment that carries with it an imbedded program or virus. When the e-mail finds its destination, the Trojan and/or virus can be released upon opening.

In the past, as long as you did not open e-mail attachments, the receiving computer would not be hurt. But now, with the advent of the "bubble-boy" virus, that is no longer the case. This ushers in the next evolution in viruses. It breaks one of the long-standing rules that you have to open an e-mail attachment to become infected.

You should never open an attachment unless you can successfully answer the following questions:

1. Who sent the e-mail?
2. What attachments are they sending?
3. Am I expecting this e-mail?

If you can satisfactorily answer these three questions, then opening the e-mail may pose *LESS* of a threat. However, that does NOT mean there is no threat.

As with any application, e-mail applications need to be updated over time for fixes and updates. You need to make sure that your e-mail program is up to date or that your system administrator has your e-mail patches up to date.

Another security concern relative to e-mail is sending out documents and files in their original format. For example, whenever you create, open, or save a document in Microsoft Word, the document may contain content that you may not want to share with others when you distribute the document electronically. This information is known as "metadata". Metadata is used for a variety of purposes to enhance the editing, viewing, filing, and retrieval of MS Office documents.

Some metadata is easily accessible using Word, but other metadata is only accessible using special tools. Examples of metadata that can accompany the files you send out in Word or Excel format include your name and initials, your company or organization name, name of your computer, name of the network server or hard disk where you saved the document, document revisions and versions, template information, hidden text, deleted text, and comments.

Because of this additional information that is contained in the Word document, it is recommended that you send documents out in a format that does not contain the hidden information. A popular way to send out data is in Portable Document Format (PDF). Sending documents in PDF will reduce the possibility of sensitive data being sent out inadvertently.

Another critical application that *must* be on every machine is virus-scanning software. This software should be running at all times and should be updated continuously or at a minimum of once a day. Configuring anti-virus software to update the definition files automatically via the Internet is the preferred method. Antivirus software can aid in the identification of bad e-mail attachments, so it is very important that it be up to date.

Often, users are not sure if they have been infected with a virus and wait before notifying the network or system administrator of the issue. It is imperative that at the first sign of a virus, you notify the network or system administrator immediately. Depending on the nature of the virus or the attack, the sooner the notification, the less the damage.

How to protect your computer from E-mail eavesdropping, viruses, and Trojans sent via e-mail:

- Never send any sensitive information via e-mail unless it is encrypted.
- Never open an attachment unless you can satisfactorily answer the following three questions:
    1. Who sent the e-mail?
    2. What attachments are they sending?
    3. Am I expecting this e-mail?
- If possible, do not e-mail sensitive documents in a format that includes metadata or other imbedded information. Send the document in a format that reduces this potential, such as PDF format.
- Ensure that you have up-to-date anti-virus software on your computer and that it is always running.
- Ensure that all updates and patches are applied to your e-mail and virus scanning software.
- If you are part of a network, check with your system administrator before attempting to install the updates.
- If you are part of a Network, notify the network or system administrator immediately once infected with a virus. If you are in doubt, notify them.

7. Web Browsing

The Internet is rich in content. The amount of useful information is boundless. Through the World Wide Web we can all find information at the click of a mouse that would have taken months to compile just a few short years ago. Furthermore, the web is getting easier to use. Content-rich sites are making it easier to navigate, e-commerce is making shopping easier, and paying our bills online is becoming as normal as waking up to fresh brewed coffee from an automated coffee maker. As usual, though, there is a downside. Just as there are inherent dangers with every new highway built, there are some inherent dangers on the information superhighway as well.

To browse the Web, we use a web browser. Internet Explorer and Firefox are the two most popular browsers in use today. Web browsers can be security and privacy risks for your home

and office. The primary risks are with things called cookies, Java, Java applets, and Active X controls.

A cookie is a small text file that contains information about you and your computer. Often, these cookies are generated by web sites and stored on YOUR computer. The next time you return to the web site, that information is retrievable by the web server and the web site "remembers" who you and your machine are by reading the cookie file.

Cookies are generally harmless and can add functionality to a web site. But some web sites or trojans can take advantage of your cookie file and capture it, allowing access to the history of the locations that you have visited. This is an issue of privacy and concerns many users. Java and Active X controls are executable codes that run on your local machine and Java applets are scripts that are downloaded with a web site. Executable code such as Java and Active X can make system calls that can affect the operation of your computer and Java applets can assist hackers in making your computer assist in attacks on other computers. In short, there are some security concerns in using a browser on the World Wide Web.

According to Pamela Jerskey of Boston College, more and more web sites now use executable programs and other forms of plug-ins. These executable programs and plug-ins are allowed to operate through your web browser based on the browser settings that you configure. When a user allows an executable program to run, adverse applications can cause damage resulting in

- System crashes from faulty applets that may result in a loss of work in process.
- Theft of personal data from applets browsing the user's hard drive and transmitting information from it.
- Forged e-mail from applets sent to other recipients conveying messages that the user may not want.

As an end user, you may want to adjust the settings of your web browser to be more secure. At a minimum you should configure the browser to use cookies only if they are stored on the remote web server. You should also check with your network or systems administrator for policies regarding these settings.

Users should be aware that some web sites exist for the sole purpose of collecting information and launching attacks against your computers. Configuring your browsers properly can help minimize the affects that these sites can have on your system.

How to configure your Web Browser against unwanted snooping and rogue code:

- For systems that are connected to networks, check with network or systems administrator for policies that may be in place for your network.
- Adjust the cookie control in your browser to reflect how you wish your browsing history to be handled. It is preferred that you configure your browser to only accept cookies if they are sent back to the originating server.
- Adjust your web browser to allow or disallow Active X, Java, and Java as appropriate. It is recommended that you configure your browser so that Active X controls are disabled

and Java and Java Applets are disabled. Disabling these controls will hamper the operation of some web sites on your browser.
- Adjust web browser for highest security settings possible.

8. Power Protection

There are two unfortunate realities of the electronics age: the power utility simply cannot provide the clean, consistent power demanded by sensitive electronics, and the customer is ultimately responsible for the health and safe operation of his or her equipment.

A study by IBM has shown that a typical computer is subject to 120 power problems per month. The effects of power problems range from the subtle – keyboard lockups, hardware degradation – to the dramatic – complete data loss or burnt motherboards. According to a survey by the Yankee Group, almost half of the corporations researched put their downtime costs at upwards of $1,000.00 per hour with nine percent estimating costs up to or more than $50,000.00 per hour.

It has been said that there are two types of computer users: Those who have already experienced data loss due to power problems and those who are going to. Power problems are the single largest cause of data loss and can be prevented through the use of an Uninterruptible Power Supply (UPS). A UPS is simply a surge suppressor with a battery attached to it. It protects against the following:

- Sags: Also known as brownouts, sags are short-term decreases in voltage levels. This is the most common power problem, accounting for 87 percent of all power disturbances according to a study by Bell Labs.

- Blackout: Total loss of Utility Power

- Spike: Also referred to as an impulse, a spike is an instantaneous, dramatic increase in voltage. Akin to the force of a tidal wave, a spike can enter electronic equipment through AC, Network, serial or phone lines and damage or completely destroy components.

- Surge: A short-term increase in voltage, typically lasting at least 1/120 of a second.

- Noise: More technically referred to as Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI), electrical noise disrupts the smooth sine wave one expects from utility power.

How to protect yourself against data loss due to power fluctuations.

- On all computers, use an appropriately sized uninterruptible power supply with surge protection.

9. Backups

A security primer would not be complete without addressing the issue of backups. A backup is *the* last defense against malicious attacks against you and your network. If you regularly backup your data to a protected location, if all else fails, you can always revert to your last backup. If that backup was from yesterday, you have only lost one day of work. If that backup was from 5 weeks ago, then have lost 5 weeks of effort.

You can measure the value of your time in your backup. If your time is not worth much and you don't mind regenerating work, then having a backup is probably not going to be a priority. I suspect, however, that your time is worth quite a bit. For that reason, a regular backup scheme is warranted. There are different backup schedules that one can follow, but you should backup your sensitive data on a daily basis.

How to protect your data from the ultimate attack in which your system is completely destroyed:

- Perform regular backups following a regular backup schedule.
- Store the backups in a safe location.
- For extremely important information, store a copy of the backed up data at an offsite location.

Summary

Security is truly becoming an issue that end users have to address in their daily work. Viruses, Trojans, and malicious code can create havoc as well as allow access to sensitive data by individuals who are not authorized. For this reason, users must assist the network and system administrators to verify that proper protocols are followed to ensure the protection of the network and its systems. Without the assistance of a well-educated end user, network and system security will be incomplete.

References:

1. "The Complete Social Engineering FAQ," URL: http://netsecurity.about.com/cs/socialengineering

2. www.searchSecurity.com, URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html

3. "Remote Control Trojan Horse Software," http://www.jmu.edu/computing/info-security/engineering/issues/remote.shtml, December 17, 2001

4. "Sci/Tech E-mail security bubble bursts," URL: http://news.bbc.co.uk/hi/english/sci/tech/newsid_514000/514145.stm, November 15, 1999

5. "Is Internet Browsing Safe." URL: http://www.bc.edu/bc_org/fvp/ia/other/internet.html

6. www.searchsecurity.com, URL: http://searchsolaris.techtarget.com/sDefinition/0,,sid12_gci212415,00.html

7. "How to minimize metadata in Microsoft Word Documents," URL http://support.microsoft.com/default.aspx?scid=kb;EN-US;q223790

8. "Solutions '99," American Power Corporation, January 1999.

9. Cole, Eric. Hackers Beware, Defending Your Network from the Wiley Hacker. New Riders Publishing, 2001

9. "Basic Security Guidelines for Network Administrators, " URL: http://net-services.ufl.edu/~security/

Ten questions relating to the End User Security Primer

1. When is it appropriate to give an administrator your password?
    a. During System Upgrades
    b. Whenever they ask for it
    c. When you are fired
    d. Never

2. Who should be allowed to have physical access to the wall plate in your office?
    a. Electricians
    b. Computer repairman
    c. Only Authorized personnel from your office
    d. Your family

3. Which windows operating system allows true workstation locking and file level security?
    a. Windows XP Pro
    b. Windows Millennium
    c. Windows 98
    d. Windows 95

4. Which of the following is NOT an important characteristic of a password?
    a. It should be a word that is easily identified with you including your name, user id, birthday, address, phone number, social security number, etc
    b. It be at least 8 characters long
    c. It will be difficult to guess.
    d. It will contain alpha, numeric and shift characters, not be found in the dictionary

5. What is a Trojan?
    a. A horse
    b. A secure computer
    c. A Hidden program
    d. A password protector

6. Which of the following is NOT an important question to ask when receiving an attachment via e-mail?
    a. Who sent the e-mail?
    b. What attachments are they sending?
    c. What operating system will this attachment run on?
    d. Am I expecting this e-mail?

7. What is a cookie?
    a. An embedded program
    b. A file containing executable code
    c. A small text file that contains information about you and your computer
    d. A Java Script

8. What is the single largest cause of data loss?
    a. Hackers
    b. Bad backups
    c. Power Problems
    d. Trojans

9. What is your last defense against malicious attacks?
    a. Good Intrusion Detection Software
    b. A good backup
    c. Antivirus software
    d. Operating system patches