





The Cyber-Barbarians at the Gate: Protecting your Computer from Security Threats.

Nerino J. Petro, Jr.
Attorney/CEO
CenCom, A Div. of Centro, Inc.
349 E. Riverside Blvd.
Loves Park, IL 61111
815.636.1001
njpetro@lawofficetech.com

<u>THE EVILS INSIDE:CAN WE STOP SPAM, SPYWARE AND VIRUSES?</u>	1
1. INTRODUCTION:	1
2. THE CYBER- BARBARIANS: OVERVIEW OF SECURITY THREATS:	1
2.1 General Threats - Viruses, Worms and Trojans:	1
2.2 Spyware and Adware:	3
2.3 Social Engineering Attacks, Cracking and Script Kiddies:	3
2.4 Physical threats and catastrophes:	4
2.5 Wireless and Mobile Computing Threats:	4
3. DEFENDING THE GATES: COMMON SENSE STEPS TO DETER AND DEAL WITH SECURITY THREATS	6
3.1 Operating System:	6
3.2 Passwords:	8
3.3 Anti Virus:	9
3.4 Firewalls:	10
3.5 Encryption:	12
3.6 Physical Security:	13
4. DEFENDING THE COLONIES: PRACTICING SAFE WIRELESS COMPUTING:	15
4.1 Dangers in the “Wild”	15
4.2 Practicing Safe Wireless Computing in the Wild:	15
4.3 Protecting the Office:	15
5. CONCLUSION:	17
APPENDIX A	19

ICON TABLE

	Valuable information
	Keyboard/Mouse Actions
TEXT	Key terms

Copyright Notice

All materials contained in this paper are copyrighted 2004 by Nerino J. Petro, Jr. and CenCom, A Div. of Centro, Inc.. All rights reserved worldwide. No part of these materials may be reproduced, transcribed, stored in any retrieval system, or translated into any language by any means without the author's prior written consent.

No claim made to other than original works.

Acknowledgments:

All trademark and service marks are the property of their respective owners and should be treated as such

Microsoft, Windows, Internet Explorer and Outlook Express are registered trademarks of Microsoft Corporation.

Wi-Fi, WEP and WPA are registered trademarks of the WECA and the Wi-Fi Alliance

CERT is a registered trademark of Carnegie Mellon University

Mac and Mac OS X are registered trademarks of Apple Computer, Inc.

ShieldsUP and LeakTest are registered trademarks of Gibson Research Corporation

All references to companies and websites are the trademarks of the respective companies.

CenCom, A Div. of Centro, Inc.

349 E. Riverside Blvd.

Loves Park, IL 61111

TEL 815.636.1001

FAX 815.636.8660

info@lawofficetech.com

www.lawofficetech.com

THE EVILS INSIDE: CAN WE STOP SPAM, SPYWARE AND VIRUSES?

1. Introduction:

There are numerous issues and dangers that threaten the security of your computer, your network and your data. These "evils inside" not only threaten loss of time and damage to your systems, but can also result in loss of irreplaceable data and unauthorized disclosure and/or distribution of confidential and privileged information leading to potential claims against you and your company. These threats are much like the barbarians of old, looking to tear down, loot and pillage. I look at these evils as the Cyber-Barbarians, modern day descendants of those who brought terror to the civilized world.

What follows is an overview: detailing all possible threats and the possible protective steps to counter them is beyond the scope of this paper. Instead, it will focus on threats I believe you are most likely to encounter and common sense steps that you can take to protect yourself and your data from falling victim to current security threats.

Protecting your computer from these threats is truly an instance where you are better to be proactive, to "go on the offensive" to take steps to safeguard your self, your firm and your clients. So man the walls, raise the drawbridge and prepare for battle because the Cyber-Barbarians are at the Gate intent on pillaging what you hold dear!

2. The Cyber- Barbarians: Overview of Security Threats:

Everyday, you and your computer systems face ongoing threats of which you may not even be aware. These threats can take many forms, and be both internal and external in nature. However, before you can take reasonable steps to protect yourself, you need to have some idea of what these threats are.

2.1 General Threats - Viruses, Worms and Trojans:


Some of the most common threats (and also the most prolific that you may face) include virus, worms and Trojan horse programs. These can infect your systems by a) someone installing a program, running a macro command or loading data that they bring into the office or b) from the Internet via email or download.

Depending on the level of security settings in your Internet Web Browser and email programs, being hit by one of these threats may not even require any action on your part other than previewing a message or clicking on an online advertisement.

A virus is a program or a piece of computer code surreptitiously placed and running on your computer without your knowledge or consent. Some viruses are benign and others malicious. However, whether a virus is benign or malicious to me is irrelevant. Even a benign virus can impact your computing performance and operation and a malicious virus will definitely create havoc for you. The key point is that the virus has been emplaced through stealth or deceit onto YOUR system! VIRUSES can infect your computer operating system or its files. They can be embedded in macros in word processing or spreadsheet files. Disk_Killer is an example of a VIRUS that resides on your Hard Drive for 48 hours and then encrypts your entire hard drive making access impossible.

A worm is a virus that can replicate itself in addition to wreaking havoc through its malicious actions. The “Bagle” and “Netsky “ worms are two examples of worms that have infected systems recently and are high on the threat warnings of the major anti virus companies. One of the most recent Bagle variants is WIN32.Bagle.AQ, which can be found in e-mails or in file sharing downloads. WIN.32.Netsky.P propagates in the same way as Bagel. WORMs such as these harvests your email addresses to replicate and send out copies of itself in addition to doing damaging files and causing other problems such as making noises or allowing someone to exploit a security hole gaining access to your data. It also makes numerous copies of itself and places them on your system (making it difficult to find them all and remove them). WIN32.Bagel.AQ opens backdoors into your computer system allowing remote access to the infected computer. Netsky variants will often include information in the body of the e-mail that says +++ *Attachment: No Virus found* +++ *Panda AntiVirus - www.pandasoftware.com* or something similar from another anti virus company. The purpose of this being to get you to think the message is safe and to open its attachment. Based on vulnerabilities in some programs, all it takes is to preview an infected email message to infect your computer.

A Trojan Horse a/k/a Trojan (yes it’s named after THAT Horse) is a malicious program that masquerades as a benign application. A recent example of a Trojan that hit in September 2004 is Win32.Agobot. Computer Associates Virus Information Center details this TROJAN as “...an IRC controlled backdoor that can be used to gain unauthorized access to a victim's machine. It can also exhibit worm-like functionality by exploiting weak passwords on administrative shares and by exploiting many different software vulnerabilities, as well as backdoors created by other malware.” Another example is VBS.Bootconf.B: like many other such programs, this one changes Internet Explorer settings to redirect searches from legitimate search sites that you use to another site with advertising or to a pornographic website.


 ► The following websites are just a few of the many where you can obtain additional information on Viruses, WORMS and TROJANS.

Symantec Corporation: <http://securityresponse.symantec.com/>

Computer Associates International, Inc. <http://www3.ca.com/virusinfo/>

2.2 Spyware and Adware:

SPYWARE (and many people include ADWARE when speaking of SPYWARE since ADWARE often includes code which tracks personal information and sends it to a third party) are programs designed to collect information on you, your habits and other private information without your knowledge and transmit it across the Internet to a company or person. SPYWARE is similar to a TROJAN, as it can be installed when a person installs another program. These programs can be used to record keystrokes, scan files and websites that you use. The most common ways to fall victim to SPYWARE is to download peer-to-peer downloading software (such as “Grokster” or “Gnutella”) for sharing files or from site cookies. Some SPYWARE programs can self install as a result of a “drive-by download”. Xupiter is an example of a drive-by download. After it installs, the user finds his homepage replaced, browser settings changed and searches wedirected to a search site other than he one the user wants.,

 ► The following websites are just a few of the many where you can obtain additional information on SPYWARE and ADWARE.

PestPatrol, Inc. <http://www.pestpatrol.com>

Spyware-Guide.Com <http://www.spywareguide.com>


2.3 Social Engineering Attacks, Cracking and Script Kiddies:

I’m not talking about sociology, drugs or daycare. Loss of data, damage or infection by viruses can occur from human directed sources. Social Engineering Attacks include the classic example of old time business espionage: gaining physical access to the computers in an office through deception. In a recent computer magazine article about HACKING, they relate how a White Hat Hacker (i.e. a hacker who alerts a company to a security vulnerability) was hired to gain access to a company’s network. Impersonating a telephone repair person, he gained access to offices and cubicles. He went through those until he found access codes in an unoccupied office giving him access to the network. Social Engineering Attacks can also take place in instant messaging (a type of private communication across the Internet) or Internet Chat Rooms (similar to Instant Messaging provided by many Internet Service Providers) with a Hacker gaining the persons trust and then obtaining personal information or even offering a screen saver or other program. This will contain a TROJAN which will track the persons keystrokes and send them to the Hacker.

HACKERS are those persons who seek to gain entry into computer systems through unauthorized means. Many hackers try to differentiate themselves today based on their activities: White Hat hackers see themselves as providing information that can help companies by exposing vulnerabilities before someone else can exploit them. Black hat

hackers a/k/a CRACKERS use their talents with malicious intent to harm or damage the victim. To many, the intention makes no difference.

Script Kiddies are HACKER wannabes. They are unskilled and use pre-compiled hacking scripts and programs to try and gain access to a computer or network. Unlike HACKERS, they have little or no programming ability. However, for many unprotected or updated systems, the available tools can allow them to do significant damage.

 ► To find websites on hacking, run a search in any popular search engine for “hacking websites”.

2.4 Physical threats and catastrophes:

What happens if your computer is damaged, destroyed or stolen? Or your hard drive crashes due to age? Security threats include not only those discussed above, but also loss of your computers and data through theft, catastrophe or human error. Computers can be damaged by both fire and water and can be stolen. You can sustain the loss of a hard drive from mechanical failure. Failure to keep backup sets offsite and to verify that the backups are valid will be of little comfort when you need them to recover from a loss or theft.

Events such as these can either be a nuisance or a disaster. Failure to plan for these events can cause as much damage as the threats discussed in the preceding sections of this article.

2.5 Wireless and Mobile Computing Threats:

Allowing outside access to your wireless network
Unauthorized access to a wired computer network is known as HACKING.
Unauthorized access to a wireless network is known as WHACKING.

2.5.1 War Driving:

Using wireless technology at your home or office also presents its own set of dangers. Failing to take precautions with your SOHO (Small Office Home Office) wireless network can lead you to be a victim of a practice commonly known as War Driving. This is the practice of people literally driving around with a notebook computer, wireless network card and software such as NetStumbler (which is free) looking for unsecured wireless networks. Run a search on your favorite Internet search engine for war driving and you'll be amazed at the information regarding this practice and available tools to do it.

War Driving traces its roots back to the older concept of War Dialing. This phrase apparently originated in the movie "War Games" – Matthew Broderick set up his computer to dial thousands of random telephone numbers. The purpose was to find a system that had a modem attached to it and then try to access it.

2.5.2 Failing to change default wireless network settings:

Most SOHO wireless ROUTER/ACCESS POINTS (these are the devices that allow you to establish a bridge between your wireless devices and your wired network and/or Internet connection) and network cards are designed for ease of use. They come pre-configured with manufacture default user names, passwords and settings to facilitate setup. However, most people don't change these default settings! As there are a limited number of manufacturers for this equipment, it takes little effort for someone to run through the default settings to see if they've been changed or not when they find a wireless network.

2.5.3 Failing to enable security:

Wireless networking includes optional security to encrypt the information as it is being broadcast to authorized users. However, it must be enabled by the end user as the default from the manufacturer is that it is disabled. Unfortunately, it can a) be difficult to enable and b) cause a decrease in performance, so many people don't enable it. By doing this, you are in effect, sending your data over the public airwaves unencrypted! Anyone who intercepts it can read it

3. Defending the Gates: Common Sense Steps to Deter and Deal with Security Threats

3.1 Operating System:

The first place to start in protecting yourself and your data, is by keeping your Operating System (“OS”) up to date. Microsoft Windows is the most widely used OS and is therefore the primary target for HACKERS and CRACKERS. No protection plan that you undertake will survive contact with the Cyber-Barbarians if you fail to keep your OS up to date. If you use Mac OS X or Linux, you’re not out of the cross hairs: vulnerabilities have been found in both of these and as they become more widely used, the number of attempted exploits will also increase.

Updates

Windows XP provides for several different options for automatic updates which can be activated as follows:




Click Start > Control Panel > Performance and Maintenance > System > Automatic


3.1.1 Updates:

 ► This method will work if using the Category View for folders.

or

Click Start > Control Panel > System > Automatic Updates.

 ► This method will work if you are using Windows Classic view for folders. Make sure that the “Keep my computer up to date” checkbox is marked. Then select from one of the three options for downloading and installing updates.

 ► The first two options allow you to control and requires you to be involved in installation of each update. The third option will automatically download and install updates on the schedule you establish, thereby automating this process.

 ► Microsoft now publishes security updates on the Second Tuesday of every month.


You can also manually scan your system and download updates by accessing the Windows Update website at:


<http://v4.windowsupdate.microsoft.com/en/default.asp>


or



Click Start > Help and Support > Keep your computer up-to-date with Windows Update.

 ► This will take you to the Windows Update website which you can allow to scan your system for updates.

 ► Critical Updates and Service Packs are those updates that affect security and vulnerabilities of your computer – these should be downloaded. Windows Updates may include helpful updates, but also updates that you may not want, so review these before downloading. Driver Updates affect device drivers for your system and you should review these and consider them carefully before downloading.

 ► If you are using Windows Internet Explorer (“IE”) as your web browser, the Windows Update will also download updates for IE as well.

3.1.2 System Settings:

In IE, you need to have your Security Settings for the Internet set to at least a Medium Level. This will prevent anyone from installing ActiveX or Java Scripts without requiring your approval.



To make changes to these settings:

Open IE.

Click Tools > Internet Options > Security > Internet > Custom Level.

You also need to set your Privacy level to at least Medium as well to prevent unauthorized cookies (messages from a web server to your browser that can be used for good as well as bad purposes) from being placed on your system.



To make changes to these settings:

Open IE.

Click Tools > Internet Options > Privacy.

If you are using Outlook Express (“OE”) as your email client, you should disable the preview pane.



To disable the Preview pane:

Open OE.

Click View > Layout .

Uncheck “Show Preview Pane”

You should also disable OE’s ability to automatically complete the address field and to disable the ability to send messages immediately.

Disabling the auto address complete prevents you from inadvertently sending a message to the wrong party. Disabling the Send Immediately function, allows you an opportunity to verify the correct address and to prevent you from sending before you are positive it is ready to send. This removes the possibility of committing malpractice by sending a message to an improper party.




To disable auto address complete

Open OE.

Click Tools > Options > Send.

Uncheck Send Messages Immediately.

Uncheck Automatically complete e-mail addresses when composing..

 ► YOU SHOULD BE CAREFUL ABOUT OPENING MESSAGES OR FROM A SENDER YOU DON'T KNOW AND NEVER OPEN AN ATTACHMENT IF YOU ARE NOT EXPECTING IT WITHOUT VERIFYING WITH THE SENDER THAT IT WAS INTENDED TO BE SENT TO YOU. BE SUSPICIOUS OF MESSAGES WITH SIMPLE REGARDING LINES SUCH AS 'HI' OR 'HELLO'. ALSO BE EXTREMELY CAUTIOUS IF WORDS ARE MISPELLED OR THERE ARE CHARACTERS OR NUMBERS INTERSPACED. AS LAWYERS, WHEN WE DEAL WITH ANOTHER PARTY IN A LAWSUIT WE ARE SUSPICIOUS OF ANYTHING WE GET FROM THEM – YOU NEED TO ADOPT THE SAME MINDSET WHEN DEALING WITH EMAILS AND ATTACHMENTS.

3.2 Passwords:

Using strong passwords is another common sense method of protecting yourself, and yet most people fail to use them. The excuses range from difficulty in remembering them, they take too long to enter, to plain laziness. Passwords, especially those that are words that can be found in a dictionary, are easy prey to a Cyber-Barbarian through the use of a dictionary attack. These utilize programs that literally run through the words in a dictionary. With modern computers and broad band access speeds, these types of attacks take little time to complete.

3.2.1 Do's and Don'ts:

Do use a mix of upper and lower case letters

Do include characters as well as numbers

Do make it 8 or more characters in length

Do change your passwords on a regular basis

Do secure your password

Don't use names, birthdates or other important dates

Don't write it down in an unsecured location

Don't use Windows Remember My Password Feature

Don't give it to someone else.

3.2.2 What Makes a strong Password:

Strong passwords are those that are difficult for a HACKER to discern, but easy for you to remember. This doesn't mean that the password should be easy, but whatever process you use should make it easy for you to remember.

Numerous methods exist and are suggested, including using the first letters of a phrase, using a combination of portions of key words and dates, or combining portions of multiple addresses. An example of the first option would be using something like "tnstaaf" (the author Robert Heinlein coined this term to represent the phrase "There's no such thing as a free lunch").

There are also programs available for generating passwords, which rely on the random number generators and other formulas.

📁 ► Programs:

Advanced Password Generator 2.82 available at
<http://www.cnet.com>

📁 ► Websites about Passwords:

<http://www.adpc.purdue.edu/BSC-Pete/ARIBA/passwrds.htm>
<http://oneman.cs.ucl.ac.uk/adsl/v2sld2.html>

3.3 Anti Virus:

To protect against viruses, you can purchase computer programs to protect your computer against infection. These are known as Anti Virus ("AV) programs and provide varying levels of protection. AV programs can be placed on a single computer as well as on an entire network. While it seems to be common sense to have an AV program running on every computer, many people still don't. Even more fail to keep the Signature Files updated on a regular basis, and even more fail to renew their subscriptions for updates after they expire.

Signature Files allow your AV program to identify viruses and allows an AV manufacturer to provide updates as new viruses are discovered.

Bottom line, you must run an AV program. Arguably, failing to do so could be seen as malpractice if failing to do so allows confidential information to be lost or compromised.

3.3.1 What it should check:

An AV program should check both outgoing and incoming files. It should also check email messages that you receive and send. Better AV programs also allow you to scan inside compressed files.

3.3.2 Updating virus signature files:

AV programs also provide for a method of updating their Signature Files and the program itself. Most provide for this process to be totally automatic so that all a user has to do is select how often it happens. In the current environment, you should have it check no less than once a week and preferably at least every day.

It is also important that you keep your subscription current and renewed each year to prevent any lapse in obtaining the latest information and updates available.

There are numerous programs available, including some free ones for personal use.

📁 ► Free AV Programs:

Kaspersky AV : http://www.grisoft.com/us/us_index.php

📁 ► Commercial AV Programs

eTrust AV: <http://www.ca.com>

Norton AV: <http://www.norton.com>

McAfee AV: <http://us.mcafee.com>

3.4 Firewalls:

Firewalls are designed to prevent unauthorized access to a computer or network. Sometimes referred to as gateway or perimeter devices, firewalls sit between the Internet and your computer or network. They are the first line of defense against HACKERS and other attempts to gain unauthorized access. There are 2 types of Firewalls that can be used a) software and b) hardware. Firewalls also block Ports used by programs to communicate, thereby preventing unauthorized use of them by anyone.

You can use both types of firewalls for maximum protection.

3.4.1 Hardware Based:

Hardware firewalls are generally easier to implement and require less user intervention. However, hardware Firewalls do not prevent a Trojan from sending information out from your computer or network, they only block intrusions to your computer or network.

📁 ► Hardware based Firewalls can be obtained from companies including:

SonicWall

CheckPoint

Symantec

D-Link

Netgear

3.4.2 Software Based:

Software Firewalls can prevent both incoming and outgoing traffic. This requires a greater level of flexibility, but also means that in order to function most effectively, it must be trained by the user.

📁 ► Software based Firewalls include:

ZoneAlarm Pro

Tiny Firewall

BlackIce Defender

The are also available form Norton and McAfee

3.4.3 Techniques:

Firewalls use one or a combination of several techniques to operate and provide protection:

3.4.3.1 Packet Filtering:

Packet Filtering – the Firewall inspects each packet of information to verify compliance with the firewall rules. The best method is Stateful Packet Inspection which digs deeper into each packet of information.

3.4.3.2 Application Proxy:

APPLICATION PROXY- the Firewall controls access by each Program. It can allow certain commands to be executed from behind the Firewall, but block others if originating from outside the Firewall.

A combination of the above techniques is commonly used.

3.4.4 NAT ≠ Firewall:

Many SOHO Routers claim they provide a Firewall by using Network Address Translation (“NAT”). NAT does not equal a true FIREWALL. NAT is used to allow one internet address to be shared between several computers. It does this by hiding computers on a network from the Internet and assigning a series of Private network Addresses to those computers. By doing this, the computers that NAT serves are

hidden from view, but that's all it does. You need to make sure that you are running either or both packet filtering and application proxy in addition to NAT.

📁 ► You can test the effectiveness of your Firewall and system information by going to Gibson Research Corporations website at: <http://grc.com>. Select ShieldsUp and LeakTest to test your system.

3.5 Encryption:

Encryption converts information that you store or send into a secret format that requires use of password or key to access. Encryption can be used to encrypt email as well as data stored on your computer or network.

3.5.1 Public Key:

The most widely used method of encryption for personal use is called Public Key encryption. This method uses a private and a public key to encrypt and decrypt information. Using a persons public key, you can encrypt data and send it them and they use their private key (known only to them) to decrypt it.

3.5.2 Asymmetric encryption:

Asymmetric encryption uses the same key to encrypt and decrypt data. This method requires both the sender and recipient to know and use the same key, thereby introducing an additional level of complexity and a failure point should the key fall into the wrong hands..

3.5.3 Is Encryption required for Email?

There is no set answer to this question. Different professions have different requirements. Lawyers in Illinois are not required to use Encryption to send email to clients. The Illinois State Bar Association Ethics Committee has stated that lawyers may use electronic mail services, including the Internet, without encryption to communicate with clients unless unusual circumstances require enhanced security measures.

📁 ► Some clients may request that you encrypt messages to them, so you should be familiar with how to do this. You may also want to obtain a program such as PGP (Pretty Good Privacy) to do this. You can obtain more information at: <http://www.pgp.com>

📁 ► Encryption can also be used on your computer files which does lessen the chance of the disclosure of confidential information in the event of hacking or theft.

3.6 Physical Security:

Many of us take physical security for granted when it comes to our computers and the data maintained on them. Threats come not only from the Internet, but also from good old fashion casualty loss and theft. Commons sense can again help you limit the damage and risk in even in these instances.

3.6.1 Access to Hardware:

Servers and backup media should be in a secure location. You may want to consider a locking cabinet or cable security device if your office is not protected by an alarm system. Even with an alarm, computers that are readily accessible can be grabbed or damaged immediately after a break-in. Computers should also be raised off the floor to prevent water damage resulting from leaking pipes or coming in under a door. By securing servers and backup media, you lessen the chance that an unauthorized person will gain access to them.

3.6.2 Data Backup and Storage:

Verified backup sets kept off site can allow you to save data in the event of a casualty or theft. Different people have different opinions as to which is the best media to make backups, how often to make them and where to keep them. My opinion is very straightforward: Pick a solution, make regular backups and verify that the backups are good! Below I outline a seven step plan designed to help you set up a back up schedule for your office.

The Seven Step Plan:

Step 1: Determine how much information you need to backup.

Step 2: Select your backup media.

Step 3: Select your backup software.

Step 4: Determine a backup schedule and follow it.

Step 5: Verify whether your backups are working.

Step 6: Keep at least one backup off site.

Step 7: Perform your backup regularly

You need to pick a schedule that is reasonable for your practice and that you can maintain. Remember, if you suffer a data loss, you're only as good as your last backup! If that was 3 months ago, you will have lost 3 months of data and you will need to recreate it.

Don't just use one or two backup tapes or disks. If a backup media fails (tapes and disks do wear out) or the backup does not take for any reason, you have a better chance if you have been rotating your backup media using new backup tapes/disks at least once or twice a year and are using multiple tapes/disk for your backups.

You also need to verify that the backup is working: backups don't always work. Verifying your backups assures you that you have really saved all the information you wanted to backup. How often you do this is up to you: I recommend that you verify your backup at least once a month, if not more often.

If you keep your backup sets at the offices in your safe, in a file drawer or anywhere else in the office, this will only help you if your hard drive crashes, but will not be of any help if your office is destroyed by fire, flood or theft. Therefore, I suggest you keep at least one backup set offsite. One method is to take the Friday backup set home with you on Monday after it is done and bring back the backup set from the previous week. By doing this you build in redundancy by keeping a set off site.

3.6.3 Disabling Access for Suspended & Former Staff:

When a staff member is suspended or has left, too many times no one disables their access to the network. You need to insure that their accounts are initially disabled and eventually deleted from network and system access.

4. Defending the Colonies: Practicing Safe Wireless Computing:

Just as there are dangers in using the Internet from a wired network, these and more exist for the wireless world. There is the danger of “eaves dropping” on your system by other wireless users near your office or home as well as at public hot spots located at coffee stores, parks, airports and other locations. These Cyber-Barbarians are lurking about looking for people that have failed to enable security measures on their wireless network. They’re looking for people who have not disabled their wireless card’s ad-hoc mode allowing for peer-to-peer connections to their computer and also have file and print sharing enabled. You’re also still vulnerable to all the usual dangers like a worm, virus and spyware. However, you can take reasonable steps to limit these dangers and to make the task of these Cyber-Barbarians that much more difficult, if not impossible.

4.1 Dangers in the “Wild”:

Public hot spots are usually set-up for ease of use, not security and most likely won’t allow use of any standard connections security. But there are still steps that you can take to protect yourself.

4.2 Practicing Safe Wireless Computing in the Wild:

The steps outlined earlier regarding your OS and AV software should be followed when using your notebook and a public hot spot. In addition to these steps, you should:

Use a Software Firewall.

Consider using encryption for your e-mail and digital signatures.

Disable your wireless cards ad-hoc option.

Disable file and printer sharing.

Disable your wireless card if you’re not working online.

Be aware of anyone looking “over your shoulder” as you enter your passwords.

Consider using VPN software and a VPN endpoint if you have them.

Don’t provide your credit card number unless the site is protected by Secure Socket Layer (SSL). These sites are identified by https// in their URL.

4.3 Protecting the Office:

Your options for securing your wireless network are greater than if you are using a public hot spot. In this environment, you again follow the steps outlined earlier regarding your OS and AV software.

You also need to enable ENCRYPTION available for wireless networks. There are currently 2 different encryption protocols for encrypting the information sent across a wireless networking.

4.3.1 Wired Equivalency Protocol (“WEP”):

WEP is the first protocol established for use by wireless networks. The intent as demonstrated by its name, was to provide the same level of security as provided on a wired network. Unfortunately, not long after it was introduced, ways to circumvent WEP were found, which for technologically adept persons, could be used to break the encryption and gain access to the network and its information.

4.3.2 Wi-Fi Protected Access (“WPA”):

The Wi-Fi Alliance has now introduced WPA, which resolves the security issues found with WEP. It uses a higher level of encryption and therefore a greater level of security. However, at the time of this paper, vulnerabilities in WPA have been found which can compromise the efficacy of WPA..



Despite known vulnerabilities, you are still better using either WEP or WPA than not using them.

4.3.3 Service Set Identifier (“SSID”):

Every wireless Router/Access Point has an SSID which is set at a factory default when initially setup. This is what differentiates one wireless network from another and is sent in plain text. To make it more difficult for someone to identify your wireless network you need to change the standard SSID and Administrator Password of your Router/Access Point.

4.3.4 Disable SSID broadcast if possible:

If possible, you should disable the SSID broadcast.

4.3.5 Limit Number of Computers:

If you only have x number of computers which will attach to the wireless network, you should limit the number of machines that can access the network to that number. As long as those computers are connected to the wireless network, no other machines can attach.

4.3.6 Router/Access Point Placement:

Since the Router/Access Point generally broadcasts in all directions. Place the access point in the center of your building/office/home if possible - the closer to an outside wall that you place it, the further the range that someone can pick-up a signal.

Select infrastructure mode.

You can select from 2 wireless modes – ad hoc and infrastructure. ad hoc mode allows wireless equipped computers to communicate directly with each other without the need of first communicating with a Router/Access Point. infrastructure mode requires each wireless equipped computer to use of the Router/Access Point to communicate.

4.3.7 Limit access by specific Media Access Control (“MAC”) address:

Each network card is identified by a unique MAC address. By limiting access to the wireless network by MAC address, even if one computer isn't attached, no one else can communicate with the Router/Access Point since their MAC Address will not be approved for access.

4.3.8 Consider disabling DHCP and assigning static IP addresses:

This allows you to control which network addresses are assigned and which ones will be recognized by your Router/Access Point

5. Conclusion:

The security threats that you face each day are numerous and are changing constantly: each day brings new threats and new means of countering them. Very few systems can withstand a concentrated, human guided assault to gain access. However, if you take the common sense steps outlined above, you make it more difficult for your system to fall before such an assault. Time is your friend in these matters and the longer it takes for someone to break through your defenses, more likely they will move on to find easier prey.

In addition to the steps outline above, you should also consider having an acceptable use policy for your staff dealing with what is and isn't allowed on work computers. This can be as simple or as complex as you want to make it. At a minimum it should set out download policies and whether or not staff can load other than approved programs provided by the firm. You should also consider establishing client email policies to set the parameters for clients and prospective clients to communicate with you over the Internet. Sample e-mail policies can be found at the end of this paper in Appendix A.

The bottom line is that you must be constantly vigilant and prepared to deal with security threats or else the Cyber-Barbarians will wreak havoc in your system.

Appendix A

Policy Sent by E-mail to each new client.

The following are samples of a client e-mail policies that can be sent to each new client or posted on a website:

Client Policy Sample #1

Subject: Greatlaw, P.C. Client E-mail Policy

Dear New Client:

You may contact or respond to me using e-mail.

The following should be followed if you choose to use e-mail to contact me:

1. While e-mail may appear to be quicker for getting me information or to get a response, I treat this form of communication no differently then I do a fax or a written letter and my response may take the same amount of time as if responding to a fax or letter. If you are sending me something that is important or time sensitive, please call and let me know.
2. Do not send any type of attachments to messages except graphic files such as .gif, .jpg and .tiff, unless we discuss them in advance.
3. Do not send or forward e-mail that is not related to our matter or work.
4. Replies to your e-mail will be sent to the "reply-to address" of your own e-mail. If you want me to reply to another e-mail address, you must tell me specifically at the start of my representation of you.
5. If you are sending the e-mail from work, remember that you might be violating your employers e-mail policy by receiving and sending private e-mail and that your employer might have the legal right to read your e-mail.
6. If you wish to contact me by e-mail, please send to: iamManager@greatco.com

Respectfully:
Iam Manager
Greatco, Inc.
111Main Street
Rockford, IL 61101
815.999.1212

SAMPLE E-MAIL AND INTERNET USE POLICY

To maximize the benefits of our company's computer resources and to minimize potential liability, ABC Management Co. has created the following policy. You are required to observe this policy at all times.

1. Use of computer network is for business purposes only. Access to ABC Management Co.'s computer network, including the e-mail system and Internet, is provided to assist you in performing your job. You should use the network for business purposes only.
2. No privacy should be expected. The entire computer network, including the hardware and software and e-mail systems, belongs to ABC Management Co. You should consider any communication or information on the computer network to be public information. You should not have any expectation of privacy in anything you create, send, store, or receive on the computer network.
3. Company can review any material on network. Without prior notice, ABC Management Co. has the right, but not the duty, to review any material created, stored, sent, or received on or through its computer network.
4. Use of personal passwords is prohibited. You are prohibited from using computer passwords not known to the company. Personal passwords should not be considered a guarantee of privacy.
5. Network may not be used for prohibited activities. Use of ABC Management Co.'s computer network or resources for any of the following activities is strictly prohibited.
 - Sending, receiving, downloading, displaying, printing, or otherwise disseminating material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or that is otherwise unlawful.
 - Disseminating or storing personal advertisements, solicitations, promotions, destructive programs, political information, or any other unauthorized material.
 - Wasting computer resources by, among other things, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic.
 - Using or copying software in violation of a license agreement or copyright.
 - Violating any state, federal, or international law.
6. Prior authorization is required for transmission of certain information. You should not place on the Internet or transmit by e-mail any information that is of a confidential, sensitive, or proprietary nature to ABC Management Co. without authorization from your supervisor.

7. All e-mail should be considered public information. The mere deletion of an e-mail message may not fully eliminate the message from the system. E-mail can be “undeleted” using special software. Do not write any e-mail messages that you would not want to become public information.

8. Violation of policy may result in disciplinary action. Violation of this policy will be taken seriously and may result in disciplinary action, including possible termination and civil and criminal liability.

9. Agreement to comply with policy. I have read and understand ABC Management Co.’s E-mail and Internet Use Policy and agree to comply with its terms. I also consent to ABC Management Co.’s review of any material I create, store, send, or receive on or through ABC Management Co.’s computer network.

Signature _____
_____ - _____ Date

Printed name _____

Nerino J. Petro, Jr.

Attorney Nerino J. Petro, Jr. is a practicing attorney in Loves Park, Illinois as well as CEO and senior legal technologist for CenCom, a Division of Centro, Inc.. He is currently Secretary of the Illinois State Bar Committee on Legal Technology, serves on the ISBA Special Committee on Electronic Research Services for Members, the Winnebago County Bar Association Web Site Committee, the ABA GP, Solo and Small Firm Section Legal Technology Committee and the ABA TECHSHOW Advisory Board for Tech University. Since 1988, he has worked with technology service providers in the imaging, computer hardware and software fields and founded CenCom in 1994. He is an Authorized Independent Consultant for all editions of TimeMatters® practice management software and Billing Matters® time and billing software, and is an authorized reseller of TABS® time and billing software, and Practice Master® practice management software. He provides professional and legal technology services to businesses, lawyers and their staff throughout the country including consulting, training, installation and customization. His articles can be found in both state and national publications on a range of technology topics. He can be reached at njpetro@lawofficetech.com and www.lawofficetech.com.



349 E. Riverside Blvd.
Loves Park, IL 61111
815-636-1023 tel
815-636-8660 fax
njpetro@lawofficetech.com
www.lawofficetech.com

Nerino J. Petro, Jr.
Attorney/CEO