

New Years Security Resolutions

by: Randy M. Nash, 01/17/2005

<http://www.securitydocs.com/library/2873>

Happy New Year! I know many of you have received some nice to tech toys for Christmas recently, so its time to talk about making them secure and keeping them that way.

I know many of you have new computers in your homes, but how many of you realize that this computer is *already vulnerable*? How can this be? How can a brand new computer be vulnerable? There are many reasons for this:

- Most computers have insecure default configurations.
- Your software is probably already outdated. New vulnerabilities have likely been discovered between the time the computer was built and configured by the manufacturer and the day you power on your new system.
- Numerous viruses and worms are already circulating on the Internet capable of taking advantage of the latest vulnerabilities.
- Hackers know where you are! They regularly scan the common broadband and dial-up IP address ranges.

As a result, if you immediately connect your new computer to the Internet, it could be compromised before you've even had a chance to set up your email account.

Before You Connect

Let's talk about what you should do before you connect this new system to the Internet.

Firewalls

You should not connect your computer directly to the Internet. You should, instead, use a network firewall or firewall router. A network firewall or firewall router is a hardware device that users can install between the computers on their Local Area Network (LAN) and their broadband device (cable/DSL modem). By blocking inbound access to the computers on the LAN from the Internet at large (yet still allowing the LAN computers' outbound access), a hardware-based firewall can often provide sufficient protection for a user to complete the downloading and installation of necessary software patches. A hardware-based firewall provides a high degree of protection for new computers being brought online.

If you're running Windows XP (and if this is a new system, you probably are) you enable the Internet Connection Firewall (ICF). Microsoft has provided [instructions](#) for enabling the built-in Internet Connection Firewall on Windows XP.

If your operating system does not include a built-in software firewall, you may wish to install a third-party firewall application. Many such applications are available at relatively little (or sometimes no) cost. However, given that the issue we're trying to address is the relatively short lifespan of an unprotected computer on the open Internet, we recommend that any third-party firewall application be installed from media (CD-ROM if possible) before connecting to a network rather than downloaded

directly to the unprotected computer. Otherwise, it may be possible for the computer to be exploited before the download and installation of such software is complete. If possible, download the software to a protected computer and burn it to CD. If you do not have this capability yourself, then you need to limit your exposure as much as possible. Connect the system to the Internet, go to one of the following website and download the desired firewall product, then disconnect immediately. My two personal favorites are:

- ZoneAlarm from [ZoneLabs](#)
- Personal Firewall from [Kerio](#)

ZoneAlarm is a nice and easy firewall that anyone can use without a technical background. If you're a bit more technical, or would like to learn more about firewalls in general, Kerio's product has a bit more granularity. There is a comprehensive listing of firewall software available [here](#) and [here](#).

Disable nonessential services, such as file and print sharing. Most operating systems are not configured with file and print sharing enabled by default, so this shouldn't be an issue for most users. However, if you are upgrading a computer to a new operating system and that computer had file or print-sharing enabled, it is likely that the new operating system will have file and print sharing enabled as well. Since the new operating system may have vulnerabilities that were not present in the older version being upgraded, disable file and print sharing in the older version before beginning the upgrade process. After the upgrade is complete and all relevant patches have been installed, file sharing can be re-enabled if needed. The following should work in most versions of Windows:

- Go to Start/Settings/Control Panel.
- Double-click the "Network and Internet Connections" icon.
- Open "Network Connections".
- Right-click on the network connection you wish to change (e.g., "Local Area Connection") and select "Properties".
- Make sure "File and Printer Sharing for Microsoft Networking" is unchecked.

First Steps After Connecting to the Internet

Download and install software patches as needed. Once the computer has been protected from imminent attack through the use of either a hardware or software-based firewall and the disabling of file and print sharing, it should be relatively safe to connect to the network in order to download and install any software patches necessary. It is important not to skip this step since otherwise the computer could be exposed to exploitation if the firewall were to be disabled or file/print sharing turned back on at some later date.

- Go to <http://windowsupdate.microsoft.com/>.
- Follow the instructions there to install all Critical Updates

Install and use antivirus software

With all the malicious software floating around the Internet (viruses, worms, Trojan software, etc) an up-to-date antivirus software package is a definite MUST. Anti-Virus software is not a cure-all, but it is your best front-line defense against compromise. A couple of my favorites (free for personal use) are:

- [AVG Free Edition](#)
- [AntiVir Personal Edition](#)

There is also a good listing of commercial Anti-Virus products available [here](#).

Spyware/Adware Protection

A growing problem is the plethora of [spyware](#) and [adware](#) that can be surreptitiously installed on your system, either while browsing the Internet, or sometimes by downloadable programs that we install on our own. I recommend you download and install the two following programs:

- [Spybot-S&D](#)
- [Ad-aware SE Personal](#)

These two programs, working in concert, provide optimal protection against the latest spyware and adware.

Pop-Up Protection

Pop-up Ads! We all get them; we all hate them! There's nothing more irritating than surfing along, minding my own business, and getting blasted with multiple windows popping up and begging me to buy the latest junk software. At least, nothing other than SPAM, but we'll get to that later.

Pop-ups are a fact of life on the Internet, but they can be minimized to some degree. First, there are many pop-up blockers available. I personally like the [Google Toolbar](#), but many of my friends and colleagues like the [Yahoo! Toolbar](#) just as much. Both of these toolbars provide a pop-up blocker, along with some nice features unique to their service. I like Google's toolbar because it lets me set my default search engine to Google. The Yahoo! Toolbar claims not only pop-up blocking, but some anti-spy abilities as well (I've not tested this myself). Either one works well, but neither one can get rid of ALL pop-ups. No matter what we do, new techniques are being developed to get around these blockers. It's a running battle.

Phishing

Phishing has become one of the fastest growing threats related to identity theft. Phishing attacks use a fake e-mails or webpage to fool you into giving up sensitive personal information that can be used to steal your identity (for financial purposes). This information can consist of personal financial data such as credit card numbers, account usernames and passwords, and social security numbers. The use of well-known names (banks, AOL, eBay, etc) enables these phishers to convince up to 5% of recipients to respond to them. Beware!

So, how can you detect a phishing scam? First of all, any reputable agency will NOT ask for your account information, user id, password, SSN, or related information via an email. If you get an email asking you to go to a website and *confirm* any of this information be extremely cautious as well. Websites can be faked very easily. The [Anti-Phishing Working Group](#) has made it their mission to track and report this sort of activity. You can review their website for more information. If you do a lot of online banking or online purchasing and you're concerned about this threat, [Netcraft](#) has developed their own [toolbar](#) (yes, I know... another toolbar) to help you identify potential scam sites. Please review

[their site](#) for more information.

Wireless (Wifi) Security

Another hot item found in many Christmas stockings this year is wireless routers. This presents a whole new host of security issues that need to be addressed. A wireless router makes it easy to expand your home network. No more dragging cables around your house, or trying to snake them through the walls. Simply purchase a wireless router and wireless network card and you're ready to go... right? Wrong!

Sure, you can plug everything in and if all goes well you can be up and surfing in no time. The problem is that wireless network is completely insecure. If you just set up the equipment and use it right out of the box you have very likely opened your whole network and Internet access to anyone else with wireless connection. The default settings allow ANYONE to connect to your wireless router and, by extension, your Internet connection. Wireless networking can provide connectivity beyond the walls of your home. Your neighbors, or even someone driving down the street with a wireless laptop could connect to your network without your knowledge. There are some steps that you should take to provide some measure of protection to your wireless network.

A good friend of mine has written some excellent guidelines for Wireless Security. The full guides are available via his website: [Blackthorn Systems](#). He has written a both a [Home Security Guide](#), and a [Small Business Security Guide](#). With permission of the author, the primary steps for home users are:

1. **Change ALL the default settings on your Access Point, wireless cards, and routers.** These include the SSID, Administrative passwords and User passwords. The default names and passwords are published by the manufacturers on the Internet and are available to anyone.
 - o Choose an SSID (Network Name) that will not attract unwanted attention. Do not use your telephone number, family last name, the name of the residence, the address of the residence, etc.
 - o Choose a unique SSID.
 - o Disable Automatic SSID Broadcast. If you have more than one AP set up to allow roaming, you might not want to do this due to technical considerations. However, most users should consider this option.
 - o Change the default channel. While this is not truly a security issue, it may help with radio interference, as many devices use the same channel.
2. **Always use encryption (WEP or WPA) on your wireless network.** If possible, use a 128-bit or higher variation.
 - o Whenever possible, use additional encryption such as SSL or VPN.
 - o Change the encryption key on a periodic basis.
 - o NEVER use the SSID (Network Name) as the Encryption Key.
3. If the following features are part of your AP or router, make sure you use them:
 - o **Firewall:** Restrict wireless usage to only the minimum TCP and UPD ports needed. And disable all other ports. For example, you may wish to enable TCP Port 80 (HTTP), and TCP Port 110 (POP) yet disable TCP Port 25 (SMTP) to prevent becoming a wireless mail relay, and TCP Ports 20, 21 (FTP) to prevent unauthorized file transfers. Also, block file sharing ports for programs such as Kazaa.
 - o **Address Control List:** The ACL limits the Machine Address Code addresses that may access your AP. Each wireless Network Interface Card has a unique MAC address, so this limits which wireless NICs (and therefore which computers) may access your network.
 - o If a fixed number of mobile devices are connecting to the AP, **disable DHCP** and use static IP addresses.

- If a varying number of devices will be on the wireless network segment, **limit the size of the DHCP address pool** to the absolute maximum number of needed addresses. Many people use DHCP to make it easier on the users. However, there is no need to for the network to give out 254 addresses, or even 30, if you only need 3.
4. Most Access Points have built in logging. Periodically, review the access logs and look for any abnormalities.

Summary

This covers just some of the basics for securing your home computing environment. I hope this gets you all of to a safe and Happy New Year!