

Personal Computer Computer Security (Windows XP)

Introduction

Security for personal computers, at first, may seem a very obscure & highly technical area where most of us fear to tread. And in many areas this is true. However, this need not always be the case. We do use a lot of technical terms here, this can not be helped. However, if you point your browser to <http://www.wikipedia.org> and type the term into the search box, this may help you. The following suggestions apply not only to the average home user but to many small businesses that **must** have access to the Internet 24 X 7. We will discuss these areas in detail and offer pictorial guides or in some cases, a video “how to” as well. These are available FREE at <http://www.techinstructor.info> web site. So let us begin.

There are 3 components to be concerned about:

First, is your physical connection device to the Internet. This is usually your cable or DSL modem. This is the door way for Internet access. This is supplied to you by the Inter Service Provider (ISP). These devices are usually designed to allow only one computer to connect to the “net”. They DO NOT provide any inherent security. The ISP may offer software solutions to you. These may be free or supplied at additional cost. They are designed to run on your computer.

Second, is your computer. Again, very little physical security is present here. Most modern computers have the capability of protecting the BIOS (this is firmware software built into your computer that tells the Operating System-OS- what is available in the form of hardware resources) from unauthorized access by

means of a password. However, this is easily defeated by an experienced user. If the computer is a multiuser system, then you must rely on the OS password to lock out other users.

Third, the computer Operating System, in this case, Windows®XP. This is where we will offer the most advice. Here, with a little help from us, you can make the biggest difference in securing your computer system on the Internet.

HARDWARE

I mentioned earlier that, your physical connection to the Internet was your Cable or DSL modem and that these devices had no security. This is true. And you can not connect more than one computer to “net” at one time. Many households and small offices need this capability. So what can you do? Spend an extra \$50 or so and invest in a “NAT router”-(Network Address Translation). This device serves 2 purposes. First, it forms the basic infrastructure for your home or office computer network and secondly isolated this private network from the public Internet network.

When you sign up for that new high speed connection, your ISP's computer server will issue a special number (IP) that is associated with your modem. This is your “public” IP address. This number identifies your ISP but not your individual computer/network. The router technology translates the IP addresses of your local area network to the IP address assigned to your computer by your ISP. Each computer that is added on to your network, it is given a private IP address. ***Think of the public IP address as your modem's phone number.*** However, I feel this router, is a necessary component for computer security. Let me explain.

Routers come in two flavors. **Wired** and **Wireless** versions. I am referring to the wired system. We will discuss various forms of networking at a later time.

Router manufacturers have made the installation of this hardware device, pretty a much plug-it-in process. The router serves 3 main purposes.

1. It allows multiple computers to have simultaneous access to the Internet without additional charges from your ISP-a big plus here.
2. It is a way, also, to allow you to share files and hardware resources such as printers. This is **your** network.
3. It serves, most importantly, as device to **isolate** your computers directly from the Internet-kinda sorta like a firewall. I discuss this later.

Numbers 1 and 2 are indirectly security related but number 3 is one of our big 3 security defenses. This does require a little technical definition of how the Internet works. Please bear with me, it does make sense.

When your ISP installs your Cable or DSL modem (or they send it to you and you install it), to you home or office, they assign you a dynamic IP address (Internet Protocol). Think of this a changing (dynamic) “phone number” for your modem. This address is yours until the next time your reboot or power down the modem, then the ISP computer will assign a new one to you. This number allows your computer to call another computer with an IP address. The IP address of the distant computer usually has a name instead of a number. For example, when you open your web browser, you do not type in a number, instead you type in a name like,

www.techinstructor.info or www.msnbc.com . These names are linked to the IP address of that site. This all takes place in the Internet backbone computer systems located throughout the world. This, basically is how the Internet works.

So why is this important, because this is not a perfect world and there are web sites out there who wish to disrupt the Internet or for creating Spam zombies for instance and other nefarious reasons, all of which **CAN** and will affect your computer if you do not take some safeguards.

If your system is behind a router, it is in effect, invisible to **most** all of these nasties out on the net. I say most. Because, the bad guys are getting smarter & more clever. They take advantage of these “holes” in the net and your Internet ignorance. We will discuss this later.

So, invest in that router. The pluses out-weigh the additional cost. Now let us talk about the software side of things. Windows XP in particular.

Software

When discussing computer security, we must be aware of the GOOD, the BAD and the UGLY that exist on the Internet. By this, I mean securing the Operating System and maybe changing some of our behavior. In this case, the operating system is Windows XP and our behavior is our use of the applications inherent in Windows- such as email practices.

So where do we start? Windows XP, like all modern operating systems, is a very large & complex piece of software. The manufacturer does their best to try to secure this software. In the case of Windows XP, the bad guys have found and exploited many, many holes in Windows to accomplish many devious actions. Microsoft, the manufacturer, has been trying to stay ahead of these guys. They do this by offering operating system, sometimes mandating, updates and or offering other software solutions.

Windows XP is the most popular operating system in the world today and because of that (and other issues), it is the number one target for exploitation. These exploitations take the form of viruses, Trojan horses or taking advantage of allowable scripting functions in Windows, just to name a few.

So what can we do? We will tackle the what we can do for Windows XP and then our computer behavior.

1. Make sure your Windows XP system is updated with current Service Pack 2 and “patched” with latest releases. To do this, make sure the auto update function is enabled.
2. Make sure your system has anti virus software installed and that it is current.
3. Make sure you have an anti-spyware software installed as well and is also current.
4. Make sure your Windows Internet browser is updated to the latest version-currently 7.0 or use a different browser.
5. Make sure that Windows XP firewall is enabled.
6. Set up a limited user account for daily usage instead of the default Administrator account.

You can check your Windows XP system for patches and firewall by opening the Security Center icon in Windows control panel (again,

visit the www.techinstructor.info web site for the video for this procedure). This will advise you if auto update and the firewall is turned on, and whether you have antivirus software installed and up to date.

The Attacks

Even with all of the above, your system may still be vulnerable. How? The enemy (yes, this is war) now have many incentives, everything from mischief, to profit, to national defense and everything in between. And guess who is “in between”. Is my system under attack? To answer this I'll use an example. Shortly after Windows XP was released, there were many nasty and destructive attacks. These attacks were in the form of specially written or crafted snippets of software code, which when introduced into the Windows system, caused the computer to do strange things (like rebooting without operator involvement), programs either not running or simply disappearing, or worse yet, doing all of these things and taking control of your email client and sending email, with the malicious code inside, to all the addresses in your address book. The purpose being to spread itself. If you received an email from your friend with an attachment, then you can assume they sent it to you, not knowing that their system was “compromised”. Now your system is infected and the process starts all over again. All of this with out your knowledge or consent.

Microsoft not so quickly release later Service Pack 2 (which you should have installed NOW) which corrected many of these initial holes. If we take a computer today and install Windows XP without SP2 or antivirus/spyware software and the firewall off (which was how Windows was released) and connect it to the Internet directly

through a cable modem, after 1 week, the system will be compromised in some form. At that point you will probably have to re-format the system hard drive and re-install Windows (this time with out connecting to the Internet), and contacting Microsoft and have them mail you a disk with SP2. Even when this is done, the malicious software is still present in the Internet. But how can this be if Microsoft “fixed” the holes. That's because on about 60% of Windows XP system world wide are NOT patched. And until they are, the old stuff will continue to live -of course this does not account for the new attacks that happen on a daily basis).

These attacks take advantage of poor or no computer / Windows security or user behavior due to lack of knowledge or simply visiting a malicious web site of dubious reputation. We have seen what to do to secure the computer console and Windows XP but what about behavior. You system may be infected by:

1. Email, detaching attached files to you computer and running them.
2. Email again. This time clicking on embedded active links in an email message. These can re-direct you to a possibly questionable site.
3. Email again. ***NEVER***, and I mean ***NEVER***, give a web site any personal information such as credit card or banking information or social security number without calling the site, requesting this information, to verify their legitimacy or verifying by some other means. Most of the big Internet retailers (Amazon, Barnes and Nobel, Yahoo, etc.) have secure connections to their web site and can be trusted.
4. Downloading certain software and running it. Even if you uninstall this program, it may leave behind nuisance ware (ads, pop up windows and such) or worse case a Trojan, key stroke logger or who knows what.

5. Allowing others to use you computer with out restrictions.

The Defense

Anti virus software

Aside from the required patches and Service Packs for Windows XP, we should have a firewall (this is on by default with SP2) and installed anti virus and anti spyware software.

The later, fall into 2 broad categories. Commercial and free for personal use. There are many fine anti virus (AV) software products available today. All of these products require regular updates. These updates are files that contain certain strings of code or behavior that many viruses have in common, or exhibit. The manufacturers of the AV software are constantly scouring the Internet for these characteristics to try to keep even or slightly ahead of the bad guys. This is a multi-billion dollar industry.

My recommendation for a good and FREE AV product and needed updates, for personal use only, is AVG from www.grisoft.com. Is it the best? I do not know. But I can tell you this. It is generally rated among the top 5 that I have seen. I also speak from personal experience and you can not beat the price.

****** A word of warning here. **DO NOT** have two or more anti virus programs installed on your system at the same time. They can and usually will conflict and may cause programs not to run. So if you have an older version or a competitor product installed, uninstall it prior to installing the new one.

Anti spyware software

Noted programmer, Steve Gibson of www.grc.com, coined the word spyware. During his evaluation of firewall software on his Windows 2000 system, he noted that some downloaded programs installed “other” software not related to the initial program. This other software also “phoned home” with information about Steve's computer. All of this without his knowledge or permission.

The information being sent was benign. Had Steve not had a firewall installed, he would have been oblivious to this. This was the discovery of spyware. It is estimated to be a multi million dollar a year business and now in some states, illegal.

This is usually nuisance ad ware or pop up windows. In the more serious forms, special loader software can be activated and call home to download a more potent version. This new version can make your system a “zombie” for Spam or other nasties. It can also install something called a key stroke logger. This can record all of your keyboard key strokes and email the file to a hacker. The hacker then scans this file for things like social security or credit card numbers. All of this taking place with out your knowledge.

What can you do? Go to www.microsoft.com/defender and download and run this program. It. Like AV software, it has needed updates. It does a fairly decent job. But because the attack is so pervasive and the creators so clever, you may need to run a different anti spyware software. We recommend here, a free product called SpybotSearch and Destroy. Get it here: <http://www.safer-networking.org/en/index.html>. If your system is so heavily infested, you only real likely option would be to backup your data (which you should be doing regularly) reformat the hard

drive and re-install Windows XP.

The Firewall

What is a firewall and why do I need it ? From www.wikipedia.org : A **firewall** is an [information technology](#) (IT) [security](#) device which is configured to permit, deny or [proxy data](#) connections set and configured by the organization's [security policy](#). Firewalls can either be [hardware](#) and/or [software](#) based.

I dislike technical definitions. From the days of the early automobile, the firewall is a physical “wall” between the engine and the driver.

In the computer world, a firewall can be a physical or software based wall between your computer and the Internet. Remember the NAT router. While technically not a true firewall, it is non the less a physical barrier between your system and the Internet. The NAT stand for Network Address Translation. It has two primary functions. The first is to isolate your computer from the outside world and secondly, to block unwanted intrusions. It does these function extremely well. When coupled the Windows patches, the AV and AS software, your about a secure as you can get.



A software firewall protects your individual computer from Internet security threats such as viruses, worms, or other unauthorized software.

Well do I need the software firewall? Probably not. Remember, the firewall and the NAT router block unwanted incoming intrusions but not unauthorized outgoing traffic. If you detach a file attachment in email and your AV program is not up to date, a Trojan or key stroke logger may be installed on your system. It then can do send out the captured information through the firewall. Third party firewall software have the ability to block or allow, with your approval, out going traffic. But this is rare.

The Summary

1. Backup your data regularly
2. install patches for Windows XP
3. Make sure Windows XP firewall is on
4. Install and update an Anti virus software
5. Install and update an Anti spyware software
6. Install a hardware router (www.linksys.com)
7. Backup your data regularly