Internet Security for Everyone

by

Mark Hasting
http://www.pchell.com

Keeping a computer up-to-date and safe on the Internet can be quite a chore. Not only do you have to watch out for Viruses, Trojans, Worms, and Spyware, but Spam, Phishing Scams, Identity Thieves and Hackers can also pose huge threats to the computer and the information stored there.

Understanding how to secure your computer can be a daunting task for the average user. This guide will help you understand the basics of how to secure and protect your system along with some tools and knowledge to prevent future problems.

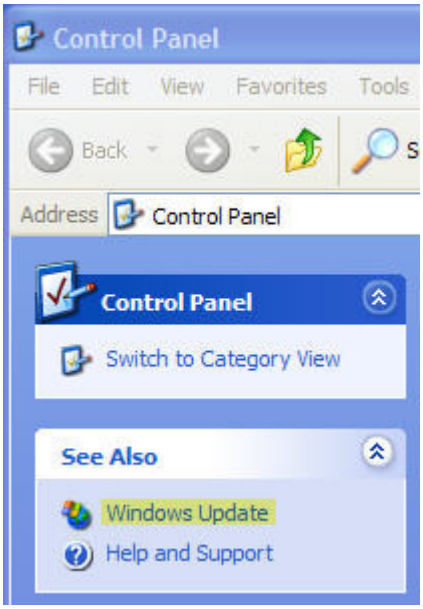
Computer Updates

The first line of defense in computer security involves updates. Keeping your computer up-to-date with the correct patches for the operating system, updates for your antivirus, and updates for anti-spyware is half the battle in preventing problems.

Windows XP Updates

Windows XP, although it's fairly easy to use, is very insecure without all the current updates. Because it's the most popular computer operating system, it's also the preferred target for hackers and others to attack. Making sure your computer has all the current critical updates for Windows XP is the highest priority. Follow the steps on the next page to check for updates and install them.

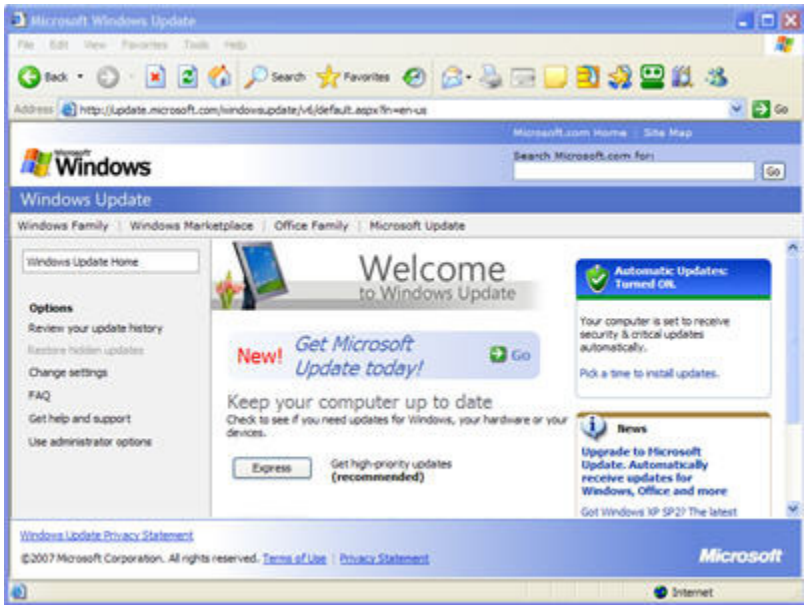
1) Open Control Panel, click on the Windows Update link in the left column



Alternatively, you can open Internet Explorer and go to the following site

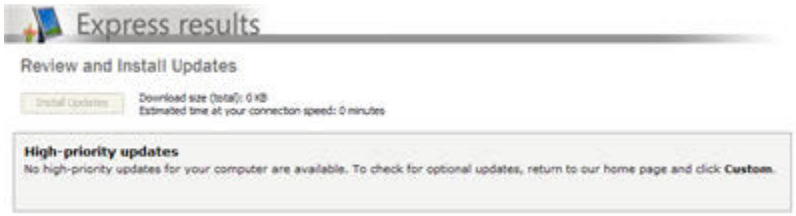
http://windowsupdate.microsoft.com

1) Click on the Express Button on the updates screen to allow the site to check for any critical updates that are not installed on your computer.



2) The site will check for any missing critical updates for your computer

3) If your computer has all the Windows critical updates installed, you should see the following screen. If there are updates to install, check them and install them. The computer will generally force you to reboot after installing them.



You should regularly check for Windows updates at least **once a month** to maintain the security of Windows XP.

Antivirus Updates

Your antivirus is only as good as its last update. One of the most common problems I run across is an antivirus program with old, outdated virus signatures. Generally once an antivirus is installed it will update on its own as long as it can connect to the Internet. However, if the antivirus subscription has expired, the program will stop updating and can leave your computer vulnerable to new threats.

For this reason, it's a good idea to check your antivirus program at least once a month to make sure its updating properly and protecting your system from virus, worm, and trojan threats.

If you have Norton, McAfee, or Trend antivirus installed on your computer, you can visit the following page to learn how to update your antivirus and keep it protecting your computer.

http://www.pchell.com/virus/virusupdates.shtml

If you don't have a current antivirus program, you can download a free antivirus by visiting any of the following links

Grisoft AVG
http://www.pchell.com/linkto/avg.shtml

Avast
http://www.pchell.com/linkto/avast.shtml

AntiVir
http://www.pchell.com/linkto/antivir.shtml

All three of the free antivirus programs are excellent alternatives to the more popular commercial programs. They are free for personal use, and have paid versions for business and commercial use.

Be sure to check your antivirus **once a month** to make sure its properly updating.

Anti-Spyware Updates

Spyware and Adware not only can cause frustration because of pop-up advertisements and sluggish performance, but they can also install backdoor holes for spam, phishing schemes, and identity thieves. Running anti-spyware scans and keeping the signatures of the programs up-to-date is also an important step in securing your computer.

Although you can purchase any number of programs to remove spyware and adware, in most cases the free anti-spyware software does an adequate if not better job of removing these pests than paid versions. It's also important to realize that each antispyware program will find different items on your computer so it's a good idea to run a couple different programs to thoroughly clean your system of these pests. I highly recommend the following programs to remove spyware and adware.

Ad-Aware SE 1.06 by Lavasoft
http://www.pchell.com/linkto/adaware.shtml

One of the first and still one of the best removal programs for adware, you can choose between a paid and a free version.

Spybot Search and Destroy 1.4
http://www.pchell.com/linkto/spybot.shtml

Another pioneer in the field of adware and spyware removal and always free.

Microsoft Defender
http://www.pchell.com/linkto/msdefender.shtml

Microsoft purchased a company called Giant Software and morphed their anti-spyware program into what is now known as Windows Defender. With realtime protection and monitoring, this program helps to prevent spyware and adware from ever getting on your system

Keeping your computer up-to-date is the easiest way to protect your computer from viruses, hackers, and other online issues. There are many programs to do this, and everyone has their personal favorite. The key is actually having these programs installed, up-to-date, and being used on a regular basis.

Home Networking

When you are connected to the Internet, you are assigned a unique IP address. This IP address allows other computers on the Internet to find you properly. This IP address is called a public IP, it's sort of like a telephone number. The IP address is made up of 4 sets of numbers from 0 to 255 separated by periods (0-255.0-255.0-255.0-255), this creates a total of over 4,228,250,625 possible addresses. Although not all of them are available for use.

What happens if there are more than 4.2 billion computers that want to access the Internet, that's where private IP addresses are used. Three groups of IP address have been set aside for private networks, they are:

10.0.0.1 to 10.255.255.255
172.16.0.1 to 172.31.255.254
192.168.0.1 to 192.168.255.254

Private IPs allow you to connect multiple computers to the Internet using only 1 Public IP. The task of knowing which computer on the network gets what data is handled by a device called a router. Routers sort out information that comes from the Internet on a public IP and sends that information to the correct private IP address behind the router. The process of mapping the public IP to the private IP is called Network Address Translation or NAT for short.

NAT is important in computer security because it provides a natural firewall between the outside world and your private network. Unless something is requested from your network, nothing will be able to get through. This creates a hardware firewall to protect your computer. The NAT firewall also has a second layer of security called **stateful inspection**. This means if the router receives data from a website, it looks at a list of the computers attached to it and determines which computer requested the data. If none of the computers behind the router asked for the data, the router discards it. In other words, unless a computer behind the router asked for the information, the router won't let it pass through.

Firewalls

Firewalls protect your computer from being accessed from the outside. There are two types of firewalls, hardware and software. Most broadband routers have NAT firewalls built into them to help, and many have more advanced firewall options to block intruders.

A hardware firewall blocks data from entering your computer, while a software firewall like Windows XP Firewall, ZoneAlarm, or Kerio Personal Firewall, can stop data from coming in OR going out of your computer. If your computer

becomes infected with a virus, it could send data from your computer to another computer. A properly configured software firewall would prevent this action.

When a software firewall is first installed, it has to learn which programs on the computer are allowed to gain access to the Internet, anytime the user opens a new application that needs internet access a screen will popup asking you to allow it permission to go online. These firewall rules allow the firewall to know what's good and what's bad. Unfortunately if during this time, you accidentally block a program like iexplore.exe, you will not be able to get online with Internet Explorer since iexplore.exe is the filename for Internet Explorer. You need be careful when these screens appear. Read them carefully and either accept or reject the request. If a program stops working shortly after a screen like this popped up, the chances are high that a firewall rule was set to block the application. In this case, you'll have to open the firewall and unblock it to continue.

Firewalls are important and help prevent you from threats, however an improperly configured or corrupted firewall will cause your computer not to be able to get online. So please be careful when installing and configuring software firewalls.

I recommend the following software firewalls for use:

Windows XP SP2 Firewall

An easy to turn on firewall, it silently does its job, and it doesn't slow down your computer system. However it only looks at traffic coming into your computer.

Kerio Personal Firewall
http://www.pchell.com/linkto/kerio.shtml

Kerio is an excellent two-way software firewall with a free and paid version. It even has the ability to block popup ads.

ZoneLabs ZoneAlarm
http://www.pchell.com/linkto/zonealarm.shtml

One of the most well known software firewalls and has been protecting computers since 1997. ZoneAlarm is recommended by countless experts as the best software firewall to use.

Once you have your computer up-to-date with your antivirus, spyware, firewall, and Windows updates, you should check to see how secure your connection is by visiting Steve Gibson's site Shields Up.

Shields Up
http://www.pchell.com/linkto/shieldsup.shtml

There are also a few other important security scanners on the Internet you may want to check out.

Scanit Browser Security Test
http://www.pchell.com/linkto/scanit.shtml

Windows Clipboard Test
http://www.pchell.com/linkto/clipboardtest.shtml

Email Security Test
http://www.pchell.com/linkto/emailtest.shtml

Symantec Security Test
http://www.pchell.com/linkto/symantectest.shtml

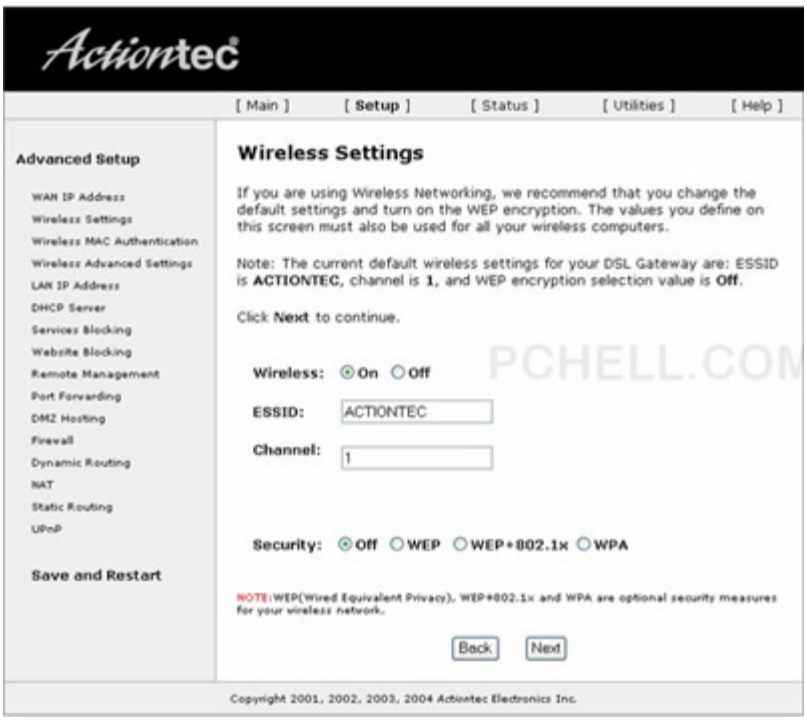
Wireless Networking and Encryption

Wireless networks open a huge hole in your home network if they are left in their default settings. These "open" networks allow anyone with a wireless network device such as a notebook computer to connect to your network, browse the computers connected, look at your shared files and even print to a shared printer if the network allows.

They work great for coffee shops, airports, and other convenience locations, but should be locked down using wireless encryption for home and business networks. To do this, you have to access your wireless routers administration interface by typing in the URL for it in your web browser. This is usually a private IP like 192.168.0.1 or 10.0.0.2. For the Actiontec modems that Qwest uses for DSL, the URL is

http://192.168.0.1

Once there, click on the Wireless settings screen and you should see something similar to the following screenshot.



You'll notice at the bottom of the screen the Security feature, generally there are two basic encryption schemes WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). WEP is harder to setup because it involves setting up a 64 or 128 bit security key.

A 64 bit security key uses 5 sets of hexadecimal numbers 0-9 and letters A-F, so a typical 64 bit key would look like the following:

01-5A-44-3C-8F

A 128 bit security key comprises of 13 sets of hexadecimal numbers, so a typical 128 bit key would look similar to:

00-43-E3-5F-93-2B-FF-6E-88-39-CB-71-DB

WPA encryption is easier to setup because it uses a passphrase to create a key. Its also a more secure encryption technique that WEP. For this reason, I would recommend using WPA encryption on your wireless network. The only thing you'll need to remember is the passphrase when you want to connect.

MAC Address Filtering is another technique used to block access, it can be used along with wireless encryption to create a very secure network. Here's how MAC filtering works. Every networked device is assigned a MAC (Media Access Control) address. This address is a unique identifier for the hardware device, sort

of like an electronic fingerprint since no two MAC addresses are ever the same. You can enable MAC filtering in your router to thoroughly secure your network.

You can find the MAC address for your network card in Windows XP by following these steps.

1) Click on the Start button, then choose RUN
2) Type **CMD** and click OK and a black DOS like box will appear
3) At the C:\> prompt type **IPCONFIG** /**ALL** and press Enter
4) Look for the Local Area Connection section and find the item called Physical Address. The hexadecimal code next to it is the MAC Address.
5) Type Exit at the prompt to return to Windows

Extra Precautions for Wireless Networks

1) Change your router's default password
2) Change or hide your wireless network SSID (Service Set Identifier)
3) Be careful with File Sharing on your Network, only share the folders you need
4) Disable DHCP and assign IP addresses manually

Privacy and Passwords

Passwords should be used to protect your computer, especially the Administrator account in Windows XP. You should also use the Limited and Guest accounts to restrict access to your computer. Employees who don't need to install programs or make system changes on the computer should be assigned a Limited account.

If you are not using the Guest account in Windows XP, turn it off to prevent access. By limiting access, you are also securing the computer if it becomes stolen or otherwise compromised.

Tip: Remember your password, don't put it on a Post-it Note and place on your monitor. Passwords only work if they are private.

Here are some more great tips for keeping your privacy.

1) If you are using a password manager on your computer like **Roboform** to remember website logins, be sure to use a Master password to secure the software.

   http://www.pchell.com/linkto/roboform.shtml

2) Use a program like **CCleaner** to clear cache, internet history, and most recently used lists from programs.

   http://www.pchell.com/linkto/ccleaner.shtml

3) Password protect your email program

4) Use a file shredder program like UltraWipe to delete sensitive data permanently.

   http://www.pchell.com/linkto/ultrawipe.shtml

5) Use a file protection program to hide files and folders from prying eyes. An excellent utility to do this is called Hide Folder and it can be freely downloaded from

   http://www.pchell.com/linkto/freehidefolder.shtml

6) Privatize your files. If you have multiple administrator accounts on your Windows XP machine, you can Share a folder and make the folder private. This will prevent anyone except that user from accessing the data stored there.

7) Use Data Encryption to encrypt sensitive files. If your computer is stolen, the intruders wont be able to get to your files unless they have the correct passwords. Unfortunately file encryption in Windows XP is rather extensive, for this reason if you would like to know more about how to encrypt your data and recover it, please read the following excellent tutorial on the subject.

   http://www.pchell.com/linkto/dataencryption.shtml

8) Protect yourself from phishing scams by installing the Netcraft Anti-Phishing toolbar. The toolbar will assign a risk rating to each site you visit, so you can protect yourself from identity theft and online scams. The Netcraft toolbar can be downloaded from:

   http://www.pchell.com/linkto/netcraft.shtml

Data Backups

Using External Drives and USB "Thumb" Drives

Backing up your vital data from a computer is an absolute must to protect from hard drive crash, virus attack, and other destruction. With the addition of external USB drives and small thumb drives, there is no reason NOT to backup your data.

You can use free programs like Microsoft Synctoy or Karen's Replicator to backup your data on a daily basis, or use program like Symantec's Ghost or Acronis True Image to create an image of your computer's hard drive on CD or DVD.

Microsoft Synctoy
http://www.pchell.com/support/synctoy.shtml

Karen's Replicator
http://www.pchell.com/linkto/karenware.shtml

Symantec Ghost
http://www.pchell.com/linkto/ghost.shtml

Acronis True Image
http://www.pchell.com/linkto/trueimage.shtml

Offsite storage

You should also store backups of your data and hard drive off site so in case of fire or other destruction, you can restore your data and get back to business. This can be done simply by taking a copy of your backup CDs, DVDs, or USB drive to an alternate location or you can opt for an online backup solution. Two of the more popular online solutions are

Mozy
http://www.pchell.com/linkto/mozy.shtml

XDrive
http://www.pchell.com/linkto/xdrive.shtml

Both are very cost effective and secure ways to store your data online, although I would not recommend storing your tax records there simply because its online. I would recommend taking backups of your CDs home or to another location and putting them in a safe and secured environment offsite.

Conclusion

I hope these tips will help you in securing your computer and network and keeping it clean of viruses, spyware, and other problems. If you are still having problems with your computer, I would suggest reading through more of the articles on PC Hell for solutions.

If you are interested in a more thorough E-book on Internet Security I suggest you pick up a copy of **The Hackers Nightmare**, an excellent and extensive (over 400 pages) look at personal computer security and what the average person can do to make their computer safe.

You can read more about The Hacker's Nightmare by visiting the following link:

http://www.pchell.com/linkto/hackersnightmare.shtml

Thank you for your time.

Mark Hasting
PCHell.com