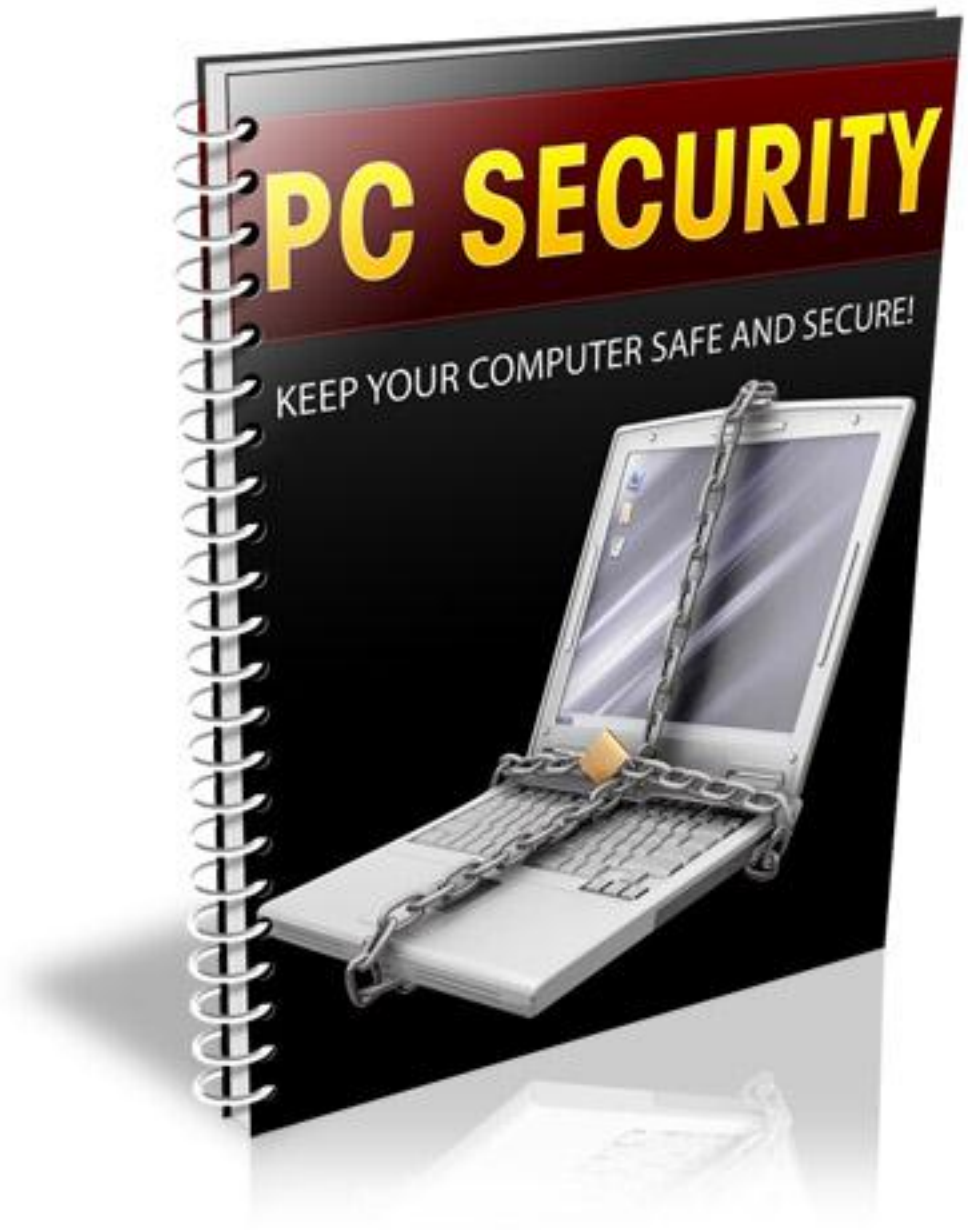
PC SECURITY
KEEP YOUR COMPUTER SAFE AND SECURE!

Table of Contents

Protecting Your Personal Computer

Whether you use your personal computer for work or personal reasons, security and protection against malicious Trojans and viruses is incredibly important in ensuring that your computer not only performs as its best, but that your personal information is safe from prying eyes and hackers.

Identify theft affects thousands of people each year, and even if you don't feel that you have any identifying information or sensitive data on your computer you're probably wrong. If you've ever entered your credit card information into a website order form or logged into your personal banking from your computer, you're at risk.

The information stored on your computer can sometimes be accessed by anyone who wants to and might take just a little time – this really amounts to no work at all for someone who knows what they're doing.

Hackers find little "doors" that you leave "open" and get inside your computer to find your personal and private information, then send it somewhere so they can pick it up safely. You just have to know how to plug the leaks in your computer and you should be fine.

Your Operating System

No matter which system you use, there are probably updates for it already unless you've managed to check in the past week. That's because there's usually a download available every week that will provide updates for various drivers and other critical components in your Operating System.

If you have just bought your computer from a store, then you can pretty much bet it's already at risk. Think about it – your computer was sitting in a box in a store and probably has been for the past few weeks, if not months. There's no way it would have been updated.

So the first thing you should do when hooking up your new computer and getting on the internet is to verify that the software is up to date. I'm only going to single out the two main vendors for paid, private sector software: Microsoft and Apple.

The others are more for the hobbyists, enthusiasts, or users of experimental software but can be used people who want to save a bunch of money on commercial software because the alternatives are mostly free. While that may sound like a good deal, you probably wouldn't be able to use any of the software you may be using right now.

Windows

For as long as it actually matters, Microsoft has provided updates by the internet which can be accessed by doing directly to windowsupdate.com, which will redirect you to the appropriate page for your Windows version. Alternatively, you can click your Start button or Start Orb (usually found at the bottom left of your screen), and then click “All Programs”, then click “Control Panel”. Windows Update is listed near the end.

An extension, so to speak, for Windows Update is Microsoft Update. Whereas Windows Update will only update Windows, Microsoft Update will update all other Microsoft software such as Office.

OSX

On a computer running the Panther version of OSX or later, you can click your Apple menu, and choose “Software Update”. If you’re using something earlier than Panther, you have to choose “System Preferences” from the Apple menu, and then “Software Update” from the “View” menu in the Preferences dialog.

Firewalls

A firewall is software or hardware that controls your internet traffic, making sure to keep all the bad stuff away from your internet experience. Most people may have heard about software firewalls, and if you have a home network then you've already seen a hardware firewall in the form of your router/gateway to the internet.

In order to communicate to other computers on the internet, you have to "open a connection" to them. But, usually only one kind of communication goes through the open connection, or the networks expect certain communication to come through the same connection all the time.

You can think of the connections as phone numbers and the communications as a caller. You wouldn't expect someone to contact the library when they're trying to reach the fire department.

Every single program that you use for the internet uses a particular port (open connection) for its purposes. Some can be changed more easily than others. A lot of times, a computer's default setting is to allow all communications on all basic ports. This simplifies things since under most

circumstances you wouldn't need these to be monitored or policed. But that would be in a perfect world.

The truth is you *can* accidentally install a file that will wait for a call on a port that it will open when you *accidentally* installed it. When that program gets the call it's been waiting for, *it will respond with a special message*.

What will the message be? It will probably be something along the lines of the following:

"Hi, the owner of this computer's name is Jane Smith because it's all over the computer as a registered user. While Jane was using her computer, I managed to record the number, expiration date, and CVV2 code of her credit card. Well, it's a debit card, and it's tied to her bank account, and I have that number right here, along with her login and password."

You may think that's an exaggeration but it's barely the beginning. That's a minimum amount of information you can expect from a successful financial information hack on your computer.

Unless you specifically have a need to, there is no legitimate reason you should be accepting incoming connections. Any piece of information you

need is requested by your computer from a reliable source and then is responded to by the same. The first, biggest security flaw is too many open ports; too many ways for a hacker to gain access to your system.

Sometimes it's not your fault, and you can have the situation above happen to you or even something worse: your computer can be controlled remotely. If there is a human sitting at the other end actively looking through your files then you could have other problems such as potentially embarrassing information or even personal information about your family being freely available.

The good news is, starting with Windows XP, you already have a working firewall installed on your system. The Windows Firewall technology was improved in Windows Vista and also with the latest version in Windows 7. While not the best solution for a firewall, it is better than not having one. That being said, it's not a poor choice; there are some advantages in using the Windows Firewall over a third party one.

If you're unsure whether your computer has existing firewall protection, and you're on a Windows Vista or Windows XP machine, click on "Start" and then enter into your Control Panel. Click "Security Center" and then click "Windows Firewall".

I mentioned earlier that if you used home networking that you probably already had a firewall on your network. That's usually true but it's not quite thorough enough unless you've spent a lot of money getting the equivalent of a small desktop computer.

What the router on your network can do is filter your traffic – it can block certain ports or certain communications but it doesn't really have the "intelligence" to discern what kind of traffic is passing through its network and make a judgment.

That being said, if you're having network issues and you've checked your computer, the next thing to check would be your router. It could be blocking traffic that you want or not blocking the traffic you don't.

You can find information on advanced networking and router management online simply by starting at the manufacturer's website. If you go to their support section, you will usually find firmware upgrades and manuals. All of the major manufacturers also have a community where people can post questions and get answers for their specific networking needs.

Firmware is like the operating system for the router, you should update this like you would your computer's operating system.

Anti-Virus

Viruses for computers are just as desirable as they are for people: they're not really. To continue along the same analogy, a virus can invade your computer and compromise its immune system and can spread to other computers doing the same.

Viruses can be picked up from literally anywhere – whatever site you go to could inadvertently or intentionally distribute harmful software to your computer. This is done by making you think you need to download a file, or sending you an email with an attachment that you open.

I'm only mentioning Windows here because there are hardly any OSX viruses. That's not saying there isn't OSX antivirus software available, but because of how OSX operates it's really difficult for a Mac to become infected.

If you want something that will integrate nicely with Windows, then you'll probably want to pick up Microsoft Security Essentials. Besides being free, t can be updated whenever Windows Update is scheduled to update your computer's software and security.

Other Protection

Besides just infecting your computer and slowing it down or being maliciously inclined to infect any other computers connected to it, you could pick up an infection that will search actively on your computer for information someone might find useful.

Also, protecting your computer from several different “angles” is important when there are just as many angles used by hackers to get to your sensitive information.

Anti-Spyware

Spyware behaves differently from viruses or other programs, and you’ll want to get a program that will actively search your computer and monitor its activity for potential spyware behavior.

With the latest Windows, there’s the latest version of Windows Defender; it’s a program that installs with your operating system and monitors your computer of potentially harmful software. The definitions (or criteria list) are updated regularly as new threats arise.

Anti-Malware

I could go on and on with the different types of harmful software that could get on your computer, but I'm going to let this encapsulate all of the miscellaneous attacks. There is one more line of defense you can have against adware, browser hijackers, and other exploits.

Spybot Search & Destroy (http://www.safer-networking.org) is a tiny program that can scan your computer's system files, memory, browser files, registry, and just about every other important area to see if spyware has been installed on your computer.

It comes with a couple of options, one offers real time activity scanning to see if your registry is being changed (another way to install malware or spyware) or if your system files have been maliciously patched. The other option is browser protection; it will protect your browser from being tricked into downloading harmful software.