Andrew's Safe Surfing Guide:
How to Safely Connect Your Personal Computer to the Internet

http://www.andrewpatrick.ca/SafeSurfing
Updated: July 22, 2005

Introduction

It is not safe to connect a new computer to the Internet without first installing some **security software** (personal firewall, anti-virus, anti-spyware) and a **hardware firewall** if you have a high speed connection. This guide explains how to do this for **Windows XP** (Service Pack 2) computers. The **first section** outlines what you need to do and when you need to do it. The **second section** provides details on each of the steps you need to take.

What are the Risks?

There are two main **risks** involved when connecting to the Internet: **bad traffic** directed at your computer (e.g., hackers, intruders, viruses, worms, etc.) and **bad programs** that can get installed on your computer against your wishes (e.g., viruses, trojans, spyware). This guide describes methods that are available to protect against bad traffic and bad programs. If you do not do this you are virtually **guaranteed** to have problems ranging from unwanted **advertisements** to **slow** performance to **theft of your personal information**. You must **follow all the steps** in this guide in order to gain any reasonable level of protection when surfing on the Internet.

What To Do and When To Do It

When You Connect to the Internet the First Time

1. If you have a **high-speed** connection, install a **hardware firewall**
2. If you chose to buy **commercial security software**, install it before you connect to the Internet. Otherwise, **download and install** a **personal firewall**, **anti-virus** software, and **anti-spyware** software
3. Run **Windows Update** and install all the available updates

Every Time You Use the Internet

1. **Do not use Internet Explorer** to surf the web. Internet Explorer contains features that allow good integration with other Microsoft software, but those features also increase the risk of getting bad programs, especially spyware. A good alternative is **Firefox**. Download it, use it, and keep it up-to-date.
2. Pay attention to **pop-up boxes**. Some bad programs are disguised as attractive programs that are offered to you as you surf the Internet. If in doubt, **SAY NO** to any offer appearing in a pop-up box.
3. **Do not open email attachments** you were not expecting. Some bad programs get installed when they are opened by people reading their email.
4. Be on the lookout for **email con-artists** who attempt to lure you to banking or financial sites (so called "**phishing**" attacks. These bad guys create **false bank or financial sites** (Paypal is a popular choice) and then attempt to lure you there to capture your username and password. Do not respond to email requests to login to your financial accounts and do not click on links contained in suspicious email messages.
5. Choose **good passwords** that cannot be guessed. It is OK to write your passwords down as long as the paper is kept in a secure place (e.g., in your wallet).
6. If you are using a **dial-up** connection, **unplug the computer from the phone** jack when not in use.

Every Day

1. **Reboot** your computer and check for messages and warnings during the startup.

Every Week

1. Manually update and scan for **spyware**
2. **Backup** your data files

Every Month:

1. Review recent **news** about Internet security issues and solutions
2. **Check for updates** for other software packages. For example, Microsoft Office has an update service similar to Windows Update and you should use it to check for updates and fixes.

Every Year

1. Review the **age** of your **computer**, the **operating system**, and your **application software**. Many problems are caused by having old programs with known problems. Considering upgrading or replacing your computer and/or software if they are getting too old. If you are not running the latest operating system (currently Windows XP Service Pack 2), you may be vulnerable.

Making the Connection: Dial-Up or High Speed

There are two common ways to connect to the Internet: a **dial-up** connection using a traditional modem, and a **high-speed** connection using a DSL or Cable TV service.

Traditional Dial-Up Modems

To connect these devices, simply connect the modem to a telephone jack using a standard telephone cable. To be safe, you should **unplug the telephone** cable whenever the computer is not connected to the Internet because bad programs have been known to make long distance phone calls using your telephone ("trojan dialers"), resulting in large, unexpected phone bills.

High Speed Connections

One of the advantages of high speed connections that use DSL or Cable TV services is that they are designed to be connected to the Internet all the time. This avoids the connection delays experienced with traditional dial-up modems, but it also increases the risk of bad

things happening. So, when using high-speed connections you must install a **hardware firewall** (often called a high speed router). The firewall is installed between your computer and the high-speed modem, and acts to hide and protect your computer from bad traffic coming from the Internet. High speed firewalls also allow multiple computers to connect to the Internet (and each other) at the same time. Popular hardware firewalls include:

- Linksys Cable/DSL Router
- D-Link Broadband Router
- Netgear Cable/DSL Router

Your Security Software: Purchase or Download?

You must install some **security software** before or soon after you connect to the Internet. At a minimum, you will need **anti-virus** software, **anti-spyware** software, and a **personal firewall**. You have a choice of **buying commercial software**, which tends to be more complete and easier to use, or you can **download free software**, which tends to be more basic and difficult to use. The commercial programs can be purchased at computer stores, either separately or in combination packages. Popular commercial **combination packages** include:

- Norton Internet Security: includes anti-virus, anti-spyware, personal firewall, and other features
- McAfee Internet Security: includes anti-virus, anti-spyware, personal firewall, and other features

If you choose to download free software, you should first enable the **Windows XP firewall** and then download and install the security software immediately after you connect to the Internet for the first time. Tests have shown that unprotected computers connected to the Internet can be infected with bad programs within 15 minutes, so it is important to work fast.

Personal Firewalls

You need to have a **personal firewall**. This software provides **protection from bad traffic** getting into your computer, and also protects you from any bad programs **sending your personal data back to the bad guys**. You should install a personal firewall even if you have a high speed connection with a hardware firewall because the hardware firewall may not protect you from bad programs sending data back to the bad guys.

The **Windows XP firewall** provides basic, incomplete protection. Until you get your personal firewall installed you should use it, but it should be disabled when proper personal firewall software is installed. Popular firewall software includes:

Commercial

- ZoneAlarm Pro
- Norton Personal Firewall
- McAfee Personal Firewall

Free Downloads

- ZoneAlarm (Free)
- Sygate Personal Firewall
- Kerio Personal Firewall

When you install a personal firewall, you will have to **teach it** what programs should be allowed to connect to the Internet. Most software will recognize common programs that connect to the Internet (e.g., web browsers, mail programs) but you will be asked if other software should be allowed to connect to the Internet. This training periods is usually brief and painless.

Anti-Virus Software

You must also install **anti-virus software** and configure it properly. The software should be configured to **scan all running** programs, to scan your entire computer **each night** while you sleep, and to keep itself **up-to-date**. These are standard features in all the programs. Popular anti-virus software includes:

Commercial

- McAfee VirusScan
- Norton AntiVirus

Free Downloads

- AVG Anti Virus Free

Anti-Spyware Software

Spyware refers to **bad programs** that either monitor your Internet activities to display extra **advertising**, or to **steal** your personal information. Like anti-virus software, anti-spyware software will watch for bad programs and help you remove them. Popular anti-spyware software (in free and commercial versions) include:

- Ad Aware
- Spybot Search and Destroy

(I recommend using **both** these products since they provide somewhat different forms of protection.)

Updates and Patches

When you connect to the Internet for the first time, you should connect to the **Windows Update** service immediately and install all of the available updates.

It is **very important** that you keep your Windows system up-to-date at all times. Many Internet problems occur when bad guys learn to exploit flaws in old versions of the operating system. For Windows XP, you should enable **Automatic Updates** so that fixes are downloaded and installed automatically when they are ready. Your firewall, spyware, and anti-virus programs may also support automatic updates, or you may have to check for fixes every once in a while.