05 **Internet Safety**

Protecting Your Computer from Internet Threats

Introduction

Viruses, Trojan horses, worms and spyware are all threats that can damage our computer systems. We know we need to protect our computer, but with so many antivirus programs on the market, how do we know what's best for our specific needs?

What Protection Do You Need?

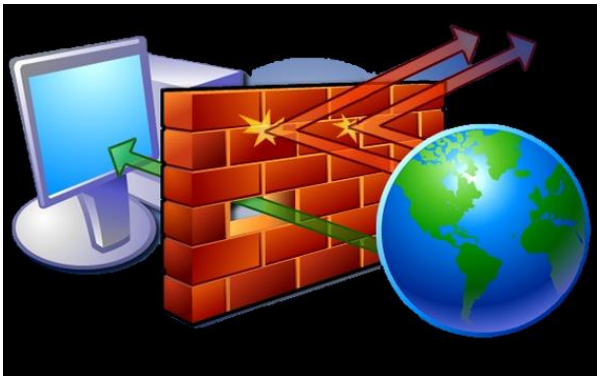
The best defense against internet threats is good **antivirus software**, or **anti-malware** as it is sometimes known. Antivirus software can protect you from infected email attachments, corrupt websites, internet worm viruses, spyware and more. There are a ton of antivirus products on the market, so figuring out what you need can be quite confusing and overwhelming. Therefore, we will outline the things you need to consider to give you a better idea of what you should be looking for in an antivirus program.

Multiple Protections

The protection you obtain should include the following three components:

- **Antivirus** - specifically protects against viruses
- **Anti-spyware** - protects against malicious software that may be gathering your information without your knowledge
- **Firewall** - screens out threats that try to reach your computer over the internet

Some security suites offer a lot of additional protections, but these are the three main components that you will need.



Security Suites

Most antivirus companies offer both a stand-alone product that only scans for viruses, and a packaged security suite that offers additional protections like firewalls, spam filtering, anti-spyware tools and more.

- **Security Suites**
  Security suites are generally easier to manage and offer a wide range of protection which can be useful if you are a beginner. However, in some cases the extra functions of a suite are not as good as the stand-alone products for that function. In addition, some suites have a tendency to slow down a computer.
- **Stand-Alone Products**
  More advanced users sometimes prefer to take a pick-and-mix approach, researching and selecting the best products for each component and building their own security system.

Things to Consider Before You Buy

Investigate Your Computer

If you are purchasing a new computer, you should ask the sales representative about what types of protections are already provided. Some computers come with **security software**, but you may need to subscribe to it after a trial period. Windows and Mac Operating Systems already have **built-in firewalls**, however they cannot help you unless you make sure they are turned on.

In addition, your **web browser has security settings** that you should review. Before you choose a new antivirus software, it would be a good idea to fully investigate what protections you already have on your computer.

Free vs. Paid Premium Software

There are a number of **free antivirus software** available that can offer an adequate amount of protection. However, many free antiviruses are scaled-back versions of paid software programs that companies hope you will eventually upgrade to. The disadvantage of free antiviruses is that they often do not include technical support and may have limited functions and updating capabilities.

It should be noted that most paid software is based on a **yearly subscription** that will need to be renewed in order to receive the latest software and updates.

Mac Users

For the most part, Mac users do not need to worry about antivirus software. At this time, the way Macs are built keeps them fairly protected against the viruses that plague PC users. Some experts would still recommend a security program that protects against malware, like Trojans or spyware that can be downloaded by the user. However, turning on the **Mac OS Firewall** and avoiding suspicious downloads may be all you need to stay safe on a Mac.

Scareware

Malicious links disguised as **security warnings** have become a popular tactic with **cybercriminals**. These official-looking notices warn you that your computer has a virus, and claim that you need to click a link or download a program to fix it. They are trying to scare you into clicking the link, but in reality the link leads to malware.

Scareware also shows up in a lot of advertisements for antivirus software, so as you begin browsing for this software make sure you are checking the address domains and going to legitimate websites for your research. Just note that any virus warnings that show up through your web browser or email are bogus.

Strategies for Using Antivirus Software

The most important thing to remember is that new viruses are being introduced on a constant basis; therefore, your antivirus software is only as good as the **latest update**. Follow these strategies to make sure you are using your antivirus software effectively:

- Make sure the **automatic update** function is turned on.
- Don't ignore your **renewal notices**. Once your subscription expires, you will stop receiving updates.
- There may be times when you need to disable your antivirus to allow certain programs, upgrades or downloads. Just make sure you don't forget to **re-enable your program** when finished.
- Your antivirus should give you specific instructions for dealing with difficult problems, but if you are having trouble with an issue, **contact technical support**.
- If you are unhappy with an antivirus program, make sure you **uninstall it** before installing a new product.

Additional Computer Safety Practices to Consider

Restart Your Computer Regularly

Some of us leave our computers on all the time, but it is a good practice to turn it off and **restart it at least once a week**. This gives your computer a chance to perform regular diagnostic checks, and fix minor issues before they become a problem.

Install Software Updates

When your operating system informs you of a **software update**, download and install it. Software updates are designed to fix security vulnerabilities and other bugs in your operating system. This will help protect your computer against some of the latest threats.

Back Up Your Computer

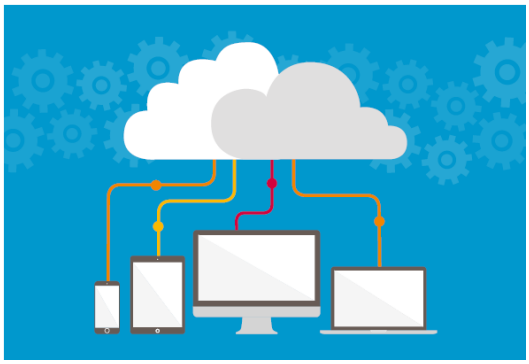
With antivirus protection, your chances of losing your files to damaging malware are greatly reduced. However, **no product offers 100% security**; therefore, it is a good idea to **back up your files on an external source**. Windows and Mac Operating Systems do come with an internal backup system, but this will not help you if your computer is **lost**, **damaged** or **stolen**. For externally backing up your files, there are two basic options for home users: external hard drives or online backup services.

External Hard Drives

You can purchase an **external hard drive** and copy the contents of your computer to it. The **initial backup could take several hours**, so you will need to select a period of time where you do not need access to your computer. Running the backup overnight usually works best. Follow-up backups should be conducted on a regular basis, but will not take as long because the drive will only need to copy your most recent files.

Western Digital, **Iomega** and **Seagate** produce popular external hard drives. Conduct some research on which product best suits your storage needs, or ask a computer sales representative for recommendations.

One drawback, compared to online backup services, is that your external hard drive can be lost, damaged or stolen just as your computer might be. Therefore, it is important to keep your drive in a **secure location** when not in use.



Online Backup Services and the Cloud

You can also back up your files online - in other words, **in the cloud**. When you store something in the cloud, it's saved to servers on the internet, instead of on your computer. That way, you can always access your files, even if your computer is lost, damaged or stolen.
One drawback to online backup services is that the **initial backup can be slow** and may even take days to upload if you have a large amount of files. However, subsequent backups should not take as long.