

# Shinn Technology Corporation

P.O. Box 173  
Fishers , IN 46038

(317) 545-3650  
<http://www.ShinnTechnology.com>



**TITLE:           Securing Your Computer Against Viruses and Hackers**

---

In response to our customers' questions, we have developed this web page to provide you with some tips on how to better protect your computer against online viruses and to better protect your computer from unauthorized accesses. There are a number of tools that are available to all Internet users that will help to secure the user's computers, and provide a much safer environment when going out on the Internet.

## **1. Use Anti-Virus Software**

One of the best tools to protect yourself when receiving content from the Internet, whether it comes from downloading web pages or emails, is anti-virus software. Anti-virus software resides in your computer's memory, and when set up correctly, can scan attachments, emails, software programs, and downloaded Internet content for viruses.

Viruses are small programs that are created by malicious individuals in order to destroy your computer's files. They are also designed to be very easily spread from one computer to another by automatically attaching themselves to outgoing data and emails from your computer. Most users are unaware that they may have a virus on their computer until it is too late, and damage to the computer or its files has already occurred.

Anti-virus software can scan your incoming and outgoing data automatically. When a virus is found, it can either isolate the virus or destroy it in order to keep it from spreading to other computers and other files. There are a large number of manufacturers of anti-virus software, including:

- Norton:                   <http://www.symantec.com/av>
- McAfee:                   <http://www.mcafee.com>
- PC-Cillin:                <http://www.trendmicro.com/au/pccillin>
- Panda ActiveScan:      <http://www.pandasoftware.com>

Some vendors provide their software on a yearly subscription basis, while others allow free online scans of your computer for viruses. Most vendors also offer regular updates of their virus definitions that you can download to your computer as well. As new viruses are discovered by the vendors, they develop downloadable patches that can keep your computer safe from new types of virus infections.

Network Associates has a free application download, called Stinger, which will detect over thirty of the most common viruses. This program does not interfere with your existing anti-virus software. Stinger is available at <http://vil.nai.com/vil/stinger>. Please make sure that your anti-virus software is fully updated and running at all times.

Many newer viruses can automatically attach themselves to your outgoing emails, thus infecting each person to whom you send email. These viruses can be non-destructive, but most viruses are designed to cause computer or files damage to each computer upon which it resides.

Shinn Technology Corporation recommends that you not only install anti-virus software, but that you configure it to do the following as well:

1. Run complete system scans on a weekly or monthly basis, which includes all of your files, drives, and memory.
2. Configure the anti-virus software to automatically activate upon each computer start-up, and allow it to run continuously while the computer is turned on.
3. Configure the anti-virus software to automatically scan all sent and received emails and attachments, and any removable media that is inserted into the computer (this includes floppy disks, Zip disks, and other removable media).
4. Check for virus definition updates from the vendor's website.

## **2. Be Wary of Email Attachments**

Most viruses spread through the use of email attachments. The vast majority of "virus senders" are online people such as your friends and family that do not use anti-virus software on their own computers. In this instance, they are not even aware they are sending you hidden malicious code inside their email attachments. Using anti-virus software on your computer will help protect you from infecting your own system.

Many attachment viruses are files that disguise themselves as other types of files. Since many Internet users send pictures to one another as attachments in an email, pictures have become an easily transported method of moving viruses around the Internet. Picture files have a number of different types of extensions, including .jpg, .gif, .bmp, and more. Most Internet users know that these types of extensions mean that the file included in an email is a picture file, and will open the file to view it.

The problem is that when you open a file to view it (otherwise known as "launching" the file), any malicious virus code that may be inside it is also opened up and activated on the computer. Also, many virus writers will disguise the true file name, by hiding the virus extension and replacing it with a graphics extension such as .gif or .jpg.

One of the ways to check the attachment for viruses before opening it is to make sure you are using anti-virus software that scans the attachments before they are opened. Another way to catch some viruses is to follow the process below:

1. Right-click the file attachment in the email you've received.
2. Left-click the **Properties** choice in the drop down menu.
3. This will show you the true name of the file that is attached.

Most viruses are files with the following extensions:

1. .vbs (Visual Basic Script)
2. .exe (executable)
3. .bat (batch file)
4. .com (Component Object Module)

All of the above extensions are types of "executable" files. By double-clicking or opening any file with an executable extension, the user will launch any internal malicious code that may be inside the attachment.

### **3. Only Open Attachments From People You Know**

This is probably the most obvious way to help eliminate viruses from your computer, but one of the most often overlooked. Always make sure that if you doubt the validity of the attachment, that you contact the sender for confirmation regarding the attachment's contents BEFORE opening it on your computer.

### **4. Install a Hardware or Software Firewall**

A firewall is a barrier that filters Internet traffic, and can prevent unauthorized access to your computer. Hardware firewalls are devices, such as routers, that provide a physical barrier between the Internet and your computer. Software firewalls are applications that you can install on your computer that monitor the incoming and outgoing traffic that your computer transmits.

### **5. Use Only Supported Operating Systems**

Each new release of the Windows and Macintosh operating systems incorporates new security features to help protect your computer while you are on the Internet.

### **6. Download the Latest Security Updates for Your Operating System**

Shinn Technology Corporation recommends that you check with the manufacturer of your operating system on a routine basis to get their latest security patches. As operating system vulnerabilities are found, both Microsoft and Apple release updates to their operating systems to fix these issues. You can find security patches for your Windows and Macintosh operating systems by visiting one of the following sites:

Microsoft's Windows operating systems: <http://windowsupdate.microsoft.com>

Apple's Macintosh operating systems: <http://www.info.apple.com>

If you are using Windows 2000 or XP, please make sure to download the "Critical Update Notification" updated in the "Recommended" section on the Windows Update site. This may already be installed on your computer, but if it appears in the "Recommended" listing, it is not currently installed.

## **7. Disable File & Print Sharing on Your Computer**

Your computer's operating system has the ability to share files and printers with other computers that may be on your own network, or on any connected network. With file sharing enabled, other computers can get access to files and programs on your system.

Shinn Technology Corporation highly recommends that the file and print sharing feature of your operating system be disabled to prevent unauthorized accesses to your system and/or printers. By disabling file and print sharing, you make it that much harder for an individual to gain control of your computer and its associated resources.

## **8. Use Microsoft features with the Windows Operating Systems**

Microsoft has a feature built into all versions of Windows (from 98 to XP) called Windows Update. This feature allows the computer user to keep their computer up to date with all patches and fixes that Microsoft has developed after initially releasing a particular version of Windows.

To assist our customers with learning how to use Microsoft's Windows Update, as well as Windows XP's built-in firewall, we are providing the link below so that you may learn more about these features:

<http://www.microsoft.com/security/protect/default.asp>

The above referenced walk-through is customizable for each operating system.