

Viruses are small programs, usually written by some bright but rather misguided folks, which are designed to either harass computer users and companies or actually destroy data or hardware.

With the increased sophistication of personal computer hardware and software there has, unfortunately, also been increased sophistication in the development of viruses affecting computer components. A healthy concern about computer viruses is smart, and there are ways to protect your computer.

When you exchange disks with someone, download a file or a program from a web site or an email attachment or click a link in an email program or instant message there is a chance that you may download a virus. Some web sites are safer than others. Downloading from a large corporation or a government site is probably safe. Your Internet provider is also a good place, as they will want to keep their computers clean of any unwanted programs. Dangerous places might be some newsgroups, unsolicited email or instant messages.

Email, without an attachment, usually cannot carry a virus since it is just text. However, there has been an instance in which a virus code was attached to a subject line in Microsoft's Outlook Express email software leading Microsoft to release a "patch" to fix this problem. In almost all cases, viruses are programmed to be sent with some attachments that may come with email. Some attachments are more susceptible than others. You should look for the three letters, known as extensions, at the end of a file before downloading it. Files that end with .exe, .com, .ini, .pif or .vbs pose a risk because a virus could attach to such a file. Files that end with .txt, .wps, .gif or .jpg are generally considered safe. Links in email messages or instant messages also may lead to a virus. Some viruses attack your email address book and send out emails with virus attachments that appear to be coming from the people listed in your address book. So you can't always trust emails that come from people you know.

### **Anti-virus software**

There are ways to minimize the chances of "catching" and spreading a virus. You must install anti-virus software that can detect and can remove most viruses. McAfee and Norton by Symantec are probably the best known. Beyond installing the anti-virus software, you must regularly update the anti-virus software. New viruses and new methods of destruction are created frequently, so you need current files to combat them. Most anti-virus programs have settings you can adjust to automatically download and install updates. Most anti-virus programs have an automatic update feature that you can enable.

### **Virus hoaxes**

There are also the ever-present "hoaxes"—information about a supposedly dangerous virus that is simply not true. You won't be on the Internet very long before a well-meaning friend or relative will send you what appears to be an official email warning against the latest and most terrifying virus. Check it out before you act on the information or pass it on.