WHY DID MY COMPUTER GET A VIRUS?

How Do Computers Get Infected?

There are many ways a computer can become infected by a virus, Trojans, spyware, or other malware. Many of them depend on your cooperation, or at least your inattention. Below are some of the most common ways that your computer can get infected, and suggestions for preventing it.

Clicking without questioning is one of the best ways to get a virus. Whether browsing the Web or installing new software, many people just "follow the prompts" given to them by a Web site or installation program. Malware distributors take advantage of this mindless behavior, prompting users to ploys that seem crude but actually work quite often. Before clicking “Next” while moving through an installation wizard, cautiously examine each page of text.

A favorite trick is to pre-check "permission" buttons in installation programs, implying that the "default" thing to do is accept whatever malware-laden toolbar or add-on program that is offered.

Scare tactics are often used to induce hasty clicks. A pop-up window may scream, "YOUR PC IS INFECTED!" and urge you to click for a cure. Often the "cure" is really the disease, which did not exist on your PC until you downloaded it by clicking.

"This Web page requires the “LetsBelieve” plugin; click here to install" is another con that malware pushers use. ("LetsBelieve" is a made-up name, not a real plug-in.)

***Clicking on email attachments is another way to activate a spyware or virus*.** Curiosity often plays a role in getting people to click on attachments from unknown senders. Sometimes an email attachment that seems to come from someone you know is actually a forgery.

There is a common misconception that only executable file attachments - those ending in .exe, .com, or .bat - are dangerous. In fact, malicious code can be hidden in files of other formats to exploit vulnerabilities in the programs that open them. Thousands of malware payloads have been delivered via Adobe PDF and Microsoft Office files. If a file can be opened with a click, it can be dangerous.

***Pirated music, movies, and software often contain hidden payloads of malware*.** If you hang out with dishonest people, it should come as no surprise when they

burn you with malware. Similarly, so-called "adult" sites are often traps for the unwary.

Downloading freeware, shareware, and other software from <u>unfamiliar</u> Web sites can bring an infection to your computer.

Sharing files via USB flash drives or CDs is another potential way to pass malware between friends.

***Not keeping your operating system, browser, and other software up to date with the latest security patches is asking for malware trouble*.** Even the best anti-virus program can't do its job if you fail to keep its signature databases current.

Turning off firewalls or anti-malware software, or never installing them at all, is inviting trouble.

To summarize: Malware comes in many forms and from many directions. Think before you click. Be wary of email attachments. Keep your software up to date. Always keep your firewall and security defenses up. Stay out of the shady parts of the Internet. Following these tips, and giving regular reminders to others who use your computer, will go a long way toward keeping you virus free.