Malicious Code Tip Sheet

According to a study done by the Pew Internet & American Life Project, 68 percent of home Internet users, or about 93 million American adults, have experienced at least one computer problem related to malicious code, adware, or spyware in the last year.

Internet users with Internet connections that are always on, such as broadband, DSL, or cable connections, are at greater risk of becoming victims of malicious code.

Malicious code is a computer program that modifies, destroys, or steals data, allows unauthorized access to your computer, and exploits or damages a system.

A computer virus is a type of malicious code that infects or attaches itself to other computer programs to perform malicious or mischievous acts, such erasing or editing files, or locking up systems.

Worms are self-propagating computer viruses embedded in a file that create copies of themselves, which in turn create even more copies as they travel through a computer network and/or across the Internet by various means, most frequently via e-mail.

Trojan horses, named after the wooden horse from Greek mythology in which Greek soldiers snuck into the city of Troy, are malicious codes that appear harmless, but when executed, can launch a virus or worm. Trojans may also be hidden inside another program, so when the innocent program is installed, the Trojan program also is installed. Once installed on the victim's computer, the other party is notified each time the victim is online. The remote attacker then has virtually unfettered access to most aspects of the victim's computer, allowing him to access personal information and files, and have control of the victim's computer.

Spyware refers to software that hides on your computer with the purpose of collecting your personal information and computer activities, and reporting them back to the one who distributed the spyware.

Adware, a close relative of spyware, is software that downloads to your computer to play, display, or download advertising material to a computer. In addition to being an annoyance, adware slows down your computer and often contains inappropriate content.

You may have malicious code, spyware, or adware on your computer if:

- pop-up ads appear when you are not connected to the Internet
- your browser home page has changed without your consent
- a new toolbar is present on your browser
- your computer takes longer than usual to complete certain tasks
- your computer is suddenly taking a long time to perform certain tasks, unexpectedly begins doing strange things, or crashes without warning

Remember to turn on your computer's firewall, keep the operating system up to date, and use up-to-date antivirus and antispyware software.

Malicious Code Tip Sheet

Malicious code can be spread through just about any computer medium, including e-mail, infected floppy disks, instant messages, file-sharing services, and pop-up ads.

i-SAFE Inc. has created this list of security tips to help you recognize, avoid, and respond appropriately to malicious code.

- **Install antivirus software, and update it regularly.**
  Antivirus software only protects your computer if it is running. Set the program to auto-start when the computer is on. Set your software to auto-update from the manufacturer's Web site. If virus protection is out of date, it cannot detect the newest viruses, worms, and Trojan horses being created daily.

- **Do not open e-mails or attachments from persons or businesses you do not know.**

- **Always scan incoming e-mail attachments before opening them.**
  Even if the e-mail is from someone you know, save attachments to your desktop, then scan with your virus-protection software before opening. Viruses can spoof the sender of the e-mail, making it appear that it was sent by someone you know.

- **Downloading files is risky business!**
  This includes freeware, screensavers, games, and any other executable program (files with extensions like .exe, .pif, or .scr). File-sharing and downloading media is very risky. Always save files to your hard drive, and virus scan before opening.

- **Beware of the floppy disk.**
  Scan all floppy disks before using. Never leave a floppy disk in the computer when not being used. If a floppy is infected with a boot sector virus and is in the floppy drive when the computer is rebooted, the infection will be transmitted to your system.

- **Keep your operating systems patched.**
  Operating system vulnerabilities are discovered almost daily. Windows updates should be set to update at least weekly to make sure your computer is protected.

- **Never click "Yes" when prompted to install or run content from a web page that you are not sure you can trust.**
  Just say "No," or if given the option, save to your hard drive, and virus scan before opening.

- **Install antispyware tools in addition to your virus-protection software.**
  Spyware is designed to hide on your computer and monitor and report your personal information and Internet activity to the remote attacker. Antispyware software that can detect and remove spyware from your computer is available.

- **Always read the user agreements, privacy statements, or other disclaimers before downloading or installing programs.**
  Programs that you install can contain spyware. By accepting the user agreement, you are giving permission to download spyware to your computer.

- **Use a firewall to further protect your computer from intrusions.**