computer BYTES
www.comp-bytes.com

The Technology Minute

What is Malware?

The term 'Malware" is commonly used as a catch-all phrase for Viruses, Spyware, Trojans, Roots Kits, and Worms. Malware is malicious programs that are designed to infiltrate or do damage to your computer (viruses, trojans, rootkits, worms), track what you do, and, in some cases, steal your personal information (spyware). Regardless of its overall purpose, malware is not something you want inhabiting your personal computer. The things you as a computer user should be concerned about is how infections typically happen, what you can do you to help prevent an infection, and, if the worst happens, how to disinfect your machine and get it back to a properly working state.

How Infections Happen

The most common ways you can get infected are through email (specifically email attachments), file sharing both through external storage devices and through the internet, installing 'free' programs, and through general use of the Web.

Spreading malware through email attachments is as common now as in the past. If the email comes from an unknown source, the attached files could be intentionally designed to infect your computer. The best course of action is to never open emails or attachments coming from senders you do not know. If the files come from a known source (friend, relative, business associate) you can still get infected. This typically happens when the sender's computer is infected and they unknowingly send you an infected file. An example of a common email that contains an infected file are the Greeting Card emails; most commonly seen around holidays. Good news, though, is that most up-to-date virus protection programs stop these before they become a problem.

Infections from file sharing can happen when an infected disk (Floppy or CD), flash drive, or external hard drive contains infected files. Once you attach the drive or inset the disk into your computer, the infection can spread. The same can happen when sharing/downloading files over the internet. Always be cautious when downloading files from the internet.

The internet is filled with 'free' shareware programs that you can download, install, and use. These include weather tracking programs, toolbars, games, screensavers, and a multitude of other 'helpful' programs. While many are perfectly fine and do not pose a hazard, others are more malicious in nature and contain spyware. The act of installing the shareware is the authorization for the 'spyware' portion to be installed. Once installed, it can track your online habits, download and send advertising pop-ups to your screen, and in worst cases download additional malware to further infect your machine and potentially compromise your personal information.

Other methods of spreading malware to your machine include infected Web sites that you may be visiting. The act of simply loading the Web page or clicking on various links on the page can infect your machine. Once installed, they can continue to contaminate your machine by downloading additional files without your knowledge or consent.

Preventing the Worst

"An ounce of prevention is worth a pound of cure" is a famous quote by Ben Franklin and it could be said he was thinking ahead to this very situation. Well, probably not exactly, but it definitely applies. You can defend yourself from malware with some simple planning:

- Install a good Antivirus and Antispyware program on your machine and make sure they are running at all times. Two very good products to use are Norton Antivirus and SuperAntiSpyware (Both available through Computer Bytes).

- Keep your computer's software patched and up-to-date. Both your operating system and protection programs must be updated on a regular basis.

- Download your updates from reputable sources. For your windows operating system, always use the Microsoft update site. For your other software, always use their specific company Web sites.

- Always think before you install any software, especially software downloaded from the Internet, and weigh the risks and the benefits. This goes for downloading/opening email attachments you receive too.

Reclaiming an Infected Machine

While following all the various prevention methods will significantly reduce the likelihood that you will be infected, the worst case can still happen. If your protection software cannot remove the malware that has inhabited your computer, then it may be necessary to seek professional help. With professional help, the malware can typically be removed and Windows can be repaired without the loss of data; but, with the most pervasive and damaging infections, a reformatting may be required. It is best to seek help sooner than later once an infection has been detected and prevention failed.

If you are not sure that your system software is up-to-date, you lack prevention software, or you feel you may be infected, stop by and see your friends at Computer Bytes. They can evaluate the current state of your computer and provide the assistance you need to sleep well at night.