U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow @arcyber

Protecting Home Networks

What are some ways I can protect my home network from malware, viruses, and hackers?

USE AND UPDATED VIRUS PROTECTION SOFTWARE

Install antivirus software on all Internet-connected computers and be sure to keep it up-to-date. Many antivirus packages support automatic updates of virus definitions.

USE A FIREWALL

Use a firewall product such as a network appliance or a personal firewall software package. Intruders constantly scan home user systems for vulnerabilities. Network firewalls, whether software or hardware-based, can provide some degree of protection, but no firewall can detect or stop all attacks, so it's not sufficient to simply install a firewall and ignore all other security measures.

DON'T OPEN UNKNOWN EMAIL ATTACHMENTS

Before opening any email attachments, be sure you know the source of the attachment. It's not enough to know that the mail originated from an address you recognize; the "Melissa" virus spread precisely because it originated from a familiar address. Malicious code can be distributed in amusing or enticing programs. If you must open an attachment before you can verify the source:

1. Be sure your virus definitions are up to date.
2. Save the file to your hard disk.
3. Scan the file using your antivirus software.
4. Open the file.

For more protection, disconnect your computer's network connection before opening the file.

Following these steps will reduce, but not eliminate, the chance that malicious code contained in the attachment might spread from your computer to others.

DON'T RUN PROGRAMS OF UNKNOWN ORIGIN

Never run a program unless you know it was authored by a person or company you trust. Don't send programs of unknown origin to your friends or coworkers simply because they are amusing as they might contain viruses.

DISABLE HIDDEN FILENAME EXTENSIONS

Windows operating systems contain an option to "Hide file extensions for known file types." The option is enabled by default, but you can disable this option to have file extensions displayed by Windows. After disabling this

option, there are still some file extensions that, by default, will remain hidden.

There is a registry value which, if set, will cause Windows to hide certain file extensions regardless of user configuration choices elsewhere in the operating system. The "NeverShowExt" registry value is used to hide the extensions for basic Windows file types. For example, the ".LNK" extension associated with Windows shortcuts remains hidden even after a user has turned off the option to hide extensions.

KEEP ALL APPLICATIONS PATCHED, INCLUDING OPERATING SYSTEMS

Vendors usually release patches for their software when a vulnerability has been discovered. Most product documentation offers a method to get updates and patches. You should be able to get updates from the vendor's website. Read the manuals or browse the vendor's website for more information.

Some applications will automatically check for available updates, and many vendors offer automatic notification of updates. The vendor's website may have information about automatic notification. If no mailing list or other automated notification is offered, you may need to check periodically for updates.

TURN OFF YOUR COMPUTER OR DISCONNECT FROM THE NETWORK WHEN NOT IN USE

Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or completely disconnected from the network.

DISABLE JAVA, JAVASCRIPT, AND ACTIVEX IF POSSIBLE

Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a website, such as a URL, an element in a form, or a database inquiry. Later, when the website responds to you, the malicious script is transferred to your browser. The most significant impact of this vulnerability can be avoided by disabling all scripting languages. Turning off these options will keep you from being vulnerable to malicious scripts. However, it will limit the interaction you can have with some websites. Many legitimate sites use scripts running within the browser to add useful features. Disabling scripting may degrade the functionality of these sites.

DISABLE SCRIPTING FEATURES IN EMAIL PROGRAMS

Because many email programs use the same code as web browsers to display HTML, vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to email as well as web pages. Therefore, in addition to disabling scripting features in web browsers (see "Disable Java, JavaScript, and ActiveX if possible" above), users should also disable these features in their email programs.

MAKE REGULAR BACKUPS OF CRITICAL DATA

Keep a copy of important files on removable media such as CDs or DVDs. Use software backup tools if available, and store the backup disks away from the computer.

MAKE A BOOT DISK

To aid in recovering from a security breach or hard disk failure, create a boot disk before you have a security event, to help recover your computer after an event has occurred.