

1. Use virus protection software

Please make use of anti-virus software on all Internet-connected computers. Be sure to keep your anti-virus software up-to-date. Many anti-virus packages support automatic updates of virus definitions. We recommend the use of these automatic updates when available.

2. Use a firewall

We strongly recommend the use of some type of firewall product, such as a network appliance or a personal firewall software package. At minimum make use of the built in windows firewall. It's not difficult to find weaknesses in the Windows Firewall, but it's safe enough for most PC users, and it's much better than using no software firewall at all.

3. Don't open unknown email attachments

You probably receive lots of mail each day, much of it unsolicited and containing unfamiliar but plausible return addresses. Some of this mail uses social engineering to tell you of a contest that you may have won or the details of a product that you might like. The sender is trying to encourage you to open the letter, read its contents, and interact with them in some way that is financially beneficial – to them. Even today, many of us open letters to learn what we've won or what fantastic deal awaits us. Since there are few consequences, there's no harm in opening them. Email-borne viruses and worms operate much the same way, except there are consequences, sometimes significant ones. Malicious email often contains a return address of someone we know and often has a provocative Subject line. This is social engineering at its finest – something we want to read from someone we know.

4. Don't run programs of unknown origin

Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- they might contain a Trojan horse program.

5. Keep all applications, including your operating system, patched

Vendors will 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 obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information.

Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered you may need to check periodically for updates.

6. Turn off your computer or disconnect from the network when not in use for long periods of time.

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 otherwise completely disconnected from the network.

7. Make regular backups of critical data

Keep a copy of important files on removable media such as recordable CD-ROM disks (CD-R or CD-RW disks), flash drives or external hard drives.. Use software backup tools if available, and store the backup disks somewhere away from the computer. Quality Networks remote backup service can assist you in obtaining secure, off-site backups.

8. Use an alternative Browser

Internet Explorer continues to be one of the most widely attacked and vulnerable pieces of software installed on computers today. We recommend using an alternative browser like Mozilla's Firefox, and keep it up to date!.