

Ten Tips for Protecting Your Computer

1. Use protection software "*anti-virus software*" and keep it up to date.

Make sure you have anti-virus software on your computer! Anti-virus software is designed to protect you and your computer against known viruses so you don't have to worry. But with new viruses emerging daily, anti-virus programs need regular updates, like annual flu shots, to recognize these new viruses. Be sure to update your anti-virus software regularly! The more often you keep it updated, say once a week, the better. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software. Stop viruses in their tracks!

2. Don't open email from unknown sources.

A simple rule of thumb is that if you don't know the person who is sending you an email, be very careful about opening the email and any file attached to it. Should you receive a suspicious email, the best thing to do is to delete the entire message, including any attachment. Even if you do know the person sending you the email, you should exercise caution if the message is strange and unexpected, particularly if it contains unusual hyperlinks. Your friend may have accidentally sent you a virus. Such was the case with the "I Love You" virus that spread to millions of people in 2001. When in doubt, delete!

3. Use hard-to-guess passwords.

Passwords will only keep outsiders out if they are difficult to guess! Don't share your password, and don't use the same password in more than one place. If someone should happen to guess one of your passwords, you don't want them to be able to use it in other places. The golden rules of passwords are:

(1) A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters and numbers, e.g., xk28LP97.

(2) Change passwords regularly, at least every 90 days.

(3) Do not give out your password to anyone!

4. Protect your computer from Internet intruders -- use "*firewalls*".

Equip your computer with a firewall! Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. They work by filtering out unauthorized or

potentially dangerous types of data from the Internet, while still allowing other (good) data to reach your computer. Firewalls also ensure that unauthorized persons can't gain access to your computer while you're connected to the Internet. You can find firewall hardware and software at most computer stores nationwide. Don't let intruders in!

5. Don't share access to your computers with strangers. Learn about file sharing risks.

Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to "share files". This ability to share files can be used to infect your computer with a virus or look at the files on your computer if you don't pay close attention. So, unless you really need this ability, make sure you turn off file-sharing. Check your operating system and your other program help files to learn how to disable file sharing. Don't share access to your computer with strangers!

6. Disconnect from the Internet when not in use.

Remember that the Digital Highway is a two-way road. You send and receive information on it. Disconnecting your computer from the Internet when you're not online lessens the chance that someone will be able to access your computer. And if you haven't kept your anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet. Be safe and disconnect!

7. Back up your computer data.

Experienced computer users know that there are two types of people: those who have already lost data and those who are going to experience the pain of losing data in the future. Back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, save copies of your data on another computer in the network. Most people make weekly backups of all their important data. And make sure you have your original software start-up disks handy and available in the event your computer system files get damaged. Be prepared!

8. Regularly download security protection update "*patches*".

Most major software companies today have to release updates and patches to their software every so often. Sometimes bugs are discovered in a program that may allow a malicious person to attack your computer. When these bugs are discovered, the software companies, or vendors, create patches that they post on their web sites. You need to be sure you download and install the patches! Check your software vendors' web sites on a regular basis for new security patches or

use the new automated patching features that some companies offer. If you don't have the time to do the work yourself, download and install a utility program to do it for you. There are available software programs that can perform this task for you. Stay informed!

9. Check your security on a regular basis. When you change your clocks for daylight-savings time, reevaluate your computer security.

The programs and operating system on your computer have many valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security at least twice a year -- do it when you change the clocks for daylight-savings! Look at the settings on applications that you have on your computer. Your browser software, for example, typically has a security setting in its preferences area. Check what settings you have and make sure you have the security level appropriate for you. Set a high bar for yourself!

10. Make sure your family members and/or your employees know what to do if your computer becomes infected.

It's important that everyone who uses a computer be aware of proper security practices. People should know how to update virus protection software, how to download security patches from software vendors and how to create a proper password. Make sure they know these tips too!