

Online opportunities are abundant these days. Thanks to the Internet, you can share vacation pictures with friends and family around the world. You can order a refrigerator at a discount. Your kids can learn directly from scientists doing rainforest research.

But online risks are also part of this interconnected world. Downloading a song or game could install a virus or spyware on your computer. Your children may stumble across inappropriate Web sites. Criminals try to trick you out of your money by promising easy rewards or by impersonating legitimate businesses.

Fortunately, you can take a few simple steps to help protect your computer, your family and your personal information online.



Protect Your Computer

These four steps will help you protect your computer from malicious and unwanted software.

1. Turn on your firewall.

A firewall creates a barrier between your computer and the Internet, managing information that comes into and leaves your computer. Most newer operating systems, including Windows XP SP2 and Windows Vista®, along with many reputable antivirus programs, include an Internet firewall.

2. Keep your software up-to-date.

It's important to install software updates as soon as they are released. You can use Automatic Updates in Windows XP SP2 and Windows Vista to automatically download and install updates. Other software programs often include regular update reminders.

3. Run up-to-date antivirus software.

Antivirus software helps protect and clean your computer from viruses and other malicious software. Update your antivirus software at least once a week to help protect against the latest threats.

4. Run up-to-date antispyware software.

Antispyware software helps protect against software that tracks your online activities and information. As with antivirus software, update antispyware software at least once a week.

Protect Your Family

You can help keep your family safe online with the following steps.

1. Talk with your kids about what they do online.

Regular open conversations are the best way to understand what your kids are doing online. Learn about the Web sites they visit, how they talk with their friends, what games they like. Ask your kids to teach you something new about the Internet.

2. Teach your kids to keep personal information private.

Advertisements and downloads can promise cool things in exchange for e-mail addresses and other personal information. Explain to kids that they should not give out this information. Review the pictures and information that your kids share online to make sure they don't reveal identifying features like school or sports team name.

3. Set clear rules for Internet use.

Agree as a family on a set of rules for using the Internet. Discuss what activities are appropriate, what information to share, and how much time to spend on the computer. Post the rules next to every computer in your home.

4. Use family safety software.

Family safety technology, such as Windows Live OneCare Family Safety or the tools in Windows Vista or Xbox Live, can help you set limits on what your kids do online. Family safety software can help keep younger children from viewing inappropriate material.

Protect Yourself

By taking the following steps, you can help protect your personal information online.

1. Follow Internet safety guidelines.

Simple guidelines can help reduce your online risk: Use strong passwords that have 8 characters and include letters, numbers, and symbols. Don't open unknown e-mail or attachments. Be careful what you download. Don't reply to spam, or unsolicited e-mail.

2. Manage your personal information carefully.

When you shop online, make sure to read a company's policies for how it will handle your personal information. Make sure they use secure online forms for purchasing. Never send your financial or credit card information by e-mail.

3. Use technology to reduce risk and alert you to potential problems.

Most online e-mail providers filter out spam; they also enable you to report spam mail that makes it past the filter. Internet Explorer 7® includes the Phishing Filter, which alerts you to potential phishing Web sites that appear to be from legitimate companies in order to steal your personal information.

4. Report any problems you encounter.

If your personal information is stolen or misused, contact your bank, the credit card company or the business in person, not online. Your local and regional government agencies also have branches that can help resolve your situation and track the criminals.

Resources

For more information on how to protect your computer, your family and your personal information online, please see these resources.

- www.microsoft.com/protect
- www.staysafe.org