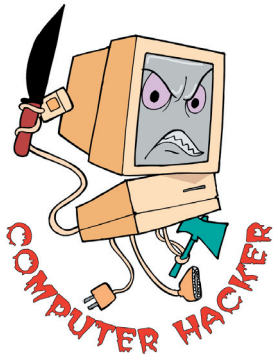
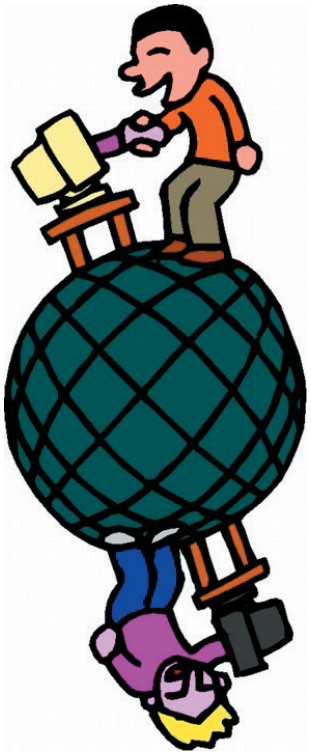
Teacher Bulletin Volume 6

Technology

Internet Safety
Internet Messaging Safety
Safer Chatting
Spam Basics
Spyware
Strong Passwords





School is in:

7 Computer Security Tips for Students

adapted from: http://www.microsoft.com/athome/security/children/backtoschool.mspx

Preparing for school used to mean filling a backpack with a handful of sharpened pencils, spiral notebooks, and a dozen textbooks. Today, computers are often on the top of that list. Study these tips to help protect the computers you use for school from viruses, hackers, spyware, and other attacks.

Things to Consider

1. Perform basic computer safety maintenance
2. Don't open files from strangers
3. Help fight spam and online scams
4. Learn how to protect yourself from spyware
5. Take precautions when you go wireless
6. Password protect your computer—and lock it
7. Back up your work (and the fun stuff, too)

1. Perform basic computer safety maintenance

Before surfing the Web, you should perform three key maintenance steps to help improve the computer's security. Visit our Protect Your PC section and follow the steps online to:

- Use an Internet firewall.
- Update your computer.
- Use up-to-date antivirus software.

2. Don't open files from strangers

E-mail and instant messaging (IM) are two quick ways to communicate with friends, classmates, and family. E-mail and IM can also spread viruses and worms if you aren't careful. Did you know that most e-mail viruses are spread by people who are fooled into opening an infected file? Don't be tricked! You should never open a file attached to an e-mail or an instant message unless you recognize the sender and you are expecting the file.

3. Help fight spam and online scams

As long as you're helping to prevent viruses and worms, you may as well learn how to help fight spam and online scams.

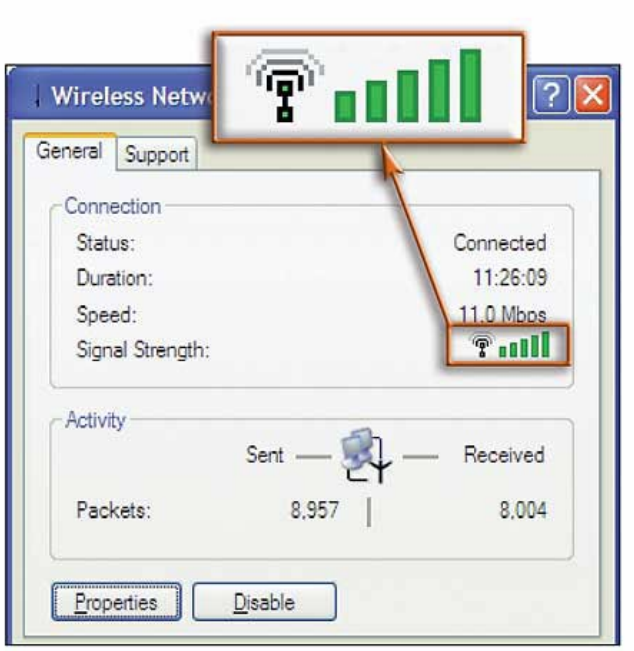
Phishing is another threat to your privacy that could lead to the theft of your credit card numbers, passwords, account information, or other personal data. To learn how to help protect your personal information from identity theft, read Help prevent identity theft from phishing scams.

4. Learn how to protect yourself from spyware
Has your Web browser been taken over by pop-up ads? Are there toolbars on your computer that you don't remember downloading? You might be the victim of spyware. Spyware is software that collects personal information from you without first letting you know what it's doing, and without asking for your permission. You might get spyware if you download: music or file-sharing programs, free games from sites you don't trust, or other software programs from a suspicious Web site.

5. Take precautions when you go wireless
Many high school and college campuses now have wireless networks. That means you can surf the Web in the library, cafeteria, or a classroom. You may have already used wireless networks in your home, in airports, coffee shops, or even public parks. These networks are convenient, but they do come with a security risk.

6. Password protect your computer—and lock it
Passwords are the first line of defense in protecting your computer from criminals, pranksters, or a careless roommate. If you don't use a password to log on to your computer, anyone can access your computer and unlock it. Be sure to build good passwords now, and be sure to lock your computer when you're not using it. To "lock" your Windows computer, hold down "Windows logo key + L." Follow the instructions on the screen to unlock your computer when you're ready to use it again.

7. Back up your work (and the fun stuff, too)
The image of students losing their term papers because they forgot to back up their work has almost become a cliché. Still, many of us don't have the time to back up. If you use Windows XP, you can let the Backup utility do the work for you.



9 Tips for Safer Instant Messaging

adapted from: http://www.microsoft.com/athome/security/online/imsafety.mspx

Instant messaging (commonly referred to as IM) is a method of online communication similar to e-mail, except that it is generally faster. Using an IM program such as Windows Messenger, AOL Instant Messenger, or Yahoo Messenger, you can type the message you want to send and the person you send it to can see it almost immediately. When your friend types a response, you see that right away as well.

Sometimes people refer to instant message conversations as "chatting," but chatting and IM are not the same. IM involves a conversation between two people, while chatting is a conversation in an Internet "chat room." Use IM more safely
Communicating by using an IM program has some of the same security and privacy risks as e-mail, but there are a few unique dangers that you should be aware of.

1. Be careful when creating a screen name. Each IM program asks you to create a screen name, which is similar to an e-mail address. Your screen name should not provide or allude to personal information. For example, use a nickname such as SoccerFan instead of BaltimoreJenny.

2. Create a barrier against unwanted instant messaging. Do not list your screen name or e-mail address in public areas (such as large Internet directories or online community profiles) or give them to strangers. Some IM services link your screen name to your e-mail address when you register. The easy availability of your e-mail address can result in your receiving an increased number of spam and phishing attacks.

3. Never provide sensitive personal information, such as your credit card numbers or passwords, in an IM conversation.

4. Only communicate with people who are on your contact or buddy lists.

5. If you decide to meet a stranger that you know only from IM communication, take appropriate safety precautions. Make sure your parents know. Do not meet that person alone, (take a friend or parent with you), and always meet and stay in a public place, such as a cafe.

6. Never open pictures, download files, or click links in messages from people you don't know. If they come from someone you do know, confirm with the sender that the message (and its attachments) is trustworthy. If it's not, close the instant message.

7. If you use a public computer, do not select the feature that allows you to log on automatically. People who use that computer after you may be able to see and use your screen name to log on.

8. Monitor and limit your children's use of IM. One way to do this is to sign up for the MSN Premium IM service that enables you approve all of your child's contacts before she can receive instant messages from those contacts. You'll also get a report of your child's online activities. See the MSN Messenger Web site for more information on the parental controls included with the service.

9. When you're not available to receive messages, be careful how you display this information to other users. For example, you might not want everyone on your contact list to know that you're "Out to Lunch." For more information, read Control Your Online Status Using Windows Messenger and Set Your Online Status.

TIPS FOR SAFER CHATTING

adapted from: http://www.microsoft.com/athome/security/online/chatsafety.mspx

You've probably heard of Internet chat rooms where people meet online to exchange messages on a certain topic. You may have even participated in a few chats yourself. Chat rooms, where chats are held, are virtual places on the Internet where people can type messages that will appear on other people's computers almost immediately. Chats are usually anonymous since the participants use nicknames to identify themselves.

Many people refer to instant message (IM) conversations as "chatting," but there is a slight difference between IM and chat. IM usually refers to a conversation between two people, whereas chat is a conversation with a group.

Microsoft has two main avenues for chatting:
- Microsoft.com Technical Chats
- MSN Chat

Get or offer help on technical issues with Microsoft's technical chats
Microsoft regularly holds technical chats where you can get help with your computer or learn about new products. These chats are open to people of all skill levels. There is no registration, Microsoft does not ask for any personal information, and when you sign in you choose an anonymous nickname.

Participate in informal chats on almost any subject with MSN Chat
With MSN Chat, you can participate in chats of a technical or non-technical nature. To protect you from spam, unwanted conversations, and advertisements, MSN Chat is now a subscription service. If you subscribe to any MSN service, you will be eligible for MSN Chat. To find out more, visit the MSN Chat page.

There are other technical and non-technical chats on the Web that can be a great place to discuss a certain topic with people all over the world. However, there are a few common sense approaches to follow when you participate in chats.

Five safety tips for chat rooms
1. Never give out your personal information in a chat room.
2. Never agree to meet a stranger in person whom you met in a chat room.
3. When you're asked to enter or sign up for a chat nickname, choose a name that doesn't give away your personal information. For example, you might use SassySue instead of DetroitSue.
4. Be wary of other chatters who ask you to meet in private chat rooms.
5. Review the terms and conditions, code of conduct, and privacy statement at the chat site before you begin chatting.

Chat rooms are a popular form of communication for kids. Unfortunately, predators know this. Therefore, chatting poses a particular threat for kids and teenagers. The five rules

above apply to children and adults. But here are five additional tips specifically for parents of kids who want to participate in chat rooms.

Five chat room safety tips for kids

1. Monitor your child's use of chat. Remember, kids can participate in chats using Web sites, chat software programs, cell phones, and even some online games.

2. Tell your child that if something in a chat room makes them feel uncomfortable, they should immediately leave the chat room and tell an adult.

3. Insist that your child never send photographs of themselves to anyone they meet in a chat room.

4. Learn the chat lingo. Kids often communicate using shorthand. For example, POS means "Parent over Shoulder."

5. Tell kids to stick to moderated chats.

IMPROVE YOUR FAMILY'S WEB SECURITY

adapted from: http://www.microsoft.com/athome/security/children/childrenonline.mspx

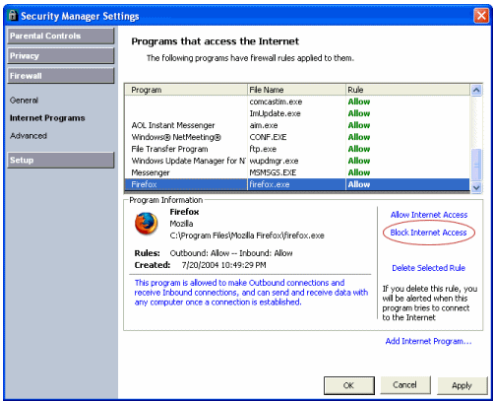
The Internet offers your children a world of new ways to expand knowledge, play games and movies and research ideas. Along with these benefits come challenges. The good news is that you can take steps to help protect your children online and teach them how to use the Web in a way that helps keep them safe. Although no technology can be a replacement for parental involvement, there are ways to use Microsoft software to help protect your children from inappropriate content.
Here are some tips for protecting your children's privacy and safety when they're using the computer.

Step 1: Decide where your child can and can't go on the Internet
Step 2: Increase your security and privacy
Step 3: Keep track of where your kids go online
Step 4: Remind kids not to talk to strangers online

Step 1: Decide where your child can and can't go on the Internet
If you don't spend a lot of time browsing the Internet, your first step should be to see what's out there for yourself. Even if you're familiar with Web sites that appeal to your interests, it's a good idea to check out some sites for kids. Pay particular interest to sites that collect personal information.

There's no shortage of safe places for kids to go on the Internet. If you don't agree with the privacy statement of a particular site, or if you don't want to give away any of your child's personal information, do a little searching and you may find a similar site that doesn't request any information at all.

Block inappropriate content



Internet Explorer 6 Content Advisor.
As a parent, you have a unique opinion on what kind of content is appropriate for your child depending on his age, maturity and your personal beliefs. The Content Advisor feature in Microsoft Internet Explorer 6 helps you limit what your children can view online. You can set limits by using your own criteria, the Platform for Internet Content Selection (PICS) rules, or the rating system of another organization you trust. These rating controls usually provide graduated levels of privacy choices that help prevent the display of inappropriate content—coarse language, nudity, sex, violence—provided that the Web sites your child visits put accurate content rating information on every page.

MSN 9 Parental Controls.
MSN 9 Internet software also includes parental controls to help you protect your child from inappropriate content. You can choose separate levels of security for each child in your house, depending on her age and maturity level. The parental controls features provides a full list of everything MSN 9 can do for you and your kids.

Xbox Parental controls.
The Microsoft Xbox® video game system includes similar parental controls that help you restrict your child's ability to play inappropriate games and watch inappropriate DVD movies.

Step 2: Increase your security and privacy
In addition to blocking inappropriate content, it's a good idea to block sites and downloads that may be a risk to your security and privacy. We recommend the following tips even if your kids never use the computer.

Create different user accounts.
Microsoft Windows® XP Home Edition allows you to create multiple user accounts for your computer. Each user can log on separately and has a unique profile with his or her own desktop and My Documents folder. As a parent you can give yourself an administrator account with full control over the computer, and give your children limited user accounts, with restricted controls. Limited users cannot change system settings or install new hardware or software, including most games, media players and chat programs.

Adjust Web browser security settings.
You can also help protect your child through your Web browser. Internet Explorer 6 helps you control your security and privacy preferences by allowing you to assign security levels to Web sites. Internet Explorer 6 also helps protect your privacy while you're on the Web by providing features that help control how Web sites track your activities. Use Security and Privacy Features in Internet Explorer 6.

Step 3: Keep track of where your kids go online
It may not always be possible to be present while your children are surfing the Web. But it is possible to check later to see where your children have spent their time online. By reviewing the History list in Internet Explorer, you can see all the places your children visited on the Web. To view your Internet History, click the History button on the browser toolbar. You can learn more about using the History list by reading Find and Return to Web Pages You've Recently Visited.

Click on a folder to expand it and view the individual pages your child visited at a certain site.

With MSN 9 parental controls you can receive a weekly e-mail report that details your child's recent online activity, including the total time spent online, Web sites he visited or tried to visit, e-mail addresses and MSN Messenger IDs of people with whom he corresponded, and files he downloaded.

Step 4: Remind kids not to talk to strangers online
Real-time chats and instant messaging can be a great way for children to discuss their interests and build friendships. But the anonymity of the Internet can also put children at risk of falling victim to imposters and predators. To help minimize your children's vulnerability, teach them to take precautions such as:
• Using only a first name or nickname to identify themselves.
• Never disclosing a phone number or address.
• Never sending photographs of themselves.
• Never agreeing to meet someone they met online without supervision.

To help protect your children from being contacted by strangers while instant messaging, configure your software to allow only approved contacts.

To block unknown contacts in Windows Messenger:
1. Click Tools.
2. Select Options.
3. Choose the Privacy tab.
4. Add people you know to the Allow list and block all other users.

An "approved list" to help parents limit their children's e-mail exchanges is also a feature of MSN 9.

Set family rules for Internet use
Although software can help you protect your family from inappropriate content on the Web, there is no substitute for teaching your children a few basic rules. Talk to your children about the risks of going online, and teach them how to handle uncomfortable situations. And finally, set limits, and discuss them with your children. Together, you can create a fun and safer environment for your children online.

Help Keep Spam Out of Your Inbox

adapted from: http://www.microsoft.com/athome/security/email/fightspam.mspx

You have three powerful tools at hand to help stem the tide of spam:

Use technology to help block junk e-mail
Be careful about sharing your e-mail or instant message address
Improve your computer's security

Use technology to help block junk e-mail

Recent research estimates that 80 percent or more of all e-mail sent these days is spam. An astonishing figure, yet you may see only a tiny portion of that deluge.

Many Internet service providers (ISP) and e-mail programs provide junk e-mail filters that can serve as the first line of defense against spam. For example, MSN Hotmail uses patented Microsoft SmartScreen Technology and other tools to keep more than 3.2 billion (yes, billion) messages from reaching its customers' e-mail accounts every day.

You, too, can take advantage of technology to help you deal with the spam that evades these filters.

Get spam filters to suit you

- Microsoft Outlook, MSN Hotmail, and Entourage (for the Mac) have strong natural defenses against junk e-mail. They also let you take matters into your own hands. Find out how to step up your defense against spam using Outlook, MSN Hotmail, and Entourage.

Tip: Create a (virtually) spam-free MSN Hotmail account. Although the Microsoft SmartScreen junk e-mail filters are very clever, some spam may still get through. If you want to reduce spam even further (particularly to protect your children), find out how to set up an account with MSN Hotmail that will be about as impervious to unsolicited e-mail as is possible.

- If you're using an e-mail program (such as Outlook Express) that's not listed above, check out Windows Marketplace to learn more about many of the anti-spam software packages that are available.

- Make sure your spam filters work the way you want. If your spam filter is set at a very restrictive setting that weeds out as many suspect messages as possible, it might be sending legitimate e-mail to the electronic dump. Check your junk e-mail box regularly to make sure that every message going there is truly junk, or loosen the restrictions.

Block unwanted instant messages (IM)

In addition to a healthy dose of caution, your best defense against IM spam (or spim as it's becoming known) is to block unwanted messages. If you're using MSN Messenger or Windows Messenger, see How you can help reduce instant message spam.

Block images
Just as a lighthouse beacon beams a message with light, pictures in e-mail messages—also called "Web beacons"—can be adapted to secretly send a message back to the sender. Spammers rely on information returned by these images to locate active e-mail addresses. Images can also contain harmful code embedded inside them and can be used to deliver a spammer's message in spite of the filters.

The best defense against Web beacons is to stop pictures from downloading until you've had a chance to review the message. Both MSN Hotmail and Microsoft Outlook 2003 are preset to do this automatically for e-mail from addresses not in your address book. Outlook Express also increases its protection against Web beacons if you're using Windows XP Service Pack 2.

Keep your filters current
Spam is a cat-and-mouse game with spammers working relentlessly to outwit the filters. Do your part by keeping your junk e-mail filter up to date. To do this if you're using Outlook 2003, go to Microsoft Update, and follow the instructions on the screen.

Be careful about sharing your e-mail or instant message address

- Only share your primary e-mail address with people you know. Avoid listing your e-mail address in large Internet directories and job-posting Web sites. Don't even post it on your own Web site (unless you disguise it as described below).

- Set up an e-mail address dedicated solely to Web transactions. Consider using a free e-mail service to help keep your primary e-mail address private. When you get too much spam there, simply drop it for a new one.

- Create an e-mail name that's tough to crack. Try a combination of letters, numbers, and other characters—Don2Funk9@example.com or J0e_Y0ng@example.com (substituting zero for the letter "O"). Research shows that people with such names get less junk e-mail.

- Disguise your e-mail address when you post it to a newsgroup, chat room, bulletin board, or other public Web page—for example, SairajUdin AT example DOT com. This way, a person can interpret your address, but the automated programs that spammers use often cannot.

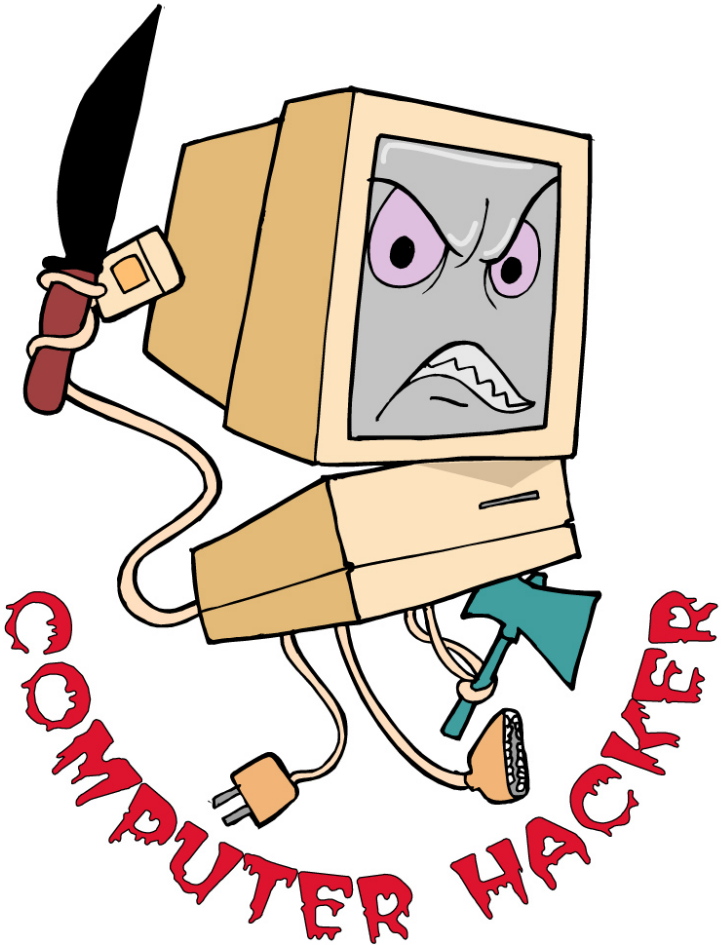
- Watch out for pre-checked boxes. When you buy things online, companies sometimes pre-select check boxes to indicate that it's fine to sell or give your e-mail address to responsible parties. Clear the check box if you don't want to be contacted.

Tip: When you sign up for Web-based services such as banking, shopping, or a newsletter,

carefully read the privacy policy before revealing your e-mail address so you don't unwittingly agree to share confidential information. The privacy policy should outline the terms and circumstances regarding if or how the site will share your information. If a Web site does not post a privacy statement, consider taking your business elsewhere.

Improve your computer's security

You can greatly reduce your risk from hackers, viruses, and worms if you use a firewall, install antivirus software (and update it routinely), and keep your Windows and Office software up to date.



Spam dos and don'ts:
What to do with spam

adapted from: http://www.microsoft.com/athome/security/email/options.mspx

Despite your best efforts, you no doubt have received e-mail and instant messages you didn't ask for. Here's what you can do about all that junk:

Ignore spam
Report fraudulent, abusive e-mail

Ignore spam

- Delete junk e-mail messages without opening them. Sometimes even opening spam can alert spammers.

- Don't reply to spam unless you're certain that the message comes from a legitimate source. This includes not responding to such messages that offer an option to "remove me from your list."

- Don't give personal information in an e-mail or instant message. It could be a trick. Most legitimate companies won't ask for personal information by e-mail. If a company you trust, such as your credit card company or bank, appears to ask for personal information, check into it further. Call the company using a number you retrieve yourself from the back of your credit card, a bill, phone book, or the like, not a number from the e-mail message. If it's a legitimate request, the company's customer service department should be able to help you.

- Think twice before opening attachments or clicking links in e-mail or instant messages, even if you know the sender. If you cannot confirm with the sender that an attachment or link is safe, delete the message. If you must open an attachment that you're less than sure about, save it to your hard disk first so that your antivirus software can check it before you open it.

- Don't buy anything or give to any charity promoted through spam. Spammers often swap or sell the e-mail addresses of those who have bought from them, so buying something through spam may result in even more spam. Plus, spammers can make their living (and a lucrative one, too) on people's purchases of their offerings. Resist the temptation to buy products through spam, and help to put spammers out of business.

  Criminals use spam to prey on people's desire to help others. If you receive an e-mail request from a charity you'd like to support, avoid donation scams by calling the organization directly to find out how to contribute.

- Don't forward chain e-mail messages. Not only do you lose control over who sees your

e-mail address, but you also may be furthering a hoax or aiding in the delivery of a virus. Plus, there are reports that spammers start chain letters expressly to gather e-mail addresses. If you don't know whether a message is a hoax or not, a site like Hoaxbusters can help you separate fact from fiction.

Note: It can be troubling to receive spam from what appears to be your own account. Your first suspicion may be that someone has hacked into your account to send you mail—or worse, send others e-mail that is allegedly from you. The truth is these fears are not likely to be real. More likely, a spammer has forged the headers (which include your e-mail address) to lend authenticity to their junk e-mail, and also potentially help the message bypass some e-mail filters.

Report fraudulent, abusive e-mail

If you receive abusive, harassing, or threatening e-mail messages or have been the target of a phishing e-mail scam, report it. If nothing else, perhaps you'll save someone else from becoming a victim.

- Report abusive, harassing, or threatening e-mail messages to your Internet Service Provider (ISP). Contact your service provider to find out what to do.

- Contact the organization directly and not through the e-mail you received. The company may also have a special e-mail address to report such abuse—for example, abuse@msn.com to report abuse of MSN.

  Tip: If you use MSN Hotmail, you can report junk e-mail before you even open it using the Junk button. If you use any Microsoft e-mail programs, such as Microsoft Outlook or MSN Hotmail, find out exactly how to report abusive or fraudulent e-mail.

- File a complaint with the U.S. Federal Trade Commission (FTC). First review the FTC tips for fighting spam, and then file your complaint.

- Forward your complaints to system administrators who can act on them with the assistance of the Network Abuse Clearinghouse.

Spyware and Other Unwanted Software : What to Do?

adapted from: http://www.microsoft.com/

Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent. You might have spyware or other unwanted software on your computer if:

- You see pop-up advertisements even when you're not on the Web.
- The page your Web browser first opens to (your home page) or your browser search settings have changed without your knowledge.
- You notice a new toolbar in your browser that you didn't want, and find it difficult to get rid of.
- Your computer takes longer than usual to complete certain tasks.
- You experience a sudden rise in computer crashes.

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. That does not mean all software which provides ads or tracks your online activities is bad. For example, you might sign up for a free music service, but "pay" for the service by agreeing to receive targeted ads. If you understand the terms and agree to them, you may have decided that it is a fair trade off. You might also agree to let the company track your online activities to determine which ads to show you.

Other kinds of unwanted software will make changes to your computer that can be annoying and can cause your computer slow down or crash. These programs have the ability to change your Web browser's home page or search page, or add additional components to your browser you don't need or want. These programs also make it very difficult for you to change your settings back to the way you originally had them. These types of unwanted programs are also often called spyware.

The key in all cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer.

There are a number of ways spyware or other unwanted software can get on your system. A common trick is to covertly install the software during the installation of other software you want such as a music or video file sharing program. Whenever you are installing something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it may appear at the end of a license agreement

or privacy statement.

Continue reading to learn the signs of a spyware infection, how to get rid of spyware, and how you can prevent spyware from getting on your computer.

How to get rid of spyware

Many kinds of unwanted software, including spyware, are designed to be difficult to remove. If you try to uninstall this software like any other program, you might find that the program reappears as soon as you restart your computer. If you're having trouble uninstalling unwanted software, you may need to download a tool to do the job for you. Several companies offer free and low-cost software that will check your computer for spyware and other unwanted software and help you remove it.

Some Internet Service Providers (ISPs) include anti-spyware software in their service packages. Check with your ISP to see if they can recommend or provide a tool. If your ISP doesn't offer a removal tool for spyware and other unwanted software, ask people you trust to recommend one, or see the links in step 1 below. Keep in mind that removing unwanted software with these tools may mean you will no longer be able to use a free program that came with the spyware.

To remove spyware

1. Download the new Microsoft Windows AntiSpyware (Beta) or another spyware removal tool. (See Spybot information below.)

2. Run the tool to scan your computer for spyware and other unwanted software.

3. Review the files discovered by the tool for spyware and other unwanted software.

4. Select suspicious files for removal by following the tool's instructions.

Spybot - Search & Destroy
http://www.microsoft.com/athome/security/spyware/spywareremove.mspx
This program can detect and remove a multitude of adware files and modules from your computer. Spybot also can clean program and Web-usage tracks from your system, which is especially useful if you share your computer. Modules chosen for removal can be sent directly to the included file shredder, ensuring complete elimination from your system. For advanced users, it allows you to fix Registry inconsistencies related to adware and to malicious program installations. The handy online-update feature ensures that Spybot always has the most current and complete listings of adware, dialers and other uninvited system residents.

Adaware

http://www.lavasoftusa.com/software/adaware/

Ad-Aware Personal provides advanced protection from known data-mining, aggressive advertising, Trojans, dialers, malware, browser hijackers, and tracking components. This software is downloadable free of charge.

How to prevent spyware

Step 1: Update your software
If you use Windows XP, one way to help prevent spyware and other unwanted software is to make sure all your software is updated. First, visit Microsoft Update to confirm that you have Automatic Updates turned on and that you've downloaded all the latest critical and security updates.

Step 2: Adjust Internet Explorer security settings
You can adjust your Internet Explorer Web browser's security settings to determine how much, or how little, information you are willing to accept from a Web site. Microsoft recommends that you set the security settings for the Internet zone to Medium or higher.

To view your current Internet Explorer security settings:

1. In Internet Explorer, click Tools and then click Internet Options.

2. Select the Security tab.
   For a step-by-step guide to adjusting your settings without blocking content from sites that you trust, see Working with Internet Explorer 6 Security Settings.
   If you're running Windows XP Service Pack 2 (SP2), and you use Internet Explorer to browse the Web, your browser security settings for the Internet zone are already set to Medium by default. Internet Explorer in Windows XP SP2 also includes a number of features to help protect against spyware and many other kinds of deceptive or unwanted software.

Tip: Don't know which version of Windows your computer is running? Find out.

Step 3: Use a firewall
While most spyware and other unwanted software come bundled with other programs or originate from unscrupulous Web sites, a small amount of spyware can actually be placed on your computer remotely by hackers. Installing a firewall or using the firewall that's built into Windows XP provides a helpful defense against these hackers. To learn more about firewalls, read "Why you should use a computer firewall" and get answers to your frequently asked questions about firewalls.

Step 4: Surf and download more safely
The best defense against spyware and other unwanted software is to not download it in the first place. Here are a few helpful tips that can protect you from downloading software you don't want:

- Only download programs from Web sites you trust. If you're not sure whether to trust a program you are considering downloading, ask a knowledgeable friend or enter the name of the program into your favorite search engine to see if anyone else has reported that it contains spyware.

- Read all security warnings, license agreements, and privacy statements associated with any software you download.

- Never click "agree" or "OK" to close a window. Instead, click the red "x" in the corner of the window or press the Alt + F4 buttons on your keyboard to close a window.

- Be wary of popular "free" music and movie file-sharing programs, and be sure you clearly understand all of the software packaged with those programs.

Strong Passwords: How to Create and Use Them

adapted from: http://www.microsoft.com/

Your passwords are the keys you use to unlock your computer and online accounts. The stronger the password, the better the security against intrusion by hackers and thieves, who could use your information to open new credit card accounts, apply for a mortgage, or even chat online disguised as you—and you wouldn't know it until it was too late. It's not hard to create strong passwords. With a small amount of effort on your part, and some tricks provided in this article, you can help improve the security of your computer.

Strong password checklist
Create a strong, memorable password in 4 steps
Keeping your passwords secret
How to access and change your passwords
What to do if your password is stolen

Strong password checklist
A good, strong password should meet all three of these criteria:

1. Over eight characters in length. Short passwords are easier to crack than long passwords.

2. Combines letters, numbers and symbols, but:

   • Not sequential or repeating combinations, such as "12345678," "222222," "abcdefg," or adjacent letters on your keyboard.

   • Not common words with letters replaced by numbers or symbols, such as "M1cr0$0ft" or "P@ssw0rd". Unfortunately, hackers know these tricks, too.

3. Easy for you to remember, but difficult for others to guess, and:

   • Not your login name, your spouse's name, or your birthday.

   • Not words found in the dictionary, in any language. Hackers use sophisticated tools that can rapidly guess passwords that are based on words in the dictionary, in a variety of languages, and using words spelled backwards.

   • Not hard-to-remember. Random combinations of letters, numbers, and symbols that must be written down to be remembered, can be misplaced, or found by others and used.

Help gauge the strength of your passwords with the password checker.

Create a strong, memorable password in 4 steps
One way to create a strong and memorable password is to come up with a "passphrase."

Here's a way to create a passphrase-based password in four easy steps:

1. Think of a sentence that you can remember, such as "My son Aiden is three years older than my daughter Anna." This will be your passphrase.

2. Take the first letter of each word of the sentence to create a new word. Using the example above, you'd get: "msaityotmda".

3. Then mix it up by using a combination of upper and lowercase letters and numbers. Example: "MsAi3yotmdA"

4. Finally, substitute some special characters that look like letters, to make this password even stronger. These tricks finish the example password to read "M$8ni3y0tmd@".

If you're worried about remembering your passphrase, start with a common phrase as your passphrase, such as "You can't teach an old dog new tricks," then inject at least one number or symbol into the password. In this case, "yctaodnt" can become "YctaODnT", or even "U(t@0DnT".

Keeping your passwords secret
Treat your passwords and passphrases seriously.

- Don't give them out to friends or family members (especially children) who could pass them on to other less trustworthy individuals.

- Don't store written passwords in your desk. If found, such a note, created for your convenience, can provide easy access to your computer for burglars.

- Never provide your password over e-mail even if a trusted company or individual requests it. Internet "phishing" scams might use fraudulent e-mail to entice you into revealing your user names and passwords so criminals can access your accounts, steal your identity, and more.

Change passwords regularly. Ideally, you should create new, strong passwords for your accounts every few months. This can help keep hackers off balance if they're monitoring a Web site that you visit frequently.

Do not use the same passwords for multiple accounts. You should create a new, strong password each time you open a new account.

Don't enable the Save Password option. If you receive a dialog box asking if you would like the computer to remember the password, choose No. This option lets anyone who uses your computer also use your pre-saved passwords on these accounts.

How to access and change your passwords for online accounts

Web sites have a variety of policies that govern how you can access your account and change your password. Look for a link (such as "your account") somewhere on the site's home page that goes to a special area of the site that allows password and account management.

Computer passwords

You can usually find information about how to create, modify, and access password-protected user accounts, as well as how to require password protection upon startup of your computer in the help files of your operating system, or online at the operating system software manufacturer's Web site. For example, if you use Microsoft Windows XP, online help can show you how to manage passwords, change passwords, and more.

What to do if your password is stolen

Be sure to monitor all your monthly financial statements, and any credit reports that are available to you. Strong, memorable passwords can help protect you against fraud and identity theft, but there are no guarantees. If someone does steal your password, notify authorities as quickly as you can. Get more information on what to do if you think your identity has been stolen or you've been similarly defrauded.