Internet Safety Tips For Elementary and Middle School Students, Educators and Families

1. Be a safe and responsible cyber citizen.

If you use the Web, e-mail or chat online, then you are a cyber citizen. Just like being with people face-to-face, use good manners when you communicate online. Obey laws and rules your parents and schools make to help you stay safe when using your computer.

Keep yourself safe. Do not give out personal information such as your address, telephone number, parents' work address/telephone number, or the name and location of your school without permission. Tell your parent right away if you come across any information in cyberspace that makes you feel uncomfortable.

2. Tell your family to protect your home computer. Use anti-virus software and a firewall. Never allow a stranger to use your home computer.

Viruses can sneak into computers from the Internet and hurt or destroy information. Using anti-virus software is necessary to guard against computer viruses. Make sure that anti-virus software is up-dated regularly. Other software on your home computer should also be updated because the manufacturer may release new security protection "patches."

Firewalls create a "wall" of protection between your home computer and the Internet by stopping anyone who might harm your computer or steal your personal information from it (bank and credit card information, for example). Your home computer may already contain firewall software. If so, check to make sure it's being used. Firewall hardware and software is also available at most computer stores.

Never allow strangers to access files on your computer. File sharing can allow others to infect your home computer with a virus, and allow others to look at the information on your computer.

3. Do not open an email from someone you do not know and trust.

If you don't know and trust someone who has sent you an email, the best thing to do is delete it quickly. Computer viruses can spread to millions of people through email, and it's never a good idea to read email from strangers.

4. Use hard-to-guess passwords and change them regularly.

Do not write passwords down on small pieces of paper taped to your computer. Passwords that are easy-to-guess are a bad choice. In other words, if your name is "Dan" don't make your password "Dan." Ask yourself a question that only you (or your parents) can answer, and use that answer for your password. Remember to change your password every three months.

5. Turn off the Internet when it's not being used, and back up personal files regularly.

The Internet is a public place where you get information and also send information. Turning off the Internet makes sure that someone else on the Internet can't enter your computer and cause harm. Backing up personal files is important to make sure your personal information is never damaged or lost.

Note to educators and parents: Please review these tips with your students/children. For more information on cyber security topics visit www.staysafeonline.info. To test your knowledge of cyber security visit www.staysafeonline.info/selftest.adp

Top Ten Cyber Security Tips
For Teens, Educators and Families

1. Be a secure and responsible cyber citizen.

If you use the Web, e-mail or chat online then you are a cyber citizen. Just like being a citizen in the face-to-face world, cyber citizens have responsibilities. Use good manners when you communicate online. Obey laws and rules your parents and schools make to help you stay safe when using your computer.

Keep yourself safe. Do not give out personal information such as your address, telephone number, parents' work address/telephone number, or the name and location of your school without permission. Tell your parent right away if you come across any information in cyberspace that makes you feel uncomfortable.

2. Use "*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!

3. Don't open email or attachments from unknown sources. Be suspicious of any unexpected email attachments even if it appears to be from someone you know.

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. If you are determined to open a file from an unknown source, save it first and run your virus checker on that file, but also understand that there is still a risk. If the mail appears to be from someone you know, still treat it with caution if it has a suspicious subject line (e.g. "Iloveyou" or "Anna Kounikova") or if it otherwise seems suspicious (e.g., it was sent in the middle of the night). Also be careful if you receive many copies of the same message from either known or unknown sources. Finally, remember that even friends and family may accidentally send you a virus or the e-mail may have been sent from their machines without their knowledge. Such was the case with the "I Love You" virus that spread to millions of people in 2001. When in doubt, delete! If you receive an email from a trusted vendor or organization, be careful of phishing, a high-tech scam used to deceive consumers into providing personal data, including credit card numbers, etc. For information about "phishing" go to the FTC document titled "How Not to Get Hooked By a Phishing Scam", http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf. The best way to make sure you're dealing with a merchant you trust, and not a fraudster, is to initiate the contact yourself. Type the merchant's address into your Internet browser instead of clicking on a link in an e-mail.

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 and in some operating systems. Don't let intruders in!

5. Regularly download security updates and "patches" for operating systems and other software.

Most major software companies today release updates and patches to close newly discovered vulnerabilities in their software. Sometimes bugs are discovered in a program that may allow a criminal hacker to attack your computer. Before most of these attacks occur, the software companies or vendors create free patches for you that they post on their web sites. You need to be sure you download and install the patches! Check your software vendors' web sites regularly for new security patches or use the automated patching features that some companies offer. Ensure that you are getting patches from the correct patch update site. Many systems have been compromised this past year by installing patches obtained from bogus update sites or emails that appear to be from a vendor that provides links to those bogus sites. 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!

6. Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long.

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, symbols and numbers, e.g., xk2&LP97.
2) Change passwords regularly, at least every 90 days.
3) Do not give out your password to anyone! For enhanced security, use some form of two-factor authentication. Two-factor authentication is a way to gain access by combining something you know (PIN) with something you have (token or smart card).

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. Many 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. 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!

9. 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. and help protect others: disconnect!

10. 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!

Note to educators and parents: Please review these tips with your students/children. For more information on cyber security topics visit www.staysafeonline.info. To test your knowledge of cyber security visit www.staysafeonline.info/selftest.adp.