

## Internet Safety

Surfing the Internet can be very informative as you are able to find information on any topic you wish. However, what many people don't think about when perusing their favorite websites is other people online trying to access your personal information. Now with ever increasing advancements in technology, "cyber-crime" has increased so much that billions of dollars annually are being lost to online hackers!

Computer hackers can find every nook and alley that you don't even know about to get into your computer. The main focus of computer protection is to make sure you have the security measures such as anti-virus, anti-spyware and anti-spam. Once you have security, make sure to keep it up-to-date. Annual check-ups and updates on your security software is a necessity to keep thieves out of your computer and away from your personal information. When it comes to online purchases, make sure to always check credit card statements and receipts so that you catch any purchases you did not make. Something to consider is creating an alternate web-based email address to use for receiving discounts or e-mail updates from websites. When shopping online, pay attention to signs the website is secure such as "https" or a lock icon in the browser status bar. Also, avoid any pop-ups or free giveaways; these are the hotspots for hackers to get into your computer.



### Tips for Internet and Computer Safety:

- In any situation, **DON'T** give out any information that could indicate your identity. This includes your full name, address, birth date, telephone number, and the school you attend or your workplace.
  - In situations that require this information, such as online shopping or registration, take great caution in providing private information and make sure your security software is up-to-date.
- Don't share your passwords or usernames for any site with other people - even friends. Only share your password with your parent or another trusted adult.
- Use caution when talking with someone you don't know online:
  - Never chat, e-mail, or text with someone who is a stranger or makes you feel uncomfortable or scared.
  - Don't agree to meet a person you met on the Internet
  - Don't send a picture of yourself to a stranger.
  - *No matter how many times you "chat" with someone online, a person you meet online is a stranger. People on the Internet may not be who they say they are.*



- Ask someone to help you block texts, e-mails, or posts from people who you do not want to communicate with.
- Be aware of the mood you are in and make sure even if you are stressed or frustrated you are cautious of what you put on the Internet.
- Tell a trusted adult if a stranger contacts you. Also, tell an adult if you read or see something on the Internet that makes you feel uncomfortable.
- Don't post pictures or videos of yourself online that could give strangers personal information (what your house or bedroom look like, where you work or go to school). Know that some games or applications with location services (like GPS) could tell strangers where you are or where you are going. Ask someone to help you check your privacy settings to be sure your location is only shared with people you know and trust.

Computers and the Internet can be a scary place where criminals can get your personal information. However, if you follow safe tips and have appropriate security on your computer, technology can be a wonderful tool. Just as you have the freedom to surf the web; other individuals have the freedom of putting information on the Internet. Everyone knows the main guidelines to have in mind when researching information for a school project or research assignment, but how can you determine if a site is credible for non-research information?

### Tips on Credible Sources:

- **Is the site for an established institution?** Look for websites associated with already trusted institutions. For example, if you are looking for a site to learn about nutritional risks of an illness or disease, you will want to gravitate toward medical websites associated with the local hospital. Also, is the website associated with established institutions? This can be determined by entering the website in the search field and taking into account other links that are found in association with the one you are accessing.
- **Stay away from commercial websites.** Besides the obvious online store websites, most often websites associated with companies or businesses are trying to sell you products. The websites normally end with “.com.” Be careful when accessing these websites and the information you receive because the company may be giving you false information to get you to buy products.
- **Watch out for political websites that put bias on their information.** Political websites and reporters put a lot of articles and information on the Internet that are full of bias. Steer clear of these websites and search for ones that present both sides of the issue equally.
- **Dates.** When was the last time the website was updated? The most up-to-date information is commonly more credible than not.

### Examples of Credible Websites on Health Information:

- Centers for Disease Control and Prevention: <http://www.cdc.gov>
- Mayo Clinic: <http://www.mayoclinic.com>
- NetWellness: <http://www.netwellness.org>

