Internet Safety and Security for Students

When you're in college, your computer and mobile device are primary tools in your educational and social life. Most students use the Internet for homework, research, social networking, online purchases, and more. The Internet is an amazing tool, but must be used safely and securely.

Keep your devices up to date.

Keep security software current: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

Automate software updates: Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.

Protect all devices that connect to the Internet: Computers, smart phones, gaming systems, and other web-enabled devices all need protection from viruses and malware.

Protect Your Personal Information.

Secure your accounts: Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site. For example Paypal offers a security key FOB that significantly strengthens security.

Consider using a Passphrase instead of a password. We all understand that passwords made of a string of random letters, numbers and special characters are very hard to remember. As a result, some folks use simple passwords which are easy to crack. A passphrase solves the problem. The following are examples of passphrases:

Mynieceis#1
HCCRocks!
Downbythelibrary9
RockFishare Cool3

Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals. If one account is compromised the others remain safe. Keep the bad guys from obtaining the "keys to the kingdom."

Own your online presence: When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit who you share information with.

Keep your eye on your technology: Never leave your laptop or other devices unattended, even for a few minutes. Do not loan your digital devices to others.

Don’t click it unless you expect it: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete it.

Get savvy about Wi-Fi hotspots: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.

Protect your $$: When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.

Log out and clear browser cache: When you use a lab or kiosk computer, be sure to log out of applications (email, distance learning, etc.) and clear the browser cache to remove your personal data.

Be Web Wise

Keep pace with new ways to stay safe online: Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.

Think before you act: Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.

Back it up: Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.