6 Back-to-School Online Privacy & Security Tips

Today's young people are likely going back to school with laptops, tablets and mobile phones. But, before parents arm kids with the latest Internet-enabled devices, it's a good idea to share some tips on IT Security & Privacy.

- **Password protect your devices: your computer, smartphone, IPad, Tablet, etc….**
  A lot of personal data is stored on these devices, including automatic logins and passwords to your email and other accounts. Choosing not to password protect these devices is the digital equivalent of leaving your home or car unlocked. A good password is a mix of letters, numbers & symbols.

- **Install a Theft-Recovery Application.**
  When a stolen computer is connected to the Internet, these utilities attempt to send network information back to a central server. This information can be used to track down which ISP is used for Internet access, and helps law enforcement track down the stolen devices. Some of these utilities can remotely destroy the data so you can protect yourself from identity theft if your device is stolen. And others will even snap a photo of the thief to collect crucial evidence that the police can use to get your laptop back. A couple of popular Theft-Recovery utilities include GadgetTrak and Apple's Find My iPhone (Free).

- **Do Not Share your passwords with your friends.** Roughly one in three online teens (30%) reports sharing one of their passwords with a friend, boyfriend, or girlfriend. Many teens consider this a matter of trust. But not all relationships end happily. What if someone you trusted with your password does something to hurt your online reputation? Or steals from you? If you have already shared your password, change it.

- **Take Control of your Social Network Privacy Settings.**
  Review your privacy settings for each service you use. Look at your profile to see what information is public. Determine who can see your posts, your pictures, and your location. Determine what 3rd party applications can access your information and if possible make changes.

- **Protect your online Reputation.**
  Assume everything you post is public and accessible to anyone, forever. You should only post what you are comfortable with others seeing. Once something is posted, such as a Facebook comment or a Tweet, and made public, it can be indexed and recorded on the public web by various third parties and search engines. As a result, it may be visible later to employers, potential employers, or college admissions officers. Once you post it, you can't take it back.

- **Keep the software on your computer updated.**
  Much vulnerability on a computer can be avoided with a few simple precautions. You need to update your operating system, your security software, and all other programs on your computer on a regular basis. One of the most important things you can do to avoid infection from malicious software is to keep all of your software updated.