Peer to Peer Computer Safety

Technology is changing the way children interact. While social interaction is now just a call, post or text away, it also puts children at higher risk of identity theft. Social interactions take place on social network sites, chat rooms, virtual worlds and blogs. Children use cell phones, game consoles, handheld gaming devices, iPods, tablets, laptops and desktops to communicate with each other. This wide array of devices and social forums is making it more and more difficult for parents to monitor their children's online activity or apply parental controls. The amount of personal information that children store on their devices and social media profiles such as pictures, videos, games and schedules makes them vulnerable to online predators and identity theft.

Parents should research and understand the privacy settings of the numerous social media websites their children use. To teach children to communicate online safely, parents should talk to them about the dangers of impostor friends; limiting what they share and keeping personal information private. Work together as a family to promote safe computer habits and follow these tips for keeping a clean machine:

- **Keep security software current:** Update antivirus and antispyware on all devices and install a firewall to protect against malware and other online threats.
- **Enable automated updates:** Many software programs will automatically connect and update to defend against known risks.
- **Watch where you click:** Links in emails, tweets, posts and online advertising are often vehicles for cybercriminals to install malicious software. If it seems suspicious (even if the source looks familiar), it's best to delete the message or mark it as junk.
- **Log out and shut down:** Don't stay permanently logged into accounts.
- **Back up data regularly:** Copy important files to a removable disc and securely wipe old data off of your computer hard drive before selling it, giving it away or throwing it out.
- **Protect yourself on public Wi-Fi networks:** Look for the "s" in "https" so make sure the site is encrypted.
- **Strong passwords: "**Long and strong" is the motto, with a mix of upper case and lower case letters, numbers and symbols. Use different passwords for all of your accounts, change them often and don't share passwords with anyone.
- **Turn on two-factor authentication:** An added layer of security that combines something you have, a physical token such as a card or code, with something you know, like a personal identification number (PIN) or password.

We lock our windows and doors when we leave the house, keep our valuables in a safe place, and even install burglar alarms; we should guard our devices with the same level of protection. Practicing good computer hygiene will strengthen the security of devices and protect the privacy of children's personal information online.

For more information, visit the Bureau of Consumer Protection or call 1-800-422-7128.

Follow the Office of Privacy Protection!