



NYS Office of Cyber Security

Monthly Security Tips NEWSLETTER

June 2012

Creating a Cyber-Secure Environment at Home

From the Desk of Thomas D. Smith, Director

Most workplaces have cyber security policies, processes, and technologies in place. You can create a more cyber-secure environment at home by implementing similar strategies. Below are some helpful tips to keep your family's computers, tablets, smartphones and other mobile devices secure.

Policies:

- Keep your computer in a central location so you can monitor your children's activities online.
- Use parental control settings to block access to inappropriate sites.
- Clearly explain the rules and expectations regarding online behavior. Discuss issues such as cyber bullying, keeping personal information private (not posting it online), and the dangers associated with talking to strangers online.

Processes:

- **Develop strong passwords.** Use a minimum of eight characters with a combination of upper and lower case letters, numbers and special characters. Passwords should be changed periodically to reduce the risk of disclosure (e.g., every 60 to 90 days). The more critical the account, such as banking or e-mail, the more frequently the password should be changed. Be sure to use different passwords for all personal accounts. Work passwords should not be re-used for personal accounts.
- **Backup your information.** Determine what needs to be saved and how frequently it needs to be saved. Know how to perform backups and how to save backups so you can restore information when needed. Test your backups to make sure they work properly.
- **Get support.** Before your computer crashes or gets infected with a computer virus, determine who is going to provide your support.
- **Erase your hard drive.** When it's time to dispose of your computer or mobile device, make sure you have the tools and a process in place to completely erase your information or physically destroy the hard drive. Properly erasing your hard drive thwarts efforts to steal your information.

Technologies:

- **Parental control software.** These programs can prevent access to inappropriate websites, limit the amount of time spent online, set a schedule for what time of day Internet use is permitted, limit access to games based on Entertainment Software Rating Board (ESRB) ratings, and monitor instant messaging conversations. Most programs are hardened to prevent them from being disabled.
- **Automatic updates.** Set your computer to automatically update the latest security patches for operating systems and application software. This will minimize risk from hackers taking advantage of software vulnerabilities or bugs.

- **Security software.** Ensure all computers have up-to-date security software on them. At a minimum, the security software should include anti-virus, anti-spyware, and a firewall. Newer products include functions to block downloads and access to and from malicious websites. Some browsers have safeguards built in that detect phishing websites and protect against downloading malicious software. For mobile devices -- like tablets and smartphones -- look for security software that allows you to locate a lost or stolen device and remotely erase it.
- **Wireless Network.** Configure your wireless network for security. Change your router's default password to a secure password to prevent someone from gaining access to it and disabling your security settings. Use a minimum of 128bit encryption to make your network more secure. Choose WPA2 encryption over older encryption, like WEP or WPA. Lastly, change the Service Set Identifier (SSID) from its default to something unique. Use a name you can remember to identify your network, but choose a name that doesn't identify you or your family. For example, don't make your SSID "Smith's home network." Check your router vendor and Internet Service Provider (ISP) for secure configuration instructions.
- To help select the right tools, check product ratings and reviews from well-known PC and consumer magazines.

Resources for More Information:

OCS Newsletter – Cyber Security and You: Top 10 Tips:

<http://www.dhSES.ny.gov/ocs/awareness-training-events/news/2011-10.cfm>

National Cyber Security Alliance – What Home Users Can Do:

<http://staysafeonline.org/cybersecurity-awareness-month/what-home-users-can-do>

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

