Multi-State Information Sharing and Analysis Center

Monthly Security Tips NEWSLETTER

May 2012 Volume 7, Issue 5

Creating a Cyber-Secure Environment at Home

From the Desk of William F. Pelgrin, Chair

Most workplaces have cyber security policies, processes, and technologies. You can create a more cyber-secure environment at home by implementing similar strategies.

Policies

At home, determine:

- A central location for your computer so you can monitor your children's activities online.
- Whether you allow access to certain sites. You may choose to use parental control settings to block access to inappropriate sites.
- Acceptable online behavior and expectations. Clearly explain the rules and expectations regarding online behavior. Include issues such as cyber bullying, keeping personal information private (not posting it online), and treating people met online as the strangers that they are.
- Your monitoring strategy. How will you assure your family complies with your "Acceptable Use Policy?" You may choose to monitor your family's online activities, and let them know their activity is being monitored.

Processes

To create a more cyber-secure enviornment at home, implement and maintain the following processes:

- Develop strong passwords and change them every 60 to 90 days. Passwords should be changed periodically to reduce the risk of disclosure. The more critical the account, such as banking or e-mail, the more frequently the password should be changed. Use a minimum of eight characters with a combination of upper and lower case letters, numbers and special characters. Have different passwords for each account for which you provide personal information. Do not re-use work passwords for any personal accounts.
- **Backup your information**. Determine what needs to be saved, how frequently it needs to be saved, how to perform the backups, how to save the backups so you can restore information when needed, and to test the 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 process to completely erase your information from it or physically destroy the hard drive. Properly erasing your hard drive thwarts efforts to steal your identity. There are many resources for the process of that disposal.

Technologies

- Use the following technologies and tools to help keep your family and computers, tablets, smartphones and other mobile devices secure. To help select the right tools, check product ratings and reviews from well-known PC and consumer magazines.
- **Parental control software**. As mentioned previously, you may choose to use 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. And 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, such as Internet Explorer's SmartScreen Filter that detects phishing websites and protects 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 the default password to a secure password for your router to prevent anyone from gaining access to it and disabling your security settings. You should also 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.

Resources for More Information:

MS-ISAC Newsletter – Cyber Security and You: Top 10 Tips:
http://msisac.cisecurity.org/newsletters/2011-10.cfm

National Cyber Security Alliance – What Home Users Can Do:
http://staysafeonline.org/cybersecurity-awareness-month/what-home-users-can-do

Brought to you by:

MS-ISAC
MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY