Creating a Cyber Secure Environment at Home

Most workplaces have cyber security policies, processes, and technology. Creating a cyber secure environment at home isn't hard — just follow your workplace's example.

Policies

Determine your Acceptable Use Policy. At work, it describes what you can and cannot do with your work computer, like surfing porn or sending political emails. At home, determine:

- **Whether your kids (and spouse) are allowed to have Internet access in their bedrooms**. You may choose to allow Internet access only in the family room so you can monitor their activities online.
- **Whether you allow access to certain sites**. You may choose to use parental controls to block access to obscene, pornographic, racist, hate, or other categories of sites.
- **How much time your family spends online**. You may choose to limit the amount of time your family spends web surfing or texting.
- **Online behavior and expectations**. Clearly explain your rules around your family's 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 about it.

Processes

A process is a collection of activities that together describe how to accomplish a goal. For your cyber secure environment, develop processes to:

- **Change your passwords**. Determine how many passwords you need, like different ones for online banking, email, and social media, how frequently to change them, and how to store your passwords securely (if you can't remember them).
- **Backup your information**. Determine what needs to be saved, how frequently to back up your information, how to perform the backups, how to save the backups so you can restore when needed, and how to test the backups to make sure they worked properly.
- **Get support**. Before your computer crashes or gets infected with a computer virus, determine who is going to provide your support. For example, have the contact information of your computer vendor, local electronics store, or neighbor's teenager.

- **Wipe your hard drive**. When it's time to dispose of your computer or phone, make sure you have the tools and process to wipe your information from it. This may mean taking a sledgehammer to your hard drive, or using a wipe program.

Technology

Use the following technologies and tools to help keep your family and computers, tablets, and smartphones secure. To help select the right tools for you, 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 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 prevent hackers from 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 lets you locate a lost or stolen device, and remotely erase it.

- **Wireless Network**. Configure your wireless network for security. Use 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 128 bit 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 that doesn't identify you. For example, don't make your SSID "Smith's home network." Check your router vendor and Internet service provider (ISP) for configuration instructions.