Cybersecurity Tips

General Tips

- Set secure passwords and don't share them with anyone. Avoid using common words, phrases, or personal information and update regularly.
- Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies.
- Verify the authenticity of requests from companies or individuals by contacting them directly. If you are being asked to provide personal information via email, you can independently contact the company directly to verify this request.
- Pay close attention to website URLs. Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.

Email

- Turn off the option to automatically download attachments.
- Save and scan any attachments before opening them. If you have to open an attachment before you can verify the source, take the following steps:
  - Be sure your anti-virus software is up to date.
  - Save the file to your computer or a disk.
  - Run an anti-virus scan using your computer's software.

Social Media, Video Games, Forums, Chat Sites and more.

- Limit the amount of personal information you post. Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your friend posts information about you, make sure the information is something that you are comfortable sharing with strangers.
- Take advantage of privacy and security settings. Use site settings to limit the information you share with the general public online.
- Be wary of strangers and cautious of potentially misleading or false information.

Mobile

- Only access the Internet over a secure network. Maintain the same vigilance you would on your computer with your mobile device.
- Be suspicious of unknown links or requests sent through email or text message. Do not click on unknown links or answer strange questions sent to your mobile device, regardless of who the sender appears to be.
- Download only trusted applications from reputable sources or marketplaces.

At Home

- Talk to your children about Internet safety. Keep your family's computer in an open area and talk to your children about what they are doing online, including who they're talking to and what websites they're visiting.
- Inform children of online risks. Discuss appropriate Internet behavior that is suitable for the child's age, knowledge, and maturity. Talk to children about the dangers and risks of the Internet so that they are able to recognize suspicious activity and secure their personal information.

At Work

- Restrict access and secure the personal information of employees and customers to prevent identity theft.
- Be suspicious of unsolicited contact from individuals seeking internal organizational data or personal information. Verify a request's authenticity by contacting the requesting entity or company directly.
- Immediately report any suspect data or security breaches to your supervisor and/or authorities.

Last Published Date: *June 29, 2012*