Cyber Security

Cybercrime is defined as the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. The following tips and guidelines can help protect yourself and your loved ones from cybercrime:

Use strong passwords

- All passwords should be the strongest you can use and remember. Strong passwords are at least 8 characters long and use combinations of uppercase and lowercase letters, numbers, and punctuation. Strong passwords contain words typically not found in a dictionary.
- Do not use the same username and password on multiple websites. Hackers can find that information and use it to access your information on many other sites.

Use security software tools

- Anti-virus software can be used to detect and remove viruses from computers. Configure your anti-virus program to perform a full scan every week, and ensure the "automatic update" settings are configured to keep the program up-to-date and working correctly.
- Install a firewall. Firewalls control the flow of information between your computer and the Internet. When information coming into or going out of your computer does not meet the "safety rules," the firewall blocks that information to prevent the transfer of any dangerous or harmful material. For tips on how to install a firewall, contact your Internet service provider.

Know who you are dealing with online

- Never run a program unless you know it is from a person or company you trust. Do not send programs of unknown origin to others.

Leadership for a Safe and Secure Indiana

- Be alert when file-sharing. File-sharing is often used to download music, games, and software through an informal network of computers, and millions of users, running the same software. Without checking the program's privacy settings, others may be able to gain access to information on your hard drive such as tax information, emails, photos, and other personal documents. You may also unwillingly download pornography or copyrighted material labeled as something else, which means you could be breaking the law.

- Do not open unsolicited or unknown email. Often in these emails the senders wants you to click on a link that will install malware on your computer. The email may have a provocative subject line, or use the return address of someone you know. If you must click on a link or open an attachment in an email, make sure your anti-virus software is up-to-date. Save the file to your hard drive, scan it with the anti-virus software, and then open the file.

Keep your web browsers and operating system up-to-date

- Patches and updates for software are released when vulnerabilities have been discovered. Some companies release updates at a consistent time each month. Keep an eye out and check for available updates to your software and operating system.

Back up important files

- Use a flash or zip drive to back up any important files or information you may have on your computer. Software backup tools are also available. If information is backed up onto removable hardware such as an external hard drive or flash drive, store it in a secure location such as a fireproof safe.

Take precautions with mobile devices

- Always keep mobile computers and devices with you when traveling until they can be locked up in a secure location.

- Protect all information with a strong password.

- Encrypt all confidential or personal information.

- Ensure important data is backed up, as it will be lost if your device is lost or stolen.

Be cautious when shopping online

- Be wary if the price for the item you'd like to buy is severely undervalued. If it is, it is likely fraudulent.
- If you are on an auction site and lose an auction and the seller contacts you later saying the original bidder fell through, the situation is likely a scam.
- Use only well-known sites, and make sure they are secured and authenticated before purchasing an item.
- If looking for a car, research car dealerships to determine if they are real and how long they have been in business.