Cyber Security Info Sheet

Cyber Threats

Virus/Malware - Attacks computing devices. Can be used to steal passwords and other data. Can be a general nuisance (browser hijacking). Spreads through websites, flash media and emails

Email (SPAM) - Unsolicited, undesired, or illegal email messages. Can contain attachments and URLs that are malicious

Malicious Websites - Websites built with the specific purpose of infecting users with malware. Can also be a legitimate site that has been compromised and injecting with malware to attack unsuspecting visitors

Social engineering - Methods used to deceive an individual into doing something that would compromise security. Could result in malware, identify theft, etc. Includes phishing (via email), smishing (via text messages) and vishing (via phonecalls)

Ransomware - Malware that will lock a computing device to prevent use or lock data to prevent access until the victim pays a ransom usually in the form of Bitcoins. The only recovery for this attack is to have solid data backups

Vulnerable Software/Hardware - Usually caused by bugs introduced by developers (usually unintentional). Some legitimate features can also introduce vulnerabilities.

Distributed Denial of Service Attack (DDoS) - Multiple computing devices are used to send bogus traffic requests to a specific target with the intention of overwhelming the target. A successful DDoS attack will prevent legitimate users from accessing the targeted system

Internet of Things (IoT) - Network connected devices that provide specific services. Examples Thermostats, Smart Locks and Cameras/Digital Recorders, etc. Many of these devices are vulnerable to attack due to manufacturers rushing products to market without first implementing proper security

Kinetic Attacks - Cyber-attacks with physical consequences. Examples: Hacking into a person's insulin pump to tamper with their dosage. Stuxnet is an example of a kinetic attack

Protect Your Library

- **Lock your desktops before walking away**
- **Change the default /factory set passwords on all devices**
- **Use updated Antivirus Software**
- **Encrypt Laptops and other mobile devices**
- **Patch operating systems (OS) and third-party software**
- **Use Intrusion Detection Systems (IDS)**
- **Use Network Access Controls (NAC)**
- **Use Firewalls**
- **Use Port Security**
- **Use Application Whitelists**
- **Pay attention to built-in OS tools like PowerShell and RDP**
- **Proper Data Backups**
- **Secure EZproxy Configuration**
- **Perform periodic vulnerability assessments**
- **Create a User Awareness Training Program**
- **Purchase Cyber Incident/Breach Insurance**
- **Become a Champion for the National Cyber Security Awareness Month (NCSAM)**

General Tips for Safe Computing

Phishing/Smishing - Do not click on links or attachments in emails or text messages even if you know the sender. Send a quick text to the person or call them to verify that they did send you the message in question

Phone (vishing) - Do not give information to unsolicited callers representing themselves as someone you have a legitimate business relationship with. Hang up and call the number from the organizations website or in the case of financial institutions, the number on the back of your debit/credit card. Common vishing schemes are someone posing as your financial institution, an IRS agent, a court clerk referencing jury duty or a fake technician offering computer support

Typos - Be careful when visiting websites. Do not type website URL directly into your browser. Instead search for the site and then click on the link from the search results and then bookmark

Passwords - Be sure to use strong passwords and be aware of your surroundings when entering passwords. Someone may be looking over your shoulder (shoulder-surfing)

Debit/Credit Cards - When using an ATM, self-checkout in a grocery store or gas pump use your body and/or other hand to cover the keypad as you enter your pin. Also when using these services grab the card reader mechanism and attempt to wiggle it. If it moves do not insert your card as this may be a skimmer device

Equifax - To help protect yourself you can take several steps. Freeze your credit with each bureau, closely monitor your financial statements, call your financial institutions and ask about adding a verbal password to your existing accounts to add a layer of security that is outside of the info taken during the breach

