Personal Cyber Security Considerations

Cyber security is a set of principles and practices designed to safeguard your computer assets and personal information against threats. SCN has developed this list to provide a strong cyber security baseline for individuals to diminish the likelihood of falling victim to a cyber-attack by implementing internet hygiene best practices.

Use complex, unique passwords that combine upper and lower-case letters, numbers, and special characters. Avoid using passwords across multiple accounts and use a reputable password manager, such as Keeper Security.

Enable two-factor authentication (2FA) for accounts containing personal, financial, or other sensitive information. Avoid text message (SMS) based 2FA.

Ensure software is up to date. This includes your operating system (Windows, MacOS, Android, iOS, etc.), other applications, and antivirus software. It is better to install patches quickly and risk a bad patch than not to patch at all.

Use a virtual private network (VPN) for all online activity. A VPN masks your location and IP address from bad actors, e-commerce sites, social media, etc. This greatly reduces the risk of external attacks.

Beware of phishing emails and malicious attachments. Always verify the sender's email address and be cautious when clicking links or opening attachments, especially from unknown sources. Enable spam filters to help detect and block malicious emails.

Enable disk encryption and a firewall from the settings of your operating system. This will provide additional online protection and protect your data.

Make regular backups of your data. Having more than one backup stored in different locations or services is best. *"Two is one, and one is none."*

Secure your devices. Enable a password, PIN, and/or biometric access for your computers and mobile devices and lock them whenever they are not in use. Enable geolocation on your devices (i.e., find my iPhone) to increase the chance of recovery if the device is lost or stolen.

Keep visitors, guests, and contractors off your network. Create a separate guest network with a different password that only allows guest users access to the internet.

Take control over the personally identifiable information (PII) available online. Limit the information you provide on public sites and social media accounts. Privacy protection services, such as DeleteMe, will actively work to remove your PII from a wide array of databases and search results.