Cyber Security Best Practices

Practicing cyber safety can go a long way toward protecting your identity and sensitive personal information. Cyber security is about education and risk reduction. Taking these steps can reduce your risks.

Think Before You Act

To avoid identify theft, avoid sharing personal information like your Social Security number or credit card number when answering an unsolicited email, phone call, text message, or instant message. Emails or phone calls that create a sense of urgency such as a problem with your bank account, taxes, or family member are likely a scam. Never divulge or enter personal information in response to an email, pop-up webpage, or any other form of communication you didn't initiate.

Understand Phishing

In a phishing scheme, the attacker poses as someone or something to trick the recipient into divulging credentials by sending email with a malicious link, or opening an attachment that infects the user's computer system with malware. Malicious links can also come from friends who have been infected too. Remember that scammers can commandeer friends' email addresses and send you messages posing as them. Turn on spam filters for your email account to help filter suspicious messages. Be sure to check to see who is sending you an email before you click on any links contained in it.

Use Strong Password Protection

Unique, strong, and complex passwords can help stop cyber criminals from accessing your information. A strong password contains at least 10 characters and includes numbers, symbols, capital and lowercase letters. Companies should ask you to change your passwords on a regular basis.

Use Two-Factor Authentication

Companies may also require two-factor authentication when you try to access sensitive information because this adds an additional layer of protection. You will be asked to take at least one extra step to log in, such as providing a temporary code that is sent to your smart phone.

Connect to Secure Wi-Fi

Wi-Fi networks should be secure, encrypted, and hidden. Public Wi-Fi networks can be risky and make your data vulnerable to being intercepted.

Enable Firewall Protection

Install a firewall for your home network to help protect data against cyber attacks. Firewalls prevent unauthorized users from accessing your websites, mail services, and other sources of information that can be accessed from the web.

Install Quality Security Software & Keep it Up-to-Date

Invest in quality antivirus and malware detection systems so that all of the computer devices are protected. You should keep your security software, web browsers, and operating systems updated with the latest protections because these are frequently revised to target and respond to new cyber threats.

Back Up Files

Utilize an external hard drive to back up data to protect against loss.

Regularly Review Your Online Accounts & Credit Reports for Changes

It's important to safeguard online accounts and monitor credit reports. A credit freeze is the most effective way for you to protect your personal credit information from cyber criminals. Essentially, it allows you to lock your credit and use a personal identification number (PIN) that only you will know.

Share with Care on Social Media

Be aware of what you share publically on social media sites like Facebook, Twitter, etc. Adjust your privacy settings to limit who can see your information. Avoid sharing your location.

Enlist Support

If you live alone or spend a lot of time by yourself, consider a trusted source to serve as a second set of eyes and ears. Adult family members and grandchildren who are computer savvy may be willing to help.