INTERNET OF THINGS

The internet is something we connect to every day—usually by logging onto our devices or computer at work.

Hackers and cybercriminals can exploit unsecured systems to invade your privacy or install ransomware.

When buying any device that's internet connected, always choose a reputable brand and vendor.

Most internet-enabled devices come equipped with a default password that you can manually change. Failing to do so can make you vulnerable.

Don't allow your wifi to automatically connect to public networks. Stay away from networks that don't require a password.

But did you know that smart TVs, gaming systems, media players—even baby monitors—can connect to the internet, too?

The internet of things is here to stay. Keep it safe by understanding how it works and what you can do to protect yourself.

Keep your home network secure and up to date. Be sure it's configured so that it doesn't send out data without your permission.

Using a Virtual Private Network, or VPN, can further protect you by hiding your IP address from hackers and encrypting your communications.

DON'T FORGET! Cybercriminals, like myself, can access your network—and the devices tied to it—by sending phishing emails that encourage you to click malicious links or download malware. These emails are typically alarmist in nature, may include misspellings and often end with an urgent call to click or download now. **Don't fall for them!**

CLICK THINKING