CLICK THINKING

Quick insights for protecting yourself and your company from online threats.

spotlight

INTERNET of THINGS

Those internet-enabled devices that make your life convenient can also make it easier for cybercriminals to target you.

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

It's easy to forget about this 'internet of things' we rely on to make life easier and enjoyable.

And because of this, it's also easy to forget that these things can leave us vulnerable.

WHAT YOU NEED TO KNOW TO PROTECT YOURSELF

- When buying any device that's internet connected, always choose a reputable brand and vendor.
- While it may be tempting to choose something less expensive, cheaper items may not have the latest security features and updates.
- Most internet-enabled devices come equipped with a default password you can manually change. Failing to do so—especially with older devices—can make it vulnerable to hackers who want access to your network.
- 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. In addition, keep your password safe and be careful about giving it out.
- Using a Virtual Private Network, or VPN, can further protect you by hiding your IP address from hackers and encrypting your communications.
- Cybercriminals 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!**