CLICK THINKING

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

spotlight

BRING YOUR OWN DEVICE (BYOD)

Using a personal device can introduce security risks to your company network and critical data if you're not careful.

Many companies allow employees to use their smartphones, laptops, tablets and other devices for work-related purposes.

This policy, called Bring Your Own Device, or BYOD, is designed to benefit employees and employers.

WHAT YOU NEED TO KNOW TO PROTECT YOURSELF

- Never leave your device unattended when working in public, even for a moment.
- Always be on the lookout for shoulder surfers—people who try to steal log-in information without your knowledge.
- In the unfortunate event your device is lost or stolen, taking preventive measures can stop the thieves from gaining access.
- Create a strong defense for your device by putting letters, numbers and special characters in your password.
- To make it even stronger, include a pass phrase—a familiar phrase of your choosing—into your password.
- Set your smart phone's auto-lock feature to engage after five minutes or less of inactivity.
- Steer clear of sites that offer you free streaming or downloads. These almost always install malware in the background.
- Be careful about the websites you visit. Some may attempt what's called a drive-by download, installing malware without your knowledge.
- When using your device for personal and work-related business, be sure to keep both worlds separate.