CLICK THINKING

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

spotlight

PUBLIC WIFI

Internet browsing is the same no matter where you log on, right? Wrong—in public, there are risks you need to consider!

When you use public wifi you join millions of people worldwide who rely on it for convenient online access.

Unfortunately, you also join a growing community of cybercriminals who use it to steal sensitive information from unsuspecting users.

WHAT YOU NEED TO KNOW TO PROTECT YOURSELF

- Savvy cybercriminals can gain access to your critical data within minutes of logging onto public wifi if you're not careful.
- Most public wifi attacks occur when cybercriminals exploit vulnerable systems to eavesdrop on your browsing activity.
- Make sure the public wifi network you're joining is the legitimate network of the establishment that's providing it. If you're not sure, ask an employee to confirm it.
- Stay away from networks that don't require a password. And don't allow your wifi to automatically connect to public networks.
- Use a VPN—it encrypts the information you transmit, so even if a cybercriminal does gain access to the network, your data is nearly impossible to decode.
- Disable file sharing and turn off your device's wireless connections when you're not using it. And log out of accounts when you're finished.
- Visit only sites with the HTTPS protocol or secure padlock icon. And never use public wifi to access sites that contain sensitive financial or personal data.
- Always be on the lookout for shoulder surfers—people who steal log-in information without your knowledge.