Public WiFi

What you should know about it:

Open, unsecured public WiFi networks can be dangerous. Criminals can set up routers to provide WiFi service in public places. Once you connect, they can intercept, capture, and divert all your communications. That means criminals can access everything from your logins and company email file attachments to the credit card information you enter on e-commerce sites.

How to safeguard against it:

- **Don't use public WiFi networks that don't require a password.**
- **Pay attention to warnings that you're connecting to a network that hasn't been secured.**
- **Use a Virtual Private Network (VPN) wherever possible,**
  and always use the company's VPN to connect remotely to company resources.
- **If you're on a public WiFi network, limit your browsing to sites that use encryption (sites with names starting with HTTPS instead of HTTP).**
- **Avoid logging into websites where there's a chance that cybercriminals could capture your identity, passwords or personal information — such as social networking sites, online banking services, or websites that store your credit card information.**
- **If relaying sensitive information, consider using your mobile device's data network instead of WiFi.**
- **Make sure your device has the most current updates and patches.**