((((THE DANGERS OF PUBLIC WIFI))))

Savvy cybercriminals can gain access to your critical data within minutes of logging onto public wifi if you're not careful.

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

Make sure the public wifi network you're joining is the establishment's legitimate network. If you're not sure, ask an employee to confirm it.

Criminals who hover nearby in an attempt to steal passwords and other sensitive information are called 'shoulder surfers.'

Most public wifi attacks occur when cybercriminals exploit vulnerable systems to eavesdrop on the transmissions between your device and the sites you're visiting. You can protect yourself, however, by taking precautions when using public wifi.

Cybercriminals often mimic public wifi networks, giving them similar names to fool unsuspecting users.

Use a VPN—it encrypts information you transmit, so even if a cybercriminal does gain access to the network, your data is nearly impossible to decode.

Cybercriminals seek sensitive information, such as passwords, log-in credentials and anything else they find useful.

Disable file sharing and turn off your device's wireless connections when not in use. Log out of accounts when you're finished accessing them.

CLICK THINKING