Wi-Fi Security

Wi-Fi hotspots in public places are convenient, but often not secure. If you connect to a Wi-Fi network and send information through websites or mobile apps, it has potential to be accessed by someone else.

Encryption is the key to keeping your personal information secure online. Encryption scrambles the information you send over the internet into a code so it's not accessible to others. When you're using wireless networks, it's best to send personal information only if it's encrypted, either by an encrypted website or a secure Wi-Fi network. An encrypted website protects only the information you send to and from that site. A secure wireless network encrypts all the information you send using that network.

The Federal Trade Commission offers these tips to protect your information when using public Wi-Fi:

- When using a hotspot, log in or send personal information only to websites you know are fully encrypted. To determine if a website is encrypted, look for **https** at the start of the web address (the "s" is for secure). Look for **https** on **every** page you visit, not just when you sign in. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Unlike websites, mobile apps don't have a visible indicator like **https**. Researchers have found that many mobile apps don't encrypt information properly, so it's a bad idea to use certain types of mobile apps on unsecured Wi-Fi. If you plan to use a mobile app to conduct sensitive transactions — like filing your taxes, shopping with a credit card, or accessing your bank account — use a secure wireless network or your phone's data network. If you must use an unsecured wireless network for transactions, use the company's mobile website rather than the company's mobile app, so you can check for the **https** at the start of the web address.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up-to-date.
- Consider changing the settings on your mobile device so it doesn't automatically connect to nearby Wi-Fi. That way, you have more control over when and how your device uses public Wi-Fi. Once you are all done with your web browsing, make sure to log off any services you were signed into. Then, tell your device to forget the network.

Visit www.cellcom.com/security for additional mobile security tips.

Cellcom is an innovative wireless company that provides nationwide service for its customer base throughout Wisconsin and Michigan, with nearly 70 retail and agent locations. Cellcom is respected for its long-standing reputation of delivering extraordinary customer care, being a strong community partner, and for its renowned network, which is customized to its rural markets. As a subsidiary of Nsight, Cellcom is part of a family of companies offering complete telecommunications services.