

# Quick Tips

## on Protecting Your Information on Unsecured Wi-Fi Networks

These days, Wi-Fi networks are everywhere and easier than ever to access. For instance, in addition to using your smart phone as a hot spot to connect, you'll also find Wi-Fi in countless other places: airports and hotels, libraries, and of course just about every corner coffee shop. These Wi-Fi networks, however, are often not secure.

That's why, as a precaution when using a Wi-Fi hotspot, you should only log in or send personal information to fully encrypted websites. The encryption feature scrambles the information you send over the Internet into code, making that information inaccessible to others.

Logging into an unencrypted site over an unsecured network, or a site that only uses encryption on the sign-in page, can allow other users on that network to see what you see and any information that you send. So someone could easily hijack your session and log in as you. Or, more alarming still, by using your name and password, a hacker could try to gain access to other websites – such as sites that contain your financial information.

If you're the least bit unsure whether a Wi-Fi hotspot is secure or not, just remember to ask yourself if the risks and long-term problems that can stem from identity theft are worth the short-term convenience. Better safe than hacked, so just wait if in doubt.

### Tips for using Wi-Fi networks/hotspots:

- Only log in or send your personal information to websites that you have verified to be fully encrypted.
- To be completely secure, make sure your entire experience on a site, page by page, is encrypted: when you log in, when you visit other pages on the site, right on through to when you log out.
- When you see "https" at the beginning of the web address, that's a good sign. The "s" stands for secure. But remember, some websites use encryption only on the login page. While using a web site, look to see that "https" is on every page, not just the login page.
- Staying permanently signed in to accounts creates more of a window of opportunity for anyone trying to hack your accounts. Be sure to log out when you've finished using an account.
- Create different passwords for different sites.
- Regularly update your browser and security software.
- Log out immediately if you believe you're logged in to an encrypted site but suddenly find you're on an unencrypted page.

