Tips for Using Public Wi-Fi Networks

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but often they're not secure. If you connect to a Wi-Fi network, and send information through websites or mobile apps, it might be accessed by someone else.

To protect your information when using wireless hotspots, send information only to sites that are fully encrypted, and avoid using mobile apps that require personal or financial information

How Encryption Works

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.

How to Tell If a Website is Encrypted

If you send email, share digital photos and videos, use social networks, or bank online, you're sending personal information over the internet. The information you share is stored on a server — a powerful computer that collects and delivers content. Many websites, like banking sites, use encryption to protect your information as it travels from your computer to their server.

To determine if a website is encrypted, look for **https** at the start of the web address (the "s" is for secure). Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, your entire account could be vulnerable. Look for **https** on **every** page you visit, not just when you sign in.

What About Mobile Apps?

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 (often referred to as 3G or 4G).

If you must use an unsecured wireless network for transactions, use the company's mobile website — where you can check for the **https** at the start of the web address — rather than the company's mobile app.

Don't Assume a Wi-Fi Hotspot is Secure

Most Wi-Fi hotspots **don't** encrypt the information you send over the internet and **aren't** secure. In fact, if a network doesn't require a WPA or WPA2 password, it's probably not secure.

If you use an unsecured network to log in to an unencrypted site — or a site that uses encryption only on the sign-in page — other users on the network can see what you see and what you send. They could hijack your session and log in as you. New hacking tools — available for free online — make this easy, even for users with limited technical know-how. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs.

An imposter could use your account to impersonate you and scam people in your contact lists. In addition, a hacker could test your username and password to try to gain access to other websites – including sites that store your financial information.

Protect Your Information When Using Public Wi-Fi

Here's how you can protect your information when using Wi-Fi:

- When using a hotspot, log in or send personal information only to websites you know are fully encrypted. To be secure, your entire visit to each site should be encrypted – from the time you log in to the site until you log out. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Do not use the same password on different websites. It could give someone who gains access to **one** of your accounts access to **many** of your accounts.
- 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 that 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.

- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can get a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees. What's more, VPN options are available for mobile devices; they can encrypt information you send through mobile apps.
- Some Wi-Fi networks use encryption: WEP and WPA are common, but they might not protect you against all hacking programs. WPA2 is the strongest.
- Installing browser add-ons or plug-ins can help. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don't protect you on all websites — look for **https** in the URL to know a site is secure.

Article from OnGuardOnline.gov March 2014