FREEDOM BANK

Tips for Using Public Wi-Fi Networks

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but they're often not secure. When using a hotspot, it's best to send information only to websites that are fully encrypted.

You can be confident a hotspot is secure only if it asks you to provide a WPA password. If you're not sure, treat the network as if it were unsecured.

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 that it's not accessible to others. When 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, such as 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 beginning 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.

Don't Assume a Wi-Fi Hotspot is Secure

Most Wi-Fi hotspots **don't** encrypt the information you send over the internet and are **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 you care about. 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 Yourself When Using Public Wi-Fi

So what can you do to protect your information? Here are a few tips:

FREEDOM BANK

- When using a Wi-Fi hotspot, only log in or send personal information to websites that 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.
- 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 obtain a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees.
- Some Wi-Fi networks use encryption: **WEP** and **WPA** are the most common. WPA encryption protects your information against common hacking programs. WEP may not. WPA2 is the strongest. If you aren't certain that you are on a WPA network, use the same precautions as on an unsecured network.

Installing browser add-ons or plug-ins can help, too. 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.