Internet Security

Tips On Using Wi-Fi Hotspots

(NAPSA)—Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities and other public places offer free access to the Internet.

However, public Wi-Fi networks often are not secure. You're sharing the hotspot with strangers, and some could be hackers.

Experts at the Federal Trade Commission (FTC) say that when using wireless hotspots, it's best to send only personal information that is encrypted—either by an encrypted website or a secure network.

Encryption scrambles information sent over the Internet into a code so that it's not accessed by others. An encrypted website protects only the information sent to and from that site. A secure wireless network encrypts all the information you send while online.

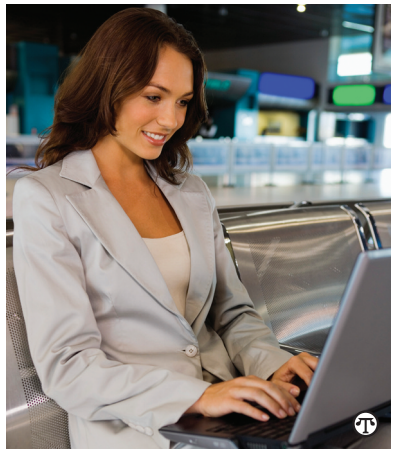
To tell if a website is encrypted, look for **https** at the beginning of the Web address (the "s" is for secure), and a lock icon at the top or bottom of the browser window. Some websites use encryption only on the sign-in page, but if any part of the session isn't encrypted, the entire account could be vulnerable. Look for https and the lock icon throughout the site, not just at sign in.

Is this hotspot secure?

• If a hotspot doesn't require a password, it's not secure.

• If a hotspot asks for a password through the browser simply to grant access, or asks for a password for WEP (wired equivalent privacy) encryption, it's best to proceed as if it were unsecured.

• A hotspot is secure only if it asks the user to provide a WPA (Wi-Fi protected access) password. WPA2 is even more secure than WPA.



Only log in to websites that are fully encrypted when using a Wi-Fi hotspot.

For a safer Wi-Fi experience, the FTC recommends:

• When using a Wi-Fi hotspot, only log in or send personal information to websites that you know are fully encrypted. The entire visit to each site should be encrypted—from log in until 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. After using an account, log out.

• Do not use the same password on different websites. It could give someone who gains access to one account access to many accounts.

To learn more about protecting your privacy online and what to do if your information is compromised, visit OnGuardOnline.gov.