

FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Division of Consumer & Business Education

Wise Up about Wi-Fi: Tips for Using Public Wireless Networks

Public wireless networks – those Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places – allow people to access the internet through a shared network. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information.

Using a Wi-Fi hotspot?

Only log in to websites that are fully encrypted.

Technology experts at the Federal Trade Commission (FTC), the nation's consumer protection agency, say 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 accessed by 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 network. An encrypted

website protects **only** the information you send to and from that site. A secure wireless network encrypts **all** of the information you send while online.

How to Identify an Encrypted Website

If you send email, share digital photos and videos, use online tools to manage calendars and contact lists, 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), and a **lock icon** at the top or bottom of your browser window. The exact position of the lock depends on which browser you use. Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, the entire account could be vulnerable. Look for **https** and the **lock icon** the entire time you're on the site, not just when you sign in. You can also click on the lock icon to display information about the site and help you verify that it's not a fraudulent website.

Public Wireless Networks

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

Is this hotspot secure?

- If a hotspot doesn't require a password, it's not secure.
- If a hotspot asks for a password through your browser simply to grant access, or it asks for a WEP password, it's best to treat it as if it were unsecured.
- You can be confident a hotspot is secure only if you are asked to provide a WPA password. If you're not sure, the information you enter could be at risk. WPA2 is the most secure.

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, an attacker could test your username and password to try to gain access to other websites – including sites that store your financial information.

Protect Your Information

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

- When using a Wi-Fi hotspot, only log in or send personal information to websites that you know are fully encrypted. And keep in mind that 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 take the extra minute or so to 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. 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 and the lock icon to know a site is secure.

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

The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a new video, *How to File a Complaint*, at ftc.gov/video to learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.