

## Tips for using public Wi-Fi

“Wi-Fi” (short for “Wireless Fidelity”) is a radio wave-based technology that allows computers, smartphones, and other electronic devices to connect to the internet or to communicate with one another wirelessly.

A number of coffee shops, libraries, airports, hospitals, hotels, fast food restaurants, and other businesses are using Wi-Fi to provide free public access points (or hotspots) that their customers can use to connect wirelessly to the internet. A single hotspot typically has a range of about 65 feet indoors and a greater range outdoors.

Accessing the internet using a public Wi-Fi hotspot is convenient and often free for mobile users, but hotspots typically are not secure. If you are not required to enter a password provided by the Wi-Fi host (i.e. coffee shop or hotel) before gaining access to the network, another Wi-Fi user could hack into your electronic device and view your personal information and what you are sending. They could change your passwords and block you out of your own files. They could even use your account to impersonate you and scam the people you care about. So if you are not certain that a network is secure, treat it as if it were unsecure.

### How encryption works

In addition to using secure networks, it is best to send sensitive information only to encrypted websites. If you send email, share digital photos and videos, use social networks, or bank online, you are 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 between your computer and their servers. Encryption is the key to keeping your personal information secure online. Encryption scrambles the information you send over the internet into a code that it is not accessible to others. When using wireless networks, it is best to send personal information only if it is 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

Encrypted websites will have “**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 is not encrypted, your entire account could be vulnerable. Look for **https** on every page you visit, not just when you sign in.

### Do not assume a Wi-Fi hotspot is secure

Most Wi-Fi hotspots **do not** encrypt the information you send over the internet and are **not** secure. If you use an unsecured network to log on to an encrypted website 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 log-in credentials could be compromised.

## Turn on two-factor authentication if offered

Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized, such as a personal identification number (PIN) or password.

## Protect yourself when using public Wi-Fi

- When using a Wi-Fi hotspot, only log in or send personal information to websites that you know are fully encrypted. To ensure security, your entire visit to each site should be encrypted (look for **https** in the address bar). If you are not sure if you are on a secure page, log out right away.
- Do not stay permanently signed in to accounts. Log out when you are done using any account.
- Do not use the same password on different websites. It could give someone who gains access to one of your accounts access to all of your accounts.
- Many web browsers alert users who unknowingly attempt 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.
- WEP and WPA are the most common types of Wi-Fi encryption available. WPA encryption protects your information against common hacking programs while WEP may not. WPA2 is the strongest. Use the same precautions as on an unsecured network if you are not certain that you are on a WPA network.
- Installing browser add-ons or plug-ins can also 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 are not encrypted. They do not protect you on all websites, so remember to look for **https** in the URL to confirm if a site is secure.
- For more information on using public Wi-Fi hotspots, visit:

StaySafe Online  
staysafeonline.org

OnGuardOnline  
onguardonline.gov

Federal Trade Commission  
ftc.gov

For more information or to file a complaint, visit our website or contact the Bureau of Consumer Protection.

**Bureau of Consumer Protection**  
**2811 Agriculture Drive**  
**PO Box 8911**  
**Madison WI 53708-8911**

**E-MAIL:**  
**DATCPWisconsinPrivacy@wi.gov**

**WEBSITE: datcp.wi.gov**

**(800) 422-7128**

**(608) 224-4976**

**FAX: (608) 224-4677**

**TTY: (608) 224-5058**

## Common Wi-Fi terms

### Encryption

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

### FTP

A protocol that allows users to copy files between their local system and any system they can reach on the network.

### HTTPS – Hypertext Transfer Protocol Secure

HTTPS is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication and secure identification of a network web server. HTTPS connections are often used for payment transactions on the Internet.

### “Man-in-the-middle” attacks

A “man-in-the-middle” attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection – when in fact the entire conversation is being controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones. For example, an attacker within reception range of an unencrypted Wi-Fi access point can insert himself as a man-in-the-middle. Or an attacker can pose as an online bank or merchant, letting victims sign in over a SSL connection, and then the attacker can log onto the real server using the victim’s information and steal credit card numbers.

### Modem

A modem is a device that encodes digital computer signals into analog telephone signals and vice versa and allows computers to communicate over a phone line.

### SSL – Secure Sockets Layer

SSL protocol is for securing data communications across computer networks. It establishes a secure session by electronically authenticating each end of an encrypted transmission. It is used by websites whose names begin with **https** instead of **http**.

### VPN – Virtual Private Network

A Virtual Private Network (VPN) secures and privatizes data across a network, usually the internet, by building an “encrypted tunnel.” Data passes through this tunnel, protecting it from anyone who tries to intercept it. Even if the data is intercepted, it is hopelessly scrambled and useless to anyone without the key to decrypt it.

### WEP – Wired Equivalent Privacy and WPA/WPA2 – Wi-Fi Protected Access

WEP and WPA are types of security connections that are used to protect home wireless networks. WEP is a security algorithm that was introduced in 1997 to provide confidentiality comparable to that of a traditional wired network. Since 2001, several serious weaknesses in the WEP protocol have been identified, and today a WEP connection can be cracked within minutes. In 2003 WEP was superseded by Wi-Fi Protected Access (WPA). WPA and WPA2 are certification programs that test Wi-Fi product support for IEEE-standard security protocols that can encrypt data sent over the air, from Wi-Fi user to Wi-Fi router.