Wireless Connections and Bluetooth Security Tips

Español | 繁體中文 | Tagalog | Tiếng Việt | 한국어

Wi-Fi networks and Bluetooth connections can be vulnerable points of access for data or identity theft. Fortunately, there are many ways to decrease your chances of becoming a victim.

Encryption is the best way to keep your personal data safe. It works by scrambling the data in a message so that only the intended recipients can read it. When the address of a website you're visiting starts with "https" instead of "http," that indicates encryption is taking place between your browser and site.

The two most common types of encryption are Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WPA). The strongest one commonly available is WPA2, so use that if you have the option. Home Wi-Fi systems and public Wi-Fi access points, or "hotspots," usually will inform you of the encryption they use.

Public Wi-Fi Access | Bluetooth Security | Home Wireless Network Security | Passwords

Public Wi-Fi Access

Many Wi-Fi users choose to use public networks instead of their devices' data plans for accessing the internet remotely. But the convenience of public Wi-Fi can be risky. If you're not careful, hackers may quickly access your connection and compromise sensitive information stored on your device and in online accounts. Here are some steps you can take to minimize the risk:

- Check the validity of available Wi-Fi hotspots. If more than one hotspot appears claiming to belong to an establishment that you're in, check with the staff to avoid connecting to an imposter hotspot.
- Make sure all websites you exchange information with have "https" at the beginning of the web address. If so, your transmitted data will be encrypted.
- Install an app add-on that forces your web browsers to use encryption when connecting to websites -- even well-known sites that may not normally encrypt their communications.
- Adjust your smartphone's settings so it does not automatically connect to nearby Wi-Fi networks. This gives you more control over where and when you connect.
- If you use public Wi-Fi hotspots on a regular basis, consider using a virtual private network, which will encrypt all transmissions between your device and the internet. Many companies offer VPNs to their employees for work purposes, and individuals may subscribe to VPNs on their own.
- When transmitting sensitive information, using your cellphone data plan instead of Wi-Fi may be more secure.

Printable Version

Wireless Connections and Bluetooth Security Tips **(pdf)**

Date Last Updated/Reviewed: Tuesday, October 8, 2019

Bureau/Office:
Consumer and Governmental Affairs
Tags:
Consumers - Online privacy - Privacy Consumer Issues

Alternate Format Requests

People with print disabilities may request braille, large print, or screen-reader friendly versions of this article via the email form at fcc504@fcc.gov. For audio and other access, use the "Explore Accessibility Options" link.

Consumer Help Center

Learn about consumer issues - visit the FCC's Consumer Help Center at fcc.gov/consumers.

File a Complaint with the FCC

File Your Complaint

Visit our Consumer Complaint Center at consumercomplaints.fcc.gov to file a complaint or tell us your story.

Federal Communications Commission
45 L Street NE
Washington, DC 20554

Phone: 1-888-225-5322
ASL Video Call: 1-844-432-2275
ASL Video Call: Web
Fax: 1-866-418-0232
Contact Us