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

Bluetooth Security

Bluetooth connections to your mobile devices can be used to connect to wireless headsets, transfer files, and enable hands-free calling while you drive, among other things. Most of the time, a user must allow a Bluetooth connection to occur before data is shared - a process called "pairing" - which provides a measure of data security. But just like Wi-Fi connections, Bluetooth can put your personal data at risk if you are not careful. Here are some steps you may wish to take when using Bluetooth:

- Turn Bluetooth off when not in use. Keeping it active enables hackers to discover what other devices you connected to before, spoof one of those devices, and gain access to your device.
- If you connect your mobile phone to a rental car, the phone's data may get shared with the car. Be sure to unpair your phone from the car and clear any personal data from the car before you return it. Take the same steps when selling a car that has Bluetooth.
- Use Bluetooth in "hidden" mode rather than "discoverable" mode. This prevents other unknown devices from finding your Bluetooth connection.

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

1 digg 112

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.

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