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

Passwords

Remembering all of your assorted passwords can be a pain. Web browsers and other programs may offer to remember passwords for you, which can be a significant timesaver. However, certain password shortcuts can leave you less safe secure. The following best practices may help keep your personal information safer:

- Don't use the same password for multiple accounts, especially for the most sensitive ones, such as bank accounts, credit cards, legal or tax records and files containing medical information. Otherwise, someone with access to one of your accounts may end up with access to many others.
- Don't have your web browser remember passwords and add them for you, particularly for your most important financial, legal and medical accounts. If an unauthorized person gains access to your computer or smartphone, they could access any account that your browser automatically logs into.
- Don't use passwords that can be easily guessed, such as common words and birthdays of family members. Instead, use a combination of letters, numbers and symbols. The longer and stronger the password, the safer your information.

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.

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