Wireless Connections and Bluetooth Security Tips

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

Many Wi-Fi users prefer choose to use public networks instead of their devices' data plans for accessing the internet remotely. But the convenience of public Wi-Fi does not come without risk. If you're not careful, a hacker can access your connection in a matter of seconds, and potentially put sensitive information stored on your device and in online accounts at risk. 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.

Bluetooth Security

Bluetooth connections to your mobile devices can be very useful, from connecting a wireless headset to transferring files to enabling hands-free calling while you drive. Most of the time, a user must allow a Bluetooth connection to occur before data is shared – a process called "pairing" – which provides a

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/consumer-governmental-affairs-bureau

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. If you keep Bluetooth active, a hacker may be able 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, a good deal of data from your phone may get shared with the car. Be sure to unpair your phone from the car and clear any personal data, such as call logs and saved numbers, from the car before you return it. Take the same steps when selling a car that has Bluetooth.
- When using Bluetooth, use it in "hidden" mode rather than "discoverable" mode. This prevents other unknown devices from finding your Bluetooth connection.

Home Wireless Network Security

Home wireless networks are exceedingly popular, in large part because they enable computers and mobile devices to share one broadband connection to the internet without having to use up minutes on a cellular data plan. They also provide the convenience of not having to connect all these devices with wires to do so. But like all other wireless network technologies, home wireless networks present vulnerabilities that could be exploited by hackers to obtain sensitive data and commit other crimes. To help protect your home wireless network from unwanted users, consider the following steps:

- Turn the encryption on. Wireless routers often come out of the box with the encryption feature disabled, so be sure to check that encryption is turned on shortly after you or your broadband provider installs the router.
- Change the network's default network name, also known as its service set identifier or "SSID." When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. Manufacturers usually give all of their wireless routers a default SSID, which is often the company's name. It is a good practice to change your network's SSID, but to protect your privacy do not use personal information such as the names of family members.
- Change the network's default password. Most wireless routers come with preset passwords for administering a device's settings (this is different from the password used to access the wireless network itself). Unauthorized users may be familiar with the default passwords, so it is important to change the router device's password as soon as it is installed. Again, longer passwords made up of a combination of letters, numbers and symbols are more secure.
- Consider using the MAC address filter in your wireless router. Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" (Media Access Control) address. Wireless routers can screen the MAC addresses of all devices that connect to them, and users can set their wireless network to accept connections only from devices with MAC addresses that the router will recognize. To create another obstacle to unauthorized access, consider activating your wireless router's MAC address filter to include your devices only.
- Turn off your wireless router when it will not be in use for any extended period of time.
- Use anti-virus and anti-spyware software on your computer, and use similar apps on your devices that access your wireless network.

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 input 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.

Consumer Help Center

For more information on consumer issues, visit the FCC’s Consumer Help Center at www.fcc.gov/consumers.

Accessible formats

To request this article in an accessible format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last Reviewed: 04/03/19

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/consumer-governmental-affairs-bureau