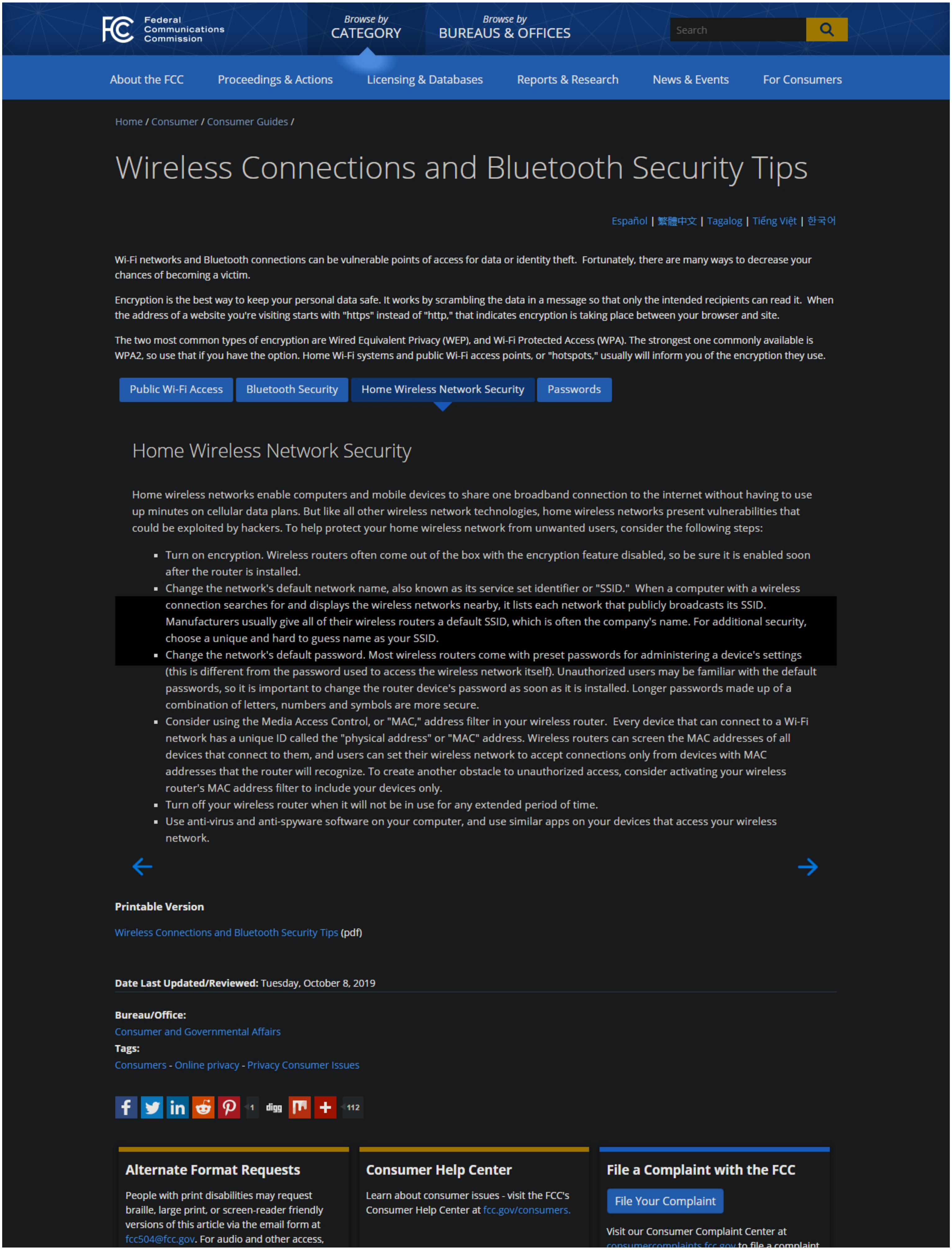


Wireless Connections and Bluetooth Security Tips

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.

Home Wireless Network Security

Home wireless networks enable computers and mobile devices to share one broadband connection to the internet without having to use up minutes on cellular data plans. But like all other wireless network technologies, home wireless networks present vulnerabilities that could be exploited by hackers. To help protect your home wireless network from unwanted users, consider the following steps:

- Turn on encryption. Wireless routers often come out of the box with the encryption feature disabled, so be sure it is enabled soon after the router is installed.
- 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. For additional security, choose a unique and hard to guess name as your SSID.
- 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. Longer passwords made up of a combination of letters, numbers and symbols are more secure.
- Consider using the Media Access Control, or "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" 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.

← →

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,

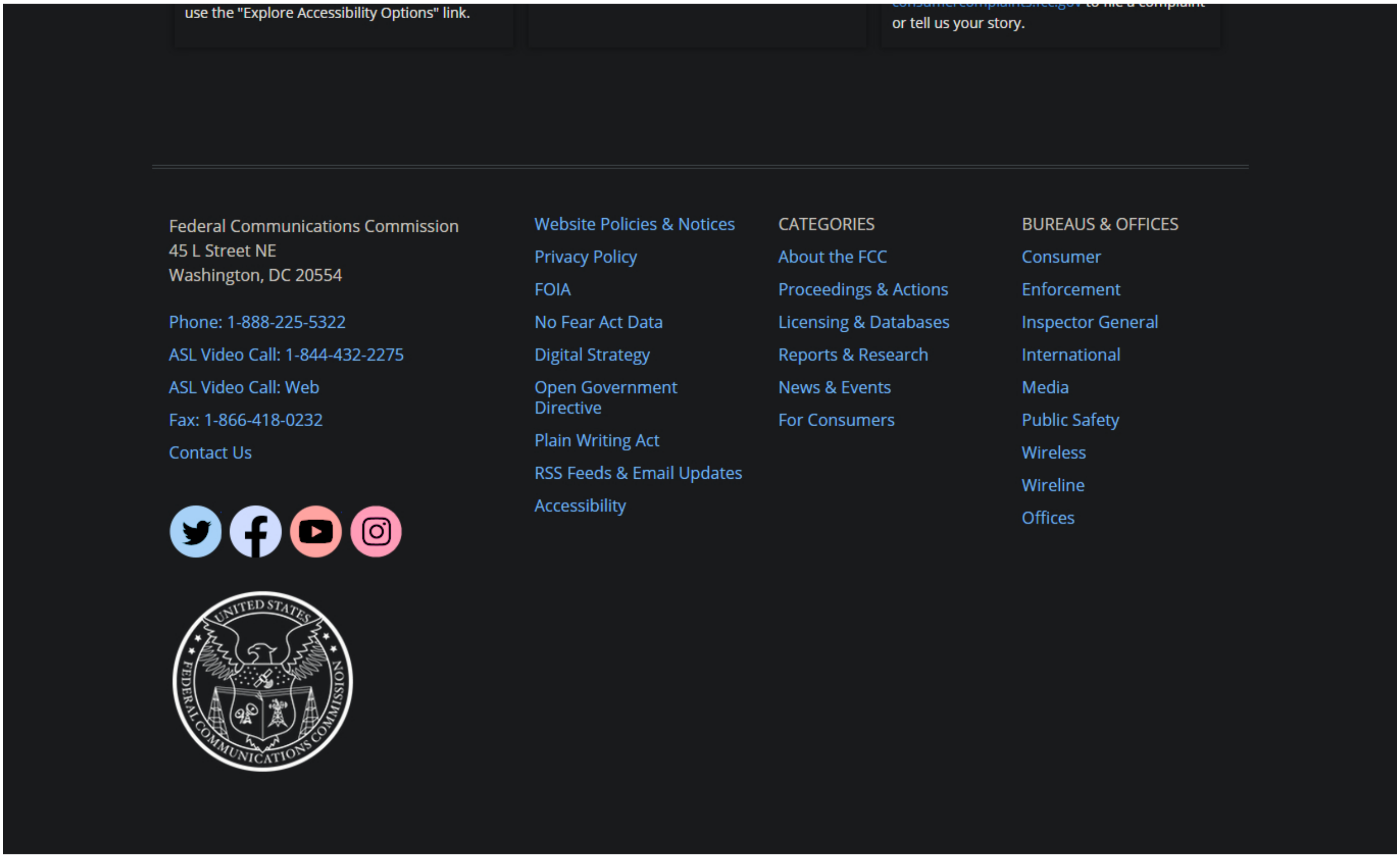
Consumer Help Center

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



use the "Explore Accessibility Options" link.

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

Website Policies & Notices

Privacy Policy

FOIA

No Fear Act Data

Digital Strategy

Open Government Directive

Plain Writing Act

RSS Feeds & Email Updates

Accessibility

CATEGORIES

About the FCC

Proceedings & Actions

Licensing & Databases

Reports & Research

News & Events

For Consumers

BUREAUS & OFFICES

Consumer

Enforcement

Inspector General

International

Media

Public Safety

Wireless

Wireline

Offices