U.S. Coast Guard Auxiliary
Computer Software & Systems Directorate
Cybersecurity Division
CYBERSECURITY AWARENESS BULLETIN

USING PUBLIC WI-FI NETWORKS SAFELY

Serial:	CI-AWA-2020-217-02
Date:	04 AUGUST 2020

Overview

Wireless Internet access points, usually referred to as Wi-Fi networks, are everywhere. Whether at home, at work, or on the go, Auxiliarists can use public Wi-Fi networks to browse the web and use Internet-based applications, such as email or social media platforms. But the public nature of these Wi-Fi networks also means that they are vulnerable to hacking and disruption. That potentially places you, your data, your shipmates' information, and Auxiliary systems at risk. It is critical to take basic precautions when using public Wi-Fi to reduce the possibility of harm to Auxiliary networks.

Why use public Wi-Fi networks?

Public Wi-Fi networks offer several convenient advantages over other Internet connectivity methods. Mobile devices like smartphones connect to the Internet via wireless telephone providers—that is, your smartphone connects over the air to a nearby cell phone tower. Accessing the Internet in this way uses data that your wireless provider allocates to you. However, if you use your smartphone to connect to a public Wi-Fi network, you can reduce your wireless data consumption for the month, since you are tapping into a different resource to access the Internet.

In addition, some devices—such as laptop computers—cannot connect to wireless telephone network on their own. Instead, users must use the laptops' built-in Wi-Fi cards to connect to the Internet.

Why are public Wi-Fi networks risky?

Despite their advantages, public Wi-Fi networks pose risks.

- Public Wi-Fi networks are controlled by third parties. This means that, in theory, the third party—a café owner, an airport administrator, or a hotel staff member, for example—could read their wireless access logs and learn about the websites you visit and the apps that you use on your smartphone.
- Second, Wi-Fi networks are vulnerable to "Man in the Middle (MITM)" attacks. A malicious actor can deploy a phony Wi-Fi network that appears legitimate, but which in fact intercepts your personal data. In this way, the malicious actor can record enormous amounts of information about your Internet use, while you remain oblivious to the fact that your data is being intercepted.

How to stay safe when using public Wi-Fi networks

Wherever possible stick to well-known networks. These Wi-Fi networks are likely less suspect because the people and companies operating them already have you as a customer. No public Wi-Fi network is absolutely secure, but in terms of relative safety, known quantities generally beat out that random public Wi-Fi network that pops up on your phone in a shopping mall, or a network operated by a third party that you've never heard of.

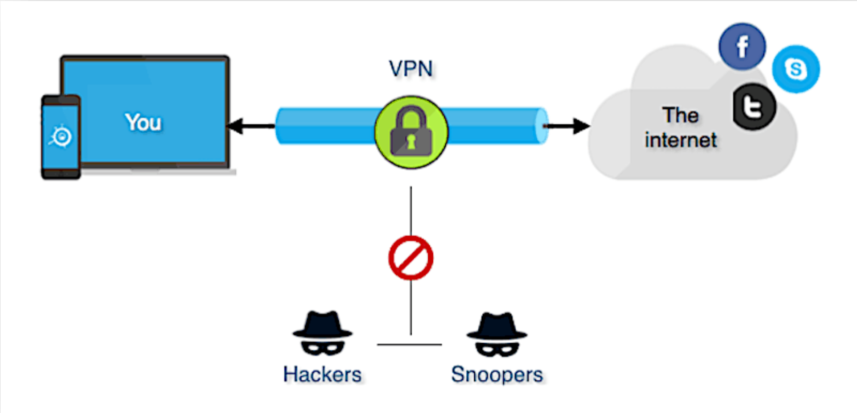

Image from Network Encyclopedia (www.networkencyclopedia.com)

To keep your data secure when you are using public Wi-Fi, it is worth considering an investment in a Virtual Private Network (VPN). VPNs create an encrypted tunnel through which your data travels when you are connected to a public Wi-Fi network. By utilizing a VPN, the owner of the Wi-Fi router, as well as the owner's Internet Service Provider, will be unable to determine what websites you are visiting, what apps you are using, and the data you are sending and receiving. This helps to keep your information safe. For a basic primer on the features and advantages/disadvantages of various VPN providers, click here.

If you are in the company of others and have a shared need to be online, then you may also be able to keep your data safer by using a smartphone as a hot spot. This hot spot capability, which is built into most new smartphones, uses the smartphone itself as a Wi-Fi router. In this way, multiple devices can access the Internet via the smartphone, rather than using a third-party Wi-Fi network.

There are certain types of information that you should avoid entering online when you are connected to any public Wi-Fi network. If you are not using a VPN connection, then you should refrain from typing financial information—such as online banking logins and passwords, credit card website login information, and/or investment data—while connected to public Wi-Fi networks. It is also advisable to limit entry of other high-value personally identifiable information, such as full legal names, dates of birth, and Social Security numbers.

You may wish to consider using a privacy-focused web browser. These kinds of web browsers are geared toward limiting the amount of personal information that websites collect about your browsing habits. In this way, they help to limit the amount of data that is sent and received through public Wi-Fi networks. Examples of these browsers include the Tor browser, Mozilla's Firefox browser, the EPIC privacy browser, and the Brave browser. We do not endorse any specific web browser. In addition, some networks may block access to one or more of these browsers. Nevertheless, Auxiliarists are encouraged to research their options and to choose the web browser that best fits their needs and preferences.

Finally, disconnect when you are done using the internet. By not leaving your device connected, you reduce the opportunity to have your device or data compromised while not in use.