Questions and Answers about Public Wireless Networks

Office of Information Technology
Division of Information Security
SEPTEMBER 2022

Can I trust that a publicly available wireless network is safe and secure?

Absolutely not! There is no guarantee that any place with public W-Fi put any effort into protecting user information. It's possible that organizations with public Wi-Fi available set up their wireless networks without considering security settings, and that they don't maintain their network security sufficiently either.

Can I be sure no one can see my activity when I use a public wireless network?

You can never be sure. A hacker can be indistinguishable from others because they may just be using a laptop or even a smartphone. A hacker may also use a device with an antenna that can function while hidden in a backpack. Someone monitoring public network traffic may be out of sight, such as on the other side of a wall.

You might be looking out for someone like this…

but the hacker actually looks like this…

If I'm in Restaurant ABC, then the wireless network named "Restaurant ABC" is legitimate, right?

No. A hacker can create a fake wireless network and give it any name. The hacker will likely use a name that sounds real to make people think they are connecting to a legitimate wireless network. The fake wireless network is called an "evil twin." The hacker can then capture the internet activity data of people using the evil twin network. This data can include websites people visit, and what they type on those websites, such as usernames, passwords, credit card numbers, or other personal information. Malicious actors can even access your machine and install software without your knowing.

If I confirm I'm connecting to a legitimate public wireless network and not an evil twin, then is it safe to use that real network?

Even if you're using a legitimate public wireless network, you still may not be safe. A hacker can also connect to it, and when they are on the same network as you, they can capture your internet activity data.

If connecting to a publicly available wireless network requires a password, does that make it safe?

No. While requiring a password is somewhat safer, understand that anyone, including you or someone malicious, have the same ability to learn the wireless network password and join the network. Remember that if a hacker is on the same network as you, they can capture your internet activity data.

Is it unsafe for me to conduct any internet activity on a public wireless network?

Not all internet activity is equally unsafe to conduct. When you're on a public wireless network, you should treat certain internet activity with much more caution than other types. Never type any information a cybercriminal could use for financial gain. For example, if you type your credit card information on a website, a cybercriminal can make purchases with that information. If you type your personal information such as address, birthdate, and social security number, a cybercriminal can steal your identity. If you type your password to check your email, a cybercriminal can log in to your email account and see the accounts linked to your email. The cybercriminal may attempt to log in to those accounts using a password they have already captured from you, so be sure to use a different password for each of your accounts and change them regularly. Enabling multi-factor authentication for your accounts prevents cybercriminals from being able to log in to them with just the passwords.

These are examples of what to be careful about. In contrast, you don't need to be as careful about using a public network to check the weather, a store's hours of operation, or the score of a sports game. Having said that, always use strong passwords. If you searched for dolphins on a public network and one of your passwords is "dolphins123," a hacker can use your internet activity to crack your password.

Is there a secure way to access the internet on my smartphone when I'm in a public place?

Fortunately, yes, there is. If you don't turn off Wi-Fi, your smartphone may connect to wireless networks used previously automatically, which will expose you to the vulnerabilities explained earlier. If you need to access the internet securely on your smartphone, go to your settings and toggle the Wi-Fi off. (See Figure 1, below.) After ensuring your smartphone's Wi-Fi is off, you can browse the internet as you normally would using your cellular data. Check your cell phone provider plan for your cellular data allowance. Once you no longer need a secure connection, toggle the Wi-Fi back on to stop using your cellular data.

How do I safely access the internet on my laptop in a public place?

To access the internet on your laptop, you must connect it to a network. When you're connecting wirelessly at home, your home router provides a trustworthy link to the internet. In contrast, you can't trust a public place to safely connect you. You can't bring your home router to a public place in order to connect to it, but you can bring another type of wireless access point called a mobile hotspot.

A mobile hotspot is a device designed to provide internet access when you're away from your trusted networks. The only people who can connect to the mobile hotspot's wireless network are those who know its password. When you're in a public place, be careful not to write or display the mobile hotspot's password where others might see it.

You can buy a mobile hotspot device, or you may be able to use your smartphone as a mobile hotspot. Check your cell phone provider for this functionality and pricing. If your smartphone has hotspot functionality, go to settings and select the hotspot option, which may read as "Personal Hotspot," "Hotspot & tethering," or a similar term depending on your smartphone. (See Figure 1.) Toggle the hotspot on. Your smartphone will display the hotspot name and password. Your laptop will detect your mobile hotspot wireless network, and you can connect to it in the same way that you connect to other wireless networks.

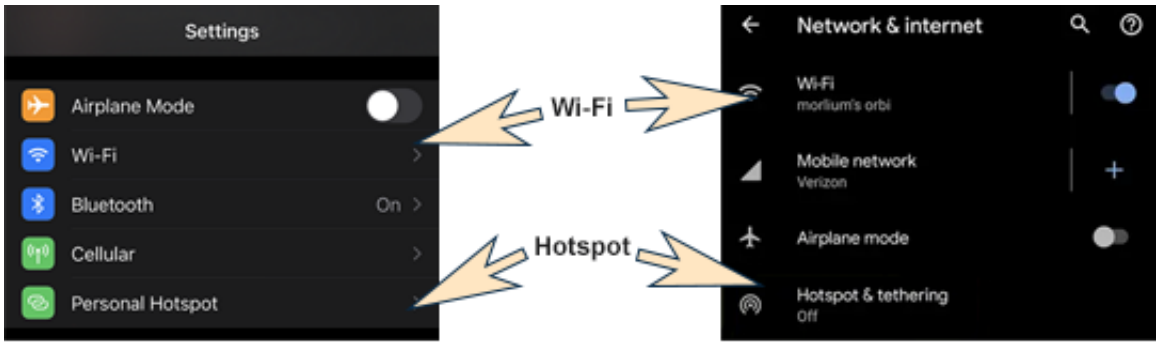
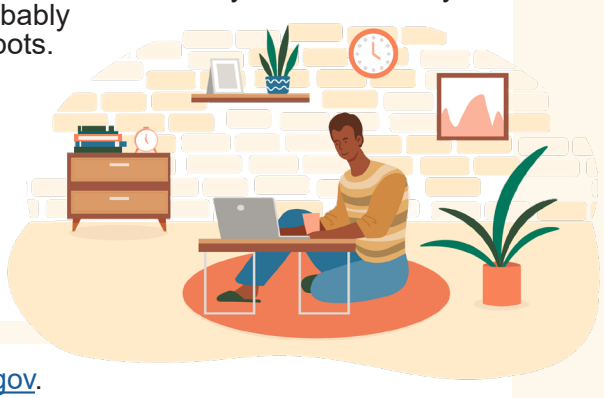


Figure 1

Using your smartphone as a mobile hotspot saves you from having to purchase an additional device. However, buying a mobile hotspot device provides you with better wireless performance (https://www.business.com/internet/tethering-vs-hotspots). If you need to use the internet often when away from your home or office, you might want to research mobile hotspot devices and see if the cost is worth the benefit for your situation. If you rarely use the internet away from your trusted networks, then you probably don't need to buy a mobile hotspot device or subscribe to mobile hotspots.

What's a best practice for connecting to wireless networks?

Try to conduct as much of your internet activity as you can at your home or office where you can be more confident of the security settings. Then you don't have to worry about the risks of public wireless networks.



For any questions about this article, please contact Cybersecurity@ihs.gov.