Is Public Wi-Fi Safe and What Can You Do to Use Public Wi-Fi Safely?

This article was published March 15, 2023 in the online magazine, **MUO** (Make Use Of), Sandeep Babu, author. The entire article can be accessed at https://www.makeuseof.com/is-public-wi-fi-safe-and-what-can-you-do-to-use-public-wi-fi-safely/.

It is presented here as a public service for our OLLI members who perhaps, may not have given much thought to using free Wi-Fi. It has been annotated by Jeanne Dyer, OLLI Technology Coordinator. The text in blue, are links which provide additional information and instructions.

So a business is offering free Wi-Fi? Great! But you probably shouldn't use it. At least, not without protection.

Public Wi-Fi hotspots are almost everywhere. Be it a hotel, café, restaurant, or airport, you can get a free Wi-Fi connection in most public places.

But is public Wi-Fi actually safe? And if not, are there ways to access public Wi-Fi networks safely?

WHY BRANDS OFFER FREE WI-FI

Free Wi-Fi increases sales. Customers with access to a free Wi-Fi network are more likely to stay longer on business premises. As a result, they will buy more products.

Some companies offer free Wi-Fi to promote their products or services, as some Wi-Fi solutions allow businesses to create landing pages to share real-time offers. Also, free Wi-Fi is an easy way for businesses to stand out and make customers feel welcome.

By offering free Wi-Fi access, companies create an edge over their competitors that don't provide free internet to customers.

IS PUBLIC WI-FI SAFE?

No, public Wi-Fi is not safe. Connecting to public Wi-Fi in coffee shops, hotels, airports, or other public places makes you susceptible to the following security threats.

Evil Twin Attacks

In an evil twin attack, a hacker sets up a malicious hotspot with the name of a legitimate network. And when you connect to the malicious hotspot, the hacker gains access to your online activities. But you think you are connected to the brand' legitimate Wi-Fi network.

So be sure to watch out for the signs of evil twin public Wi-Fi networks run by hackers to avoid getting connected to a malicious hotspot.

Man-in-the-Middle-Attacks

In a Man-in-the-Middle (MITM) attack, a third-party intercepts the data between two points.

When you connect to an internet connection and visit a website, data travels between your device and the website. Poorly secured public Wi-Fi connection makes it easy for hackers to intercept this data in the middle and read everything you're doing.

Wi-Fi Sniffing

Wi-Fi sniffing is one of the most common ways hackers steal your identity on public Wi-Fi and intercept data. With inexpensive kits and tools, hackers can eavesdrop on your public Wi-Fi connection if your device is not secure enough and know everything you're doing online.

Malware Infection

Due to the poor security (or no security at all) of public Wi-Fi networks, the threat actors can install various types of malware on your inadequately secured device, stealing or encrypting data.

Data Interception

A Wi-Fi router has the option to enable an encrypted connection between a device and the router. If this option is turned off in any public Wi-Fi network, it will create an unsecured network, meaning hackers can know what you are doing if they are able to intercept the traffic between the router and your device.

A bad thing is you can never know whether the public Wi-Fi network you are going to use is an encrypted network or not. Click the short video below or watch it at YouTube.com for more information.

Wi-Fi HERE
Check your wireless device, you can now connect!
SSID: FreeWiFibyHTCONE
MTA
The Dangers of Public Wi-Fi

HOW TO USE PUBLIC WI-FI SAFELY

The following are some ways to minimize security risks while using public Wi-Fi networks.

Enable Firewall and Antivirus on Your PC

A good firewall and antivirus software program can thwart malware attacks when you are using public Wi-FI networks. So make sure you have enabled the firewall on your PC and that your antivirus program is up-to-date.

Though Microsoft Defender offers reasonable security, investing in a premium antivirus software program would be better considering the growing number of cyberattacks.

Use a Disposable Email Address to Signup for Public Wi-Fi

Wi-Fi hotspots often ask you to submit your email address to start using the free internet. Instead of giving your personal email id, you can use a disposable email address to protect your privacy. If you use iOS or iPadOS devices, you are offered this when you select Sign in with Apple for a website.

Check for a Secure Connection

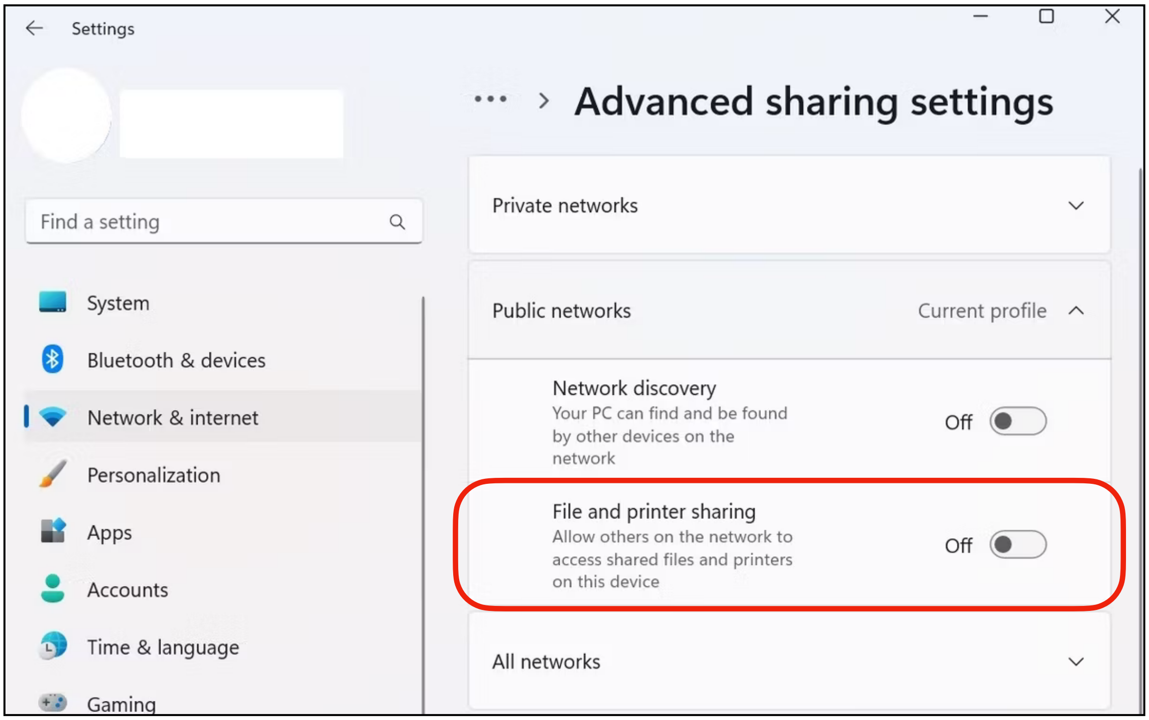
Always visit secure websites when using free internet connections offered by brands. To ensure the website you are visiting is secure, look at the website address carefully. If the web address doesn't include "HTTPS," it is not a safe website to visit. The “S” stands for “secure”.

Ensure Your Network File Sharing Is Turned Off

When network file sharing is enabled, threat actors on the same network can access shared files on your computer. So you must keep sharing turned off when connecting to a public Wi-Fi network.

Additionally, keeping sharing off when connected to an open network help you prevent sharing essential files with the wrong person by mistake.

To turn off network file sharing on your Windows PC, go to ***Settings*** > ***Network & internet*** > ***Advanced network settings***. Then, click on **Advanced sharing settings**. Toggle off **File and printer sharing.** You can also consider toggling off **Network discovery** for better privacy (screenshot on next page).



Advanced sharing settings

Private networks

Public networks — Current profile

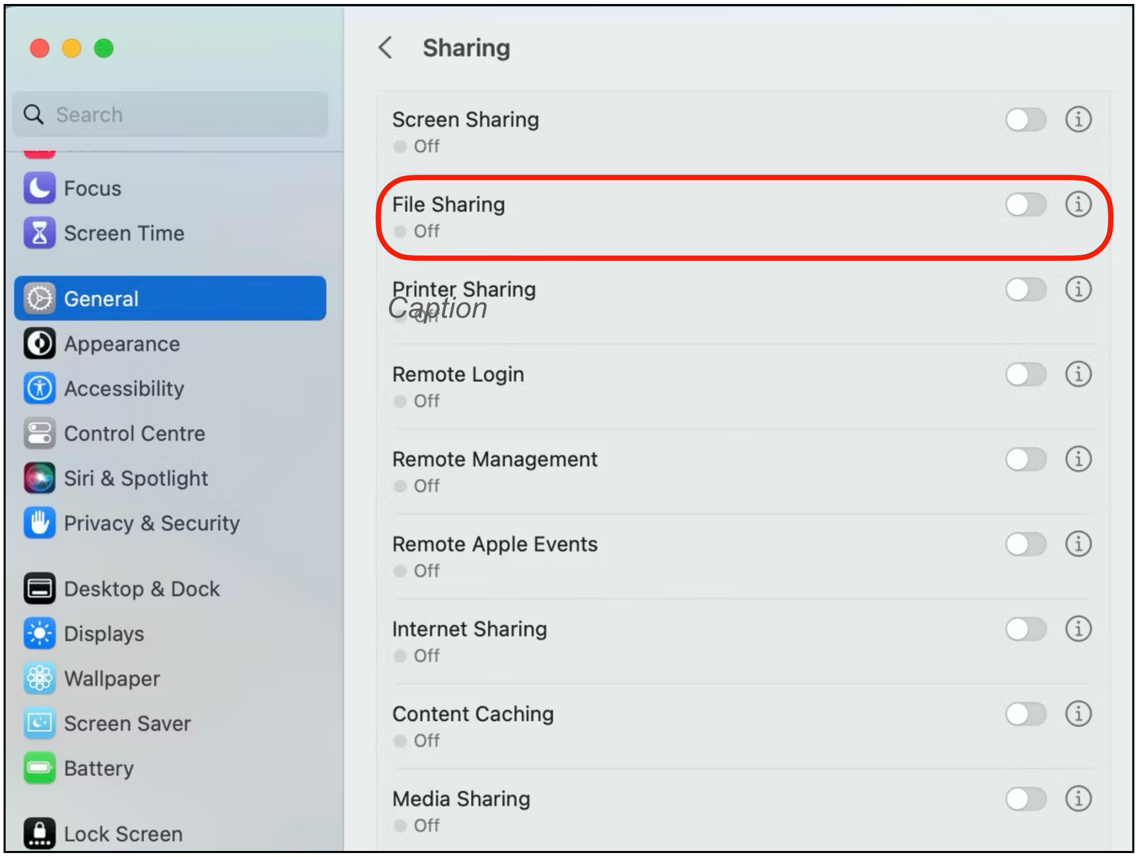
Network discovery
Your PC can find and be found by other devices on the network — Off

File and printer sharing
Allow others on the network to access shared files and printers on this device — Off

All networks

File Sharing on a PC

Mac users should go to ***System Settings > General > Sharing***. Then, uncheck ***File Sharing***.



Sharing

Screen Sharing — Off

File Sharing — Off

Printer Sharing — Off

Remote Login — Off

Remote Management — Off

Remote Apple Events — Off

Internet Sharing — Off

Content Caching — Off

Media Sharing — Off

File Sharing on a Mac (Apple Computers)

Avoid Submitting Personal Information

When using a public Wi-Fi network, you should avoid submitting sensitive information online, such as:

- Card details
- Social security number
- Address
- Phone number
- Date of birth

If you must share your private information with any trusted web application, use your smartphone's internet (cellular) to be on the safer side.

Forget the Network After Using It

Once you have used a public Wi-Fi network, always forget the network. This will prevent automatically connecting to the network when you are in the range, reducing the time your device is connected to a public Wi-Fi network.

Keep Your OS and Software Updated

Threat actors also exploit vulnerabilities in operating systems and software programs to carry out various cyberattacks on devices connected to public Wi-Fi networks. So you should always keep your device and software programs updated.

NOW YOU CAN USE PUBLIC WI-FI SAFELY

A public Wi-Fi network poses severe security risks, and being careless while connecting to a free Wi-Fi connection can cost you dearly. So you should always keep your guard up and follow these tips to stay protected while using public Wi-Fi.