PUBLIC WI-FI SECURITY TIPS

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of May 2025.

With most people carrying smart devices, whether smartphones or tablets, access to Wi-Fi is basically a necessity nowadays. And if your device's mobile or data plan isn't generous or you don't have access to a private network, finding public Wi-Fi while you're out and about can be a lifesaver. But just how risky is using public Wi-Fi?

Should I really be worried about public Wi-Fi?

When using public Wi-Fi, your device and personal information are at risk because someone else might be able to access them. There are two main ways this can happen: (1) someone could gain access to your device and its contents, and (2) they could intercept the information you send and receive while online, which may include the websites you visit and sometimes your usernames and passwords.

Access to your device

When you connect to public Wi-Fi, your device becomes part of a network alongside other devices connected to the same network. Depending on your device's settings, other users on that network may see your device and potentially access your files. To prevent this, check your settings for "discovery" and "file and print sharing" and turn them off when using public Wi-Fi.

For MacBook, iPhone, or iPad users, it is important to turn off AirDrop or adjust the settings to allow connections only from your contacts.

Although it is less common, a malicious individual (i.e. a hacker) can access your device by scanning for open ports to see if they can exploit them. A port enables your device to send and receive data while connected to the internet, a normal part of the process. Typically, a port opens only when connecting to the internet, such as when sending an email or visiting a website. To enhance your device's security, ensure that your firewall is activated, that you are running antivirus software on your devices, and that you regularly turn your device off completely for several minutes.

Access to your internet traffic data

Hackers have various methods to access personal information, including intercepting internet traffic. This can include data such as the websites you visit and your login credentials (usernames and passwords). Typically, a hacker needs to be connected to the same public Wi-Fi network to actively intercept the internet traffic of other users. Depending on their level of sophistication, skill, and intent, a hacker may eavesdrop on your internet activity or manipulate your data as it is transmitted, directing you to fake websites or sites containing malware.

Some hackers set up fake Wi-Fi hotspots, allowing them to monitor the internet traffic of anyone who connects to these fraudulent networks. This will enable them to access usernames, passwords, and other sensitive information.

What can I do to increase my security?

Ensure you're connecting to a legitimate Wi-Fi network. Anyone can create a free Wi-Fi hotspot, and names can be reused, allowing cybercriminals to impersonate legitimate hotspots. To ensure a safe connection, check the hotspot name on signage or confirm with venue staff. Turn off features like "auto-join" for public networks. Opt for networks that require a password and avoid open or unsecured ones. After use, remove the hotspot from your Wi-Fi settings to prevent automatic reconnection. If in doubt, do not connect. Wait for access to a trusted network like your home or office.

Use a VPN (Virtual Private Network). If you're concerned about someone intercepting your information, a VPN can help by encrypting your internet traffic. A VPN works by taking your data, encrypting it, and then sending it to a separate server located elsewhere on the internet. Once the encrypted data reaches this server, it is decrypted and forwarded to its final destination. This process disguises both the content of your web requests and their destination while travelling over public Wi-Fi, making it appear that the requests are coming from the alternate server. As a result, your IP address and location remain anonymous.

VPNs can be beneficial even when connected to a password-protected Wi-Fi network, as hackers can still infiltrate these networks and potentially eavesdrop on your communications. Free and subscription-model VPN options are available for computers, laptops, tablets, and mobile devices. When choosing a VPN, research the provider and its privacy policies. Since VPNs can access user data, it's important to understand how they store and share information. Check independent reviews to choose well.

Turn on the firewall on your laptops. Most laptops have built-in firewalls, but some may not be enabled by default. A firewall helps protect your computer from potential hacking attempts through open connections. To see if your laptop's firewall is turned on, check the firewall settings in the Control Panel if you're using Windows, or look under System Preferences, then Security & Privacy if you have a Mac. Apple's iOS and Android

OS have firewall-like protections that control what apps can and can't do, limit interaction between apps, and prevent suspicious or unsafe connections.

Turn off file sharing, printer sharing, and discovery on your laptops. If your laptop is connected to the same public Wi-Fi network, the current settings could allow someone on that network to view and access files on your computer if those settings are enabled. You can disable these settings through the Control Panel on Windows or System Preferences on a Mac. When joining a new Wi-Fi network, you may be asked to select whether the network is public or private. Selecting "public" will also automatically disable file sharing.

Use HTTPS. Most major browsers and websites offer HTTPS, which you can identify by the "s" at the end of HTTP or a lock symbol. Although cybercriminals have been luring unsuspecting people to malicious sites that look secure, an HTTPS connection is still recommended, especially when accessing an open or public Wi-Fi network, as it encrypts the information exchanged between your browser and the website you visit. It's important to remember that while HTTPS encrypts the content of your communication, it does not hide the destination. This means that if a hacker monitors your connection, they may see that you visited Facebook, but they won't be able to view your username or password. Most web browsers provide extensions that will automatically connect you to an HTTPS version of a site when it is available. If your browser displays a warning message when you try to visit a website, stop using the Wi-Fi network, disconnect, and 'forget' it on your device. Learn how to turn on HTTPS at "HTTPS Everywhere".

Run antivirus/malware software. The most significant risk posed by hackers is the potential to infect your devices, such as laptops, tablets, and smartphones, with viruses and malware. Hackers can compromise your device with malicious software if you are vulnerable and you connect to an open network, like public Wi-Fi. To protect yourself, audit the apps on your device and run antivirus and anti-spyware software. Antivirus software will scan your device and any downloaded files for malware, and if it detects any threats, it will prevent the malware from being installed. Turning off your device for several minutes regularly can also knock off weak forms of malware and improve functionality.

Update the security software on your devices and perform regular backups. Hackers can exploit vulnerabilities in your devices, including how they connect to the internet. When such vulnerabilities are identified, companies typically release security updates to fix them. Therefore, scheduling regular backups and updating your device, software, or apps is important whenever an update is available. However, keep in mind that some older devices (like specific Android mobile devices) or operating systems may no longer receive security updates. Consider following the other advice in this article or upgrading to a newer device or operating system.

Be careful with public Wi-Fi hotspots without passwords. Some people choose not to use public Wi-Fi due to concerns about hackers accessing their devices and personal information. However, others weigh the benefits of having internet access against these risks. In such cases, some public Wi-Fi networks may be safer than others.

Be cautious when connecting to Wi-Fi hotspots that do not require a password. These open networks allow anyone to connect, making them easy targets for hackers. Additionally, be wary of Wi-Fi hotspots in busy locations, such as airports, where many people are logging in simultaneously. The high volume of users on one network can attract cybercriminals looking to exploit vulnerabilities.

Turn off Wi-Fi. If you're not using public Wi-Fi or have finished, turn it off on your device and "forget the network" to prevent your device from reconnecting automatically and becoming vulnerable to hackers. You can easily enable it again when you need it. While you're at it, consider turning off Bluetooth as well. Like Wi-Fi, Bluetooth can be exploited when enabled in public spaces, as it works over shorter ranges and has its own security vulnerabilities.

Resist accessing sensitive accounts and ensure you use MFA. When using public Wi-Fi, it's crucial to avoid accessing sensitive accounts, such as your bank, email, or any accounts that contain personal information. There is a risk that hackers could intercept your online activities, and the Wi-Fi network administrator might also be able to see which websites you visit and could potentially sell your data. Before checking these accounts, wait until you are connected to a more secure network. Additionally, consider using 2-step verification or multifactor authentication (MFA) on all your accounts for added security.

Use a privacy screen and a Faraday bag. Lastly, don't overlook the presence of that nosy neighbour who might be watching what you're doing. They don't need hacking skills to see the websites you visit or what you're typing on your screen. Consider using a privacy screen protector on your laptop, tablet, or mobile device to enhance your privacy. This way, others won't be able to see your screen unless they look directly at it. Additionally, Faraday bags can block all wireless signals and shield your electronic devices, helping to prevent hacking, tracking, and spying.

Follow solid laptop, mobile, and internet practices. The best way to protect yourself is by adopting good security practices on your laptop or mobile device, or while online. Encrypt your data, resist leaving devices unlocked and unattended, and explore Wesnet's additional resources for helpful tips and advice.

Could my abuser hack my device while I'm on public Wi-Fi?

Many survivors worry about whether their abusers can hack their devices when using public Wi-Fi. It is possible for someone to gain access to your device or eavesdrop on your internet traffic while connected to the same public Wi-Fi network. However, this typically requires the hacker to possess specific skills, tools, and knowledge about the network. If the abuser is not on the same network, the chances of them being able to remotely hack into the network to access your information are low.

If your abuser has already gained remote monitoring access to your devices, it doesn't matter whether you connect through public Wi-Fi, your home Wi-Fi, or mobile data—they will still be able to monitor your device. If you find yourself in this situation,

please refer to Wesnet's other computer and mobile spyware advice for further information.