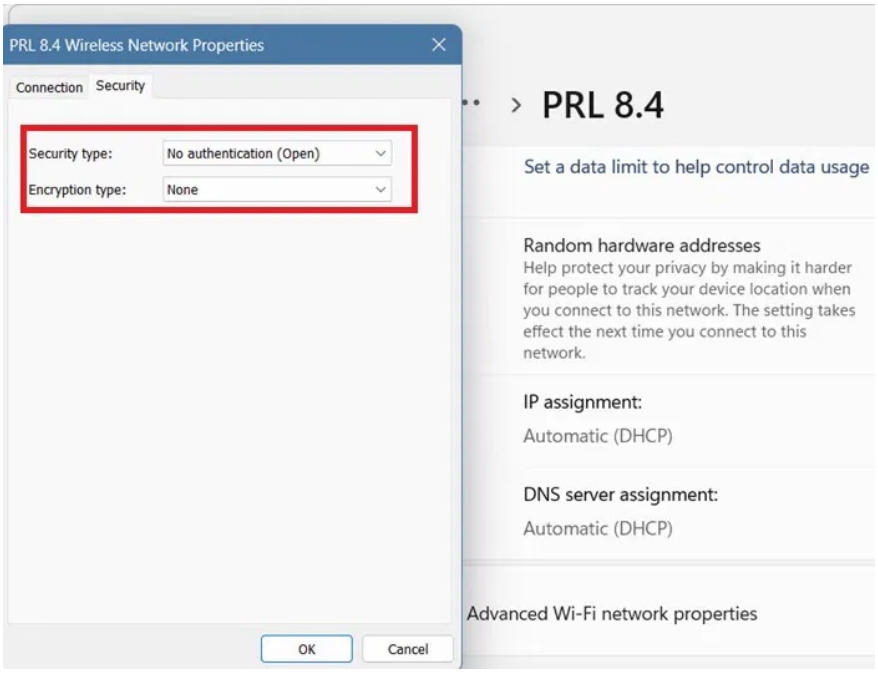
Should You Use Public Wi-Fi in 2025?

Nowadays, free wifi networks are installed everywhere, from coffee shops, amusement parks, shopping malls, etc. This is very convenient for us users to be able to connect to the network everywhere to surf Facebook and work. However, is using free wifi safe?

While Wi-Fi security is more advanced in 2025, it's not perfect. The following threats continue to emerge, so think twice before browsing on an unknown connection.

1. Old Wi-Fi protocols still exist

Many people still use public Wi-Fi networks normally to send emails and watch videos, seemingly oblivious to the potential risks.



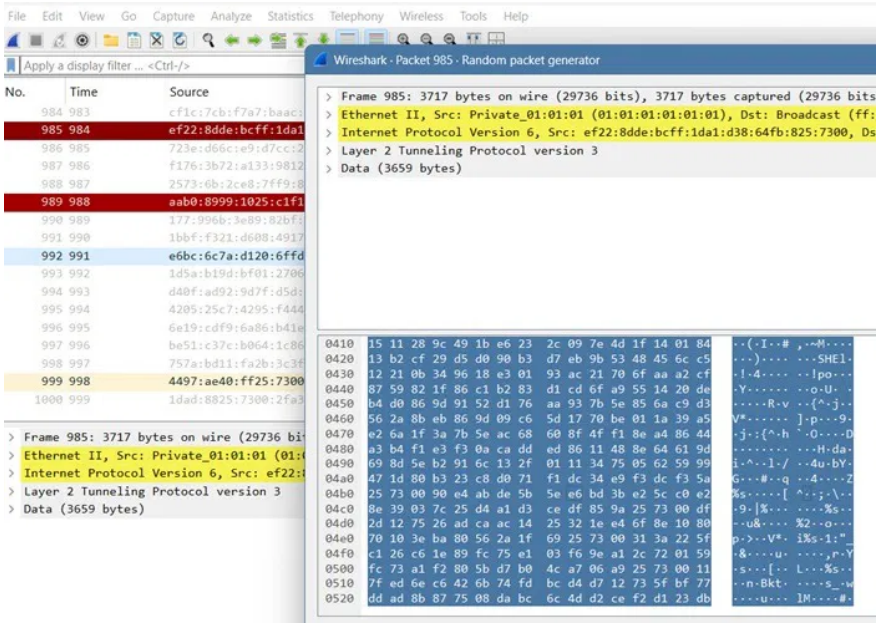
In addition to open Wi-Fi networks, you can still find older protocols like WEP and WPA. If you're in a hurry, you might connect to these networks without verifying their integrity. These older networks have weak encryption and are vulnerable to hacking and session hijacking tools.

To help you stay safe, here are a few different methods for checking your Wi-Fi network's encryption on Windows, Android, iOS, and Mac—especially useful if you're traveling internationally or living as a digital nomad .

2. Lack of Forward Secrecy – A Challenge with WPA2

The biggest challenge with WPA2-AES or WPA2-TKIP is the lack of forward secrecy. Public Wi-Fi networks continue to use simple passwords that are shared with everyone. Anyone with access to this key can decrypt all past or future sessions on the network.

Penetration tools like Wireshark provide a glimpse into captured SSL/TLS traffic. If someone has access to the server key, they can decrypt all the data. This can potentially expose login credentials, emails, etc., so using a VPN is important on public Wi-Fi networks as it encrypts all your data transmissions.



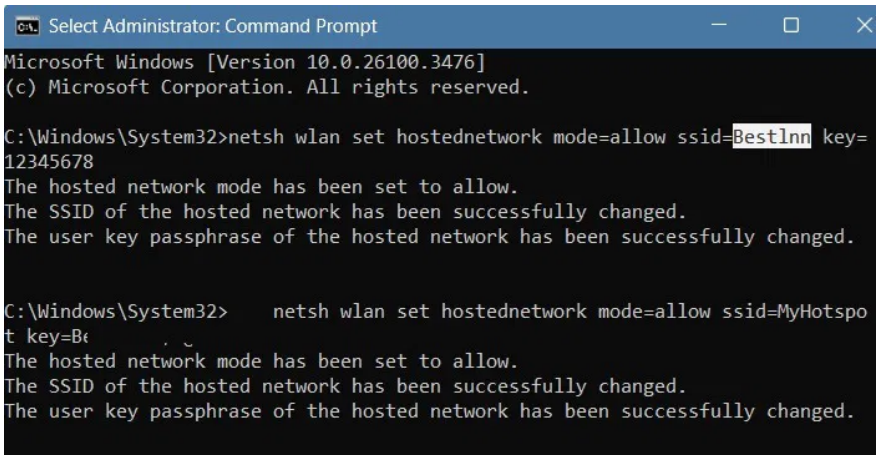
WPA3 is the gold standard for Wi-Fi security, providing strong protection against the above attacks. It uses Simultaneous Authentication of Equals (SAE), which encrypts each user session separately. You may have encountered this at airports, where a unique session key is generated after you share your passport number.

While WPA3 is highly secure, unfortunately it will take a few more years before it is widely used in public places.

3. The real problem of fake hotspots

As many frequent travelers have begun to notice, fake hotspots are becoming a big problem in hotels and other public places. Essentially, anyone can create a fake SSID to mimic the original SSID provided by your location.

All the crooks have to do is enter a set of commands that look similar to the original Wi-Fi hotspot. For example, instead of a hotel name like 'Best Inn,' the 'I' might be replaced with a lowercase 'L.' Hackers even copy captured portals and logos to give it an authentic look.



Again, the best way to spot a fake hotspot is to check the Wi-Fi encryption protocol it uses. Of course, they won't use WPA3 to protect your session. If there are multiple hotspots with the same name, you'll need to use a VPN or one of the alternatives.

4. Beware of hijacked browser sessions

Most websites today use HTTPS , but that doesn't mean all information is safe from hackers. HTTPS protects the content of your communication, but not the metadata.

If you're using a public Wi-Fi network on secure WPA3, you'd think all the security holes would have been patched. But hijacking can attack your device on a public network – even if you're on a very secure connection. Session hijacking involves hackers taking over your browsing data through account takeover (ATO) attacks or malware, which can originate on the dark web .

The human factor is one of the biggest reasons behind these attacks. Your identity is at the heart of device security. On Android, you can use Identity Check to prevent your device from being taken over. Similarly, iOS, Windows, and Mac devices also use biometric authentication to prevent your accounts from being taken over.

Safety precautions when using public Wi-Fi

While the risks of public Wi-Fi have decreased significantly compared to a few years ago, they are still very common in 2025. However, you can still use public Wi-Fi, as long as you remember to keep the following safety precautions in mind:

1. Always keep your browser and operating system up to date.
2. Use only top VPN apps for iPhone and Android to encrypt your connection.
3. Use antivirus software on your desktop device. This software should include a firewall , email and web protection, and anti-phishing protection.
4. Enable two-factor authentication (TFA) on all important user accounts.
5. This feature is quite useful to combat the latest threats, such as QR code phishing .
6. Do not automatically connect your device to unknown Wi-Fi networks. Verify the encryption protocol used for each user session.

7. Use mobile data when in doubt. If you're doing financial transactions or anything very sensitive, it's safer to stick with your mobile data plan.

You finished reading the article "**Should You Use Public Wi-Fi in 2025?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com