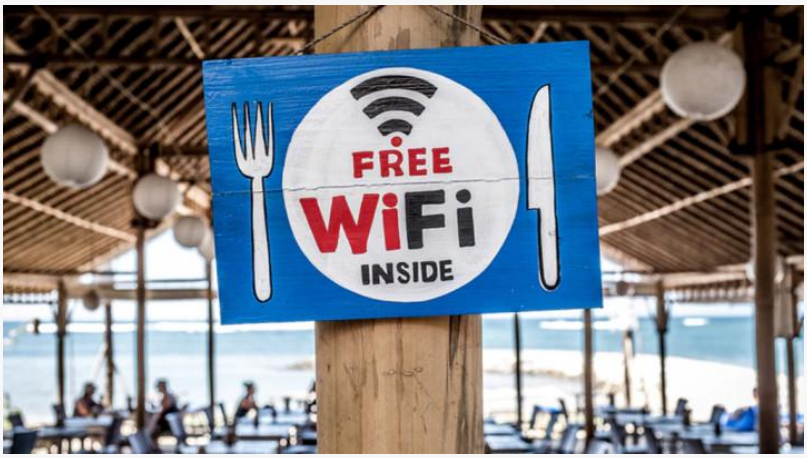
How to Safely Use Public Free Wi-Fi

How to Safely Use Public Free Wi-Fi

WASHINGTON, USA, October 21, 2021 /EINPresswire.com/ -- Public Wi-Fi is everywhere, from the hotels to the local coffee shops and airports. Free Wi-Fi is covered in almost all public places. “According to a recent survey, 53% of the smartphone/mobile phone owners and 70% of the tablet owners said they use the free public Wi-Fi spots.”

Speedefy Logo 1



Free Public WiFi

Public free makes life easier and convenient when people have to do large traffic online work. People can easily check emails on the move, surf the web and keep themselves updated on social media. However, the data users send through public Wi-Fi can easily be spied on, intercepted, and transmitted across the link by hackers.

Public Wi-Fi risks have been increased due to the explosion in free Wi-Fi at public places, and many laptops and mobile users are risking their digital identity, personal info, and money. Furthermore, if the device is not protected by an effective anti-malware security product, the risks could be even higher.

Protect Users Information When Using the Public Wi-Fi

No doubt, public Wi-Fi attacks are common, but there are ways by which users can protect themselves from threats and risks. Some of them are as follows:
- Stay With VPN (Virtual Private Network)

If Users use a VPN while connecting to the public Wi-Fi network, users efficiently use the private tunnel that encrypts all of the data that moves through the network. This measure can help hinder the cybercriminals that are hiding over the network and stop them from catching users' data.

iPhone

- Never Sign-in to the Accounts Permanently
Always make sure users are logging out from all of the users' accounts. Also, don't sign in permanently to any public account.

- Don't Giveaway too Much Info
Be very conscious of when signing up for public Wi-Fi access. If users are being questioned for a bunch of users' personal information like phone number and email address, only stick to the platforms users recognize and trust. Users can also provide an email that is not the users' primary email.

- Don't Use the Same Passwords Everywhere!
If users are using the same passwords while surfing through the public networks, users need to stop there! Because it could provide someone access to those accounts which have the same passwords by only achieving accessibility to one of the users' accounts.

- Avoid Using Sites With Red Signals
Many web browsers alert the users before they download a malicious program or visit a scammy website. Please don't ignore such warnings and also keep the browser's security up to date.

- Never Access Users Financial and Personal Information
While using the free public Wi-Fi, always assume that this network is unsafe, and users should not access users' personal info until they have a reliable network.

While guarding against the risks of public Wi-Fi, home routers should be equally guarded against risks, and having a secure router like Speedefy KX450 can provide a safe online environment.

Key Takeaways
Remember, any devices like laptop, smartphone and tablet is at risk when using public Wi-Fi. Understand that free Wi-Fi is risky to prevent leaking personal information. Some tips mentioned above are simple and easy to remember, which helps users avoid network traps.

Speedefy Marketing Team

www.speedefy.com
+1 610-674-6618
email us here
Visit us on social media:
Facebook