

Tips For Staying Safe On Public Wi-Fi Networks

Public Wi-Fi is a boon in today's digital and borderless world.

With many shops, shopping malls, restaurants, airports and public transport offering free wi-fi facilities, it has become convenient for citizens to stay up to date with their educational, professional & social activities when they are out and about.

Public Wi-fi helps in building a well-connected society by encouraging more agile interactions between citizens & service providers. A technologically advanced place offers convenience and attracts tourists & businesses, ensures inclusion and helps underprivileged.

In India, the government has launched PM WANI (Prime Minister Wi-Fi Access Network Interface) initiative intending to make Wi-Fi prevalent across public spaces. This will ensure Wi-fi availability across lengths & breadths of the country.

While many users are aware of the benefits of the public Wi-fi network, not many are well informed about its security risks.

Not only internet users but public Wi-fi also attracts cyber criminals, online predators and hackers. The data transferred using public W-fi networks can be easily intercepted & many electronic device users risk their personal

information, money & online identity. The risk of the security breach is greater when the electronic devices are not protected by adequate security software products.

Public Wi-fi is the favourite target spot of cybercriminals as multiple users are already connected to it. A hacker gains access to the network & intercepts the communication between the users & the router. This is called the Man in the Middle (MITM) technique; by deploying this tactic the hacker can control the data, steal your online identity & share files infected with malware.

Another way a hacker can access your personal information is by creating a fake Wi-fi public network. The uninformed users may join the network. Consequently, sabotaging their sensitive information & giving the cybercriminals abundant opportunities to use the data for illegal activities.

Users can avail of the benefits of public wifi networks by ensuring that they are well-protected & following some preventative measures.

Here are some tips for staying safe on public Wi-Fi networks:

1. Verify the Wi-fi network

It is important to ensure that the network is legitimate. Confirm the offering IP address & double-check the name with the owner.

2. Choose your sharing preferences.

Switch off your file sharing preferences to avoid receiving any virus-infected files from the hackers.

3. Use a VPN

A VPN (Virtual Private Network) prevents hackers from intercepting your data by creating a private & protected tunnel between the users & the router. It encrypts your data and hides your IP address.

4. Visit HTTPS sites.

Websites with HTTPS address encrypt the data between browser & web server. Thus, preventing any potential data security breach.

5. Install Anti-Virus software & security solutions.

Antivirus software alerts the system in case any virus is present in the files being sent or received.

Avoid falling prey to the threats of using public Wi-Fi network by following these easy & inexpensive tips. Digital safety is important! Maximize your security & surf the internet on public Wi-fi networks with extreme caution.