How to Stay Safe on Public Wi-Fi

Using public Wi-Fi can expose your device to numerous security risks, including data theft, malware infections, and unauthorized access. When connecting to unsecured or shared networks, it's essential to take steps to protect your personal information and devices. Here are some critical precautions for maintaining security on public Wi-Fi:

Use a Virtual Private Network (VPN)

A **VPN** encrypts your internet connection, ensuring that data transmitted between your device and the network remains private. It helps prevent hackers from intercepting sensitive information such as passwords or financial details.

Enable Your Firewall

Ensure your **firewall** is turned on to monitor and control incoming and outgoing network traffic. Most operating systems enable it by default, but it's wise to double-check before connecting to public networks.To enable the firewall on MacOS, check out these links below:

- **Change Firewall settings on Mac**
- **Block connections to your Mac with a firewall**
- **Use stealth mode to keep your Mac more secure**

Install and Update Antivirus Software

Use reputable **antivirus software** to detect and block malware or suspicious activity. Keep it regularly updated to ensure protection against the latest threats.

Browse Only on HTTPS Sites

When visiting websites, look for **HTTPS** in the address bar. HTTPS encrypts your connection, reducing the risk of attackers intercepting your data during transmission.

Keep Your Operating System Updated

Regularly install updates for your **Windows** or **macOS** system. Security patches fix vulnerabilities that cybercriminals could exploit on unsecured networks. Check out **How to install Windows Updates** and **Update macOS on Mac**.

Connect Only to Password-Protected Networks

Whenever possible, choose **Wi-Fi networks that require a password**. Open networks are more susceptible to attacks because anyone can connect without authentication.

Enable Two-Factor Authentication (2FA)

Turn on **2FA** for your online accounts. Even if your password is compromised, an attacker would still need a secondary verification method to gain access.

Forget Networks After Use

After finishing your session, **disconnect and forget the network**. This prevents your device from automatically reconnecting to potentially unsafe hotspots later.

Use a Personal Hotspot Instead

When possible, use your **mobile hotspot** instead of public Wi-Fi. Personal hotspots are typically encrypted, less crowded, and far less likely to be targeted by cybercriminals. They also offer a more stable and private connection.

Final Thoughts

While public Wi-Fi is convenient, it is inherently risky. By using a VPN, enabling firewalls, keeping your software updated, and avoiding open networks, you can dramatically reduce your exposure to cyber threats.