In this presentation, you're going to learn the five ways to protect yourself against cyber attacks when using public Wi-Fi. There is no denying that public Wi-Fi can be a hotbed for cyber attacks, particularly man-in-the-middle attacks and similar methods. To protect yourself, we're going to give you a list of five ways to stay safe. So let's get right to it.

## Use a Virtual Private Network (VPN)

The first method we'll look at is using a Virtual Private Network (VPN). It is highly recommended to use one when you are on public Wi-Fi. A VPN creates a secure, encrypted channel between your device and the Internet, protecting your Internet traffic from interception. Additionally, a VPN will mask your IP address, making it more challenging for a hacker to track your online activities.

Be sure to choose a reputable VPN service and install it on the device you typically use. Connect to the VPN before you connect to the public network. When you're on public Wi-Fi, make sure the VPN remains on.

## Enable Two-Factor Authentication (2FA)

Another measure you can take is using two-factor authentication (2FA). If available on any accounts you use, make sure to enable it. This serves as a second verification method that confirms you are truly logging in to your account. You could enter a code sent to you via email or SMS, or use biometric authentication such as a fingerprint or face scan.

## Avoid Accessing Sensitive Information

When using public Wi-Fi, avoid accessing sensitive information such as online banking, personal email, or anything tied to your identity. This is because cybercriminals seek personal data. However, if you must access such information while on public Wi-Fi, remember to use a VPN.

## Keep Your Software and Devices Updated

It's essential to keep your devices and software updated regularly. Most updates include security patches that address vulnerabilities. The operating system, browser, and apps on your device need to be updated accordingly.

Enable automatic updates for your operating system and apps, and check for updates regularly. You can also update them manually if necessary. Ensure your antivirus software is also updated for optimal protection.

## Use HTTPS Connections

Lastly, check whether the websites you visit use HTTPS instead of HTTP. The "S" in HTTPS stands for secure, indicating that the connection is encrypted, particularly in data transmission between your device and the website. Look for the padlock symbol in the address bar of your browser next to the URL. If the symbol is missing, you may want to leave the website immediately.

## Conclusion

While public Wi-Fi offers convenience, it also lacks security. So please use these five ways to protect yourself against cyber attacks, especially when you use public Wi-Fi regularly. Thank you for checking out this presentation. We appreciate it greatly. Be sure to follow these steps and more for a safe internet session.