

5 applications to secure Wi-Fi Hotspot connections

Do not allow eavesdroppers to capture passwords, emails and other sensitive data. In this article, I will show you some useful applications that can encrypt wireless traffic.

***Network administrators* - Do not let eavesdroppers capture passwords, emails and other sensitive data. In this article, I will show you some useful applications that can encrypt wireless traffic.**



Most Wi-Fi hotspots do not use encryption to protect web browsing and other actions on the Internet like private networks. In addition, encryption does not exist on most wired connections you connect at hotels, airports or other public locations. Securing all public networks is impossible.

However, users can easily protect their Internet sessions to prevent nearby Wi-Fi users from snooping around the sites you are visiting and can capture email, passwords and information. Your other sensitive.

You can use a solution called Virtual Private Network (VPN), which is designed for secure access to remote networks. In this public network security scenario, a VPN server is hosted by a company, such as a company that we will discuss below. These companies will also provide VPN client applications, which you need to install on your computer.

When connecting to your company's VPN server, wherever you are, all your Internet browsing and traffic will be routed into and out of the corporate network through an encrypted tunnel on the Internet.

VPNs provide several advantages for protecting network traffic to avoid eavesdropping:

1. They ignore filtering to see blocked websites.
2. They use limited services: like VoIP, chatting, and instant messaging.
3. Hide your IP address - surf anonymously
4. Avoid Internet restrictions of a certain country.

There are several variations in VPN solutions. The most common for public network security is VPN based on SSL, which is the solution that uses encryption for sites that need security such as government sites and banks.

No need to bother, here are 5 hotspot applications and services that you can use to secure your public web browsing.

1. UltraVPN

This solution is based on the popular OpenVPN client / server. Fortunately, they follow strict open source methods and do not include ads to increase their income - OpenVPN is really free. Plus OpenVPN does not impose restrictions on traffic, so you can use the service comfortably if you want.

UltraVPN client is basically a modified version of the OpenVPN client, provided for Windows and Mac OS X. The settings are pre-configured, in addition to a system tray icon, a custom GUI. Provide a more user-friendly experience.

Linux users can download UltraVPN source code and create binary files. UltraVPN servers are hosted by Lynanda.

Although you have to create an account to use the service for free, the process is very simple. All you need to do is enter your username and password. No need for email authentication or even addresses.

When installing on Windows, you will see an icon appear in the system tray. To connect, right-click the icon and select **Connect** .

This icon also has shortcuts to Proxy settings if needed.

2. Hotspot Shield of AnchorFree

Although this is a free application, you will be offered utilities to prevent viruses and spyware, browser tools and other features during the Hotspot Shield installation process.

If you do not have these features on your computer, this is a very useful way, but most of it will make users feel annoyed.

Even worse, Hotspot Shield intercepts an ad bar above most websites you watch while connecting to the service.

However, Hotspot Shield is a free utility and it can completely protect your Internet actions. Currently Hotspot Shield is providing users with 5 GB of space per month, enough space for normal use cases on insecure networks.

Hotspot Shield also supports Windows 7 and Mac OS X Snow Leopard.

When installing in Windows, you will see an icon appear in the system tray. At a glance you can see its different colors, when you move your mouse over it, you will see the connection status immediately: connecting,

connected, or disconnected with the VPN service.

To summon the connection properties window, click on the icon and select **Properties** . A simple web interface will appear, in this interface you can see the connection status and know other details about the connection: VPN IP address, server VPN address, bytes sent. and receive, the time you connect.

To disconnect from the service, click on the icon and select **Disconnect** .

3. FreeVPN of WSC

This solution not only supports Windows 7 and earlier versions but also supports Apple's iPhone and iPad. However, to use this free service, you must encounter many ads.

Every time you connect to the VPN service, it will change your browser's homepage to its custom search engine. There is no change back to your original home page when you cancel the connection and you must do it yourself if you wish.

Installing FreeVPN client is very simple. When you open the program, you will see a small program, ready to allow connection to many different VPN servers in many different countries.

If paid, users can enter their login criteria to disable ads and allow large amounts of usage when connected to the service. On the client side, you will see a location to enter Proxy settings if needed.

4. iPIG of iOpus

IOpus VPN server and client is a free and open source service for Windows. With it, users will not see the annoyance of appearing ads during the installation process on the client. However, you will have to create an account to use the service.

In addition, this free service is also restricted to free 10 MB traffic; In order to use excess traffic, you need to pay to get it.

When you exceed the traffic limit, you can install and use your own iPig VPN server for free.

After installation, an icon will appear in the system tray. Double clicking on this icon will appear the client application.

If you don't have an account, you can click the shortcut button to create an account. Then, enter the username and password, click **iPig On** , and now you are protected when accessing the web.

Note: The settings in the client provide some advanced controls.

For example, block traffic if it is not possible to encrypt, encrypt UDP traffic (like DNS) and even enforce or aggregate traffic to encrypt.

5. CyberGhost

This is a company that provides free and fee-based services of Germany. Monthly traffic is limited to 1GB, enough space for most users to occasionally surf the web in public. However, you will get a comprehensive and safer solution with a fee-based service.

The installation process is quite simple. However, it still needs components like Microsoft .NET 3.5 Framework, but the CyberGhost installer will download and install it yourself.

When launching the client for the first time, you will see an account creation button. It is not complicated, but you must perform an email verification.

When you log in, you will see the main CyberGhost client. To use the free service, press the **Connect Basic** button and wait a moment to be connected.

From the client, you can also see usage performance, settings, and exceptions. When closing the client, you will still have an icon in the system tray.

Right-click on it you can find shortcuts in the menu that appears.

You finished reading the article "**5 applications to secure Wi-Fi Hotspot connections**" 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.