

VPN for Travel: Quick Setup Tips (5 Basics You MUST Know)



A virtual private network (VPN) allows you to use the internet as if you are on a different IP address in a different country or city. Whether you're a business professional working remotely or a leisure traveler, setting up a VPN is crucial for various reasons. Here, we'll look at what a VPN does and the basics you must know for setting up a VPN while on the go.

In essence, the primary function of a VPN is based on **encryption**. This means that a VPN, using encryption protocols, converts information into a code that is unreadable. It protects your sensitive information from being intercepted and read, such as personal data, login credentials, and financial information.

Encryption makes this data unreadable to anyone, so the data exchanged between your device and the websites or online services you are accessing will be secure.

By using encryption and masking your IP address, a VPN allows you to **bypass geographic restrictions**, granting you access to region-locked content and websites.

To use a VPN while traveling, sign up for a reputable service, download the app, and connect to a preferred server for secure, fast, and uninterrupted online access to critical services. Once connected, your IP address will be hidden, location spoofed, and traffic encrypted.

Let's dive into the **setup process** - something that some travelers may be a little intimidated by if they don't see themselves as technical or tech-savvy.

1. Choose a VPN Service

Selecting a reliable VPN service is the first step in setting up a VPN for travel. There are numerous options available, ranging from free to premium services.

It's easy to get stuck in deciding due to the plethora of good choices available.

Selecting the best VPN for travel involves choosing a reputable service like ExpressVPN, NordVPN, or Surfshark VPN. These are just three examples of VPN services that are well-known for their security and extensive global server networks.

Prioritize features such as a wide server network, fast connection speeds, and device compatibility.

You should ideally avoid free VPNs due to bandwidth limits, fewer servers, and slower speeds.

In summary, here are three top attributes of a good VPN service you should look out for, besides security:

- **Server Network:** When selecting a VPN for travel, the **number** and **locations of servers** offered by the provider are significant factors. A VPN with a vast network of servers around the world ensures that you can access region-restricted content and enjoy a stable, high-speed connection. This is particularly important if you are traveling to countries with strict online censorship laws.
- **Connection Speed and Performance:** Speed is crucial. Some VPN services, especially free ones, may impact your connection speed. Look for providers with high-performance servers.
- **Device Compatibility:** Ensure the VPN supports the devices and platforms you use, whether it's Windows, macOS, Android, iOS, or others. Check for the **number of simultaneous connections** allowed on a single subscription - this detail is especially important for travelers who might access a VPN on both their phone and tablet/laptop.

Don't get stuck at this step. Pick a reputable VPN service and move - there are many decent options so just pick one. You'll see why this is important in the [subsequent section](#).

To reiterate, select any reputable VPN service you can afford that has a vast server network on a global scale and offers strong, fast, and reliable connections across a multitude of devices.

2. Purchase a Subscription

Once you've chosen a provider, sign up for a plan that suits your needs.

Some of you might've decided on a free VPN service. Despite the disadvantages, some free VPNs offer reasonable speeds and adequate server locations, amongst other benefits. Yet, if you're new to using a VPN, I recommend that you opt for a **cost-effective subscription** with a **premium VPN service**, instead of a free VPN.

Even if you have absolutely no budget for a premium service at the moment, there's still a way to utilize a top-tier VPN service at zero costs - which I'll now discuss in this very section.

True, some 'free' VPNs may offer free usage initially, attracting a larger user base.

However, these free versions typically come with limitations, and the "catch" is that users are encouraged to upgrade to subscription tiers for enhanced features and better performance. The costs associated with upgrading to premium plans are usually much higher, compared to plans offered by reputable VPN providers in the first place.

On the other hand, premium VPN services offer several advantages that free VPNs lack:

- **No Bandwidth Limits:** Compared to free VPNs that limit your usage, premium VPN services usually offer unlimited bandwidth. They allow unrestricted usage, such internet speeds and overall performance are not compromised.
- **Server Options:** Premium VPNs usually have a more extensive server network, providing you with a greater number of server locations to choose from. This is beneficial if you want to access content from specific regions or improve your connection speed by connecting to a nearby server when you travel.
- **Reliable Performance:** Premium VPN services invest in infrastructure and technologies to ensure more reliable and stable performance, minimizing disruptions during your online activities.
- **Customer Support:** Premium VPN services typically offer dedicated customer support, helping you troubleshoot issues and address concerns promptly.

So, how do you select a subscription plan for a 'premium' reputable VPN company, if you're new to this?

Premium VPNs (like Surfshark, ExpressVPN, and NordVPN) often offer a **7-day free trial** and **30-day money back guarantee**.

I'd suggest that you take advantage of the free trials and money-back guarantees to sign up for their services, especially if you're newly utilizing a VPN for a short period of travel. After a trip, you can decide to discontinue the service before the free trial expires, or even cancel your subscription *within a month*. This way, you get your money back.

In this manner, you get to experience the full range of services, including advanced security features, a wide server network, and internet access that is fast, consistent, and unrestricted.

This is why you'd want to purchase a subscription, even if you ultimately spend \$0. It's technically a plan purchase since you'd have to fill in your debit card information. But the potential benefits outweigh any perceived 'hassle,' if there is any inconvenience at all.

3. Download and Install the VPN App On Your Laptop and Phone

Depending on the VPN service, the process of setting up a VPN can vary in complexity, but is often simple enough. Many VPN providers aim to make the setup process user-friendly, even for those without extensive technical knowledge.

To address technical concerns and encourage VPN adoption, VPN providers usually offer user-friendly interfaces, step-by-step setup guides, and even customer support.

The next step after signing up for a VPN service is to **download and install the VPN application on your devices**.

Most VPN providers offer applications for various platforms, including Windows, macOS, Android, and iOS. Download the application onto your device. Then, follow your chosen VPN service's (usually simple) instructions to complete the installation.

Launch the VPN app and log in using the credentials you created during the signup process.

During this step, ensure that you download the app onto both your laptop AND phone, **especially your phone**. It's common for people to install apps on their laptops and overlook their phones.

When you're on the move, your phone is often the most easily accessible device, serving various purposes from productivity to leisure.

A good VPN app on your mobile phone will enable you to bypass any geo-restrictions to critical content or services while staying secure, ensuring that your personal, business, and corporate life does not get disrupted. Wherever you are, you ensure continuity and stay connected.

4. Choose a Server Location and Connect

After logging in, your VPN app will connect you to the VPN server and initiate the encryption process for your internet connection.

Now, you'll have the option to choose a server location.

Choosing the right server location when using a VPN overseas is an important decision that can impact your online experience.

How do you decide which country you should connect to when using a VPN overseas? In fact, should you set your VPN to a different country?

To select the ideal VPN server location, prioritize server proximity for speed, and choose a server in a country without restrictions if your aim is to bypass geo-restrictions. In essence, opt for a server close to your country that provides the necessary access to content and services.

Here are the main factors to consider:

- **Server Proximity:** Connecting to a server **close to your physical location** can improve your VPN connection speed and internet performance. This is because

when your server location is far away, it normally takes time for the data to travel from the server to your device.

- **Bypassing Restrictions:** If your primary goal is to bypass geo-restrictions or censorship, select a server in a country **where the content or service you want to access is not restricted**.
- **Geographic Location:** If you want to access region-specific content or services, **choose a server in the location where that content is available**. For example, if you're in Asia and want to access content (such as movies and shows) only available in the United States, connect to a U.S. server.

5. Configure Additional Settings (If Desired)

You may want to explore the settings menu of your VPN application to configure additional options.

Advanced options are too advanced to go into detail here, but there are a few main ones. One is a **kill switch**. A kill switch serves to automatically disconnect your internet if the VPN connection drops, so this prevents your internet traffic from getting exposed without the protection of encryption.

Another setting is **split tunnelling**. It basically allows you to direct *some* of your internet traffic through the encrypted VPN tunnel, while allowing *other* traffic to travel directly over the unencrypted public internet. This can lead to improved internet speeds, as certain data can bypass the VPN encryption, reducing processing load.

Finally, you want to ensure you're connected to VPN in times of need. The setting is simply your "connection status".

Most VPN providers offer a user interface with a visual indicator, such as an icon or symbol, that displays the current connection status. Check the VPN client for indicators such as a 'connected' status, the server location you are connected to, and any error messages that might indicate an issue. This will indicate whether you are in fact connected to the VPN or not.

Conclusion

Setting up a VPN for travel is a straightforward process that significantly enhances your online freedom.

Follow these simple steps, starting from selecting a reliable VPN service.

You can ensure that your internet connection remains secure and unrestricted from any corner of the globe, allowing you to make the most of your travels.