Using a VPN for security

Description

- # Using a VPN for security

  It is possible for people to steal the data transmitted over your internet connection, stealing details such as credit card details and personal information. That’s why shopping website addresses start with “https” (the “s” stands for “secure”), and have the lock on them. The website sets up a temporary, very secure encrypted connection between you and its page, so you can safely transfer financial and personal information.

- ## What a VPN is and how it works

A Virtual Private Network (VPN) sets up a similarly secure encrypted connection for an entire internet connection. Regardless of what you're connecting to, people can't "see" – and therefore steal – your data. They are an excellent idea for providing security, but they can slow down your internet service significantly, particularly if you're using a satellite connection.

If the internet is a highway, a VPN is a fully-enclosed tunnel with password-protected toll gates at either end. Once the tunnel is created, either all your internet traffic, or specific parts of your traffic, is directed through the tunnel instead of going through the general public highway. You have one end of the tunnel. The other end is located at the VPN supplier. This can include:

- Your place of business.
- Your anti-malware software provider.
- Your commercial VPN provider.

Normally, when you connect to a website, mail server, streaming video service, or any other service provided over the internet, you connect to your ISP, and then to the relevant internet site. When you use a VPN, you'll have software on your computer, device, or router – different kinds of VPN may run differently. There are many different types of VPN software and suppliers, but they all work broadly the same way.

- 1
  Step 1

  Using the username, password, and server address provided to you, you first log into the VPN supplier, which creates the secure tunnel.

- 2
  Step 2

  Connect to your specific internet services, which will all go through the VPN supplier and tunnel instead of directly.

- 3
  Step 3

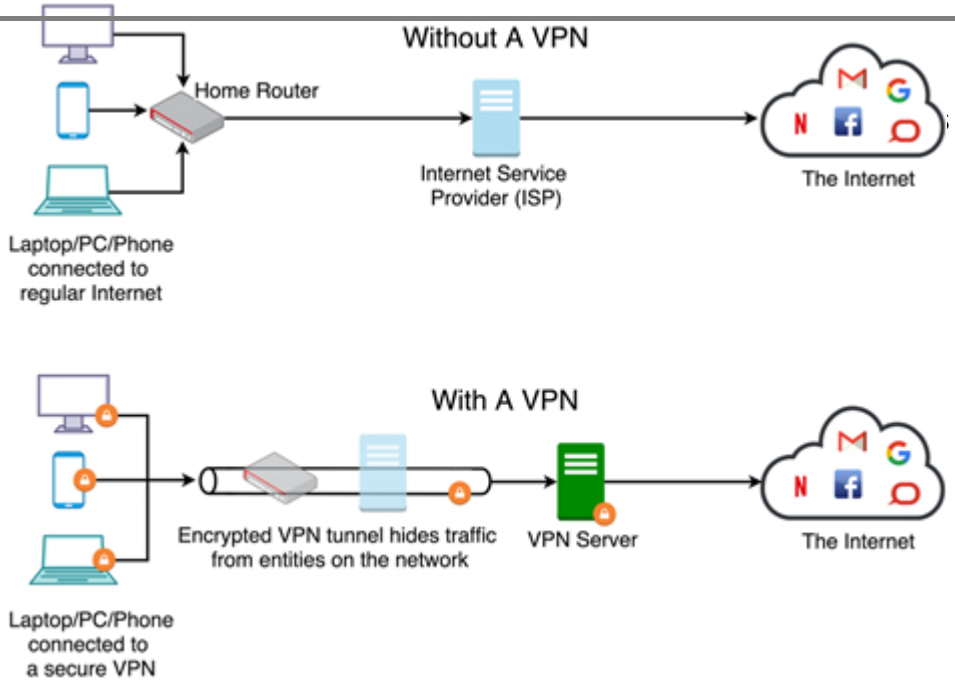
  Every piece of data you send and receive over a VPN connection is secured and checked before it goes along the tunnel.

Frequently Asked Questions

- 1What equipment do I need to run a VPN?

  VPNs can be applied or installed in one of two locations:

  1. **Your router.**This is the easiest and most secure option. Every computer or device that goes through the router will be running through that encrypted tunnel. You don’t have to remember to turn it on and off again.You can fine-tune your VPN router software to manage traffic, if you’re confident in tweaking router settings.However, if VPNs cause an excessive slowdown to your internet connection, a router-applied VPN will cause all your devices to be extremely slow.
  2. **Your computer or device.**This is a more flexible option. You can turn the VPN on or off using the software on your device, and you can keep one device for secure VPN use and one for faster connections.It means that any VPN slowdowns will only affect that one device, not all of them.However, it’s not as



you need it.

Illustration of a router-applied VPN. From “How a VPN secures internet activity”. Mohammad Taha Khan, The Conversation, Is your VPN secure? CC BY-ND.

- 2Do VPNs work on all connections?

  Yes, but it works best on connections with high speed and low latency. It can add a noticeable slowdown to even the fastest connection, due to the cross-checking done to keep the connection secure.

- 3Why are satellite connections a problem?

  Satellite internet connections have long latency. This is the time it takes for data to get from your computer to the remote computer via the satellite in orbit. VPNs can therefore be a particular problem over a satellite connection, as the latency makes the VPN software think the connection isn’t working properly, or that the connection is insecure, or simply times out.

  This can result in:

  - Being unable to make a VPN connection at all
  - Being able to connect, but the connection dropping out constantly.
  - The connection is holding stable, but every action is incredibly slow (for example, typing takes many seconds to display on the screen).
  - The connection is holding stable, but some software or services are not working,

either effectively or at all.

- 4How does a nbn® satellite connection work with a VPN?

  If you're on nbn® Sky Muster® Plus, VPN traffic is all metered, as nbn can't see what sort of traffic is being carried. You'll want to turn the VPN off to take advantage of unmetered services. Your VPN provider can also make adjustments to settings on the VPN software to make it work more effectively with a satellite connection.

  Some SpaceX Starlink satellite use may also be impacted, as some VPNs may restrict international IP addresses. This may mean some VPN services won't work without adjustments to their settings. Your VPN provider will have the best advice on what to do in this situation.

  You can find out more about nbn Sky Muster satellite connections and VPNs with the nbn-sky-muster-vpn-fact-sheet.

- 5How do I get a VPN?
  1. **Business or employer**If you need to access workplace office services, files, or software, your employer may provide you with workplace VPN details, in addition to other secure office equipment such as a laptop, mobile phone, or remote access token.Alternatively, they may use a cloud-based office service such as Microsoft Office 365, which requires secure logins but no VPN.
  2. **Anti-malware/virus packages**Many anti-malware packages now include a VPN. They claim this provides complete protection of your devices and of your connection.
     - The anti-malware package protects your computer and devices.
     - The VPN protects your connection, by encrypting everything sent over it.

     Packages with VPNs come from providers such as Norton, Kapersky, McAfee, Avast, and Bitdefender. Some run their own VPN computers, while some resell third-party suppliers.

     - PC Mag Australia: The Best Security Suites for 2024
     - Safety Detectives: 5 Best Antiviruses with VPN Included (& Both Don't Suck) in 2021

     If you plan to use the VPN included in these packages, check two things first:

     1. Where is the VPN server located? If the server is overseas, it may add noticeable slowness to your connection.
     2. Can you turn the VPN on and off as need be?

     If the VPN is turned on by default, it may be the cause of an unusually slow

internet connection. Test this by turning it off and re-checking your speed.

3. **Own purchase**There are many third-party VPN businesses you can use to secure your internet services, whether for home, business, office, farm, education provider, or other purposes.We do recommend discussing your needs with a trusted technical advisor. However, the following articles may give you a reasonable idea of the names, costs, and services available.While there are free VPN services available, look very closely at what they mean by “free”. For example, they may have fine print allowing them to sell your data, have very limited daily data (such as 200Mb), or deliberately slow down your connection until you upgrade to a paid service.
    1. Wired Magazine: The Best VPNs to Protect Yourself Online
    2. PCMag Australia: The Best VPN Services for 2024
    3. TechRadar: The best VPN service 2024

- 6Should I be using a VPN?

This isn’t a simple yes/no answer.

You can choose to add a VPN for your home or business internet connection, to keep your data, and your internet connection as secure as possible.

Most security articles will strongly recommend this.

Such security articles, however, are assuming their readers are based in cities, with a wide choice of connections available.

If you’re working from home, you probably won’t have a choice about using the VPN provided by your employer to keep the business files secure.

Ask yourself these questions when considering a home or small office VPN connection.

- Where are the VPN servers located? The closer the VPN supplier is to you, the faster your connection will be. Aim for Australian servers, preferably.
- How secure is the location? Check the fine print very carefully. VPN businesses are in it to make money. While they’re securing your data from everyone else, they can see it, and they have your data. Again, aim for Australian-based suppliers who are bound by Australian privacy laws
- What is the cost? Is it in Australian dollars?
- Will the VPN allow you to connect to everything you need? Some VPNs don’t connect effectively to streaming video sites such as Amazon Prime, Netflix, or Stan.
- Do you have enough data? VPN-encrypted data is between 5% – 15% larger

than unencrypted data. VPN data is also metered on an nbn? Sky Muster? Plus connection.
- Can you turn it off if you need to? How do you connect? Is the software easy to access and use?

General tips for using a VPN

- - If possible, apply the VPN on a computer or device only, and not your router.
  - If you're transferring large files, try to do this on off-peak times, so lighten the load on your VPN.
  - Turn the VPN off for video conferencing if possible. If not, consider using audio only.
  - If the VPN is supplied by your employer, ask the IT department to adjust the VPN settings on the remote access portal (the computer you log in to from home) to allow for a high-latency connection. They may need to speak to their VPN supplier to make this change.
  - If the VPN is applied on your router,

connect directly into the NTD to bypass it.

- If you have an alternative connection – for example, mobile broadband – reserve it for your VPN sessions and use that.
- Turn off the VPN when you absolutely don't need it, or when you're using unmetered content on an nbn? Sky Muster? Plus connection.
- When using the VPN, turn off everything else using the same connection.
- Close all unneeded apps or software on your computer or device.
- Keep VPN sessions as short as you possibly can.
- Consider upgrading your router. High-powered routers with VPN-specific settings may manage the connection better, and you may be able to tweak the settings to make the best of your connection.
- Talk to your service provider about your needs. They may have a business-grade satellite connection that will manage VPNs better, or suggestions for a better router.

Technical adjustments you can make if you feel confident

If you're comfortable working with the configuration for a VPN, and if your software allows you to make changes, find and adjust these settings.

1. Set the protocol to TCPv4 instead of UDP.
2. Disable IPv6 altogether.
3. Change the destination port from 1194 to 443.
4. Enable the tcp-nodelay setting.
5. Ensure the inactive keepalive is enabled.
6. If keepalive is enabled, then increase the keepalive timeout (for example, double whatever the number is).

Test and adjust (lower) the MTU/frag thresholds.

- **For more information**
  - nbn blog: What is a VPN? Understanding virtual private networks
  - nbn VPN fact sheet: nbn Sky Muster satellite service fact sheet
  - SkyMesh: How to use a VPN to work-from-home

- # Other popular articles

- News
  November 4, 2024
  Telstra 3G shutdown is now complete

- News
  October 25, 2024
  Phones using the 3G network to call triple zero will be disconnected on 28 October 2024

- News
  October 25, 2024
  NBN Co accelerating higher speed tiers in September 2025

- Guides
  October 17, 2024
  Connectivity definitions

- Back to resources

-

Didn’t find the answers you were after?

Chat to us on our hotline with one of our team members and let’s get the conversation

started. If we don’t answer, we’ll get back to you in no time at all.

1300 081 029

Category

1. Tech Tips

Date
19/05/2025
Date Created
13/03/2024