Reasons to use a VPN

What is a VPN?

VPN is an acronym for Virtual Private Network. What that means is that the VPN program you use is creating a "private network" between you and the VPN service's server to which you connect. That network connection is encrypted between your device running the VPN and the VPN server at the far end for ALL your traffic. When you use a browser to access a secure site like your bank (or even lccug.com), the traffic is encrypted only between that site and your browser. All other traffic on the network is not encrypted, so someone could intercept your connections to the DNS server and route your traffic to a fake Internet site for instance. That is an extreme example, but when you use a VPN service, ALL your network traffic is encrypted to the far end VPN server to which you connect, so no one can eavesdrop on your local traffic. This is especially important when using a wireless connection, and even more important when using PUBLIC wireless, since anyone can connect to that network and eavesdrop on all traffic on that network.

There are many VPN services out there and many charge less than $5 per month for their service. However, you can sometimes find a sale for a lifetime VPN subscription for as little as $20 to $40. LCCUG has notified its members in the past when such sales have occurred.

Use Public or Hotel Wi-Fi in Confidence

Public wi-fi offers no encryption security to its users, and your signals are broadcast for anyone savvy enough to eavesdrop.
Your browsing is unencrypted, and unencrypted radio waves can be picked up by anyone.
Malware from one laptop in the coffee shop could find its way to your device via the router.
The free Wi-Fi on offer could be a trap — a fake internet connection operating as the pleasant face of a phishing scam.
If you log into a public wi-fi network and then connect to a personal VPN, all of your hotspot web use will then be encrypted and hidden from prying eyes. If you are a traveler or a user who is regularly using public wireless, then a VPN is a very wise investment in privacy.

Access Full Streaming Content (access Geo-based content)

Sometimes content is restricted to a particular country or area. Most providers base this decision on the IP address assigned to you by your ISP. Using a VPN will make your IP address appear to come from the area of the remote server to which you connect. For example, if you connect to a server in the UK, you can watch streaming content from the BBC free of charge (you just need to complete a free registration account).
The reverse is also true if you are travelling and need to access content that is only available in the US or your local area from which you came. Some popular streaming services like Netflix, Hulu, Amazon Prime, etc. as well as some social media sites like Facebook and Instagram are restricted or blocked outside the United States.

Avoid Location-Based Price Targeting

Some online stores will display different prices for the same item, based on the country from which you're browsing.
In one example, prices for the same plane ticket were cheaper via a Norwegian IP address than via a Malaysian IP.
The solution is to search for prices carefully, methodically switching VPN servers with each attempt, until the lowest price can be found. It might take a bit longer, but perhaps saving hundreds of dollars (if not more) may be worth the effort.

Improve Online Gaming Speeds

Sometimes an Internet Provider will throttle the speeds for online gaming traffic. A VPN service can be used to hide the fact that you are playing games online. Just be sure to connect to the closest VPN server to your location so the traffic isn't slowed too much.

Bypass the Country's Web Censorship and Content Surveillance

Since the traffic is encrypted when using a VPN, the government cannot see what sites you are visiting and block them if it deems them inappropriate. However, if the government blocks all traffic to known VPN sites, you might be out of luck on this ability.

Break Out of a Restrictive Network at Work/School

This is similar to bypassing a country's censorship, but at a smaller, local level.

Download and Upload P2P Files in Privacy

While Bittorrent peer-to-peer networking has been identified as a leading means of software piracy and copyright theft, the truth is that it is so widely used by legitimate services that it cannot be banned. The privacy and protection from surveillance by using a VPN service are definitely worth it.

Cloak Your VOIP Phone Calls and voice chats

Voice-over-IP (internet telephoning) is relatively easy to eavesdrop.
If you regularly use VOIP services like Skype, Lync, or online voice chatting, definitely consider implementing a VPN connection. The monthly cost will be higher, and the VOIP speed will be slower with a VPN, but personal privacy is invaluable.
Note that any speed reductions imposed by the VPN can cause Skype to drop calls it considers to be "low" quality. So unless you're talking about something of considerable sensitivity, it might be best to leave your VPN disabled for Skype chats.

Use Search Engines Without Having Your Searches Logged

If you get a VPN, you can cloak your IP address so you can keep your searches private (unless you are signed in to your Google or Microsoft account when you run your searches).

Avoid Reprisals and Traceback Because of Your Researching.

Many topics may be considered "sensitive". Or maybe you just don't want Google knowing that you're searching for "head lice" or "bed bugs". This can be useful also if you're a researcher, whistleblower, activist or journalist.

Private collaboration

Cloud drives and group chat tools can be the target of hackers, copyright thieves, and even agencies engaged in industrial espionage. A VPN can be used to encrypt your data and protect against these risks.

Because You Believe Privacy Is a Basic Right

Even if you're a normal citizen and you think you've got nothing to hide, a VPN service can act as your best friend very often, especially if you're a firm believer in personal privacy and the right to broadcast and receive without being surveilled and cataloged by authorities.

Final note

Just remember that there is no true 100% privacy on the internet. You can't be Superman on the internet- impervious to all assaults. The best you can hope for is just being a dude with a bullet proof vest that only protects you so much.
Using a VPN doesn't mean you're invulnerable. You should still make sure you're using HTTPS whenever possible, and you should still be careful about what you download.

Links for more information:

How-To Geek: Should You Use a VPN for All Your Web Browsing?
https://www.howtogeek.com/710378/should-you-use-a-vpn-for-all-your-web-browsing/

Make-Use-Of: 10 Reasons Why You Should Be Using a VPN
https://www.makeuseof.com/tag/reasons-to-use-vpn/

Avast: 8 reasons to use a VPN
https://blog.avast.com/8-reasons-to-use-a-vpn

Lifehacker: Why You Should Be Using a VPN (and How to Choose One)
https://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs