How do VPNs work? A VPN forms an encrypted tunnel between you and your VPN provider, which then passes all your connections through the service's exit servers (nodes), then back to you. To the sites you visit, this makes it appear that all traffic comes from the VPN service instead of your computer or phone, thus preventing association with your devices—or your location.

How do I choose a VPN provider? There are many available, but look for features such as the following:

- IPSec/SSL/OpenVPN encryption
- **No traffic logging**
- Exit node locations in friendly countries
- Unlimited data transfer and bandwidth

Be sure to look for reviews about a provider before you sign up. Free providers exist, but remember that you get what you pay for—expect to pay between $4 to $10/month for a quality service that won't monitor your traffic itself.

Remember, a VPN provider can see all your traffic, so trust is very important, and no traffic logging is an absolute must.

To protect your privacy even further, consider only visiting HTTPS-enabled websites, and install an ad-blocking browser plugin. The Electronic Frontier Foundation (http://www.eff.org) offers two useful plugins for Firefox and Chrome. One is HTTPS Everywhere, a browser plugin that makes sure that you are only using HTTPS encrypted websites. Privacy Badger is another plugin that helps block advertisers from tracking your activity across the entire web.

You may also wish to learn about and use browser plugins like NoScript, UBlock Origin, Ghostery, or Adblock Plus.

Protecting Your Digital Privacy With a VPN

Internet advertisers, search providers, data brokers, hackers, law enforcement (local and state police, county sheriffs, FBI, and others), government-sponsored mass surveillance agencies both domestic and abroad (CIA, NSA, and overseas intelligence agencies), and even your internet service providers (ISPs, such as Comcast, AT&T, Verizon, and others) are all capable of collecting your personal data online for analysis and/or sale.

The information collected may include what websites you visit, what web-based services you use, when and how often you use them, what you download, and more. Under current laws, you often have absolutely no say about how your information is collected, used, or transferred, whether it's by a company, law enforcement, or government agencies around the globe.

A Virtual Private Network (VPN) provider is one way to protect your privacy. VPNs are a tool used by individuals, groups, professionals, and corporations of all kinds to protect internet traffic from prying eyes, and you should consider using one, too, especially if you use public WiFi hotspots in cafes, bookstores, airports, libraries, and other places. Public hotspots are notoriously insecure, and can leak your data to anyone on the network. VPNs can also be used to protect your home and mobile internet, too.

Flip this card to learn more about how a VPN works, what features to look for in a VPN provider, and a few other tips you can use to protect your digital privacy.