BLACKCLOAK®

Virtual Private Network (VPN) Overview

This guide explains the ins and outs of a VPN, and how to set one up.

What Is a VPN?

As the name implies, a virtual private network offers improved security when using the Internet.
It is an encrypted connection between two endpoints.
VPNs once had a bad reputation as they were a primary tool for users who wanted to illegally download music or stream movies through torrent sites. The VPN kept their IP address and other transmitted data hidden so that they couldn't get in trouble with their Internet Service Providers. But a virtual private network is much more than a simple tool for movie buffs. Many organizations require employees to connect to the corporate network via a VPN when working remotely.

What Does a VPN Do?

A VPN creates an encrypted tunnel between your device and an endpoint server. This connection allows you to transmit data in a secure and private manner.
In addition to creating an encrypted tunnel, a VPN also temporarily changes your Internet Protocol Address (IP Address) to keep your activities anonymous.
A VPN will keep your Internet traffic safe from prying eyes and prevent your online activity from being traced back to your location.

To learn more, please visit:

blackcloak.io

Why Should I Use a VPN?

For starters, always use a VPN when on a public Wi-Fi network. You'd be surprised how many hackers set up fake hotspots, or hack into existing ones. When you use a public Wi-Fi network you increase the risk of having your online activity seen by cybercriminals. However, with a VPN in use, you can browse the Internet safely and privately. We generally recommend using a VPN when you are on a public or foreign WiFi network - coffee shop, airport lounge, yacht, plane, hotel or another person's house. This is because data exchanged on a public network is visible to everyone else connected to that network, including cyber criminals.

We don't typically recommend using a VPN when you're at home. When on the virtual private network, it will display a different IP address than your home IP address. Some internet service providers actually block the sending and receiving of emails if the home and device IP addresses do not match. We'd hate for you to be unable to send or receive emails! If you're concerned about websites and advertisers tracking you when you're on your home Wi-Fi, consider a privacy-focused web browser, like Brave, and/or a search engine like Duck-Duck Go.

A virtual private network is also useful for disguising your location, enabling you to conduct online activity safely when in another country.

Are There Downsides to using a VPN?

Using a VPN will degrade the speed of any network (due to it being encrypted), so be mindful that your online activity may experience a lag when on a VPN. Additionally, some programs, applications or email servers may not cooperate when a VPN is turned on due to the IP address change. If you have any problems (biggest one being not receiving email), then turn off the VPN. Some planes also limit or restrict the use of VPNs. If VPNs are allowed, make sure to connect to the plane's WiFi first before turning on your VPN. You will want to also follow that same process when connecting to hotel WiFi networks.