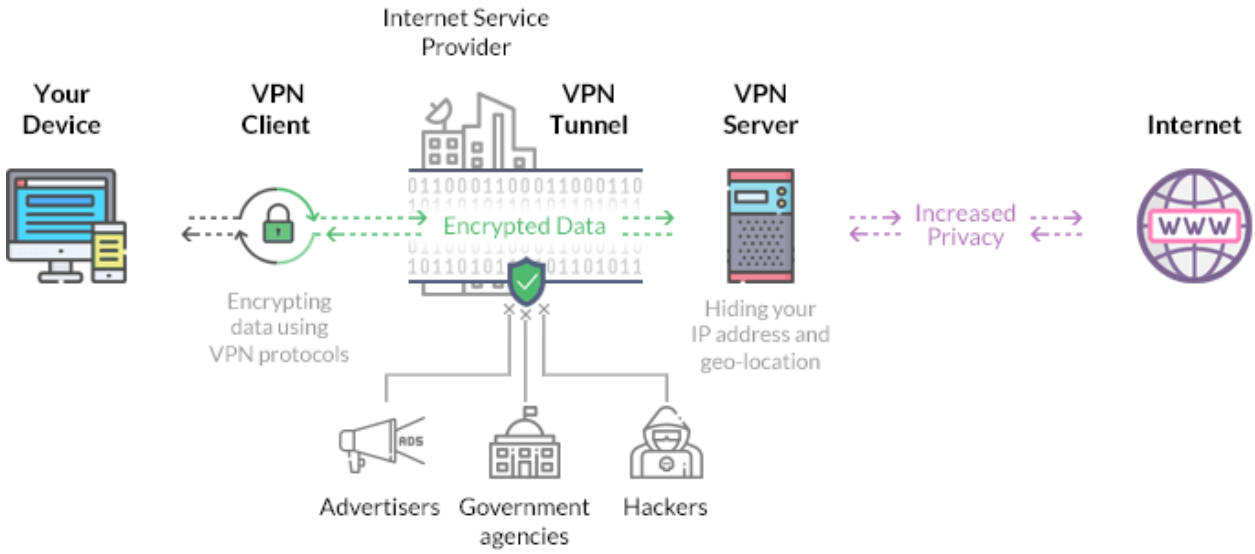
How VPNs and encryption secure your data

You might know that “encryption” is something that keeps you and your data secure from cybercriminals and others who want your information.

But how does encryption work? And how does your VPN provide encryption?

You can think of data encryption as basically two things - encoding and decoding. Encryption converts data from a readable format to an unreadable format using an algorithm. Then it’s decoded using the right decryption key. The key in this instance is usually a bunch of letters and numbers that are only known to yourself and those you trust.



A Virtual Private Network or “VPN” service essentially converts the data coming to and from you to a format that looks like unreadable gibberish to those trying to eavesdrop on your activity like when you’re using public WiFi. Your ISP or a government agency (either domestic or foreign) could also be attempting to snoop on you. For most people, VPN encryption helps users feel safe from cybercriminals who want to get at sensitive data like credit card numbers, bank account details, and login credentials.

A VPN provides a secure tunnel where even if your data is read by unknown parties, those parties are unable to decrypt it. As more functions such as banking go online, many experts consider a VPN a necessity when going online.

To learn more about VPNs and what to look for in a VPN, please visit our website:
vpntrust.net