

OUCH!

The Monthly Security Awareness Newsletter for You

Virtual Private Networks (VPNs)

Overview

You may find yourself needing to use public Wi-Fi for Internet access when you are away from home, such as when you are at your local restaurant or coffee shop, or when you are traveling at a hotel or airport. But how secure are these public networks and who is watching or recording what you are doing online? Perhaps you do not even trust your ISP (Internet Service Provider) at home and want to be sure they can't monitor what you do online. Protect your online activities and privacy with something called a VPN (Virtual Private Network). A VPN is a technology that creates a private, encrypted tunnel for your online activity making it much more difficult for anyone to watch or monitor what you are doing online. In addition, a VPN helps hide your location, making it much harder for websites you visit to determine where you are located.

How Does It Work?

A VPN works by creating a private, encrypted tunnel to a VPN provider that you select. All your online activity goes through this tunnel, then leaves your VPN provider's network to your intended destination. For example, if you're based in Tampa, Florida and you connect to a VPN server in Munich, Germany, any website you connect to will think you are connecting from Munich, Germany. A VPN is simple to use. The first step is finding a VPN provider you trust and then creating an account with them (this usually requires you purchasing their service). Once you have an account, you download, install, and configure their VPN software. Once installed and configured, you connect to the Internet as you always do. The VPN software will silently create your encrypted tunnel and start protecting your privacy without you even realizing it.

Selecting a VPN Provider

Your online activities are only as secure and private as your VPN provider. Be sure to select one that you can trust. Here are key points when selecting a VPN service provider.



Logging: Look for a service which does not keep any logs and focuses on privacy. If your VPN service provider does not collect any logs, it is much harder for anyone to go back and see what you have done online.



Where the Company is Based: Different VPN providers are based in different countries. Be sure you select a VPN provider that is based in a country that has strong privacy laws. VPN providers located in countries that have very few or weak privacy laws may be forced to give up information they collect on you.



Servers: Look for a VPN service that has the servers located in the countries or cities you need. Some VPN providers have thousands of servers and locations across the globe. Do you have a need to make your connections appear like they are coming from a specific country? Can the VPN provider provide that?



Compatibility: Look for services that work across different computers and mobile devices. For example, you may use a Windows laptop, a tablet, and an iPhone. You'll want a VPN service that will work on all those devices.



Avoid Free: Be very cautious of "free" VPN services; how are they making money and staying in business? Free services may collect and sell your information.

A VPN is a fantastic way to help protect your online privacy. However, a VPN does nothing to secure your computer, devices, or your online accounts. Even if you are using a VPN, be sure you always follow basic security steps, including ensuring your devices are updated, using a screen lock, and using strong, unique passwords for all your accounts.

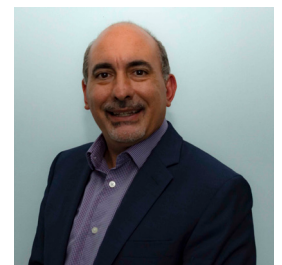


Subscribe to OUCH! and receive the latest security tips in your email every month - sans.org/ouch.

Do you think you've got what it takes to get into the cyber security industry? Or are you looking to improve your existing skillset? Training with SANS helps you achieve your goals. Level Up with SANS today! sans.org/Level-Up-Ouch

Guest Editor

Phil Johnsey ([@peakreflections](https://twitter.com/peakreflections)) is an IT professional at Palm Beach County experienced in security, forensics, and auditing. He is SANS certified in digital forensics, security essentials, and a member of the OUCH! Community Review Board. His passion is making security simple for others.



Resources

Making Passwords Simple: <https://www.sans.org/u/Sd8>

Securing Your Mobile Devices: <https://www.sans.org/u/Sdd>

Stop Malware: <https://www.sans.org/u/Sdi>

OUCH! is published by SANS Security Awareness and is distributed under the [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley