Article on IP proxies

There are many different methods on changing your ip address , changing Ip addresses has become very useful for both security as well as for hacking purposes,changing Ip address is mainly seen as a way to mask your actual location.

So here I am going to list 3 ways on how you can change your IP address for free

**Use a proxy to change your IP address**

Proxy works similarly to VPN but is much less flexible and secure. Your Internet connection goes through an intermediary server so that websites and other online resources see the IP address of the proxy server, not yours. Unlike VPNs, proxies generally lack encryption, only affect certain applications, and may disclose your IP address in other ways.

### Use Tor to change your IP address for free

Tor, short for The Onion Router, is an anonymous network run by volunteers. The easiest way to get started with Tor is to download and install Tor Browser, a simple web browser that routes all web traffic through the Tor network. Tor encrypts your connection multiple times, then sends data through multiple nodes - servers offered by Tor supporters. Each button removes a layer of encryption, and the button sequence used changes each time you visit another website. This makes it almost impossible to trace Tor traffic back to the source.

### Change networks to get a different IP address

It might sound obvious, but you can get a different IP address by disconnecting from the network you're currently connected to and connecting to a different network. For example, you can switch to another wifi network or switch from wifi to a mobile data connection if you are using a smartphone.

Remember that open, public wifi hotspots are often the main hunting grounds for hackers. Attempting to connect to a wifi network requires a password and is encrypted with WPA2.

### Proxy Vs VPN

Privacy and security are increasingly important, whether it's your corporate data or your own personal data that you need to protect. Make sure you invest time and money in the right tools for your security goals: Proxies and VPNs add an extra layer of security and privacy to your data.

If you want to allow your team to work remotely with secure access to corporate resources, configure and manage VPN users to access the network using the VPN.

If your concern revolves around "which websites my users are visiting", a proxy server is a better tool.

For the best results (and to protect your data as a citizen with security software), sign up for a well-monitored VPN service. For the most part, VPN services allow you to use servers in different locations to bypass content restrictions. If you also need to use a free proxy server every now and then for this purpose, just be aware of the risks.

If you are just starting to implement your enterprise-level data security strategy, there are more complex attack vectors to consider. Insider threats, APT, privileged account reports - as well as pure old-fashioned social engineering - are just as dangerous to your data as an unencrypted data stream.

Neither proxies nor VPNs will protect you against 100% of the cybersecurity threats your business will face: they won't stop insiders from stealing personal data, ransomware attacks, or coordinated entry hacking attempts.

Varonis Edge adds perimeter telemetry to security analysis - proxy, VPN and DNS monitoring to help fill this gap: you will be able to see when attackers enter the VPN, receive alerts when sensitive data is uploaded to external websites, etc. See how it works with a 1: 1 demo - and find out how Varonis helps secure your data against frontal attacks.