

Forum:[Hack Forums](#)

Thread: [Zyped's Guide to Staying Anonymous on the Internet](#)

Zyped - December 11, 2014, 8:14 am

Overview: Alright, this thread is meant to help keep you safe, and anonymous on the internet. I'm writing this guide to help you guys out. I see people have issues with this daily. In this thread I'll go over some methods to keep yourself safe. But please remember you can never be too safe.

VPN'S: A very common method of anonymity is to use a VPN, or Virtual Private Network. A VPN is essentially a server that allows you to route all of your connections through. It's like another network. An 'extra-layer'. This extra layer can be helpful in some situations, but not all. Many VPN's have DDoS protection, which is great. They hide your IP address, and even if they are attacked they rarely do go down. VPN's are great, but they can be expensive at times. A few negatives to using a VPN is a slower connection speed, and they are legally obliged to keep logs. That means if you are doing something illegal and the FBI go and seize the VPN server there's a log file that says everything you did on it. Not very effective for avoiding legal trouble.

Proxies:

Proxies are another common method of anonymity. They work similar to a VPN. You route your connection through a server and it serves as an extra layer. Proxies do not keep logs. But proxies don't always work out perfectly. Sometimes they won't connect to pages using SSL or you may lose connection, revealing yourself to the next page you visit. That's no good.

Lets Look at Where You're Identity is Vulnerable.

So, in many aspects you are vulnerable to your identity being found. Your internet service provider logs everything you do. So if you are in legal trouble and the FBI, or whoever is searching your case, can find out your ISP, they can check logs and see what connected where and what happened. And you will be caught.

Your IP address isn't always the most important thing to hide on the internet. Sure your IP is your identity, but you always have your real identity. Avoid making yourself searchable. Don't use common usernames. Like don't have a 'hacking' alias Johnyboy250, and have your personal twitter as Johnyboy250. Anybody could easily search that back and find more, and more info on you. That's called DOXING. There's many tutorials on that here on HF.

Encryption:

You always, always want to encrypt everything you can. Encryption is basically rearranging data to a point where you need a key to arrange it back in place. If you're smart you will encrypt all of your internet traffic using SSL(HTTPS), and encrypt your hard drive, just in case your computer gets compromised, seized, stolen, etc.

Personal Info is PERSONAL: Sometimes on the internet there are bad people who like to fuck with you for fun. They can often be mistaken as friends, because it's so easy to lie over the internet. Keep your personal info personal. Don't post pictures from your Facebook to a bunch of strangers on Skype. Things like that. If you really want to upload the image to a separate site.

Good luck and stay anonymous.

Multin - December 11, 2014, 10:39 am

good for a basic tutorial for newbs, maybe make an advanced one next ?

R?DSPY - December 11, 2014, 12:35 pm

Good guide, could possibly include steps on how to be more anonymous on the web. Like, securing Skypes, how to remove your information from search engines etc.

8/10

Siryn - December 11, 2014, 6:03 pm

I don't know if I would exactly call this a guide, but more of an explanation thread than anything. Nice typography though.

sens1fens1 - December 11, 2014, 9:34 pm

nice and simple explanation there i bet it can be useffule to someone :D