

Forum:[Hack Forums](#)

Thread: [\[TUT\] Best ways to stay as much anonymous as you can on the web.](#)

DumbChicken - April 6, 2021, 1:30 am

Hello there,

Those are the best FREE ways to stay anonymous and safe on the web.

To be anonymous (you can't be 100% anonymous):

- Use TOR browser.
- Use a proxy or even better, proxychains.
- Use a special OS like tails, whonix or kodachi.
- Use a free VPN.
- Use the firefox addons: NoScript and HTTPSeverywhere.
- Use StartPage as search engine instead of google
- Don't use your browser in full screen (TOR avoid that risk)
- Change your MAC and IP address before you start your browser.

To be safe and avoid malwares or steal of data:

- Never use the same password for each website.
- Check the recent leaks of databases or new websites vulnerabilities to know if you data is in danger.
- Never download files you can't fully trust. Exemple : Hello, my name is Patrick, download my SQL injection software for free!!! ---> <http://ifuckedyou.biz>
- Crypt your private files before you put them on the cloud.
- Use antiviruses. (I love kaspersky, but it isn't free ???.)
- Stay away from strange websites. Example: <http://www.efjzdkz.xyz>
- Don't type your passwords into sites that don't support https. (avoid MITM attack)

I hope this will help you, those are the basics things to do if you want to stay safe and anon.

Edit: Like some comments says, some techniques in there don't avoid the fact that the government could find you, such as VPNs, however, they still are effective against hackers, there are also techniques that have conditions and without those, you won't be anon, like when each Tor node is owned by the same person.

DumbChicken - April 6, 2021, 3:42 am

(Apr 6, 2021 03:05 AM)Incog Wrote: [\[CITE\]](#) "Use a free VPN."

Free vpns make money off free accounts by selling personal data they scrape from when you use it, so not really anonymous.

Also having a vpn before tor can also possibly be insecure if the connection between the tor node and vpn isnt secure

Others were okay, tbh you dont even need an additional antivirus if you just dont run stuff that isnt

from a company.

Yeah, that's true, but you can crack a paid VPN instead, but if you do illegal stuff, they can find you... This is why in said in the post that you can't be 100% anonymous, all you can do is try to be as much as you can...

Ampere - April 6, 2021, 12:45 pm

Not a bad list to get a beginner started! You could also add that using specific Password Managers may also alert you to when an account has been compromised. I believe LastPass uses that, although I don't think they are free anymore.

Void - April 6, 2021, 1:13 pm

(Apr 6, 2021 01:30 AM)DumbChicken Wrote: [\[CITE\]](#) Hello there,
Those are the best FREE ways to stay anonymous and safe on the web.

To be anonymous (you can't be 100% anonymous):

- Use TOR browser.
- Use a proxy or even better, proxychains.
- Use a special OS like tails, whonix or kodachi.
- Use a free VPN.
- Use the firefox addons: NoScript and HTTPSeverywhere.
- Use StartPage as search engine instead of google
- Don't use your browser in full screen (TOR avoid that risk)
- Change your MAC and IP address before you start your browser.

To be safe and avoid malwares or steal of data:

- Never use the same password for each website.
- Check the recent leaks of databases or new websites vulnerabilities to know if your data is in danger.
- Never download files you can't fully trust. Exemple : Hello, my name is Patrick, download my SQL injection software for free!!! ---> <http://ifuckedyou.biz>
- Crypt your private files before you put them on the cloud.
- Use antiviruses. (I love kaspersky, but it isn't free ???.)
- Stay away from strange websites. Exemple: <http://www.efjzdkz.xyz>

I hope this will help you, those are the basics things to do if you want to stay safe and anon.
Good post my dude! This is some good information I think everyone should look into.

psickophant - April 17, 2021, 5:41 pm

I guess you did talk about tor but using a script like anonsurf or nipe to tunnel all traffic through tor or like proxychains.... Good stuff.

ManKors - May 21, 2021, 1:38 pm

Use Protonvpn.

Never use [censored], because it sells data to the police.

Slatori21 - May 22, 2021, 8:45 am

<dkslafjldsa>

bold

SIM-5020961 - May 24, 2021, 12:54 pm

some good tips but i wouldnt reccomend using a free vpn because they often sell users data, i would reccomend using a vpn through tor if you are on windows and use proxy chains if you are on linux or if you have the time, turn a raspberry pi into a tor router

SIM-4741898 - May 24, 2021, 9:34 pm

Good post donot use free vpns

FooF - May 25, 2021, 8:36 am

the new mozilla vpn seems good.

Karen McMahon - May 26, 2021, 1:32 am

(Apr 6, 2021 01:30 AM)DumbChicken Wrote: [\[CITE\]](#) Hello there,
Those are the best FREE ways to stay anonymous and safe on the web.

To be anonymous (you can't be 100% anonymous):

- Use TOR browser.
- Use a proxy or even better, proxychains.
- Use a special OS like tails, whonix or kodachi.
- Use a free VPN.
- Use the firefox addons: NoScript and HTTPSeverywhere.
- Use StartPage as search engine instead of google
- Don't use your browser in full screen (TOR avoid that risk)
- Change your MAC and IP address before you start your browser.

To be safe and avoid malwares or steal of data:

- Never use the same password for each website.
- Check the recent leaks of databases or new websites vulnerabilities to know if you data is in danger.
- Never download files you can't fully trust. Exemple : Hello, my name is Patrick, download my SQL injection software for free!!! ---> <http://ifuckedyou.biz>
- Crypt your private files before you put them on the cloud.
- Use antiviruses. (I love kaspersky, but it isn't free ???.)
- Stay away from strange websites. Example: <http://www.efjzdkz.xyz>
- Don't type your passwords into sites that don't support https. (avoid MITM attack)

I hope this will help you, those are the basics things to do if you want to stay safe and anon.

Edit: Like some comments says, some techniques in there don't avoid the fact that the government could find you, such as VPNs, however, they still are effective against hackers, there are also techniques that have conditions and without those, you won't be anon, like when each Tor node is owned by the same person.Does

That help bypassing Google device security me not got a clue thanks

Vyreazz - May 27, 2021, 1:02 pm

Great post, thank you very much

DumbChicken - February 16, 2022, 4:09 pm

Edit after almost a year: I said that a tor tunnel is vulnerable if each tor node of the said tunnel are

owned by the same person. I was totally wrong. A tor tunnel is vulnerable if the exit node is compromised, aside this, the owner of the tor exit node can see all your traffic, so the use of a vpn can be quite interesting in that case.

PS: I also just seen how much grammar mistakes I did in the thread, please forgive the me of the past year.

Frequency - February 16, 2022, 6:06 pm

Also to add to this for new into fraud, illegal stuff and whanot:

1. Using the same machine for the illegal stuff and your daily life is weak. Buy yourself a cheap machine for 50\$ from second-hand or use amnesiac system like tails. If you are extra paranoid you can physically remove camera and microphone from your throwaway machine.

2. You NEVER hold any data related to any illegal activity in your house. In most cases, because the small percentage of people encrypt with key in file, you are encrypting the data with usage of passphrase. It's tragedy if you use in your passphrase any data connected to you like birthday, phone number fragments and whatnot.

Police always uses all possible combinations of your personal data, after that they just use dictionary. But that's if you live in civilised country, in some countries, like mine, if police sees that you have any files encrypted, passwords are weaker with every slap to the face received and other bullying. Not to mention whole matter gets 5 times more difficult for you.

3. If shit happens, you were stupid and you need to remove files from your disk, remember that only legit data removal method is overwriting of whole disk. Putting your disk to microwave, throwing it from third story or getting under tap water does nothing to data.

From the remains of WTC data was collected from, I think 400 hard drives, some were partially melted, some shattered, some had particles of dust "ironed into" disk plates.

?urt - February 16, 2022, 6:23 pm

"Use free VPN's" lol. Don't post a tutorial if you don't know what you're talking about..

Frequency - February 16, 2022, 6:41 pm

(Feb 16, 2022 07:23 PM)Grifter Wrote: [\[CITE\]](#) "Use free VPN's" lol. Don't post a tutorial if you don't know what you're talking about..

I mean, most of topics on forum are just quick and low quality rep whoring, but if you wanna make this place better and if you have time, just add to topic or explain to OP why he is wrong.

Also I just saw earlier someone recommending protonVPN, proton is good for for your grandpa if he wants to access blocked websites or is normal citizen that wants "secure" email, but Proton at it's base isn't suitable for anyone doing anything illegal.

?urt - February 16, 2022, 9:42 pm

(Feb 16, 2022 07:41 PM)Frequency Wrote: [\[CITE\]](#) I mean, most of topics on forum are just quick and low quality rep whoring, but if you wanna make this place better and if you have time, just add to topic or explain to OP why he is wrong.

Also I just saw earlier someone recommending protonVPN, proton is good for for your grandpa if he wants to access blocked websites or is normal citizen that wants "secure" email, but Proton at it's base isn't suitable for anyone doing anything illegal. For ProtonMail, It depends on the level of illegality. Unless you're doing something that's extremely black-hat and would catch the attention of

three-letter agencies then you're probably fine, but even then if you have good OPSec and a secure VPN (and don't leak your real IP address) then it doesn't really matter at all. This can also be said about Gmail as well. As long as there isn't any information that can compromise your identity the the "security" of a email service doesn't really matter.

JEFFrey - *February 19, 2022, 8:22 am*

I think its worth to buy a VPN its not much cash and its more saver then using a Free... cause nothing realy is free they also need to make cash of something...

ThewayHome - *February 21, 2022, 2:27 pm*

Tor is able to exploited by Intelligence Agencies or Huge Companies. But nonetheless it is better than a stock browser.