

Forum:[Hack Forums](#)

Thread: [How to be Anonymous on the Internet](#)

Untippable - June 25, 2017, 9:28 am

Ive want to be anonymous on the internet so websites cant see my ip address

Lisk - June 25, 2017, 9:30 am

(Jun 25, 2017 09:28 AM)Untippable Wrote: [\[CITE\]](#) Ive want to be anonymous on the internet so websites cant see my ip address

You can use a VPN or Tor.

Freakyy - June 25, 2017, 9:32 am

This is one of the best tuts on how to maintain your privacy online.

<https://hackforums.net/showthread.php?tid=5377222>

Caliban - June 25, 2017, 9:34 am

<https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/>

Asdethprime - June 25, 2017, 11:00 am

If all you want is to make sure the websites you visit can't determine your IP, you can use a TOR Browser

<https://www.torproject.org/projects/torbrowser.html.en>

TOR provides the best security when it comes to anonymity with your HTTP/HTTPs traffic. However, it's slow which is sadly the price you pay for a secured anonymity service.

As long as website allow connection using a TOR relay, use that. This way the website will see the IP address of the TOR exit node as opposed to yours.

You can always check what IP is being shown by simple searching "what is my ip" on google.

You might want to run a DNS Leak Test (<https://www.dnsleaktest.com/>) to make sure your DNS is not leaking. This is normally not that crucial because virtually every website you are going to obtain logs from your ISP and a DNS leak only identifies your ISP and not your computer.

Im af ni1 - June 25, 2017, 11:19 am

(Jun 25, 2017 11:00 AM)Asdethprime Wrote: [\[CITE\]](#) If all you want is to make sure the websites you visit can't determine your IP, you can use a TOR Browser

TOR provides the best security when it comes to anonymity with your HTTP/HTTPs traffic. However, it's slow which is sadly the price you pay for a secured anonymity service.

As long as website allow connection using a TOR relay, use that. This way the website will see the IP address of the TOR exit node as opposed to yours.

You can always check what IP is being shown by simple searching "what is my ip" on google.

You might want to run a DNS Leak Test () to make sure your DNS is not leaking. This is normally

not that crucial because virtually every website you are going to obtain logs from your ISP and a DNS leak only identifies your ISP and not your computer.
no it doesn't provide 'the best security'

lol

Asdethprime - June 25, 2017, 12:19 pm

(Jun 25, 2017 11:19 AM)Im af ni1 Wrote: [\[CITE\]](#) no it doesn't provide 'the best security'

lol

Name a single tool that provides better security than Tor?

Why do you think security focused operating systems , for example Whonix, Tails, Qubes VM TOR all use it?

Why do you think website like Banking specifically block TOR exit node.

It's because it provides the best security out there.

You can like it, you can hate it, but it is what it is.

shifty1337 - June 25, 2017, 12:25 pm

check this out

<http://www.techadvisor.co.uk/how-to/internet/how-use-vpn-set-up-vpn-for-private-browsing-2017-3466190/>

Im af ni1 - June 25, 2017, 12:30 pm

(Jun 25, 2017 12:19 PM)Asdethprime Wrote: [\[CITE\]](#) Name a single tool that provides better security than Tor?

Why do you think security focused operating systems , for example Whonix, Tails, Qubes VM TOR all use it?

Why do you think website like Banking specifically block TOR exit node.

It's because it provides the best security out there.

You can like it, you can hate it, but it is what it is.

a double-bounce proxy is more secure than TOR

lol

Asdethprime - June 25, 2017, 12:38 pm

(Jun 25, 2017 12:30 PM)Im af ni1 Wrote: [\[CITE\]](#) a double-bounce proxy is more secure than TOR

lol

Yeah because having 2 proxies to bounce between is better than TOR that allows you to set up as many proxies in the middle as you want, all of which are encrypted, compartmentalized, intentionally created unintelligent and don't record logs.

??????????????

Are you freaking kidding me?

Im af ni1 - June 25, 2017, 1:08 pm

(Jun 25, 2017 12:38 PM)Asdethprime Wrote: [\[CITE\]](#) Yeah because having 2 proxies to bounce between is better than TOR that allows you to set up as many proxies in the middle as you want, all of which are encrypted, compartmentalized, intentionally created unintelligent and don't record logs.

??????????????

Are you freaking kidding me?

yes because having MORE points of attack = greater security

having slower bandwidth = greater usability

unintelligent = greater routability

yeah TOR is a joke made by the military, chill the fuck out- any investigators worth their salt will find you if you're behind TOR or not.

now i under-exaggerated, 2 proxies is not good enough- but in ways it's better to have a terminating node for the initialization data somewhere in the middle of the proxychain so that when you create a diagram it makes a loop-like infrastructure which is harder to resolve to the source.

i.imgur.com/vQYlja0.png

there are many ways to implement the deconstruction at the link endpoint or the server endpoint, perhaps invalid checksum, or treated as valid- regardless it's a two way system which'll confuse anybody for some time.

?ndrew - June 25, 2017, 1:10 pm

FBI cant track you in incognito mode

Im af ni1 - June 25, 2017, 1:11 pm

(Jun 25, 2017 01:10 PM)?ndrew Wrote: [\[CITE\]](#) FBI cant track you in incognito mode sometimes the fbi has a cup of coffee and you can use the normal browser

it's only around 8am-10am tho

Asdethprime - June 25, 2017, 7:45 pm

(Jun 25, 2017 01:08 PM)Im af ni1 Wrote: [\[CITE\]](#) yes because having MORE points of attack = greater security

having slower bandwidth = greater usability

unintelligent = greater routability

Are you a troll?

It's not about having more than one point of attack, it's having more than 1 node , running in more than one country, to prevent anonymity.

Being slow is just the side effect and being unintelligent even the nodes themselves don't have tracking information about you , the information they have are only related to the next node on the hop.

But it's obvious you are an absolute idiot who has no idea what you are talking about so have fun being a tool.

andrius94 - June 26, 2017, 4:09 am

(Jun 25, 2017 07:45 PM)Asdethprime Wrote: [\[CITE\]](#) Are you a troll?

It's not about having more than one point of attack, it's having more than 1 node , running in more than one country, to prevent anonymity.

Being slow is just the side effect and being unintelligent even the nodes themselves don't have tracking information about you , the information they have are only related to the next node on the hop.

But it's obvious you are an absolute idiot who has no idea what you are talking about so have fun being a tool.

I agree with you. I believe TOR is more than enough in most cases (if you are going really big money stealing (hundreds and millions of dollars), hacking world wide important websites (fb, twitter, nasa, google, cnn, bbc and others very popular) and doing a lot of damage - then maybe yes. TOR might not help you). But just for hiding IP, doing easy hacking I totally believe it's more than enough. Double proxies - be always sure, every second sure that nothing will fail and all proxies will not provide any info.

I also like VPN but once again, you can't never be totally sure.

Im af ni1 - June 26, 2017, 4:58 am

(Jun 25, 2017 07:45 PM)Asdethprime Wrote: [\[CITE\]](#) Are you a troll?

It's not about having more than one point of attack, it's having more than 1 node , running in more than one country, to prevent anonymity.

Being slow is just the side effect and being unintelligent even the nodes themselves don't have tracking information about you , the information they have are only related to the next node on the hop.

But it's obvious you are an absolute idiot who has no idea what you are talking about so have fun being a tool.

Nope, did you ever learn basic network security?

half the shit you said makes no sense, unintelligent nodes don't need to primarily have information on you where the fuck did you learn that, they can easily have much more implementations- and become intelligent- without needing to know information about the origin.

also your description legit makes no sense, why WOULD a node far beyond the second one even remotely know about the first node.

an intelligent node would be defined by it's characteristics to be able to manage routing, deal with dead nodes and be somewhat dynamic in its nature.

you can add in "knows about first and last node" completely fine assuming the user is using a VPN.

you seriously don't know shit about TOR's structure yet you try to argue about it.
tool

Asdethprime - June 26, 2017, 8:19 am

(Jun 26, 2017 04:58 AM)Im af ni1 Wrote: [\[CITE\]](#) half the shit you said makes no sense, unintelligent nodes don't need to primarily have information on you where the fuck did you learn that, they can easily have much more implementations- and become intelligent- without needing to know information about the origin.

Really?

The nodes are unintelligent in transit, it does not mean that the physical hardware of the node is dumb or the node does not have functionality. It simply means that node has all the information, however most of them are encrypted. Each node only has the key to decrypt information regarding which node to send the message to. This is critical because in the unlikely event of the node being compromised your information is not leaked because it simply does not have the key to decode it. The way encryption has evolved it is no longer feasible to bruteforce a secured encryption even with a huge series of servers.

Quote:also your description legit makes no sense, why WOULD a node far beyond the second one even remotely know about the first node.

an intelligent node would be defined by it's characteristics to be able to manage routing, deal with dead nodes and be somewhat dynamic in its nature.

I don't get what you are saying. The nodes makes it's own routing table and other stuffs that you would expect a router to be able to do. It's just that the node simply has no way of knowing, and hence no way of disclosing, details about the actual origin and the actual destination of the request.

This greatly enhances security.

Are you just coughing nonsense to sound smart?

ExDeeMan - June 26, 2017, 8:44 am

Try using a VPN such as Mullvad, R4W, or 143 VPN. They all keep minimal to no logs and are quite cheap.

Asdethprime - June 26, 2017, 8:47 am

(Jun 26, 2017 08:34 AM)Im af ni1 Wrote: [\[CITE\]](#) greatly enhances security from who

if you gain access to the node, you'll still manage

Enhances security for anyone using TOR because individual nodes themselves are incapable of revealing identifying information.

If you get access to the node , all you will be able to manage is to track what node it passes the information to next.

Not to mention something you keep glossing over, no proxy has the system of multiple encryption keys , and compartmentalization of data.

Now you are typing just plain garbage, compared to before where at least you were PRETENDING not to type garbage.