

Forum:[Hack Forums](#)

Thread: [5 Main Keys to Being Undoxable](#)

ZachariahOG - January 12, 2018, 10:35 pm

This tutorial isn't for getting away with doing illegal activities. If you want a tutorial for that just tell me. This is also what I recommend.

1.) New Identity - To prevent your real identity getting leaked.
 - Search "identity generator" on Google.
2.) Operational Security / Information Security - To keep small information secure.
 - Search "OPSEC" and "Info Sec" on Google.
3.) VPN - To protect yourself from ISP doxing, ddos attacks, database lookups, and general location.
 - [censored]
4.) Antivirus - To protect yourself from RATs, Trojans, Spyware, Malware, etc.
 - ESET Nod32
5.) Password Manager - To manage your accounts, create secure passwords. and prevent accounts from getting jacked.
 - LastPass

If you want me to go further in depth, let me know and I will give a better tutorial and reasons to why these 5 things are very important.

EPLS - January 12, 2018, 10:41 pm

The only way to prevent a DOX is by being extremely careful with your information. All it takes is your email to be publicly listed on a forum and then searching that email on leaked DBs and following the data trails.

ZachariahOG - January 12, 2018, 10:46 pm

(Jan 12, 2018 11:41 PM)EPLS Wrote: [\[CITE\]](#) The only way to prevent a DOX is by being extremely careful with your information. All it takes is your email to be publicly listed on a forum and then searching that email on leaked DBs and following the data trails.

But if you didn't have any of the things I mentioned it would be a lot easier to trace someone.

Pyrotechnics - January 19, 2018, 11:57 am

If you need to get rid of some info its good to use some of the "detracers" online like deseat.me. However even erasing the information, it could be still in the database, you'd literally have to go to every website and ask to have your old identity taken down. Regardless info is always cached. If a person knows what they are doing your information is always up for grabs.

SIM-1073426 - January 19, 2018, 1:26 pm

You're not going to be undoxable because of this, you're putting the wrong ideas in to peoples minds which might actually hurt them if they want to be anonymous for the right reasons. I'm gonna poke some holes in your statement and I hope you'll take some time to reflect on it.

Quote:4.) Antivirus - To protect yourself from RATs, Trojans, Spyware, Malware, etc.
- ESET Nod32

You can avoid getting detection rates with malware by different methods of cryptography and most likely other un-related methods.

Quote:5.) Password Manager - To manage your accounts, create secure passwords. and prevent accounts from getting jacked.
- LastPass

Lastpass has been a victim of Odays because, take a look at [this](#)

Also [this](#)

Quote:3.) VPN - To protect yourself from ISP doxing, ddos attacks, database lookups, and general location.

- [censored]

Although a brief overview of this VPN seems promising you should always keep in mind that a VPN provider might lie or exaggerate on their features, if put enough pressure they can track you down depending on the situation and could get hacked. You should always use Tor instead of any other anonymity service just because it's open source and it's being suggested by respected figures in the security field.

Other than the previously mentioned options there's a few theoretical methods, some more likely than others but I don't really think they belong in this thread.

Bubblez - January 19, 2018, 1:29 pm

It would be interesting if there was a service to help remove info on you online.

Malicious` - January 19, 2018, 1:31 pm

(Jan 19, 2018 02:29 PM)Bubblez Wrote: [\[CITE\]](#) It would be interesting if there was a service to help remove info on you online.

There's a website showing all the steps you need to delete personal/account information from said website. I completely forgot about the name of this website though.

SuperiorUser - January 19, 2018, 1:35 pm

It's literary impossible to be completely undoxable. maybe from randoms trying to dox you but anybody with some access to isp logs such as country leaders, feds, ect would be able to find you. You may be able to make it harder but it won't be impossible. Either way I don't understand why protection from malware would be on the list.

SIM-1073426 - January 19, 2018, 1:46 pm

(Jan 19, 2018 02:31 PM)Malicious` Wrote: [\[CITE\]](#) There's a website showing all the steps you need to delete personal/account information from said website. I completely forgot about the name of this website though.

Listen to this man! He's an intelligence expert working on exclusive projects involving all of the security agencies in the Five Eyes. I have had very in-depth discussions with this man about various kinds of traffic correlation and SIGINT. He has infected almost 75% of the VPN's currently running around the world, he has contacts in a lot of corporations with huge amount of P.I.I such as ISPs

and banks. He runs his own private doxing website called The Lighting Kraken which correlate social media accounts and government issued ID's across the globe.

Truly a remarkable man..

ogwhitey - January 19, 2018, 1:51 pm

(Jan 19, 2018 02:26 PM)Aces. Wrote: [\[CITE\]](#) You're not going to be undoxable because of this, you're putting the wrong ideas in to peoples minds which might actually hurt them if they want to be anonymous for the right reasons. I'm gonna poke some holes in your statement and I hope you'll take some time to reflect on it.

You can avoid getting detection rates with malware by different methods of cryptography and most likely other un-related methods.

Lastpass has been a victim of 0days because, take a look at

Although a brief overview of this VPN seems promising you should always keep in mind that a VPN provider might lie or exaggerate on their features, if put enough pressure they can track you down depending on the situation and could get hacked. You should always use Tor instead of any other anonymity service just because it's open source and it's being suggested by respected figures in the security field.

Other than the previously mentioned options there's a few theoretical methods, some more likely than others but I don't really think they belong in this thread.

All software has vulnerabilities and 0day's so discounting a peice of software that has encountered only one 0day in it's long history speaks to it's quality.

Using Tor alone isn't sufficient either. A VPN with Tor is ideal.

Using anti-virus is a best practice in general for most people.

Using your logic, no one should use anything because everything is hackable. It's about serializing mitigating controls. The more well placed and configured controls the less the likelihood of data leakage.

SIM-1073426 - January 19, 2018, 2:08 pm

(Jan 19, 2018 02:51 PM)ogwhitey Wrote: [\[CITE\]](#) All software has vulnerabilities and 0day's so discounting a peice of software that has encountered only one 0day in it's long history speaks to it's quality.

Using Tor alone isn't sufficient either. A VPN with Tor is ideal.

Using anti-virus is a best practice in general for most people.

Using your logic, no one should use anything because everything is hackable. It's about serializing mitigating controls. The more well placed and configured controls the less the likelihood of data

leakage.

The first mentioned vulnerability could be used to potentially (although most likely) completely compromise your security and anonymity with little to no efforts. Lastpass have had several vulnerabilities in the past. It wouldn't have mattered if you used an anonymity service, this is literally the worst case scenario and the exploitation process is actually not that difficult to deploy. Meaning I don't trust them with my information, and someone serious about their anonymity shouldn't either.

I'm not well researched on the Tor and VPN combination beside the fact that VPN's should be used for privacy and Tor for anonymity, as well as the fact that The Grugq recommends using Tor before you run the VPN program. I'd be grateful for some thoughts about it.

Using an anti-virus is a good practice, from a security perspective.

No, I'm saying the guide is okay but it's giving false promises. In practice and in theory purely this won't make you as safe as you possibly can be.

ZachariahOG - January 19, 2018, 2:29 pm

(Jan 19, 2018 02:26 PM)Aces. Wrote: [\[CITE\]](#) You're not going to be undoxable because of this, you're putting the wrong ideas in to people's minds which might actually hurt them if they want to be anonymous for the right reasons. I'm gonna poke some holes in your statement and I hope you'll take some time to reflect on it.

You can avoid getting detection rates with malware by different methods of cryptography and most likely other un-related methods.

Lastpass has been a victim of Odays because, take a look at this

Also this

Although a brief overview of this VPN seems promising you should always keep in mind that a VPN provider might lie or exaggerate on their features, if put enough pressure they can track you down depending on the situation and could get hacked. You should always use Tor instead of any other anonymity service just because it's open source and it's being suggested by respected figures in the security field.

Other than the previously mentioned options there's a few theoretical methods, some more likely than others but I don't really think they belong in this thread.

Thank you for the feedback but "This tutorial isn't for getting away with doing illegal activities." I'm not talking about people who dox, swat, ddos, etc. The average person that only plays games or talks to people, etc. Not for someone who is being targeted daily.

(Jan 19, 2018 03:08 PM)Aces. Wrote: [\[CITE\]](#) The first mentioned vulnerability could be used to potentially (although most likely) completely compromise your security and anonymity with little to no efforts. Lastpass have had several vulnerabilities in the past. It wouldn't have mattered if you used an anonymity service, this is literally the worst case scenario and the exploitation process is actually not that difficult to deploy. Meaning I don't trust them with my information, and someone serious about their anonymity shouldn't either.

I'm not well researched on the Tor and VPN combination beside the fact that VPN's should be used for privacy and Tor for anonymity, as well as the fact that The Grugq recommends using Tor before you run the VPN program. I'd be grateful for some thoughts about it.

Using an anti-virus is a good practice, from a security perspective.

No, I'm saying the guide is okay but It's giving false promises. In practice and in theory purely this won't make you as safe as you possibly can be.

I'm gonna write something else for people that goes a lot more in depth on how to prevent getting doxed. This was just for people that don't wanna get doxed by random people they find online with little experience.