How To Be A Ghost - The 10 Rules Of Operational Security

by **Wipe_TS**

This article was posted on GREYSEC.NET. To see the complete discussion, please visit https://greysec.net/showthread.php?tid=7753.

Alright, welcome everyone, I've seen a lot of questions about OPSEC, a lot of OPSEC failures, and a lot of stupid statement which I think shouldn't have their place on the internet. It's time to clear the fog of Operational Security, how do I become a Ghost, and how do I stay a Ghost?

*(Those 10 rules are not a technical tutorial, these are **RULES** to follow, if you want to learn about PGP, Tor, VPN, VPS, Hacked Wi-Fi and so on, you should look at others topics, maybe I'll do one for the technical aspect.)*

THE TEN RULES OF OPERATIONAL SECURITY

1. KEEP YOUR MOUTH SHUT

Don't tell anything. Don't say how much you make. Don't say how you do it. Don't give away your smartphone / laptop / desktop or hardware models. Don't talk about TOR or PGP. Don't talk about anything, really. If you don't talk, you don't have to encrypt. If you have to talk, talk encrypted.

2. TRUST NO ONE

Everything and everyone is a threat. Don't trust anyone. Don't trust your partners, don't trust your lovers, don't trust your brothers and sisters. A Ghost has no friends. The less you tell to people, the better. Don't let people have power over you, if you can act alone, do it alone.

3. NEVER CONTAMINATE IDENTITIES

Don't share anything between aliases. Every identity should be disconnected from the others. Don't use the same e-mail, don't use the same IP, if you can, don't even use the same *geo-localization* or OS. Don't use the same passwords for multiple identities. Don't be on different identities at the same time, even if you compartmentalize your identities, you could make a mistake.

4. BE UNINTERESTING

Stay under the radar. Hide your knowledge. If you can avoid forums, do it, the less presence you have online, the better. Don't get caught doing stupid things, you don't want LE to search your house because you couldn't resist to go 170mph(270kmh) on the highway. Create a realistic identity, be uninteresting, don't be a computer geek, again, hide your knowledge, again, shut your mouth, don't talk about tor, you don't know these things. Don't do anything longer than you could.

5. BE PARANOID, RIGHT NOW

They already are after you. *(No, they probably aren't, but act has if it was true.)* Don't make the mistake to tell yourself that it is okay for now to be relax, it is not. You better **Wipe_T**he **S**ystem right now, and start fresh. Don't let weird USB on your desk, don't let weird files *unencrypted*. Hope for the best, but be ready for the worst case scenario. Be ready for the knock on your door. Do you have full disk encryption? Do you have an escape route? A hidden car? Do you have tape on your webcam? Did you remove the microphone of your computer? Assume that all network are under constant surveillance. Don't let your hardware unattended, don't let them unlocked where you are not around.

6. KNOW YOUR LIMITATIONS

Operate at the lever of you abilities. If you don't fully understand what you are doing, stop doing it, or accept the risk that your ignorance could lead you to jail. Keep it as simple as possible. Complexity is the nemesis of security. You'll be better with a simple setup that you understand, than with a complex *nested-multi-layer* setup that could create more attack vectors.

7. MINIMIZE INFORMATION

No logs = No crime. Avoid logging anything. Destroy everything, that's the best way to delete logs. No history browser, no logs, etc. If you can, use a live operating system, if you can't, at least use snapshots. The less said the better, again, don't talk, but if you have to talk, minimize information. Don't say things like *"Hey John, I bring the computer and the hard disks, meet me at James house at 8."* Say things like *"Hey, I bring the things, meet me at the location, same hour as last time."* No clear text, ever. If you have to talk to someone, encrypt it. No money trail. Don't link your real identity to anything. Use offshore accounts and shells company.

8. BE PROFESSIONAL

Don't be an amateur and get caught. Operational Security is a business, be professional. Educate yourself, don't rely on stupid topics like this one to cover your ass. Have a logic and systematic approach before every operation. Do multiple verification. Exclude luck. This is a business.

9. EMPLOY ANTI-PROFILING

Don't tell anything about yourself that could help create a profile. Don't talk about your hair color, your height, your country, your gender, where you were born, what you like, etc. If you have to talk, use your fake identity to create fake profile, use fake gender, fake country, use another language if you can. Don't log anything, but if you have to logs information, choose the information you log.

The hours of your posts can be used to determined your Time Zone, change it, don't always be on your favorite forum at 8PM. Be careful, don't use special letter who only exist in your language, don't use weird accent that only exist in your language, again, if you can speak another language, use that other language. Modify the metadata of the files you upload to create fake trail to follow. **DO IT EVEN WITH YOUR PARTNERS IN CRIME.** Again, you have no friends, all of that is not only for LE.

10. PROTECT YOUR ASSETS

That one is easy, encrypt everything. Don't say anything, don't leave a trace. If you have to, encrypt it. If you don't need it anymore, destroy it physically.

Alright, as I say it sooner, these are rules, not a technical tutorial. If any of this seems overkill, you probably don't need it for your required level of anonymity. If you have any question about one of these rules, don't hesitate to ask, and I will tell you why that rule exist. If you take an hour or two to read about cases of OPSEC failure, you will see that everyone of them break at least one of the ten rules. And for anyone thinking that all of that is black hat related and shouldn't be on GreySec, crime is not necessarily what you think it is. You could just be a whistle-blower, you'll be considered illegal, even without hurting anyone.

GREAT GREYSEC TOPICS ON THE SUBJECT:

Security and Encryption:	http://ytxmrc3pcbv5464e.onion/showthread.php?tid=7514
OpSec Fails Compilation:	http://ytxmrc3pcbv5464e.onion/showthread.php?tid=7706
General OPSEC Resources:	http://ytxmrc3pcbv5464e.onion/showthread.php?tid=2859
Practical Anonymity:	http://ytxmrc3pcbv5464e.onion/showthread.php?tid=1276