

Forum:[Hack Forums](#)

Thread: [\[UPDATED\]\[Tutorial\] Tighten up your Anonymity and Security \[Tutorial\]\[NEW\]](#)

EmperorDAZ - September 20, 2012, 2:13 am

So, there probably are many tutorials about this, but I think I should expand more about the topic I am going to talk today: Anonymity | Security

Let's begin with the Internet Browsers.

(Browser: Google Chrome and Mozilla Firefox)

Recommended plugins: Do Not Track Plus aka DNT+

This plugin is maintained by Abine, inc and it is free of charge.

What does it do? : This plugin will block the load of some resources on the webpage known for tracking you. They have 3 categories: Social Networks, Ad Networks and Social Networks. It will also allow you to white-list some sites where you would like the load of such resources.

Download at: <http://47a4>

HTTPS Everywhere

This plugin was produced as a collaboration between The Tor Project and the Electronic Frontier Foundation.

What does it do? : This plugin consists on a local database of the hosts that would support HTTPS. You might want to use HTTPS as always as possible in every situation since it will encrypt your connection.

Download at: <http://47a6>

Adblocker Plus aka ABP

[img=100x100]http://adblockplus.org/images/abp_icon.png[/img]

Wow, why the hell would I mention an Ad-Blocker? Ads can be consistently annoying and sometimes, they are known to spread malware. Who can tell us, the next time you go to some page, a "flash" based Ad pops up and it had a malicious payload? Who can tell us there isn't a new 0 Day exploit awaiting to exploit your precious computer and sending it to the botnet owner network and use it for dark purposes?

Download at: For Firefox Users: <http://47aq>

For Google Chrome Users: <http://47ar>

For K-Meleon Users: <http://47as>

Next, we shall move to securing our OS. Windows Operating Systems Secure your OS with Regular Updates

Reader: "What the hell, why we need the annoying Windows Updates running again? It makes me need to restart my PC after every goddamn update!"

Windows has it's reasons to make updates. In fact, updates are what makes your computer harder and harder to be exploited. Microsoft releases regularly updates to patch the flaws on your currently running Windows. Without it, the Conficker worm would have been very successful. But Microsoft had to release updates to patch the [MS08-067] vulnerability.

Get a good Antivirus and a good Firewall

Anti-Malware Protection: To be honest, I don't see many goods in getting a AV. Antivirus won't

pickup the {currently} FUD viruses (unless by heuristic and luck), so, if you get infected and your AV decides to release the signature updates to detect it, it's already too late. The virus is now probably blocking your AV from working properly now. If you are one of the guys who think the AV is a must, then go ahead and grab one. I have no suggestions on AVs.

Firewall: Firewalls are indeed a good mechanism to prevent some unauthorized network traffic. Indeed, they also will block/skew most of the Port Scanning techniques. I recommend Comodo Firewall.

Download at: <http://47bp>

Use a Keyscrambler

So, let's say, you get mysteriously infected with a keylogger. I know, the situation is very delicate now. Wait, how can I prevent this?

By using a keyscrambler. It will encrypt anything you type on the keyboard at ease. No complicated setup.

Download KeyScrambler Premium v.2.9.0.1 at: <http://12ww>

Use Sandboxie to run suspicious programs

Sandboxie is a program that will create an isolated environment for a suspicious file. Simply run a file in sandboxie and your files will be freed of harm. Sandboxie is a paid program but you can easily search for it's cracked version around.

Linux | Unix based systems Use sudo instead of logging in as root

With a root account, sometimes, some mistakes can be dreadful. And, with very bad luck, you catch a malware that targeted nix based systems. You are pretty much screwed in these situations.

Install rkhunter and chkrootkit utilities.

These utilities, which can be only executed by root will check your system for known rootkits. Ensure to update the rkhunter definitions file periodically by typing in the terminal:

Code `sudo rkhunter --update` Install ClamAV virus scanner

This command-line utility (you can get a GUI for it) will check your systems for any infected file. As usual, ensure to update it regularly.

Enable ExecShield Protection (if available)

This will protect you from Buffer Overflow attacks.

Link with more information regarding it: <http://47ce>

Disable root login from SSH

This is ridiculous in my opinion and it will only increase the risk if you allow root login.

Edit the file `/etc/ssh/sshd_config`

And find the line with

Code `PermitRootLogin yes` Change it to

Code `PermitRootLogin no` Then save.

Setup DenyHosts to countermeasure Brute-Forcers (SSH)

We all hate those brute-forcers trying to penetrate our PC. So here's a guide on how to setup DenyHosts.

URL: <http://47d3>

Use Public Key Based Authentication (SSH)

Tip: Never use passphrase-less keyfiles.

URL: <http://47d6>

Android Get Wifi-Protector

This application will protect you from ARP poisoning attacks and ARP based Denial of Service Attacks (Works better with ROOT support). This is a paid application but here I release the free .apk

Download at: <http://47ct>

General Do NOT use telnet

Telnet has been proven extremely dangerous, since it transmits it's data in PLAINTEXT. Anyone

sniffing on the network will quickly get access to your stuff. Instead use SSH which is much more safe and it's data transmission is ENCRYPTED

Use SFTP instead of FTP

The same reason from above, FTP also transmits data in PLAINTEXT.

Now, let's move on to Anonymity. Use VPNs that stores NO logs

These kind of VPNs, will ensure that the police won't have any evidence (except your physical computer) regarding your actions. Most of the VPNs store logs and the few who don't are paid ones. If you are really in need for a free one I suggest proXPN but I am not sure if they store logs or not.

Use truecrypt

This amazing software will encrypt the data in your drives with some pretty strong Algorithms. It is both available for Windows and Linux Operating systems and have their portable version.

Some HF wrote a guide about it: <http://47dh>

TOR is NOT 100% safe.

Although TOR is a very nice "network", it's not 100% safe. The data is encrypted and transmitted through various nodes. Good. But the data must be decrypted at the Exit Node so it can reach the internet and retrieve/submit it's data. But this data is in "plaintext" now. Who can guarantee us that the dudes running the Exit Nodes aren't sniffing the traffic? Even with the use of SSL, what if they launch a SSLstrip attack? See, it's wasn't that safe as it sounded at first. So, don't use TOR when you are going to use online services that require "login" else you run a risk of getting your credentials or cookies stolen. TOR does NOT support UDP protocol, so don't use any Bittorrent client with it.

Here you have a list of the TOR projects: <http://47du>

Misc. Use online virus scanning engines

So we downloaded X file from the internet, how can we be sure that it isn't infected? Simple. Submit to one of these online virus scanning sites that will scan your file with 20+ more antivirus engines. Such sites for example VirusTotal.com will even submit your files to analysis to several AV vendors to see if there's any FUD malicious code on it. If there is, it will be added to the signature database of them.

Make a Self-Destruct message after being read

So, we may have to tell someone stuff which is incredibly secret or we don't want anyone else other than the person you talking to see it. Privnote.com exactly provides that. After you writing a small note, it will generate an URL which you will send that to your friend. Once the URL is browsed/clicked, the note self-destructs and it's irrecoverable.

Use an encrypted chat server that stores NO logs

So, we have to talk about something highly confidential but we all know that the logs always comes to ruin up our lives. Fear no more! With ChatCrypt.com which uses AES-256 CTR encryption on messages we all can talk about whatever we want without fearing the others and the logs.

I took 1 hour writing this (probably more, I am regularly updating this thread), please leave feedback | comments. Thank you and I hope you enjoyed reading this.

PS: Really like my job? Drop me a bitcoin at 1PQbbxLJqxfQifbPUHATxG4RdPVe6rYY9m to fund my crazy projects*. ?

- The current crazy project is to make a render farm ?

sandeep1024 - September 20, 2012, 2:25 am

nice info and thanks for tools good work :)

Cyba - September 20, 2012, 2:28 am

Very nice tutorial, good job mate. ;)

ali_3boody - September 20, 2012, 6:04 am

great informations thank you alot .

frankie777 - September 20, 2012, 6:12 am

Very nice tutorial man, worth more than the over an hour you put in. Keep it up

akon24 - September 20, 2012, 6:30 am

Thanks for the tutorial m8 .

The best defense is a good offense

Zymfk - September 20, 2012, 6:33 am

Very nice tutorial, I'll bookmark this for later.

Thanks for sharing this to the noobs of HF, makes them feel more secure.

Chelsea Monday - September 20, 2012, 6:36 am

Good TUT, very nice job. Didn't know about DNT, so thank you.

Dr. Michio Kaku™ - September 20, 2012, 7:49 am

Very HQ tutorial.

Thanx for this mate.

samrokzz - September 20, 2012, 9:07 am

Nice info .

Good tutorial. Thanks for sharing this .

EmperorDAZ - September 21, 2012, 3:26 am

Thank you everyone for your feedback.

Dimeblade - September 22, 2012, 9:53 am

really useful TUT, Thankx for the post. :D

EmperorDAZ - September 23, 2012, 12:56 am

@Dimeblade Thank you.

186 views and only 11 replies? What the hell...

Yugen - September 23, 2012, 2:18 am

Amazing Tutorial you have made here.I love how you covered everything,Even a few new thing's that i did not know about :).Thank's.

33Arsenic - October 1, 2012, 1:30 pm

Good tutorial, great information, thanks for sharing!

Cha0 - October 19, 2012, 5:36 am

Very HQ. Good job man. I got something I think you should consider adding. How about Anubis? Even if a virus is totally FUD, you will be able to see what the file actually does.

Cyrqisia - October 19, 2012, 7:37 am

great informations thank you alot . good job

zerocool - October 23, 2012, 4:08 pm

Nice HQ share , well done some very good info ! ?

ps
thanks for key scrambler :0)

Atharva - October 28, 2012, 10:45 pm

Nice Information.
Good Plugins.
KeyScrambler Premium
Thank You !

karthikavinash - October 29, 2012, 1:16 pm

Something i always wanted to know since i joined HF.
Thanks for this :)

Whiteh4t - October 29, 2012, 1:24 pm

WHY DO YOU GUYS KEEP ADDING THE SAME THREADS. THERE IS NOTHING NEW. THIS IS
JUS A BAD VERSION OF THE ONES THAT IS ALREADY HERE.

And no. i havent seen one yet that even helps you not get caught if you do something serious.

DISCO - October 29, 2012, 6:21 pm

Great tutorial. Good information. Very helpful. Good job!

Breakout07 - October 29, 2012, 6:30 pm

wow .. this is a must read for noobs like me haha. thanks alot

triplex-x - October 29, 2012, 10:01 pm

Bro thanks for making such wonderfull tut on Anonymity and Security really helpfull to me

kubalu - October 30, 2012, 1:31 am

Excellent tutorial on anonymity, thanks for taking the time to inform

JasonDotExe - October 30, 2012, 1:48 am

Thats some pretty good info! Thanks alot :)

EmperorDAZ - October 30, 2012, 2:45 am

(Oct 29, 2012 01:24 PM)Whiteh4t Wrote: [\[CITE\]](#) WHY DO YOU GUYS KEEP ADDING THE SAME
THREADS. THERE IS NOTHING NEW. THIS IS JUS A BAD VERSION OF THE ONES THAT IS
ALREADY HERE.

And no. i havent seen one yet that even helps you not get caught if you do something serious.
Is it prohibited? Don't think so. Think it's bad? Ok, I can't really please everyone on the planet so
there's nothing much to do. Well, since you say it's bad, care to make something better instead of
bullshitting it?

jayksp - October 30, 2012, 4:11 am

a very nice guide mate thanks keep it up

Whiteh4t - October 30, 2012, 6:44 am

(Oct 30, 2012 02:45 AM)EmperorDAZ Wrote: [\[CITE\]](#) Is it prohibited? Don't think so. Think it's bad?
Ok, I can't really please everyone on the planet so there's nothing much to do. Well, since you say
it's bad, care to make something better instead of bullshitting it?
yes. maybe i will. i might as well put you in the credit list.

Gable - October 30, 2012, 8:35 am

Nice information. Very nice, and easy to read. Thank you for sharing :-)

meisdave - October 30, 2012, 6:41 pm

this is one of the better tuts thanks a lot bro big help :D

xLJH - October 31, 2012, 10:24 am

Good tutorial, I will try this. Thanks :)

Sly29 - October 30, 2013, 6:48 pm

I am so impressed by this! This is EXACTLY what I have been looking for since day one!!

Many thanks my friend :)

Sly29

The.Repeater - October 30, 2013, 8:33 pm

this is really nice and awesome tutorial. Keep it up.

CaptainDynamic - October 30, 2013, 11:17 pm

solid tutorial, thanks man will put it to good use.

finax - October 31, 2013, 2:29 am

nice tutorial! Thank you, very good explained!

FinaX

hacki27 - December 5, 2013, 9:00 am

Nice tutorial, very good job. Thank you very much for this and keep on...

Killa Priest - December 7, 2013, 7:57 am

Thanks bruh for helping me aware of these.,very great tut.

razzer1337 - December 7, 2013, 9:37 am

Nice information and easy to read. Thank you for this m8.

roks7074 - December 22, 2013, 5:31 pm

Quick question, would multiple VPNs help increase anonymity? Would the 2nd VPN mask the IP from the first VPN or would they both mask your original IP and conflict or does it just not work?

Aman_rempeyek - December 28, 2013, 9:57 pm

Thanks bro for this guide through anonymity. This is also some of the many tips I've searching for....)

Wink Emoticon - January 2, 2014, 10:07 pm

Thanks for the tutorial man. I am not trying to go to jail.

Sedulous - January 20, 2014, 8:54 am

Amazing tutorial! Really helpful, I'll be using this later :)

CrypticTheKing - January 20, 2014, 12:15 pm

Thanks this will help me out in the long run

Lord Mhoram - January 26, 2014, 8:05 am

Thanks this is great, just what I was looking for!

Nightmare™ - February 3, 2014, 7:13 pm

This was a very good tutorial and I really got a lot of good information from it. Great work!

Sexy Devil - February 4, 2014, 10:30 am

Thank you for the detailed tutorial.

Its good to see you recommend AdBlock+

Jarlaxle - February 4, 2014, 2:46 pm

Thanks for the tutorial, useful information ;-)

I????? - February 4, 2014, 6:19 pm

DNT+ works really well.

Although I don't use other services.

I can take care of my anonymity by myself, I made my own VPN, cleared my own tracks and I'm careful enough. :)

Nice post though man!

Fajerfoks - February 23, 2014, 3:13 am

Awesome tutorial! Thanks a lot for this tutorial man.

TheBlackPoison - June 26, 2014, 11:59 pm

I thought that this thread would be exactly like all the other anonymity tutorials i've read but you actually had some unique concepts here. Thanks for sharing

God of Tits - July 3, 2014, 3:33 pm

Does this still work today? Can anyone confirm this today?

asalada - July 18, 2014, 6:30 am

thank you so much for the information

NyxCoder - July 23, 2014, 11:56 pm

nice info and thanks for tools good work :)

OnlyOneNut - July 26, 2014, 3:20 pm

Not a bad tutorial!

Thanks for sharing this!

Not a bad tutorial!

Thanks for sharing this!

Mazinga - October 24, 2014, 4:09 pm

thank you man for this great tutorial

Tsubasa - November 14, 2014, 7:03 pm

Great tutorial. thanks for sharing all the infos

cmind - December 21, 2014, 4:03 pm

thank you really very much i found the tutorial very helpfull and detailed i really think i will use it :D

xJ2eaction - December 22, 2014, 7:50 am

nice info and thanks for tools good work :)

OnlyTigerAlive - December 25, 2014, 9:17 am

Good tutorial op thanks for sharing with us. Going to be useful.

haxedsh1t - December 27, 2014, 8:37 am

I am using ghostery as browser plugin too. You might look into that aswell!

TheHighProphets - December 27, 2014, 4:12 pm

Thank you for this OP I can see you put a lot of effort in and will make sure to use these.

Motojojo - December 28, 2014, 5:49 pm

Privnote.com is rarely used, also there better ways to chat without lgos being stored.

Just a note; why are the links replaced with #'s?

Olethea - December 28, 2014, 6:54 pm

(Dec 22, 2013 06:31 PM)roks7074 Wrote: [\[CITE\]](#) Quick question, would multiple VPNs help increase anonymity? Would the 2nd VPN mask the IP from the first VPN or would they both mask your original IP and conflict or does it just not work?

I'm not sure if it does work, but if it does, it would work very slowly. You're layering encryption and TCP packets on top of more encryption and TCP; I don't know the math, but I'm pretty sure it would dramatically slow downloads and uploads, maybe exponentially. Not to mention that VPNs aren't panaceas; layers of them sound like more trouble and time to implement than they're worth. You'd probably be better off with just one.

Anonload - January 8, 2015, 10:11 am

Thanks for this fucking awesome tutorials.....
u r awesome..

#Infinite - January 8, 2015, 10:16 am

Thanks for sharing this HQ tut.

Thanks Again.

dastyrus - January 9, 2015, 10:46 am

Nice tutorial, you did a great job.

MentalWarfare - January 9, 2015, 12:14 pm

Great tutorial, I'm now using some of the things you recommended :)

woahxx - January 10, 2015, 1:39 am

Found some cool chrome addons that could help me.

ISO - January 10, 2015, 2:54 am

Good ressource man , thanks for the share.

PrettyMelvin - January 14, 2015, 5:40 pm

This is an amazing tutorial. Thanks OP

jakedav - January 15, 2015, 6:43 am

Commenting to bookmark this amazing anonimity post

Bucked - January 15, 2015, 7:30 am

Nice tutorial, but do NOT use true crypt. I cant believe that people still think that it is safe...

voldemort725 - January 15, 2015, 12:55 pm

Very nicely written. A lot of sites that I haven't heard of before.

Fajerfox - January 19, 2015, 9:49 am

Thanks for all link and very nice tutorial bro!

Gangolian - January 27, 2015, 9:44 am

Great all around information on hardening networks/user systems. You can never go wrong with spreading good privacy & protection information techniques. Thank you.

FRANKIE - January 27, 2015, 9:44 am

(Jan 27, 2015 10:44 AM)Gangolian Wrote: [\[CITE\]](#) Great all around information on hardening networks/user systems. You can never go wrong with spreading good privacy & protection information techniques. Thank you.

You just gravedug a thread from 2012.

Xch4ng3 - January 27, 2015, 9:47 am

(Jan 27, 2015 10:44 AM)FRANKIE Wrote: [\[CITE\]](#) You just gravedug a thread from 2012.

As long as the post isn't breaking any rules, there's no specific rule against grave digging. A thread from 2009 may well still be relevant.

Please don't abuse the report button.

FRANKIE - January 27, 2015, 9:47 am

(Jan 27, 2015 10:47 AM)Xch4ng3 Wrote: [\[CITE\]](#) As long as the post isn't breaking any rules, there's no specific rule against grave digging. A thread from 2009 may well still be relevant.

Please don't abuse the report button.

That's a good point and I understand you are busy. My mistake.

afexmillion - February 8, 2015, 7:50 am

Great tutorial. I sure need something like this for total security. Thanks

Silver Fang - February 8, 2015, 7:59 am

Im not sure if its just rumours but truecrypt have been exploited and someone stated that its not safe to use anymore for some reason.

itoxiik - July 30, 2015, 1:20 pm

great tutorial buddy. Thanks for the share!

playback121 - January 12, 2016, 7:10 pm

thx man. LOTS of help. :)

n3cr0 - February 5, 2016, 1:10 am

good tutorial. There are good benchmark guides put out by CIS which are good to follow to lock down your machine. Also its good to use virtual machines for web browsing Tails 2.0 was just released which is good for TOR browsing. I always would use a VPN on top of this. Veracrypt is a

good fork of truecrypt with a few more features. I would also recommend getting a FREE firewall such as zone alarm or comodo just as a basic level of protection, Peerblock is a good tool for downloaders. Some additional extensions such as Ghostery, Noscript, Quickjava, Web of trust, bug me not and trashmail (for temp emails). Another one is to not use the same username and password everywhere make sure you mix it up save it in a password manager such as keepass.

SIM-2122005 - *February 5, 2016, 2:22 am*

Thanks for the tutorial, guess im learning something new every day on here.

1x10x1x10x1 - *February 5, 2016, 6:06 am*

Seems like a good tutorial! Thanks OP.

zer0pwn - *February 5, 2016, 7:25 am*

i feel like the noscript addon is mandatory as well

ingenious - *February 5, 2016, 12:30 pm*

Thankyou for this tutorial

It helped me alot!