

Forum:[Hack Forums](#)

Thread: [\[TUT\] Complete Anonymity Online! \[Detailed\]](#)

S-Moneyy - February 4, 2012, 9:12 pm

Main Tips:

Encrypt everything.

Wipe everything non-encrypted.

Audit your networks connections (look for DNS queries going to your ISP).

No open ports.

Use a different machine for Anonymous.

Make fresh OS installs every month or so (and keep it updated).

Try to re-route your connection at least 2 times.

Keep secure. http://cryptoanarchy.org/wiki/Main_Page

-> DONT talk to the police. Ever. So dont even explain why you arent saying anything, just shut your mouth untill you are back home again, no matter how long it takes. They will lie to you. They will threaten you. They may even hurt you. But you CANT say a SINGLE WORD.

Contents:

Encryption

Document Shredding

MAC Spoofing

VPN/VPS

Tor & I2P

DNS

Assorted

Firefox Plugins

Encryption

Store sensitive files on encrypted volumes. Encrypt your files AES256

Use Truecrypt! - <http://www.truecrypt.org/>

Document Shredding

Shred all your documents non encrypted on a daily/weekly basis.

Keep them centralized.

NOTE for SSD disks users: enable the TRIM function, usual shredding methods are not suitable for them.

<http://askubuntu.com/questions/18903/how-to-enable-trim>

Linux

apt-get install wipe

wipe -r -P 7 folderToTrash

Mac OS X

For the Terminal Savvy:

srm -r

Others:

Put files into the bin and then Finder > Secure empty Trash

Windows

Expert needed

MAC Spoofing

MAC Spoofing is changing your unique MAC address to something more secure; like a line of zeros.

Linux

apt-get install macchanger

after that do:

sudo macchanger -A eth0 <--- eth0 is the interface, use sudo ifconfig -a to show all interfaces, don't use lo0, that is a loopback interface

or

sudo ifconfig wlan0 down

sudo ifconfig wlan0 hw ether 00:00:00:00:00:00

sudo ifconfig wlan0 up

-> You can do this every boot up automatically.

<https://we.riseup.net/riseuphelp+en/auto-random-macs>

Script to be placed and chmod +x in /etc/network/if-pre-up.d/macchanger

```
#####
```

```
#!/bin/sh
```

```
MACCHANGER=/usr/bin/macchanger
```

```
ifconfig eth0 down
```

```
macchanger -A eth0
ifconfig eth0 up
#####
```

->>> Replace eth0 with the interface you use to connect to the net. In order to know that, type in console: `sudo ifconfig` or `/sbin/ifconfig`

->>> The output will be a list of interfaces,

lo : local loopback
wlan0: wireless interface
eth0: ethernet interface
tap or tun0: VPN interface.

-> Also keep in mind that, even if you spoof your mac, if you are behind a router, it's the routers mac that's exposed, not your computers, so if you want this to work, you need to use a vpn. (Tips to firewall a vpn conn would be niceness too)

-> A good way of firewalling your linux, is using ufw (uncomplicated firewall) it's easy, and you don't need to know shit about iptables to make it work + it has a very simple interface (gufw). A more complete gui, and more complicated, is the well known firestarter.

-> To know the services listening on your box type the following in console
`$sudo netstat --tcp --udp --listening --program`
You're done when there's 0 listening programs in that list. (Avoid dhclient if you can, as for openvpn, firewall it properly)

-> send to /dev/null all the users that have suspicious activity (such as nobody, or in some cases proxy when u got tor installed.)
`$sudo chsh -s /dev/null nobody`

-> check this article for tor advanced (and very interesting) usage.
<http://thesprawl.org/memdump/?entry=8>

Mac OS X

1. Paste the following into Terminal (Applications/Utilities/Terminal.app):

```
sudo su
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport
/usr/sbin/airport -z
sudo ifconfig en1 ether 00:00:00:00:00:00
```

2. Reconnect to a wireless network!

For wired connections, change 'en1' to 'en0.'

BSD

1) Bring down the interface: `"ifconfig xl0 down"`

2) Enter new MAC address: `"ifconfig xl0 link 00:00:00:AA:AA:AA"`

3) Bring up the interface: "ifconfig xlo up"

Linux

1) Bring down the interface: "ifconfig eth0 down"

2) Enter new MAC address: "ifconfig eth0 hw ether 00:00:00:AA:AA:AA"

3) Bring up the interface: "ifconfig eth0 up"

Windows 2000/XP

Method 1:

This is depending on the type of Network Interface Card (NIC) you have. If you have a card that doesn't support Clone MAC address, then you have to go to second method.

a) Go to Start->Settings->Control Panel and double click on Network and Dial-up Connections.

b) Right click on the NIC you want to change the MAC address and click on properties.

c) Under "General" tab, click on the "Configure" button

d) Click on "Advanced" tab

e) Under "Property section", you should see an item called "Network Address" or "Locally Administered Address", click on it.

f) On the right side, under "Value", type in the New MAC address you want to assign to your NIC. Usually this value is entered without the "-" between the MAC address numbers.

g) Goto command prompt and type in "ipconfig /all" or "net config rdr" to verify the changes. If the changes are not materialized, then use the second method.

h) If successful, reboot your system.

Method 2:

This should work on all Windows 2000/XP systems

a) Go to Start -> Run, type "regedt32" to start registry editor. Do not use "Regedit".

b) Go to "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}". Double click on it to expand the tree. The subkeys are 4-digit numbers, which represent particular network adapters. You should see it starts with 0000, then 0001, 0002, 0003 and so on.

c) Find the interface you want by searching for the proper "DriverDesc" key.

d) Edit, or add, the string key "NetworkAddress" (has the data type "REG_SZ") to contain the new MAC address.

e) Disable then re-enable the network interface that you changed (or reboot the system).

Method 3:

Use the program Etherchange from <http://ntsecurity.nu/toolbox/etherchange/>

Windows 9x

Use the same method as Windows 2000/XP except for the registry key location is "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Net" and you must reboot your system.

VPN/VPS

Links about tested VPNs services:

<https://www.vpntunnel.se>

<https://www.perfect-privacy.de>

<https://www.swissvpn.net/>

<http://nvpn.net/index.php>

Links about offshore VPS offers:

ipo

<http://heihachi.net/>

http://zhangltd.net/plans_at.html

<http://www.dataclub.biz/en/site/services>

<http://www.santrex.net/vps-hosting.php>

Other anonymisation services to hide your IP address

JonDonym <https://anonymous-proxy-servers.net> uses mix cascades with 2 or 3 mix servers around the world. Free mix cascades can be used only for anonymous surfing. Premium services can be used for all internet services like IRC, email or IM.

Tor <https://www.torproject.org> uses a route of 3 onion routers around the world. The route will change every 10 minutes. Because everybody can run a Tor node it is possible for intelligence services to insert spying nodes. Use SSL encryption to avoid traffic sniffing by spying exit nodes.

I2P

The very best of the deep internets. Anonymously host, visit, and everything else. Recommended.

<http://www.i2p002.d>

<https://www.vpntunabout:startpagenel.se>

e/

#Anonymous on I2P standard IRC.

DNS

Open DNS Servers:

=> Service provider:Dnsadvantage

Dnsadvantage free dns server list:

156.154.70.1

156.154.71.1

=> Service provider:OpenDNS

OpenDNS free dns server list / IP address:

208.67.222.222

208.67.220.220

=> Service provider:Norton

Norton free dns server list / IP address:

198.153.192.1

198.153.194.1

=> Service provider: GTEI DNS (now Verizon)

Public Name server IP address:

4.2.2.1

4.2.2.2

4.2.2.3

4.2.2.4

4.2.2.5

4.2.2.6

=> Service provider: ScrubIt

Public dns server address:

67.138.54.100

207.225.209.66

Other anti-censorship DNS servers:

85.88.19.10 (German Xail.net) sehr schnell!

85.88.19.11 (German Xail.net)

87.118.100.175 (German Privacy Foundation e.V.)

94.75.228.28 (German Privacy Foundation e.V.)

62.141.58.13 (German Privacy Foundation e.V.)

62.75.219.7 (German Privacy Foundation e.V.)

85.214.73.63 (FoeBuD e.V.)

212.82.225.7 (ClaraNet)

212.82.226.212 (ClaraNet)

213.73.91.35 (Chaos Computer Club Berlin) +1

58.6.115.42 (OpenNIC, Australien)

58.6.115.43 (OpenNIC, Australien)

119.31.230.42 (OpenNIC, Australien)

200.252.98.162 (OpenNIC, Brasilien)

217.79.186.148 (OpenNIC, Deutschland)

82.229.244.191 (OpenNIC, Frankreich)
216.87.84.211 (OpenNIC, USA)
2002:d857:54d2:2:20e:2eff:fe63:d4a9 (OpenNIC, IPv6 USA)
2001:470:1f07:38b::1 (OpenNIC, IPv6 USA)
2001:470:1f10:c6::2 (OpenNIC, IPv6 USA)
66.244.95.20 (OpenNIC, USA)
204.152.184.76 (f.6to4-servers.net, ISC)
2001:4f8:0:2::14 (f.6to4-servers.net, IPv6, ISC)
194.150.168.168 (dns.as250.net; anycast DNS!)
80.237.196.2 (Erdgeist)
194.95.202.198 (UDK Berlin)
88.198.130.211 (Dataflash)
78.46.89.147 (ValidOM)
129.206.100.126 (URZ Uni Heidelberg)
79.99.234.56 (justnet.ch, Schweiz)
208.67.220.220 (OpenDNS)
208.67.222.222 (OpenDNS)
156.154.70.22 (Comodo Secure DNS)
156.154.71.22 (Comodo Secure DNS)
85.25.149.144 (Freie DNS-Server)
87.106.37.196 (Freie DNS-Server)
8.8.8.8 (Google Public DNS)
8.8.4.4 (Google Public DNS)
88.198.24.111 (jali/CCCHB)

Google ones

8.8.8.8

8.8.4.4

-> These ones are good. We all know google is evil, but their DNS services process much traffic. This is security by obscurity, finding a request to them is like finding a needle in the sea!

What about Level3 dns servers? safe?

youtube link for dns tut

<http://www.youtube.com/watch?v=r8d-Sv2> ifconfig eth0 lladdr 00:00:00:00WCQ

http://www.youtube.com/watch?feature=player_embedded&v=CBJalahhH20

http://www.youtube.com/watch?feature=player_embedded&v=wwS6Jufjqds

http://www.youtube.com/watch?feature=player_embedded&v=CBJalahhH20

http://www.youtube.com/watch?feature=player_embedded&v=wwS6Jufjqds

bypassing DNS filters

<http://pastehtml.com/view/ax99xkcpi.rtxt>

Assorted

- rule #1 before dishonour and rule #2
- /dev/null before dishonour

- do not mention your involvement with \$operations
- do not swank with your e-peen
- do not mention your YT, Twitter, FB... accounts
- do not swank with any special knowledge
- speak english only
- use password with more than 10 characters
- dont re-use passwords

-> Generating strong passwords (Linux)

```
$ cat /dev/urandom | tr -dc '[a-z][A-Z][0-9]_!@#$%^&*()_+{}|:<>?=' | fold -w 64 | head -n 5
```

This will generate a 5 rows of 64 char long password with symbols, numbers and letters. Change the -w value suit your needs. -w 128 will generate a 128 char passwd

- use keepassx
- use Live-CDs and thumbdrives and portable software
- do not keep logs of any kind
- repeat after me: I will not keep any logs
- pay your VPN with bitcoin, Ukash etc.
- choose a VPN-Provider in a safe jurisdiction (that means not US, UK, France)
- using your neighbours Wifi is not a very good idea, but on the other hand... better than get arrested
- only inexistent data is good data, because any existing data will be used against you
- Govs will even use inexistent data against you
- do not use your anonops-nick anywhere else (Change your nicks oftenly)
- it is a good idea to change the OS every now and then
- it is a good idea to physically separate anything Anon from anything not Anon, use different machines
- do not use the same E-Mail or VPN you use for Anon for other activities
- if you have to keep data, put it on thumbdrives so they can easily be destroyed > micro sd drives are twice as easily destroyed and die after an ammount of writes.
- keep in mind that a single Anon is unimportant to Anonymous
- the media will not keep your identity secret because the media sell information, do not trust the media (<https://www.eff.org/deeplinks/2011/06/ws...wers-false>)
- do not expose yourself too much, avoid IRL-Interviews, avoid Voice Interviews
- sadly, you cannot trust other Anons
- report suspicious activities
- be paranoid
- keep a low profile
- tell others when you will not join the IRC for al longer time
- before issuing any documents erase their metadata

Port Scans

<http://www.port-scan.de>

Links

<http://www.truecrypt.org> (encrypting software , who cant read will not know)
if they see that you have truecrypt installed, they will know. see <http://xekcd.com/538/>
<http://www.comodo.com> (firewall)
<https://wiki.archlinux.org/index.php/LUKS> (even more encryption)

Firefox Configuration

Firefox about:config

network.proxy.socks_remote_dns = true
browser.search.suggest.enabled = false
layout.css.visited_links_enabled = false
network.http.sendRefererHeader = 0
geo.enabled = false
browser.display.use_document_fonts = 0

Try to have a common fingerprint for your browser:

<http://panopticklick.eff.org>

-> The more unique your browser looks, the more the bad guys will identify you.

Firefox Addons

- Cookieculler (cookies can trace u do not keep logs !)
- HTTPS everywhere (secured is encrypted (Y))

Modify Headers

<https://addons.mozilla.org/en-US/firefox...y-headers/>

RequestPolicy

<https://addons.mozilla.org/en-us/firefox...estpolicy/>

NoScript

<https://addons.mozilla.org/en-us/firefox.../noscript/>

Certificate Patrol

<https://addons.mozilla.org/en-us/firefox...te-patrol/>

AdBlock Plus

<https://addons.mozilla.org/fr/firefox/ad...lock-plus/>

Mafiasa redirector

<https://addons.mozilla.org/en-US/firefox...edirector/>

Better privacy

<https://addons.mozilla.org/fr/f/encryptfirefox/addon/betterprivacy/>

User Agent switcher

<https://addons.mozilla.org/en-US/firefox...-switcher/>

<http://techpatterns.com/downloads/firefo...itcher.xml>

xxjokerxxx - February 4, 2012, 9:15 pm

wow thanks much for all these tips man , i just needed something like this , i was not sure if iam anonymous online and when i read this i can be sure iam not :D That was the prob my state searched and found me once -.-

thx dude hers a comment for your nice and detailed work !

HQ

Fr33zeface - February 4, 2012, 9:16 pm

I am planning on reading all of this, looks extremely HQ. We need more posts/TUTs like this!

Johnny Ramone - February 4, 2012, 9:17 pm

Great tut. Thank you very much putting up this thread. An excellent firefox proxy addon is anononymoX. It's faster and easier to use than most web based proxies.

kwmwtaj - February 4, 2012, 10:17 pm

Would you recommend Technitium MAC address changer or do you think my anonymity would be comprised if I overlooked logs that they might keep of people. O.o

Superior1 - April 14, 2012, 2:09 am

when you said they may even hurt you.. is that in canada too cuz i hear they go soft on you here

crackhackforum - April 14, 2012, 2:24 am

Great tutorial.Thanks :)

Bookmarked :P

Superior1 - April 14, 2012, 2:59 am

GREAT tutorial i hope this helps me

kjohn - April 14, 2012, 3:41 am

Thanks for sharing dude :)

Very nice!

Root - April 14, 2012, 8:54 am

Good guide, however the majority of users dont seem to be interested in anonymity, even though it is so important. Shame really (check my sig, same thing happened to me)

MaxPain - June 12, 2012, 10:30 am

That is really awesome tutorial brother, seems that you know what you doing, remember guys using no logged software, and use malware bytes ofc :D , good luck everone ?

Dynasty@HF - June 12, 2012, 11:27 am

perfect explanation and guide on how to stay hidden online.

SIM-1317084 - June 12, 2012, 12:22 pm

(Feb 4, 2012 10:15 PM)xxjokerxxx Wrote: [\[CITE\]](#) wow thanks much for all these tips man , i just needed something like this , i was not sure if iam anonymous online and when i read this i can be sure iam not :D That was the prob my state searched and found me once -.-

thx dude hers a comment for your nice and detailed work !

HQ

lol

lol lol

lol lol lol

only lol

KaRwaN - *June 12, 2012, 3:41 pm*

Great tut. Thank you very much putting up this thread

A New Newb - *June 13, 2012, 7:40 am*

When the cops come at your door, just say that you have the right to remain silent. They can't do anything to you then. As long as they do not have solid proof (email history of you sending your friend "1mz 31337 h4x0r" is not enough) they can not harm you.