Anonymous – The Über-Secret Handbook

Version 2.0
Date 20.02.11

DRAFT VERSION

contains Typos
contains <°-(-(-(-<
contains no (o) (o)
also, no 8====D
also, tl;dr & cocks

Preface

The greatest threats to your safety are:

I. Social engineering and your behavior - see Social Threats.

II. Revealing your IP address - see Technical.

Try to follow as many of these suggestions as possible to ensure maximum privacy.

Social Threats

Basic rule: Blend in with the crowd, disperse into the stream. Keep a low profile. Don't try to be special. Remember, when in Rome, do as Romans do. Don't try to be a smart ass. Feds are many, Anonymous is Legion, but you are only one. Heroes only exist in comic books keep that in mind! There are no old heroes; there are only young heroes and dead heroes.

Do not give any personal information on the IRC chat as it is public, you mom could read what you write there and so could the Police. And don’t mention your involvement with Anonymous in your real life.

DO NOT:

∗Include personal information in your screen name.

∗Discuss personal information, your address or where you're from.

∗Mention your gender, tattoos, scars, piercings, body modifications, your weight or your physical and/or psychological capacities (got the idea?).

∗Mention your profession or hobbies or involvement in other activist groups.

∗Mention whether you're in a relationship.

∗Musical tastes/preferred literature/films are good ways to know someone, don't mention any of those.

∗Use special characters, which are existent only in your language, as they would reveal where you are from.

∗Give even bogus info. Lot's of no's, make a yes.

∗Blend anything from your real life with Anon, don't talk about Anonymous in real life except posting posters anonymously, etc.

*Mention congresses that you have been at, schools or universities, etc.

*Mention your time zone, this can reveal where you live.

*Connect at the same time regularly. Try to alternate.

*Post on the public net while you are in the IRC, and definitely do not mention that you are posting something on Twitter. This is easy to correlate. Stagger your login & log out times on FaceBook, Twitter & IRC. They can be compared for user info.

*Discuss whether you are personally DDoSing or writing How-To's or making graphics etc. or not, just discuss general strategy.

*Post pictures hosted on Facebook. The filename contains your profile ID.

Technical

Basic Rule: Use as many security layers as possible. The question is not whether you are paranoid, but whether you are paranoid enough?

A good start is to use a VPN and run Anonymous related Software from a USB device. A proxy will also do, but it is not as secure as a VPN.

Always use as many security layers as possible. Make sure to use them in the right way. If you don't know how to use them, learn first.

Most Anonymous' use VPN to hide their traces. They use SSL encrypted connections and #vhost when they are on irc.anonops.ru.

Portable Software

Portable software is a software which you can run from an USB drive, so that it leaves almost no traces on your computer.

* http://portableapps.com
* http://portableapps.com/apps/internet/firefox_portable
* http://portable-i2p.blogspot.com

When you join the Anonymous IRC network, do so only via SSL (point you IRC client to port 6697). Port 6697 is an unusual SSL port, just checking the "Always use SSL" box will not work, check for both.

After connection you can register your nickname by using a fake email address, then you join `#vhost` and AFTER that procedure you join the channels.

Make sure you start by launching I2P with the "I2P Launcher" button in the portable apps tray icon.

You can then use the integrated PChat client; it automatically connects to the I2P IRC server anonymously.
Join #anonops for to keep track of Anonymous activity. Many Operations channels are relayed between I2P and anonops.ru.

VPN

When thinking of a VPN service, think first about the legislation of the country. A USA VPN might provide user data upon warrant issue. In other countries such as Sweden and Iceland, this is unlikely to happen. They have a strong privacy policy, which makes it harder for law enforcement agencies to get access. In addition, some servers do not keep logs of users. Also try to get VPN services that accept anonymous payments (For those that keep user billing information)

More info:

https://secure.wikimedia.org/wikipedia/en/wiki/Vpn

Free VPNs -- **Not recommended.**
If they aren't selling you a service they are selling you.

* http://cyberghostvpn.com
* http://hotspotshield.com -- Occasionally hijacks your traffic to redirect you to advertisers.
* http://proxpn.com
* https://anonymityonline.org

* http://www.bestfreevpn.com
* http://www.your-freedom.net
* http://www.ultravpn.fr
* http://www.itshidden.com
* http://www.thefreevpn.com
* http://www.packetix.net

Commercial VPN providers

* http://www.swissvpn.net
* http://perfect-privacy.com
* https://www.ipredator.se
* http://www.anonine.se
* https://www.vpntunnel.se
* http://www.relakks.com
* http://www.steganos.com
* http://www.bananavpn.net > logs IPs
* http://www.strongvpn.com > logs IPs
* http://www.secureix.com
* http://www.secretsline.com

* http://www.findnot.com
* http://www.trackbuster.com
* http://www.vpngates.com
* http://www.perfect-privacy.com
* http://www.trilightzone.org
* http://www.vpnaccounts.com
* http://www.securstar.de
* http://www.witopia.net
* http://www.tiggerswelt.net
* http://www.xerobank.com > logs IPs

Extra info about VPNs

List September 2010 - (Korben source)

* http://itshidden.com - PPTP Vpn - 2 offers: Free and Premium ($ 12.99 / month - $ 24.99 / 3 months). Regarding free: there are regular disconnections every 20 minutes, the P2P is legal but inconceivable. The charge: Premium offers including improved speed for downloading, a static IP and port forwarding. The two options both offer direct access to a VPN secure and anonymous. Servers in the Netherlands in particular.

* http://www.bestfreevpn.com
* http://www.cyberghostvpn.com - OpenVPN - Installing a software house - 1 GB / month - off after 6h (reconnection possible) - no guarantee of flow
* http://www.peer2me.com - PPTP - Provides free and unlimited. French company banned = P2P in France. You can create a private community to share your data.
* http://www.hotspotshield.com/ - Software - U.S. servers, adds advertising on web pages. Firefox with adblock and found no ads. Note that you can use it with the public HotSpots New / SFR WiFi.
* http://www.ultravpn.fr/ Openvpn - Vpn free. - Server Lynanda France, the United States. P2P forbidden on this vpn.
* http://www.hideipvpn.com/ Hide - PPTP - VPN offering 100 free accounts beginning of each month. The paid version allows you to connect to openvpn. P2p is not allowed with this vpn.
* http://www.janusvm.com/ - JanusVM VPN Free (open source) and free. - Using VMware virtual machine and based on OpenVPN, Squid, Privoxy and TOR. An old but useful tutorial incompleted is available in French. - A VPN Hardware JanusPA called hardware-based brand Yoggie is also since 2009. P2P forbidden because of the philosophy TOR.

Payable VPNs:

* http://www.vpnfacile.fr - VPN - Site in French, without limits or quotas. The web's cheapest (and en) 5 € / month maximum, minimum flow guaranteed 5mb / s! 2048bits encryption and support very responsive!
* http://proxydaddy.net - OpenVPN / PPTP - quick access without limitations Europe and USA. Site and support in French and English.

* https: / / www.change-my-ip.com - OpenVPN, and PPTP VPN SSTP - From 5 € / month. Servers in the Netherlands, USA and UK. Support and French site. No logs, speed and unlimited tranfer.
* https://www.anti-hadopi.com - OpenVPN / PPTP / Routers - Website in french, no speed limits or transfer. The network is fast (the site a bit slow but certainly housed outside U.S.), IP access with Europe or USA for € 4.99 per month. Just the logo on the page worth visiting. Staff nice.
* http://s6n.org/arethusa/fr.html - OpenVPN Established by an association campaigning for freedom of expression.
* http://xangovpn.com/ - OpenVPN, 4.90 € per month with no speed limit, server in the Netherlands, no logs, SSL key-1024, open enrollment. XangoVPN supports Quadrature du Net qu'FDN well.
* http://fvpn.fr/ - OpenVPN, from € 1.35 per week with no speed limit, server in France, 4 ip changeable 24/24, private VPN creates for French, 2048 and encryption keys with AES- 256.Inscriptions still open.
* http://www.hidemynet.com/ - OpenVPN, L2TP and PPTP VPN using OpenVPN-AS - $ 5 per month is about 3.50 €. Servers in Germany, United Kingdom, Netherlands and USA
* https://www.ananoos.com/ - OpenVPN - from € 4.58 per month, registration reopened!
* http://ipjetable.net/ - PPTP Vpn - 15 € per quarter, closed Beta invitations.
* https://ConnectionVPN.com / en - OpenVPN - Site in French - about 4 € and 5 € per month, unlimited traffic and speed, Key of 2048 bits, a company registered in Greece, servers in Luxembourg, the Netherlands ...
* http://www.psilo.fr/ - OpenVPN - 4.50 € per month, servers outside of France (Europe or USA, your choice), P2P servers allowed on Europe, AES-256 encryption, open enrollment.
* http://www.IdealVPN.com/ - Site in French - PPTP Vpn - 4.90 € per month, unlimited volume and speed, open enrollment. Quality service for a small price. Servers in the Netherlands, Germany ...

* http://www.tonvpn.com - Site in French. SOCKS, PPTP VPN, OpenVPN - 4 to 13 € per month Discount over time. Allopass possible! Speed and unlimited traffic. Free trial of 3 days. Servers in France, Slovenia, Luxembourg, Bulgaria.
* https:// www.ipredator.se/ - PPTP Vpn - 149kr or 14.9 € for 3 months, open enrollment. Uses the network Relakks Sweden.
* https://www.relakks.com/?lang=en - PPTP Vpn - 149 SEK (about 15 €) per quarter, and 449 SEK (about 45 €) per year. Servers in Sweden.
* http://www.anonine.com/ - PPTP VPN, 40Kr or 4 € per month with no log and no speed limit, server in Sweden. Registration open.
* http://www.blackvpn.com/ - Vpn unlimited speed available with openvpn or pptp server choice in europe or the usa for 5 € a month or two for 10 € a month, entries open ..
* http://www.mullvad.net - OpenVPN - 5 € / month with 50 GB of traffic - Free Trial 3h - Company in Sweden, servers in the Netherlands in particular - Redirection of a port.
* http://unblockvpn.com - PPTP Vpn - $ 5 per month but only 2GB per day guaranteed.
* http://www.vpnboy.com - PPTP Vpn - $ 5 per month or about 3.5 € - Reviews free 7d.
* http://www.torrentfreedom.com/ - VPN is the only specially configured for P2P applications - and BitTorrent in particular. OpenVPN on all accounts and subscribers can use both public and private trackers. 2048-bit key that changes automatically every 20 minutes. $ 17 per month
* http://www.perfect-privacy.com - $ 24.95 per month with an additional setup fee of $ 10. The VPN also offers solutions with keys of 4096 bits: PPTP, OpenVPN, 4096 bit SSH-2, 4096-bit SSL / TLS, Squid Proxy, CGI Proxies, Servers and more ... all over the world. In the peak of the servers (usually between 7am and 11am)

subscribers are "encouraged" not to exceed 100GB per month. The rest of the time no limits. Anonymous payments possible (Liberty Reserve, Web Money, Cash ... and PaySafeCard).

* http://vpngates.com - $ 15/month. No setup fees. PPTP, L2TP IPSec VPN services.
* http://www.linkideo.com - PPTP - From 2 € to 10 € / month depending on connection speed and getting or not to open ports. Support friendly and responsive enough. Servers in the U.S., France, the Netherlands.
* http://www.flashvpn.com - Starting from $ 5/month for VPNs, and $ 8 for OpenVPN. Found in the forums of people screaming for the scam that VPN (payment and no account), so caution.
* http://www.purevpn.com - PPTP and L2TP/IPSec VPN. From $ 6 per month. Servers in the U.S., Britain, Germany and Canada. Dedicated IP VPN for $ 15/month. "There are no limits to our VPN service. However, we do not recommend using it for torrents and p2p in violation of copyright. "According to the administrator. Is it to cover themselves or to protect its bandwidth ...
* http://www.securenetics.com - From $ 9.49 per month to $ 39.45. Opportunity also to use the proxy only for $ 5.49 per month. A choice between the Secure Anonymous OpenSSH Proxy, OpenVPN, PPTP VPN, Socks Proxy, or HTTP proxy servers. An industry first to offer this variety of options. Free anonymous email included in all accounts. Servers in the U.S., Britain, Canada, Germany, Netherlands, Malaysia. Anonymous payments by Liberty Reserve, Pecunix, and PaySafeCard.
* http://vpnprivacy.com/ - PPPTP Vpn - $ 15/month, $ 5 for a week. Gladly accepts P2P (the owner says). Servers in the U.S. and Canada.
* http://www.smallvpn.com - From $ 19.95/month to $ 34.95 depending on the OpenVPN server (2048 bits)
* http://www.lamnia.co.uk/ * - From £ 6.5 per month. Servers in the U.S., Britain and Canada.

* http://vpnpronet.com/ - A nice selection of alternatives. Per month, $ 8, there is a good classic. At the time (10h, 20h etc. ..) handy when you will spend the weekend with friends and we do not want "" rot "their IP. Or as the limit of the bandwidth required
* https: / / www.cryptocloud.com/ - $ 17/month. 2048-bit key. Very reliable (a disconnection in six months). About once a week, your server output changes (transparently) so that your IP changes and it is also extra security. It's not always easy to install OpenVPN client type. This provides a vpn setup very simple, just enter the username and password. This vpn is very committed to the freedom of the internet worldwide. He collaborates with the Electronic Frontier Foundation and opened free accounts for militants threatened in their country. If you fear a VPN keeps your logs, this one is one of the safest.
* http://www.banana-vpn.info - PPTP and L2TP/IPSec Vpn - $ 15/month, $ 60 per semester. Servers in the U.S., Britain and Germany. "P2P and Other Illegal use it Not Allowed. Filesharing ports, protocols and sites are blocked. "Says the site in red.
* http://ivacy.com/ * - Price: 10 € / month, 25 € / 3 months, € 0.5 / 1Gb, 100 Mb free for testing - Payments: Paypal, Visa, MasterCard, Ukash - Connection: OpenVPN, PPTP, IPsec - Encryption: MPPE PPTP 128, IPSec ESP 3DES, AES-256 Firefox Extension, OpenVPN 2048bits RSA for authentication and Blowfish 128 for the data - Servers: Great Britain, Russia, United States (down at the moment, seems Is it because of the DMCA notices ...) - P2P: Port forward from 5 random ports, TCP and UDP-Bonus: Firefox Extension, usenet server, internal ivacy sites, utilities ivacy.
* http://www.drakker.com/ * - Price: 25 € / year, 1 week free evaluation - Data encryption via VPN to 1024 bits - certificates exchanged are unique to each user. Changing the IP address: IP address is replaced by that of Drakker servers. Servers in Great Britain, Netherlands, Sweden, Canada. Confidentiality: The network collects and Drakker do not have any data about its users. Portability: it takes is a username / password to use his account Drakker

worldwide. The network Drakker promotes freedom of expression and press freedom worldwide. He is a partner of Amnesty International, Reporters without Borders, and the project 'Enough' for Africa.

* http://www.yourprivatevpn.com - PPTP. Site in French, Price: 6 to 15 € per month free trial. Servers in Great Britain, Netherlands, United States. Changeable servers at each connection. Ideal for sites like hulu.com geo-limits, BBC iPlayer. Very reliable and has great speed.

Proxies

You may use them in conjunction with a VPN.

* http://www.freeproxies.org
* http://www.socks24.org
* http://www.samair.ru/proxy

How to IRC

Basic Rules:

Use SSL Port (in this case 6697). Always.

Use a #vhost. Always.

IRC is public, if don't want an information to be spread in public, don't give this information in the first place.

Ignore trolls. Always.

http://anonnews.org/help/en.html

General:

By connecting to SSL-Port 6697 your IRC-Client may give you a warning because the SSL-Certificate is self-signed. That is OK; you can trust the anonops' certificate.

*****Nicknames:
Make sure to pick a good username. For Anonymous related activities it means: don't use a nickname that you already use in general or public online spots. This way you ensure that you won't be tracked down by a common username you use on your gamer profiles or other websites where you might have put real life related info.

*Vhost:
On Anonymous' IRC servers you can ask for a Vhost. Example (by default you will have a host based from you Internet service provider, something like this: `<mynick@theservicefrom.125.comcast.suck.net>` or a hash if you've logged by SSL (recommended) : `<mynick@6969E1A1T1COCK152.69.IP>` After setting a desired vhost you could be identified as: `<mynick@myvhostRocks.org>` . Before you can enable your Vhost you first have to register a nickname so you can be identified when logging in on IRC. It's recommend that you take a look at the above link under (HOW TO IRC): `http://anonnews.org/help/en.html`

Requesting a vhost:

Now that you are logged in and have registered your nickname you can activate your Vhost.

Go to the channel #Vhost (`/join #vhost`), after joining the channel.

You can use the command `!vhost` which is used to activate your vhost.
You should use it like this:

```
!vhost [optional@]new.host.here
```

`!vhost` is the command, followed by the host name you want to use just as stated above.
Be aware to use at least 2 dots to separate 3 words. The first parameter optional@ speaks for itself its optional but I suggest you use it!

So a vhost command could look like this:
!vhost `middlefinger@the.corrupt.feds`
If everything is fine you should be kicked out of the channel, this is to prevent spam and other malicious use of the vhost.

Now if you try to look at your host you will still see your original host but this can only be seen by you, so don't panic. If you really want to know if it worked you could ask some one to whois you and get there feedback on what host you use!

Now that you have set your Vhost it will be activated as soon as you login to IRC on your registered nickname.
If you want to change your vhost, you will have to wait 3600 sec.
Also be aware that the vhost only account for the IRC network from anonops
Eventually you can directly ask for the vhost via command without getting in the
specific channel.

*Command:
/hs request vhost@hosthere

Explanation: this will avoid getting into the specific channel. But is not enough to get it
working. The vhost@ part is optional, the important part is the hosthere part.

Considering the previous explanation, use the following:
/hs request hosthere

*Command 2:
/hs on

Explanation: This will effectively activate the vhost.

Vhost Troubleshooting

Q: I have registered my vhost, but once I log in it doesnt activate.
A: Have you identified with your nick? You will only get your regular vhost back once your nick is correctly identified, redo step 2.

Q: I just changed my vhost but it wont apply, why?
A: You need to update your status, in order to make it fully working. Use this:
/msg nickserv update

*Output: HostServ- Your vhost of hosthere is now activated.
*Output: NickServ- Status updated (memos, vhost, chmodes, flags
Once you do that, you normally should have a fully functional vhost.

Basic list of IRC Commands

`/join #channelname`	Joins #channel
`/part`	Parts active #channel
`/query nick`	Opens private conversation with nick
`/msg nick <message>`	Sends <message> to nick
`/whois nick`	Displays info on nick
`/msg nickserv identify <password>`	Identifies your nick
`/ignore <nick>`	Ignore a troll
`/topic`	See the topic of a channel
`/list`	See a listing of available channels

Extended commands:

* http://www.ircbeginner.com/ircinfo/m-commands.html

Where to find current IRC information incase you can't connect:

* http://www.anonnews.org
* http://www.anonops.ru/?id=servers
* Facebook (search Anonymous, Operation Tunisia) http://www.anonnews.org/chat
* (Loads web based IRC client with current server info)

Security:

* Use SSL to connect to the IRC. Server port is 6697.
* Use VPN software, or accounts to hide your IP. IRC servers are pretty secured, but not invulnerable. Tor software is NOT an option (It's banned in the network due to malicious abuse).

IRC-Clients

Mac:

Download Colloquy from one of these:

* http://colloquy.info/downloads/colloquy-latest.zip
* http://files5.majorgeeks.com/files/aaea265a9054b3b8c5df99c64685ec2e/mac/messaging/colloquy-latest.zip

Get a webproxy, one of these. Make sure you connect with SSL. ("ipadress:port")

* 62.112.33.2:80
* 200.125.243.122:8080
* 120.39.24.156:808
* 58.22.151.6:80
* http://www.proxy-list.org/en/index.php?
* pp=any&pt=2&pc=any&ps=y&submit=Filter+Proxy

Usage

* Start Colloquy
* Click on New
* Enter a Nickname (not your real name)
* Enter a Chat Server, for our purpose, irc.anonops.ru.
* Click on Details
* Select the Secure Web proxy and check the SSL option, use port 6697
* Don't put your real name in either User/Real Name. Invent something.
* If you want, click: Remember Connection
* Hit Connect
* Click Join Room and enter the Chat Room #tunisia, for example.
* Or, one of these: #opTunisia #Lobby View Macintosh instructions below.

Linux:

Xchat (Gnome)

* Debian/Ubuntu/Knoppix... :

```
sudo apt-get install xchat
```

* Redhat/Fedora(64bit only):
http://www.xchat.org/files/binary/rpm

* Gentoo:
```
sudo emerge --sync | sudo emerge  -av xchat
```

Usage

Start X-Chat

Click Add button on the network list, and rename to whatever you choose.
Click the Edit button with new network selected, change the server entry from newserver/6667, to irc.anonops.ru/6697 (or use one of the newer domains found from links below).
Then select the two check boxes that say Use SSL for all servers on this network and Accept invalid SSL certificate.
Click Close, then Connect.

Konversation (KDE) http://konversation.kde.org
* Debian/Ubuntu/Knoppix... :
`sudo apt-get install konversation` // Usage : similar to X-Chat

Windows:

X-Chat2

* Freeware version: http://www.silverex.org/download
* Mirror: http://download.cnet.com/X-Chat-2/3000-2150_4-10972145.html

XChat

* http://xchat.org/download

mIRC

* http://www.mirc.com/get.html

Usage

* Download SSL Library: http://www.mirc.com/download/openssl-0.9.8q-setup.exe

* Install it either in the mIRC folder (typically C:\Program Files\mIRC or C:\Program Files(x86)\mIRC) or in the Windows System folder (typically C:\Windows\System32).
  By running mIRC it should find and use the OpenSSL library automatically. To confirm whether mIRC has loaded the OpenSSL library, you open the Options dialog and look in the Connect/Options section to see if the SSL button is enabled.
* Type `/server irc.anonops.ru:6697`

  Webbased
* http://01.chat.mibbit.com
* In the mibbit page, click server, and enter in the box: `webirc.anonops.ru:+6697`
  Click Channels.

Q - How do I know if it is working?

A - Just do /whois your_nick and it should inform you that you are using a secure connection.

`http://www.anonops.ru`

General Browsing Safety

Basic Rule: Always browse in "Private Mode" so that fewer traces of your web history remain on your HDD. Opera, Chrome, Firefox, Safari, and Internet Explorer all include a form of Private Browsing.

- Using a free VPN will ensure your privacy in most situations online.
- If possible, use USB drives. You can nuke them if needed and if leaves no traces on your hard drive
- Recycle your online accounts as needed. A virtual name is just that, something people use to refer to you in given situations.
- When creating accounts, use VPN or TOR bundle that will give a bogus origin as well.

*Tip: Use a different VPN for each of your online personas. When checking real email accounts, fb, use a different VPN than from the one you use for Anonymous activities.

Useful (mandatory) plugins/extensions for Firefox:

* BetterPrivacy (Removes persistent cookies from flash stuff >> *.sol)
* NoScript (blocks Javascript)
* AdBlock Plus (blocks Ads) (Subscribe to Easylist and Fanboy's List)
* Element Hider for Adblock Plus
* Ghostery (tracking pixels)
* TACO (More adblocking)
* Redirect Controller
* Refcontrol
* WorldIP (know your country, know your rights)
* Flagfox
* GoogleSharing (GoogleProxy, anonymizes the search) - Scroogle.org is also a very viable (and worthwhile) alternative
* User Agent Switcher: Sends bogus browser identity to servers.
* Optimize Google: Allows to block loads of scum google uses to track searches.
* Outernet explorer (MacOS): Searches for a whole pile of shit on the net every 10 seconds or so, ensures anyone tapping packets will have a hell of a time.
* Https everywhere: automatically loads https on a site if available. <https://www.eff.org/https-everywhere>
* Scroogle SSL search (Google anonymously) url: https://ssl.scroogle.org

Download TOR:

https://www.torproject.org/

- Download Torbutton for Firefox (enable or disable the browser's use of Tor)

  https://www.torproject.org/torbutton

- Make sure your cached data is securely destroyed before re-starting firefox by the following 'debug' procedure - you'll need to go to Start > Run and then open 'cmd' for Command Prompt:

System Safety

Basic rule: Security is a continuing process, not a state. Do audits on a regular and scheduled basis. And do encrypted backups. Backups are important, as there are two types of people, those who have backups and those who have lost their data.

Use the operating system you are familiar with (Linux and Unix are better though)

* Uninstall everything you not need.
* Disable all remote tools.
* Shred or encrypt /temp, /var/temp and all world-readable files.
* Use Linux for activism purposes. Inside Linux use virtual machines. Use truecrypt + removable devices + hidden volumes if you plan on reusing a virtual machine more than once. - This is just for those who have knowledge of Linux.

∗Encrypt your hard disk (Truecrypt : `http://www.truecrypt.org .`

∗Debian and other distros offer to encrypt the hard drive during installation. Use it.

∗Use a distro that boots from DVD/CD/USB.

∗Never ever keep logs.

∗Shutdown all unneeded services.

∗Use a firewall, (and tail the output do you can see what happens every moment.) NOT FOR NEWBIES - Basic info could be read out of /var/log/auth.log for example but keep in mind that already compromised systems will likely have modified/wiped that.

∗If you detect any unwanted activity INSIDE your computer, shut down the Internet, and reinstall everything.

∗If you think your router might have been hacked, contact your ISP at once, reset it, and/or reinstall its firmware or buy a new one.

∗Public access points are perfect - just about. (Correlating logins with CCTV could prove disastrous so security cameras should be avoided while using such 'free' services. Cybercafés, McDonald's, and many companies offer free internet access, remember though, not to surf those nets without a vpn and/or Tor.

∗Keep private keys (pgp gnupgp) in a removable device, and that removable device away from curious eyes. Encrypt the private key before doing this.

∗Keep vpn certs away from curious eyes via removable device, or common hidden folders.

∗Never use the same users/passwords on reinstall. Take the time to create a new one each time.

∗Use random password generators.

∗BE paranoid. All rare activity in your computer must be checked and monitored. That will provide 2 things: knowledge once you identify it, and added safety.

Detecting security issues on *Nix:

But be careful, if you don't know how to read Lynis' output, you'll become paranoid.

* http://www.rootkit.nl/projects/lynis.html

Scanner for rootkits, backdoors and local exploits on *Nix:

Again, if you don't know how to read Rootkit Hunters output, you'll get paranoid.

* http://www.rootkit.nl/projects/rootkit_hunter.html

Destroy data securely in Unix/Linux:

To securely destroy data under Linux you have some possibilities. The command shred -u overwrites single files and deletes them finally; with wipe you overwrite and delete directories. Be careful because shredded/wiped data cannot be recovered.

Open a Terminal and type:

```
shred -u <filename>
wipe -rcf <directory>
```
(read the manual first: man wipe)

If you feel the need to wipe the whole hard drive, the command is as follows for IDE-HDs (/dev/hda is the first HD):

```
wipe -kq /dev/hda
```

For SATA and SCSI HDs you type (/dev/sda ist the first HD):

```
wipe -kq /dev/sda
```

If wipe is not available to you, you can use dd. Use *both* commands, one after the other, if you're paranoid use them multiple times (again the first HD):

```
dd if=/dev/zero of=/dev/hda
dd if=/dev/urandom of=/dev/hda
```

Destroy data securely on Mac:

Anonymous' Privacy Pack for Mac users. It includes a Top Secret (like HBGary's ones) Docs secure Shredder & AES-256 Encryption tool (and some Design as extra stuff) download links:

http://www.megaupload.com/?d=L2VQBEFE

or

http://www.mediafire.com/?1xmu0m8jpy9b2a1

MD5 (Anonymous-MacPackage-Privacy.dmg) = 36e9ea524a86b94a451577ca46d3e15f

Destroy data securely in Windows:

AxCrypt http://www.axantum.com/AxCrypt

i2P - Anonymizing Network

What is I2P?
I2P is an anonymizing network, offering a simple layer that identity-sensitive applications can use to securely communicate. All data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties.

Many applications are available that interface with I2P, including mail, p2p, IRC chat, instant messaging and others.

Enjoy your anonymity and privacy!

There's a version for Windows (also portable), Linux, MacOS.

I2P Tutorial for Windows Video:
https://www.youtube.com/watch?v=5J3nh1DoRMw

I2P Tutorial for Linux - Video:
https://www.youtube.com/watch?v=QeRN2G9VW5E

How to set up your own website on I2P - Video:
https://www.youtube.com/watch?v=2ylW85vc7SA

http://geti2p.net
http://i2p2.de

IRC on i2p:

127.0.0.1:6668
Channels: #operationpayback, #opegypt , #opIran, #opTunisia, #opHBGary, #opitaly
Sites: (currently down) anonops.i2p qr.i2p

For more and active I2P sites visit: http://inr.i2p
The ports I2P is using: http://www.i2p2.de/faq#ports
See also your router's configuration.

I2P installation and running on Linux

I2P on Linux: just download and extract the installation files, no need for separate install (such as apt-get install). Run the router from /i2p folder with 'sudo sh i2prouter start'. In seconds, I2P should open a Konqueror-browser page of I2P-main console. Configure your bandwidth settings. You might also consider opening some ports on your firewall for optimizing the use of your bandwidth.

Portable I2P (windows only)

Windows users can use a portable package; it contains I2P, several plugins (email, torrent client), preconfigured browser, preconfigured IRC client and messenger. Download located at:

http://portable-i2p.blogspot.com

! Before you can use anything on I2P, you have to start the I2P router from the portable apps tray icon-menu with the button "I2P Launcher".

Anonymous surfing with I2P

To enable I2P to anonymize you in your browser, go to your browser options/preferences (depending on your browser) -> network/connection settings -> select manual proxy configuration and in http insert 127.0.0.1 and 4444 for port, in https 127.0.0.1 and 4445 for port. Make sure that you have 'No proxy for' as 'localhost, 127.0.0.1' so you'll be able to reach your I2P configuration page. To test your anonymity, go as example to: cmyip.com

TroubleShooting.

FAQ (in no particular order)

Q: Can you help us?
A: See http://www.anonops.ru/?id=contact or join irc.anonops.ru, join a channel and contact an operator. Or contact Anonymous on Twitter, Facebook.

Q: Do you guys have a website?
A: http://www.anonops.ru

Q: How do I know what's hot?
A: Lurk in the IRC channels or go to http://www.anonnews.org

Q: Is the news on Anonnews official?
A: Well, in some way, it is official, on the other hand, it is "official“ and on the third hand, the more people support an operation, the more official it becomes.

Q: Why not attack that newspaper/TV/Radiostation?
A: Anonynmous does not attack media.

Q: That is no media! It only spreads lies and propaganda!
A: Freedom of speech counts for assholes too.

Q: What is a netsplit?
A: A netsplit is Internet-Darwin doing evolution.

Q: But, but...
A: As Evelyn Beatrice Hall said, "I disapprove of what you say, but I will defend to the death your right to say it.“ Freedom of speech. Got it?

Q: What are DDoS and defacements good for anyway? It doesn't help the people.
A: DDoS is all about steering media's attention towards the problems of the people. If media takes notice, this will help the people. The fine art of defacing a website is about sending a message to the people and the owner of that website. Besides that Anonymous provides the people with information and guides and software to circumvent censorship, also know as The Care Package“

Q: What's in the Care Package?
A: Software like Tor Onion Router, a Circumventing Censorship Manual, more software, other guides and useful stuff.

Q: Can you give me a How-To about building botnets?
A: Such how-to does not exist.

Q: I have seen some strange download links in the channel, can I trust them?
A: Anonymous recommend to not trust links spread in the chans. The only trustworthy links are those spread by Admins, Operators and those in topic.

Q: Some guy asked me in the IRC where I live and what my name is.
A: Do NOT provide personal information in IRC. Instead contact an operator and tell him what happened. Same goes for other suspicious behavior.

Q: How can I join your club?
A: Anonymous is not a club.

Q: But how does that Anonymous' thing function anyways?
A: Best way to find out is, to join a channel, lurk around and get an impression of it. Anyone who thinks that the freedom of speech is a remunerative goal can fly under the flag of Anonymous.

Q: I am not a hacker, how can I help you?
A: If you:

can collect/spread information
can organize things
can make contacts
can provide insights
can share experiences
can push the IMMA FIRING MA LAZOR button
can write guides
can do artwork
can speak a foreign language and/can translate
... you can be helpful.

Q: Is there a Hive??????????????????
A: 1. Look at the topic by typing /topic
2. Probably not, but you don't need a hive, you can fire manually, as you wish.

Q: What's the target???????????????????????
A: Look at the topic by typing /topic

Q: What's the target???????????????????????
A: N00b, look at the topic by typing <tt>/topic</tt>

Q: Is the target down???????????
A: Got to www.watchmouse.com and ask there.

Q: Is there a LOIC for Linux/Unix/Mac?????????????
A: Yes, it is called loiq. See http://sourceforge.net/projects/loiq

* Nixfags may use PyLoris http://sourceforge.net/projects/pyloris and Hping3 as well.

Q: Some guy keeps saying, there were Danish girls in #channel.
A: This is obviously a lie; there are not girls on the Internet.

Q: I am a Media-Guy, how can I contact you?
A: See http://www.anonops.ru/?id=contact or send an email to press@anonops.ru

Q: I am a Media-Women, how can I contact you?
A: Please see http://www.anonops.ru/?id=contact or send an email and personal pics to press@anonops.ru

Some useful Links

Throw-away-emails

Use them for registering activism related email-/Facebook-/... accounts.

* http://10minutemail.com
* http://www.sofort-mail.de
* http://www.trash-mail.com
* http://www.guerrillamail.com
* http://www.spam.la

Portable Software

Portable software is software, that you can run from an USB drive, so that it leaves nearly no traces on your computer.

* http://portableapps.com
* http://portableapps.com/apps/internet/firefox_portable
* http://portable-i2p.blogspot.com

Proxies

You may use them in conjunction with a VPN.

* http://www.freeproxies.org
* http://www.socks24.org
* http://www.samair.ru/proxy

VPN

* http://cyberghostvpn.com
* http://hotspotshield.com
* http://proxpn.com
* https://anonymityonline.org
* http://www.swissvpn.net
* http://perfect-privacy.com
* https://www.ipredator.se
* http://www.anonine.se
* https://www.vpntunnel.se

I2P

http://geti2p.net

Chat for more info about I2P
The channels #i2p, #i2p-chat and #irc2p are supported.

https://www.awxcnx.de/i2p-irc-en.htm

Tor Onion Router

http://www.torproject.org

Privacy Box

The PrivacyBox provides non-tracked (and also anonymous) contact forms. It is running primarily for journalists, bloggers and other publishers. But it is open for other people too. Think about an electronic mailbox.

https://privacybox.de/index.en.html

Sending anonymous email

https://www.awxcnx.de/mm-anon-email.htm

Send free faxes

* http://sendfreefax.net (Text only)
* http://www.freefax.com/ff_snd.html (Text only)
* http://www.eztel.com/freefax/ (Text only)
* http://www.popfax.com

Free and uncensored DNS-Servers

87.118.100.175 (Ports: 53, 110)
94.75.228.29 (Ports: 53, 110, HTTPS-DNS, DNSSEC)
62.75.219.7 (Ports: 53, 110, HTTPS-DNS, DNSSEC)
87.118.104.203 (Ports: 53, 110, DNSSEC)
62.141.58.13 (Ports: 53, 110, HTTPS-DNS, DNSSEC)
87.118.109.2 (Ports: 53, 110, DNSSEC)

To see wether you're using them properly, open your browser and type :

`http://welcome.gpf` into the the adressbar. If you're using them you should see a website saying :

« Congratulation You are using a censorship free DNS server! ».

Else, you failed.

If you're a hax0rz you can use a terminal. Open it and type

```
nslookup welcome.gpf
```

this should result in the following output:

```
Non-authoritative answer:
Name: welcome.gpf
Address: 62.75.217.76
```

Else, you failed. (Else is General Failure's sister. Avoid meeting them at all costs.)