irc.anonops.ru #anonsec

/dev/null before dishonour

Anonymous – the uber-secret handbook

compiled by Anonymii

Version 0.2.1
Date 09. April 2011

DRAFT VERSION,

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

Summary for the impatient

Anonymous - An Introductory Guide to Safety during Social Instability

---
Foreword [fwd1]

Political activists, dissidents, and even nonpartisan bystanders caught in social instability are often fearful for their protection and protection of their families. Citizens may face harsh and even violent opposition by authorities and security forces in such situations. This guide is designed to introduce the reader to the mentality needed to stay safe during unrest and protests - both online and offline. It furthermore aims to assist in continued communications during periods of internet and phone line restrictions.

Index [ind2]

To skip between sections of this article, use the search function on your computer [Windows: Ctrl-F / Macintosh: Command-F] and type in the four character code listed after the section in the index listing. For example, to jump to the foreword on Windows, you would press Ctrl-F and type "fwd1" [without the quotations].

*** Introduction [idn3] ***

The first section of this article will focus on personal safety. Personal safety can be spoken of in two different spheres: Physical Safety and Internet Safety. It is important to remember that these two spheres overlap: a lapse of internet safety could lead to physical identification. However, by keeping in mind a few important rules you can drastically reduce the chance of being singled out and identified.

The second section of this article will go into specifics regarding technology that can be used to communicate anonymously, maintain secrecy, and protest effectively.

*** Personal Safety [prs4] ***

Physical Safety [phy5]

The key to physical safety is to act normal so as not to draw undue attention to yourself and to not reveal identifying information to anyone. Important steps in achieving this can be separated into two lists: The Do List, and The Do Not List. These steps are especially important if you are an activist, as this puts you at more of a risk to start with.

The Do List:

+Blend in with crowds
+Disperse into streams of people
+Keep a low profile
+Keep up to date on the news, especially protest rallying points and security checkpoints or roadblocks
+Look for signs of plainclothes police in your presence
+Cover anything that could be used to identify you such as tattoos or scars
+If you come into contact with anonymous materials or protest guides, try to get them to protesters - they contain key safety information.

Additional Do's for Protesters:

+Establish secure means to communicate with other protesters
+Plan your protest point, escape plan, and regrouping point before attending a protest
+Make backup plans - not just one, but many
+Search for communications by Anonymous and Telecomix - read "Communications"
+Try to obtain Anonymous' Riot Guide for homemade gas mask instructions, advanced coordination strategies, etc.

The Do Not List:

+Do not trust anyone to be who they say they are
+Do not give any personal information that could be used to identify you to anyone
+Do not mention anything about relationships, family, or relatives
+Do not mention ties to activist groups
+Do not mention the group Anonymous to anyone you do not know
+Do not mention anything about your past - education, employment, etc.

Internet Safety [int6]

Any use of the internet could potentially be used to physically locate you. It is important not to reveal information on the internet. If you are doing anything controversial online - such as discussing protests or blogging - you must be sure to conceal your IP. Please refer to the section on "Internet Security."

The Do List

+Keep in mind that any interaction you have online may be seen by others
+Think about actions before you make them - do not say anything that you may regret, as it could be recorded
+Create unique and secure usernames and passwords - Use letters, numbers, and special characters
+Use a VPN if at all possible - see "Internet Security"
+Delete your history, cookies, and cache after each internet session
+Use Private Mode browsing whenever possible
+Try using clients like Firefox instead of Internet Explorer
+Use temporary or throw away e-mail accounts to create facebook accounts, etc. See [eml4]
+Use Firefox plugins for added security. See [ffx5]

The Do Not List

+Do not use any or all of your actual name in account and usernames
+Do not mention anything that could be personally identifying - see "Physical Safety" [phy5]
+Do not mention time zones
+Do not mention physical characteristics or abilities

+Do not mention relationships, family, or relatives
+Do not connect/disconnect from services such as Twitter and Facebook all at once - stagger your access so they can't be connected

---
*** Internet Security [isc7] ***

Each online device has an 'IP Address.' An IP can be used to help physically locate an individual. For this reason, it is important to hide your IP. There are many ways of doing this. You should use as many layers of security as possible at any given time to increase your protection. Prepare internet security methods ahead of time in case internet restrictions are enforced suddenly. The three primary methods that will be discussed in this article are VPNs, I2P, and proxies.

Virtual Private Networks [vpn8]

A Virtual Private Network, or VPN, is a method of securing information communicated over the internet. When choosing a VPN service, try to pick a service from a country that will not easily hand over your private information. For example, services from Iceland or Sweden would be much safer than a service from the USA. Also try to find a service that does not keep user logs or payment information [if using a paid service].

Guides to installing the OpenVPN client:
---
* Windows: http://www.vpntunnel.se/howto/installationguideVPNtunnelclient.pdf
* Linux (Debian flavoured): http://www.vpntunnel.se/howto/linux.pdf
* Mac: http://www.vpntunnel.se/howto/mac.txt

Free VPN Services [Not Recommended]:
---
* http://cyberghostvpn.com
* http://hotspotshield.com
* http://proxpn.com
* https://anonymityonline.org

Commercial VPN Services [Recommended]:
---
* http://www.swissvpn.net
* http://perfect-privacy.com
* https://www.ipredator.se
* http://www.anonine.se
* https://www.vpntunnel.se

Free VPN Downloads [Not Recommended]:
---
*Windows: HotspotShield - http://hotspotshield.com
UltraVPN - https://www.ultravpn.fr/download/ultravpn-install.exe
*Mac: Ultra VPN - https://www.ultravpn.fr/download/ultravpn.dmg
*Linux: UltraVPN - https://www.ultravpn.fr/forum/index.php?topic=204.0

I2P [i2p9]

I2P is an anonymizing network that supports many secure applications. We recommend using pchat to connect to anonops.ru and joining channels such as #anonops and #oplibya .

I2P Websites

---

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

I2P Tutorial for Windows Video

---

* https://www.youtube.com/watch?v=5J3nh1DoRMw

I2P Tutorial for Linux Video

---

* https://www.youtube.com/watch?v=QeRN2G9VW5E

Active I2P sites

---

* http://inr.i2p

I2P Port Usage

---

* http://www.i2p2.de/faq#ports

* See also your router's configuration.

I2P Installation and Running on Linux
---
* Download and extract the installation files, no need for separate install (such as apt-get install).
* Run the router from /i2p folder with <tt>sudo sh i2prouter start</tt>. In seconds, I2P should open a Konqueror-browser page of I2P-main console.
* Configure your bandwith settings. You might also consider opening some ports on your firewall for optimising the use of your bandwith.

Portable I2P (Windows Only)
---
* http://portable-i2p.blogspot.com
    -Contains I2P, several plugins, preconfigured browser, preconfigured IRC client and messenger.
    -Before you can use anything on I2P, you have to start the I2P router from the portableapps tray icon-menu with the button "I2P Launcher".

Anonymous surfing with I2P
---
* Go to your browser options or preferences (depending on your browser) -> "network/connection settings"
* Select "manual proxy configuration"
* In "http" insert 127.0.0.1 , for "port" insert 4444
* In "https" insert 127.0.0.1 , for "port" insert 4445

Make sure that you have No Proxy set for "localhost, 127.0.0.1" so you'll be able to reach your I2P configuration page. To test your anonymity, go eg. to: cmyip.com.

Proxies [prx0]

Proxies are intermediary connections that may help hide your IP. They do not encrypt data. They may also help in accessing restricted web sites. Use them with VPN services to increase VPN security. See the following sites and [tor2]:

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

Tor Onion Router [tor1]

Tor is a proxy network that helps hide your IP. It does NOT encrypt data. There have been some claims of specific countries [such as Iran] circumventing Tor protection.

Download Tor
---
* https://www.torproject.org

Download TorButton for Firefox (Enable / Disable the Tor on the Browser)
---
* https://www.torproject.org/torbutton

Tor is also included in the Anonymous care package [pkg6] .

*** Communications [cmm2] ***

Anonymous encourages citizens of protesting countries to ask for assistance. This is best done using IRC to connect to #anonops. Please remember that it is safest to use a VPN [vpn8] or I2P [i2p9]. The IRC can be joined through a link at anonops.ru .

In the event of an internet shutdown, you can be sure that Anonymous and Telecomix will be trying diligently to restore communications. There are a number of things you can do to help.

*Try connecting to the internet at various locations - sometimes only certain ISPs shutdown while others remain operational
*Try using dial-up connections if possible
*Find ham radio owners and scan for communications by groups such as Telecomix - they may be able to provide you with directions for alternative internet connection methods.
*Locate universities and businesses with fax machines - we often try to use these machines as one-way communication devices to provide updates, safety guides, and inspirational material.

*** Additional Information [add3] ***

Temporary / Throwaway Email Accounts [eml4]

E-mails can be set up quickly at the following sites:
---
* http://10minutemail.com
* http://www.sofort-mail.de
* http://www.trash-mail.com
* http://www.guerrillamail.com
* http://www.spam.la

An email provider with an emphasis on security can be found at: http://hushmail.com [not recommended, hands out data if Government demands it]

Useful Plugins / Extensions for Firefox [ffx5]

---

* BetterPrivacy - Removes persistent cookies from flash stuff
* NoScript - blocks Javascript
* Ghostery - Detects tracking pixels
* GoogleSharing - GoogleProxy for locations where Google is censored
* User Agent Switcher - Sends bogus browser identity to servers.
* Optimize Google - Removes information Google uses to track searches
* Outernet Explorer (MacOS) - Creates numerous searches to help prevent packet sniffing.
* https://www.eff.org/https-everywhere - Automatically loads https on a site if available.
* Scroogle SSL search (Google Anonymously): https://ssl.scroogle.org

---

Anonymous Care Package [pkg6]

Anonymous provides an often updated care package that contains useful guides and software. The best way to access it is to join an IRC channel and ask for it. The IRC may be accessed at anonops.ru and channels such as #anonops [/join #anonops] may be of assistance. Please keep in mind security protocols such as the use of a VPN [vpn8] or I2P [i2p9] when accessing the IRC.

End of summary

Foreword

The greatest threats to your safety are A) social engineering and your behaviour and B) revealing your IP address.

for A) see Social Threats

for B) 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. There are no old heros, there are only young heros and dead heros.

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
- don't discuss personal information, your address or where you're from
- don't mention your gender, tattoos, scars, piercings, bodymodifications,
- over-/underweight, physical or psychological (in)abillities (got the idea?)
- don't mention your profession or hobbies
- don't mention whether you're in a relationship
- don't mention your involvement with other activist groups
- musical taste/preferred literature/films is a good way, to know someone, don't mention any of these
- don't use special characters, that are existent only in your language as
- they would reveal where you are from
- don't give even bogus info. Lot's of no's, make a yes.
- Everything is completely seperate between your real life and online

- life(s), don't blend anything from your real life with anon, don't talk
- about Anon in real life except posting posters anonymously, etc
- don't mention congresses that you have been at
- don't mention your school, university etc.
- don't mention what time it is where you live, mentioning the time can reveal where you live
- Never connect at same time. Try to alternate.
- Do not 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.
- Don't discuss whether you personally are DDOSing or writing How-Tos or Nmap'ing the target, making graphics etc. or not, just discuss general strategy
- Do not post pictures hosted on Facebook. The filename contains your profile ID.
- Stagger your login & log out times on FaceBook, Twitter & IRC. They can be compared for user info.

Technical

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

A good beginning is to use a VPN and running Anonymous related Software from USB device or a Live CD. A proxy will do also, but is not as secure as a VPN.
Always use as much security layers as possible. Make sure to use them in the right way. If you don't know how to use them, learn it before you use them.
Most Anonymii use VPN to hide their traces, they use SSL encrypted connections and they use #vhost, when they are on irc.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, wich makes it harder for law enforcement agencies to get access. In adition, 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

Guide for installing OpenVPN client

(taken from the FAQ by vpntunnel.se)

- Windows: http://www.vpntunnel.se/howto/installationguideVPNtunnelclient.pdf
- Linux (Debian flavoured): http://www.vpntunnel.se/howto/linux.pdf
- Mac: http://www.vpntunnel.se/howto/mac.txt

Free VPN -- Not recommended. (see explanation)
If they aren't selling you a service. They are selling you.

- http://cyberghostvpn.com
- http://hotspotshield.com
- http://proxpn.com
- https://anonymityonline.org

Commercial VPN providers

- http://www.swissvpn.net
- http://perfect-privacy.com
- https://www.ipredator.se
- http://www.anonine.se
- https://www.vpntunnel.se

Free VPN direct downloads -- Not recommended. (see explanation)
If they aren't selling you a service. They are selling you.

Mac

- Ultra VPN: https://www.ultravpn.fr/download/ultravpn.dmg

Linux

- UltraVPN: https://www.ultravpn.fr/forum/index.php?topic=204.0

Windows

- HotspotShield: http://hotspotshield.com
- UltraVPN: https://www.ultravpn.fr/download/ultravpn-install.exeSoftware

Explanation

1.- Free VPN: It is not recommended, cause many features are capped, and in addition, many free VPN providers will hand user data upon warrant issue. Also, many free VPNs work with ad companies.

2.- Commercial pptp: It's been said, as telecomix pointed out, that some operating systems (Windows 7, Vista) might be vulnerable to an attack consisting in requesting p2p conns, wich could lead the malicious attacker to get the user real ip.
See https://www.ipredator.se/?lang=en For more information on this matter. Seems flaw has to do with ipv6 conns, so just ensure you use ipv4.

3.- Recommended VPN's. All that use the OpenVPN service. And that include specific policies on user data storage and policies regarding that data. (Best option, no data loggin + no user billing loggin, + safe payment methods ie: Ukash and similar services).

I2P - Anonymizing Network

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. All anonymous.

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 automaticaly connects to the I2P IRC server anonymously.
Join `#anonops` for to keep track of Anonymous activity. Many Operation channels are relayed between I2P and anonops.ru.
Enjoy your anonymity and privacy!

Websites

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

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

IRC with I2P

- 127.0.0.1:6668
- Channels: #anonops , #opegypt , #opitaly, #opmesh
- Sites: (currently all down) anonops.i2p qr.i2p
- Telecomix IRC allows i2p tunnel

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

- 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 bandwith settings. You might also consider opening some ports on your firewall for optimising the use of your bandwith.

Portable I2P (windows only)

contains I2P, several plugins (email, torrentclient), preconfigured browser, preconfigured IRC client and messenger.

- http://portable-i2p.blogspot.com

Before you can use anything on I2P, you have to start the I2P router from the portableapps tray icon-menu with the button *I2P Launcher*.

Anonymous surfing with I2P

- Go to your browser *options/preferences* (depending on your browser) -> *network/connection settings*
- Select *manual proxy configuration*
- In *http* insert `127.0.0.1`, for *port* insert `4444`
- In *https* insert `127.0.0.1`, for *port* insert `4445`

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 eg. to: cmyip.com.

Tor Onion Router

Basic Rule: Tor does not encrypt the data you send. It just hides your IP by means of cascaded Proxies. Just installing Tor does not mean you're safe. For example, if you use Tor and log in to your real-life-email-account, you're doomed.

Download Tor

- https://www.torproject.org

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

- https://www.torproject.org/torbutton

Anonymous provides a so called Care Package. It contains Tor as well as a bunch of other usefull things. If you cannot access the Torproject website, you may ask in the IRC channels for the Care Package.

How to IRC

Basic Rule: Use SSL Port (in this case 6697). Always. Use #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.

What is IRC? IRC is a free chat program that people around the world can use to communicate. It features multiple rooms for different chat topics, and private messaging between users.

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 function. 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 certificate.
After connection you register you nickname by using a fake email adress, then you `/join #vhost` and AFTER that procedure you join the channels.

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>`	Identifys your nick
• `/ignore <nick>`	to ignore a troll
• `/topic`	to see the topic of a channel
• `/list`	to 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).

Extra security consists in getting a vhost (Virtual Host)

- Register your nick:
  `/msg nickserv register password fake@email.com`
- `/join #vhost`
- when in #vhost type: `!vhost any.fake.host`

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 #LobbyView` 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* http://konversation.kde.org

Konversation (KDE)

- 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 on *server*, and enter in the box: `webirc.anonops.ru:+6697`
- How do I know if it is working? Just do `/whois your_nick` and it should inform you that you are using a secure connection.

http://www.anonops.ru

- click *Chans*

How to Vhost

On the anon IRC servers you can ask for a Vhost. This will ensure that you are anonymous on the irc network. By default you will have a host based from you ISP, something like this: *mynick@theservicefrom.125.comcast.suck.net* or a hash if you've logged in by SSL: *mynick@6969E1A1T1COCK152.69.IP.*
After setting a desired vhost you could be identified as: *mynick@myvhostRocks.org*.

1.- You must own a registered nick to get a vhost.

- Command `/msg nickserv register password fake@email.com`
  Explanation: This will tell the register service to reserve your nickname for later use

2.- You must identify on that nickname to get it working.

- Command: `/msg nickserv identify password`.
  Explanation: Once you do this step you are ready to set up a vhost.
- Output: *services.anonops.net sets mode +r Yournick*
  Explanation: The +r flag states a given nick is effectively registered and identified.

3.- Join the #vhost channel in order to get the vhost working.

- Command (in channel): `!vhost fake.host.here`
  Explanation: After you apply for a vhost, the service will ban your nick from that channel for a given ammount of time. Reasons are many. Lurkers can get real ip's from people. Switching vhosts each 2 seconds might lag the server, and so on.

3.b.- 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 Trouble Shooting

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.

Analyzing your Interwebz

Glasnost: Bringing Transparency to the Internet
„ISPs are increasingly deploying a variety of middleboxes (e.g., firewalls, traffic shapers, censors, and redirectors) to monitor and to manipulate the performance of user applications.“

- http://broadband.mpi-sws.org/transparency

GTNOISE Network Access Neutrality Project
„NANO identifies performance degradations that result from network neutrality violation by an Internet service provider (ISP), such as, differential treatment of specific classes of applications, users, or destinations by the ISP.“

- http://www.gtnoise.net/nano

The ICSI Netalyzer
„What's up with my network? Some services seem broken? Things are very slow? Is there something wrong?“

- http://netalyzr.icsi.berkeley.edu

What your browser reveals

„BrowserSpy.dk is the place where you can see just how much information your browser reveals about you and your system.“

- http://browserspy.dk

How unique and trackable is your browser?

„Panopticlick tests your browser to see how unique it is based on the information it will share with sites it visits“

- http://panopticlick.eff.org

Is this website censored?

„Have you ever come across a web site that you could not access and wondered, "Am I the only one?" Herdict Web aggregates reports of inaccessible sites“

- http://www.herdict.org/web

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 harddrive

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

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 and make use of the Throw-away-emails.

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, i use it because Google is censored where i live, 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 searchs.
- 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://www.eff.org/https-everywhere: automatically loads https on a site if avaliable.
- Scroogle SSL search (Google anonymously): https://ssl.scroogle.org

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
- Encrypt your hard disk (Truecrypt : www.truecrypt.org)
- Debian and other linux distros offer to encrypt the harddrive during installation. Use it.
- Use a distro that boots from DVD/CD/USB
- Never ever keep logs
- Shutdown all unneeded services
- Use a firewall
- 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. Cyber cafés, Mc Donalds, 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 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 potentially security flaws on *Nix

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

- 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

Destroying data securely

Unix/Linux
To securely destroy data under *Nix you have some possibillities. The command `shred -u` overwrites singe files and deletes them finally, with `wipe -rcf` you overwrite and delete directories. Be carefull because the shredded/wiped data cannot be recovered.

Open a Terminal and type

- `shred -u` <filename>
- `wipe -rcf` <directory>

If you feel the need to wipe the whole harddrive, 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`. (again the first HD)

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

Use *both* commands, one after the other, if especially paranoid. Use them multiple times.

Mac

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

- http://www.megaupload.com/?d=L2VQBEFE
  or
- http://www.mediafire.com/?1xmu0m8jpy9b2a1

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

Windows

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

On non-violent protests (compiled from: http://www.aeinstein.org/organizations103a.html)

Formal Statements
Public Speeches
Letters of opposition or support
Declarations by organizations and institutions
Signed public statements
Declarations of indictment and intention
Group or mass petitions

Communications with a Wider Audience
Slogans, caricatures, and symbols
Banners, posters, and displayed communications
Leaflets, pamphlets, and books
Newspapers and journals
Records, radio, and television
Skywriting and earthwriting

Pressures on Individuals
"Haunting" officials
Taunting officials
Fraternization
Vigils

Symbolic Public Acts
Displays of flags and symbolic colors
Wearing of symbols
Prayer and worship
Delivering symbolic objects
Protest disrobings
Destruction of own property
Symbolic lights
Displays of portraits
Paint as protest
New signs and names
Symbolic sounds
Symbolic reclamations
Rude gestures

Group Representations
Deputations
Mock awards
Group lobbying
Picketing
Mock elections

Drama and Music
Humorous skits and pranks
Performances of plays and music
Singing

Processions
Marches
Parades
Religious processions
Pilgrimages
Motorcades

Withdrawal and Renunciation
Walk-outs
Silence
Renouncing honors
Turning one's back

Honoring the Dead
Political mourning
Mock funerals
Demonstrative funerals
Homage at burial places

Public Assemblies
Assemblies of protest or support
Protest meetings
Camouflaged meetings of protest
Teach-ins

The methods of social noncooperation

Ostracism of Persons
Social boycott
Selective social boycott
Lysistratic nonaction
Excommunication
Interdict

Noncooperation with Social Events, Customs, and Institutions
Suspension of social and sports activities
Boycott of social affairs
Student strike
Social disobedience
Withdrawal from social institutions

Withdrawal from the Social System
Stay-at-home
Total personal noncooperation
"Flight" of workers
Sanctuary
Collective disappearance
Protest emigration (hijrat)

The methods of economic noncooperation: (1) Economic boycotts

Actions by Consumers
Consumers' boycott
Nonconsumption of boycotted goods
Policy of austerity
Rent withholding
Refusal to rent
National consumers' boycott
International consumers' boycott

Action by Workers and Producers
Workmen's boycott
Producers' boycott

Action by Middlemen
Suppliers' and handlers' boycott

Action by Owners and Management
Traders' boycott
Refusal to let or sell property
Lockout
Refusal of industrial assistance
Merchants' "general strike"

Action by Holders of Financial Resources
Withdrawal of bank deposits
Refusal to pay fees, dues, and assessments
Refusal to pay debts or interest
Severance of funds and credit
Revenue refusal
Refusal of a government's money

Action by Governments
Domestic embargo
Blacklisting of traders
International sellers' embargo
International buyers' embargo
International trade embargo

The methods of economic noncooperation: (2) The strike

Symbolic Strikes
Protest strike
Quickie walkout (lightning strike)

Agricultural Strikes
Peasant strike
Farm Workers' strike

Strikes by Special Groups
Refusal of impressed labor
Prisoners' strike
Craft strike
Professional strike

Ordinary Industrial Strikes
Establishment strike
Industry strike
Sympathetic strike

Restricted Strikes
Detailed strike
Bumper strike
Slowdown strike
Working-to-rule strike
Reporting "sick" (sick-in)
Strike by resignation
Limited strike
Selective strike

Multi-Industry Strikes
Generalized strike
General strike

Combination of Strikes and Economic Closures
Hartal
Economic shutdown

The methods of political noncooperation

Rejection of Authority
Withholding or withdrawal of allegiance
Refusal of public support
Literature and speeches advocating resistance

Citizens' Noncooperation with Government
Boycott of legislative bodies
Boycott of elections
Boycott of govt employment and positions
Boycott of govt depts., agencies, and other bodies
Withdrawal from govt educational institutions
Boycott of government-supported organizations
Refusal of assistance to enforcement agents
Removal of own signs and placemarks
Refusal to accept appointed officials
Refusal to dissolve existing institutions

Domestic Governmental Action
Quasi-legal evasions and delays
Noncooperation by constituent governmental units

Citizens' Alternatives to Obedience
Reluctant and slow compliance
Nonobedience in absence of direct supervision
Popular nonobedience
Disguised disobedience
Refusal of an assemblage or meeting to disperse
Sitdown
Noncooperation with conscription and deportation
Hiding, escape, and false identities
Civil disobedience of "illegitimate" laws

Action by Government Personnel
Selective refusal of assistance by government aides
Blocking of lines of command and information
Stalling and obstruction
General administrative noncooperation
Judicial noncooperation
Deliberate inefficiency and selective noncooperation by enforcement agents
Mutiny

International Governmental Action
Changes in diplomatic and other representations
Delay and cancellation of diplomatic events
Withholding of diplomatic recognition
Severance of diplomatic relations
Withdrawal from international organizations
Refusal of membership in international bodies
Expulsion from international organizations

The methods of nonviolent intervention

Psychological Intervention
Self-exposure to the elements
The fast
- Fast of moral pressure
- Hunger strike
- Satyagrahic fast

Reverse trial
Nonviolent harassment

Political Intervention
Overloading of administrative systems
Disclosing identities of secret agents
Seeking imprisonment
Civil disobedience of "neutral" laws
Work-on without collaboration
Dual sovereignty and parallel government

Economic Intervention
Reverse strike
Stay-in strike
Nonviolent land seizure
Defiance of blockades
Politically motivated counterfeiting
Preclusive purchasing
Seizure of assets
Dumping
Selective patronage

Physical Intervention
Sit-in
Stand-in
Ride-in
Wade-in
Mill-in
Pray-in
Nonviolent raids
Nonviolent air raids
Nonviolent invasion

Alternative markets
Alternative transportation systems
Alternative economic institutions
Nonviolent obstruction
Nonviolent occupation
Nonviolent interjection

Social Intervention
Establishing new social patterns
Overloading of facilities
Stall-in
Speak-in
Guerrilla theater
Alternative social institutions
Alternative communication system

Guide to Safety in Street Confrontations

compiled from: http://www.dailykos.com/story/2011/2/3/941050/-Guide-to-Safety-and-Victory-in-Street-Confrontations-UPDATE

The tips below are provided by veterans of street battles within various contexts. Everyone who seeks to use them should try to bring as many of the described materials as possible in order to provide extras to others. But don't carry too much, as it will make it harder to move quickly when quick movements may be required. Remember: When you record and document, you allow the world to watch, and to act; bring more than one recording device and keep one concealed if possible, and in such a way that you may set it to record without it being known.

Remember, the carrying capacity of the group also counts. Distribute supplies as per your group strategy and do so as evenly as possible among protestors.

Protection & Safety

Head

Bicycle helmets provide good protection. Those designed for down-hill racing provide full-face cover and are the most secure. Construction helmets (hard hats) will also help protect the head, and are as widely available as bicycle helmets.

A towel or thick cloth wrapped around the head can provide some protection, but is not optimal. It can then be covered with a metal bowl or pot for more protection but it is important that you are still able to see.

Remember: The momentum shock to the head can still cause internal injuries, even if the outside of the head appears uninjured. Don't wear things which can easily be grabbed (such as dangly earrings or other jewelry).

Face

Masks make it difficult to identify individuals, and if everyone wears masks none will stand out. Hoods will cover most of your face and baseball caps protect you from most cameras mounted above. Some of the best masks are t-shirts. Put your head in a shirt, use the neck hole for the eyeholes and tie the sleeves around the back of your head

The best protection against chemical weapons is a gas mask. Any kind of mask should be tried on and sized before you're in the streets fumbling with unfamiliar straps. When paired with goggles, respirators make an excellent alternative to gas masks. It is necessary to do some homework beforehand and find goggles that are shatterproof, don't fog up, and that fit tightly on your face with the respirator. Respirators may be available at safety supply or welding supply vendors. Ask for filters for particulates and organic chemicals and tell the clerk what you're filtering to double check.

A bandanna soaked in water or vinegar and tied tightly around the nose and mouth is a last resort. It is far better than nothing, but remember that it is merely a barrier and not a filter and so won't do much for long-term protection. You can keep it soaking in a plastic bag until ready to use. Bring several, as multiple uses will render a bandanna as gassy as the air around you.
For protecting your eyes, swim goggles work well as they have a tight seal. Shatter resistance is very important (a rubber bullet to the eye can be disastrous). Most goggles have air holes to prevent fogging—fill these with epoxy. Covering these holes with duct tape can work in a pinch against an initial attack, though not for long term protection. Try them on with your respirator or bandanna to ensure that they are compatible and that both will provide a tight seal.
Don't wear contact lenses, which can trap irritating chemicals underneath.

Clothing

Wear thick clothes if you will be in range of rocks or other objects being thrown. Multiple layers may help protect against broken bones or other severe injuries. Wear heavy-duty gloves if you plan to handle hot tear gas canisters, fresh clothes in plastic bag (in case yours get contaminated by chemical weapons)

Shoes

These should be relatively sturdy, but still comfortable to run in, and non slippery, and, if possible, resistant to chemicals. Dont wear anything that may slip off, make sure laces are double knotted, etc.

Skin

Avoid use of petroleum jelly, mineral oil, oil-based sunscreen, lotions, moisturizers, or detergents on skin because they can trap chemicals and thereby prolong exposure. Wash your clothes, your hair and your skin beforehand in a detergent-free soap. We recommend using a water or alcohol- based sunscreen (rather than oilbased). If your choice is between oilbased or nothing, we advocate using the sunscreen. Getting pepper sprayed on top of a sunburn is not fun. We also recommend minimizing skin exposure by covering up as much as possible.

Arms

Something to protect forearms with as these are a natural guard to cover face/head. Chin guards or rolled up news papers are good alternatives. Foam plastic is a handy and light-to-carry protection against all kinds of blows. Chairs, and folding step ladders also work as personal protection.

Supplies

Keep blankets and water on hand to be used together in case of a person on fire. Use a wet blanket to put out the fire. Do not try to use water to put petroleum (gasoline) fires out. Even a simple first-aid kit can prove very helpful in unpredictable circumstances (see below).

Safety in numbers

Remain alert and aware of your safety and the safety of people around you.
Remember you must try to avoid violence to protect the legitimacy of your movement.

Food

Avoid heavy protein intake during active times. It is difficult to digest and will slow you down. Carbohydrates are recommended to keep your body in energy. Banana's are good. Sugar is a quick remedy in situations of energy lack, but it can cause your blood sugar level to drop rapidly later on. Take care of drinking enough. At downtime, when you will have a few hours to rest, try if you can to eat a healthy balanced meal, and get some rest.

List of objects needed to assist protesters

- Towels
- Water
- Fire extinguishers (do not take all fire extinguishers from an area, only extra's you can spare)
- Blankets, and fire blankets if possible
- Hard hats, bicycle helmets, and other head protection, sports protective gear, motorcycle and offroad equipment
- Pots and metal bowls which can act as protection for the head in combination with a towel or other padding
- Thick clothes
- First Aid kits, supplies, and bandages
- Ladders
- Step ladders or other items which can provide some use as shields
- Soap and disinfectants
- Safety Pins and Tape

Some Recommended Contents for a First Aid Kit

- Adhesive tape
- Alcohol
- Rubbing and wipes
- Aspirin
- Cotton swabs
- Disposable latex gloves
- Elastic bandages
- Face mask for CPR
- Flashlight
- Hot-water bottle
- Hydrogen Peroxide
- Safety pins
- Salt
- Scissors
- Sugar or glucose solution
- Thermometer
- Waterproof tape

The source of this document will have other documents for you soon. Also see the Guide to Protecting the North African Revolution series for additional expertise on defense, offense, tactics, and security; this may be found via Google.

Teargas

If expecting

- If you see it coming or get a warning, put on protective gear.
- If able, try to move away or get upwind.
- Stay calm. Panicking increases the irritation.
- Breathe slowly and remember it is only temporary.
- Blow your nose, rinse your mouth, cough and spit. Try not to swallow.
- If you wear contacts, try to remove the lenses or get someone to remove them for you, with clean, uncontaminated fingers.

If exposed to

For the eyes

We recommend a solution of half liquid antacid (like Maalox) and half water. A spray bottle is ideal but a bottle that has a squirt cap works as well. Always irrigate from the inside corner of the eye towards the outside, with head tilted back and slightly towards the side being rinsed. It seems from our trials that it needs to get into the eye to help. This means that if the sprayed person says it's okay you should try to open their eye for them. They most likely won't be able/willing to open it themselves, and opening will cause a temporary increase in pain, but the solution does help. It works great as a mouth rinse too.

For the skin
We recommend canola oil followed by alcohol. Carefully avoiding the eyes, vigorously wipe the skin that was exposed to the chemical with a rag or gauze sponge saturated with canola oil. Follow this immediately with a rubbing of alcohol. Remember that alcohol in the eyes hurts A LOT. Anyone whose eyes you get alcohol in will not be your friend.

Secondary treatments can include
spitting, blowing your nose, coughing up mucous (you don't want to swallow these chemicals!), walking around with your arms outstretched, removing contaminated clothing, and taking a cool shower. In fact, it is essential to shower and wash your clothes (this time in real detergents) as soon as you are able. This shit is toxic, and will continually contaminate you and everyone around you until you get rid of it. Until then, try not to touch your eyes or your face, or other people, furniture, carpets etc. to avoid further contamination. Remember, it is only temporary, and we are extremely strong.

Staying Safe & Sensible in an Action

A demonstration where police might attack requires a higher level of tactical awareness than your run-of-the-mill picket. Here are some generally applicable suggestions to help you stay safe and effective in the streets.

Always have a safe space in mind. All demonstrators need to be aware of a safe place to get to if a situation grows out of hand. You define "safe" and "unsafe" for yourself. For some, safe is among the locked arms of fellow activists, right on the front lines; but there's no shame in a lower threshold, for any number of reasons. Safe spaces change depending on movement and barriers by other demonstrators and the police, etc. In some cases they include wide open spaces or public areas. Other times they may take the form of an alleyway or similar hiding spot. There's no hard and fast rule about finding a safe space, but the time to have one in mind is before the shit hits the fan.

Always have an exit in mind. Assess how to leave a bad situation. Maybe it is best to be in a large group for protection. But if the police are herding you like cattle, then the large crowd is their focus and you may need to break up and leave in small groups. Getting away one moment might be your only chance to be active the next. Arrange with your buddies how to leave, and how to re-connect if you get separated.

Use the buddy system and move in a group. If at all possible, make sure to have a partner you can trust, to whom you will always stay close. That way, at least one person always knows your whereabouts and condition. Working in small groups of people, all of whom you know well and trust with your own safety, is another important factor. Even if you are not part of an organized group with a plan of action, it is helpful to at least be with folks you can rely on.

Be aware of crowd dynamics and dangers. You need to know what is going on - not just in view, but around the corners and a few blocks away. Pay attention to the mood of the crowd and the police. Certain actions like property destruction and violence will likely be caused by or result in violent behavior on the part of police. Be aware of police movement and different groups of protestors entering or leaving an area. Try to monitor the vibes and focuses of friends and foes at all times.

Know what is going on out of view by regularly sending out scouts to investigate what the police and other demonstrators are up to. Since the situation at a dynamic protest will change frequently and rapidly, scouts need to check around and report back often. It's a good idea to appoint a pair of group members as scouts.

Don't act on rumors. It's common at demonstrations for someone to approach a group of activists shouting, "The riot cops are coming!" As often as not, of course, there are no police coming at all. These people may simply be panicking, or they may be agents trying to confuse you. Acting on bad information is disruptive at best, and often dangerous. All critical information needs to be verified. If the person conveying info can't claim to have witnessed something directly, or if he or she is a stranger, then that information is unreliable.

Assume the riot cops may be coming. While acting on rumors and fear-mongering can be disruptive and dangerous, it shouldn't be surprising when the "authorities" do decide to blockade, surround, penetrate or break up a demonstration. This happens frequently, and the key to not being caught off guard is to stay prepared.

Don’t panic; help others stay calm. Sometimes at actions, the situation grows just plain frightening. But panic reduces critical judgment, adapting and coping abilities, and it can spread rapidly. Our best defense in a crisis is our collective cool - keeping each other centered & focused. If you can’t stay focused and centered, then you need to quit the demo to calm down. Similarly, if someone else can’t be calmed down, they need to leave.

Your best offense and defense is being part of a solid group. Groups combine various skills and powers. Savvy groups practice often, plan, and develop amazing strategies and tactics that are beyond the abilities of individuals. They have the numbers to do the various tasks: act, scout, medical, communicate with others, security, etc, yet they are small enough to act quickly.

Fighting Police Tactics

Often, the police strategy at a protest they want to end is to disperse the participants. They tend to operate in coordinated units, and use the following tactics

- Show of force to intimidate and scare people away.
- Surprise attacks by troops hidden in reserve.
- Surround and isolate entire crowds – sometimes not allowing people to leave or enter. They may also try to divide the crowd by moving into it at its weakest point. If you see the police about to attack your weak spot, try to reinforce it. When dispersing demonstrators, they may try to drive them like cattle towards certain areas and away from other areas. Your group can avoid the cattle drive dynamic by splitting off from the crowd. This can be effective if the police are operating as small units and not splitting up to deal with smaller groups outside the crowd.

- Police will often use snatch squads to perform surprise arrests of individuals they have chosen at random from the crowd, or whom they identify as "leaders" or "troublemakers". Snatch squads often are made up of, or collaborate with undercover agents, and can strike at any time. The best time to stop a snatch is as soon as the snatch has happened. You need a group of people to break the police's grip and some people to act as blocks. An important and low risk role in the de-arrest involves simply placing your body between the police and their target. Once you have your person back, all should link arms and disappear into the crowd. The police may try to snatch back or arrest one of the de-arresters. Surrounding police vehicles containing arrestees and preventing them from moving might lead to them being released. Cars don't move very well when they have flat tires, but keep in mind that when tires are punctured they can be loud.

Always be on the look-out for where your friends are, and be ready to act clearly and sensibly at a moment's notice.

Outmaneuvering The Police

Don't let yourself be intimidated onto the sidewalk. Police will push marches onto sidewalks in order to thin them out and divide them into smaller groups. Once the police force a march onto the sidewalk they can much more easily direct its movements and single out troublemakers.

Street crossings can be used to move into the roadway though groups may have to turn. In instances like this people walking bicycles can help form barriers, which will slow down police trying to push into the march.

Police move slow, so move quickly and in a large tight group. Occasionally running in a coordinated manner will help to keep the police always behind you. Countdowns will not only intimidate the police but they get you all charged up before running. Moving the wrong way down one-way streets my thin out the demonstration (as people have to make room for stopped cars) but it makes it very difficult for large groups of police to follow. Look outwards from the crowd. If someone is being administered first aid, face away from them.

Form cordons around anything the police want. (buildings, sound equipment, etc.)
Sitting down is good for dissuading police charging but only in large numbers. Sometimes sitting is not really worth it. Horses and camels are unpredictable. Particularly violent cops, especially those employing gases or rubber bullets, may be dangerous to sit in front of.

Throwing is a defensive act. It may not be wise to throw stuff at the best of times – that will only provoke them and make them want to hit you harder. If you want to throw, do it defensively, strategically, and en masse – a constant hail of debris will create a 'sterile area' where the police will not want to go.
Remember: don't throw to attack or cause injury. Throw from the front and then disappear into the crowd. Only jerks throw from the back.

Gas canisters can be thrown or kicked away from the crowd before they explode. Be careful! Don't pick up with your bare hands, as they can be very hot. They will explode.

Barricades can be more hassle than they are worth. Impassable blockades may be an inconvenience to you when you need to run. The best barricades are random material like newspaper boxes, dumpsters turned on the side, and road or construction material, strewn all over. One or two groups can lift small parked cars

and place them in the street with out damaging them.

The best defense is chaos. If situations change constantly the police cannot keep up. Keep moving. Change your appearance. Open new directions and possibilities. Be unpredictable.

Watch out for provocateurs including but not limited to "peace police". These self appointed enforcers of "peace" infiltrate demonstrations and try to prevent people from walking in the street or engaging in many forms of protest. They sometimes wear armbands (usually white) and will report people to the police or attempt to apprehend them personally. Also watch out for individuals trying to instigate violence against obvious non-targets. These people are often police or employed by them to discredit us.

Countering the Police

With any rowdy crowd, the police will be trying to break it up.They will try to intimidate and disperse crowds using baton line charges, horse charges, vehicles, gases, rubber/wooden bullets and a few violent arrests.

The dance steps will include one or more of these:

- Cops in lines will surround you.
- Either from the middle or one side, the cop lines will force everyone onto the sidewalk trying to create 'spectators' & 'actors' out of the crowd.
- Baton/horse/gas attack to lower morale.
- Loud speakers, and concussion grenades, to disorient and breakup the crowd.

- Line charges will slowly push the crowd down the street to where they want you (rush of cops à fall back à strengthen line à repeat).
- The police cannot arrest large groups of people unless they have lots of little plastic handcuffs.
- The police won't use tear gas unless they have their own gas masks on.

Stop the lines from forming! Surrounding you, preventing you from going where you want to go, and pushing you down the street to where they want you to go, all require the police to be in a tight line. It is important to prevent the first lines from forming. If the crowd seems volatile, they will hold back and form their lines a distance away. But if the crowd is hanging around looking confused and passive they will sneak in and form the lines amongst you.

- Don't stand and watch them. Always stay moving
- Don't look like you'll let them anywhere near you.
- Spot gaps in the crowd and fill them. stick together.
- Figure out where they want to go and get there first.
- Protect your escape routes by standing in front of them.
- Get those people who turned into 'spectators' back into the crowd and moving around.

Now they may just charge and start arresting. At least you are in a stronger position to deal and your escape routes are secured. Whatever happens next, don't stand there waiting for it. Keep moving and acting defensively.

If they have blocked your only exit try counter advancing

- this involves moving your lines into theirs thus gaining more space and opening up more exits.
- Use the front line as a solid wall, linking arms and moving slowly forward.
- Try a countdown for a faster advance.
- Use the banner as a plow (this prevents them from breaking your line). Dumpsters on wheels, saw horses and fencing also work.

If they have blocked your only exit try reforming

always look for ways to increase your number, by joining up with other groups and absorbing stragglers. Everyone has to get out and you'll stand a better chance of getting out unharmed, with all your belongings and equipment if you leave together at the same time.

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! It is government owned!
A: Freedom of speech counts for assholes too.
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.“

In the words of Noam Chomsky: „Either you believe in freedom of speech precisely for views you do not agree with, or you do not believe in freedom of speech at all.“

Freedom of speech. Got it?

Q: So, there are rules? WTF?!
A: Yes, do not attack media and do not promote violence. Easy, eh?

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 and spread the news, 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 usefull stuff.

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

Q: I have seen this downloadlink in the channel, can I trust it?
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 behaviour.

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

Q: What is Anonymous?
A: Anonymous is a very general movement. It is not a group with fixed members or rigid objectives. It is a fluid movement which anybody can become part of, simply by participating. To become part of 'Anonymous' all you have to do is join in with some of Anonymous' activities.

Q: But how does that Anonymousthingy 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 can I help you?
A: By

- collecting/spreading information
- organizing things
- making contacts
- providing insights
- sharing experiences
- pushing the *IMMA FIRING MA LAZOR* button
- writing guides
- translating
- ...

Q: Is there a Hive??????????????????
A: 1. N00b, 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: Where can I download LOIC??????????????
A: N00b, see topic in channel by typing `/topic`
Or go directly to https://github.com/NewEraCracker/LOIC/downloads

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

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

Q: Some guy keeps saying, there were danish girls in #channel.
A: This is obviously a lie, there are no girls on the internet.

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

Q: Why can't I join the Anonymous' IRC when on Tor?
A: Because of some vandalism *not looking at anyone*, Tor is not allowed on Anon's IRC chans anymore. You may use I2P instead, for help ask a bot named „muninn“. Muninn is the bot that the I2P-guys use to join Anonymous' IRC.

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 pics to *press@anonops.ru*.

Q: Ok, I am from the media and need to talk to Anonymous' spokesperson/leader/strategist then.
A: Anonymous has no leader, nor a spokesperson or strategist.

Some Links

Collaborative work

- http://piratepad.net
- http://www.typewith.me
- http://www.piratenpad.de

Polls

- http://pollcode.com

Pastebins

- http://pastebin.com
- http://pastebin.de
- https://www.pastee.org (lets you encrypt your stuff, have a fucked up SSL-certificate)
- http://tinypaste.com

Information about websites

- http://www.robtex.com
- http://news.netcraft.com

Throw-away-emails
Use them for registering activist 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 electronic mailbox.

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

Sending anonymous email

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

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.)

Other free and uncensored Nameservers

- 85.214.73.63 (anonymisierungsdienst.foebud.org)
- 204.152.184.76 (f.6to4-servers.net, ISC, USA)
- 2001:4f8:0:2::14 (f.6to4-servers.net, IPv6, ISC)
- 194.150.168.168 (dns.as250.net; anycast DNS!)
- 213.73.91.35 (dnscache.berlin.ccc.de)
- 80.237.196.2
- 194.95.202.198

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
  (.pdf-capable; 2 free faxes when signing up for free trial, no credit card/payment details needed)

On non-violent protests
http://www.aeinstein.org

Telecomix
(…) is a decentralized cluster of net activists who have joined forces to collaborate on issues concerning access to a free Internet without intrusive surveillance.
For short: If your Gov shuts down phonelines and or the Internets, Telecomix are there to help you, they provide new lines.

- http://www.telecomix.org
  - http://intercom.gs
    „To develop and support technologies that allow individuals to communicate during times of crisis or oppression.“
  - http://twitter.com/emcomstream
  - http://chat.telecomix.org **#emcom**