The Activist Guide to Secure Communication on the Internet

Posted by: The Militant
Posted on: September 3rd 2008
Updated on: September 8th 2008

Introduction

In several countries today, it is difficult for the common people to express their political beliefs or to voice injustices they often fall victim to. Many countries face this problems nowadays and activists are arrested daily and imprisoned for having voiced their opinion. That's why I was inspired to write a guide that activists worldwide can use to safely communicate with each other, and with the outside world, without having to worry that the the government may intercept communications and potentially use the intercepted information against them.

This guide was written for activists who believe in improving the common people's condition, who believe that countries should not be governed with the corporate interest in mind, who believe that corruption should be eradicated and made public, who need to release sensitive information to the media and to the world but have no means of doing so.

An e-mail address will be set-up and I will personally check that e-mail account on a regular basis to see if important information is contained and try to publish information that you specifically request to be published. If you submit other requests by e-mail, I will do my best to answer accordingly.

You are encouraged to contribute to the translations so that this guide can be made available to all who need it. If you have ideas on how to improve the guide, or if you believe that some of the information it contains is wrong, please let me know and I will investigate and make additions and/or corrections.

Section 1: Secure Internet Access

You may feel that you are anonymous on the Internet, but you are not.

Places where you access the Internet can be traced using your IP address. An IP address is just like a street address, but for the Internet. Every computer connected to the Internet needs to be assigned an IP address to access the Internet. Once you are assigned an IP address, you can connect to the Internet. The Internet is made up of millions of other computers that exchange information between them. So if you send a message to someone, the message will leave your computer, go through several other computers and finally arrive at its destination (the person you are sending the message to). If anyone has control over the other computers where the message is going through, they will see your message and the IP address attached to it. They will know where you are. They will also know who you are sending the message to.

```
[YOUR COMPUTER]
[ip address]
|
[The internet]
```

```
[many computers] -> People here can see you message
|
[ip address]
[Destination]
```

People who have control on these other computers can also see what you are accessing. They know if what you are accessing is prohibited content. If they need to, they can find you.

I will explain here some methods you can use to access the Internet anonymously. No method is 100% perfect. You have to be careful.

There are two rules you should follow when accessing the Internet anonymously:
1- Never log in to a personal email account and an email account used for activism from the same place. If you need to exchange prohibited information, log in to your activism email account and make sure you are browsing the Internet anonymously. If you need to access your personal email, disconnect to the Internet, access the Internet from somewhere else. Not anonymously. You will avoid official suspicions that way.
2- If using your own computer, clear your cache and cookies (temporary internet files) before accessing the Internet anonymously.
-In Firefox: Click on: Tools -> Clear Private Data -> Check all boxes and click Clear Private Data
-In Internet Explorer 6: Click Tools -> Internet Options -> General -> Delete Cookies and Delete Files

1.1 - Internet Cafes

Cybercafes or Internet Cafes are often good places to exchange information anonymously. If officials see that someone is exchanging prohibited information in an Internet Cafe, they will only see the Internet Cafe's IP address. The Internet Cafe's IP address is not tied to your name.

Important notes:

- If the information you are exchanging is highly sensitive, do not spend much time in the Internet cafe after you have exchanged the Information.
- Make sure the Internet Cafe does not have a camera
- If they have a camera, wear dark glasses, wear different clothes than you usually wear, wear a hat.
- Try to go to different Internet Cafes, not always the same one.
- Go to an Internet cafe where people do not know you personally.

1.2 - Using your portable computer

If you exchange prohibited information using your own portable computer, you should use a different computer for politically sensitive activities than for personal activities. You should never leave personal information about yourself or about others on the computer used for activism. You should not install programs that you don't need on that computer. You should not install messaging programs on that computer, unless you know what you are doing. You should use that computer only to exchange sensitive information, and always browse the Internet anonymously using that computer.

Most of today's portable computers can connect to the Internet wirelessly. That is very useful. If your computer has a wifi card (can connect to the internet wirelessly), you can find an open wireless access point. An open wireless access point means that you don't need to enter a password to connect to the access point. Many businesses offer wireless access points to their employees. You can try to connect to a business access point if it's not protected by a password. You can go to the city center, try to find several open wireless access points that you can use if you need to.

Important notes:

- Do not always send prohibited information through the *same* wireless access point.
- Avoid using a wireless access point near your home.

1.3 - Understanding Encryption

Encryption means that the data you are exchanging is made unreadable to anyone who is in the middle unless they have the "key" to decrypt the information (to make the information readable again).

When you connect to a banking site, you will often use an encrypted connection that prevents people in the middle to read the information you are exchanging. Only you and the bank can read the information because you have exchanged the keys that allow both of you to decrypt the information.

When you connect through an encrypted connection (such as a banking site), you are still revealing some information to the people in the middle. You are revealing your IP address, the destination of the information, and some other details. Only the content of the information is encrypted, and cannot be read by the people in between.

Important note: Given enough time and resources, any encrypted content can be decrypted by someone even if they don't have the key. The kind of encrypted connection with a banking site is not a very strong encryption. The government has very powerful computers which can be used to decrypt the information that has been exchanged. Some encryption methods are much more powerful and even the government won't be able to decrypt it.

There are many different types of encryption, that work at different levels. I will try to explain some of these methods here.

1.4 - Connecting to a website banned by the government

The method explained at section 1.5 requires you to download a program on your computer. That program is banned in some countries, like China. It may be difficult to obtain that program if you are in such a country. It is possible to use proxies to bypass the ban on certain websites.

Proxies are not safe and should not be used to exchange personal or sensitive information. They can be used if you are accessing the Internet anonymously to access websites that are banned by the government. You don't know who maintains the prsoxy and you should not trust the proxy. Only use it temporarily.

You can find proxy server addresses here (many of these sites may be banned in certain countries, try them to see):

- http://www.samair.ru/proxy/
- http://www.aliveproxy.com/us-proxy-list/
- http://www.freshproxy.org/
- http://www.proxyblind.org/free-proxy.shtml
- Find more by searching for "list of proxies" in Google.com

In Internet Explorer 6, you can enter the proxy information by doing this:

- Click on: Tools -> Internet Options -> Connections -> LAN Settings
- Check "Use a proxy server" -> Click "Advanced"
- Enter the Proxy server's IP address and the port in the appropriate fields
- Apply the settings

In Firefox 3, you can enter the proxy information by doing this:

- Click on: Tools -> Options -> Advanced -> Network -> Settings
- Select "Manual proxy configuration" and enter the Proxy Server address and port number.
- Apply the settings.

1.5 - Hiding and encrypting your Internet connection using TOR

There is a way you can hide the source of your Internet Connection to people in the middle, and also encrypt the data that you are exchanging. No method is 100% perfect, this one included.

TOR is a program you install on your computer. Many other people in the world also have TOR on their computer and they are connected to each other using TOR. When you request information or submit information when connected to TOR, the information is first encrypted, then sent through many computers connected to TOR across the world, and finally it reaches its destination.

The advantages of TOR are the following:

- People in between cannot find out what is the source or the destination of the information exchanged.
- People in between cannot read the information that is exchanged because it is encrypted.

Important notes:

- The computer where the information exits can potentially read the information you are sending or receiving.
- It may be illegal to use TOR where you are, try to avoid using it too often, it may alert suspicions. Try to use it when connected to an anonymous Internet connection.
- I suggest that you use Firefox when using TOR, Firefox is a very safe browser and TOR automatically installs a plug in to use TOR with Firefox. Get Firefox here: http://www.mozilla.com
- I suggest that you use the NoScript addon for Firefox when using TOR. If you allow scripts like Java or Flash, your identity can still be revealed when using TOR. Get the NoScript addon here: https://addons.mozilla.org/en-US/firefox/addon/722

How to install TOR (on Windows)

If you cannot reach the website http://www.torproject.org/ in your country, it may be banned you will need to configure a proxy to connect to the website (see section 1.4)

1- Download the TOR installation program, direct link for most recent version: http://www.torproject.org/dist/vidalia-bundles/vidalia-bundle-0.2.0.30-0.1.8.exe (this may be outdated. Go to the TOR website to find out what the latest version is)
2- Install TOR on your computer (just follow click "Next" several times and "Finish")
3- Once you have installed TOR, and that the TOR button extension has successfully been installed in Firefox, and that you have installed the "NoScript" extension, you are ready to start using it. A small icon will show up in your system tray, when it turns green, it means it's connected to the TOR network. Connecting to the Internet using TOR is slow. Be patient when using it.

To start browsing the Internet anonymously using TOR, click on the "Tor Disabled" text (in red at the bottom right of Firefox), it may show you a warning about your Timezone and Livemarks potentially leaking through TOR. It's not very serious (unless you have saved Livemarks with sensitive information, livemarks are like "Favourite websites" saved in your browser, but they are always updated using syndication like RSS or ATOM). Once the it indicates "Tor Enabled" in green, you will be browsing the Internet anonymously.

Advanced: TOR has more advanced functions, you can use it as a SOCKS proxy to connect to non-HTTP networks, for example, you can start an SSH proxy through TOR, so your connection will be double-encrypted.

1.6 - Connect to the Internet anonymously through an SSH proxy.

You can connect to the Internet anonymously using an SSH, it's a special protocol which encrypts all communications between you and the SSH server.

This REQUIRES that you have access to an SSH server somewhere in the world. You may first need contacts abroad to be granted such an access. This is very useful because you can "tunnel" all of your Internet connections through the SSH proxy so that the officials in your country will only see encrypted, unreadable data (like when using TOR).

If you have access to an SSH server somewhere in the world, download putty here: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html Putty does not require an Install, just run it.

Instructions on how to tunnel data through SSH are available here: http://kimmo.suominen.com/docs/proxy-through-ssh/

Section 2 - How to exchange encrypted emails

In this section, I will explain how you can freely exchange encrypted email messages with other people, simply and effectively, using Google's free email service and a few programs which you can download for free. These messages will be encrypted using a very effective technology called openPGP, an effective openPGP encryption key will practically impossible for anyone, even the government, to decrypt without the associated pass phrase.

When referring to a PGP password, I will use the term pass phrase.

2.1 - Sign up for a free Google Mail account and set it up

This is the simple part, Google offers a very good email service, just visit http://mail.google.com and sign-up for a free account. When signing-up, Do not enter a secondary e-mail address that can be traced back to you if you plan to use this account to exchange sensitive information. Leave that box empty. Within minutes, you will be shown to your Inbox.

In order to use PGP encryption, we will have to use a client-side application (on your computer) that uses the POP protocol, therefore you must enable POP access on Google mail's side.

Here's how you do it:

- Log on to your Google mail account
- Click settings (top right)
- Click the "Forwarding and POP/IMAP" tab
- Select "Enable POP for all mail"
- So that you don't download messages multiple times, select "When messages are accessed with POP, archive Google Mail's copy"
- Click "Save Changes"

2.2 - Download and install programs

You will need the following programs to exchange encrypted messages:

GnuPG

Download here http://www.gnupg.org/download/

Installation is straight-forward, click next, next, (etc) and Finish

Mozilla thunderbird

Download here http://www.mozilla.com/en-US/thunderbird/

Installation is very simple, once the installation is complete, it will launch the wizard to set-up your email account.

Wizard: Select Gmail -> Next -> Enter your name and email address (without the @gmail.com) -> Next -> Finish

Enigmail addon

Download here: http://enigmail.mozdev.org/download/index.php (select your operating system and version of Thunderbird, defaults are probably correct, click the Download link, save it to your Desktop)

Installation:

- Open Thunderbird, click Tools -> Addons -> Install
- Navigate to your Desktop, open the Enigmail file you have just downloaded, click Install -> Restart Thunderbird
- When Thunderbird re-opens, it may start a Wizard to generate an Encryption key (if not, click OpenPGP -> Key management and the Wizard may start.

Wizard

- Select Yes I would like to sign all my emails -> Next
- Select Yes I have public key for most of my contact OR No I will create per recipient rules for those that send me their public key (The first option assumes that you have an encryption key for all of your contacts, the other one assumes that you don't) I chose No. -> Next
- Where it asks Do you want to change a few settings to make openPGP work better on your machine? Select Yes -> Next
- Create a pass phrase
- Make sure that your pass phrase is very long, this is not like a password, you can write a complete sentence, and you ***should*** do so if you want very safe email exchange. You might even want to include numbers, capital letters etc.
- Once the password has been created, click -> Next -> Next again and it will generate a key for you
- It will ask you to create a revocation certificate in case your key gets compromised. I suggest you do so.

If Enigmail doesn't show you the wizard, you can still manually create your encryption key from the Key Management interface available in the OpenPGP menu.

2.3 - Sending and receiving encrypted emails

To send out an encrypted email, you need to know the recipient's Public OpenPGP key.

To share your Public OpenPGP encryption key to someone with whom you want to exchange encrypted messages with, simply click on the OpenPGP menu, select Key Management, right-click on your own key and select "Send public Keys by email". It will bring up a "New message" window and the key will be included as an attachment. Just type-in a recipient's email address and send the message.

When you receive a public key from someone, it will be included as an attachment, you can right-click on the attachment and click on "Import OpenPGP key", it will automatically be added to your Key Manager.

You can also import keys from a file (see example below)

It is OK to send your **PUBLIC KEY** to people, they can only use it to encrypt messages, not to decrypt them. NEVER SEND YOUR **PASSPHRASE** OR YOUR **PRIVATE KEY** TO ANYONE, keep them secret.

To create an encrypted message, simply click on "Write", enter a recipient's email address in the To: field. Enter your message and subject, and under the OpenPGP menu, select "Encrypt message". If you have that recipient's OpenPGP key in your list, it will automatically encrypt it and send it after clicking the Send button. If you do not have the recipient's PGP key, it will show you the list of keys you have with an error message.

Before sending an email with sensitive data, you MUST make sure that you encrypt the data. If the data you are sending is sensitive, forgetting to encrypt a message can be a serious mistake! Remember: On your new message, go to the OpenPGP menu and select "Encrypt message", and **make sure it is CHECKED**.

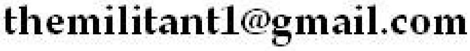
To decrypt an encrypted message sent to you, it's also very simple.
Once Enigmail detects that the message is encrypted, it will prompt you for your pass phrase. Enter the pass phrase you have entered earlier and the message will be decrypted.

Only the sender and the recipient have seen this message! Nobody who has intercepted the message will be able to read it, they will know the From and To email addresses, but they will not be able to read the content of the message! This is very safe.

You want to test it out?

- Open notepad.
- Copy my PGP encryption key (shown below, copy everything from "-----BEGIN" all the way to "BLOCK-----" inclusively)
- Paste the key in notepad.
- Save the file on your Desktop.
- In Thunderbird, open the "OpenPGP Key Management", then click File -> Import Keys from file.
- Choose the file on your Desktop in which you saved my public key and click Open
- I will now be added to list of public keys. Send me an encrypted email if you would like to test it. Send me your own public OpenPGP encryption key if you would like me to send you an encrypted test message.

My email address:


themilitant1@gmail.com

My public key:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (MingW32)

mQGiBEi/axMRBADNt5iYJl8tHFOgFv2Nb/h+OdVwl9qyNsaGF8YfAGuxa9LGnTwl
lArCFlyJW9YkoSC9kIEzcqDtJo1Zu1/X36SSks0s3NkGuPJUraCHeRX/EDKiDpvz
TxnHbdGXN1vis9oIe/wiCiTdozl8yt65bK2z6Qs4gLM+dby6PYQTuJ+WNwCgmRVl
rLQ2EKzzKtnHuyEhF1zeMjkD/3Hf5k7gncVNp9m9QBtdjUwGliAE8AhqmFoHaUdD
TYhdvYvkwr7G+IWjVBLxkAai1HJ/rlYbrfOvLy1UnkybuodH5fsvT+Cem/XVU/Cl
7WiY0UMYssHQxlbeQrdfyL37796M9sEbwqw5wSCPxVJjqyQiO2x3PmAJkzEbegeo
O/v9BAC/XMJavzADYATpa9ThD6zUXjlhE8EeFgZfAm33u1MIpXRpDoyR3FIzIIOe

```
5ZG07FOZtM571Odk2O6tyYum8yjbDzFIq7QUXDDydDP+Ywr8IHMguAU9BxF9mMjI
nYfo5UFZspKGvy+IPYQmY4Ey5ZY3TpS8Wgb0lqL48N+x/lPCWbQlVGhlIE1pbGl0
YW50IDx0aGVtaWxpdGFudDFAZ21haWwuY29tPohmBBMRAgAmBQJIv2sTAhsjBQkJ
ZgGABgsJCAcDAgQVAggDBBYCAwECHgECF4AACgkQtEhii+xIxw6ScQCgh+vBS95D
mW9TLxKZ+WkpXF+XnEoAnis5Qa+P83ANgaASequ198/314JduQINBEi/axMQCAC3
N+JdmTItpBSVHdy3V6Q5tB0XEa3AmyCXN9EQRMeyIA/HabTg/y6kfOiT6o4zRz0K
1RsJXfkOekKUdlL3kO68q33hK7PCWV9xFiq4a7kvb/cAoD3Db2kpAIGMVPTSPDKN
Yh5tVGBX459uLlNsDu4hy4KrSollwLwYe9UYpBH6DmJ5HKTEYNPJv+M/aN98hzKE
T39kiihF/Ev641kTjdZEienZMBNJVi9qrLBEY/Q3oTMB8l4gylq82aO650DVgjO9
cIZ1MSIT54tnGcaLFto570LgZWI4aTxFXtygnTSeDkmnSxgDzO0FZL+vUeHnIf29
7Rzsny944OkYnTlcfJyjAAMFB/4r8azo8CbQ2zvN19Cj+KmAGt1wrwSNy09u7Kdi
8U7h2g7ISJ5S7fQV2aH91mHdBYb/NrynhukBlazFMv2I+E2ORMcTiOGKo6u5Pmm1
39OgUuxeQYYGofU5gRTZiwEGxexArBFhibNQZlOv8PsYiODP3hDfQYJsLSEcTwxY
YLSY0G+siZB1w78sLdGkPvJpQrdaYN0N/J9CmZjqnf7dskk+XlTEnK5poUUginxl
xQvF9prGo+LdkrhUROpa6+0w1EsrNk0v0drmQ07W/S/qN3oCiI4uGbOqnO+2f4kX
LxVt5BjD98zzFVLZjx86fDFwv8fQ7us7724hwpIjXOopiYKiiE8EGBECAA8FAki/
axMCGwwFCQlmAYAACgkQtEhii+xIxw7giwCfcdNe7Onz9tlHjexedd8+80lYSJ4A
ni7gEU3f3rofSLJ5U0J15eEw/o5W
=r4an
-----END PGP PUBLIC KEY BLOCK-----
```

Important notes:

- When using this method, your email address, your IP address, along with other informations will be visible to the recipient. If you do not want the recipient to find out who you are, make sure that you are not connected to the Internet at your home connection and make sure that you are using an anonymous email address. You can also send encrypted emails through TOR, see the next section for more information.
- Sending and receiving messages through Google Mail using the method described here is quite safe because the connection between your computer and Google is encrypted (both when sending and receiving emails). But remember that if a government agency really wanted to find out who you're

sending an email to, it would be possible for them to do so. Decrypting your email message on the other hand would be extremely difficult.

2.4 - Sending and receiving email through the TOR network

It is possible to configure Thunderbird to tunnel all outgoing and incoming communication through the TOR network and it's quite simple to do so. Sending mail through TOR will prevent the email recipient from knowing your IP address.

- First, make sure that TOR is running (see section 1.5)
- Then open Thunderbird, click Tools -> Options -> Network and disk space -> Connection
- Select Manual proxy configuration
- Under SOCKS Host, type localhost
- Next to that field, in Port, type 9050
- Apply the settings.

Now all outgoing and incoming mail will go through the TOR network.

Important Note:
Because of the nature of the TOR network, Google's spam filter may assume that you are trying to spam through Google's service. It is very likely that sending mail through the TOR network will often fail, once it has failed, you will have to go back to your Google mail account settings and re-enable POP access (see step 2.1)

Section 3 - Wrap-up

Be Smart!
Remember that all online service providers log information, IP addresses, referring URLs, accessed URLs, any information that is available, they are likely to log it! If you do something that is prohibited by the law, you may gat caught, possibly months, or even years after the fact!

Combine!

Feel free to combine some of the methods you learned here to insure the greatest privacy and to insure that you will stay safe!
For example, go to a Cybercafe, install TOR there and if you have access to an SSH server abroad, tunnel through TOR to your SSH server and open a SSH tunnel!

Be careful!

Also remember that Cybercafes often have key loggers, spywares or other harmful applications that may monitor what you type! Be careful Whatever you do, make sure that the information you exchange isn't too straight forwards, keep your identity secret at all times when involved in politically sensitive activities in repressive countries!