How to Create and Maintain an Anonymous Identity Online

By
Anonymous33

Email:
anoncitizen@ymail.com

Revision 1
Date: 23/03/2011

WARNING: The information contained in this guide is for educational and protection purposes only. Under no cases does the author condone or encourage the use of these techniquest to break the law or evade law enforcement. While anonymity is a powerful tool, I encourage you to use it responsibly.

Introduction:
There are many reasons why you might want to create an anonymous identity online. Perhaps you're a whistle-blower funneling information about your organization to the police or a reporter, maybe you're a political activist who could suffer unspeakable persecution if your true identity were to be know, or maybe you're just a run-of-the-mill citizen who values privacy and believes that no one but you should have access to your private data and communications. Whatever your reasons for wanting to remain private, this guide will give you the steps to effectively create and use a completely anonymous online identity.

Loose lips sink ships:
Before we get started, let me say a word about talking to people. Everyone loves to be social. We value our friends and we don't want to be constantly paranoid that someone is out to get us. But remember that everyone you tell about your anonymous identity is one more person that can be compromised or turned and, in turn, compromise you and your security. Now is the time to be paranoid. Never discuss your anonymous identity with anyone who knows your real identity and never discuss any details about your real identity with anyone while using your anonymous identity. Keep the two completely separate.

You might be sitting there thinking "my friends are cool. They would never compromise me; they're loyal". That might be true now and it might remain true in the future. But I personally know of several cases where people have been sent to jail by their 'loyal friends' after the friend decided to turn on them after a fight. Why expose yourself to the risk? Keep your mouth shut!

The importance of open source:
Open source software is software where the underlying computer code is provided by the developer to anyone who wants to review it. Contrast that with what is known as 'proprietary software' (like Microsoft Windows, Office, most Windows software, etc) where the code is not available for you to inspect.

The truth is you have no reason to trust a software developer with your privacy. If you have no way to verify that what they say is true, you can never know if the software does what it says it does and that you are even protected at all. For all you know, that 'unbreakable encryption' program you just paid $30 for could have a back door built in that lets law enforcement in whenever they want. It might not but, the point is, you just don't know unless you can examine the

software code yourself.

That's why I recommend using open source software exclusively for your anonymous identity. And I don't mean just 'user land' software like encryption tools - I mean everything from the operating system up. If you are forced to run Microsoft Windows, learn how to run Linux in a virtual machine and use that for your anonymous identity. If you're not using open source software from the ground up, don't do anything anonymous because, chances are, you're not nearly as anonymous as you think you are.

The Tools of the Anonymous Identity

Surprisingly, creating an online identity is remarkably easy. It's because it requires a bit of work to use it effectively that most people never bother. Most people have the belief that if they aren't doing something 'wrong' then they don't need to be anonymous. This is a lie governments and law enforcement around the world have sold to the population and it couldn't be more false.

So let's assemble all of the tools we need to create our new identity then we'll move on to actually creating and using it.

1. Download and install both Tor and I2P Tor and I2P are anonymizing systems that allow anyone to surf the Internet or use Internet services like chat, email, and the web, completely anonymously. While both serve a similar purpose, there are some places where you will have to use one or the other (most IRC networks, for example, ban Tor users) so it's important to have both installed and ready for us.

Download and install the "Tor Browser Bundle" from the following location:

http://www.torproject.org

Download and install I2P from:

http://www.i2p.de

Both software packages are available for Windows, Mac, and Linux, but keep in mind our discussion about open source software earlier so I again encourage you to use Linux, even if it's just through a virtual machine.

Spend some time reading how both tools work until you're comfortable that you can and have properly set them up for your use. It's not too hard but it's vital that the tools be working correctly for the next step.

2. Start the Tor software and the anonymous browser that's included
The Tor browser bundle comes with a special customized version of the Firefox web browser that's ready to use anonymously. Once you click on the 'start-tor' icon in the Tor directory, it will set up an anonymous connection and then automatically launch the secure browser.

This is an important note so don't skip past this section: it is important that you only use the Tor browser for anonymous things. Under no circumstances should you ever check your personal email, bank account, or anything connected with your real identity while anonymized. It is imperative that you separate your two identities as much as possible. Even one slip up could completely compromise your security and make this entire exercise useless.

When the secure browser starts, it will automatically take you to a web page that will tell you if Tor is working properly or not and will give you the Internet address you appear to be coming from. If everything is working then you're completely anonymous while using the secure browser.

Important security note: your anonymity ONLY applies to the secure browser!! No other browser on your computer is safe except the browser launched by Tor. Even if you use Firefox as your regular web browser it is not secure unless it is started by Tor.

Extra paranoia note: It is always a good idea to check which country owns the IP address you are assigned. Having an IP address outside of the United States, Canada, or Western Europe can greatly increase your security. You can find out what country your IP address is located in by doing a Google search (in your anonymous browser) for 'ipwhois' and using one of the tools in the search results. If you want another IP address, shut down Tor and restart it. Continue this process until you get an IP that is acceptable.

Once you're familiar with Tor, it's probably a good idea to learn how to anonymize any of the Internet programs like chat that you use. This will allow you to communicate in a variety of ways without having to reveal your real

identity. The Tor manual explains how to do this pretty easily. Read it.

3. Create an anonymous email address
I've investigated different email providers to determine which ones are the easiest to remain anonymous using. Yahoo Mail comes out on top for a number of reasons. First, it does not require any real personal information. GMail, for example, requires a real mobile phone number which complicates the process greatly. With Yahoo Mail, you can use completely bogus information and be totally anonymous.

So the next step is to point your anonymous browser to

http://mail.yahoo.com

and click the link to create a new account. It is important that you use completely bogus information here and any information you use should have absolutely no connection to your real life. That means no real birthdays, no real first, middle, or last names, nothing. Fake everything! And, for God's sake DO NOT be dumb enough to use your real zip code, city, or state (or even country) while setting this account up. I like to use a postal code and city in whatever country my current anonymous IP is from. Just a nice touch. Also, do not use a real recovery email address. If you've ever touched something in real life, don't touch it in your anonymous life, period.

Once your anonymous email address is set up, be sure to create a file somewhere on your computer with all your 'personal' information in case you need to do a password recovery. We'll encrypt this file later so there's no worry about a compromise.

Important security note: Remember the rule to never cross your anonymous and real lives. NEVER ever ever check this new email address while not anonymized. NEVER ever ever send email from that address to your real life email address or one that was created when you weren't anonymized (or the reverse) and NEVER ever ever send email to real life friends. All of this COMPROMISES YOUR SECURITY AND CAN LEAD TO YOUR REAL IDENTITY!! If you EVER do any of the things I just mentioned, abandon the email address immediately and go through the process of setting another anonymous one up. This one will become useless.

Congratulations! You now have a completely anonymous email address. It will remain completely anonymous as long as you follow the advice above.

3. Set up an anonymous Box.net account
Box.Net is a fantastic service that allows you to store up to 2GB of files (each file can be up to 25MB in size) for free. It's a great way to securely exchange files with others in an anonymous way if it's set up correctly.

First, make sure you're in your anonymous browser and go to

http://www.box.net

Sign up for a free account using completely bogus information again. It's OK if you use the same information you used to set up your Yahoo account since these two accounts will be tied together anyway. When asked for your email address, remember to use the new anonymous address and NOT your real email address or any you created while you were not anonymized.

Once you've completed the sign-up process, you will be required to validate your new account. Just go to your Yahoo mail account (again, in your anonymous browser) and do the validation. Easy as pie.

You now have a secure way to share files with others. Just remember NEVER upload a file to the BOX.NET account unanonymized. If you do it even once, scrap the account and start over. This will also mean you need to set up a new anonymous email account as a correlation could now be made by an investigator.

4. Download and install GnuPG (the GNU Privacy Guard)
You've probably heard of PGP. It's an encryption program that allows you to encrypt files and email so that they can only be decrypted by either the intended recipient or by a specific password. GnuPG (GPG)is an open source implementation of PGP that is fully compatible with the commercial version of the software but with no potential deliberate back doors!

Once you've installed GPG, you will need to create a new encryption key pair. Each encryption key has two parts: a public key which you share with anyone you communicate with and a private key that only you have access to.

You can get GnuPG from

http://www.gnupg.org

Let's create a key pair now for your anonymous identity.

First, drop to your operating systems command line (Start->Accessories->Command Prompt in Windows and Terminal in Linux) and type the following command:

gpg --gen-key

This command calls the GPG program and tells it you want to create a new key pair. The program will ask you a few questions such as your real name and email address (use the fake name and email address you just created) and a few other things.

When you're asked what kind of key you want to create, I recommend that you use the following information:

Type of Key: RSA / RSA
Length of Key: 4096 bits
Key Expiration: 3y

At the present time, 4096 bit RSA keys seem to be unbreakable. We're making the assumption that they will remain unbreakable for the next 3 years which is why we'll have our key expire in 3 years, at which time we will re-evaluate if we want to continue using them or create something stronger.

You will also be asked to create a passphrase for your key. This is very very very important. The only thing standing between your private data and an intruder is your passphrase. DO NOT use common words, phrases, etc. I recommend you use a string of 64 random characters that contain upper and lowercase alphabet, numbers, and special characters. Store this passphrase somewhere safe so it can't be found.

After a bit of work, you will have a new key. You are now able to encrypt data so that it is inaccessible to anyone, including law enforcement.

Data encryption note: The same type of password should be used when encrypting data as when creating your key: a random, long string that contains a mix of characters and no real words. The passwords should all be at least 64 characters but the longer the better. I have personally protected extremely sensitive files with 900+

character passwords. If you need help remembering your passwords/passphrases, we'll discuss that in the next section.

You now have a PGP/GPG encryption key-pair. One more step to security. I'll leave it to you to research how to send and receive encrypted emails or handle encrypting and decrypting files. It's all on the GnuPG website in the manual. Spend some time reading it.

5. Download and install Keepass (or KeepassX)
Keepass and KeepassX are programs that allow you to securely store your password. To remain completely anonymous and secure, your passwords need to not be easily breakable. That means long, random, meaningless strings of characters that you can't (and shouldn't) remember. Storing them in Keepass allows you to store them in a secure AES-128 bit encrypted store that is currently thought to be unbreakable.

You can get Keepass from

http://www.keepass.info

Since the software is easy to set up, I'll leave you to figure it out. One note though is to make sure you use both a password (something you can remember but not easily guessable) AND a key file to protect your passwords. This double layer of security makes sure your passwords are only accessible to you.

it's also a good idea to store both your key-file and your password safe on removable media like a flash drive. This way, it's not even accessible for attack if your computer is ever stolen.

Extra paranoia tip: If you're really concerned about protecting your password, encrypt both your key-file and your password safe using GPG and a password that is easy to remember but hard to guess (preferably with some random bits. That means you'll need to decrypt both your password safe and your key-file every time before you use them but it might be worth it depending on how secure you need to be.

8 **Encrypt your anonymous information file**

You'll remember that in an earlier step I told you to save the details of your anonymous email address in a text file so you could easily remember details if you needed them. Because you didn't set a recovery email address, if you don't remember the answers to your security questions and forget your password, you will be permantly locked out of that account.

But you can use this file for more than just your anonymous email account. I use my information file (which is really just a text file that I encrypt) to keep track of my anonymous online dealing. I have identity information, who I've contacted from what identity, what I've told them (if it's important to remember), that sort of thing. Since it's encrypted and secure, I don't have to worry about what's in it should my computers receive a special visit by law enforcement or a hacker one day.

So take the time to encrypt this file now. There are two ways to encrypt a file in GPG: 1) to a specific key in your security keyring or 2) by password. Some people like to encrypt files to their own key so they can decode them later but nobody else can even if the file falls into the wrong hands. This is a bad idea because, if you lose acces to your key, you are forever unable to access that file. Just like your key keeps your data safe from prying eyes, it will also keep you at bay if you don't have the right key.

The second reason I like to encrypt using a password instead of to a key is that I've read papers that have made the argument that a AES-256 key is as strong (or perhaps a bit stronger than) a 2048 bit RSA key. So, for those two purposes, we're going to encrypt your file using a password (long, random, at least 64 characters of course!)

Do encrypt your file, open a command prompt and type the following command

gpg -c <your_information_filename>

GPG will prompt you for a password which you are free to cut and paste from somewhere else since it's hopefully too long for you to want to type twice. Once you've entered and confirmed your password, a new file will be created in the same directory as the original and with the same name as the original but with the added extension .gpg. That .gpg file is secure, unbreakable, and safe.

Next, you probably want to get rid of the original unencrypted file since having it around kind of defeats the purpose of having it encrypted. On Microsoft Windows there are a few freeware tools that allow you to securely delete a file and I recommend one called AxCrypt. AxCrypt can also encrypt files using AES-256 bit encryption so it's like a swiss army knife of tools.

You can get AxCrypt from

http://www.axcryp.org

It comes with a handy guide on how to use it. Basically, right click on the file you want to securely delete and select 'Shred'. If it prompts you to specify how many times to overwrite the file, select 250.

On Linux, the system has a built in command called shred that accomplishes something similar However, I do suggest you read up on shred because there are specific concerns that may need to be addressed if you're running a journaling file system. Overall, securely deleting a file from your disk is a simple command:

shred -u -n 250 -z <filename>

This tells the command to shred the file, wiping it 250 times and then filling it with 0's and to truncate and remove the file after overwriting.

Congratulations You are now prepared to be completely anonymous online! You have all of the tools you need set up and ready to go. Your privacy and anonymity are completely in your hands now. You can now safely go on to connect to and use web services anonymously, share information, and do pretty much whatever you want without fear of reprisal or discovery.

You are the resistance, you have the power, use it well.

Questions?
Find me on IRC and chat with me:
Server: irc.anonops.ru
Room: #opnewblood
My Nickname: Anonymous33

How do I connect to IRC?
Go here:
http://03.chat.mibbit.com
Choose a nickname, plug in the server details an chat!

My Email Address, if you prefer to email is
anoncitizen@ymail.com