Guide to Complete Anonymity

Author: Leo Gurr

Table of context

Prologue

To make clear, I am not affiliated or sponsered by the group Anonymous.

Before you go googling different things trying to find means of protecting your privacy, there is a question you must ask yourself. Why are you concerned with your privacy? The answer to this might change your life. There are most likely a few reasons why you value your own privacy.

1. You do not want big name companies holding all of your data and selling it

2. You do not want people in your close proximity knowing what you are doing

3. You want to isolate

4. You are doing something you are not “supposed” to be doing

Lets clear the air for a second. If you care about your privacy because of reason one, there is an easy solution to this and you do not need this paper. Also, answer one is most people in this world. Why would you want Google knowing everything about you? Most people have given up all their rights to Google without even batting an eye. Google maps, Google search engine, Google with youtube, soon to be Google cars, and much more. If you were ever to be considered a valued target, Google has everything about you. The more valuable you are, the higher the cost of the information. So to fix this, just do some research on different VPNs. A VPN is a virtual private network that hides your IP to big names, such as Google. VPNs get explained later on in this paper if you are interested in reading, but you do not need this whole article. Figure out which VPNs are good and which ones are shit. Make sure to get a VPN that can only be used if you pay for it. Learn what VPNs can and can not do. But to repeat for people concerned about their privacy for reason one, do not need to go to these extremes

How about option two? Well, this is a minority for most people actually. Almost everyone does activities they do not want their family members to see online, but there is something called clearing browser history. Besides, you can always download firefox and set it up so it never saves data. You could also route your traffic through VPNs or the Tor network so people can't look at your logs and find out that way. Also, consider encrypting your entire hard drive. So someone can not just open it up and see everything you do.

Let's be honest about option three; if this applies to you, then you should not be using the internet. The internet was not built to be truly anonymous, and you should be using it to interact with other people. So this is a smaller minority than even option two. But if you are choosing to use the internet and want to isolate, then this guide might be for you. Read the paragraphs below to see if you fit better into option four.

Onto the meat and potatoes of this whole paper, people who agree with option four. There is no reason why you would want complete anonymity unless you were doing something you trying to hide. This does not mean you are buying illegal goods or looking at illegal images, though it could, it means you are trying to hide what you are doing from everybody who means you harm. This would be useful for whistleblowers, journalist, criminals, governments, hackers, and others I can not think of. I will not tell you where in that list I fit into, but I will tell you I am there. Chances are good if you are reading this, you fit into that list somehow. It is people like you and me who need this guide. I will not tell you how to use these things I will teach you, I will only teach you. A teacher teaches their students, then the students can help or destroy others.

There are quite a few tools that you will learn here in this guide. Here you will learn how VPNs and Tor work on a surface level. Learn what Linux is, and just what it can do for you. Also, how to communicate in the open air with sensitive information. Plus, how to use bitcoins to make purchases that are untraceable. If this sounds interesting and/or something that you need, keep reading. Understand that what I am going to try and teach you will take time to learn. Lots of time to learn. But, in the end, you will understand the basics of how to stay truly anonymous and also where to go to learn more information.

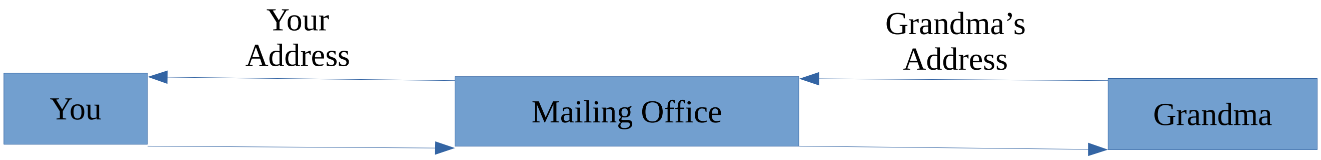
[Disclaimers] This is not a “direct guide” or “guide for dummys”, meaning I will not tell you exactly what to do. I am going to give seperate suggestions on what you should do for your own privacy. That being said, I am going to present different options, and explain what each option has to offer is on a “surface-ish” level. Then it becomes your job to do extra research on the topic. I am sorry if you are looking for direct directions. If you want a “cheat sheet” for what I would suggest, here is a path to follow. Get non-traceable computer, get Qubes, get Whonix, get crytocurrency, use GPG, create sperate identites, and never share personnal information. Really, this is a guide to help gain a better understanding of common tools that people should use for sercurity. I believe it is important that people have a foundation on topics before using them. You can even look at this guide as a history of certain tools, if you want to. If you are the type of person who likes direct explaintions, without fluff, you will not find this guide useful.

To sum up, this guide is for people who have some knowledge, but want more. Experts will not find this guide useful. People between expert and novice with find this guide the mose useful.

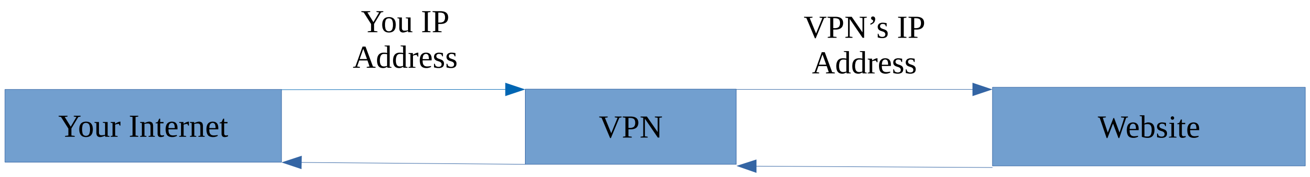
Chapter 1 – VPN vs Tor

To understand how to stay anonymous on the internet, you need a basic understanding of how the internet works. You have most likely heard the term "IP address" thrown around a few times. Most people think it is this complicated thing that only hackers need to know. But this is not true. Everyone should have a basic understanding of how the internet works, and how IP addresses relate to you. Your IP address is a key aspect of making sure your internet works.

Let's think of how you would send mail to your grandma's house. First, you write a letter, then you write your grandma's address on the card, then you write your return address, and then you send it to the mailing company. The mailing company does its thing and arrives at your grandma's house. Then your grandma wants to write you back a letter. Your grandma looks at the return address, writes her letter, writes your address down, then sends it to the mailing company. Again, the mailing company does its thing and the letter arrives at your house. If you had not written down your address for your grandma to send you mail, she would have no idea where to send it to reach you.

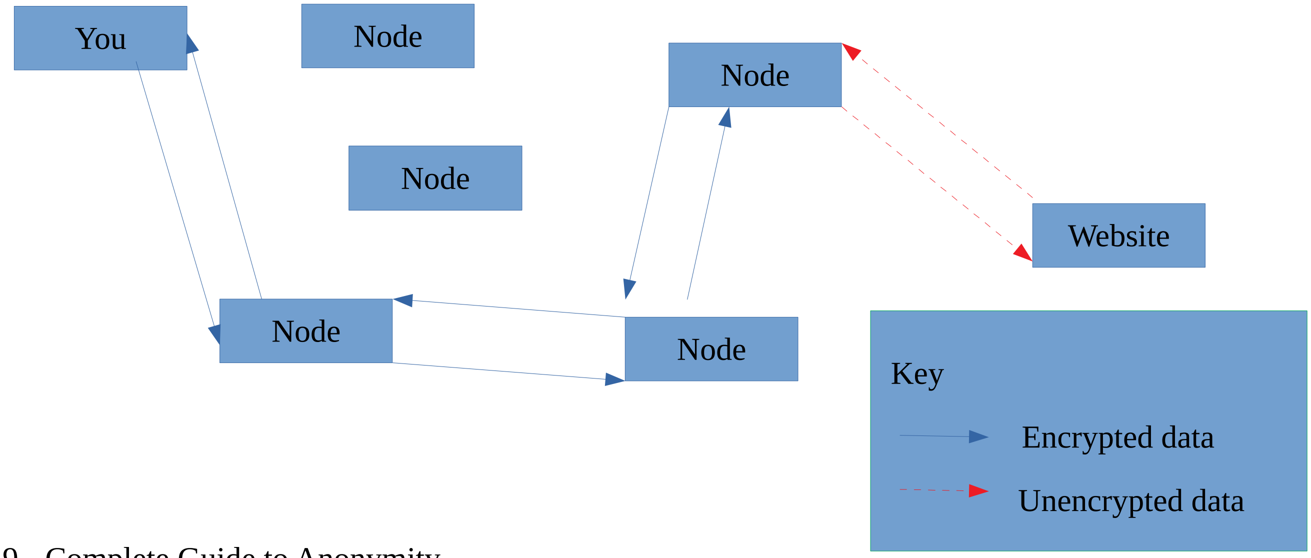


This idea is extremely similar to how the internet works. For you to get data from a website, you have to have your IP address connected to the websites IP address. These addresses are how you and the website communicate. Now say you are doing something that an adversary might take interest in. It would be very easy for them to track you using only your IP address. Because you are directly giving up your IP address to the website. Now there are quite a few ways that you can "mask" your IP address from an adversary, but we are only going to look at VPNs and Tor for the purpose of this paper. VPN stands for Virtual Private Network, the goal of a VPN is to replace your public IP address with the public IP address of the VPN. So instead of your data being sent directly to a website, your data is first sent to the VPN and then to the website. Then the website sends the data to the VPN, then the VPN sends the data back to you.



Again, to most people, a VPN is good enough. But there are a few flaws with a VPN. A VPN has the ability to log everything you are doing. Even though an adversary is only able to see that traffic is flowing to and from the VPN in use, the VPN see everything you are doing. If the adversary has enough power, they could demand the logs from the VPN and your traffic is no longer hidden. Most VPNs have at least thousands of clients so there would be no need to dig up your files unless you are doing something that an adversary would take interest in. I would recommend not using a VPN for this reason when it comes to being completely anonymous. But if you are not doing anything that an adversary would take interest in, I would definitely recommend using a VPN for everyday activities. Just make sure to get a paid VPN. Nothing is free in this world, and the VPN has to be making money to keep running. How do you think free VPNs make money? They make money by selling your data.

Now let's talk about Tor, The Onion Router. To most people, Tor sounds a lot like a VPN. The reality is, they were made for completely different purposes. VPNs were made for security, while Tor was made for anonymity. A basic overview of how Tor works is by routing your traffic through 3 different nodes. If you want, you can think of Tor as three VPNs tied together. Your data goes into an entry guard, then a middle guard, then an exit relay, and onto the website.



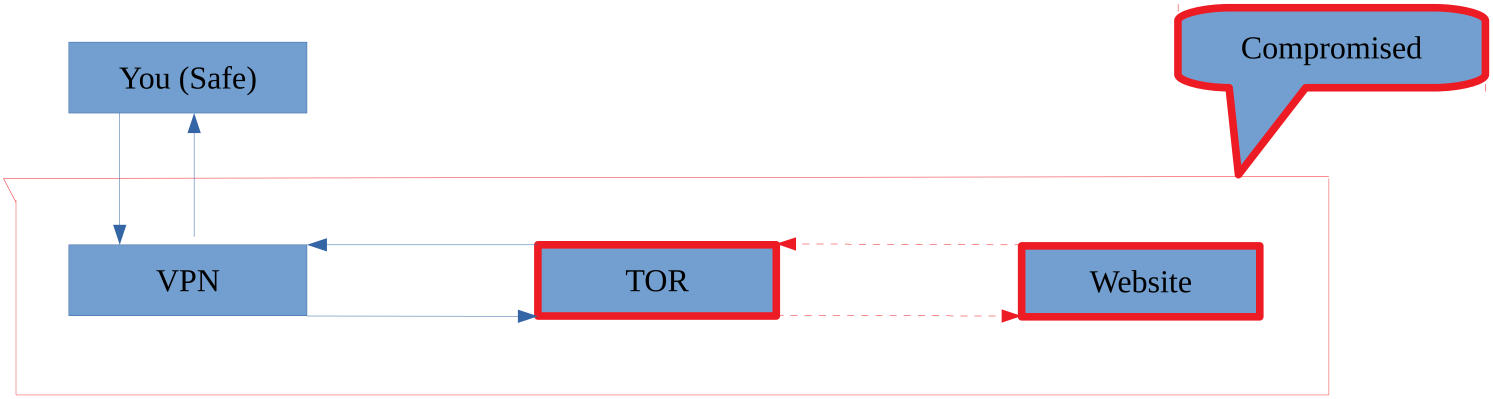
So you might be wondering why Tor might be better than a VPN, well it some ways it is not. If an adversary were to have control of both your entry node and exit node, they would be able to decrypt all your data and find out what you are doing. While this might sounds scary, Tor has things in place to try and minimize this threat. First, the three nodes, which I will call "path" from now on, changes with every website that you visit. So since your path is constantly changing, it is very difficult to track everything you are doing. This idea of using three nodes and a changing path is called onion routing. So if you are doing something that you really do not want people to find out, do not use your own wifi. Use public wifi, or if possible use your neighbor's wifi (Not encouraging illegal activities, such as hacking wifi). Botton line, Tor alone is not good enough. Go read some articles about the different bust over the years. There is some really advanced tech that people use now to keep themselves safe while hosting on the Tor network, which you will not have access to.

Another thing Tor does is it has a function built in called HTTPS everywhere. This makes sure your data is encrypted fully and has no gaps where an adversary can read your data. But HTTPS does not stop an adversary from knowing that your IP address is visiting a certain website if the entry and exit node are compromised. You will learn more the more that you practice and read.

Chapter 2 – VPN plus Tor

Somethings to note for this guide: blue boxes represent objects (such as your computer) that are connected to the internet, black boxes represent objects that are not connected to the internet, and red outlines mean either dangerous or disposable objects.

Say if you have no option but to use your own internet from home. What a lot of people do is use both a VPN and Tor. They will first route their data through the VPN, then into the Tor network. The idea is if an adversary were to gain control of both the entry and exit nodes, then they would only be able to see the IP address of the VPN. Also if there is a bug in the code of Tor that leaks your real IP address, an adversary would only be able to see the IP address of the VPN.



This may sound good on the surface, but the same problems from earlier are still present. If the adversary was motivated enough and had enough resources, they can still obtain your logs from the VPN and link you to everything you do within Tor. Plus there is the added risk that the VPN reports directly to an adversary anyways, completely negating the purpose of using a VPN.

So my recommendation, just do not use a VPN at all. If you have to use a VPN, get the Tor browser and get a VPN from inside of Tor using untraceable bitcoins, more on bitcoins later. This way the VPN does not know who you are. But, they will still know what IP address you are using and that you sending data to Tor. So again, I would still recommend using public wifi, or at the least not using your own wifi. If you want to learn about VPNs and how to link VPNs to Tor, you can do research elsewhere. I believe you are putting too much faith on one single point, which could easily break.

Chapter 3 – Linux plus equipment gathering

This is the first chapter in the guide where I will actually teach you how to do something. It is important that you learn a foundation of why you are doing what you are doing. You do not want to mindlessly do different things, just because someone said you should. Always verify what others tell you, and keep on learning. But, onto the chapter.

Glad that you know what VPNs and Tor are, and how they can benefit you. But before you go download the Tor bundle and just use it as is, there is something else that you need to know. The Tor bundle is not for everyone. Assuming you are using Tor correctly, there should never be a link between you and your online activities. The reality is, this will not be true if you using Windows. Windows is just not a secure OS.

What does that even mean? Glad you are full of great questions. OS means Operating System. So, every time you boot up your computer, your computer first goes into the BIOS. Then from the BIOS, it boots up into Windows. Anything that boots off the BIOS is called an OS by definition. There are other OS's out there than just Windows, MacOSX (What macs use), and IOS (iPhones). The main OS that is used besides these is Linux, which is used in androids and some computers/servers. When computers were first being made, there was a debate about whether manufacturers should use Windows or Linux. Linux is much more powerful than Windows, in terms of what the user can do with it. But Windows is more simple than Linux and good enough for most people. So now almost all computers ship with Windows installed unless you are buying a mac that is. But some computers do not have Windows installed as their main OS, they have Linux installed. You can actually install Linux onto a computer that already has Windows installed on it. Plus, Linux can be built from the ground up, if you learn how to programme, and be built just for your needs. So, you can imagine why we would want to use Linux over Windows. There is so much more that can be done with Linux that Windows can not do. There are many different types of Linux distros, unlike Windows. Some Linux distros were built specially for security, management, scientific research, and privacy. We will be looking at the Linux distros that were made to protect our privacy, Tail versus Whonix primarily.

You are most likely asking yourself a few questions, why is Windows not good enough? Even if I wanted Linux on my computer, how do I get these Linux OS's on my computer? Let's look at that first question first. It depends on your needs. Windows by defaults does not have backdoors when first installed that will leak your information unless you have a virus. That is our primary issue with Windows, a lack of security it provides. If an adversary were to take enough interest in your activities, they could find a way to get a virus, probably trojan virus, on your computer and gather information about you that way. Windows does very little to prevent this. Even with the best of the best firewalls, Linux is much safer than Windows. If we want to compare Mac to Windows, that is a different story. Mac has great security, and I would not put them down. But Mac has never released programming code to ensure they do not have their own backdoors installed on MacOSX. Knowing that Apple created Mac, there is a good chance they are logging everything you are doing. Again, I come back to Linux. Linux is open source and everyone the chance to go in and inspect the code and make sure it is safe. If you download Linux, there are plenty of forums to help you learn your new OS and what to do with it.

The second question, how to download these Linux distros. You could just Google "how to download Tails/Whonix" and let the websites do that talking for me, but that is risky. You, with your IP address, are asking how to hide your IP address. Since you are Googling Tails/Whonix, that means VPNs and Tor alone are not good enough, and adversaries want to know why. Let cut this out of the equation, and let's make sure you do not get red flagged. Allow me to teach you how to learn more about Tails and Whonix without getting yourself red flagged.

What I am going to suggest might sound excessive, that is because what I am going to say is excessive. But it is the people who take no chances who will keep on walking free, so listen up. Let's get some equipment. What you need to buy openly are 2 USB drives. One of these drives should be small, 8 or 16 GB, and the other at minimum 128 GB. On the small drive, download a fresh copy of Windows. On the website with the ISO file, you will be given directions on how to do this. An ISO file is an image with the OS inside that can burned onto a CD or Flash Drive. Then your next course of action is to decide how you want to get a computer.

Let me take a step back, you might think that the computer you are using right now is good enough. I will tell you right now, it is bad security practices to keep your secret activities on the same hard drive that you keep your everyday activities. So you I am going to suggest three options on how to separate your identities: Buy another computer, buy another hard drive, or find other means of gaining a hard drive or computer.

If you are going to buy a new computer using the internet as a way of finding that computer (such as Craigslist, eBay, or Amazon), follow these directions. First back up your entire computer onto the large flash drive that you have. Find out what files are important to you if your flash drive does not have room for your whole OS. Then completely wipe your drive clean using the small flash drive and install Windows. Also, install Windows in a public wifi zone. Your goal is to have this install have no ties to you in any way. So do not use your real information. Then do your shopping like normal form public wifis. I would highly suggest using Craiglist or eBay so you can call and drive to wherever you want to go. Also, pay in cash. Limit your ties between you and this computer. There should be no reason that anyone should be able to tell that you have another computer. This is to create plausible deniability. If an adversary were to show up at your house, there should be no reason they would have a reason to believe you even have another computer. Then once you have the new computer, you can wipe and reinstall Windows on your old computer with all you back-upped files. Then wipe and install Windows onto the new computer. The only trail you should have left in theory is the person seeing your face, and the phone calls you made.

There is another way to buy a computer, person to person. You could go to a pawnshop and buy on there, hopefully without needing an ID. Or you could see if you have a friend who would be willing to buy the computer for you or sell you a computer. This is just a valid as an option, and you do not need to wipe your original hard drive. This route is the one I would recommend. Just make sure to still wipe and reinstall Windows on the new computer.

If you want to use your same computer, but just change your hard drives, then your process is much easier. Well, it is easier assuming you know a few things. You should know how to take apart your computer, remove the hard drive, and put in another hard drive. All you should need to do for this is go to any technology store and buy a new hard drive in cash. Then you can wipe this and install your own Windows on here from your personal computer. I do not prefer this option. I find it very difficult use your computer. You have constantly keep changing hard drives if you are using Whonix, or remove it if you are using Tails. So this is an option, but I do not recommend it.

Those are the ways I would suggest getting equipment to keep your personal life and private life separate. If you are clever, you can come up with other ways of finding a computer or hard drive to use. Just make sure to set up your new computer/hard-drive in public wifi, do not update it, and do not use real information. This is the computer you will do some research on. So if the IP address gets red flagged for your research, it should be the public wifi that gets red flagged, not you. The first thing you need to do once this computer/hard-drive is setup is download Tor, and do all your research from within Tor. Do not use this computer/hard-drive unless you are using Tor.

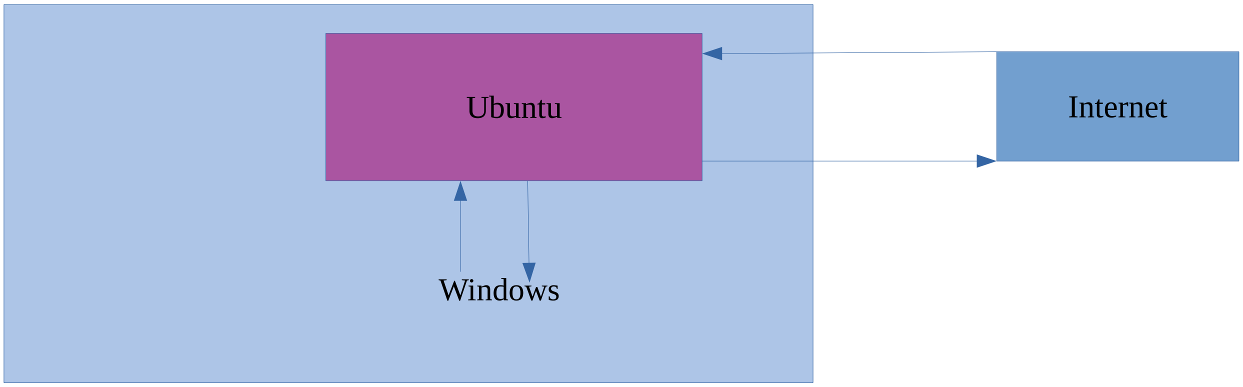
Chapter 4 – Tails vs Whonix+Qubes

You have learned a lot. You have learned how Tor and VPNs work, differences between Windows and Linux, and how to get a computer and hard drive in a safe way. By this point, you know much more than the average person. You actually know enough to be relatively safe, but that is not good enough. You are reading this because you want to be completely anonymous. So now we are going to discuss the different OS's you should be running on this new computer. The two main Linux distros that I would recommend to you is Tails and Whonix lets take about both of those.

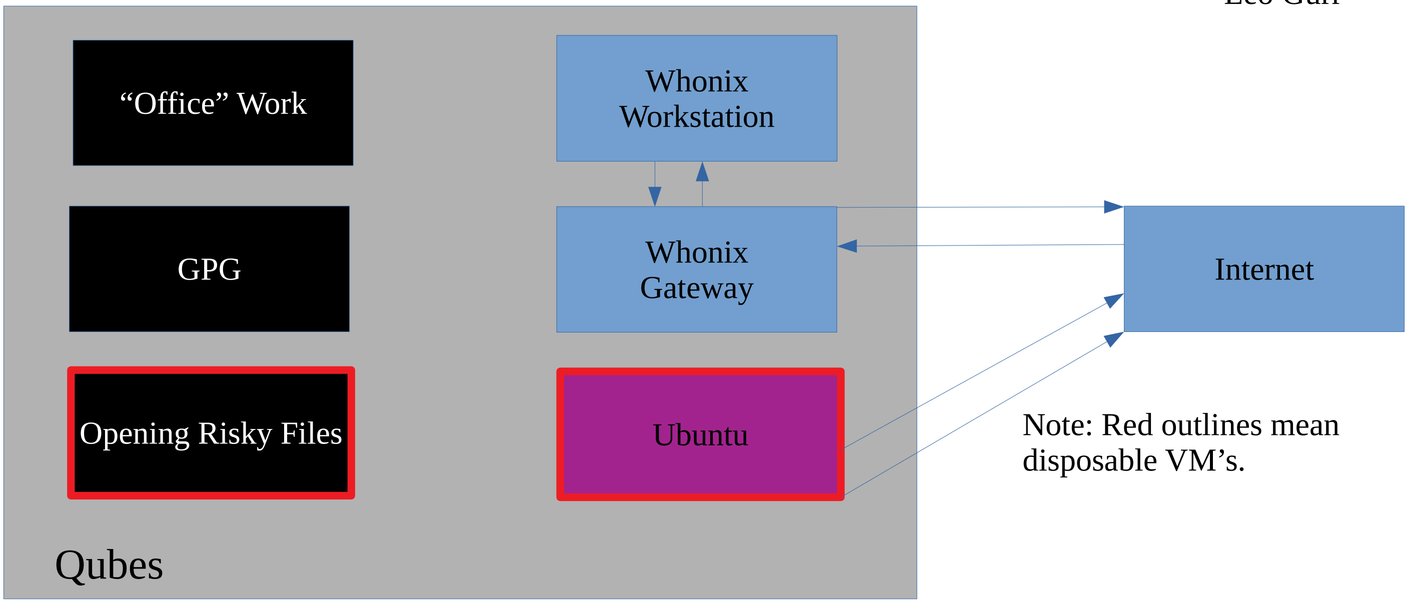
Tails, completely amnesic. The goal is to leave no traces on your computer and to have everyone using it look the same on the internet. So in theory, there is no way to tell one Tails user apart from another Tails user. Tails is also run as a Live OS from a removable media, such as a USB stick. A live OS can run on a computer without a hard drive at all. Even if you do have a hard drive plugged into your computer, Tails was designed to leave no traces on your computer. After doing some penetration testing, I have found that Tails can leave evidence behind that allows for an adversary with control to your computer to find out that Tails was run on it. So plausible deniability goes out the window if you are trying to hide only the flash drive at that point. But if you run Tails on your computer without a hard drive, there are no traces left behind at all. You can save data on persistent storage within Tails, so you never lose your progress no matter what computer you use. Again, the persistent storage is not hidden from an adversary, and there are a thousand reasons why you might have to give up your password. So if there is an adversary knocking at your front door, I would recommend destroying the flash drive. Also, all the internet that is used in Tails is routed through the Tor network. There are drawbacks to Tails, read the documents that Tails provides about what Tails can and can not do.

Whonix is much more complicated to get set up than Tails in my opinion. But Whonix is far better than Tails if you planning on using one computer for all of your private internet activity. Whonix saves everything it does on your computer, but it is only run in virtual machines. If you do not understand what a virtual machine is, allow me to explain.

A virtual machine, VM, is basically a computer that runs inside of your computer. You can learn how to install virtual machines on almost any OS. So say you download Ubuntu, a popular version of Linux, on a virtual machine inside of Windows. Everything that you do inside of Ubuntu will be separated from Windows. The drawback is that this does not go the other way around. Windows can see everything that the Ubuntu VM is doing. So if your host machine is infected with a virus, the virus can see everything that the VM is doing. So the VM is only as safe as the host machine it is run on. This means we do not want to run Windows+Whonix+Tor for the same reasons we do not want to run Windows+Tor. If you are doing this, all you are doing is adding tinted glass between you and the world. Might be harder to see and get to you, but someone motivated can still easily find you.



But on the bright side, say your ubuntu VM gets infected with a virus, it will not be able to escape the VM into the Windows host machine. Most of the time, it is very difficult for viruses and websites to even know you are using a VM in the first place. So, we want a host machine that is safe to run virtual machines on. Almost any Linux would work fine for this, but there is a special OS that was built specially for this, Qubes. Qubes was built with only security in mind. Everything you do has the ability to be run in its own VM. So if one of your machines gets infected, you can just destroy it and move on. You can even create disposable VMs that are used only to open dangerous files, then delete once you are done. This is where we are going to be using Whonix. It is important to remember, you do not have to use Whonix with Qubes. Qubes can be used for everyday activities, it just has a steep learning curve to get used to.



Note: Red outlines mean disposable VM's.

If you did not notice, there are two different VM's for Whonix in the diagram above. This was done on purpose. Whonix actually is meant to be run from two separate VM's. One is the Whonix gateway, and the other is the Whonix workstation. The gateway's only job is to connect to the Tor network and act as a router for the workstation. Since the VM's are separate, if someone were to hack the workstation they can not find out your IP address. This is because not even the workstation itself knows what the IP address is. So if someone were to gain complete control, root access, to your virtual machine, they can not find out your IP address. Because, not even the workstation knows what your real IP address is. If you are getting excited, good. There is still a lot to learn though. You still have to realize the drawbacks with using Tor are still present while using Whonix. One of Whonix's famous quotes is "the more you know, the safer you are".

Both Tails or Whonix are fine; just understand that Tails has less security and is more flexible. Whonix has more security and is less flexible. I am not saying that Tails is insecure or that Whonix is not flexible, I am saying they each have their strengths and weaknesses. Depending on your needs, you need to do research and learn how to download one or the other. The next parts of the guide are going to assume you have one of these OS's. If you do not have Tails or Whonix downloaded, but are still using Linux, you can still follow most of this guide.

Chapter 5 – Tails Basics (Veracrpyt)

I would still recommend reading this section, even if are using Whonix. I might be beneficial to have both Tails and Whonix, depending on your needs.

I am going to assume you have got Tails up and running and have downloaded everything over the Tor network. This first thing I would do is set up persistent storage and check all the boxes, you will learn how to use everything as you go. Then, I would reframe from just using Tor without reading the rest of this guide. Next, lets set up storage for more sensitive information.

Tails supports the use of Veracrpyt, a way to encrypt information onto flash drives. You might be wondering, who do I need to to have another encrypted storage if I already have my Tails drive with persistent? There are a few reasons actually. The primary reason is that Tails has to do updates to make sure that you have maximum security. When you update your Tails drive, there is a good chance that you will lose everything during the update. So keeping your important data on a separate flash drive is a must. Also, the can create plausible deniability. You can keep the Tails drive in the open and the Veracrypt in a private place. Plus Veracrypt has hidden volumes, so there is no way for an adversary to prove that a file even exists at all in the Veracrypt drive. If you are using Tails, or even Whonix, definitely looking into it.

Some other things to note, if you are using Tails in on public computers, your most dangerous threat is having others see you. I have never had to be at risk of being executed for using Tails, so learn what you should and should not do with Tails.

Chapter 6 – Whonix Basics (Gateway)

Most things that you would want to do with Whonix I would not consider basic. But something you must do the moment you get Whonix up and running is change the root and user password (instructions in chapter 7). Yet there is a point I want to make about Whonix, which is the gateway. You can use the gateway to make any VM run all its internet through Tor. Why is this useful? Say you want to learn how to hack, it would be very sloppy to have your IP address tied to everything you are doing. So you can route Kali Linux, a distro of Linux made for ethical hacking, through the gateway. The next part is going to try and teach you how to route any VM through the gateway. If you are not interested in that, then you can move on to the next part of this guide.

The gateway as designed to run only with the workstation, but we can use the gateway with any VM. So if you want to run Windows 10 with the gateway, you can do that. Qubes makes all of this fairly easy. There is a learning curve though. You need to learn how to get the IP address, gateway, and netmask from the gateway. I will teach you how to do this at the time, which may not work by the time you are reading this.

First get your virtual machine that you want to run with the gateway set up. Then shut down your VM without saving. Boot up your gateway. Then go to the setting of your VM. Afterwards go to Network. Set **attached to: internal network** then make sure the **name says Whonix**. Then boot up your VM. Once the VM is running, go to the network settings. Then go to the setting in the wired connection. Go to **IPv4** and select manual. Then type...

Address: 10.152.152.11	**Gatway: 10.152.152.10**
Netmask: 255.255.192.0	**DNS: 10.152.152.10**

If all is well, your network should connect and everything you do should be run through Tor. There is a high likely hood that something went wrong. So we can try and check if our numbers are correct for the manual IPv4 settings. Open the terminal in the gateway and type

```
user@root: ~$ sudo ifconfig
```

Then your password, if you never changed it will be **changeme**

Then look for **eth1/0: inet = gateway** **inet = DNS** **netmask = netmask**

Then the address should be on a different port than the DNS and Gateway, so if

inet = 10.152.152.X then **address = 10.152.152.Y**

Where X does not equal Y

Once you change your setting, you should now be able to run all your data through Tor on any VM.

That is all I am going to say about Whonix. Almost everything else is best if you play with the software. Whonix is something you have to get used to yourself to really learn it’s full power. Also, read the documentation that Whonix has to offer. Whonix tells you everything it can and can not do. Remember, the more you know the safer you are.

Chapter 7 – Basic Linux Commands

This is where in the guide where it no longer matters, for the most part, what version of Linux you are using. But I am going to assume you have gotten somewhat used to your new environment by now. Hopefully, you have learned how to use the internet, LibreOffice, and everything else you would normally do in Windows. But in order to fully utilize the power that Linux has to offer, you need to learn how to use the terminal. The terminal is where you will do most software installs and downloads. Also, the terminal is where you will learn to use GPG, more on that later. But before you can really get into commands, you need to have a basic understanding.

By default in Tails and Whonix, you are not a root user. That means you can not, by default, run root commands. Such as downloading, editing, or deleting files. This is for security reasons. If someone were to hack into your computer, they could take complete control and learn everything about you. But at the same time, you might want to want to download or do other things that a root user could do. So sudo user was invented in Linux.

Most power : **Root > Sudo > Normal** : Least Power

Sudo means Super User DO, which allows for a high-level user to do root commands but must type in their password each time. So for example, say you want to run updates in Tails or Whonix (I am going to assume you have set up an admin password in Tails). You can type...

```
user@host: ~$ sudo apt-get update
```

Then you will have to type in your password to run the root command. So your account is given temporary root access and is taken away after a certain amount of time or when you close the terminal. So you get both security and convince this way. Also if you are using Whonix, please update your password asap. To do so, type...

```
user@host: ~$ su
```

Default Password: changeme

Then you will be logged in as root. Here you can do all sorts of stuff, but let's change your password

```
user@root: ~# passwd user                              //changes user password
```

Type in the new password

```
user@root: ~# passwd                                   //changes to root password
```

Type in the new password

```
user@root: ~# exit                                     //exits root
```

Now you have updated your password for root and user (The default username is user).

This is not much, but it is enough to get you familiar with the terminal. Look up commands and learn how to use Linux from the terminal. Something I did was I got a VM with Ubuntu and just practiced with commands, while connected to the Whonix gateway. Tails, Whonix, and Ubuntu are all Debian based, so what you learn in one will help you in the others. I would recommend really getting used to the terminal because you will need to be familiar with it for the final chapter of this guide.

Chapter 8 – Learning how to browse Tor

You have finally gotten your computer setup and have gotten used to your new Linux environment, you are now ready to really start using Tor. Even if no one can trace you based off your IP address, they can still trace you by other means. No matter how hidden you are on the internet, if you log onto your Twitter account you are not anonymous. People will know it is you that is tweeting, regardless if they can trace you over the Tor network. You have to create a completely different identity than you use outside of Tor. You should have, at the minimum, two identities. One of those is for everyday activities, and the other is for your private business. There should never be a bridge connecting those two identities. I would recommend never logging onto any account over Tor that you did not create in Tor. You are trying to not get red flagged, remember? The definition of being anonymous is having no actions traced to an identity. But when you log onto an account that you created on Tor, you are no longer anonymous by definition. There is an identity that is correlated with that account. If you use the same name or email, which you should make sure people know you are who you say you are, then everything that identity does is correlated to one person. If you ever make a mistake, all the actions that the unknown identity did is now pointed at you. An adversary can know everything you did. The goal when using Tor is to never have the hidden identity traced back to you, similar to how bank robbers do not want people to find out they did. This idea is called pseudo-anonymity. With literally means fake-anonymity. The moment your mask is removed, they know who you are and what you were doing on Tor.

Here is the central idea when it comes to using the internet. When you are using the internet like normal; you know that people could be watching, you but assume they are not. When you are using the internet over Tor; you know that people could be watching you, *and you assume that they are.* Believe me, when I say this, there is someone logging everything that your pseudo-identity is doing on Tor, waiting to link it to you.

That is not even the worse part. Even if you do everything that you are supposed to do on Tor, you can still be traced. Things that you do not even think about can get you caught, or at least red flagged. What websites you visit at what times, how fast you type, what time do you log onto Tor, how do you type, your attitudes on certain topics, how much you know about a certain topic, and much more. This type of attack is called social engineering. Where they can try and link what you do on Tor to someone outside of Tor, and confirm it is them by following the real-life person's every move. If your real identity has an adversary's attention, they will find out what you are doing. That is the whole reason why we are were trying to avoid getting red flagged in the first place. When you visit public places to use their wifi, blend in with your environment. If you are using a college Starbucks, dress like a student or teacher. If you are at a library, were apollo or button up with blue jeans and actually read a book. Change your posture, your voices, and the way you look at people. Of course, you should be changing locations very often. The fewer people in your area, the further you should be traveling from your house. Also, make sure to buy everything in cash. Do not pay with hundred dollar bills. What am I really describing with these precautions, someone with common sense. Your goal is to stand out as least as possible. I will challenge anyone working in a public to remember someone who visits your store twice a year, especially if they are changing their posture and clothes. If there is nothing to make a person stand out, there is no reason to remember them. This is also why you want to buy a computer that you would not mind using in public, and will not turn eyes. In real life, you should be confident knowing no one is watching you because you are paranoid behind your computer screen. Also, please make sure to disable/cover up your webcam. None of this matters if your face gets plastered all over your adversary's networks. Remember what I said, always assume someone is watching you make every keystroke on Tor. As if they are watching you through your window, but as if you are wearing a mask. A truly motivated adversary will always be waiting for you to accidentally remove your mask, to slip up.

Another thing you should be doing while you using Tor is very regularly changing identities. How often really depends on what you are doing on Tor and how often. If you only buying or looking at different websites, then I would change identities every few months. If you are a vendor selling, I would recommend changing identities every year. This may seem excessive, but doing this could save your life.

Chapter 9 – Cryptocurrency (Bitcoins)

There will come a time where you want to buy or sell something, maybe on the darknet, and you do not want to be traced. Everyone has heard of bitcoins, maybe you even have invested in them yourself, but how do they work? What a bitcoin is literally, I should say digitally, is out of the scope of this paper. You are always free to do your own research about how bitcoins are generated, and why they can not just be duplicated. But, I will try and teach you how to use bitcoins.

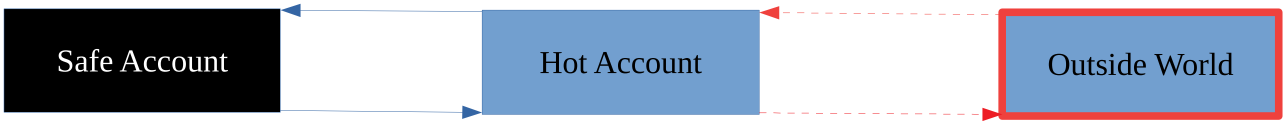
So bitcoins, similar to traditional money, is a fiat currency. It only has value because we as a society say it has value. And bitcoins are stored in a "bank" similar to how your money is also stored in a bank. But there are differences. A normal online bank is basically only good for managing your money. It moves it from point A to point B, where the money in your account relates to real life money, a physical object. Bitcoins are stored in wallets, where you do all the movement yourself. Bitcoins have no real life physical object that relates them to the real world, but they relate to a mathematical equation. So math represents bitcoins. That is why there is not an unlimited number of bitcoins because the equations to generate them are getting more complicated as more are made.

The way that bitcoins can be sent and received are through bitcoin wallets. A bitcoin wallet, like a bitcoin itself, it based off of math. So math tells blockchain, the central hub of bitcoins, how much money there is in a wallet. Unlike a regular bank, blockchain has no power over what happens to bitcoins. Blockchain is only able to view where bitcoins go. This is why you have so much control and at the same time vitality. People know that their wallets have received bitcoins from your wallet because of blockchain. So a bitcoin wallet has two different parts, the public and private address.

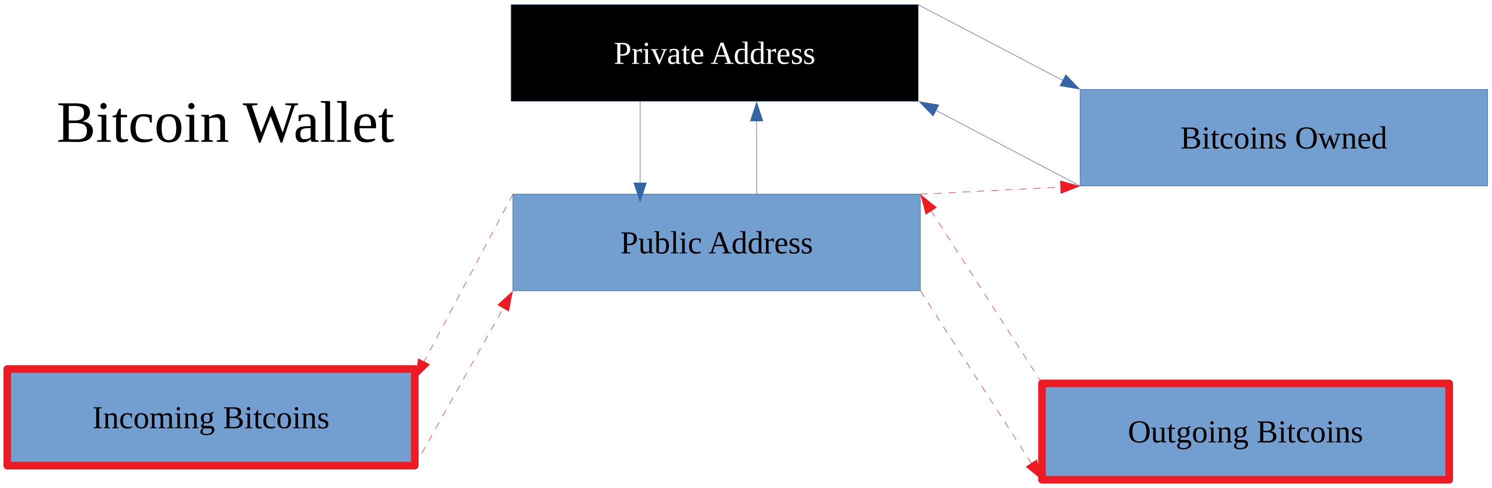
A Public address with look like: *1M9ZBp9L5iYkZVehEmNoDUkes8P67B4kR1*

Private address: *KypQgxiqpJHRAo2Fdqaccaiqd5nmkvAvd1BRfMkrNEkWtCBFsdRG*

The public address is able to receive and send bitcoins, and nothing else. While the private address has full control over all your bitcoins in the wallet. Trying to use traditional banking systems does not truly paint how bitcoin wallets work, but they can be used to try and get a vague understanding. So imagine you have two banks, just for yourself. One bank is strictly for moving money. Whenever this bank account gets money, it will physically and secretly send it to your second bank. The second bank stores all the money and can not be reached. Then when you need to send money back out, your second (and secret bank) will send the money back and your first (public bank) will send the money out.



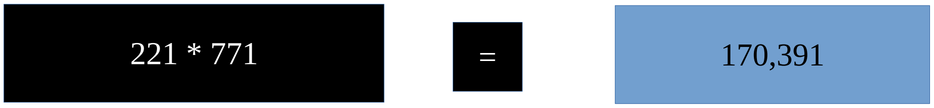
This idea is not a complete presentation of how bitcoins wallets work, but it helps to paint the idea of how the public address and private address are used in a bitcoin wallet.



Something to note, you can tell how many bitcoins are in a wallet given only the public address. So this can make certain wallets a target for adversaries.

Using bitcoin wallets has a lot of security, but can easily be compromised. If you ever lose the private address, you will lose all the money in the wallet. Because an adversary can use that address to send all your bitcoins to their own wallet. If you are wondering why you can not get the private address from the public address, it is all math related encryption using cryptography. To show you how cryptography can be used to create a link that is untraceable, listen to this question.

What two numbers multiplied together give the number 170,391? The reader would have a very hard time factoring 170,391. But, if you were given the original two numbers, you can easily multiply those together to get 170,391.



221 * 771 = 170,391

Private Address Public Address

This is grossly simplifying how cryptography works, but you can really understand why you would have a very hard time getting a public address from the private address. Yet at the same time, you can easily get the public address given only the private address. I guess by this point you are really learning how encryption works in one direction, but not the other.

If you are wondering how you get a bitcoin wallet set up, there are two different "types" of bitcoin wallets. You have hot and cold storages. There are many different definitions out there for what is defined as "hot" and "cold", with some even creating the term "warm wallet". In my mind, there are better words to use, "liquid" and "frozen" wallets. A liquid wallet is one that is connected to the internet. This could be an app or program that helps manage your bitcoins. Liquid wallets have their benefits, you can easily remove and add funds to them. Also, they tend to be simple. You do not have to worry about a private address at all with liquid wallets, only your public address. You tell the program where to send the bitcoins, and it does all the hard work for you. Then when someone sends you money to your public address, it gets added to your total. Frozen wallets are much more secure than liquid wallets. Cold wallets are to be made offline and keep offline. Think of your frozen wallet as the spot under your mattress, and your liquid wallet as your bank.

The drawback form a hot wallet is that since it is connected to the internet, there is a trail for an adversary to follow and find a way to steal your bitcoins or trace them to you. There is no such thing as “hacker proof”, believe me on this one. But there are different risk levels with hot wallets. Some factors are: how much money you are keeping on it, what service(s) is(are) running the wallet, what do you buy with the bitcoins, and where do you get bitcoins from are some. Your risk level could be really low or really high depending on the answer.

The downside with frozen wallets is their lack of mobility. You can create a cold wallet on a website such as www.bitcoinaddress.org using the brain wallet while offline, using a Live OS file, and then shutting down your computer without connecting to wifi again. This way the wallet is not stored on your computer nor found anywhere on the internet. A brain wallet is a bitcoin wallet that is generated using keystrokes that are human-made and converting that in the wallet using a hash algorithm. So, in theory, an adversary could try and brute force wallets with weak "passcodes". You do not have to remember or write down the passcode, it is only used to generate the wallet. So you should make the passphrase really, really long. Do not worry about making it so you can see the passphrase, you will not be connected nor connecting to the internet. This means no adversary can know that you ever created the wallet.

When you are generating the passphrase, the amounts of characters on this page is a little bit short. Just use random letters and character for 5 minutes, and you will be fine. Then write down your public and private address. You want there to be no link to the internet and this wallet. Well, you do not want a link for the private address. When you write down your wallet, make sure you can tell the difference between your characters. For example, be able to tell difference between 0/O, b/6. g/q, I/l, etc. The last thing you want is to try and withdraw your funds, and not be able to re-type the private address. Bitaddress has an option to test your private address, so use this to make sure you wrote down your address correctly while you are offline. If it is not clear yet, it is always better to be safe rather than sorry. When it comes to moving funds into and out of frozen wallets, that is covered in the next chapter.

Everything I have said about bitcoins has been very broad. You should be doing your own research to find out more. Bitcoins will play a large part in staying anonymous, it is important you understand how to use them. If what I used to represent bitcoins does not make sense to you, find an article that does a better job than me for you. I am going to say again, make sure you really understand how bitcoins work. Even if you do not understand how anything else works in this guide, but you are following instructions, make a valid effort to understand bitcoins. If you do not, the next part of the guide will make no sense.

Chapter 10 – Buying Anonymously

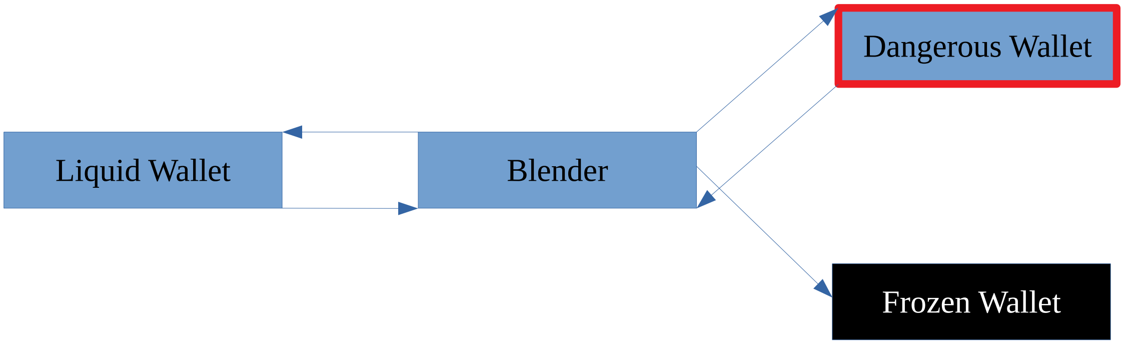
Let's imagine a scene. You are a politician and you want to get rid of the competition. You do not want to get your hands dirty, so you send guns and drugs to their house hoping to get them arrested. Even after the packages make it to their house, you still see your competitor on the news making speeches. So you leave an anonymous message to an adversary ratting out your competitor with detailed information. The next day, however, you see that they are still making speeches. How could this be?

There are laws in place from you being incriminated from someone else sending you illegal items. If you never bought the items that came to you, why should you go to jail? That is the very first point I am going to make. If there is no way to prove that you bought what came to your house, then you can not go to jail for it. So even if an adversary comes knocking on your front door and begins to question you about a package. Do not confess no matter what they might tell you. It is not your job to prove your innocence, it is their job to prove you guilty. If you decide to buy something of a questionable nature, it is very important that you buy it in a way that can not be traced to you. Even if you try to deny you bought a package, if an adversary can prove that you did then you have no plausible deniability.

If you remember from chapter 9, there was something that I mentioned that was cause for concern about bitcoins, blockchain. Blockchain is not the only service that tracks and monitors where bitcoins go, but for the purposes of this paper, it is the only one that matters. Almost all adversaries use blockchain to track bitcoins because there is nothing that other services offer that blockchain does not offer. Plus blockchain has a very large user base for its own hot bitcoin wallets. So back to the question at hand, how can bitcoins be anonymous if an adversary is able to view exactly where all bitcoins go? There are a few different ways to fix this issue. Option 1, get bitcoins in a way that does not leave any traces to you. Option 2, use bitcoin blenders to mix your coins with other people's coins to make tracking very hard. Option 3, use option 1 and option 2 at the same time. Guess what we are going to talk about, option 3.

So how can you get bitcoins in a way that does not link those bitcoins to you? Well, there are some websites, such as localbitcoins, where you can buy bitcoins using cash or gift cards. I do not find this step to be super important. As long as you do not buy bitcoins with your credit card, then however you want to get them is up to you.

So once you have your bitcoins, there is a reality that you will have to face. There is some trace between you and the bitcoins you bought. Even if you got bitcoins in a way that there no way to trace you, you do not want to take chances. Say you have found a marketplace that you do not want people knowing that you are buying from. Marketplaces have their own built-in liquid wallets that you send your bitcoins from and to buy things. So you keep your bitcoins clean, we can “laundry” them similar to how the Mafia laundry’s their money. There are hidden services, .onion websites, that are blenders that mix your bitcoins. So first you send you bitcoins to the blender, the blender "mixes" your coins with other people's bitcoins, then sends the desired amount to the target wallet.



This way there should be no link between you and the marketplace wallet. Also, this is how we are going to send funds to our frozen wallet that you made earlier. If you have funds that you do not want to be compromised, use a blender to keep your identity away from the frozen wallet. Once you are ready to move funds out of you frozen wallet, most liquid wallets provide a way to sweep fund from a wallet given the private address. This is why we want to keep our private address safe.

Even though blenders are a beautiful thing, there is still a level of trust that needed with blenders, also known as tumblers,

If you do buy something of questionable legality, make sure you can have plausible deniability. Do not ship to an abandoned house where you have no explanation for being there. Also do not look too eager to get a package. Where you ship your goods, I would recommend your house of postal box, ship other items there too. Buy things off of Amazon or eBay. Make this package look like any other package. So if an adversary were to question you, you have the ability to say you thought it was another package that was supposed to come. Have good reasons for why you are doing what you are doing. Even if the adversaries do not believe you, do not confess. Assuming you followed the steps above, there is no way to prove you bought the package. You may be in an interrogation room for 8-12 hours, but that is a short time compared to 10-20 years behind bars.

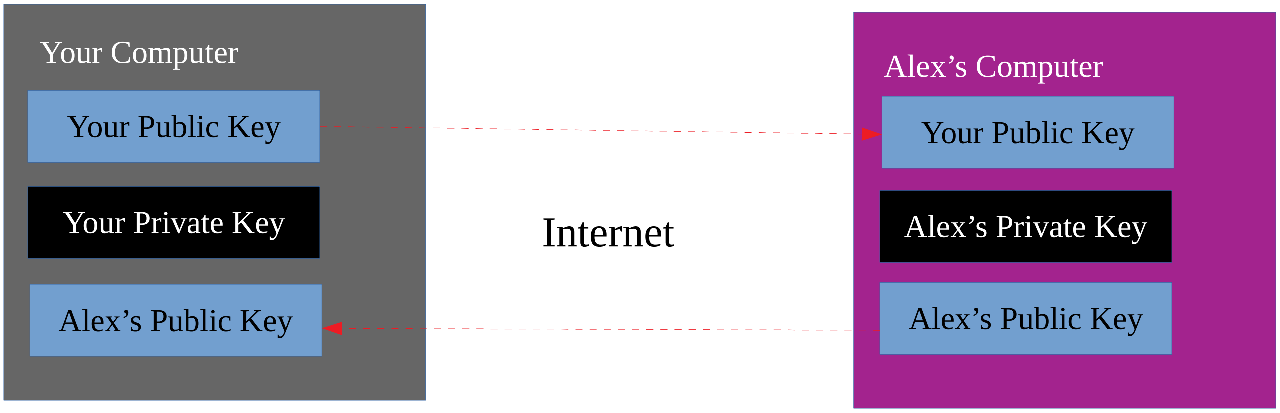
Chapter 11 – Communication (PGP + GnuPG)

This is the longest chapter in this guide, and the most useful part in everyday life. If you learn how to use GPG, you will be gaining a skill that is irreplaceable.

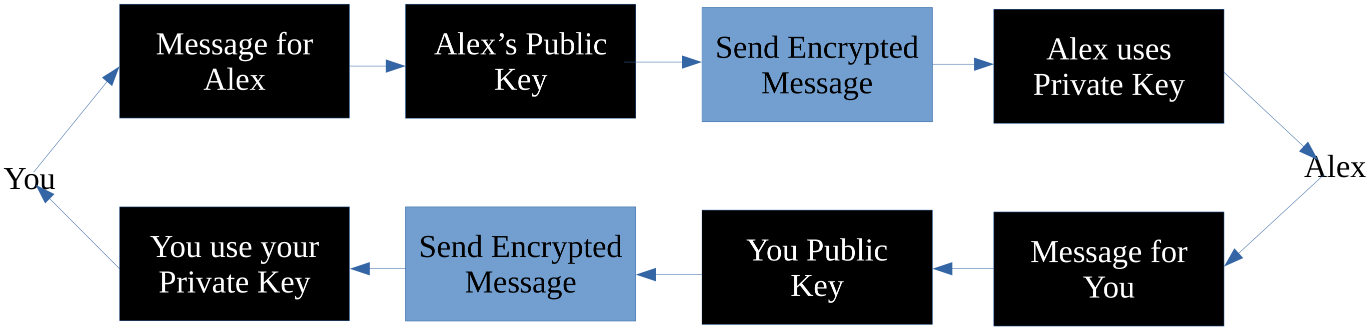
Say you have some sensitive information that you need to send over a dangerous area. This could mean you have a king send a messenger to give a message to another king. Before the messenger sends the message, the kings discuss of an encryption strategy. Every letter in the message is to be rotated four letters down the alphabet. So now a=d, b=e, c=f, d=g, e=h, etc. So to the messenger, the message just looks like a jumbled mess. This would also be true to an adversary who would take the message away from the messenger. The adversary would have no idea what the message was saying. In terms of today, this is very weak cryptography. We have much stronger encryption today than the days where kings sent messages across the battlefield. But there is a key flaw in this type of encryption. It is assuming that both the receiver and sender both know how to decrypt the message before the message gets sent. The way to decrypt the message, the key, can not be sent along with the message. Then the adversary could use the key to “unlock” the message. This is where PGP comes into play.

Some very smart person invented PGP, pretty good privacy. Things are going to get complicated, so buckle up. So imagine that you have two separate keys, public key, and private key. Similar to how bitcoin address, one of the keys is to be public and the other is to be private. You send your public key out to everyone who you want to communicate with, and you always keep your private key to yourself. You use your private key to decrypt the messages sent to you. To message people back, you use their public key to encrypt the message, then they use their private key to decrypt the message. So both people have two keys and only share one. If this sounds confusing, that is okay. I will try to paint a better picture for you. If you are not understanding, keep reading and try reading other guides. Once the idea clicks, it will all make sense.

So you and Alex want to share sensitive information. You and Alex both have a public and private key. You exchange public keys in the open air. So now you have Alex's public key, and Alex has your private key.



So now Alex can encrypt messages using your public key on his computer. Then sends you the encrypted message over the internet. Then you receive this encrypted text. If you were to try and read the text without decrypting it, the message would like random letters and numbers that no human or computer could understand. Since you have your private key, you can use that to decrypt the message. Since you are the only one with the private key, you are the only one that can decrypt the message. Then you want to send Alex a message back, you can encrypt your message using Alex's public key. No matter who gets a hold of this message, only Alex will be able to read it since he is the one with the private that can decrypt the message. This is a cycle that gets repeated for every message that gets sent. While it may seem tedious to send messages back and forth this way, it is necessary to take such precautions. Here is the flow of how messages are sent using PGP.



This same idea is how HTTPS works. The S in HTTPS stands for secure. That is why people suggest you always use HTTPS rather than HTTP. Even if someone is intercepting your data while you have HTTPS active, they will not be able to understand it. Tor browser has HTTPS everywhere enabled by default, so you should not have to worry about this.

The program that is used mainly for sending and receiving messages is GnuPG, shortened to GPG. GPG is installed in almost all Linux distros, including Tails and Whonix. It is important that you understand the fundamental ideas behind PGP before you jump into using the commands for GPG. If you do not understand how PGP works, then read other guides. If you want to try GPG before fully understanding how PGP works, understand that you might get very frustrated.

For you to use GPG from the command line in Linux, you need to have some basic experience with the command line. I am going to mimic what the Whonix command line looks like, but the commands are the same for most Linux distros. To generate a new key pair, both public and private. Type in

```
user@root: ~$ gpg --full-gen-key
```

This creates a window for you to follow. You will have to option to create different types of key, select RSA and RSA (Default) until you learn more. Then type the max amount of bits for sercurity length. 3072 is good enough for most people, but you know. Then set the key to expire at some point in the future. Make is so everytime the key expires, you create a new identity (Remember chapter 8?). I would recommend three to four months for most people unless you are a vendor. By the way; 1y = one year, 3m = three months, etc. Once you create the key, you should create a revocation certificate. You can do research for that elsewhere since that does not relate to anonymity. You do not have to use any real information for a GPG key to be generated. You do not even need a vaild email address. But, it is recommended you use information that matches your puesdo-idenity. A big part of GPG is trust, someone can easily fake being someone else. So, put information that matches your pseudo-identity, but obviously not your real identity. Then make a really strong password that you can remember. You will need it to sign and decrypt messages. Then your key pair should be generated.

Your fingerprint gets printed out after your key pair is generated, but this is not your public key. People can use this fingerprint to look up your public key if you submit your public key to a database. To actually print out your public key that will send to people from the created key pair, type...

```
user@host: ~$ gpg --export --armor [user]
```

Where user means: Name, email, or fingerprint correlated with key

Armor means: Human language

It is important to use armor, because if not GPG will print out a string of code that can not be used for anything practical.

This is the key that you can send out in the open air. I mostly communicate with people over email, you can send this as the first message to someone. Say someone gives you their public key, you can import it by using...

```
user@root: ~$ gpg --import
```

Then paste the public key into the terminal. Once pasted, leave a blank line, then press ctrl+d to exit back into the terminal.

By this point, you have your public key, your private key, and the other person's public key (Let's call them Alex). Ales has his private key, his public key, and your public key. To send Alex a message, you need a message to send. To create a message, you can open LibreOffice and type your message there. Or you can do type it from the terminal. If you want to save the message, use...

```
user@host: ~$ nano [filename]
```

Then type your text, afterward use crtl+x to exit, y to save, enter to exit back to the terminal. To encrypt the message that you just wrote, type...

```
user@host: ~$ gpg --encrypt --armor [filename]
```

You will be asked to choose recipient(s). Type the name, email, or fingerprint that belongs to Alex's public key. Afterward, a new file is created with the same name of the old file but has .asc subfix. To read the message, type...

```
user@host: ~$ ls
```

This will show all the files in your current directory

```
user@host: ~$ cat [filename with .asc]
```

Copy the cat output, this is what you will send to Alex. You can send this encrypted message to Alex by whatever means, but I always recommend using email.

If you do not want to save the file, you do that easily. Just type...

```
user@host: ~$ gpg --encrypt --armor
```

Then choose your recipient(s), and press ctrl+d when done. Copy and paste the output to send to Alex.

Something that to understand is you will not be able to check if the message was created correctly. Since you encrypted the messages using Alex's public key, you would need Alex's private key to decrypt it. Since only Alex has the private key, hopefully, then no one else can decrypt the message.

Once Alex reads your message, he can encrypt his own message using your public key. Once you get the encrypted text, type...

```
user@host: ~$ gpg --decrypt
```

Paste the encrypted message, then your password that you made earlier. Then the clear text will print, and you ready to create a new message for Alex.

Those are the basics of GPG. Once you understand how to use these commands, you can do research to learn what else GPG has to offer. GPG can be used for verifying signatures and creating your own signatures. By the way, once you learn how to verify signatures, I would recommend reinstalling everything you have downloaded. You would not want any backdoors installed on your software before you go and do important private business.

Now, you know how to send encrypted messages and receive them, but where do you send them to and from? You could in theory use Gmail, but that is risky. I would suggest setting up at least two different emails. One of your emails is created in the clearnet, and the other on a hidden service. If you need an email to verify you are human for another email, use temporary email services. You want no strings attached to you when you create this email. Learn how to create an anonymous email, I would recommend TorBox's (squirrel mail) hidden service.

Epilogue

You have learned a lot, assuming you have followed this guide. But, this is only a guide, you have to do all the work and learn. The life where a mask is needed to live is not an easy one. As time progresses, you never know who is watching. So if your life becomes at risk, you now have the tools to stay safe. A point I have made throughout this whole paper is, do not make yourself a target. As long as you do that, your privacy can come easy. But one wrong step, your whole life can come crashing down. Keep your eyes open at all times, and have good common sense. Learn what works and what does not work. By the time you read this, there might be some things that no longer help keep you anonymous. If you do these things, you will be fine. Good luck.