hackmd.io /YKjhguQES_KeKYs-v1YC1w

Untitled - HackMD

22-28 minutes

> How to stay anon
> This is a collaborative document, just add anything you feel like it's missing or improve the current advice. Editing is open to everyone.

Operations

Spend some time to come up with an online person be what you will be recognized as and remembered by as anon anon (preferably something to do with anime)

- The best would be to use a completely different phone and computer for each identity
- If you can't use a different computer, you probably are ngmi. Instead, try using a different user account for your anon identity, as it makes your time trying to remain anon short; then you can try again and ,take account separation more seriously the next time.
    - If you can't afford a new computer you might be able to buy a new SSD to boot a clean OS with a new nym, but then you'd have to physically swap out the SSDs** every time you want to do something on one identity or another
    - Question: is dual booting safe enough, anon? Currently dual booting Ubuntu and Arch (Arch for the pseudonym). Good enough opsec?

1.
    - If you are using browsers to separate accounts, you probably are ngmi. Be careful when opening links from anywhere other than the1 browser since they'll open it with your default browser, and if that's your non-anon one you could easily doxx yourself.
    - or don't login to your default browser with anything ever and make it forget everything every time it's opened or closed so that when you accidently open it it's not linked to any accounts

- If you are a sweat lord, a separate virtual machine per k identity can also work. Look into Qubes and/or Whonix if you're a true tryhard.
- Set up your anon browser as the default then immediately doxx yourself. You didn't listen the first two times when we said to take account separation seriously. Start over.
- Copy and paste discord invite links, if you just click join you might doxx yourself by joining with the wrong d
- Be careful about Bluetooth headphones and system-level usernames - if you're screensharing the names of these devices / accounts can doxx you.
- Be careful sharing screenshots of your desktop/ dev environment, especially if not on a seperate computer/vm. User profile names in the terminal, thumbnails of images, folder names etc can give info.
- Also applies when sharing your screen on a call, avoid that at all costs.
- Remove EXIF data from any images/screenshots you post. Some websites automatically remove EXIF data for you when you upload an image, but others like Discord don't. https://www.verexif.com/en/ works well for this. (should recommend a local solution imo)
- (NB: unclear if Discord does not - from a support tix it looks like photo exif is removed but video is not)
- Alternatively, don't upload images, just grab a screenshot of your image then paste it
- When setting up your anon accounts for the first time, don't follow friends/small accounts initially, it's possible to sort someones followed by date and if the first few were all small accounts it's likely main account follows them as well, reduces anonymity set.
- Use a VPN or Tor to mask your IP (you can ge VPN included with a protonmail account). If you are going the virtual machine route, set up your VMs to route network connections via Whonix

Gateway.
- Some tracking scripts use system-level properties/ such as fonts installed or screen size to identify you across sessions, linking your identities. Test how unique is your footprint through EFF's**** website and minimize it by either using brave, installing privacy extensions such as Privacy Badger or disabling javascript. Brave browser, unlike firefox, does a decent job at spoofing finger
- Don't share links with yourself by DMing or emailing between your anon and IRL accounts.
- Understand what your threat level is: are you trying to stay anon from the government or friends and family?
  - https://privacyguides.org/threat-modeling/

Friends

- going anon may be a lonely journey at start, but once you leak a few alpha or make some good memes to prove worthiness, you'll be very welcomed to most communities
- Have no friends, it's safer that way
- Friends dont doxx friends
  - except for when they do
  - no one is going to go to jail for you

Speech

- Speech to text to speech is the way to go
- You probably have some speech patterns and vocabulary that are unique to you. Try to avoid these, and replace them with sormething else. Write as simply and generically as possible.
- You can also go the paranoid route and completely change your speech like @AnteBear
- This also includes the emojis you use, try to change them since these tend to be quite personal. You can fuzz your timezone, but humor is associated to culture, so be aware of the jokes you do on the public domain.

Funds

- Send all money through Tornado Cash or monero before sending it to your anon account
- Tornado cash tracks time difference between deposit and withdrawal on each note separately, but actually all the notes are in the same anonymity pool, so you should treat them all the same. Avoid behaviours like depositing a new note and withdrawing another o^{8}ne at the same time, Tornado's app will say everything is ok since the other note was deposited a long time ago, but actually it's like depositing a note and immediately withdrawing it.
- When sending through tornado cash wait some time between each operation to make sure it's not easy to link them through temporal proximity
- Use a different seed for your anon crypto addresses, you likely have bigger things to worry about if your seed gets leaked but if your keys are** generated from same seed they are linked, even if not reversibly.
- OPTIONAL: To avoid relying 100% on only one service and for extra privacy, your tokens can be transferred to another chain such as Monero and then back to your desired chain to further break the link between source and destination.
- when transfering between chains switch service each way (if you go to monero with simpleswap go back with changenow)

Timezone

- It's really hard to properly hide your timezone since it leaks through the time when you are active (interact with people on twitter, make commits, respond to messages).
- You can try to switch that up by changing your sleep patterns but then the anonymity set becomes even smaller so I'm not sure if that's an improvement.

- I've given up on fuilly masking it but I try keep some ambiguity between the timezones around me and avoid making it really easy to guess.
- Schedule everything in UTC or GMT, as both are international standards and avoid doxxing location to any specific zone.
- When people ask me for my timezone to schedule a call I give them a random timezone that's somewhat close to me and then pick an hour that works for my timezone.
- Be careful when posting screenshots of chats (eg: discord) since these include timestamps in your local time, which allow anyone to find out your timezone.
- Websites can also get your timezone through your browser. If you live in a unique timezone, this can narrow down who you are. If you're paranoid, just change your computer time zone and use a physical clock to track the time. (This can be a suprising amount of work, since it means you might end up with Daylight Savings kicking on and off at unexpected times, and it can even affect default lang and what packages your computer tries to download, though.)
- If you are working outside your chosen timezone on code, you can still commit it by adjusting both the `GIT_COMMITTER_DATE` and `GIT_AUTHOR_DATE`
- Choosing a timezone for your identity gives you a way to timebox your work. If it happens that you want to work off your timezone, like its some unhealthy hour of the day, don't open: Twitter, Discord, Slack, or any chat application.
- Disable autostarting apps so you don't show up when you shouldn't be showing up
- Some tweets can be scheduled instead of posted right away. You can schedule tweets during the night to create confusion about your timezone.

Calls/voice

- Eventually you will want to go on calls because you might be missing opportunities such as:
  - A podcast asks you to join
  - Everyone is on a call and you want to join too
  - People keep asking you to call them
- The solution here is to use a voice anonymizer.
  - Windows - Voicemod

  Note:

- I spent a lot of time trying to get voice anonymizers working on linux, and the gist of it is that they are a pain in the ass to setup (I had to tweak alsa to get them to work) and they are all variations of a pitch changer, which doesn't anonymize your voice that well sinceno it just changes the pitch.
- After trying a lot of things I gave up and started using voicemod on a Windows virtual machine,I suggest you do the same.

  Warning:

- If you are not masking your IP be careful around call software that establishes P2P connections, those leak your IP to other people on the call.

Vtuber

- For those not familiar with it, this is an animated avatar that you can use to replace your video feed on calls

  Image Not Showing Possible Reasons

  - The image file may be corrupted
  - The server hosting the image is unavailable
  - The image path is incorrect
  - The image format is not supported

  Learn More →

- It's not needed at all since you can just turn video off but the upside is that:
    - Its fun
    - Hand gestures and facial expressions are critical to social bonding, vtubers solves this without doxing
    - Other people love it
    - It's awkward when you have to explain that you can't turn video on because you are anon
    - Alternatively, you can just say your webcam broke or something. Lying goes a long way in hiding your identity.

  Warning:

- Make sure your webcam is active for face tracking to work, so if something goes wrong you may dox yourself completely, thus the risk is much higher compared to having no video.
- You can comission an artist to make a custom model for around 50$, but you can also get free models online.
- I suggest using a native Windows machine for this, since:
    - all the programs for vtubing are windows-only, I've managed to run one of them on wine but running it inside a VM is a pain since it's too slow and getting the webcam to work is hard
    - My voice software is windows-only
    - I only managed to get hand tracking working on windows
    - The software I use is VSeeFace. I also bought a LeapMotion device for hand tracking. hi

Vtubing on linux

- I did manage to get my vtuber set-up running on linux after a lot of tinkering, but ended up switching to a windows computer at the end, which is what I would if if I were to start again.
- Still, if you want to get it running on linux here are the instructions:
    - Get VSeeFace running inside wine.
    - There's some instructions for this on vseeface's website but expect to do some tinkering.
    - Use Lutris to avoid extra tinkering with wine. You might find some instructions telling you to run a python program outside wine for the face recognition but you can ignore that since the latest versions of wine handle webcams properly.
    - Use OBS to create a fake webcam and redirect VSeeFace's output into it. You will need to change some kernel modules 6 yto get OBS' fake webcam feature to work.
    - Set the call software you are using to pull video from OBS' fake webcam
    - With this I managed to get it working, but I never managed to get LeapMotion hand tracking to work on linux.

Github

- You can and should spoof your commit details and time
- If you have a doxxed github set up a bot that creates some commits on it. Otherwise it may be possible to connect identities by linking anon and doxxed github activity graphs (you'd see an activity graph that suddenly had a drop in activity and another account that had a spike at the same time)
- When using a different github account remember to also change your git and email locally. You can set this at the per-repo level to avoid having to keep changing identities, run this script inside the repo to set it:

```
git config user.email "0xngmi@protonmail.com"
git config user.name "0xngmi"
```

- To avoid having to constantly change github accounts you can set different ssh connections to github, each associated with a different account, and link them with each repo.

  You should really change github accounts. Have a different account for every activity. Remember that GitHub is owned by Microsoft.

- To do this you'll need to add the following lines to `~/.ssh/config`:

```
Host github.com-ngmi
        HostName github.com
        User git
        IdentityFile ~/.fssh/id_ed25519_ngmi
        IdentitiesOnly yes
```

- Then modify the file `.git/config` within your repo to set its remote through the new s

```
[remote "origin"]
        url = git@github.com-ngmi:DefiLlama/DefiLlama-Adapters.git
```

Avoid repeating code patterns

- You might come across problems that you've already solved before and ight be tempting to copy code youp've [7]previously written but it's important to avoid that.
- Even if you avoid copying code it's easy to repeat the code patterns you've used before. Avoid that by using libraries you haven't used before or structuring solutions in new ways.
- Pick the most mainstream libraries available to maximize the anonimity set.

Email

- For email while you can run your own email server, that will most likely lead to more problems (another device another network to secure etc). Using something like ProtonMail can be a viable alternative, although avoid using their web frontend for it as it has been comprimised in the past.

Phone

–If use Android, best to use an unlocked Pixel device & install GrapheneOS, and install Fdroid (no Gapps Google Apps)

- It's really easy to make mistakes with the account separation options available on phones.
- For example, it's easy to send a telegram message from a different account, especially when you contact a person for the first time.
- When adding somebody as a contact in Telegram, the default is to share your phone number, double check you are not sharing this before you add a new contact.
- You can do that through Settings>Privacy and Security>Set Phone number to "Nobody".
- Get a second phone and use that to separate identities across phones.
- If you don't want a second phone and you use android you can use an app called Island to set up a second workspace and replicate all your apps, then you can separate your identities across workspaces. This lets you have two discords, each with it's own account.
- Another phone is recommended, even if you only use the second phone for Two-Factor Authentication purposes (to avoid SIM-swap attacks or other compromises)

- Be careful when opening links since these could be opened under the incorrect app. Be especially careful around joining discord servers, since when you click on the invite link discord doesn't show you which account you are on until you've entered the server, so if the link was opened under your other account you'll be doxxed.
- There are multiple services that let you pay bitcoin in exchange for a phone number, on which you can see the SMS received. However, this is risky since phone access makes it possible to steal your account and these services tend to be shady.
  - https://mysudo.com/.
  - https://www.smspool.net (Suggested for services that require non-VoIP phone numbers)
  - https://juicysms.com
  - https://silent.link/ can pay with Lightning
  - https://sms4sats.com/ can pay with Lightning

  Note: Use monero over bitcoin (if it is an option), you can check privacy rating for a btc tx at blockchair to see what behaviors reduce privacy

OS

From most private to least private desktop OSs:

1. Tails OS
2. Privacy focused Linux distros (Qubes, Whonix etc)
3. Desktop Linux distros (Arch, Ubuntu, Gentoo, Fedora etc)
4. Mac
5. Windows

Browser

- Use Firefox (or Tor Onion Browser) with the most strict security settings, and HTTPS only mode
- reduce the amount of extensions you use

Hardware

- Both Intel and AMD processors contain a hardware backdoor. For Intel, it is the Management Engine (ME), and for AMD it is the Platform Security Processor (PSP). More information can be found here.
- For a fully secure, modern computer without any backdoors, your only options are the Talos II and Blackbird by Raptor Computing. Link to both are provided below. Please note that they use a different computer architecture than Intel or AMD cpus, so make sure your OS is supported.
  - Talos II
  - Blackbird

Email

- Use Tutanota. There is no second best.
- Mailfence is another good private email provider. Easy to make multiple accounts if you have a private email to add to this one.
- Protonmail is another option, but they have a history for bending over to feds

Usernames

- Uses a word list & random number generator to create usernames that cannot be easily associated.
- There is no repetition, so you cannot influence the results according to your personal preferences.

- Unless you want to build your brand as an anonymous person, be careful not to use the same username on different sites.
- Always double-check your account settings to make sure they match the degree of privacy you want to provide to the threat model.o

Discord Nitro

- Send someone crypto in exchange for gifting you discord nitro.

Buying Stuff

- https://coincards.com/
- https://www.bitrefill.com/

VPN

- Mullvad (forget NordVPN). Your account is a number. Thats it. No email or password. Allows payment using XMR.
- IVPN also uses account numbers without any other data. Has kill switches. Can pay with XMR or crypto.
    - https://www.ivpn.net/privacy-guides/
- ProtonVPN app has a kill switch feature which is very handy when in a VM
    - App is useless on Linux if you don't use systemd, not fun to setup yourself
    - Proton has a history of cooperating with narcs (source), so it's advised to only use it behind Tor

Twitter

- At some point they'll want both email and phone verification. The phone number needs to be one you can use to verify in the future too. Using a US IP and a freshly created gmail, you can register for googleVoice by linking a phone number to your google account. Here's a good place for single-use non-VoIP phone numbers (to link to your google acct so you can get a gVoice number) and you can pay with crypto. Or just purchase a SIM instead of getting tracked by the chocolate factory in addition to Twitter.
- Don't DM yourself links or tweets between accounts.
- If possible, avoid logging in to your anon account and personal one in the same browser.
- Twitter logs the IP you used when you created your account, so be sure to use VPN

  [reference link]

Domain names

- Ensure your domains have the whois records set to private, and check before you publicise any websites.
- Provide fake information when registering a domain name, usually only the email is checked.
- Set your fake information as the default in your account if you register multiple domains.
- If you use Cloudflare, make sure to use separate accounts. Domains under the same account can be linked together.
- good host for obtaining domains anonymously with crypto would be njal.la

Real life

- It's important to avoid doxxing your anon identity to real life people.

Some suggestions from that discussion include the kipfollowing:

- Create a fake job for yourself and stick to that story
- Tell them that you are a freelancer, this allows you to be very vague about what you do exactly
- Tell them that you have a very boring job, such as accountant, so they won't ask for more info
- Say you are unemployed
- Backstories that don't match your lifestyle/means draw more attention to yourself, best to not have people thinking you're a drug dealer and looking into you for that reason

Tor vs. VPN

If you want to be hidden from most, you are probably fine with just VPN & nkkot doxxing yourself publicly. If you want to be hidden from everyone, including national governments, you're going to need to route all of your traffic through Tor and not connect your pseudo to any real-world stuff (e.g., even burner pre-paid phone is risky because all phones send their locations to local cell towers). Be forewarned that while the second category is doable, especially using Whonix or a combination of Qubes/Whonix, it's harder. Examples of why include:

- You will need a beefier computer than otherwise bcuz virtualization
- A few sites will completely block you, and many more will either ocasionally break (sometimes YouTube blocks you) or slow you down (you need to log into every site you need on bootup, lots of CAPTCHAs, sites will flag you as suspicious).

1. - Signing up for Discord & Telegram is hard, since both require a phone number (Discord doesn't allow burners) and you can't sign up for Telegram from Desktop bottom

- The best alternative here seems to be purchasing these accounts online (there are forums if you google) with Monero, but this can be risky because they might be able to get into your account later.

Other resources

- https://www.whonix.org/wiki/DoNot
- https://privacytools.io/
- https://bitcoiner.guide/toolkit/
- https://x21.tools/g
- /d/opsec
    - use https://dark.fail/ if you don't know how to get to Dread
- Privacy preserving front-ends minimize tracking and bypass shadowbans.
    - https://github.com/SimonBrazell/privacy-redirect makes it easy
- Consider using Tails Linux distro on a Live USB if using TOR. Tails on a live USB can be booted to separately from your computer's main OS, but will share the same hardware. By default Tails is non-persistent (erases all files and data on each shutdown), all network traffic is routed through TOR, and the OS has a built-in MAC address changer to spoof your hardware MAC addresses. Check out the distro here: https://tails.boum.org/
- check for alternatives to your closed source application and services via https://prism-break.org/en
- there is nothing wrong with being pseudonymous either, there are probably more pseudonymous CT accounts than fully anonymous ones
- No copy pasta from accounts you graviate towards
- Get a sense of OPSEC For Hackers from thegrugq http://www.youtube.com/watch?v=9XaYdCdwiWU
- use layers of defense, trust no one. I keep my thoughts in a custom built laptop that has no physical wifi card connected to it. Recently I even reconnected it to a cheaper monitor. Remember there are keyloggers as well. i then keep my sensitive sites on a rather secure linux machine with normal defenses.

    To other anons: Just add more sections if you feel like something is missing

Q&A

---

q: can tails reasonably be used as a dev of big project? would love more commen4tary/resources

- it is possible but quite a lot of work to set up securely
- when you use tails, it's distinctive, so services can know you're not just a tor user but a tails user, which can decrease your anonymity set and create a different threat model: in many places you will be the only person connecting to tails on the network or area, while tor itself (without tails) generally have 4-5 figures of concurrently active nodes
- one drawback is all packages must get reinstalled on each restart
- using tails to communicate is ok: you can get email text twitter working without much fuss
- it''s annoying to install any modern ide with plugins and configure things each time they do a major version update: if you can be comfortable on vim/emacs, easier

q: what are some recommendations for privacy-oriented hardware (laptop)?

- Purism Librem 14
  - Open source BIOS and bootloader (coreboot and SeaBIOS)
  - Hardware killswitches
  - Ships with Intel ME neutralized and disabled
  - Can buy with XMR or other crypto
- Framework Laptop
  - Open source hardware
  - Fully modular
- Any laptop that you can install libreboot on. Check supported list here.

q: do you think if you're already a known personality on CT, have done podcasts so your speaking patterns are linked, etc. is it impossible to do voice calls as an anon? would like help modeling this. it is not clear to me if commercial voice changer software is viable for these individuals. only works if you start as a relative unknown and don't ever link your voice to irl id.au

q: places to buy crypto anonymously?

- localmonero.com
- [bisq.network](https://bisq.nein betwork)
- The best way ygmi is by making a solid connection on your Crypto path.

..