“Fuck the Feds” Security Guide v2.0

Why?

The first rendition of this document did not contain a very comprehensive approach to online security and anti-surveillance measures. v2 aims to have a more in-depth approach.

This guide is still a response to surveillance and coordinated stalking efforts by three letter organizations.

Through this guide, you will learn strategies to mitigate attempts at surveillance and learn security practices to keep your data and personal information safe.

Clearing Misconceptions:

I did not write the original “Fuck The Feds” Security Guide v1.0, I am simply adding improvements, as well as now keeping fuckthefeds.pro alive and developing it.

Who is this for?

Much like the author of v1, I have been a target of doxxing and cyberstalking efforts by a large group of people on the internet.

This document can be used by people in a similar situation or also just people that want to learn about online security or improve their security and protect themselves from mass surveillance.

As goes with the nature of this document, you are free to share this document in its original or edited form with whoever you want.

Happy reading!

Contents:

DISCLAIMER: I AM NOT AT ALL LIABLE FOR POSSIBLE CRIMES COMMITTED BY INDIVIDUALS USING THIS GUIDE. THIS GUIDE IS NOT MEANT TO ENCOURAGE CYBERCRIME OR EVASION OF LAW ENFORCEMENT. USE AT YOUR OWN RISK.

Digital Security

Final Remarks:

Law Enforcement In North America

In the worst-case scenario, if you do anything questionable online and get caught (or it is presumed that you committed a crime), you will have to deal with Law Enforcement. This section is written with ONLY North American Law Enforcement and regulations in mind.

Questioning or interrogation:

In North America, you have the right to refuse to speak to Law Enforcement (Under the 5th amendment in the United States, or Section 13 and 11(c) of the Canadian Charter of Rights and Freedoms in Canada), and the best option is for you to use it, as if you try to talk your way out of the situation (whether you are innocent or guilty), the interrogating officer(s) will only help you dig yourself deeper.

There is a common misconception that everything an Officer says must be fact, and that Law Enforcement cannot lie due to policy, but this is absolutely NOT TRUE. Law Enforcement's one job is to create a case against you, and providing them with more information will only benefit THEIR CASE AGAINST YOU, and NOT prove your innocence.

It is recommended that you ask to speak to a lawyer, and after that invoke your right to silence. Your lawyer will handle it from there, and Law Enforcement will likely be less inclined to use techniques to force a confession out of you when a lawyer is present. It is documented in many published cases with interrogation footage that once a suspect asks for a lawyer, the interrogating officer will halt the interrogation. (Though this is not an opportunity to let your guard down.)

Device seizure and plausible deniability:

Various concepts in the field of law grant you the power to say that you lost / forgot any passwords or security devices that might be used to gain access to your systems (or something accidental happened for them to be destroyed, they may not be able to prove otherwise).

Law enforcement will likely confiscate your devices in order for them to be preserved in evidence (to be decrypted and eventually searched), or kept away from you in the case that you were to try and destroy evidence.

Devices can be seized immediately WITHOUT a warrant and usually are if they are suspected to have suspicious or illegal material on them. Law Enforcement will usually hold onto these devices until they can obtain a search warrant for them.

The only things you should say or ask:

- Why am I being detained / arrested? (Depending on which situation is applicable.)
- Why am I being questioned?
- Am I free to leave? (If the officer says yes, leave.)
- I would like to speak with a lawyer.
- I am enacting my right to remain silent.

Though the situation may seem scary or inescapable, it is important that you stay calm during the entire ordeal, as Law Enforcement benefits greatly from preying on individuals' nerves or anxiousness in order to get them to admit to the thing(s) they are accused of. Using the aforementioned questions, as well as keeping cool and collected is your best choice when faced with a situation like this.

Avoiding this entirely:

The best way to not deal with Law Enforcement is to not do anything stupid or have any kind of incriminating web activity or data on your devices.

Password Strategies

I would say that a majority of times where people end up being hacked, it ends up being the result of the user having a crackable password. Many sources list the leading cause of hacks as being "weak or stolen credentials", so this section will list not only how to create and store a secure password, but also how to protect your password.

What makes a secure password:

With technological advancements and general improvements to the speed of computing, the standard of a "secure" password is constantly changing. (For the following I will use ascii_letters, digits, and punctuation from Python's string library as valid characters, however passwords can use other characters.)

Currently, a safe standard for passwords is:

i 15-20 characters
   - An extremely fast running a brute force script that can guess ~100 billion passwords per second (cracking a password with 15 length and using letters, numbers and symbols) will take probably billions of years to be guessed)
   - The longer the better, more characters EXPONENTIALLY increases the time to guess your password (if it is secure)

ii Using a mix of letters, numbers, and symbols
   - Increases the amount of characters a brute force program would need to crack a password.
   - For a password of length 7, without symbols there are 916,132,832 (916 million) possible passwords, while with symbols there are 7,339,040,224 (7.3 billion) possible passwords. (These can still be cracked easily, but this is just an example on how sample size affects time to crack)

iii Make sure it's not present in any password list

- Make sure your password is not in a common password list such as rockyou.txt or any of these.

iv Make sure it does not contain personal information
- Do not use numbers related to birth dates or important dates to yourself, friends, family, or anything that could be related to you.
- Do not use names or words that are relevant to you or people close to you in your passwords.
- If someone knows this information is connected to you and that you use this information in your passwords, it will make cracking them much easier.

v Do not use patterns or common strings of characters
- ABCDE, 12345, 09876, qwerty
- qwqwqw, 101010, dddddd, RRRR
- Patterns are not good to include as they make your passwords incredibly easier to guess

vi Do not use words in your passwords
- Common words or words found in the dictionary make it easier to guess your password.
- It's better to use seemingly random characters in your passwords, as it makes them much harder to crack.

A common misconception is that you should change your password every few months, but unless your password is compromised, there is no clear reason to do this if your password is secure.

I like to make my important and most sensitive passwords OVER 30 characters, just to make sure that they will not be brute forced within my lifetime, or even many lifetimes.

I made a password generator at https://fuckthefeds.pro/password (that runs locally and not over the internet).

One of the most common pitfalls with password is that people tend to store them in ways that completely ruin the point of even creating a secure password.

How to store a secure password:

It's all too common for users to store their passwords in ways that make it just useless to even have a secure password, usually either putting their most secure passwords on sticky notes, or plaintext files on their computer, rather than remembering them.

Your password is only ever safe in your mind, or behind layers of encryption.

You will need to remember AT LEAST one secure and long password to truly have good security. This will be for your Password Manager.

If you use a Password Manager, make sure that it is TRUSTED, OPEN SOURCE, and RUNS OFFLINE.

I use KeePassXC, which is still a great option for managing passwords, by default using AES-256 for Database Encryption (or Twofish / ChaCha20 if changed), and Argon2 for Key Derivation. Both of these algorithms are considered very safe and resistant to various types of attacks.

The best way to increase the safety of your password is by using a separate form of authentication alongside your password, known as MFA (Multi Factor Authentication). MFA can take many forms, but the only one I would recommend is a FIDO2 security key (such as a YubiKey). This allows for both your password and security key (a physical element) to be required when decrypting your password manager.

I would extremely advise against using biometric authentication, as things like your fingerprint can be obtained through relatively simple means, and are NOT ALWAYS protected by law (they can be obtained in some areas by Law Enforcement through a warrant)

Encrypting your devices (PC & Desktop)

Desktop encryption (and truly understanding how it works) is a necessity, as though it is extremely important in protecting your sensitive data and files, there are many pitfalls that people do not understand, which leads to their encryption being basically useless.

Principles of desktop encryption:

The standard for encryption on a desktop is usually FDE (Full disk encryption), which can be achieved by many different methods, but specifically the two methods people opt for are using LUKS (Linux Unified Key Setup) or VeraCrypt.

LUKS:

LUKS is (probably) the main encryption type that Linux users opt to use for encrypting their drive. When you set up LUKS, you effectively scramble your drive and make it so that it can only be unscrambled with your Master Key during the pre-boot process. LUKS uses a KDF (Key Derivation Function) which makes brute forcing your key much harder.

The benefits to using LUKS are:

- Universal standard (similar use / setup across different Linux distributions)
- Flexibility (feature to change the cipher that is used with cryptsetup)

VeraCrypt:

VeraCrypt is a FOSS (Free & Open source) tool which can encrypt disk partitions, but can also create encrypted file containers that are treated as volumes or separate drives when mounted and decrypted.

The main advantage of VeraCrypt is that it allows FDE for Windows users, as well as streamlines the process of encryption for less knowledgeable users with a GUI.

VeraCrypt allows for these algorithms to be used for encryption:

1 stage:
AES, Serpent, Twofish, Camellia, Kuznyechik

2 stage:
AES(Twofish), Serpent(AES), Twofish(Serpent), Camellia(Kuznyechik), Kuznyechik(Twofish), Camellia(Serpent), Kuznyechik(AES)

3 stage:
AES(Twofish(Serpent)), Serpent(Twofish(AES)), Kuznyechik(Serpent(Camellia))

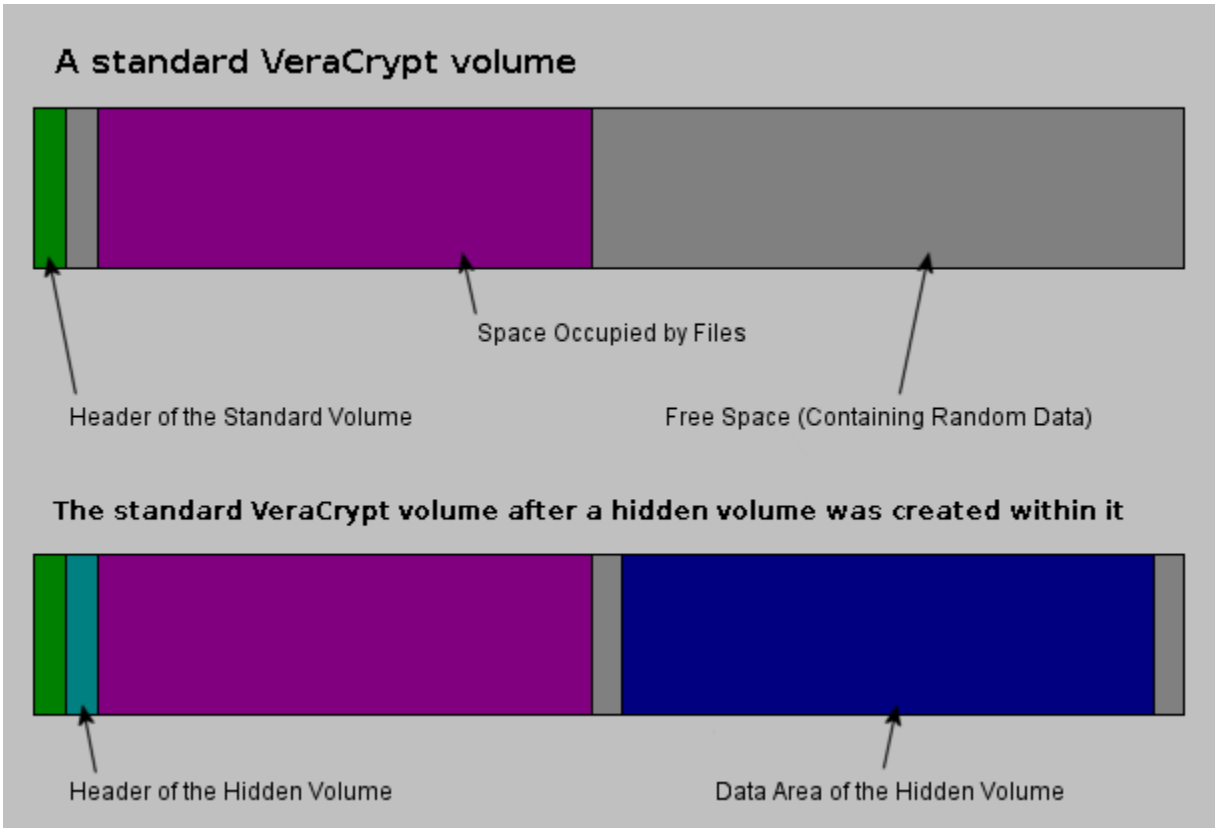
I use Kuznyechik(Serpent(Camellia)), but any three-stage algorithm will allow for the top level of encryption (at the cost of decryption speed).

<u>VeraCrypt Hidden containers:</u>

An extremely good reason to use VeraCrypt is for its “hidden containers” feature, where you can set a container to reveal one set of files with one password, and another set of files with another.

This can be useful in situations where you are forced to reveal your password, giving a fake one but passing it off as the real one. The “fake” password will open one part of the container as if it was a real one, which you can store semi-sensitive information in if you would like to pass it off as the real container.

Hidden containers are completely indistinguishable from regular containers, as VeraCrypt jumbles the data regardless of the container type, and makes the free space look like data.



(Standard volume & Hidden volume structure)

The benefits to using VeraCrypt are:

- Somewhat universal (VeraCrypt does work on Linux and Windows with the same functionality)
- Flexibility (VeraCrypt provides many different ciphers and cascades to use with differing levels of security and speed)
- Plausible deniability (containers have no VeraCrypt signatures and scrambled data allow for nobody to know that the container is actually a VeraCrypt volume)
- Hidden containers allow for your REAL information to be protected if you are ever coerced into revealing your password (which you can input a fake password as if it was the real one), and you can instead reveal fake information that appears as the true information.

Common pitfalls:

1. Keys can be recovered from memory

In order for either of these (LUKS or VeraCrypt) to function, they put their keys in the system's RAM for easy use, and they remain there while the drive / container is unlocked and in use.

The problem with this is that RAM can be dumped and read externally through many different methods if someone gains access of your system and knows what to do.

2. Your system / data is vulnerable while decrypted

When your system is in a "decrypted state" and able to read/write to your drive, your system contains all of your files in a completely decrypted state, meaning your drive can be cloned while it is in this "open" state, with or without your knowledge.

A real-life example of this exists stemming from the operation to arrest Silk Road owner Ross Ulbricht. (My direct source is the Day 6 trial transcript from the SDNY court, which has been uploaded and can be found by searching "F1MGULB1" online, or on the "FreeRoss.org" site).

Ulbricht used TrueCrypt for FDE, which is the original software that VeraCrypt is forked from. Overall, his encryption was secure and would not likely be cracked if the system was encrypted (but it wasn't).

Ross Ulbricht was distracted in a coordinated effort by Law Enforcement at a public library, leaving his computer open and decrypted, which essentially allowed authorities to create a copy image of his decrypted data using a command that most Linux distributions implement called "dd".

After the authorities obtained this image, it didn't matter if Ulbricht encrypted his computer, they already had everything on his computer that they needed.

Data erasure is not what you think:

When you "delete" data through conventional means, it's not actually deleted. Crazy, I know.

Data that is deleted simply through things like the Windows right click menu or the rm command on Linux, is still actually retrievable from your hard drive by data recovery professionals.

Before thinking that your files are simply "gone" after you "delete" them, you must consider that instead of deleting files, hard drives simply mark your file as able to be overwritten by new data if necessary and remove it from the index of the filesystem (which is like delisting the file rather than deleting it).

Secure data erasure for HDD (Linux / Unix systems):

If you need to securely erase a hard disk, partition, or file, there are options depending on your OS.

On Linux, using the "shred" command (which is bundled with coreutils) with its default 3 passes will make sure that your data is erased. Using the command:

sudo shred -vfz [device/file]

Where:

- [device/file] is your drive partition or file to be erased
- the v(erbose) flag displays progress
- the f(orce) flag will shred files with read-only permissions
- the z(ero) flag will write zeroes to the data at the end

This is good enough for sensitive information and will make your data unrecoverable.

Secure data erasure for HDD (Windows systems):

A FOSS tool called “Eraser” is widely used to erase hard disks on Windows. It allows for various methods of erasure (many of which are considered overkill but effective nonetheless) on partitions, drives, and files.

The tool is open-source on Sourceforge, but you can get the source code from a mirror on GitHub to compile yourself at https://github.com/gtrant/eraser/tree/master/eraser or from the official website at https://eraser.heidi.ie/download/.

Secure data erasure for SSD:

Data erasure on solid state drives isn’t the same, a lot of hard disk erasure methods do not work on SSDs like the do on HDDs. The best way to erase these drives is through Secure Erase, which isn’t always a universal process. Most SSD manufacturers have a specific software that they publish which has a specific function built in that will perform a secure erase on the SSD.

For example, Samsung has “Samsung Magician” which has a Secure Erase function in the software that will wipe a Samsung manufactured SSD. Kingston also has a software called “Kingston SSD manager” that also does the same thing.

I can’t advocate for the security or privacy of these apps, but I thought that including methods for erasing SSDs would be useful.

Encrypting your devices (Mobile)

This will be added in 2.1, as I'm still doing my research on Mobile devices and do not want to provide incomplete / false information.

Secure Browsing

Browsing the web safely and securely is something that many people try to do, but often fail due to oversights. When using apps like web browsers, sometimes only basic security practices get you so far.

Important Things to note:

IP Address:

Your IP address is a string of 4 octets each separated by a decimal. It's used to identify your device and route traffic specifically to you. Without IP addresses, servers would not know who or where to send information to.

An IP address can be used to find someone's APPROXIMATE location through services that have collected geographical information about the address through ISPs and other means.

Though it cannot reveal your EXACT location (99.9% of the time), you still should be careful with this information (I'll get more into this).

Using VPNs:

A VPN (Virtual Private Network) is an application that securely routes your internet traffic through an external server. A VPN will encrypt your traffic, send it to the external server, which will serve out your action, and return the result to you (which will be decrypted by the VPN app).

A VPN has many benefits, the main ones being:

- IP Masking (your IP will show up to sites as the external server's)
  - Shields your approximate location from sites & services
  - You can use it to appear as if you're accessing the web from a different country depending on the VPN server's location.
- Fully encrypted traffic

- Your traffic including sites you visit, data you send, and more are fully encrypted and if your traffic is intercepted, the person intercepting it will not be able to read it.
- The only time that your data is decrypted is on the external server

Using a VPN is REQUIRED for browsing on the web privately, as nowadays a good majority of sites have scripts or functions that record IP addresses to track users.

Choosing a VPN:

When choosing a VPN, it's important that they:

- Minimize logging and storage of user data
- Do not store (or even ask for) personal information
- Accept alternate forms of payment (such as Crypto)

There are three options that adhere to these categories:

Mullvad VPN:

Mullvad is a Sweden-based privacy-focused VPN service that has a specific no-logging policy. When you sign up for Mullvad, you don't provide an E-mail or password, and you only receive an account number which can be used to connect to the VPN.

Mullvad is also known to accept different types of payments, accepting Crypto including XMR (Monero), but they also accept cash payment through mail. You can put cash, your account number, and payment token, and it will be accepted as payment (which is viable for someone wanting to stay private, as you are not required to have any sort of personal information on an envelope to mail something).

You can get Mullvad VPN at https://mullvad.net/en for 5€/month.

IVPN:

IVPN brands itself as a “Privacy & Security-focused” VPN service. Their site and app are open-source, meaning you can compile it from source and make sure that the code doesn’t contain any malicious trackers / processes.

IVPN’s transparency report shows that they did not provide any user information to people requesting it (usually law enforcement) and they also provide a Warrant Canary, which is a document that states that no warrants have been served to IVPN, and no searches / seizures have taken place within their service.

They accept BTC, XMR, and also Cash in a similar way that Mullvad does.

You can get IVPN at https://www.ivpn.net/en/pricing/ for $6/month or yearly at a discounted price.

Cryptostorm VPN:

Cryptostorm is another privacy-focused service that is committed to not logging users’ data. They stand out for offering a variety of technical features (outlined on their site’s home page). They also encourage use of TOR routing or I2P in order to guarantee that your data is secure and not being logged They accept various Cryptocurrencies and also XMR.

You can purchase access to Cryptostorm VPN for $6/month or for longer at a discounted price at https://cryptostorm.is/#section5.

Browser Security:

Choosing your browser is important, as some browsers secretly collect information on their users. Browsers like Mozilla Firefox and Google Chrome are the biggest culprits of this.

It's important to choose a browser that is reputable (trusted by others as secure), open-source, and has a commitment to not tracking users through telemetry or other means.

There are too many to list, but I recommend LibreWolf or Tor Browser (which are both open source forks of Firefox).

Browser Tracking Techniques:

When browsing, many techniques can be used to track you through websites. I'll go over a few and their fixes.

1. JavaScript data collection (fingerprinting):

Sites use JavaScript to collect information from the browser. A good example is https://amiunique.org/fingerprint, which will show you all sorts of information that can be collected from your browser.

Though a lot of this data is hard to block individually, blocking certain tracking scripts (or whitelisting the useful scripts) is possibly helpful. A privacy browser like the ones mentioned before will also help prevent fingerprinting.

You can use an extension like NoScript in order to block specific scripts from loading on a site, though you will have to toggle individual scripts and disabling some scripts can easily break websites.

2. Canvas fingerprinting

Canvas fingerprinting is a method used to track users in a way that exploits how your browser renders a HTML <canvas> tag. Using JavaScript, a site will request you to render a canvas, and it will return a unique fingerprint (SHA256/MD5 hash of the Base64 string the canvas returns) that is based on information about your system and browser.

Using extensions like Canvas Blocker will randomize this string that's generated, making it so that your fingerprint will be unique every time the site is visited

Alternate Protocols / Browsing Methods

Using a normal browser and basic transmission of internet traffic sometimes isn't enough and people opt for different methods of transporting their traffic from client to server. The most well-known examples of these privacy-focused methods of moving traffic are TOR and I2P.

TOR Network:

The TOR (The Onion Router) Network is an anonymous network ran by thousands of people operating servers dedicated to routing traffic called "relays". Each relay routes traffic to the next, creating a path that sequentially decrypts encryption (like peeling an onion's layers).

Through the network you can access .onion sites (hidden services that can only be accessed through the TOR protocol) and clear net sites which can be accessed through a normal browser.

The benefit of using TOR is that you can access regular sites and hidden services while encrypting traffic and moving it through many different proxies, making your traffic much harder to track and identify.

I2P:

I2P (Invisible Internet Project) is an encrypted and private network layer that facilitates P2P connections between hosts. I2P uses a protocol similar to TOR's Onion Routing, with each tunnel decrypting one layer, but I2P bundles traffic that could be intended for multiple recipients and implements unidirectional tunnels (which allow for the client and server to be anonymous, rather than the client only specifically being anonymous on the TOR network). I2P tunnels are also extremely short lived (active for ~10 minutes), making tracking over a long period of time extremely difficult.

Unlike TOR, I2P cannot access sites on the clear net, and uses specific addresses that end in .i2p to designate sites. These sites (called "eepsites") are hosted anonymously and solely routed through the I2P network).

Overall, I2P is more secure than TOR due to its implementation of different features, but it comes with the caveat of not being able to access the clear net.

Secure Communication & Messaging

Communication over the internet is a necessity for most, and making sure that the channels you use for said communication are secure is essential when discussing possibly sensitive information.

Most communication apps that are widely today used are either not secure or hand your data over to third parties / law enforcement.

The main things you want from a secure communication app are:

- End-to-end encryption (so that only the sender and recipient have access to message content)
- No storage of user data (won't log IP addresses, location data, activity)
- Overall holds the least amount of identifiable data on the user.

Here are the apps I recommend (underlines are potential drawbacks):

SimpleX:

- End-to-end Encrypted
- No user information (phone number, username, email)
- Fully anonymous sign up process
- Open-source (https://github.com/simplex-chat/simplex-chat)
- QR-code based contact sharing
- Encrypted server traffic can be read by third parties
- Decentralized servers

Signal:

- End-to-end Encrypted (Signal protocol)
- Self-destructing messages
- Sign up requires a phone number
- Open-source (https://github.com/signalapp)
- Minimal storage of user data
- Centralized servers

qTox:

- End-to-end Encrypted (messages, voice, video)
- No user tracking or data storage
- No phone or email required (every user gets a unique ID)
- Open-source (https://github.com/qtox)
- You should use other tools for anonymity whem using P2P
- Decentralized servers

I would not recommend anything other these apps right now, as apps like Telegram (which are believed to be private) are not, and many “privacy-focused” communication apps have not been fully audited to the point where they can be overall trusted.

Self-hosted apps are reliant on the security of the host, and I can’t fit that all in here, so those will be left out as well.

File Metadata & EXIF

When doing things like taking photos or editing files in various applications, many people don't know that some sensitive information is often provided inside of said file.

EXIF (or Exchangeable Image File Format) is a standard of embedding metadata specifically into images, and it can contain a lot of personally-identifiable information, the most sensitive being:

- GPS coordinates of where the photo was taken
- Timestamps of when the photo was taken
- Information about the device that took the image
  - Model information
  - Possibly firmware information
  - Serial number
- Editing software used

All of these can be used to find where you live, and link you to your devices, location, etc.

EXIF isn't the only form of Metadata, though. There's Metadata attached to documents, video, audio, and more.

<u>Removing Metadata</u>

There are various open-source tools to remove all kinds of Metadata, with the main one for Exif being Exiftool (which works on all platforms). There are other ones that can remove all types of Metadata, but many are not completely trusted (you should look at the program's source code).

Refrain from using online websites that advertise the removal of Metadata, as sometimes these websites will store your data, your file, and the file's Metadata for their own nefarious purposes.

Private Cryptocurrency:

Important:

~ This guide will ignore things like price of the currency and trade volume, as it's impossible to predict these things in a document that's supposed to remain relevant for a long time. ~

About Cryptocurrency & Privacy:

When purchasing things online (like a private VPN) the most secure method is using Cryptocurrency. Unfortunately, most Cryptocurrencies are public and traceable on the blockchain (BTC, ETH, etc), which leads to things being created that are dubbed as "privacy coins", with the most well known & used being Monero & Zcash.

I'll be focusing on Monero in this guide, but some of the concepts I'll go over apply universally.

Purchasing Safely:

Most Crypto exchanges are legally required to have a process called "KYC" (Know your Customer), which is obviously a big problem when trying to maintain anonymity, as giving your ID to some exchange is a ridiculous security risk. Buying from an exchange currently is almost impossible to do without compromising yourself, as very few non-KYC exchanges exist and even then, they get shut down regularly.

The way that people bypass this is by using a P2P exchange (where one person will trade Crypto for another means of currency). Sites like xmrbazaar exist to facilitate these trades, but you will need to be wary of scams. I suggest looking into both XMR and P2P trading on your own. The good thing about exchanging like this is that you can maintain anonymity while still receiving your coins.

Holding Safely:

One of the most important aspects of utilizing Crypto is holding it in your wallet. When you create an XMR wallet, you are told to provide a password (which you can create by following the steps previously outlined in this guide), and then given a seed phrase (which is a list of words that can be used to fully regenerate your wallet from anywhere).

A seed phrase is MUCH MORE DANGEROUS for someone to have than your password, as it's tied to the wallet address itself and can allow for someone to fully regenerate your wallet and have access to all of your currency.

With a password, it's specifically for the app, and while still dangerous to leak, it's not the end of the world if you do, as you can change the password and re-encrypt your wallet within the app. If you leak your seed phrase, you can't change it like a password, and your assets are permanently open to theft from whoever has the phrase.

Never, never, never give anyone or anything your seed phrase. You should treat it with EVEN MORE security than your password.

Making purchases with XMR:

I won't explain the full process of sending and receiving XMR as the process can differ with different wallets and services, but here are some documents that outline the process:

Sending XMR:
https://www.getmonero.org/resources/user-guides/prove-payment.html

Proving a transaction was made:
https://www.getmonero.org/resources/user-guides/prove-payment.html

Disappearing:

Worst Case Scenario:

In the worst case scenario, you may have to disappear or go “off the radar” if you want to avoid people that will be looking for you.

This is what I usually use when disappearing or changing aliases, and have done before:

Discontinue use of current alias:

You will have to stop using any accounts or assets that still have a connection to your alias. Delete your social media, messaging, or any relevant accounts tied to the name you’re using.

It is important that you relinquish ALL TIES you have to this identity, and basically forget it existed, never speak about it, and deny all relation to it if it ever comes up.

If your identity has been found or leaked:

If your real life identity has been Doxxed and revealed to the public, the process is different:

The best thing you can do in this case is change your legal name, through a sealed name change. The process for a sealed name change varies depending on your location, but usually it requires evidence of extensive stalking and or harassment.

The effectiveness of obtaining a sealed name change online is not extremely clear, and success in different jurisdictions will vary, however if you are able to provide substantial evidence that public records of a name change will affect your safety, there is a chance that the motion will be accepted.

An alternate method of obtaining a sealed name change is if you are transitioning, as some states have guidelines that allow trans people to have their name changes sealed for safety reasons.

If your location is known, moving areas is definitely a good idea as well in the case that people look for you in that area.

<u>If you're being harassed over allegations of something:</u>

Never, never, never admit guilt, even in an attempt to satisfy people. A confession will only further fuel people to stalk you or try and get more evidence or talk about you more.

Remember that:

- Screenshots can be doctored (and are not real evidence)
- Unless messages are publicly available on a platform (or still on the platform's servers), that message can never be proven to be real.
- Audio of "confessions" can be faked / dubbed with AI now

The best thing you can do is just not give a reaction to attempts of trolling or such, people will be losers and will try to bait you all the time, but if you just ignore their attempts, it will possibly demotivate them.

<u>Don't forget that people can be extremely stupid:</u>

When people find someone "controversial" or intriguing to them, they will latch on and either whine and cry about your behavior or try and troll you. Let them cry about you all they want, but don't give a reaction, don't respond, don't try and fuel the fire more.

Eventually without response or interaction, a good majority of people will forget about you and stop caring. It can take a while and there WILL be people that remember you or continue to try to seek you out even after months to years of being gone.

Coming back:

When / if you come back, you must play the role of a completely different person to not arouse suspicion of allow people to draw similarities between your new identity and your old one.

Don’t go back to the same communities you were active in, as a community that is well accustomed to the old you will easily be able to find similarities between your two personas, even if you do a good job at acting as someone different.

Use a different name that isn’t similar to your old one (or any aliases / usernames that are similar or already tied to your old one). Don’t reuse names, always create new ones. Try to have different hobbies, and overall, don’t be a complete contrast of your old persona, but don’t be very similar.

Speaking differently is also a big part of having a new identity, as people’s texting patterns, emotional presence in text, certain vocabulary, and colloquialisms or specific phrases can be used to immediately pinpoint who you are. I’ve been able to point out many different people failing to act as a different person solely using their speech patterns.

More:

I’ll be releasing a guide solely focused on how to effectively disappear or change identities after the publication of this one, but I’m not sure when.

Closing words:

Overall, with technology changing every single day, this guide could be outdated in months, maybe even weeks, which is why I will try to update as much as I can when it does become outdated or certain parts become irrelevant.

The purpose of this is that hopefully now you know more than you did about protecting yourself, your identity, and your data while operating online.

The heart of digital security is keeping your information to yourself, as any piece of information, even something that may seem insignificant, can possibly be used to deanonymize and track you.

I urge anyone reading to do their own research. Learn about topics like OPSEC, OSINT, and come up with your own strategies to be more secure online.

It doesn't take a genius to learn about security. Just like how anyone can learn about surviving in the wilderness with enough research and training, anyone can learn about surviving and staying safe in the vast space that the internet is.

Information is one of the most powerful weapons that exists.

Keep it safe, always.

My future publications:

I'm planning to release more documents similar to this guide, as well as update this guide periodically. These will be released on my website at the URL: https://fuckthefeds.pro/docs.

These will contain PDF form documents as well as their PGP signatures that prove they are written by me. Modified versions of my document will not be valid. (My PGP key will be in the last section of this document)

I don't have any kind of public social media to use to update on new releases, so just check back periodically or email me if you're interested in more documents / guides. If anyone claims to be me on social media, chances are it isn't me, and if it is me I will prove it.

Currently I only have a few different documents that I've planned to write, but chances are they will take months to fully draft, research for, and type out. My goal is to write everything in an understandable yet comprehensive way, that is endured to be accurate. One mistake or one falsehood could lead to compromise.

Please check my site for more.

Supporting & Links

If you would like to support me and the future development of fuckthefeds.pro, you can donate XMR to my wallet here:

44hGNvh5PbL8rsnPER2QVo1wmkppRnXdLUgb3oQTtwgp58L2YSWj
WXCaKaDzWkHrodbdNfUhVVGEn8SmmcK7JnHZLBCe4WN

Donations are not necessary but are greatly appreciated.

For future publications, my PGP key will be available at https://fuckthefeds.pro/key.asc. This will also mean that I will sign the PDF documents that I publish, which can be downloaded by adding ".sig" after the PDF file's link.

(fuckthefeds.pro/file → fuckthefeds.pro/file.sig)

If you have questions, want to ask about a specific section, or just want to share something with me, you can reach me through:

varex@fuckthefeds.pro or admin@fuckthefeds.pro

You will probably get a response from a different address (as the domain is set to redirect to an email ending with "@proton.me", but I will make sure to sign my messages with my PGP key.

If at ANY point, I publish a message that is not accompanied by a signed PGP signature, do not trust the message. I will ALWAYS be able to produce a valid PGP signature (if it is truly me posting said message).

I hope you enjoyed this guide, Stay safe, stay secure.