Incognito Guide

Deleting your online identity and staying hidden

Note: The more privacy is emphasized, the less convenience there is in everyday life.

# Basic Privacy (Recommended for most people)

## Digital Footprint Basic:

1. Disable Google Tracking
   1. Activity Control Page in google settings
      1. Disable everything possible
2. All other services you have ever signed up for should have all information changed out for fake information and should then be deleted. This helps in case on of the accounts is compromised
   1. A good way to find these types of accounts is by going to your main emails and searching up “sign up” or “verify” and tracing back the accounts that way
   2. JustDeleteMe.xyz is a good place to find how to properly remove accounts and the viability of removing those accounts.

## Social Media Basic

1. Be sure to use basic privacy settings in any social media you use
2. Don’t add strangers on any platforms
3. Don’t comment or respond to public post
4. Don’t allow things that aren’t required by the service
   1. For example: Facebook doesn’t need location services, so there’s no need to give it to them
5. While using social media (or just in general) use VPNs.
   1. Private Cloud Relay is not a great use as a VPN as it doesn’t work outside of safari currently.
   2. Options include ProtonVPN, Mullvad, and IVPN

## General Communication Basic

1. Encrypt your instant messaging
   1. Use things like iMessage or Signal that encrypt communication
2. Encrypt your email
   1. Move to a service like ProtonMail or Tutanota which don’t require personal details and will do email encryptions for you
3. If the email isn’t needed for long time use, use a disposable email.
   1. 33mail, Guerrillamail, and TempMail are services that can be used for this

## Browsers Basic

1. Only use extensions from trusted sources
2. Change the search engine to a privacy based one
   1. DuckDuckGo as of late has fallen out of favor with the privacy community startpage.com is a google alternative with no tracking and Searx if that is an issue
3. Clear temp data frequently
   1. Personally, I have my browser clear everything on restart and I close my browser often

## Smartphones Basic

1. In settings disable analytics.
2. Check that apps aren’t getting more permissions than they need
3. Disable any unneeded radios
   1. The easiest ones for these are Wifi and NFC, and only turn them on when needed. Extra mile is Bluetooth, Wifi, NFC, Cell Data
4. Disable as many features as possible
5. Delete any unneeded applications
6. Use a VPN
7. Make sure that MAC address randomization is in use
8. Turn on Automatic Software Update

## Computers Basic

1. Disable Analytics and App data
2. Disable unneeded radios
3. Check that apps aren’t getting more permissions than they need
4. Uninstall apps you don’t need
5. Disable unused features
6. Use a VPN
7. Ensure that Automatic software updates are enabled

## Storage Basic

1. Clear temporary data as often as possible.
   1. Browser and OS tools and Bleach Bit
2. Shredding files is important
3. Keep 2 backups
   1. One on-site backup and one off-site backup

## Real Life Basic

1. Avoid using public computers
2. Avoid smart trackers like smart watches
3. Avoid IoT devices
4. Make use of Safes and Shredders

# Intermediate Privacy (Recommended for those concerned about Privacy and Security)

## Digital Footprint Intermediate:

1. Use separate online identities
   1. You can use a different one for each type of activity like online shopping or dating
   2. I use MySudo to manage a few of these
      1. It’s important that whatever is tied to that identity is only used for that identity

## Passwords Intermediate

1. No more biometric authentication

## Social Media Intermediate

1. No personal info on any social media
2. Don’t post personal photos online
3. Keep social media sandboxed within progressive web apps which are sandboxes for applications
   1. An alternative to this is using the “Add to home screen” option if available. We just want to avoid using the actual application.

## General Communication Intermediate

1. Use VOIP
   1. Google voice, mysudo, hushed are good examples of these
2. If the VOIP numbers are getting flagged, the next best thing you can use is a prepaid sim bought online through eBay or mint mobile.

## Browsers Intermediate

1. Compartmentalize web browsers. Each browser should be used for a different thing.
   1. For normal desktop you can use Tor, Firefox, Brave, or Safari.
      1. Tor is for Anonymity
      2. Firefox is good for personal privacy and security (when hardened)
      3. Brave/Safari are good for privacy and security out of the box
   2. For mobile you can do Toor, FF Focus, DDG, or Bromite
      1. Tor once again is for Anonymity
      2. FF Focus is for disposable searches, as is DDG
      3. Bromite is best for privacy

## Smartphones Intermediate

1. Switch phones
   1. Android is traced by Google, phone manufacturer, and cell providers if you get generic phones, and the update support is usually poor
   2. Google Pixel and OnePlus android phones are better in general for privacy and security since it’s only tracked by google and has better update support
   3. iPhone is more secure and privacy focused than both the previous options, and generally has much better update support.
   4. For the extra mile, Custom Android Roms can be loaded onto phones like GrapheneOS and CalyxOS. These tend to be the best you can do for smartphones.

## Computers Intermediate

1. Switch whatever you can to FOSS (Word > OpenOffice)
   1. You can search up alternatives using AlternativeTo.net and sorting by OpenSource
   2. F-droid can be used for android
   3. AltStore can be used for IOS
2. Password protect your bios
3. Consider Full Disk Encryption
   1. MacOS has Filevault
   2. Linux has GParted
   3. For Windows unless you have windows Pro you have to use VeraCrypt instead of BitLocker. If you do have BitLocker that can be used.
4. Spoof your MAC address
5. If you have windows, disabling your privacy settings doesn’t fully help the problem
   1. It’s best to use something like W10Privacy to disable extra tracking settings
6. At this level, MacOS is better for privacy and Security
7. Considering cleaning up Metadata from photos and files using tools like Metapho for photos and MAT2 for other file formats

## Real Life Intermediate

1. Have some sort of home security system set up
   1. This can include alarms and cameras
      1. It’s essential that these cameras are not managed or accessible by third parties. Old fashion types (like offline NVR) are best here
      2. Do it yourself alarms are not a bad idea
2. Consider cable locks for laptops and PC Chassis intrusion kits
3. Remove all IOT devices
4. Consider Privacy Screen Protectors

# Cleaning up online presence

## Unneeded Service Cleanup

1. Go to any emails you use and search “sign up” and “verify”, take note of every service you find (service can be something like facebook or target)
2. For every single service, sign in and change all personal data (name, address, credit card info, etc.) to random data in case the information is kept, and the data of the company is breached.
   1. Random emails can be generated via Tempmail
   2. Phone numbers can be changed to one provided by freephonenum.com
   3. Change the password to something completely random
   4. Remove other information that might be personally identifiable (PII)
3. Delete the account, if possible, else extra details might be able to be grabbed from justdeleteme.xyz
   1. In the case the account cannot be removed, just falsify all data and put the account aside
4. \*deseat.me does this to some end, but it does require giving data to the company behind it so take the risk if necessary
5. Prepare to remove email accounts. Delete all emails and flood the email with mailbomber spam.
6. Of course, anything you want to keep you can keep the privacy settings on maximum.
   1. Consider moving data from cloud services you don’t really need onto a physical disk
7. On google, in account settings to go “Delete activity by” and delete via “all time” and “all products”
   1. Consider deleting your google account. There is usually a type of journey for this and more details can be found later.
8. Check for breached accounts via google searching emails, haveibeenpwned, identity gathering sites
   1. Change passwords if necessary, delete the account if not.
9. Consider contacting site administrators to have data about you removed from sites if you do not have the ability to do it yourself
10. Check your images through reverse searching (google reverse search or tineye)
    1. Request the site take it down because you don’t give permission for it to be on there
    2. If a is refused, consider filing a DMCA takedown notice against the site
11. Social media should be as private as possible and minimize the amount of data the account has
    1. Avoid using your full name if possible
    2. Avoid pictures of yourself on the main profile
12. People searching websites are used to gather data on people for social engineering attacks and the like. These sites won’t so easily exclude data about you when asked about it. Linked here is a guide to how to get some of that information off the internet if possible
    1. This does basically include contacting every company individually
    2. Refer to this link for tips: https://www.computerworld.com/article/2849263/doxxing-defense-remove-your-personal-info-from-data-brokers.html