## toolbox and workflows

1 data encryption
   a in transit
   b at rest
2 masking identifiers
   a email (aliases and disposable)
   b phone numbers
   c keeping track with cred managers
   d ip addresses / vpns
3 travel opsec

## tools

signal, tresorit, openpgp, onionshare, cryptpad, temp-mail, notesnook, joplin, obsidian, syncthing, duckduckgo, proton ag, filen.ai, textverified, bitwarden, keepass, mullvad, tor browser, graphene os, linux

## data encryption

the process of converting information into a coded format to prevent unauthorized access and ensure data confidentiality.

## end to end encryption (e2ee)

a secure communication method that ensures only the communicating users can read the messages, preventing intermediaries from accessing the data.

encryption of data in transit

signal

is open source
is nonprofit
no metadata retention
has usernames
also video / calls, groups, stickers
files up to 100 megabytes

encryption of data in transit

other solutions

email & openpgp friction
tresorit send / wetransfer issues
onionshare
encrypted cloud services

encryption of data at rest

tools

1 full disk encryption (+bfu/afu, backups)
2 encrypted cloud & data sync
   proton, filen.io, skiff affair
   self-hosted, nextcloud & syncthing
3 note taking
   notesnook, obsidian
   joplin
4 cryptpad (collaboration / cloud tools)
   open source, e2ee, solid free plans

## toolbox and workflows

~~1 data encryption~~
   ~~a in transit~~
   ~~b at rest~~
2 masking identifiers
   a email (aliases and disposable)
   b phone numbers
   c keeping track with cred managers
   c ip addresses / vpns
3 travel opsec

## personal identifiers

refer to any information that can be used to identify an individual in digital space.

emails, usernames, ip addresses, phone numbers, links to social media profiles, cookies and tracking ids, device identifiers, payment data, location data, biometric data

masking personal identifiers

email & phone numbers

1 aliases
   duckduckgo (+ duck.ai)
   protonpass, anonaddy
2 disposable emails
   temp-mail, guerrilla mail
3 phone number masking
   disposable / burner sim card issues
   textverified / online services

masking personal identifiers

keeping track with password / crediental managers

1 bitwarden
   open source, e2ee cloud-based & selfhosted, multiplatform
   browser and android / ios integrations
2 keepass
   foss, several versions
   encrypted, offline
   automatic backup and self-sync plugins

masking personal identifiers

ip address, logical locations

1 mullvad vpn
   opensource, 5$ a month, 5 devices
   no-log policy, anonymous account and payment
   some pushback / captcha friction
2 tor browser
   foss, onion network – layers of anonimity
   slower, captchas, more suspicious

## bonus: operating systems

1 graphene os
   hardened & degoogled android os
   web-based / no-root flashing
   less exploits, sandboxing apps, profiles, duress
   google pixel exclusive
2 linux (tails, cubes os, debian)
   free and open source
   UX improved over years, most tools available

## toolbox and workflows

~~1 data encryption~~
- ~~a in transit~~
- ~~b at rest~~

~~2 masking identifiers~~
- ~~a email (aliases and disposable)~~
- ~~b phone numbers~~
- ~~c keeping track with cred managers~~
- ~~c ip addresses / vpns~~

3 travel opsec

travel opsec

henry!