

LET'S GO!

No tool offers full protection - but this zine gives you a starting point to protect yourself and keep learning.

- Location & movement 3
- Communication 4-5
- Online profiles & data 6-7
- Resources 8

TOPICS TOPICS TOPICS

If you're reading this, you've used our zine generator and answered 3 ques - tions about surveillance. This zine is your personal starter emergency kit. It highlights the dangers of surveillance + + gives you first tips to protect yourself from data access by 1312

HEY!

Your Digital Surveillance First Aid Kit

(for ppl who'd rather be cats :))



- ◆ Encrypt files (e.g. with VeraCrypt)
- ◆ Avoid unencrypted cloud uploads
- ◆ Don't share , signs, or standouts outfits
- ◆ Use strong passwords, 2FA & install updates

- ◆ Remove EXIF (e.g. ExifCleaner)
- ◆ Use Signal/Treema with DESTRUCTION

Protection Check:

It can link you to places or protests. or via apps (e.g. WhatsApp) or data brokers. From seized phones, unencrypted clouds, can use this:

That shot of your fresh kicks? It may include hidden EXIF metadata — like GPS, time, camera, and phone model.

The Digital Images & Metadata

Module 1, Answer C: 3.

Resources: 8.

As you see Surveillance tech is everywhere — from AI analyzing messages to mass tracking in public. These tools keep evolving.



Digital security is a process. Staying informed and sharing what you learn helps everyone stay safer !!!

Check out these non-profit sources for updated cybersecurity info:



CREATED By @eymeikey

These are intentionally built-in weaknesses in software or services that allow third parties (such as law enforcement or hackers) to access data without breaking the normal encryption. One example is how Meta could access WhatsApp metadata for years.

Backdoors

Some politicians are pushing for Content Scanning (ChatControl) Private chats aren't always as private as they seem — even encrypted messages can be at risk.

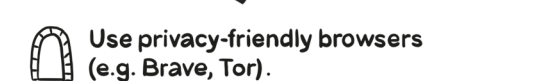
Content Scanning (ChatControl)

When Your Messages Are Read Content Scanning & Backdoors: 4.

Module 2: Block C

Protection Check:

- Use privacy-friendly browsers (e.g. Brave, Tor).
- Install blockers like uBlock Origin or Privacy Badger.
- Delete cookies regularly or limit them to sessions.
- Use a VPN to hide your IP. Switch to private search engines (DuckDuckGo, Startpage).



Like the EU's "chat control" proposal, which threatens secure communication.

Stay informed: Follow political debates

Share sensitive info securely. Only send private data via E2EE chats or trusted tools like ProtonMail (email) or Tresorit (cloud storage).

Prefer open source:

Pick messengers with open code (e.g. Signal, Element) — this allows independent security audits.

Use messengers with true E2EE:

Protection Check:

Module 3: Block A

Trackers, Cookies & Fingerprinting

Caught in the Act! That ad wasn't random — it came from invisible tools tracking your online behavior: cookies, trackers, and fingerprinting.

What's happening:

Cookies store what sites you visit. Trackers follow you across websites. Fingerprinting identifies your device using unique traits like fonts, settings, or plugins — even without cookies. These tools build a profile of your interests. A quick search on AI surveillance can instantly tag you as "relevant."

Law enforcement access:

Data brokers collect this info in bulk. Police and agencies can buy or request it to trace your activity or behavior.

