Your Digital Surveillance First Aid Kit

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

2.

HEY!

If you're reading this, you've used our zine generator and answered 3 questions 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

TOPICS TOPICS TOPICS

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

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

LET'S GO!

↑ NO COMPLETE GUIDE!

3.

Module 1, Answer C:

The D[redacted]g[redacted]tal [redacted]n Images & Metadata

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

1312 can use this:
From seized phones, unencrypted clouds, or via apps (e.g. WhatsApp) or data brokers.
It can link you to places or protests.

Protection Check:

- ◆ Remove EXIF (e.g. ExifCleaner)
- ◆ Use Signal/Threema with DESTRUCTION MODE
- ◆ Encrypt files (e.g. with VeraCrypt)
- ◆ Avoid unencrypted cloud uploads
- ◆ Don't share , signs, or standout outfits
- ◆ Use strong passwords, 2FA & install updates

4.

Module 2: Block B

State Trojans & Spyware – The Inv[redacted]s[redacted]ble Threat

"Being watched before you even type 'Hi'?"
Sounds extreme – but it's real:
State trojans are programs secretly installed on your device by police or intelligence agencies to read everything – even before it's encrypted. They can access your microphone, camera, location, and passwords.

They often enter through security flaws in apps or operating systems.
Example: one WhatsApp bug let spyware install via a missed call.
In Germoney, court orders are required, but critics warn that oversight is weak and courts often enable systemic abuse and unchecked state power.

Spyware from companies like NSO (Pegasus) has been used to target journalists, lawyers, and activists.

5.

Protection Check:

- **Keep software updated:** Always update OS & apps to close security gaps.
- **Beware of links/files:** Don't click unknown links or open suspicious files.
- **App permissions:** Limit access to mic, camera, and location – only when needed.
- **Strong passwords** & 2FA: Protects accounts from being hijacked.
- **Restart your device:** May remove temporary infections.
- **Sensitive conversations:** Best offline or on a separate device. Tool check (if suspicious): Use Amnesty's Mobile Verification Toolkit (for tech-savvy users).
- **Consult experts:** If you suspect spyware or feel unsure, seek professional support.

! MVT is complex – professional help is recommended if spyware is suspected.

6.

Module 3: Block B

Cloud Surve[redacted]llance & B[redacted]g Data

Many everyday services store massive amounts of your data in the cloud — a TREASURE for analysis algorithms.

What's happening:
Searches, emails, photos, documents, app use — everything is saved on cloud servers. AI-powered systems analyze this data to find patterns, predict your behavior, and build detailed profiles.

Targeted ads? That's the result: your interest in privacy triggered ads about "security."

Law enforcement access:
Authorities can access cloud data. The U.S. CLOUD Act allows access to U.S. companies' data even if stored abroad. Data can also be obtained via court orders or hacked accounts.

7.

Protection Check: ✓✓✓✓

- Use encrypted cloud services (e.g. Proton Drive, Tresorit)
- Upload only what's necessary
- Store sensitive files locally on encrypted drives
- Use strong passwords & 2FA Encrypt files (e.g. with VeraCrypt) before uploading

8.

Resources:

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