

LET'S GO!

↓ NO GUIDE!

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

TOPICS TOPICS TOPICS

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

If you're reading this, you've used our zine generator and answered 3 ques - ++ gives you first tips to protect yourself from data access by 1312

HEY!

2. It highlights the dangers of surveillance + + gives you first tips to protect yourself from data access by 1312

Your Digital Surveillance First Aid Kit

(info is impact)

Module 1, Answer A

GPS, WLAN & Bluetooth

You thought Maps only shows you the way? Not just you. Your phone constantly sends signals: GPS shows your exact location. Apps collect this data. WLAN & Bluetooth send unique device IDs (e.g., when searching for networks) - even without connection.

How data is collected & used:

Sensors in public places capture these signals, track your movements, and create movement profiles. Authorities can, via court order locate all devices in an area at a specific time. They can also buy this data from Databrokers.

Protection Check:

Turn off location services & location history
 Revoke location access from apps -
 Activate airplane mode (prevents real-time tracking) • Use an extra device

BURNER PHONE

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

Module 2: Block B

The Invisible Threat - State Trojans & Spyware

"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 Germany, 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.

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.

7.

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).

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.

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.