recommended it spyware is suspected. MVT is complex - professional help is

teel unsure, seek protessional support. • Consult experts: If you suspect spyware or

Mobile Verification Toolkit (for tech-savvy Tool check (if suspicious): Use Amnesty's Best offline or on a separate device.

Sensitive conversations: temporary infections.

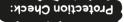
• Restart your device: May remove Protects accounts from being hijacked. Strong passwords & 2FA:

camera, and location - only when needed.

App permissions: Limit access to mic, links or open suspicious files.

● Beware of links/files: Don't click unknown & apps to close security gaps.

Keep software updated: Always update 05



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

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

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

The Inverse ble Threat State Trojans & Spyware -Wodule 2: Block B

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

Protection Check:

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

How data is collected & used:

for networks) - even without connection. device IDs (e.g., when searching WLAN & Bluetooth send unique

Apps collect this data. GPS shows your exact location. signals: ¿

Not just your phone constantly sends tou thought Maps only shows you the way?

> GPS, WLAN & Bluetooth Module 1, Answer H

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

Resources & R Online profiles & data 6 6-7 COMMUNICATION & 4-5 Location & movement [] 5

yourself from dala access by 1312 👺 + + + dives you first tips to protect It highlights the dangers of surveillance

your personal starter emergency hic. tions about surveillance. This zine is zine generator and answered 3 ques-If you're reading this, you've used our



Module 3: Block A Trackers, Cook in es & Fungerpruintuing

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 Al 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.

Protection Check:

Use privacy-friendly browsers (e.g. Brave, Tor).



Install blockers like uBlock Origin or Privacy Badger.



Delete cook to sessions. Delete cookies regularly or limit them



Use a VPN to hide your IP. Switch to private search engines (DuckDuckGo, Startpage).



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:









Your Digital Surveillance First **Aid Kit**



CREATED By @eymeikey