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

Protection Check:

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 - arewyd2 & snejorT atet2 d Wodule 2: Block B





- ◆ Use strong passwords, 2FA & install updates Don't share 1913, signs, or standout outiles
 - ◆ Avoid unencrypted cloud uploads
 - ♦ Encrypt files (e.g. with VeraCrypt)
 - ◆Use Signal/Threema with @EST ?? USU → Use Signal/Threema with ◆ Remove EXIF (e.g. ExitCleaner)

Protection Check:

8.

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

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

> Images & Metadata Istaing and I Module 1, Answer C:

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

Resonrces & & Online profiles & data 6 6-7 COMMUNICATION (4-5) Location & movement [] 5

yourself from data access by 1312 👺 + + + gives 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 C Your Online Profine

///

+social media All your online activities searches, social media, websites,

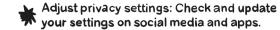
purchases, and app use-are collected and combined into a detailed digital profile.

This profile reveals not only your interests but also preferences, political views, social networks, and even emotional states. The targeted ads you see show how precisely algorithms predict your needs and fears based on this data.

For law enforcement, such profiles are a treasure. They use them for open source intelligence (OSINT), predictive policing, and targeted surveillance to identify and monitor individuals.



Share mindfully: Only share what feels necessary online.



Keep identities separate: Use different emails or profiles for different activities.

Be aware: Notice the digital footprints you leave.

Check regularly: See what data companies have about you and manage it.



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:









COMPARE US WITH DOGS WE DON'TWORK FOR THE POLICE

Your Digital Surveillance First **Aid Kit**

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

