

Go Quiet Protocol

1. The "Go Quiet" Protocol: Immediate Personal Security

Goal: Protect your identity, location, and communications instantly when you feel monitored or are in immediate danger.

This protocol focuses on actions you can do right now with minimal effort to stop giving away information.

Step	Action: What You Must Do Now	Why This Saves You (Survival Rationale)	FOSS/Resilience Tool or Practice
1. The Lock Habit	Set your phone and laptop to lock instantly (under 30 seconds) when you stop touching them or close the lid.	If you must suddenly leave your device, this prevents instant access to all your files and communications. Locking is your primary shield.	<i>Device Setting (High-Impact Behavioral Change)</i>
2. Use a Strong Passphrase	Change your login password to a long, easy-to-remember passphrase (e.g., four random, unrelated words like <i>PurpleElephantRopeSky</i>).	It's simple for you to type under pressure, but virtually impossible for anyone else to guess.	<i>Security Practice</i>
3. Only Use Secure Messaging	For all sensitive conversations, use an end-to-end encrypted app like Signal . Check that Disappearing Messages is turned ON for critical chats.	This keeps your messages private from the service provider and automatically deletes evidence, reducing your digital footprint over time.	Signal (FOSS-aligned/Highly secure)
4. Silence the Trackers	Turn off Location Services , Wi-Fi , and Bluetooth on your device when you are not actively using them.	Stops your device from telling others exactly where you are and who is nearby, conserving precious battery life as a bonus.	<i>Device Setting (Low-Bandwidth, High-Resilience)</i>
5. Browse Anonymously	If you need to search for highly sensitive information, use the Tor Browser (if available) or, at minimum, your browser's "Private/Incognito Mode."	This helps hide your location and your searches from your local internet network and potential surveillance.	Tor Browser (FOSS)