

Hide and Save

The "Hide and Save" Protocol: Data Security and Resilience

Goal: Ensure your most critical files are safe from seizure, loss, or destruction and can be accessed even with low or no internet access.

This protocol focuses on making your data unreadable to an adversary and ensuring you have multiple ways to recover it.

Step	Action: What You Must Do Now	Why This Saves You (Survival Rationale)	FOSS/Resilience Tool or Practice
1. Encrypt Your Device	If your phone or computer has an option for Full Disk Encryption (FDE) , make sure it is ON .	If your device is lost or taken, this is the single most important action to ensure no one can read your files without your passphrase.	<i>Device Setting (Essential Security)</i>
2. Create a "Secret Vault"	Know how to use a simple FOSS tool (like VeraCrypt or GnuPG) to make a separate, highly encrypted folder or "vault" on your device. Only put your absolutely most critical documents inside.	If forced to reveal your main login password, this vault is still protected by a second, unique passphrase.	VeraCrypt (FOSS) / GnuPG (FOSS)
3. The "Three Copies" Rule	Keep at least three copies of your essential files: 1) on your device, 2) on an encrypted USB drive, and 3) on a secure, encrypted cloud service.	Guarantees that even if one copy is lost or destroyed, you can still recover the information from another source.	<i>Redundancy Practice</i>
4. Low-Bandwidth Backup	Move your essential files to an encrypted cloud service that uses zero-knowledge protection (like Filen).	This is your safe off-site storage, which you can recover from anywhere in the world using even a very slow connection.	Filen (Zero-Knowledge, Encrypted)
5. Test Your Recovery	Try to access the files from your encrypted USB drive and your secure cloud backup at least once <i>without</i> using your main device.	A backup that you haven't tested is unreliable. You must know exactly how to get your data back under stress.	<i>Security Practice</i>

