PRIVACYLABPRO.COM

CHECKLIST

How to Safely Store and Manage Personal Encryption Keys

Protecting your encryption keys from loss

1. Stop writing encryption keys on paper or storing in notes apps immediately.
2. Purchase a hardware wallet like Ledger Nano S Plus or Trezor Model One.
3. Create a secondary backup of your wallet recovery phrase in a secure location.
4. Split your recovery phrase into parts stored in two geographically separate places.
5. Choose a zero-knowledge password manager like Bitwarden or 1Password for key storage.
6. Enable two-factor authentication on all password managers storing encryption keys.
7. Store backups using both offline hardware and encrypted cloud services like Proton Drive.
8. Set monthly reminders to check and verify your encryption key backups exist.
9. Rotate your backup storage locations every six months to prevent single-point failures.
10. Reserve cold storage devices for high-value assets you access infrequently.
11. Use hardware wallets for daily access and cold storage for long-term holdings.
12. Never back up encryption keys to unencrypted cloud services like Google Drive.