Operational Hygiene

Institutionalize behaviors that minimize human error and endpoint compromise across daily operations.

- Device inventory and role separation (admin vs. user).
- Password manager and hardware security keys.
- Training cadence and phishing drills.

1) Isolate signing devices; no web browsing or email on them.

2) Enforce strong authentication (hardware keys); disable SMS 2FA.

3) Standardize firmware/app updates—only from verified sources; delay non■security updates.

4) Establish code phrases and out■of■band checks for approvals.

5) Maintain logs and peer reviews for sensitive actions.

- Malware on laptops is the most common failure—keep signing air■gapped.
- Approval fatigue leads to rubber■stamping—rotate duties and set limits.
- Phishing adapts—train with realistic scenarios; verify URLs and signatures.

- Hardware security keys (FIDO2)
- Password manager with org controls
- **Coldcard** + **Nunchuk** for constrained, auditable signing flows

Monthly drills; quarterly refresher training; periodic red■team exercises.