Personal Security Guidelines for Blockchain Developers

Version 1.0

General Setup

- Enable hard drive encryption.
- Protect the machine with password and biometric authentication if available.
- Use different passwords for every service.
- Use strong passwords.
- Use a password manager.
- Always use 2FA authentication for remote services. Fido U2F (usually hardware key) or OTP (phone app) are best. Avoid SMS 2FA as it is often defeated by sim swap attacks.
- Make sure your 2FA option is backed up (offline recovery key for OTP or second hardware key)
- Keep personal and business email accounts strictly separate.
- If you use Google Chrome, use different profiles for business and private browsing.
- Only run trusted applications on a work machine.
- Scan your system frequently for key loggers and similar malware.

Development Environment

- Only use trusted and established libraries (be wary of supply chain attacks).
- Consider running the development environment in a dedicated sandbox (cloud server, virtual machine, or docker image). This can be done quite nicely with ssh tunneling and IDE's like VSCode (with remote connection).
- Use ssh with private key authentication whenever possible and disable password authentication.
- Always encrypt ssh (or other) keys with a strong passphrase.
- Do not keep production passwords or secrets in unencrypted files (avoid production `.env` files in the source code tree)

Oak Security
https://oaksecurity.io/
info@oaksecurity.io

Wallet/Key Management

- Use separate accounts derived from different mnemonics for local testing, testnet deployments and production
- Keep offline backups (cold wallet). Consider geographically different places for this. For example, keep a separate copy in a bank vault for critical keys.
- Use browser plugin wallets (MetaMask, Terra Station plugin) on their own only for testnet and pocket money transactions).
- For production and other large transactions use them in combination with a hardware wallet.
- Keep accounts used for payment separate from admin and deployment keys.
- Generate all key material used in production on a clean offline machine.
- If your building services requiring hot wallets with access to private keys on a connected system consider using a hardware security module or at least a trusted cloud-based key management enclave.
- Do not share keys with co-workers (or anyone else for convenience), even for testing.