

Blind the wallet map

Terms

- Descriptor. The wallet map. Not a seed.
- xpub. A watching key. Not a seed.
- Passphrase. Opens the map file. Not a seed.
- Plain text. Anyone who finds it can read it.

Short steps

- Boot Tails with networking off.
- Do not write xpubs on paper.
- Save the descriptor as map.txt.
- Run: `gpg --symmetric map.txt`
- Use a long passphrase. Not from the plates.
- Write that passphrase on separate paper.
- Keep that paper away from the plates.
- Keep map.txt.gpg. Delete map.txt.
- Store the encrypted file on two USBs.
- Decrypt once later. Confirm the map opens.
- Do not invent a paper cipher.