MitDepot: Din sikkerhed under og efter samtalen

I. Hvad du aldrig må gøre

- Del aldrig dine 12/24 ord – heller ikke med os[1]
- Klik aldrig på links, du ikke selv har verificeret – især hvis du bruger en usikker wallet[2]
- Brug aldrig skærmdeling, hvor dine ord kan vises ved en fejl (social engineering)[3]
- Stol ikke på “kundeservice”, der beder om adgang eller backup

II. Sådan beskytter vi dig

- Vi nævner disse trusler eksplicit – så du kan sikre dig, at selv vi ikke snyder dig
- Vi gennemgår sammen, hvordan du realistisk ville blive angrebet – og hvordan det undgås
- Vi opbevarer aldrig dine ord, nøgler eller enheder

III. Du kan og bør tjekke os

- Spørg fx ChatGPT, Grok eller søg: 'Skal man dele sin seed phrase?'
- Læs selv dokumentation fra Ledger, Coldcard, Trezor m.fl.
- Hvis du er usikker på en transaktion, wallet eller setup – så start med et lille beløb og test

IV. Før samtalen

- Sid et privat sted – undgå caféer, åbne kontorer og videoovervågning. Brug helst en bærbar med kamera slået fra – og læg mobilen i et andet rum
- Medbring noter om din nuværende opsætning, fx wallet-type, backup og evt. bekymringer
- Du bliver aldrig bedt om fjernadgang, skærmdeling (sjældent), eller dine ord. Alt foregår som samtale og skriftligt materiale

V. Efter samtalen

- Undersøg og reflekter. Alt vi gennemgår, kan og bør verificeres
- Du behøver ikke beslutte dig nu – din sikkerhed og ro er vigtigst
- Løsningen vi bygger sammen, kan nemt forklares til en betroet ven eller familiemedlem

Book samtale nu

- Book her: calendly.com/selvdepot/30min

[1] Ledger Support Docs – Never share your recovery phrase
[2] ScamSniffer: $55M drained via phishing links (2023)
[3] Casa Blog – Internet-connected wallets are attack vectors