Fake crypto support checklist (PDF)

UXS · https://uxs.nz/crypto/how-do-fake-crypto-support-accounts-on-x-try-to-steal-your-wallet/ · 2026-11-10 · Educational only, not financial advice

Print or save. Use it before you reply to any "support" or "recovery" message.

Before you reply

Platform name and its official support URL (typed by me) _____

Did I open a ticket first? Ticket number _____

Where did the message come from (reply, DM, email, phone)? _____

Red flags (tick any)

- ☐ Contact came first from them, not me
- ☐ Asked to move to DMs, Telegram or WhatsApp
- ☐ Asked for my seed phrase, private key, password or 2FA code
- ☐ Asked me to install a remote-access app or sign on a website
- ☐ Asked for a fee, or offered paid recovery

If I already shared something

Time I shared it and what I shared _____

Transaction hashes of any outgoing transfers _____

Report filed at ic3.gov (date) and with the platform _____

Sources: FBI IC3: 2024 Internet Crime Report; FBI IC3 PSA I-080124: Cryptocurrency exchange impersonation; FBI IC3 PSA I-062424: Fictitious law firms and fund recovery scams. Full explanation and links: https://uxs.nz/crypto/how-do-fake-crypto-support-accounts-on-x-try-to-steal-your-wallet/

Educational content, not financial, tax or legal advice. Trading involves substantial risk of loss. Made by UXS (uxs.nz). Free to print and share unchanged with attribution.