













# PROTECTING YOUR CRYPTO WEALTH

What to Share

—

And What to **NEVER** Share

 <b>SAFE TO SHARE</b> ( <i>Read-Only Only</i> )	 <b>NEVER SHARE — NOT WITH ANYONE</b>
 <b>Wallet Information</b> • Public wallet addresses• Blockchain used (BTC, ETH, Solana, etc.)• Wallet type (MetaMask, Ledger, Trust Wallet)	 <b>Absolute Prohibitions</b> • Seed / recovery phrases (12–24 words)• Mnemonic phrases• Private keys
 <b>Transaction Details</b> • Transaction IDs (TXIDs / hashes)• Dates & amounts of transfers• Screenshots of transaction history	 <b>Wallet Access Data</b> • Keystore or backup files• Wallet passwords or PINs• One-time passcodes (2FA)
 <b>Exchanges &amp; Platforms</b> • Names of exchanges or services used• Email address used to register• Approximate account creation dates• CSV or PDF transaction exports	 <b>Anyone with this information can drain your wallet instantly and irreversibly.</b>
 <b>Supporting Documents</b> • Police report or case number• Divorce or legal case reference• Scam messages, websites, or contracts• Bank or exchange deposit confirmations	 <b>There is no legitimate reason for anyone to request this information.</b>



## SECURITY RULES (APPLY AT ALL TIMES)

- Legitimate professionals **never need** your seed phrase
- There is **no such thing** as temporary or view-only seed access
- Crypto transactions are **irreversible**
- Asset tracing, valuation, and reporting are **non-custodial**



## RED FLAGS — STOP IMMEDIATELY IF SOMEONE:

- Asks for your seed phrase “to recover” funds
- Tells you to move crypto to a “safe” or “holding” wallet
- Uses urgency, fear, or secrecy
- Promises guaranteed recovery