USDT PAYMENT CHECKLIST

15 seconds before you pay or release the goods. Tick every box.

1 · BEFORE YOU SEND

- ☐ Agree the amount, destination AND network. ERC-20 (Ethereum) and TRC-20 (TRON) are different networks.
- ☐ Open YOUR wallet or exchange deposit page. Confirm the token, network and minimum deposit.
- ☐ Check the pasted address in FULL. Never copy it from transaction history: look-alike addresses are planted there.
- ☐ P2P to a card: accept money only from the account holder's own name. No third-party payers.

2 · CHECK THE PAYMENT

- ☐ Type etherscan.io or tronscan.org yourself. Never open the sender's explorer link.
- ☐ Compare the FULL token contract with Tether's supported-protocols page for that network.
- ☐ Check recipient, amount and status. 'Success' can still mean a fake token moved.
- ☐ Release nothing until it is credited and withdrawable in YOUR account. Screenshots prove nothing.
- ☐ Cash deal: stay in a safe public place until the transfer is credited.
- ☐ Verify EVERY later payment. One honest small test proves nothing about the big one.

3 · RED FLAGS — STOP THE DEAL

- ☐ Rush, pressure, or a discount above 2%.
- ☐ A request to sign, approve, 'activate' or 'claim' in order to receive.
- ☐ Anyone asking for your seed phrase or private key.
- ☐ A 'free AML check' site that wants your wallet connected.
- ☐ Wrong contract or network, or a deposit that is not credited.

One box unchecked? Do not pay. Do not release the goods.

Tether: tether.to/en/supported-protocols · cryptostrapon.com

Educational checklist. Not financial or legal advice.

WHY EACH CHECK MATTERS

NETWORKS

ERC-20 = USDT on Ethereum, TRC-20 = USDT on TRON. Tether also issues on other networks (Polygon, Arbitrum and more): each network has its OWN official contract on the supported-protocols page. 'Bridged' USDT on another chain is a different contract again.

HOT, COLD, CUSTODIAL — SAME CHECK, DIFFERENT PROOF

- Custodial (exchange account): the exchange holds the keys. Only the credited, withdrawable balance in YOUR account is payment.
- Non-custodial hot wallet (phone/browser app, your keys): verify the transfer yourself in the explorer — token contract, your address, amount, confirmed status.
- Cold wallet (hardware device, offline): same explorer check; connect the device only to confirm. Never type its seed phrase into any site, app or 'verification' page.

ADDRESS POISONING

Scammers send tiny or zero-value transfers from addresses that share the first and last characters with one you use, so a look-alike sits in your history. Copy from your own deposit page or address book and compare every character. Full guide: cryptostrapon.com/how-to-prevent-address-poisoning

'DIRTY' COINS AND AML CHECKS

Exchanges can freeze deposits their risk checks link to crime. A risk score is a probability, not a verdict. Never connect your wallet or enter a seed phrase on a 'free AML check' site: a wallet connection can be used to request approvals that drain it.

LIFEHACKS FROM THE DESK

- Bookmark Tether's supported-protocols page; check every deal against the bookmark, not a search result.
- Search the buyer's Telegram handle plus 'scam' before any OTC trade.
- Meet in daylight and use your own mobile data, not public Wi-Fi.

KEEP THE RECEIPT

Save: network · full contract · transaction hash · recipient · amount · time · order/chat. Keep this privately; never include seed phrases or private keys.

Contract identity is not a guarantee of price, liquidity, redemption or a trustworthy counterparty. Bridged assets need separate issuer/bridge verification. Recheck current sources before each deal.