FLASHGUARD · USDT SAFETY CHECKER · 2026 EDITION

The “One Search” Tab — a manual in plain words —

Written for people who do not do computers.

If you can use WhatsApp, you can use this.

Every picture in this book is a real photograph of the working program, taken while checking a real payment on the public ledger.

The whole manual in three lines:

1 · Someone sends you codes, screenshots or links about a USDT payment.

2 · You **copy** each thing they sent and **paste** it into the matching box in FlashGuard.

3 · You press one button — **Run all checks** — and read the colour of the answer. Red means walk away.

What is in this manual

PART 1

What is FlashGuard, and what is “One search”?

USDT (also called Tether) is digital money. One USDT is worth about one US dollar. Because it moves fast and far, cheats love it. The most common trick is **"flash USDT"** — fake money that *appears* in your wallet or in a screenshot, looks completely real, and then vanishes or turns out to be worthless. The cheat shows you this fake payment and asks *you* to send something real — goods, cash, or a "small fee".

FlashGuard is your verification counter. Think of it like the bank clerk who holds a note up to the light. It does not touch your money. It cannot spend anything. It only **reads public records** and tells you whether what you were shown is genuine.

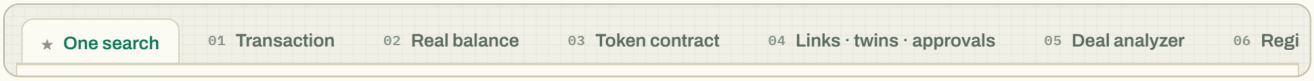
"One search" is the first tab and the only one you need. The other tabs are single instruments; One search is the full check-up. You put *everything* the other person gave you on the counter at once, press one button, and every relevant test runs together. At the top you get **one verdict in one colour**.

Comforting facts: FlashGuard never asks for your password, your secret words, or any money. You cannot break anything by pressing the wrong button. Boxes you leave empty are simply skipped.

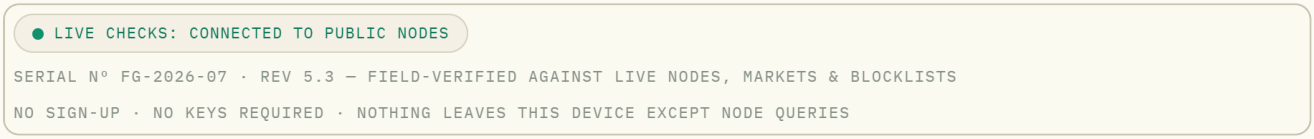
PART 2

Opening the program and finding the tab

1. **Open FlashGuard the way it was set up for you** — usually a bookmark or icon in **Chrome** (Brave, Edge or Firefox are also fine). If the file `index.html` was saved on your computer, double-clicking it opens it in the browser.
2. Across the top you will see a row of tabs, like the tabs of a file folder. **"One search", with the star ★, is the first one on the left — and it is already selected when the program opens.** If you ever get lost in the other tabs, click the star to come home.



Picture 1 — the tab row. The first tab, **★ One search**, is the one this whole manual is about. It is already open when the program starts.



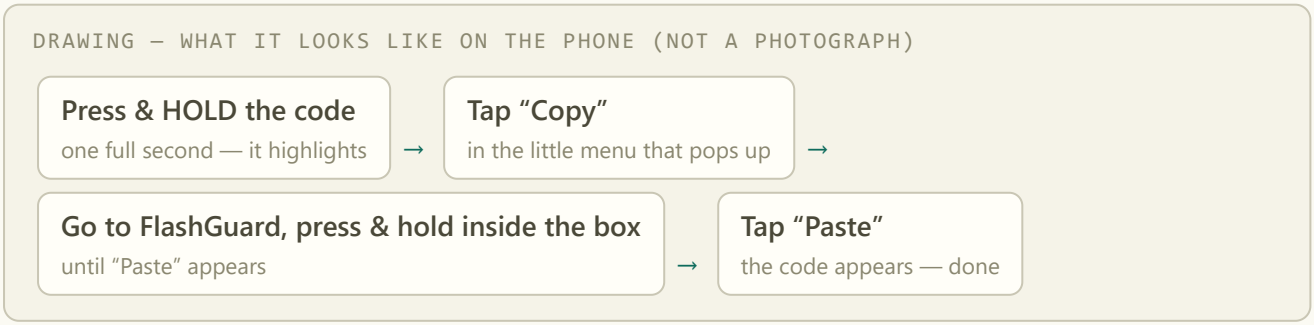
Picture 2 — the status light, just above the tabs. When it reads **"LIVE CHECKS: CONNECTED TO PUBLIC NODES"** with a green dot, all is well. If instead a yellow note says live checks are blocked, FlashGuard was opened inside another program's window — open it directly in Chrome.

PART 3

The only skill you need: copy and paste

Every code in this business is long and strange, like `TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t`. **Never type these by hand.** One wrong letter ruins the check. Always copy and paste.

On a phone (WhatsApp, Telegram, any app)



On a computer

1. Click just before the code, hold the mouse button, and drag across it so it is highlighted (or triple-click it).
2. Press **Ctrl** and **C** together — that copies.
3. Click inside the FlashGuard box, then press **Ctrl** and **V** together — that pastes.

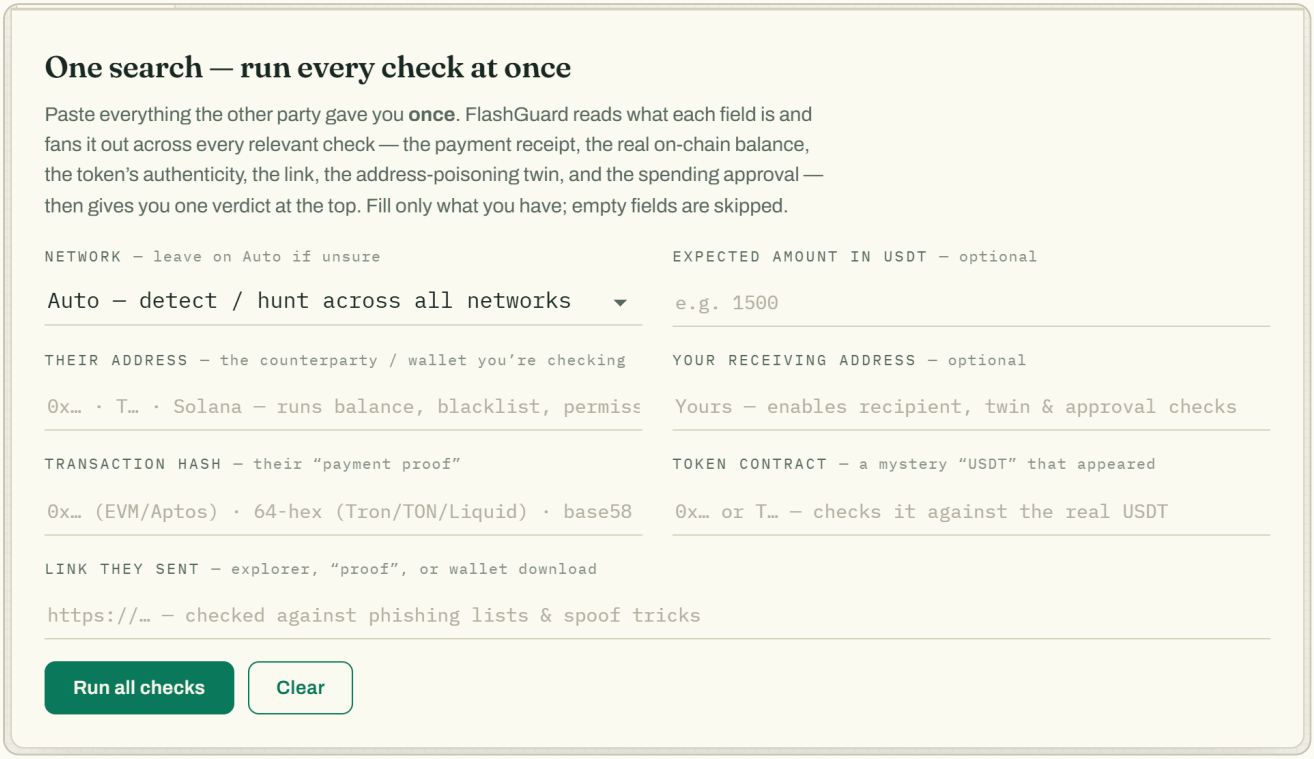
Do not worry about tidiness. If extra spaces or line breaks come along with the code, FlashGuard cleans them up by itself.

One caution about links: when a stranger sends a link, **copy it without opening it**. On the phone: press and hold on the link → **Copy**. On the computer: **right-click** it → **Copy link address**. FlashGuard will inspect the link for you — you never need to visit it yourself.

PART 4

A picture-map of the One-search screen

Picture 3 is the real screen, photographed from the program. Meet the seven boxes — each one is explained fully in Part 5:



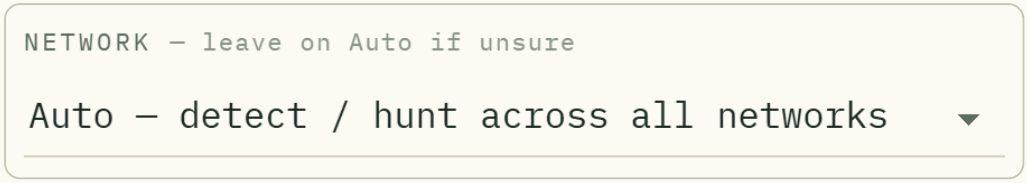
Picture 3 — the whole One-search screen. Top row: ① **Network** (left) and ② **Expected amount** (right). Second row: ③ **Their address** (left) and ④ **Your receiving address** (right). Third row: ⑤ **Transaction hash** (left) and ⑥ **Token contract** (right). Then ⑦ **Link they sent**, and at the bottom the green **Run all checks** button with **Clear** beside it.

Remember: you almost never fill all seven. Fill whatever the other person gave you, leave the rest empty, and press **Run all checks**. Empty boxes are skipped automatically.

PART 5

The seven boxes, one by one

① Network — which “rail” the money runs on



> **Picture 4 — the Network box.** It is a drop-down list: click the small triangle ▾ and choose. **If you are not sure, leave it on “Auto”** — FlashGuard then hunts across all networks by itself. You lose nothing by leaving it on Auto.

USDT travels on several rails (networks). People name them with short codes — match what you see:

If you see written…	Choose in the Network box
`TRC20` / `TRC-20` — *the most common in scams*	Tron · TRC-20
`ERC20` / `ERC-20`	Ethereum · ERC-20
`BEP20` / `BSC`	BNB Smart Chain · BEP-20
`Polygon` / `MATIC`	Polygon PoS
`TON` (Telegram wallets)	TON · Jetton

Where this word appears on common apps and websites

1. **The payment screenshot** they sent — a line usually says *Network: TRC20*.
2. **Binance app** — every Deposit / Withdraw screen has a “Network” choice showing TRC20 / ERC20 / BEP20.
3. **Trust Wallet** — under the coin name it says e.g. “USDT *TRC20*”.
4. **The chat itself** — senders often write “send me the TRC20 address”.

② Expected amount in USDT — how much they claim they paid

> **Picture 5 — the amount box.** Plain digits only: `1500`, not "1,500 USDT". For decimals use a dot: `1500.50`. Optional — leave empty if no amount was claimed.

Why it matters: a favourite trick is a **real** payment of a **tiny** amount (1.5 USDT) flashed quickly on a phone, hoping you read it as 1,500. With the amount filled in, FlashGuard compares the claim with the truth on the ledger.

③ Their address — the stranger's wallet code

> **Picture 6 — "Their address".** Paste the other person's wallet code here — the buyer, the "investment manager", the person asking you for a fee.

Every wallet has an address — one long code, like an account number:

```
TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t  ← starts with T = Tron
```

```
0xdAC17F958D2ee523a2206206994597C13D831ec7  ← starts with 0x = Ethereum / BNB / Polygon…
```

With their address, FlashGuard checks their **real balance**, whether Tether has **blacklisted** them, whether security services have **flagged** them, and (on Tron) whether their account keys look hijacked.

Where to find their address

1. **WhatsApp / Telegram chat** — the long code they pasted with the words "send here" or "this is my wallet". Press-and-hold → Copy.
2. **Their payment screenshot** — the line marked **From** is their address (see Picture 9 on the next pages — the same line exists on every explorer page).
3. **Binance P2P order page** — the counterparty's wallet details shown on the order.
4. **A QR code they sent** — under every wallet QR the same address is printed as text. Copy the text, not the picture.

④ Your receiving address — your own wallet code

YOUR RECEIVING ADDRESS — optional

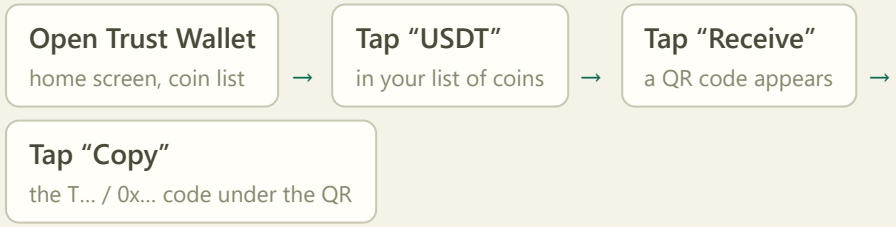
Yours — enables recipient, twin & approval checks

Picture 7 — "Your receiving address". Optional, but filling it unlocks the best checks: was the payment really sent **to you**, and does anyone hold permission to pull money **out** of your wallet.

Where to find your own address — pick the app you use

1. **Trust Wallet:** open the app → tap **USDT** → tap **Receive** → your address is under the QR code → tap **Copy**.
2. **Binance app: Wallet** (bottom) → **Deposit** → choose **USDT** → choose the network (e.g. TRC20) → tap the copy symbol ⧉ next to the address.
3. **TronLink:** your T… address is at the top of the home screen — tap it once, it copies.
4. **MetaMask:** your 0x… address is under the account name at the top — tap it once, it copies.
5. **Telegram Wallet:** Wallet inside Telegram → USDT → **Receive** → copy.
6. **Any other wallet:** always the same idea — find the coin, press **Receive**, press **Copy**.

DRAWING — THE "RECEIVE" STEPS IN TRUST WALLET (NOT A PHOTOGRAPH)



⑤ Transaction hash — the receipt number of the payment

```
TRANSACTION HASH — their "payment proof"

0x… (EVM/Aptos) · 64-hex (Tron/TON/Liquid) · base58
```

Picture 8 — the transaction-hash box. This is where their "payment proof" goes.

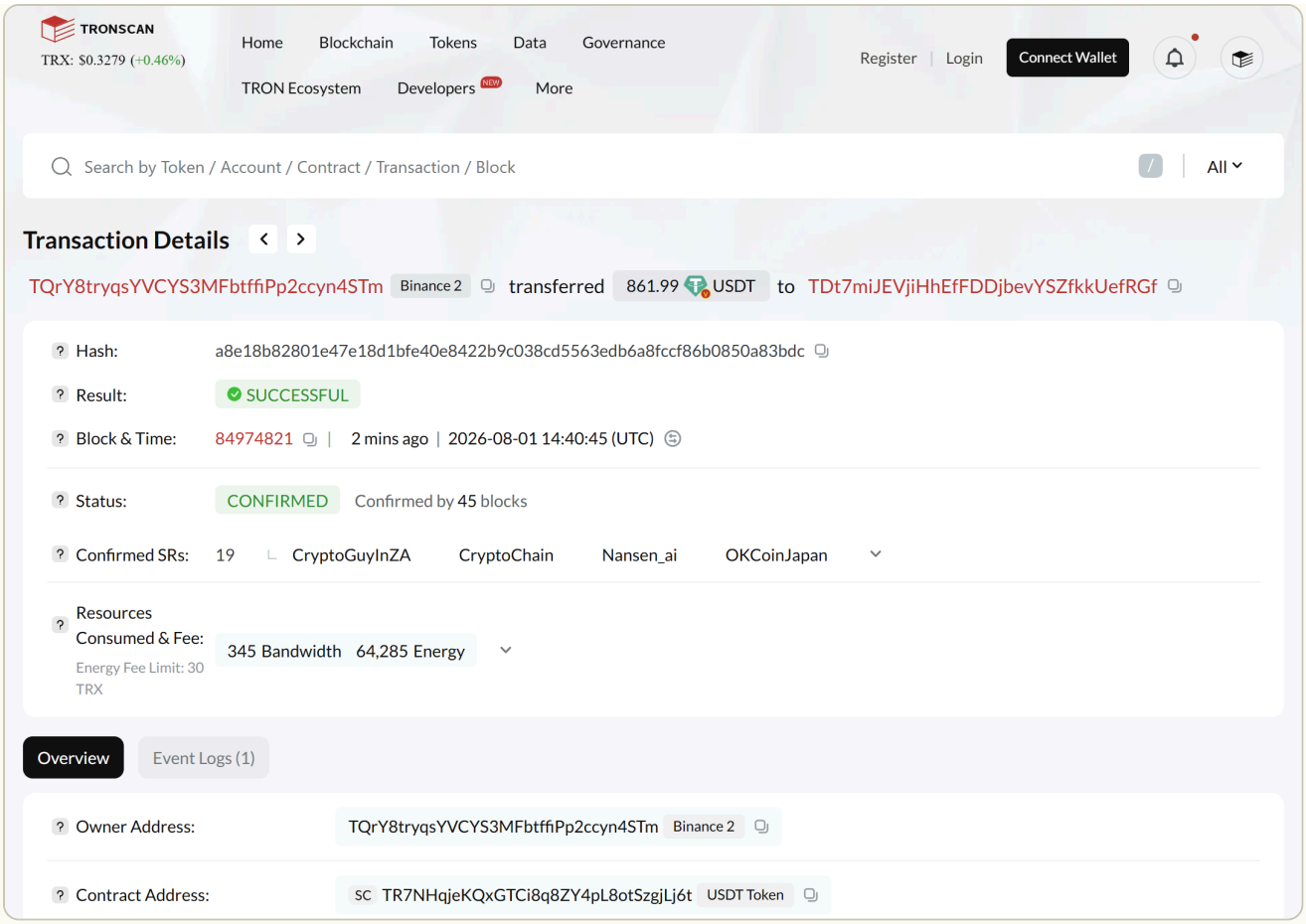
Every payment on a blockchain gets a unique receipt number — the **transaction hash** (also written **TxID**, **Txn Hash** or **Transaction ID**). A screenshot can be photoshopped; the hash cannot. FlashGuard pulls the raw receipt from the public ledger and inspects the one thing fakes cannot forge: **which contract actually moved the money** — the real Tether, or an imitation. What a hash looks like:

```
0x4f8a99… (66 characters starting 0x — Ethereum, BNB, Polygon…)
```

```
a8e18b82801e47e18d1bfe40e8422b9c038cd5563edb6a8fccf86b0850a83bdc (64 characters, only 0–9 and a–f — Tron)
```

Where to find the hash

1. **On the screenshot they sent** — the line named **TxID / Txn Hash / Hash**. Ask them to send it *as text*: "Please send me the TxID as text." A genuine payer never refuses this.
2. **Tronscan (tronscan.org)** — the "Hash:" line at the top of every transaction page, with a copy symbol beside it. **See Picture 9 below.**
3. **Etherscan (etherscan.io) / BscScan (bscscan.com)** — the "Transaction Hash:" line at the top of the page, in exactly the same place.
4. **Binance app** (if you made the payment) — **Wallet → Transaction History** → tap the withdrawal → **TxID** → copy.
5. **Trust Wallet** — tap the coin → tap the payment in the list → the detail screen shows the hash (or a "view on explorer" button whose page shows it at the top).



Picture 9 — a real payment on tronscan.org (the same payment we verify in Part 7). Learn this page once and you can read any of them: the **Hash:** line near the top is the receipt number that goes into box ⑤; the first red code in the sentence above it ("TQrY8… transferred 861.99 USDT to TDt7…") is the sender — box ③; the second red code is the receiver — box ④; and at the bottom, **Contract Address** shows `TR7NH…` tagged "USDT Token" — the genuine article from Appendix B. The small ⧉ symbols copy each code with one click.

⑥ Token contract — for mystery money that appeared out of nowhere

```
TOKEN CONTRACT — a mystery "USDT" that appeared

0x… or T… — checks it against the real USDT
```

Picture 10 — the token-contract box. For the "50,000 USDT" that appeared in your wallet by itself, or any coin a stranger helped you "import".

Every token is issued by a **contract** — its passport. Real USDT comes from exactly one contract per network (printed in Appendix B). Fake USDT comes from an impostor contract that merely wears the same name and logo. Paste the suspicious token's contract here and FlashGuard compares it with the genuine one.

Where to find a token's contract code

1. **Trust Wallet:** tap the suspicious token → tap its name / the ⓘ info symbol at the top → the detail page shows **Contract** — a 0x... or T... code → copy.
2. **MetaMask:** tap the token → the three dots ⋮ → **Token details** → contract address → copy.
3. **TronLink:** tap the token → the details screen shows the contract (T...) → copy.
4. **Tronscan / Etherscan:** on any token's page the contract is shown under the token name (it is also the long code in the browser's address bar).
5. **CoinMarketCap (coinmarketcap.com):** search “Tether” → the coin page's **Contracts** section lists the real address for every network — useful for comparing with your own eyes.

⑦ Link they sent — any website they want you to open

Picture 11 — the link box. Paste any link a stranger sends — a “proof” page, an explorer, a wallet download — **without opening it yourself**.

Some scam pages are perfect copies of real sites. FlashGuard checks the link against phishing lists and spoofing tricks — twin letters, hidden characters, fake endings like `tronscan-verify.live` instead of `tronscan.org`. You will see exactly this example caught red-handed in Part 7, Story 3.

Two bonus checks run by themselves — you do nothing.
· If the two addresses (③ and ④) look suspiciously alike, FlashGuard runs the **address-poisoning** test — a trick where a cheat manufactures an address almost identical to yours, hoping you copy the wrong one from your history.
· If you filled both addresses **and** chose a specific network in box ① (not Auto), FlashGuard also audits **spending approvals** — whether their address holds a signed permission to pull USDT out of your wallet.

PART 6

Pressing the button and reading the colours

Picture 12 — the two buttons. Run all checks starts everything (pressing the Enter key does the same). **Clear** empties every box for the next case.

Wait a few seconds while FlashGuard questions the public ledgers. Then read the **top banner first** — the summary verdict, in one of three colours. These are real photographs of all three:

1 check failed — treat this as a scam until proven otherwise
At least one hard on-chain red flag is present. No fee, "one last step", or reassurance changes a failed check. Walk away.

DO NOT PROCEED

Picture 13 — RED: "DO NOT PROCEED." At least one check failed — a hard red flag straight from the public ledger. No fee, no "one last step", no smooth explanation on the phone changes a failed check. Stop replying. Walk away.

1 thing needs your attention
No hard red flag, but something is unverified or unusual. Read each card below before you act, and never pay before an on-chain transfer confirms.

CAUTION

Picture 14 — YELLOW: "CAUTION." No hard red flag, but something is unverified or unusual. Read each card below the banner, and never hand over money or goods before a payment is fully confirmed on-chain.

The checks that ran found nothing wrong
This is not a guarantee — it means the data you gave passed. Verify the counterparty independently and never send funds first.

NO RED FLAGS

Picture 15 — GREEN: "NO RED FLAGS." Everything you provided passed. This is not a guarantee of an honest person — it means the data was genuine. Still follow the iron rules, and never send anything of value first.

> **Picture 16 — the tally under the banner.** “Checks run (3)” lists what was tested; “Skipped” lists what could not run because its box was empty. Below this come the detailed cards, one per check — you do not have to understand every line; the colours carry the message.

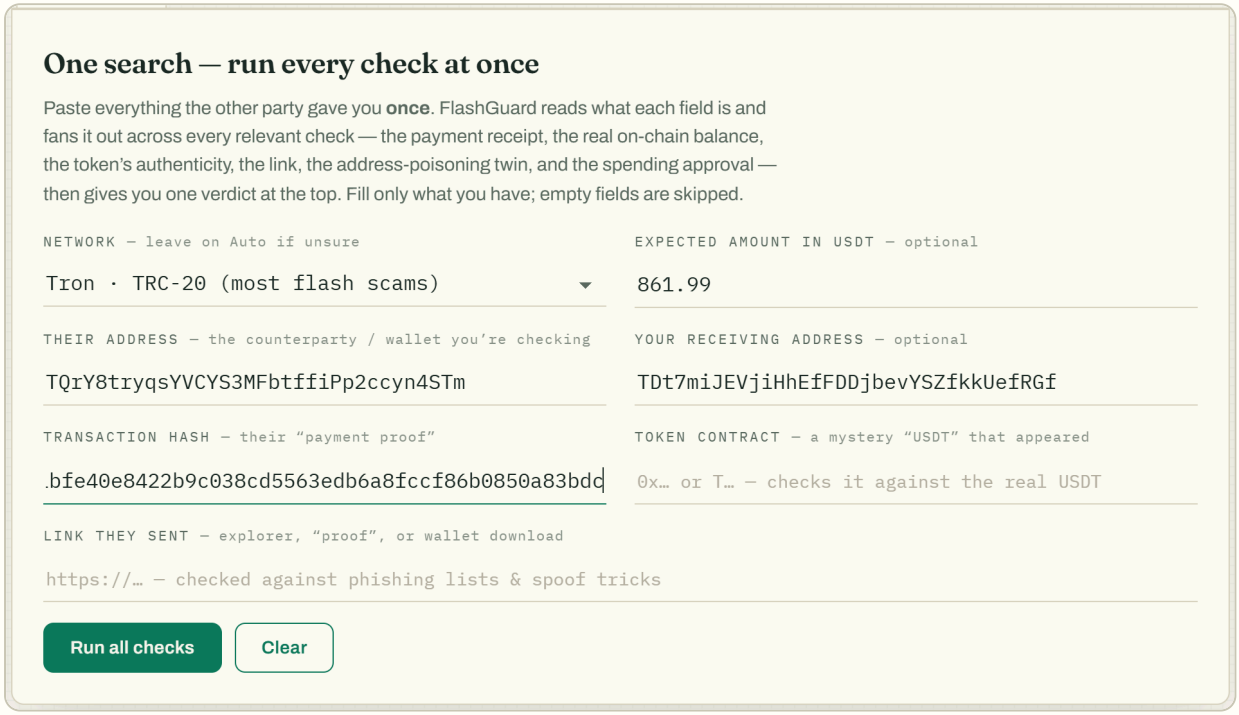
PART 7

Three true-to-life stories — with real photographs of the results

Story 1 — “I have already paid you, brother”

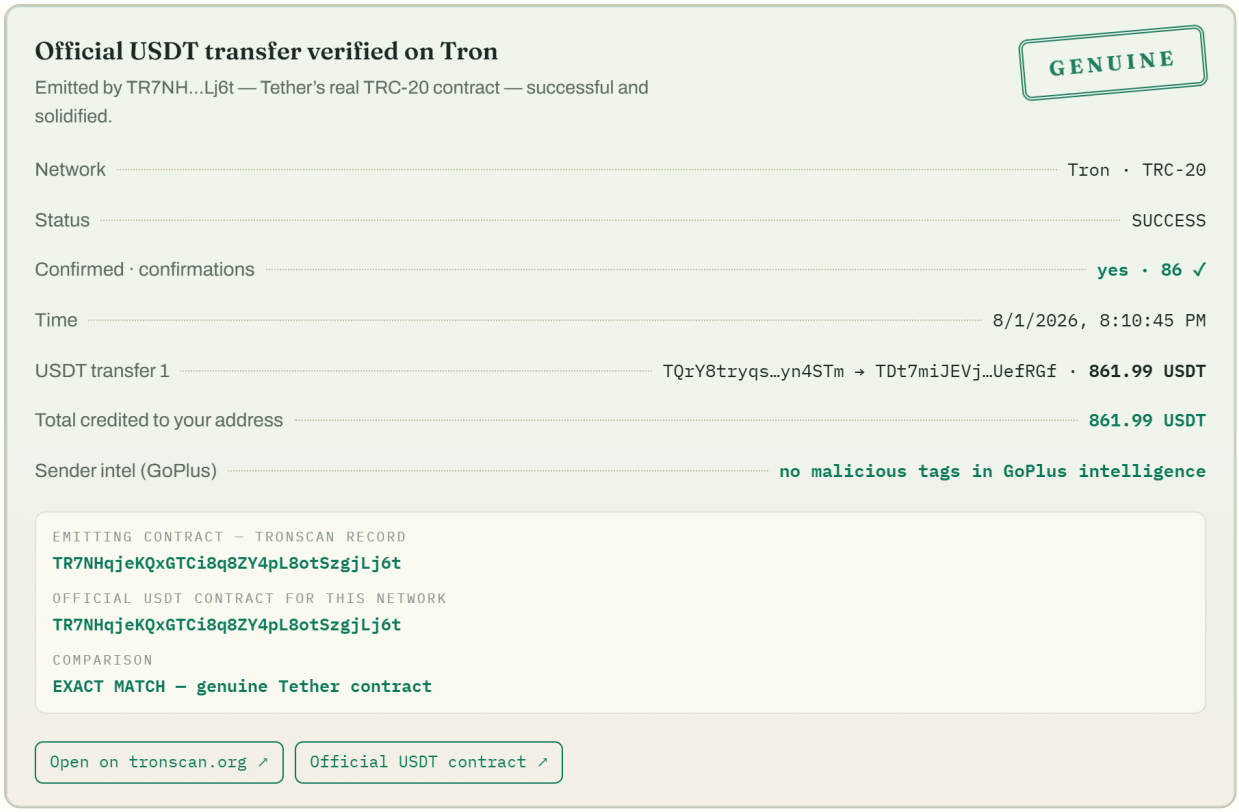
You are selling something. A buyer on WhatsApp sends a payment screenshot — green tick, USDT sent, network TRC20, a TxID at the bottom — and presses you to hand over the goods. You reply: *“please send the TxID as text”*, and you fill the boxes.

To photograph this story for you, we checked a **real payment** that had just happened on the public ledger — 861.99 USDT sent from a Binance exchange wallet. Here is the form, filled the way you would fill it:

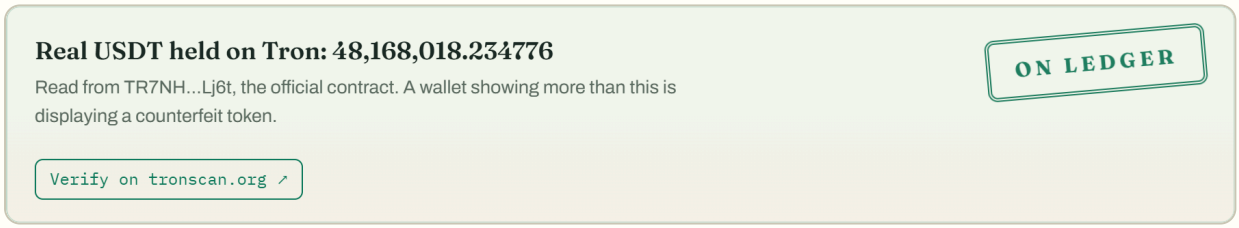


Picture 17 — the form filled in for Story 1. Network set to Tron · TRC-20 (the screenshot said TRC20), the claimed amount, their address (the sender), your address (the receiver), and the TxID pasted into the hash box. Token and link boxes stay empty — they will simply be skipped.

Press **Run all checks**. Because this payment was genuine, the banner came back green — exactly the Picture 15 you saw in Part 6 — and the detail cards prove each part:



Picture 18 — the Transaction card, stamped GENUINE. Read it like a receipt: SUCCESS, confirmed 86 times, 861.99 USDT credited to the receiving address, and at the bottom the contract that moved the money is compared letter-by-letter with the official one — **EXACT MATCH — genuine Tether contract**. A flash-USDT fake fails exactly here.



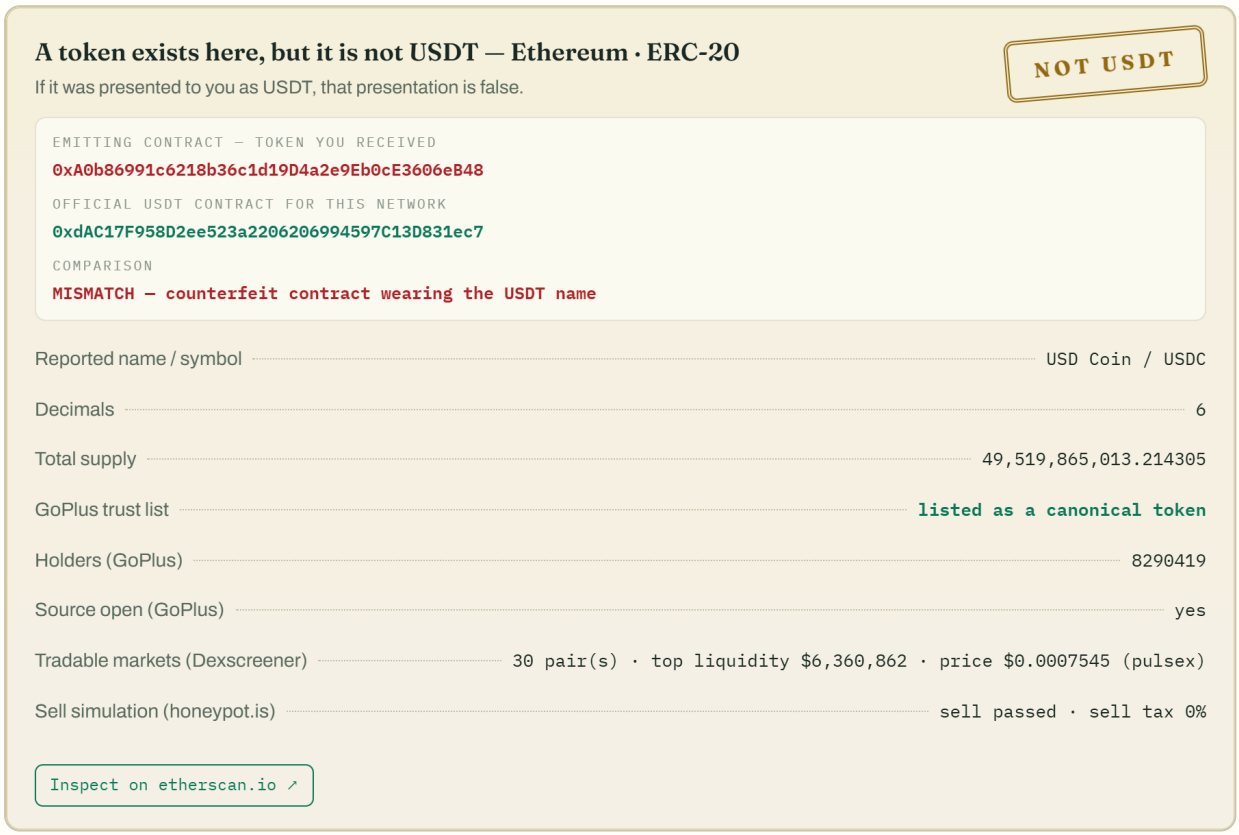
Picture 19 — the Real balance & reputation card for the sender: their true USDT holding read from the official contract, not blacklisted by Tether, no malicious tags, keys self-controlled. If a wallet *shows* more than this number, the wallet is displaying a counterfeit token.

If any of this had failed — hash not found, wrong recipient, amount 1.5 instead of 861.99, impostor contract — the banner would be the red Picture 13, and the answer to the buyer is silence.

Story 2 — money fell from the sky

You open your wallet and 50,000 “USDT” is sitting there from an unknown sender. Soon a message arrives: *“sent by mistake / pay 2% network charge to activate it.”*

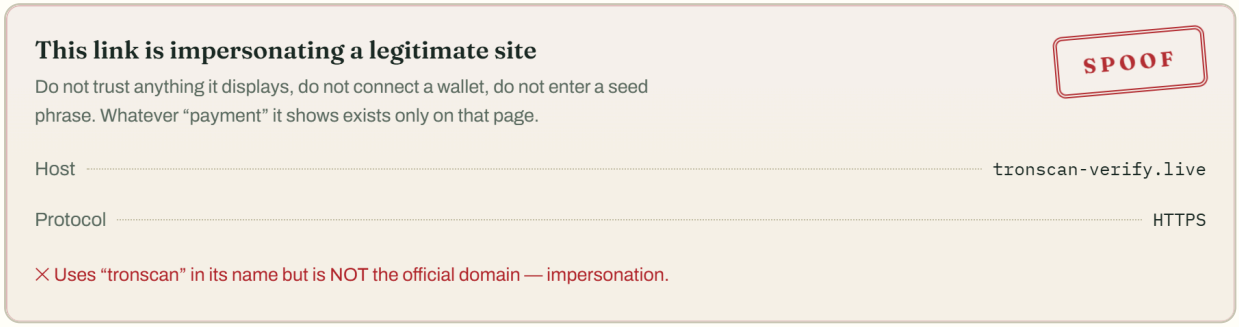
What you do: in Trust Wallet, tap the mystery token → the ⓘ info symbol → copy the **Contract** code → paste it into box ⑥ → Run. To photograph the result we pasted the passport of a different real coin that is *not* Tether — a scam token wearing the USDT name fails the same way:



Picture 20 — the Token contract card, stamped NOT USDT. The two passports are printed one above the other — the token you received versus the official USDT contract — and the comparison line says it plainly: **MISMATCH — counterfeit contract wearing the USDT name**. Whatever the wallet screen showed, this is not Tether. The 2% “charge” they want is the only real money in the story: yours. Do not touch the token, do not pay, do not reply.

Story 3 — “check the proof yourself, here is the link”

A Telegram “trader” sends `https://tronscan-verify.live/tx/…` — “see, the payment is right there on the blockchain!” The page looks exactly like tronscan. **Do not open it.** Press-and-hold the link → Copy → paste into box ⑦ → Run:



Picture 21 — the Link card, stamped SPOOF, and the top banner turns red (Picture 13). The card explains why: the site uses “tronscan” in its name but is not the official domain — impersonation. Whatever “payment” that page displays exists only on that page.

PART 8

The six iron rules

1. **A screenshot is not money.** Only a checked transaction hash is proof, and FlashGuard checks it in seconds.
2. **Real USDT never needs a fee to be “released”, “activated” or “unlocked”.** Anyone asking for such a fee is the scam itself.
3. **Never send anything of value first** — not goods, not gift cards, not a “refundable deposit” — before FlashGuard shows the payment confirmed on-chain.
4. **Copy, never type.** And take the codes as text — a genuine payer will happily send the TxID as text.
5. **Never open their links; paste them into FlashGuard instead.** And never, ever tell anyone your 12 secret words. No support person, no bank, no police officer will ever need them.
6. **Red banner = walk away.** Do not argue, do not give a second chance, do not let them “explain”. Silence is the correct reply to a cheat.

APPENDIX A

Recognise a code by its shape

When unsure what something is, match its shape here. If you guess wrong, nothing bad happens — FlashGuard says the format was not recognised, and you try the other box.

The code looks like…	It is probably…	Goes into box
`T` + 33 more letters/digits (34 total)	A Tron **wallet address**	③ or ④
`0x` + 40 characters (42 total)	An Ethereum-family **wallet address** (also BNB, Polygon…)	③ or ④
`0x` + 64 characters (66 total)	A **transaction hash** (receipt number)	⑤
64 characters, only `0-9 a-f`, no 0x	A Tron / TON **transaction hash**	⑤
`EQ…` or `UQ…`	A TON (Telegram) **address**	③ or ④
Ends in `.near`	A NEAR **address / contract**	③, ④ or ⑥
`KT1…` / `tz1…`	A Tezos **contract / address**	⑥ / ③ ④
`o` + about 50 characters	A Tezos **transaction hash**	⑤
Starts with `https://` or `www.`	A **link**	⑦
A plain number like `312769` beside the word Algorand	An Algorand **asset ID** (token passport)	⑥

APPENDIX B

The REAL USDT addresses — printed for your eyes

You never need to memorise or type these. FlashGuard already knows every one and does the comparison for you (you saw it doing so in Pictures 18 and 20). They are printed here for one reason: so you can hold a suspicious contract next to the genuine article and see the difference yourself. Compare the **first six** and the **last six** characters — if either differs, it is not Tether, whatever its name and logo say.

Network	The one and only genuine USDT contract

Tron (TRC-20) — most scams live here	`TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t`
Ethereum (ERC-20)	`0xdAC17F958D2ee523a2206206994597C13D831ec7`
BNB Smart Chain (BEP-20)	`0x55d398326f99059fF775485246999027B3197955`
Polygon PoS	`0xc2132D05D31c914a87C6611C10748AEb04B58e8F`
Solana	`Es9vMFrzaCERmJfrF4H2FYD4KCoNkY11McCe8BenwNYB`
TON (Telegram wallets)	`EQCxE6mUtQJKFnGfaROTKOt1lZbDiiX1kCixRv7Nw2Id_sDs`
Arbitrum One	`0xFd086bC7CD5C481DCC9C85ebE478A1C0b69FCbb9`
OP Mainnet (Optimism)	`0x94b008aA00579c1307B0EF2c499aD98a8ce58e58`
Avalanche C-Chain	`0x9702230A8Ea53601f5cD2dc00fDBc13d4dF4A8c7`
NEAR	`usdt.tether-token.near`
Aptos	`0x357b0b74bc833e95a115ad22604854d6b0fca151cecd94111770e5d6ffc9dc2b`
Tezos (FA2)	`KT1XnTn74bUtxHfDtBmm2bGZAQfhPbvKWR8o`
Algorand	Asset ID `312769`
Polkadot Asset Hub	Asset ID `1984`

FlashGuard also knows the newer “USDTo” rails (HyperEVM, Ink, Mantle, Berachain, Flare, Sei, Unichain, Conflux, Hedera, X Layer and more) and checks them automatically — you do not need their addresses on paper.

The last word. You do not need to understand blockchains, and you never will need to. You only need three habits: **copy** what they send you, **paste** it into One search, and **obey the colour**. Everything else is FlashGuard's job.