How to Identify a Fraudster

Fraudsters often lure individuals by offering the promise of substantial gains, high incomes, or cryptocurrency at inflated prices. This entices people to unknowingly send funds to fake accounts or fraudulent platforms. As a result, they may face difficulties when trying to withdraw their funds or receive what was initially promised. Unfortunately, this can lead to significant financial losses for those affected.

Friendly Reminder: We strongly advise against engaging in offline transactions due to unforeseen risks. Please stay alert throughout the transaction process. If you receive unsolicited project offers or suspicious file links via messaging apps such as WhatsApp, Telegram, or others, proceed with caution. Consider reporting or blocking such contacts to protect your personal assets and avoid falling victim to scams.

Common Communication Tools Used by Fraudsters

Fraudsters often use various communication channels to reach potential victims. Some of the most commonly used tools include:

- Website: Fraudsters may create fake websites that mimic legitimate entities, tricking users into sharing personal details or making financial transactions.
- **WhatsApp**: Fraudulent groups often contact potential victims via WhatsApp, spreading false information or engaging in scams.
  Note: We do not have any official WhatsApp groups. Be cautious of scams pretending to be official communication channels.
- **Telegram:** Fraudsters set up private Telegram chat groups to recruit victims or distribute misleading information.
- **Facebook:** Fake pages or accounts are created to conduct fraudulent promotions or connect with potential victims.

Common Fraudulent Tactics Used by Fraudsters

Here are some typical fraud tactics employed by fraudsters:

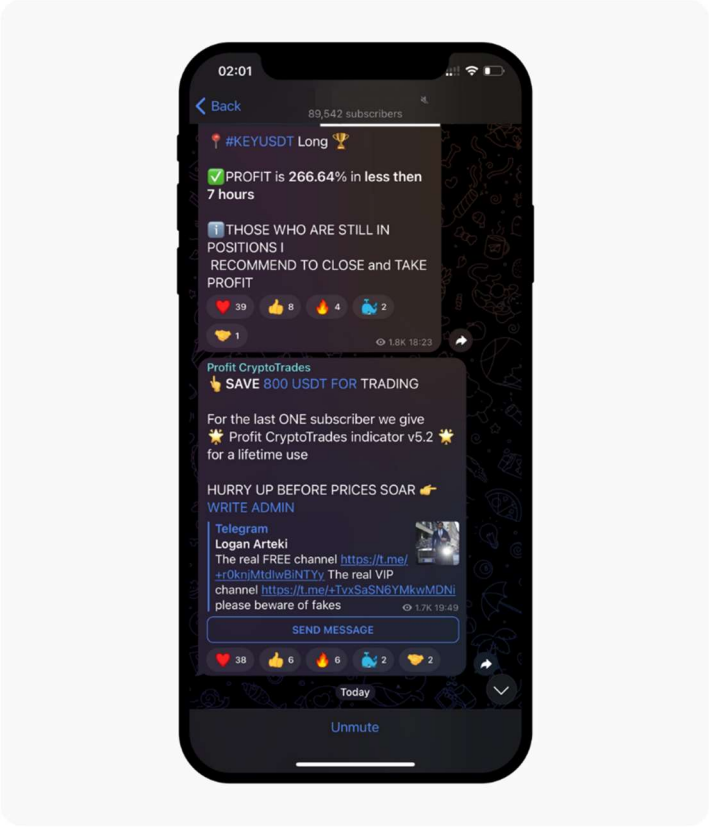
1. **Investment Scam:**

Fraudsters often reach out to users via private messages on messaging apps, claiming they can earn money through investments. They may switch to other messaging apps to communicate further, stating that investing a certain amount will yield profits. Initially, it may seem promising, but later on, the fraudster will change the terms, requesting users to pay more money to withdraw earnings. Ultimately, the user's

withdrawal requests will be denied under various pretenses.

For instance, someone might receive a message on Instagram from a stranger, claiming they can earn money by voting on car company ads. The conversation then moves to Telegram, where the fraudster convinces the user that a small investment will lead to higher returns. However, as the user attempts to withdraw their earnings, the fraudster changes the rules and demands additional payment, ultimately refusing to allow any withdrawals.

Some investment scams will start with fraudsters offering seemingly attractive opportunities, promising high returns. These opportunities can cover various assets like stocks, real estate, cryptocurrencies, and more. They often make unrealistic guarantees, emphasizing urgency and asking for confidentiality. They may also use fake information and present themselves as experts to lure unsuspecting investors.



Fraudsters offer attractive profit investment in Telegram

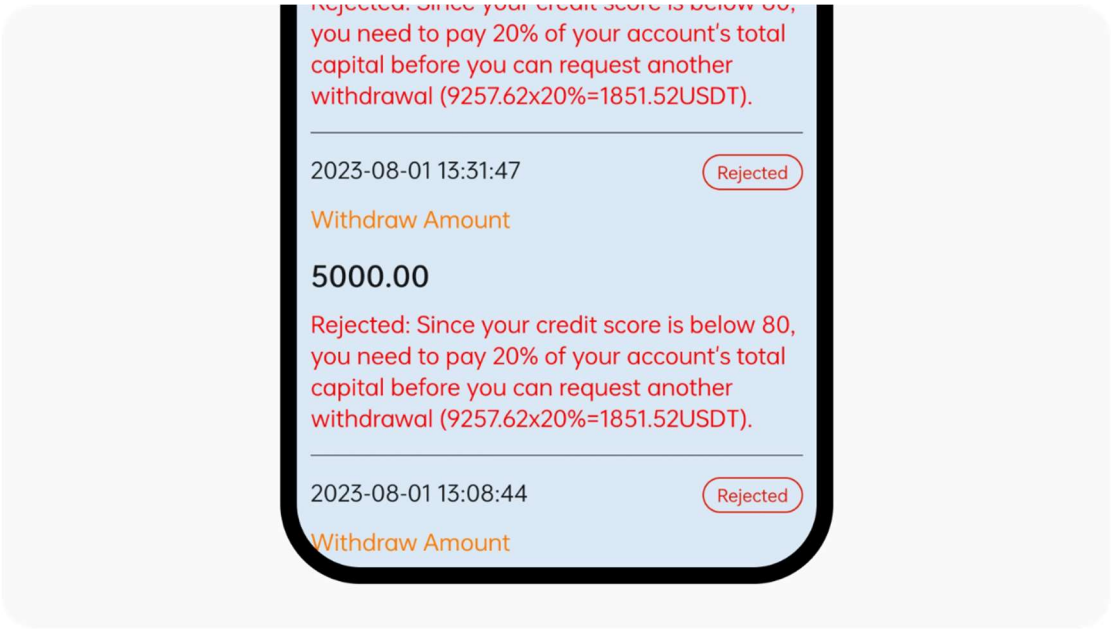
Another example is fraudsters on social media lure users with "free crypto" offers,

sharing wallet seed phrases and claiming to quit crypto. These are multi-signature wallets that the users can't control and they contain a small amount of valuable crypto but lack transaction fees. Once users pay these fees, the fraudster's script drains the wallet, leaving them empty-handed.

Note: never import unknown seed phrases or send your crypto assets to strangers.

2. **Transferring Funds to Fraudulent Platforms**

Fraudsters often entice users to transfer their funds to fake platforms by promising high returns. Initially, they may offer some small profits to build trust. However, once users invest larger amounts, the fraudsters will deny withdrawal requests using various excuses, such as citing a "low credit score," requiring an additional payment, or demanding a deposit before allowing any withdrawals.

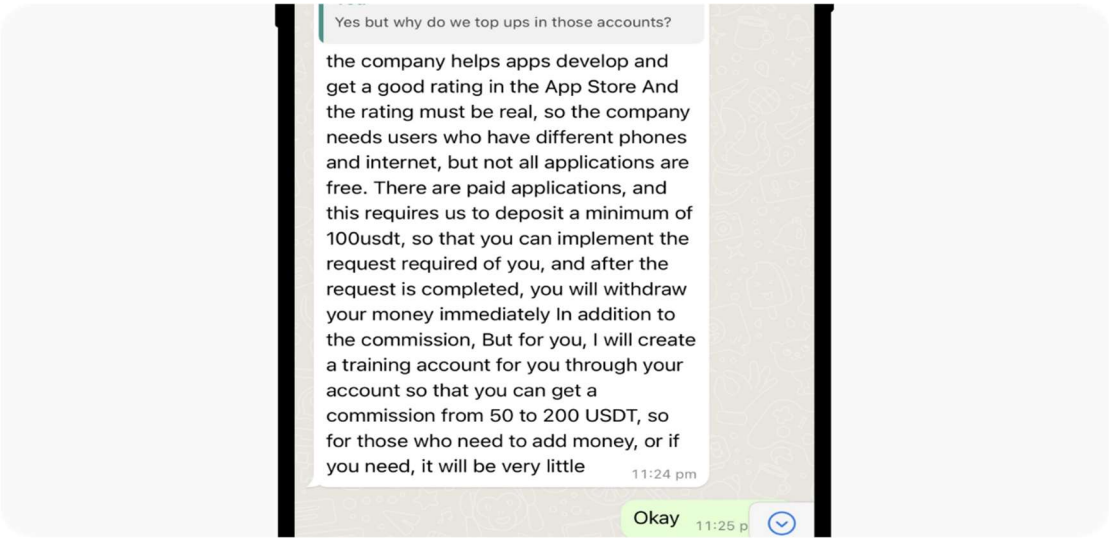


User withdrawal requests are being rejected and being requested to deposit more funds to increase the credit score

3. Working Fraud

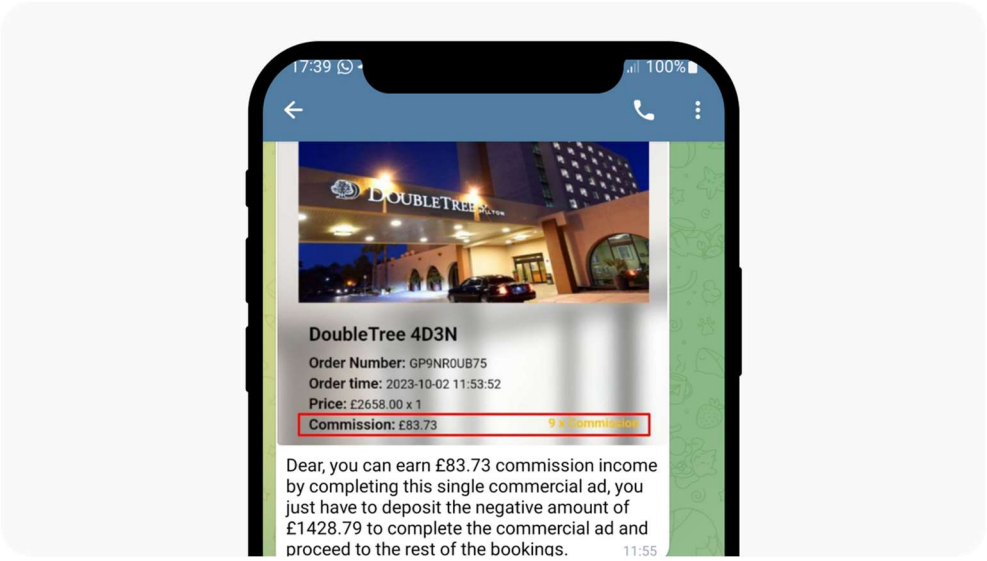
Fraudsters will lure users under the guise of high-profit earnings to deposit a small number of funds and earn a modest profit. However, as they progressively increase the deposited amount, if the user decides not to make additional deposits, their account will be frozen and they'll be prompted to deposit more funds in order to initiate a

withdrawal. For more details on the common working fraud, refer **here**.



Fraudsters offer attractive promotions to lure the user to deposit a small amount of funds and earn attractive profit

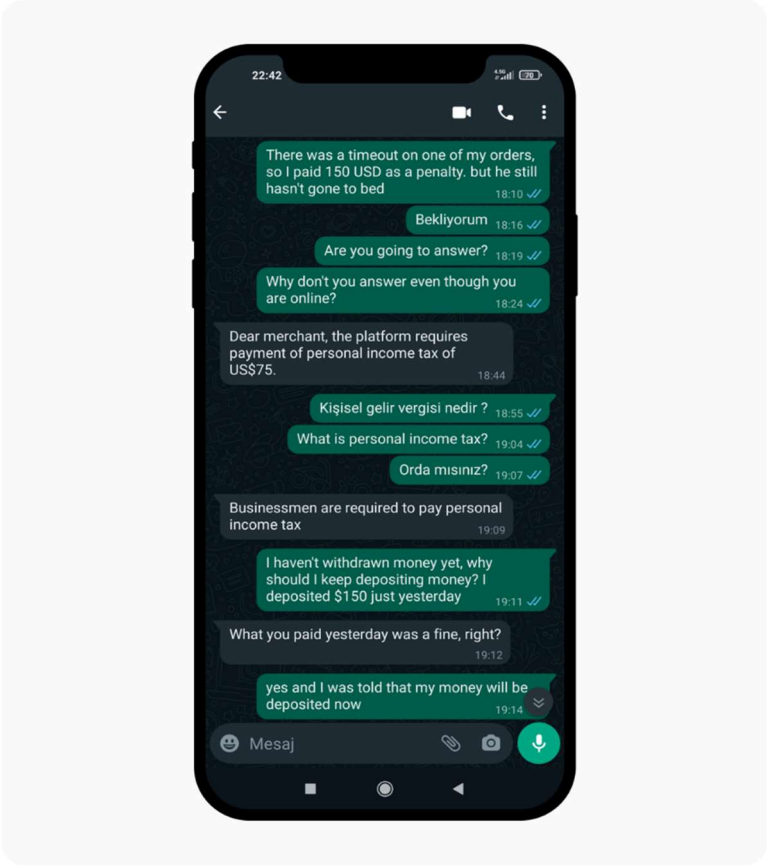
Some of the fraudsters will offer some easy, well-paying and flexible fake job opportunities which might include online marketing, data entry, product testing and others. They'll usually request upfront payment from the users, claiming it's the "training fee", "entrance fee" and other similar types of fees which are used to provide relevant training material or equipment. Once the upfront payment is made by the users, the fraudsters will assign some simple tasks to users, including posting online advertisements, filling in some surveys, clicking the provided links to complete the tasks, or other simple actions.



Fraudsters requested users to deposit a certain amount to complete the simple task

4. Impersonation Scam

Certain scammers pose as representatives from legitimate organizations, using counterfeit documents and logos to appear credible. They may offer services such as tax assistance or legal advice, requesting payment or personal information in return. In some cases, they resort to threats to intimidate individuals into handing over what they want. These scammers may ask for personal details, bank account information, or even money. Be cautious of phone scams as well, where fraudsters impersonate police officers or government officials, claiming you're in trouble and must provide them with sensitive information to avoid further issues.



Fraudsters pretend to be government officers requesting the user deposit more to pay for income tax.

5. Crypto gift scams

One of the latest tactics involves fraudsters using "gifts" or "bonus events" to deceive users into transferring funds. These scams may appear as legitimate opportunities to learn about trading or participate in exclusive promotions.

However, the end goal is always the same: to gain unauthorized access to your funds.

Here are some of the common methods used by fraudsters:

Fake trading education offers: The user reported being scammed while looking for investment trading education on Facebook. A fraudster reached out, instructed the user to call for a lesson, and asked them to share their phone screen. Under the pretense of providing education, the fraudster convinced the user to buy lithium tokens, promising a "gift" in return.

The fraudster then told the user to wait for a code, but soon after, the user noticed that their account funds had disappeared. When the user questioned the fraudster, the only response was, "Wait." As a new user, the victim was confused about how the "gift" ended up directly in the fraudster's wallet, as they had no intention of transferring any money.

Fake bonus events: The user reported falling victim to a scam through a deceptive interaction on Facebook. The fraudster promised a reward in return for entering a gift code. Trusting the offer, the user entered the code, only to find their account balance of 208U was drained.

Upon investigation, it was discovered that after the user deposited 208U, the funds were transferred to a trading account, converted to ETH, and then sent as a "gift" to the fraudster's wallet, all under the guise of a bogus "bonus event."