



WHAT WAS CHECKED

Pasted message

315 characters, analyzed on the visitor's device. The message text is not stored and is not included in this report.

HIGH RISK

RISK SCORE 100/100

High risk: stop before you send anything

We found signs that match known crypto scams. Don't send money or crypto, don't click links and don't connect your wallet.



3 serious red flags · 7 other warning signs · 5 checks run

! Stop: don't send money or crypto, don't click links and don't connect your wallet. If you already did, follow the steps below and contact your exchange or bank now.

What we found

HIGH

Guaranteed or unusually high returns

Real investments can lose money, and nobody can guarantee profits. Promises of fixed daily or weekly returns are a hallmark of Ponzi schemes and fake platforms.

Matched: "guaranteed 5% daily returns" "5% daily"

Source: Red-flag patterns

HIGH

Friendly stranger steering you toward a trading platform

"Pig butchering" scams start with a wrong-number text, dating match or social media friend who slowly builds trust, then shows you profits on a platform or app they recommend. The balance is fake and withdrawals never come.

Matched: "wrong number" "my uncle is a financial analyst and he shows me how to trade crypto"

Source: Red-flag patterns

HIGH

Link in message (coinbase-pro-secure.top): uses the name "Coinbase" but is not Coinbase's website

Coinbase's real website is coinbase.com. Sites that put a company's name inside a different domain are a common phishing trick.

Source: [Link structure](#)

CAUTION

Pressure to act right now

Scammers create a deadline so you act before you think or talk to someone. A real opportunity or a real problem will still be there after you take a day to check.

Matched: "Only 3 VIP spots left"

Source: [Red-flag patterns](#)

CAUTION

Link in message (coinbase-pro-secure.top): uses bait words in the domain

Words like "pro", "secure" in a domain name are common on fake support and wallet-draining pages.

Source: [Link structure](#)

CAUTION

Link in message (coinbase-pro-secure.top): no registration record found

We couldn't find a registration record for coinbase-pro-secure.top. Some country domains don't publish one, but a missing record can also mean the domain doesn't exist or was just taken down.

Source: [RDAP \(domain age\)](#) [about.rdap.org/](#)

CAUTION

Unsolicited contact

Most crypto scams start with a message from someone you don't know: a "wrong number" text, a DM, a dating match or a friendly comment.

Source: [Your answers](#)

CAUTION

You were asked to invest on a platform

Check that the platform is registered (FINRA BrokerCheck, SEC, or your state regulator) and that you found it independently.

Source: [Your answers](#)

MINOR

Wants to move you to WhatsApp, Telegram or another app

Moving to a private messaging app takes the conversation away from platforms that can detect and block scammers. On its own it is not proof of a scam, but it is a common first step.

Matched: "WhatsApp" "Add me on"

Source: [Red-flag patterns](#)

MINOR

Link in message (coinbase-pro-secure.top): uses a ".top" ending

Cheap domain endings like this are popular with scammers. Many legitimate sites use them too, so this is a minor sign.

Source: [Link structure](#)

What to do next

1 Stop and don't send anything

Don't send money or crypto, don't click links, don't connect your wallet and don't sign anything. Stop replying; block the sender if you can.

2 If you already sent money

Contact your exchange or bank immediately through its official app; sometimes transfers can be frozen if you act fast. Save screenshots, the addresses, transaction IDs and the conversation, then report it (links below).

3 Never share your recovery phrase

No real company, support agent or agency will ever ask for it, and The Crypto Guide never will either.

! Never share your recovery phrase

No exchange, wallet maker, support agent, government agency or "recovery" service will ever ask for your seed phrase, recovery words or private key. Anyone who has them can take everything. The Crypto Guide will never ask for them either.

Report it

FTC: ReportFraud.ftc.govreportfraud.ftc.gov

The Federal Trade Commission collects scam reports that help law enforcement spot patterns.

FBI: Internet Crime Complaint Center (IC3)www.ic3.gov

Report if you lost money or crypto. Include addresses, transaction IDs and screenshots.

Chainabusewww.chainabuse.com/report

Public scam-report database for crypto addresses and websites. Your report warns others.

Also tell your exchange or wallet provider through the support option in its official app.

Sources we checked

Red-flag patterns	MATCH	4 of 20 patterns
Link structure	ISSUE	issues found
MetaMask list	NO MATCH	not listed
Polkadot{.js} list	NO MATCH	not listed
RDAP (domain age)	ISSUE	not found

Address and link lookups were made from the visitor's browser to public sources: US Treasury OFAC SDN list (via github.com/0xB10C), ScamSniffer, Blockscout, mempool.space, MetaMask eth-phishing-detect, Polkadot{.js} phishing list and RDAP registry records. Pasted messages are analyzed on-device.

ONE-ON-ONE HELP

Not sure? Talk it through with an expert.

Book a private session: thecryptoguide.org/services

Weekly scam alerts in The Trail Report: thecryptoguide.org/newsletter

Important: This report is educational and automated. It is not financial, legal or investment advice. A "no major red flags" result is not a guarantee that something is safe; new scams appear every day and may not appear in any list yet. Results reflect public data at the time of the check. Provided free by The Crypto Guide (thecryptoguide.org).