CRYPTO · EXCHANGE SECURITY & INVESTOR TRUST

Do Crypto Investors Still Trust Exchanges After Major Hacks?

TU Research examines confidence in centralized cryptocurrency exchanges, security habits after major hacks, and how investors assess account protection and reserve disclosures.

67%
Consider centralized exchanges safe

64%
Report taking precautions after major hacks

39%
Correctly understand proof-of-reserves limitations

INSIDE THIS REPORT

01 Exchange confidence
02 Post-hack behavior
03 Account protection
04 Phishing awareness
05 Proof of reserves
06 Restoring investor trust

TU Research Team
A. Chabaniuk · C. Soni · C. Ryan

Methodology
CAWI · structured online survey

Sample
1,200 retail crypto investors

Contents

01	Executive Findings	2
02	Introduction & Research Questions	2
03	Institutional Validation	3
04	Theoretical Framework	3
05	Methodology & Research Team	4
06	Survey Results	4
07	Practical Implications	7
08	Data Sources & References	7

01 Executive Findings

TU

Investor confidence in centralized cryptocurrency exchanges remains substantial, but knowledge and preparedness vary. The 1,200-person research scenario indicates that trust can coexist with greater security awareness.

- 67% describe centralized exchanges as safe; 19% consider them unsafe.
- 64% report taking extra precautions after learning of major hacks.
- 38% choose the most comprehensive response to suspected account compromise.
- 74% use two-factor or stronger account authentication.
- 64% would independently verify suspicious alerts or contact official support; 28% would interact with a suspicious message.
- 69% primarily check official exchange channels for incident information.
- Only 39% understand that proof of reserves does not guarantee solvency or asset safety.
- 43% identify transparent reporting as the most important factor in rebuilding confidence.

02 Introduction & Research Questions

TU

Centralized exchanges simplify cryptocurrency trading and custody, but hacks, phishing, and fraudulent alerts can expose users to significant losses. The study examines whether security incidents change investors' trust and behavior, rather than assuming confidence necessarily disappears after a breach.

The research addresses eight questions:

- Do investors still trust centralized exchanges?
- Do major hacks encourage better security practices?
- Can investors respond effectively to suspected account breaches?
- Which authentication methods are used most often?
- Can investors identify fraudulent exchange security alerts?
- Where do investors verify reports of security incidents?
- Do investors understand proof of reserves?
- What would restore confidence after a major hack?

03 Institutional Validation

TU

Institutional evidence underscores both the continued use of crypto exchanges and the need for layered security. The FCA's Cryptoassets Consumer Research 2025 reported that 73% of UK cryptoasset users acquired assets through centralized exchanges, compared with 69% in 2024.

EY-Parthenon and Coinbase reported that 66% of surveyed institutional investors prioritized security and key-signing protocols when selecting custody providers in 2026, compared with 8% in 2025; 61% used multiple custodians.

TRM Labs counted 207 crypto hacks and exploits in the first half of 2026, up from 83 in the comparable prior-year period, although estimated losses fell from roughly $2.3 billion to $972 million. Chainalysis also documented substantial personal-wallet compromises during 2025.

IOSCO has recommended stronger custody safeguards. The PCAOB cautions that proof-of-reserves reporting alone does not establish financial stability or guarantee customer protection. These sources provide context; they do not directly measure the responses in this TU survey.

04 Theoretical Framework

TU

Investor trust and protective behavior are not opposites. A user may consider an exchange dependable while enabling authentication controls, monitoring withdrawals, and verifying security communications. A high-profile incident can prompt useful security changes, but urgency can also make fraudulent alerts more persuasive.

Prospect theory, developed by Kahneman and Tversky, helps explain why the prospect of losing assets may trigger rapid decisions. In the exchange-security setting, the important distinction is between measured precautions and hurried actions taken without verifying the source of a warning.

The survey therefore separates perceptions of platform safety from practical knowledge: recognizing phishing, choosing an appropriate first response to account compromise, understanding authentication, and interpreting reserve disclosures.

05 Methodology & Research Team

TU

The study uses a structured online questionnaire based on the CAWI methodology. Its research scenario covers 1,200 retail cryptocurrency investors aged 18–60 who used centralized exchanges in the previous 12 months, across North America, Europe, Asia, Latin America, Africa and the Middle East.

The survey explores perceptions of exchange safety, reactions to hacks, security practices, information verification and confidence-restoring measures. The source document does not specify a statistical confidence interval or margin of error; none is assumed here.

Research design and interpretation: Anastasiia Chabaniuk. Fact-checking and statistical validation: Chinmay Soni. Editorial and methodological supervision: Ciaran Ryan. Data collection and analysis: TU research team, including Andrey Mastykin and Oleg Tkachenko.

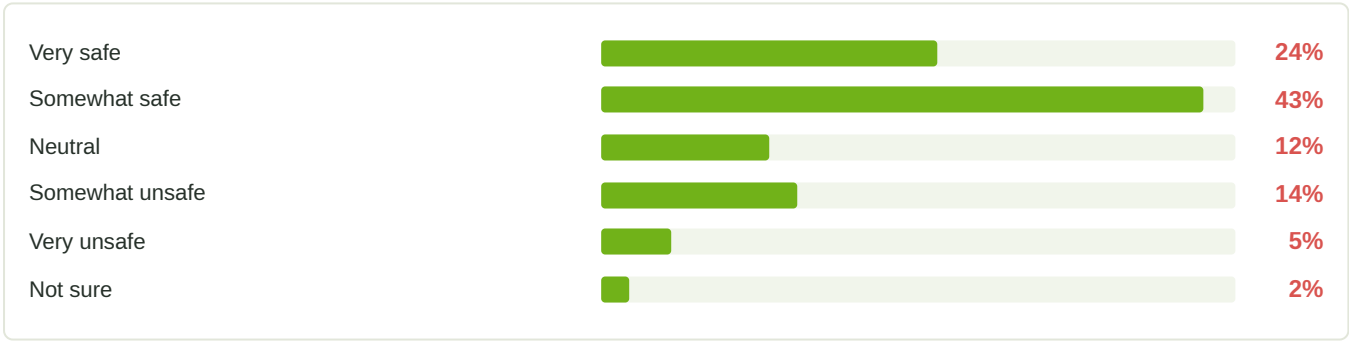
06 Survey Results

TU

Eight survey questions distinguish perceived safety from practical security preparedness. All figures below are shares of responses in the source research scenario.

Do crypto investors still consider centralized exchanges safe?

Overall perceived safety of centralized cryptocurrency exchanges.

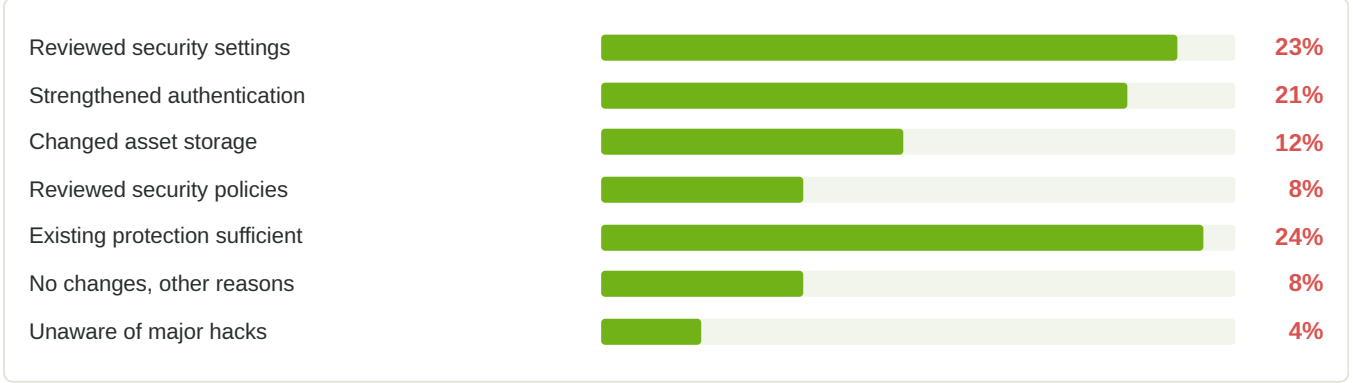


INSIGHT

A combined 67% consider centralized exchanges safe, versus 19% who consider them unsafe.

Do exchange hacks encourage investors to improve their security?

Security changes reported after major hacks in the preceding 12 months.

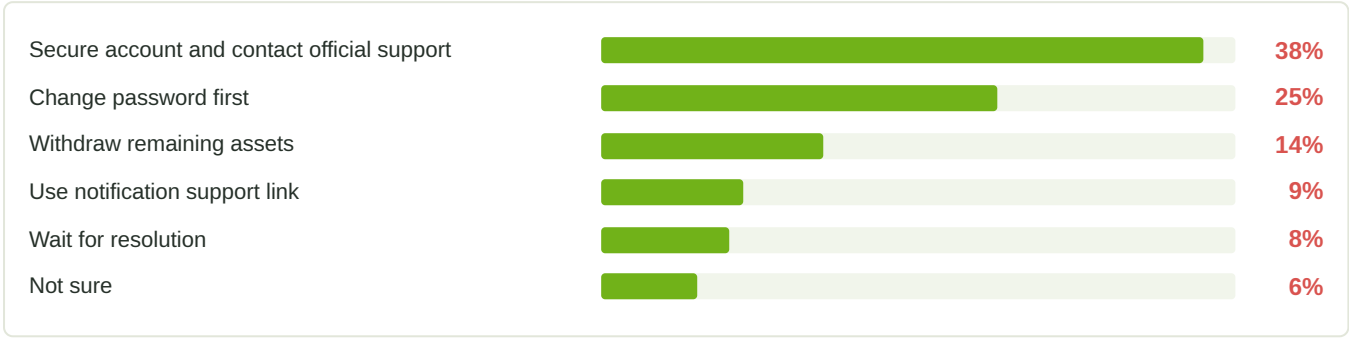


INSIGHT

64% report additional precautions, most commonly reviewing account settings and improving authentication.

Would crypto investors know what to do if their account was compromised?

First action after an unfamiliar login and attempted unauthorized withdrawal.

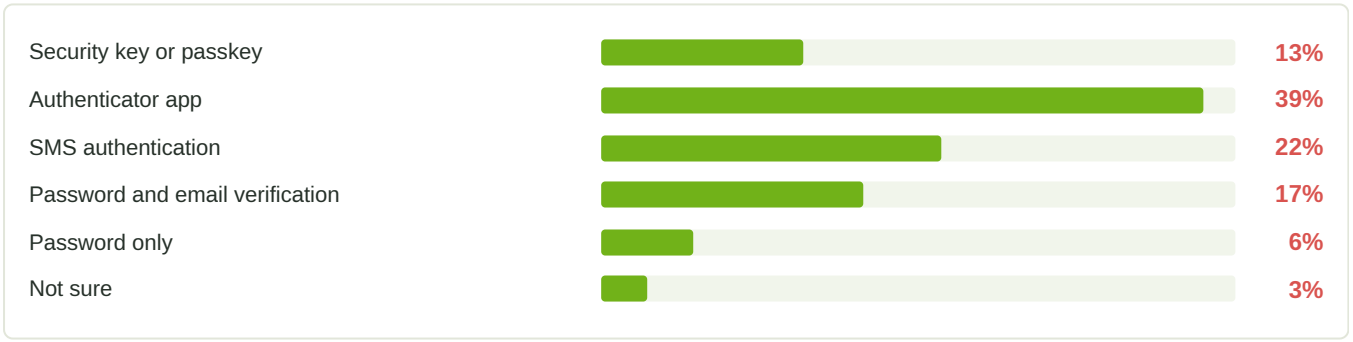


INSIGHT

38% select the most comprehensive response through verified channels; another 25% would first change their password.

Which security measures do investors use on their exchange accounts?

Strongest authentication method enabled on the primary exchange account.

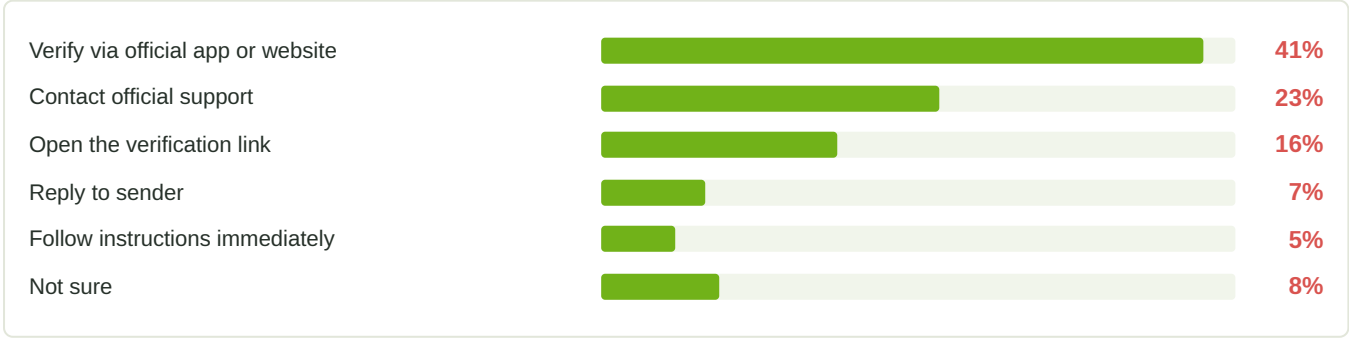


INSIGHT

74% report two-factor or stronger authentication; authenticator apps lead at 39%.

Can crypto investors recognize a fake exchange security alert?

Response to a suspicious urgent verification message.

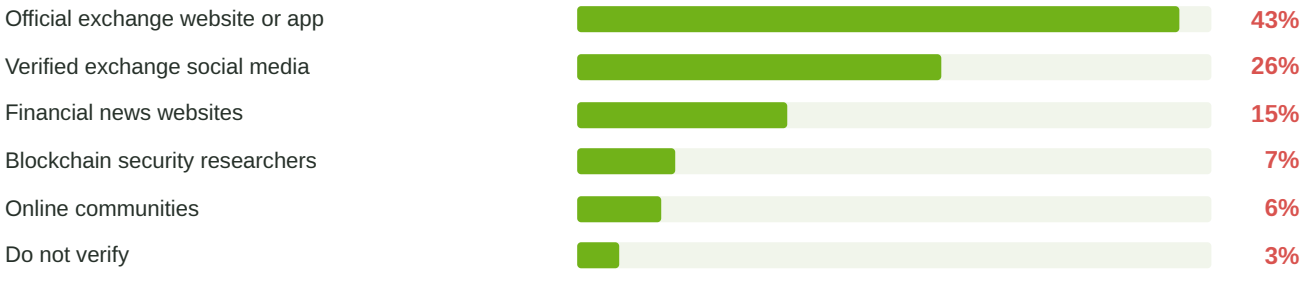


INSIGHT

64% would independently verify or contact official support, while 28% would engage with the suspicious message.

Where do investors verify information about exchange security incidents?

Primary source used to confirm an exchange hack.



INSIGHT

69% rely mainly on official exchange channels; verifying that a channel is authentic remains essential.

Do investors understand what proof of reserves actually means?

Understanding of what proof-of-reserves reports establish.

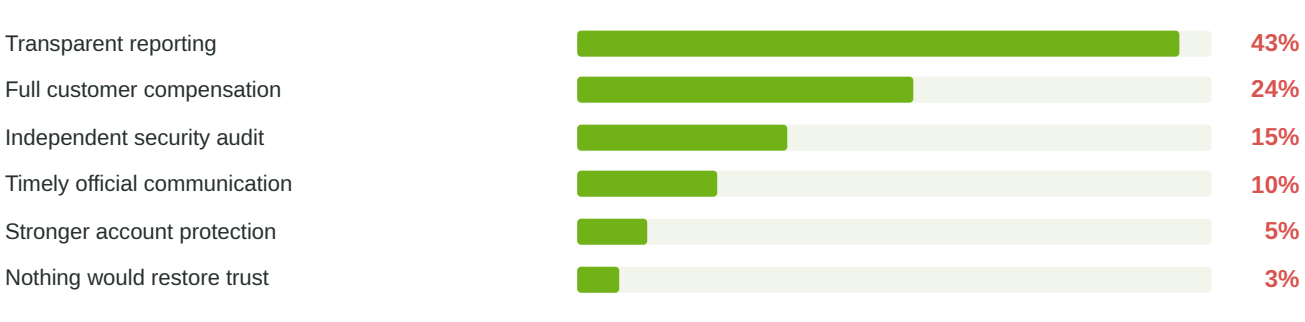


INSIGHT

Only 39% identify the limits of reserve disclosures; they do not guarantee solvency or future security.

What would help restore investor confidence after an exchange hack?

Most important factor when deciding whether to continue using an exchange.



> **INSIGHT**
>
> Transparent reporting ranks first at 43%, followed by customer compensation at 24%; only 3% say nothing would restore trust.

07 Practical Implications

TU

Exchange security requires both platform safeguards and informed user action. The following practices help reduce avoidable exposure without suggesting that any single measure eliminates risk.

- Use an authenticator app, security key or phishing-resistant passkey where available.
- Open exchange apps or previously saved addresses directly; do not follow unexpected security links.
- Learn account-locking, session management and official support procedures before an incident.
- Review withdrawal allowlists, confirmations and other sensitive-account controls.
- Verify major incident announcements using authenticated sources and reputable independent reporting.
- Do not send assets to addresses supplied in unsolicited support messages.
- Interpret proof of reserves alongside liabilities, custody and operational safeguards.
- Retain records of suspicious activity, but never share recovery phrases or authentication codes.
- Evaluate an exchange's remediation, independent assessments and communication after incidents.
- Maintain a personal security plan and review recovery settings regularly.

Exchange features and custody arrangements differ across platforms. Comparing those safeguards is useful, but no exchange or security feature can guarantee against losses.

08 Data Sources & References

TU

- Financial Conduct Authority (2025; updated 2026). Cryptoassets Consumer Research 2025.
- Financial Conduct Authority / YouGov (2025). Cryptoassets Consumer Research 2025 – Full Report.
- EY-Parthenon and Coinbase (2026). Institutional Investor Digital Assets Survey.
- TRM Labs (2026). H1 2026 Crypto Hacks Reach Record High as Losses Fall Below USD 1 Billion.
- Chainalysis (2026). 2025 Crypto Theft Reaches $3.4 Billion.
- International Organization of Securities Commissions (2023). Policy Recommendations for Crypto and Digital Asset Markets.
- Public Company Accounting Oversight Board (2023). Exercise Caution With Third-Party Verification/Proof of Reserve Reports.
- Financial Stability Board (2023). High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-asset Activities and Markets.
- Kahneman, D., and Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk.
- IdSurvey. CAWI Methodology.