

Cryptoemg.com

THE ESSENTIAL FIELD GUIDE

FREE CRYPTO SECURITY CHECKLIST

2026 EDITION

A practical, printable guide to securing accounts, recovery phrases, wallets, transactions and your response plan.



20 ACTIONS / 5-STEP SIGNING CHECK / PRINTABLE SCORECARD

01 / START HERE

Your security map

Four areas deserve separate attention. Work through them in order, then use the scorecard to revisit your setup.

01 IDENTITY

Email, exchange accounts, passwords and MFA

02 KEYS

Recovery phrase, offline backups and wallet devices

03 ACTIONS

Links, smart-contract approvals and transfers

04 RECOVERY

What to do when you spot a compromise

START WITH THE CRITICAL ITEMS

Complete the highlighted rows on pages 3 and 4 first.

02 / ACCOUNT CHECKLIST

Lock down your accounts

Secure your primary email first. Then apply these checks to every exchange and password manager you use.

**Use a unique, long password for every account**

Generate and store it in a reputable password manager.

**Turn on phishing-resistant MFA where available**

Prefer a passkey or security key; otherwise use an authenticator app.

**Secure your recovery methods**

Review recovery email, phone, trusted devices and backup codes.

**Review active sessions and withdrawal settings**

Remove unknown devices; enable alerts and allowlists where offered.

**Keep devices and wallet software updated**

Install updates from official sources and check app publisher names.

**Separate access to higher-value accounts**

Consider a dedicated email and avoid shared devices.

03 / WALLET CHECKLIST

Protect your keys

A recovery phrase can give someone control of a wallet. Never enter it into a site or share it with support.

**Keep the recovery phrase offline**

Never store it in email, a screenshot, cloud note or chat.

**Verify the backup before funding heavily**

Confirm each word and its order privately and accurately.

**Keep backups secure and separate**

Plan for theft, fire and accidental loss without advertising their location.

**Consider a hardware wallet for larger holdings**

Purchase from the maker or an authorized seller; verify on-device details.

**Separate daily-use and long-term wallets**

Keep experimental activity away from larger holdings.

**Prepare emergency access instructions**

Document the process without exposing the actual recovery phrase.

04 / TRANSACTION CHECK

Pause before you sign

A transfer or contract approval may be difficult to reverse. Run this short check every time.

1**OPEN**

Use a saved bookmark or official app. Avoid search ads for wallet access.

2**MATCH**

Check the network, full destination address and exact token.

3**READ**

Inspect the permission, spender and amount before confirming on your device.

4**TEST**

Send a small amount to a new destination and verify receipt.

5**REVIEW**

Check the transaction and revisit token allowances regularly.

05 / SCAM RADAR

Recognize the pressure

Slow down when a message promises profit, invents an emergency or asks you to leave an official channel.

**FAKE SUPPORT**

No legitimate support agent needs your recovery phrase or private key.

**GUARANTEED RETURNS**

Promises of profit and urgent deposits are warning signs.

**WALLET CONNECT TRAP**

Unexpected airdrops and mint links can request dangerous permissions.

**RECOVERY SCAM**

A demand for an upfront fee to retrieve lost crypto is a warning sign.

STOP. VERIFY THROUGH A SEPARATE OFFICIAL CHANNEL.

06 / EMERGENCY CARD

If something goes wrong

Use a trusted device and act promptly. Keep a copy of this page where you can access it during an incident.

01 STOP

Do not sign another request or send additional funds.

02 ISOLATE

Change email and exchange credentials; end unknown sessions.

03 CONTAIN

For an exposed phrase or key, move remaining assets to a new wallet created safely.
Revoking approvals does not repair an exposed key.

04 RECORD

Keep links, addresses, transaction hashes, messages and times.

05 REPORT

Contact providers through official channels and report to your local authorities. In the US, use IC3 and FTC.

07 / SCORECARD

My security scorecard

Tick only what you have verified. Repeat the check after a new wallet, device, exchange or suspicious message.

- ☐ Unique passwords on email and exchanges
- ☐ Passkey, security key or authenticator enabled
- ☐ Recovery methods and sessions reviewed
- ☐ Offline phrase backup checked privately
- ☐ Hardware wallet considered for larger holdings
- ☐ Official bookmarks and software updates done
- ☐ Full address, chain and permissions checked
- ☐ Small test transfers established
- ☐ Token approvals reviewed
- ☐ Emergency response details saved

COMPLETED: ____ / 10 NEXT REVIEW: _____

08 / REFERENCES

Sources & next steps

This guide is educational. Review product-specific controls and revisit guidance as security practices change.

FBI IC3 | 2025 Internet Crime Report

2025 US cryptocurrency investment fraud losses: \$7.2B.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

CISA | Use Strong Passwords

Password manager, strong passwords and MFA guidance.

<https://www.cisa.gov/secure-our-world/use-strong-passwords>

FTC | Cryptocurrency and Scams

Common scam patterns and reporting.

<https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams>

Ethereum.org | Trillion Dollar Security Project

Key management and approval risks.

<https://ethereum.org/reports/trillion-dollar-security/>

Ethereum.org | Scam Help & Reporting

Incident response and suspicious approvals.

<https://ethereum.org/community/support/scams/>

THE RISK IN CONTEXT

\$7.2B reported US crypto investment fraud losses in 2025 (FBI IC3).