Aegisum | Education

Crypto Security FAQ

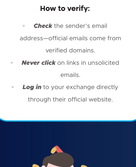
Protecting Your Digital Assets

Crypto security can be confusing, especially for newcomers. This FAQ answers the most common questions about protecting your assets, helping you stay informed and secure in the ever-evolving world of cryptocurrency.

1 What's the safest way to store my crypto?

A: The safest way is to use a hardware wallet (cold storage) because it keeps your private keys offline, making them inaccessible to hackers. If you must use a software wallet, enable 2FA, strong passwords, and secure backups.

2 What is a seed phrase, and why is it important?



A: A seed phrase (or recovery phrase) is a series of 12–24 words that acts as a master key to restore your wallet if you lose access. If someone gets your seed phrase, they can steal your funds.

—

How to protect it:

- ***Write it down*** on paper and store it securely.
- ***Never store*** it digitally (screenshots, notes, or cloud storage).
- ***Use a metal backup*** for fireproof and waterproof protection.

3 What should I do if I receive an email from my exchange or wallet provider asking for personal information?

A: Be suspicious! Exchanges will never ask for your password, private key, or seed phrase via email. This is a common phishing attack.

—

How to verify:

- ***Check*** the sender's email address—official emails come from verified domains.
- ***Never click*** on links in unsolicited emails.
- ***Log in*** to your exchange directly through their official website.

4 Can I recover lost or stolen crypto?

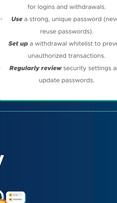
A: Unfortunately, crypto transactions are irreversible. If your funds are lost due to scams, phishing, or a compromised wallet, they cannot be recovered.

—

Prevention tips:

- ***Double-check*** addresses before sending crypto.
- ***Use a*** small test transaction before making large transfers.
- ***Only use*** trusted wallets and exchanges with strong security features.

5 How do I spot a fake crypto project or scam?



A: Scammers often lure investors with high returns, fake endorsements, and pressure tactics.

—

Red flags:

- ***Anonymous team*** with no verifiable background.
- ***Guaranteed profits*** or "risk-free" investments.
- ***No working*** product or only a vague whitepaper.
- ***No community*** engagement or locked liquidity.

Always do your own research (DYOR).

6 Is it safe to use public Wi-Fi for crypto transactions?

A: No! Public Wi-Fi is a hacker's playground—they can intercept your data and steal login credentials.

—

How to stay safe:

- ***Use a VPN*** to encrypt your internet connection.
- ***Only access*** wallets or exchanges from trusted, private networks.
- ***Enable*** hardware security keys (like YubiKey) for extra protection.

7 How can I keep my crypto safe from SIM swap attacks?

A: A SIM swap attack happens when hackers hijack your phone number to access your accounts.

—

Prevention tips:

- ***Never use*** SMS-based 2FA—use authenticator apps (Google Authenticator, Authy, or a hardware key).
- ***Set a PIN*** or passcode with your mobile carrier.
- ***Avoid*** sharing personal details online that could help hackers impersonate you.

8 What's the best way to secure my crypto trading account?

A: A secure trading account should have multiple layers of security.

—

How to stay safe:

- ***Enable*** Two-Factor Authentication (2FA) for logins and withdrawals.
- ***Use*** a strong, unique password (never reuse passwords).
- ***Set up*** a withdrawal whitelist to prevent unauthorized transactions.
- ***Regularly review*** security settings and update passwords.

Summary

Conclusion: Stay Informed, Stay Secure

Security is an ongoing process. The best way to protect your crypto is through knowledge, vigilance, and strong security practices.

Final Tip: Treat your crypto like cash—**once it's gone, it's gone.** Protect it as if your financial future depends on it!

Aegisum
Protecting the future of decentralized finance.

www.aegisum.com