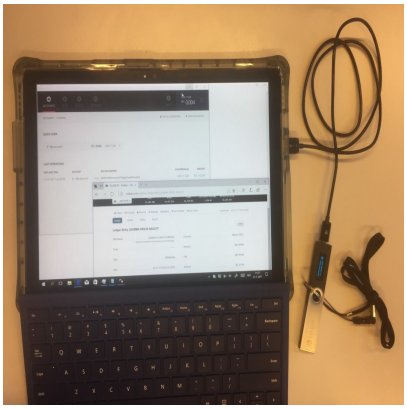

Cryptocurrency Scam Links: What a Wallet Signature Can Authorise

Description

A wallet signature is not always a harmless login. Depending on the request, it can approve a smart-contract permission that a scammer uses later to move tokens. SPFâ??s 1 July advisory also describes malicious video-call links and World Cup-themed ticket, token and streaming lures. Treat an unexpected signature request as a transaction decision, even when no amount appears on screen.

This guide is for a singapore crypto user who clicked a promotional, ticketing or investment link. It resolves one practical task: understand wallet-signature risk and contain exposure after a malicious interaction. It is desk-reported from the two cited primary sources and does not claim a field visit or professional advice.

Use this decision table first

Fact pattern	Practical result
Link opened; wallet not connected	Close it, clear permissions and inspect the device
Wallet connected; no signature	Disconnect the site and review recent sessions
Approval or permit signed	Revoke approvals and move remaining assets to a clean wallet if needed
Seed phrase exposed	Assume total wallet compromise and migrate from a clean device
Exchange credentials exposed	Freeze the account and reset security through the official app
Malware may be installed	Disconnect the device and contact SingCERT or qualified support

A signature can create future authority

Some token standards allow off-chain signatures that authorise spending later. The interface may show a login, verification or free mint while the data grants a permit. Inspect the domain, contract, token, spender and expiry; if those details are unavailable, reject the request. The controlling reference is SPF

cryptocurrency scam advisory.

Themes change faster than the mechanics

SPF cites fake tickets, tokens, livestreams and video-call links around major events. The same structure appears in airdrops, support chats and investment groups: urgency moves the user from a familiar platform to an attacker-controlled page, then asks for software, credentials or a wallet action.

Revoke permissions from a trusted route

Use the walletâ??s official approval manager or a well-established explorer reached independently, not a revocation link sent by the person who alerted you. Removing a site connection is not always the same as revoking an on-chain allowance. Check both and retain transaction hashes.

A seed phrase changes the incident level

Anyone with the recovery phrase can recreate the wallet. Revoking one approval is insufficient. From a known-clean device, create a new wallet with a new seed, transfer remaining assets carefully and retire the compromised addresses. Never type the old seed into a website promising recovery. Cross-check the operational detail against SingCERT Cyber Aid.

Secure centralised exchanges separately

If exchange credentials or one-time codes were exposed, contact the exchange through its official channel, freeze withdrawals and replace passwords and second-factor methods. Check email forwarding rules because control of the email account can undermine later resets.

Preserve evidence before accounts disappear

Record domains, usernames, wallet addresses, transaction hashes, chat exports and payment references. Report to Police and, for cyber compromise, SingCERT. Blockchain transactions may be irreversible, but fast reports can support exchange freezes and broader disruption.

A worked decision

A fan follows a fake match-stream link, connects a wallet and signs a gasless permit. No token moves immediately, but the permit may remain usable. The correct response is to revoke the approval from a trusted interface, move valuable assets if uncertainty remains, inspect the device, preserve the signed transaction and report the lureâ??not to wait for a theft notification.

Complete these checks in order

1. Disconnect from the suspicious site and network if malware is possible.

2. Freeze any affected exchange account.
3. Review and revoke token approvals from a trusted route.
4. Move assets to a new clean wallet if the seed or signing environment is compromised.
5. Reset email and account security from a clean device.
6. Preserve domains, chats, addresses and transaction hashes.
7. Report to Police and SingCERT as applicable.

For other current public-service tasks, see our public-transport savings guide and Climate Vouchers spending guide. Those pages answer distinct downstream questions and do not replace the authority rules cited here.

Common mistakes to avoid

- Assuming no gas fee means no authority was granted
- Only disconnecting the site without revoking approvals
- Entering a seed phrase into a recovery page
- Using the compromised device to create the replacement wallet
- Deleting chats before preserving identifiers

Keep a dated file containing the source pages, submitted forms, approvals, signed agreement and calculations. Rules, service interfaces and temporary concessions can change. Recheck the authority page immediately before acting, especially when the transaction will occur after a published end date or involves an unusual use, payment or occupier.

Make the decision easy to revisit

Before acting, write down the date, the fact that determines the outcome and the source page used. For this question, the decision is whether to understand wallet-signature risk and contain exposure after a malicious interaction. The two practical tools aboveâ??a six-level incident matrix from opened link to seed exposure and a no-immediate-loss permit example showing why users must revoke before waitingâ??are intended to make that reasoning visible. Save the result with receipts, confirmations or screenshots generated by the official service. If a deadline, amount, status, traveller, employee, property or health circumstance changes, rerun the decision from the beginning instead of editing the old answer from memory. Where a professional adviser, agency officer or service provider gives a different answer, ask which current rule and which facts produce the difference. That short record is valuable when two family members, colleagues or counterparties otherwise remember the same conversation differently.

Questions readers ask

Can a signature move funds later?

Yes. SPF warns that a permit signature can authorise a future transfer, depending on what was signed.

Is disconnecting the wallet enough?

Not necessarily. Site sessions and on-chain token approvals are different controls.

What if my seed phrase was revealed?

Treat the wallet as fully compromised and migrate assets using a clean device and a new seed.

Primary references and limits

SPF cryptocurrency scam advisory and SingCERT Cyber Aid were checked on 17 July 2026. The article applies their published general rules to the examples above. It does not determine an individual application, resolve a contractual dispute or replace legal, tax or regulated advice.

Date Created
17/07/2026
Author
claratan