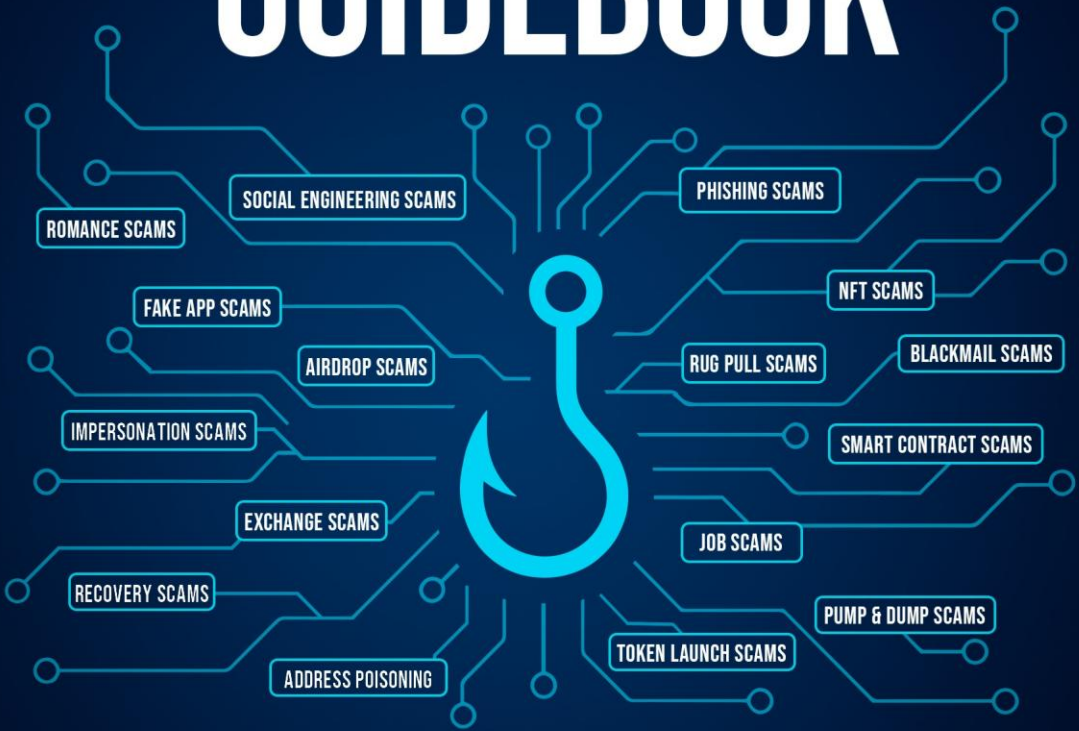
2026 EDITION

THE CRYPTO AND WEB3 SCAMS PREVENTION GUIDEBOOK



Spot and Stop Crypto Scams: Your Guide to Protecting Digital Assets in Decentralized Ecosystems

JUAN PABLO RENEDO

The Crypto and Web3 Scams Prevention Guidebook

Spot and Stop Crypto Scams: Your Guide to Protecting Digital Assets in Decentralized Ecosystems

2026 Edition

Juan Pablo Renedo

CryptoSafetyFirst.com

Copyright and Disclaimer

2026 Edition (version 2026.1, content reviewed October 2026). First edition 2025.

Copyright © 2025–2026 Juan Pablo Renedo. All rights reserved.

Published by Juan Pablo Renedo, c/o Block Services, Stuttgarter Str. 106, 70736 Fellbach, Germany · contact@cryptosafetyfirst.com

No part of this publication may be modified, sold, included in paid products or services, or reproduced in excerpts without the prior written permission of the publisher. You may share this guide free of charge, in its complete and unmodified form, including this copyright notice. Any other reproduction, distribution or modification of this work, including the copying of images, text or other materials, may infringe the author's rights under the German Copyright Act (UrhG) and may result in legal consequences, including warnings with costs and claims for damages under §§ 97, 97a UrhG. Statutory exceptions such as quotation (§ 51 UrhG) remain unaffected. This guide is offered as a free download from CryptoSafetyFirst.com, where the current version is always available.

Disclaimer of liability. The author and publisher make no representations or warranties regarding the accuracy, completeness, or timeliness of the information contained in this book. While every effort has been made to ensure reliability, to the extent permitted by law, no liability is assumed for any direct or indirect damages, losses, or consequences resulting from the use of the information presented. This does not apply to intent, gross negligence or injury to life, body or health.

This book is intended for educational and informational purposes only. The views expressed reflect the author's personal perspective and are not financial advice, investment recommendations, or legal counsel. Nothing in this publication constitutes financial, tax, legal, or investment advice under any regulatory framework, including the German Securities Trading Act (WpHG). Readers should do their own research and consult a qualified professional before making financial or investment decisions.

This publication may refer to third-party websites, products and services. The author and publisher are not responsible for their content, availability or accuracy, and a mention is not an endorsement. Trademarks and brand names belong to their respective owners. Scenarios in this book are illustrative unless stated otherwise; any resemblance to specific individuals is coincidental.

Contents

Copyright and Disclaimer 3
Contents 4
About This Edition 8
How to Use This Book 9
If You Think You May Have Been Scammed 11
Social Engineering Scams 17
1.1 How scams work: seven triggers 18
1.2 The pattern behind almost every scam 19
1.3 Social engineering scams to watch for 19
1.4 Illustrative scenario: the “free wallet” trap 22
1.5 How to protect yourself 23
1.6 CSF rules for this chapter 24
1.7 If this just happened to you 24
Impersonation Scams 26
2.1 Impersonation scams to watch for 27
2.2 How impersonators work 31
2.3 Illustrative scenario: the “security team” call 31
2.4 How to protect yourself 32
2.5 CSF rules for this chapter 32
2.6 If this just happened to you 33
Phishing Scams 35
3.1 Phishing scams to watch for 36
3.2 Wallet-connected phishing: approvals, signatures and drainers 39
3.3 Practical exercise: spot the phishing email 39
3.4 How to protect yourself 40
3.5 CSF rules for this chapter 40
3.6 If this just happened to you 41
Fake Apps and Wallets 43

4.1 Fake apps and wallets to watch for 44
4.2 Why a hardware wallet does not fix a fake setup 47
4.3 Illustrative scenario: the trading helper extension 47
4.4 How to protect yourself 48
4.5 CSF rules for this chapter 49
4.6 If this just happened to you 49
Malicious Contracts and Approvals 51
5.1 Approvals and signatures in plain English 52
5.2 Malicious contract scams to watch for 52
5.3 Illustrative scenario: the MEV bot tutorial 54
5.4 How to protect yourself 55
5.5 CSF rules for this chapter 55
5.6 If this just happened to you 56
Address Poisoning Scams 58
6.1 How address poisoning works 59
6.2 Variants to watch for 59
6.3 Illustrative scenario: the exchange deposit 59
6.4 How to protect yourself 60
6.5 CSF rules for this chapter 61
6.6 If this just happened to you 61
Giveaway and Airdrop Scams 63
7.1 Giveaway and airdrop scams to watch for 64
7.2 Unexpected tokens in your wallet 66
7.3 Illustrative scenario: the token with a website in its name 67
7.4 How to protect yourself 67
7.5 CSF rules for this chapter 68
7.6 If this just happened to you 68
Fake Investment Platforms 70
8.1 Fake investment platforms to watch for 71
8.2 The withdrawal trap 73

8.3 Signals that are not proof 73
8.4 Illustrative scenario: the profitable account 74
8.5 How to protect yourself 75
8.6 CSF rules for this chapter 75
8.7 If this just happened to you 76
Token Scams 77
9.1 Token scams to watch for 78
9.2 Signals that are not proof 81
9.3 Illustrative scenario: the community memecoin 81
9.4 How to protect yourself 82
9.5 CSF rules for this chapter 82
9.6 If this just happened to you 83
Romance Scams 84
10.1 Romance scams to watch for 85
10.2 The stages of a romance investment scam 87
10.3 Illustrative scenario: the wrong number 88
10.4 How to protect yourself 89
10.5 CSF rules for this chapter 89
10.6 If this just happened to you 89
Job and Task Scams 91
11.1 Job and task scams to watch for 92
11.2 How task scams trap you 94
11.3 Illustrative scenario: the optimization job 94
11.4 How to protect yourself 95
11.5 CSF rules for this chapter 95
11.6 If this just happened to you 96
Blackmail and Extortion Scams 98
12.1 Blackmail and extortion scams to watch for 99
12.2 Bluff or real? What to check 101
12.3 Illustrative scenario: the old password 101

12.4 How to protect yourself 102
12.5 CSF rules for this chapter 102
12.6 If this just happened to you 103
Recovery Scams 104
13.1 Recovery scams to watch for 105
13.2 What legitimate help looks like 107
13.3 Illustrative scenario: the recovery dashboard 108
13.4 How to protect yourself 109
13.5 CSF rules for this chapter 109
13.6 If this just happened to you 110
CSF Rules Index 111
Keep Learning 113

About This Edition

The first edition of this guide described sixteen scam categories. Since then, scams have changed, and so has what CryptoSafetyFirst knows about them. Every week, CSF collects and classifies real incidents reported by crypto users. The 2026 Edition is rebuilt around what that work shows.

What is new

- **Thirteen chapters that match how scams actually happen.** The chapters follow the CSF incident taxonomy, so the book, the website and the CSF assessment tools use the same categories.
- **A "Start here" section** for anyone who thinks they may have been scammed. It tells you what to do based on what you actually did: viewed, connected, approved, signed, sent, exposed your recovery phrase or installed something.
- **New chapters** on impersonation, address poisoning and recovery scams.
- **CSF rules in every chapter**, with one main rule per scam type and the supporting rules behind it.
- **Corrected and updated advice**, including the difference between disconnecting and revoking, what hardware wallets can and cannot do, and why some reassuring signals are not proof.

How examples and data are handled

- Scenarios are **illustrative** unless clearly stated otherwise. They show real patterns without naming real people, projects or loss figures.
- The book contains no incident statistics, so its advice stays valid as the numbers change. Examples are generic or illustrative unless stated otherwise.
- This edition uses CSF Rules v2, published at CryptoSafetyFirst.com.
- Tools and services are named only as examples and were checked in October 2026. Services change; when in doubt, go to the provider's official website yourself.

How to Use This Book

If you…	Go to
think you may have been scammed right now	**Start here: If You Think You May Have Been Scammed**, then the chapter for your scam.
want to understand how scams work	**Chapter 1**: the seven triggers and the five-step scam pattern behind almost every scam.
want to protect yourself from a specific scam	The chapter for that scam (see the chapter map below).
want to set up your wallets safely	The **Three-Wallet Model** guide (free at CryptoSafetyFirst.com). This book uses its terms: Vault, Frequent Use wallet and Disposable wallet.

Where to start

How each chapter works

Every chapter follows the same structure, so you can find what you need quickly: an at-a-glance infographic, the scams to watch for with red flags and how to avoid them, an illustrative scenario, how to protect yourself, the CSF rules for that scam, and **If this just happened to you**, with first actions for that chapter. Each chapter ends with a link to its page on CryptoSafetyFirst.com.

Ch	Chapter	Often combined with	Main CSF rule
1	Social Engineering Scams	All chapters (how scams work)	SDR-001
2	Impersonation Scams	3, 4, 12, 13	SDR-004
3	Phishing Scams	2, 5, 7	SDR-009
4	Fake Apps and Wallets	3, 11; Hackers guide (malware)	TSR-001
5	Malicious Contracts and Approvals	3, 7, 9	GR-004

Ch	Chapter	Often combined with	Main CSF rule
6	Address Poisoning Scams	User Mistakes guide (wrong address)	OR-005
7	Giveaway and Airdrop Scams	2, 3, 5	SDR-005
8	Fake Investment Platforms	9, 10, 11, 13	SDR-003
9	Token Scams	5, 7, 8	SDR-007
10	Romance Scams	8, 12, 13	SDR-006
11	Job and Task Scams	4, 8, 13	SDR-002
12	Blackmail and Extortion Scams	2, 10; Hackers guide (physical threats)	GR-005
13	Recovery Scams	2, 8, 10, 11	SDR-010

Chapter map: how the scams connect

Scams rarely come alone. A romance contact leads to a fake investment platform; a loss leads to a recovery scam; a fake job leads to malware. The chapter map shows the most common combinations, so you can read the chapters that belong together.

START HERE

If You Think You May Have Been Scammed

What you should do next depends on **what actually happened**. Visiting a suspicious website is not the same as connecting a wallet. Connecting a wallet is not the same as approving a token, signing an authorization, sending a transaction, exposing your seed phrase or installing malware.

Find the row that matches what you did. Each row says what to do now and what that action cannot fix.

What happened	What to do now	What this does not fix
You only saw a suspicious website, message, ad or unexpected token	Close it. Do not click links, download files, connect a wallet, sign or reply. Report the message or account to the platform. You can hide an unexpected token, but do not try to sell, swap or claim it.	Viewing alone does not compromise your wallet. If you did any of the things below, follow that row as well.
You connected your wallet but did not approve, sign or send anything	Disconnect the site in your wallet's connected-sites settings. Check carefully whether you also approved, signed or sent something; if so, follow those rows.	Disconnecting ends the site's session. It does not remove token or NFT approvals already recorded on the blockchain.
You approved a token or NFT permission	From a trusted device, open your wallet's approval list or a reputable approval checker (type its address yourself) and revoke the suspicious approval. Revoking costs a small network fee. Check for unauthorized transfers. If assets are already leaving the wallet, moving the remaining assets to another wallet you control can be faster than revoking approvals one by one.	Revoking stops future use of that permission. It does not return anything already taken.

What happened	What to do now	What this does not fix
You signed a message or authorization	Find out what you signed: check the request on the site and your wallet's activity. Some signatures (for example Permit-type token authorizations) let someone move tokens later without a separate approval transaction. If you cannot tell what you authorized, stop using that wallet for new activity and move the remaining assets to another wallet you control.	A signature cannot be undone. Revoking only helps if the signature created a permission that can be revoked.
You sent a transaction or transfer (to a scammer, a wrong address or a poisoned address)	Look the transaction up on the correct block explorer and save the transaction hash. If the funds went to an exchange deposit address, contact that exchange immediately through its official app or website; it may be able to freeze funds it controls. Report the incident (see Reporting below).	A confirmed self-custody blockchain transfer generally cannot be reversed. Nobody can pull it back for a fee.
You exposed your seed phrase or private key	Treat the wallet as permanently compromised. On a trusted, clean device and with wallet software from the official source, create a new wallet with a new recovery phrase, then move the remaining assets to it. Move assets from every network and account created from that phrase. If any coin you send for fees disappears at once, a bot is sweeping the wallet – stop sending more. If malware may be involved, do this from a different device. Never reuse the exposed phrase.	Changing a password or PIN, revoking approvals or deleting a digital copy of the phrase does not make it secret again. A hardware wallet set up with the exposed phrase is compromised too.

What happened	What to do now	What this does not fix
You installed suspicious software, or your device may have malware	Stop using that device for crypto, email and banking. From a different, trusted device, change important passwords (email first, then exchanges) and sign out other sessions. If you ever typed or stored a seed phrase on the infected device, follow the seed-phrase row from the clean device. Have the infected device cleaned or reset before using it again.	A malware scan can miss threats, and it does not make passwords or seed phrases that were already exposed safe again.
Your exchange or online account may be compromised	Contact the service only through its official app or website and ask it to lock the account. Secure your email account first. Change the password, reset two-factor authentication (prefer an authenticator app or a security key), end other sessions, and check withdrawal addresses, whitelists and API keys. Keep evidence.	Securing the account stops further access. Withdrawals already confirmed on the blockchain generally cannot be reversed.
Your phone suddenly lost service, or you got an unexpected SIM-change message	Call your mobile carrier from another phone right away, report a possible SIM swap, and ask them to restore and lock your number. Then secure the email and exchange accounts that use that number and switch them from SMS codes to an authenticator app or security key.	Getting the number back does not undo password resets or withdrawals made while the attacker had it.
A platform says you must pay before you can withdraw	Stop. Do not pay any fee, tax, deposit, verification or unlock amount. Stop depositing. Save the platform's web address, your chats and transaction hashes, and report it.	Paying more almost never releases funds; it usually leads to the next demand. The balance shown on the platform may not exist.

What happened	What to do now	What this does not fix
You sent money or crypto to a scammer (investment, romance, job, purchase)	Stop sending. Stop contact. Preserve evidence. If you paid through an exchange or a bank, contact them immediately through official channels. Report to the police.	Reporting is important but rarely recovers crypto quickly. Expect follow-up recovery offers (next row).
You are being threatened or extorted	Do not pay and do not negotiate. Save the messages. If the message shows an old password, change it wherever you still use it and turn on two-factor authentication. If you believe your physical safety is at risk, contact the police immediately.	Paying does not guarantee the threats stop; it marks you as someone who pays.
Someone offers to recover your losses	Treat it as a scam unless you contacted an official body yourself through its official website. Do not pay upfront fees, share your seed phrase or private key, or install remote-access software. Report the contact.	No one can reverse a confirmed blockchain transfer. Police do not charge victims to investigate a case.

Table 1: What to do next, by what happened

If more than one situation applies

Follow the response for the **most serious exposure**, plus any lower-level actions. For example, if you connected a wallet, approved a token and then exposed your seed phrase, disconnecting the site and revoking the approval is not enough: the exposed phrase means the wallet itself is compromised. If you installed malicious software and then entered your seed phrase, do not create the replacement wallet on the same device.

WHERE TO GET HELP

Legitimate helpers never ask for your seed phrase, your private key, remote access to your device, or an upfront fee to recover funds.

- Your wallet provider's official support, reached by typing its official website yourself, never through links in messages or search ads.
- The exchange or service involved, through its official app or website.
- Your local police or national cybercrime reporting service. Country links: cryptosafetyfirst.com/how-to-report-a-crypto-scam/

Preserve evidence

Before deleting messages, accounts or apps, save what you can safely save:

- transaction hashes and wallet addresses
- website addresses, usernames and account names
- emails, chats and screenshots, with dates and approximate times
- payment records and exchange or platform communications
- which device and which wallet you used

Never share seed phrases, private keys, passwords or PINs as evidence.

REPORTING

Country-specific links are kept up to date at cryptosafetyfirst.com/how-to-report-a-crypto-scam/

- **Preserve evidence** (list above).
- **Contact the exchange or service involved** through its official app or website. It may be able to freeze funds it controls.
- **Report to your local police** or national cybercrime reporting service.
- **Report the scam address or website** to the platform where you found it, and to an address-reporting service such as Chainabuse.

BE ALERT FOR RECOVERY SCAMS

After a loss, you may be contacted by people who claim they can trace, freeze or recover your crypto. Treat every unsolicited recovery offer as a scam. Do not share your seed phrase or private key, and do not send more money because someone says a fee, tax or deposit is needed to release your funds. See Chapter 13.

What these actions cannot undo

- Revoking an approval does not reverse a completed transfer.
- Disconnecting a site does not revoke an on-chain approval.
- Changing a wallet app password does not make an exposed seed phrase safe again.
- A hardware wallet cannot protect you from a harmful transaction you approve yourself.

CHAPTER 1

Social Engineering Scams

“The scam targets you—not your device.”

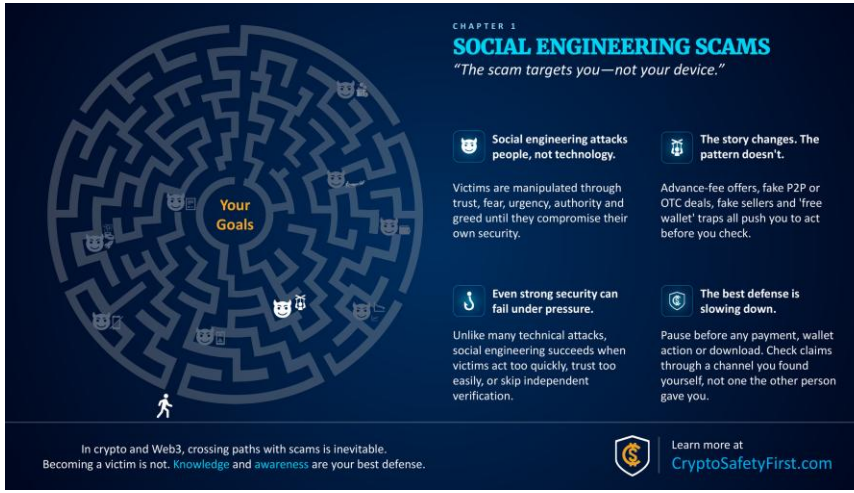


Figure 1.1: Social engineering scams at a glance

Most crypto losses do not start with a hack. They start with a message, a call, an offer or a request that gets you to do something yourself: pay, install, sign or share. That is social engineering. It attacks people, not technology, and it sits behind almost every scam in this book.

This chapter does two jobs. First, it explains **how scams work**: the triggers scammers use and the pattern that almost every scam follows. That knowledge applies to every later chapter. Second, it covers the scams that do not fit any other chapter: advance-fee offers, P2P and OTC trading fraud, fake sellers and services, “free wallet” traps and fake charity appeals.

IN THIS CHAPTER

- 1.1 How scams work: seven triggers
- 1.2 The pattern behind almost every scam
- 1.3 Social engineering scams to watch for
- 1.4 Illustrative scenario: the “free wallet” trap
- 1.5 How to protect yourself
- 1.6 CSF rules for this chapter
- 1.7 If this just happened to you

1.1 How scams work: seven triggers

Scams change their story constantly. The psychology underneath does not. Almost every scam pulls one or more of these seven triggers. Learn to notice the trigger and you can spot scams you have never seen before.

Trigger	What it sounds like	Your counter
Trust	“I’m from support.” “You know me from the group.”	Trust is earned outside the chat. Verify through a channel you found yourself.
Urgency	“Only 10 minutes left.” “Act now or lose everything.”	Real deadlines survive a 24-hour pause. Fake ones don’t.
Fear	“Your account is compromised.” “We will publish your data.”	Close the message. Check your account through the official app.
Greed	“Double your crypto.” “Guaranteed 3% a day.”	Guaranteed returns are a sign of a scam, not of an opportunity.
Curiosity	“You received a token.” “See who viewed your wallet.”	Do not click, connect or claim to find out.
Authority	“This is the police / the exchange / the tax office.”	Authorities do not ask for crypto, seed phrases or remote access.
Opportunity	“Exclusive presale.” “Early access, members only.”	Exclusive access offered to strangers is not exclusive.

Table 1.1: The seven triggers and how to counter them

Scammers rarely use one trigger alone. A typical message combines authority (“exchange security”), fear (“unusual login”) and urgency (“within 30 minutes”). The more triggers you notice, the more certain you can be that something is wrong.

1.2 The pattern behind almost every scam

Whatever the story, most scams move through the same five steps. You can break the chain at any step, but the earlier the better.

Step	What happens	Where you can stop it
1. Contact	Someone reaches you first: a DM, call, comment reply, email, ad or group invite.	Unsolicited contact about crypto is the first red flag (Rule SDR-001).
2. Trust	They build credibility: a familiar name, a logo, screenshots, small early wins.	Verify identity outside the conversation (Rule SDR-004).
3. Pressure	A trigger appears: a deadline, a threat, a bonus that expires.	Pressure is your signal to stop, not to hurry (Rule SDR-006).
4. Action	You are asked to do something: pay, install, connect, sign, share.	Never act inside the channel the scammer controls.
5. Extraction	Money or access leaves you, often followed by “one more payment”.	Stop paying. Go to the triage table (Start here).

Table 1.2: The five-step scam pattern

1.3 Social engineering scams to watch for

The scams below are pure social engineering: no fake app, no malicious contract, just deception. Scams that use a specific channel or method have their own chapters: impersonation of support and authorities (Chapter 2), fake investment platforms (Chapter 8), romance (Chapter 10), giveaways and airdrops (Chapter 7), jobs and tasks (Chapter 11).

1. Advance-fee scams

You are told that crypto is waiting for you (an inheritance, a grant, unclaimed funds, a prize) but you must first pay a fee, tax or “activation” amount to release it.

Example: A stranger contacts you about “your” funds and the next step is always to pay something first.

Red flags

- Money you did not expect, from someone you do not know.
- Fees that must be paid in crypto, before release.
- New fees after each payment.

How to avoid

- Never pay to receive money (Rule SDR-002).
- Ask yourself: why would anyone deduct a fee from you instead of from the amount they owe you?

2. P2P and OTC trading fraud

In peer-to-peer or over-the-counter trades, the scammer manipulates the payment step: a fake payment screenshot, a bank payment that is reversed after you release the crypto, a payment from a third party, or a request to finish the deal outside the platform.

Example: A buyer sends a convincing screenshot of a bank transfer and asks you to release the crypto now because “the bank is slow”.

Red flags

- Pressure to release before the money is in your account.
- Payments from a name that does not match the buyer.
- Requests to move the deal to private chat or outside escrow.

How to avoid

- Release crypto only when the payment has arrived and cannot be reversed.
- Keep every trade and every message inside the platform and its escrow.
- Treat a request to leave the platform as the end of the deal.

3. Fake sellers and services

You pay crypto for something that never arrives: hosting, servers, mining equipment, accounts, gift cards, shop items or an “escrow” service run by the seller.

Example: A seller in a group offers discounted mining hardware for crypto only, with “escrow” through a site they recommend.

Red flags

- Crypto-only payment for ordinary goods.
- Prices well below the market.
- An escrow or middleman chosen by the seller.

How to avoid

- Buy from established shops with buyer protection.
- Never use an escrow service the seller suggests.
- If crypto is the only way to pay, walk away.

4. “Free wallet” traps

Someone “accidentally” posts a seed phrase, or shares one as a gift, for a wallet that seems to hold a large balance. To move the funds you need a small amount of crypto for network fees. The wallet is rigged: the funds cannot leave, and whatever you send is taken.

Example: A comment under a video reads: “My seed phrase, I can’t access it, please help”. The wallet shows thousands in stablecoins but no gas.

Red flags

- A seed phrase shared publicly, with a visible balance.
- A wallet that needs “just a little” gas from you.
- Any story that ends with you taking funds that are not yours.

How to avoid

- Never import a seed phrase you found or were given.
- Never send crypto to unlock funds in someone else’s wallet.
- Remember: a seed phrase shared online is bait, not luck.

5. Fake charity and emergency appeals

After a disaster, war or public tragedy, scammers post wallet addresses for donations, or a contact asks for urgent crypto help.

Example: A post with a news photo asks for crypto donations to a relief fund that does not exist.

Red flags

- Donation addresses in comments, DMs or new accounts.
- No registered organization behind the appeal.
- Emotional pressure to give now.

How to avoid

- Donate only through the organization's own website, which you look up yourself.
- Check the address on that website before sending.
- If a contact asks for urgent help, call them on a number you already have.

Scam	How it works	Key red flag	How to avoid
Advance fee	Pay a fee to release funds you are "owed"	Pay first, receive later	Never pay to receive
P2P / OTC fraud	Fake or reversible payment before you release	Pressure to release early	Release only after final payment
Fake sellers and services	Crypto payment for goods never delivered	Crypto-only, seller's escrow	Buy where you have protection
"Free wallet" traps	Rigged wallet takes your gas money	Public seed phrase with a balance	Never import found seed phrases
Fake charity appeals	Donations to a scammer's address	Address in comments or DMs	Donate via the official website

Table 1.3: Social engineering scams to watch for

1.4 Illustrative scenario: the "free wallet" trap

This is an illustrative scenario, not a specific reported case.

Alex is reading the comments under a popular crypto video. One comment stands out: a user says they cannot access their wallet and posts the 12-word recovery phrase, asking for advice. Curious, Alex imports the phrase into a wallet app. The wallet shows a balance of several thousand dollars in stablecoins.

When Alex tries to move the stablecoins, the wallet says there is not enough of the network's native coin to pay the fee. Alex sends a small amount from his own wallet to cover it. Moments later, it is gone. He sends a little more. The same thing happens. The stablecoins never move.

What happened

The wallet was set up as a trap. Its permissions were changed so that the published phrase could not authorize transfers of the stablecoins, or a bot swept every incoming payment. The balance was the bait; Alex's fee payments were the profit.

Key takeaways

- A seed phrase posted in public is never a lucky find.
- The trap works because it looks like easy money, using the greed and curiosity triggers.
- Importing an unknown phrase also teaches bad habits: never type any seed phrase into an app unless it is your own and you created it.

1.5 How to protect yourself

1. **Treat unsolicited contact as a warning.** Whoever starts the conversation about crypto is the first thing to question.
2. **Verify outside the channel.** Use a website, app or phone number you found yourself, not one the other person gave you.
3. **Never pay to receive.** Fees, taxes and deposits that unlock money are the signature of a scam.
4. **Keep deals on the platform.** Escrow and support exist only inside the platform; outside it you have no protection.
5. **Use the 24-hour rule.** Any request that cannot wait a day is a request to stop thinking. Wait the day.
6. **Never import or type seed phrases you did not create.** Not to test, not to help, not out of curiosity.

1.6 CSF rules for this chapter

MAIN RULE · SDR-001

Never Trust Unsolicited Crypto Contact.

Before you pay, install or sign anything, verify through a channel you found yourself.

Rule	Statement	Why it applies here
SDR-004	Verify Identities Outside the Message Channel	The scammer controls the chat. Real verification happens elsewhere.
SDR-006	Question Urgency, Hype and Guaranteed Profits	Urgency and guaranteed returns are triggers, not information.
SDR-002	Never Send Crypto to Receive Crypto	Advance-fee offers and “free wallet” traps depend on it.
TSR-007	Slow Down Before Clicking or Installing	Most social engineering only works if you act quickly.

Table 1.4: Supporting CSF rules

1.7 If this just happened to you

First find your situation in the triage table (**Start here**). Then add the steps for your scam:

If you…	Do this now
paid an advance fee	Stop paying. Every new fee is part of the same scam. Save the messages and payment details and report it.
released crypto in a P2P or OTC trade without receiving payment	Open a dispute with the platform immediately, using the order ID, and keep all communication on the platform.
received a payment that may be reversed	Do not release anything. Contact the platform and your bank before you act.

If you…	Do this now
paid a fake seller or service	Report the seller to the platform or group where you found them and to the police. If you paid from an exchange, contact it with the transaction hash.
sent gas to a “free wallet”	Stop. The amount you sent is lost; sending more will not unlock anything. Your own wallet is not compromised by sending, but do not reuse the trap’s seed phrase anywhere.
donated to a fake appeal	Report the address and post to the platform. Warn the people who shared it.

Table 1.5: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/social-engineering-scams-crypto-web3/

CHAPTER 2

Impersonation Scams

“Real names. Fake people.”

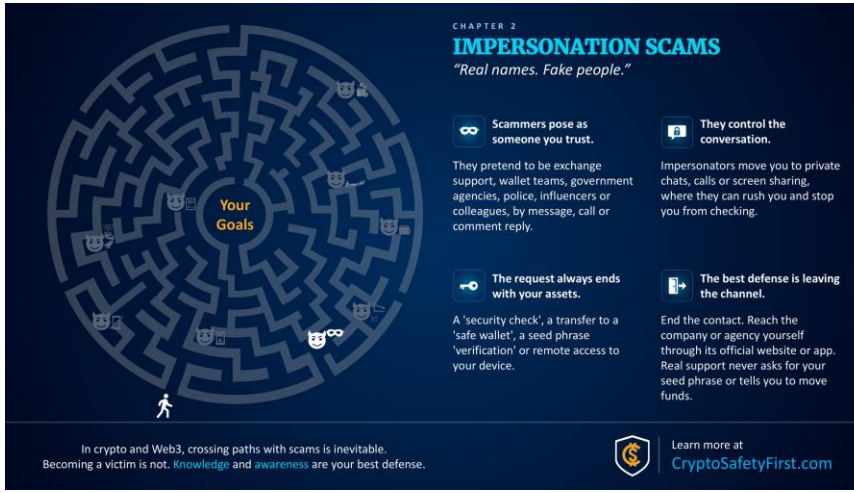


Figure 2.1: Impersonation Scams at a glance

In an impersonation scam, a real person talks to you while pretending to be someone you trust: exchange support, a wallet company, the police, a tax office, a well-known founder, or a friend whose account was taken over. The conversation is live, by message, call, video or comment reply, and that is what makes it work. The scammer can answer your doubts, adjust the story and keep up the pressure until you act.

Impersonation is different from phishing (Chapter 3). A phishing page or email copies a brand and waits for you. An impersonator talks to you, steers you and usually moves you away from the official channels you would otherwise check.

IN THIS CHAPTER

- 2.1 Impersonation scams to watch for
- 2.2 How impersonators work
- 2.3 Illustrative scenario: the “security team” call
- 2.4 How to protect yourself
- 2.5 CSF rules for this chapter
- 2.6 If this just happened to you

2.1 Impersonation scams to watch for

1. Fake customer support

You post a question or complaint about a wallet or exchange in public, and within minutes “support” replies or sends you a direct message. The account looks official. It offers to help, then sends you a link, asks for your recovery phrase, or asks you to share your screen.

Example: After a post about a stuck withdrawal, an account named like the exchange’s help desk sends a DM with a “ticket form” that asks for the 24-word recovery phrase to “verify ownership”.

Red flags

- Support contacts you first, by DM or comment reply.
- You are moved to a private chat, a form or a call.
- Requests for your recovery phrase, private key, screen sharing or remote access.

How to avoid

- Open support only from the official app or website you type yourself.
- Remember that real support never asks for your recovery phrase.
- Do not reply to “help” you did not request; report the account instead.

2. Fake security calls and “safe wallet” transfers

Someone calls or messages claiming to be the security or fraud team of your exchange or wallet provider. They warn about suspicious activity and tell you to move your funds to a “safe wallet”, to approve a “protection” transaction, or to read out a code. Many of these calls use personal details from data leaks, which makes them convincing.

Example: A caller who knows your name, address and the hardware wallet you bought says your device was compromised and walks you through sending your funds to a new “secure” address.

Red flags

- A call or message you did not expect about a security problem.
- The caller already knows personal details about you.
- Instructions to move funds, approve a transaction or share a code.

How to avoid

- Hang up. Open your account through the official app and check yourself.
- No legitimate company tells you to move funds to an address it gives you.
- Personal details in a call prove a data leak, not that the caller is genuine.

3. Authority impersonation

The impersonator claims to be the police, a regulator, a tax office, a court or a lawyer. They say your account is linked to a crime, that you owe tax, or that funds will be frozen unless you pay or cooperate. Some send official-looking letters or ID cards.

Example: A message from a “cybercrime unit” says your wallet was used in money laundering and that you must transfer your funds to a “government custody wallet” while the case is investigated.

Red flags

- Threats of arrest, fines or frozen funds.
- Payment demanded in crypto or gift cards.
- An official-looking document sent by chat or email.

How to avoid

- Authorities do not ask for crypto payments, seed phrases or remote access.
- Contact the agency yourself using contact details from its official website.
- Do not reply, pay or argue; save the messages and report them.

4. Celebrity and founder impersonation

Scammers pose as well-known founders, influencers or executives, in messages, live streams or replies under real posts. The aim is to promote a fake giveaway, an investment or a “private opportunity”.

Example: A live stream that looks like a well-known founder’s channel promotes a limited-time offer to double any crypto sent to an address on screen.

Red flags

- A famous person contacts you directly.
- Replies under real posts that push a link or offer.
- Paid verification badges and high follower counts.

How to avoid

- Famous people do not DM strangers with offers.
- Check the person’s official website and main account, not the account that contacted you.
- Treat any “send crypto to receive more” offer as a scam (Chapter 7).

5. Known contacts and hacked accounts

A friend, colleague or community member’s account is taken over, or copied, and used to ask you for money, for a quick crypto transfer, or to try a new app or link.

Example: A colleague’s messaging account writes that they are stuck abroad and asks for crypto because their bank card was blocked.

Red flags

- An unusual request from someone you know, with urgency.
- A new number or account “because my phone broke”.
- Reluctance to talk by voice or video.

How to avoid

- Call the person on a number you already have.
- Ask a question only the real person can answer.
- Warn the person and others in the group if the account is compromised.

6. Deepfake calls and videos

AI-generated voice or video imitates a real person: a manager approving a payment, a family member in trouble, or a founder announcing an airdrop. Quality is improving quickly, so you cannot rely on spotting glitches.

Example: A video call with someone who looks and sounds like a company director asks you to send a payment urgently and to keep it confidential.

Red flags

- Urgent money requests on a video or voice call.
- Requests to keep the call secret.
- A new channel or account for a familiar person.

How to avoid

- Verify through a second channel you control before acting.
- Agree a family or team code word for urgent requests.
- Do not treat a convincing face or voice as proof.

Scam	Who they pretend to be	Key red flag	How to avoid
Fake support	Exchange or wallet help desk	Support contacts you first	Use support only from the official app
Fake security call	Fraud or security team	“Move funds to a safe wallet”	Hang up and check in the app
Authority	Police, regulator, tax office	Threats plus payment in crypto	Contact the agency yourself
Celebrity or founder	Famous person or project lead	Direct offers to strangers	Check official channels
Known contact	Friend or colleague	Urgent request on a new account	Call a number you already have
Deepfake	Anyone with public video or voice	Urgency and secrecy on a call	Verify on a second channel

Table 2.1: Impersonation scams to watch for

2.2 How impersonators work

Impersonation uses the triggers from Chapter 1, especially **authority**, **trust** and **fear**. What makes it different is control of the conversation. Impersonators work in four moves:

1. **Borrow credibility.** A real brand name, logo, job title or leaked personal details.
2. **Create a problem.** A hacked account, a blocked withdrawal, a legal case, an emergency.
3. **Isolate you.** Move the conversation to a private chat, a call or screen sharing, away from official channels and people who could warn you.
4. **Offer the solution.** The "solution" is always an action that hands over your assets: share a phrase, move funds, approve a transaction, install remote-access software.

The defense is the same every time: **leave the channel**. Close the chat or hang up, then go to the company or agency through a website or app you open yourself. If the problem is real, it will still be there.

2.3 Illustrative scenario: the "security team" call

This is an illustrative scenario, not a specific reported case.

Maria gets a call from someone who says he works in the security team of the exchange she uses. He knows her name, her email address and that she logged in yesterday. He says an unknown device has been added to her account and her funds are at risk.

He asks her to install a support app so he can "secure the account", then guides her to move her balance to a "protected wallet" while the investigation runs. He stays on the line the whole time, reassuring her and saying that every minute counts.

What happened

The caller used personal data from a leak to sound genuine. The support app gave him remote access to Maria's computer, and the "protected wallet" was his. Nothing had been wrong with her account before the call.

Key takeaways

- Knowing your details does not make a caller genuine.

- No exchange asks you to move funds to an address it gives you, or to install remote-access software.
- Hanging up and checking in the official app would have ended the scam in a minute.

2.4 How to protect yourself

1. **Never act inside a conversation someone else started.** Hang up or close the chat, then check through the official app or website.
2. **Real support never asks for your recovery phrase**, private key, remote access or a transfer to a “safe wallet”.
3. **Keep your contact details private.** Do not post exchange or wallet problems publicly with your username; use the official support form.
4. **Agree a code word** with family or your team for urgent money requests.
5. **Expect leaked data to be used against you.** If you bought a hardware wallet or used an exchange that had a data leak, treat calls and letters about it with extra suspicion.
6. **Report impersonating accounts** to the platform and warn your community.

2.5 CSF rules for this chapter

MAIN RULE · SDR-004

Verify Identities Outside the Message Channel.

End the chat or call. Contact the company or agency yourself through its official website or app.

Rule	Statement	Why it applies here
GR-005	Never Follow Urgent Support or Security Instructions. Exit the Channel and Re-Enter Through the Official App or URL	The “security team” script depends on you following instructions in the call.

Rule	Statement	Why it applies here
SDR-001	Never Trust Unsolicited Crypto Contact	Impersonators almost always contact you first.
GR-001	Never Share Your Seed Phrase	The most common request in fake support chats.

Table 2.2: Supporting CSF rules

2.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: compromised account, exposed seed phrase, installed software, sent a transaction. Then add the steps for your situation:

If you…	Do this now
shared your recovery phrase or private key	Treat the wallet as compromised and follow the seed-phrase row now, from a clean device.
installed remote-access or “support” software	Disconnect the device from the internet, uninstall the software and follow the malware row. Change passwords from another device.
moved funds to a “safe wallet”	Save the address and transaction hash. If the funds went to an exchange address, contact that exchange immediately. Report to the police.
gave a login code or password	Change the password and two-factor settings from the official app, end other sessions and check withdrawal addresses.
paid an “authority”	Stop paying. Contact the real agency through its official website and report the impersonation to the police.
are still on the call or in the chat	End it now. Nothing legitimate needs to happen inside that conversation.

Table 2.3: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/impersonation-scams-crypto-web3/

CHAPTER 3

Phishing Scams

“The attack begins when you trust the wrong page.”

Figure 3.1: Phishing Scams at a glance

Phishing copies something you trust: an exchange login page, a wallet download site, a delivery notice, a support email. Unlike impersonation (Chapter 2), there is usually no live conversation. The fake page, email, text message, ad or QR code simply waits for you to type a password, enter a recovery phrase, or connect your wallet and sign.

Phishing remains one of the most common entry points for crypto losses because it scales: one fake page can reach thousands of people. The good news is that one habit defeats most of it: **never reach an important account through a link someone else gave you.**

IN THIS CHAPTER

- 3.1 Phishing scams to watch for
- 3.2 Wallet-connected phishing: approvals, signatures and drainers
- 3.3 Practical exercise: spot the phishing email
- 3.4 How to protect yourself
- 3.5 CSF rules for this chapter
- 3.6 If this just happened to you

3.1 Phishing scams to watch for

1. Email phishing

Emails that copy an exchange, wallet, email provider or delivery service and push you to log in, “verify” or “update” through a link. Spear phishing is the targeted version: it uses your name, your holdings or details from a data leak.

Example: An email that looks like it comes from your wallet provider says your wallet will be suspended unless you “verify” it today, with a button to a lookalike site.

Red flags

- Urgent deadlines and threats of suspension.
- Sender addresses or link domains that are close to the real one but not the same.
- Requests to enter a recovery phrase “to verify”.

How to avoid

- Do not click links in unexpected emails; open the app or a bookmark instead.
- Check the sender domain and hover over links before anything else.
- Remember: no service ever asks for your recovery phrase.

2. Clone websites and search-ad phishing

Exact copies of exchanges, wallet download pages, DeFi apps or NFT sites on lookalike domains. Many are promoted with paid search ads that appear above the real result.

Example: A search for a wallet app shows an ad at the top. The site looks identical to the real one, but the download installs a fake wallet, or the “restore” page asks for your recovery phrase.

Red flags

- A domain with an extra letter, hyphen or unusual ending.
- Arriving through a search ad or a link in a chat.
- A site that asks for your recovery phrase.

How to avoid

- Bookmark the official sites you use and only use those bookmarks.

- Skip search ads for anything financial.
- Download wallets only from the maker's official site or the official app store listing linked from it.

3. Smishing and messaging-app phishing

Text messages and messaging-app notes that claim to be from an exchange, bank, delivery company or tax office, with a short link.

Example: A text says a withdrawal of a large amount was requested from your account and gives a link or phone number to cancel it.

Red flags

- Alarming messages about withdrawals or logins you did not make.
- Short links or unusual numbers.
- A call-back number inside the message.

How to avoid

- Check activity in the official app, never through the message.
- Do not call numbers given in the message.
- Report and delete.

4. QR code phishing

QR codes in emails, letters, posters or fake support chats that lead to phishing pages or to wallet connection requests. Some are mailed as official-looking letters.

Example: A printed letter that appears to come from a hardware wallet company asks you to scan a QR code to "validate" your device and enter your recovery phrase.

Red flags

- A QR code you did not expect, especially in a letter or email.
- A scan that leads to a login, a wallet connection or a recovery-phrase form.

How to avoid

- Do not scan QR codes for account or wallet actions; open the official app instead.
- No hardware wallet maker asks you to enter your recovery phrase on a website.

5. Fake mint, claim and NFT pages

Pages that copy real NFT projects, token launches or reward programs and ask you to connect your wallet to mint, claim or “verify”. They often spread through hacked project accounts and fake announcements.

Example: A project’s community channel posts a “surprise mint” link after its account was compromised. The page copies the project’s design and asks for a signature.

Red flags

- Surprise mints or claims with short deadlines.
- Links posted in chats or replies rather than on the project’s website.
- Signature requests you do not understand.

How to avoid

- Check announcements on the project’s website and main channels before acting.
- Use a Disposable wallet for mints and claims.
- Reject any signature you cannot explain.

Type	Where it reaches you	Key red flag	How to avoid
Email phishing	Inbox	Urgent “verify” links	Use the app or a bookmark
Clone sites and ads	Search results, links	Lookalike domain	Bookmarks only; skip ads
Smishing	Text and messaging apps	Alarming withdrawal alerts	Check in the official app
QR phishing	Letters, emails, posters	QR code for account actions	Never scan for wallet actions
Fake mint and claim pages	Community channels, replies	Surprise mint with deadline	Disposable wallet, verify first

Table 3.1: Phishing scams to watch for

3.2 Wallet-connected phishing: approvals, signatures and drainers

Not every phishing attack asks for a password or recovery phrase. Many phishing sites ask you to **connect your wallet and then approve or sign** something. Wallet drainer kits turn that approval or signature into theft: the victim believes they are claiming an airdrop, minting an NFT or "verifying" a wallet.

Action on the site	What it can give the attacker
Connecting the wallet	Your address and balances. By itself, connecting does not move funds.
Approving a token or NFT	Permission to move those tokens or NFTs later, up to the approved amount, which is often unlimited.
Signing a message or authorization	Depending on what you sign, permission to move tokens without a separate approval transaction (for example Permit-type signatures).
Sending a transaction	Whatever the transaction does: a transfer, a swap, a new approval.
Typing the recovery phrase	Full control of the wallet.

Table 3.2: Connect, approve, sign, send: what each step can give away

Unbranded sites whose only trick is the approval or the transaction itself are covered in Chapter 5 (Malicious Contracts and Approvals). Hardware wallets protect your keys, but they cannot protect you from a harmful approval or signature that you confirm on the device.

3.3 Practical exercise: spot the phishing email

Before you act on any email about your accounts, run these five checks. If one fails, stop.

1. **Sender:** is the domain exactly the company's own domain?
2. **Link:** does the link (hover to see it) go to the company's real domain?
3. **Request:** does it ask for a password, a code or a recovery phrase? A recovery phrase request is always phishing.

4. **Pressure:** is there a deadline, a threat or an unusually good offer?
5. **Expectation:** did you do something that explains this email?

3.4 How to protect yourself

1. **Bookmark every financial site you use** and reach them only through bookmarks or the official app.
2. **Never enter your recovery phrase on a website, form or app** other than when you restore a wallet you own, on software from the official source.
3. **Read every wallet request** before you confirm it. Reject anything you do not understand.
4. **Separate your wallets.** Use a Disposable wallet for new sites, mints and claims, and keep your Vault away from websites entirely.
5. **Use phishing-resistant sign-in** for exchanges and email: a hardware security key or passkey where available.
6. **Use your wallet's warnings and a reputable security extension** as an extra layer, never as your only check.

3.5 CSF rules for this chapter

MAIN RULE · SDR-009

Verify All Links Before Logging In.

Use bookmarks or addresses you type yourself, and read every wallet request before you sign.

Rule	Statement	Why it applies here
GR-002	Always Verify the Full URL and Domain Before Connecting Your Wallet to Any Website	Clone sites rely on domains that look right at a glance.
GR-001	Never Share Your Seed Phrase	A recovery-phrase request is the clearest phishing signal.
TSR-004	Use Hardware-Based Two-Factor Authentication	Security keys resist phishing pages that capture codes.

Rule	Statement	Why it applies here
SDR-005	Never Connect Your Wallet to Unknown Websites	Drainer pages need a wallet connection first.

Table 3.3: Supporting CSF rules

3.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: viewed only, connected, approved, signed, exposed seed phrase, installed software, compromised account. Then add the steps for your situation:

If you…	Do this now
only opened the email or page	Close it. If you typed, connected or downloaded nothing, your accounts are not compromised by viewing.
entered a password or login code	Change that password from the official app or site, also wherever you reused it, end other sessions, and check your email account for forwarding rules.
entered your recovery phrase	Treat the wallet as compromised. Follow the seed-phrase row now, from a clean device.
connected, approved or signed on a phishing site	Follow the connect, approve and sign rows in that order. Revoke what you can and move remaining assets if transfers have started.
downloaded a “wallet” or file	Follow the malware row and treat any phrase typed into that app as exposed.

Table 3.4: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/phishing-scams-crypto-web3/

CHAPTER 4

Fake Apps and Wallets

“One fake app can defeat good security.”

Figure 4.1: Fake Apps and Wallets at a glance

Every crypto user depends on software: a wallet app, a browser extension, an exchange app, sometimes a hardware wallet. If that tool is fake or tampered with, everything you do with it is visible to the scammer, starting with the recovery phrase you type into it. Good habits cannot protect you from a tool that was built to steal.

This chapter covers fake or tampered wallets, apps, extensions, recovery tools and hardware devices that you install, set up and use yourself. Malicious software that infects your device in other ways (infostealers, clipboard hijackers, remote-access tools) is covered in the Hackers guide.

IN THIS CHAPTER

- 4.1 Fake apps and wallets to watch for
- 4.2 Why a hardware wallet does not fix a fake setup
- 4.3 Illustrative scenario: the trading helper extension
- 4.4 How to protect yourself
- 4.5 CSF rules for this chapter
- 4.6 If this just happened to you

4.1 Fake apps and wallets to watch for

1. Fake wallet apps and browser extensions

Copies of popular wallets in app stores, browser extension stores or on lookalike download sites. They look identical to the real wallet. When you create or restore a wallet, the recovery phrase is sent to the scammer.

Example: A search ad leads to a download page for a well-known wallet extension. The extension works normally, but every phrase entered during setup is copied to the scammer.

Red flags

- A download link from an ad, a chat or a video description.
- A publisher name, review count or install count that does not match the real wallet.
- Asking you to restore an existing wallet straight after installing.

How to avoid

- Start from the wallet maker’s official website and follow its own link to the store listing.
- Check the publisher name before installing.
- Create new wallets rather than restoring old phrases into newly installed apps you have not verified.

2. Tampered and pre-configured hardware wallets

Hardware wallets bought from marketplaces, resellers or second-hand sellers can be modified, or shipped with a recovery phrase already printed on a card “for your convenience”. Anyone who prepared that phrase controls the wallet.

Example: A discounted hardware wallet from an online marketplace arrives with a scratch card showing a recovery phrase and instructions to use it.

Red flags

- A recovery phrase included in the box.
- Damaged or missing seals, or a device that is already set up.
- Prices well below the official store.

How to avoid

- Buy only from the manufacturer or its listed official resellers.
- Always generate a new recovery phrase on the device yourself.
- Never use a recovery phrase you did not create.

3. Fake recovery, validation and “sync” tools

Websites and apps that claim to fix a stuck wallet, “validate” or “synchronize” it, recover lost funds or check its security, and ask you to enter your recovery phrase to do so.

Example: After a failed transaction, a forum reply links to a “wallet rectification” tool that asks for the recovery phrase to repair the wallet.

Red flags

- Any tool that asks for your recovery phrase to fix, check or sync a wallet.
- Links shared in replies to support questions.

How to avoid

- No legitimate tool needs your recovery phrase except your own wallet during a restore.
- Get help only through the wallet maker’s official support.

4. Counterfeit exchange and trading apps

Fake versions of real exchanges or trading platforms, distributed as app files, test-flight builds or links outside the official stores. They capture your login and two-factor codes, or show fake balances.

Example: A message offers a “pro” version of a well-known exchange app with lower fees, installed from a link instead of the app store.

Red flags

- Apps installed from a link or a file instead of the official store.
- Special versions with features or fees the real app does not offer.

How to avoid

- Install exchange apps only from the official store, through the exchange's own website.
- If an exchange app asks you to log in again unexpectedly, close it and check the official app.

5. Fake trading helpers, security tools and wallet checkers

Browser extensions and apps promising trading signals, portfolio tracking, airdrop checking or wallet security. Some read everything you do in the browser, including logged-in exchange sessions, or replace addresses you copy.

Example: A free extension that adds trading tools to an exchange's website quietly reads the session data of the logged-in user.

Red flags

- Extensions that ask for permission to read and change data on all websites.
- Tools recommended in trading groups or by influencers you cannot verify.
- Recently published tools with few reviews but heavy promotion.

How to avoid

- Install as few extensions as possible, and none in the browser you use for crypto.
- Check requested permissions before installing.
- Remove extensions you no longer use.

Type	What it steals	Key red flag	How to avoid
Fake wallet app or extension	Recovery phrase at setup	Download from an ad or chat	Start from the official website
Tampered hardware wallet	Control of the wallet	Phrase included in the box	Buy direct; create your own phrase

Type	What it steals	Key red flag	How to avoid
Fake recovery or sync tool	Recovery phrase	Asks for your phrase to fix the wallet	Use official support only
Counterfeit exchange app	Login and codes	Installed from a link	Official store only
Fake helper or security tool	Sessions, copied addresses	Broad permissions	Minimal extensions, separate browser

Table 4.1: Fake apps and wallets to watch for

4.2 Why a hardware wallet does not fix a fake setup

Hardware wallets keep your private keys off your computer, and that protects you from many attacks. They cannot help in three situations covered in this chapter:

- **The phrase was not created by you.** A pre-configured device or a pre-printed phrase gives someone else the keys from day one.
- **You typed the phrase into software.** Entering your hardware wallet's phrase into a fake app or recovery tool exposes it just like a software wallet's.
- **You approve what you are shown.** A fake app can show you a harmful transaction; if you confirm it on the device, it is signed.

Browser-session theft is a separate case. If an extension steals your logged-in exchange session, the attacker can act as you without needing your password or your two-factor code, because the session is already signed in. Strong two-factor authentication protects the login, not a session that has already been taken.

4.3 Illustrative scenario: the trading helper extension

This is an illustrative scenario, not a specific reported case.

Leo trades actively on an exchange. In a trading group he sees a free browser extension that adds advanced charts and alerts to the

exchange's website. He installs it in his normal browser and grants the permissions it asks for.

A few days later, trades he did not make appear in his account, and his balance is moved through thinly traded pairs. When he logs in, everything looks normal: his password and two-factor settings are unchanged.

What happened

The extension read the exchange session in Leo's browser and passed it to the attacker, who used the already-logged-in session directly. Leo's password and two-factor code were never needed.

Key takeaways

- Extensions with access to all websites can read what you do on your exchange.
- Keep a separate browser, or browser profile, with no extensions for crypto accounts.
- If you suspect session theft, sign out of all sessions from the official app and remove the extension.

4.4 How to protect yourself

1. **Start from the official website** of the wallet or exchange and follow its links to downloads and store listings.
2. **Buy hardware wallets directly** from the manufacturer or its listed official resellers.
3. **Create your own recovery phrase** on every new wallet and device. Never accept a phrase someone else prepared.
4. **Never type your recovery phrase into any app, website or tool**, except your own wallet when you restore it.
5. **Keep crypto in a clean browser profile** with no extensions, or on a device used only for crypto.
6. **Review and remove extensions** regularly, and check the permissions of anything you keep.

4.5 CSF rules for this chapter

MAIN RULE · TSR-001

Never Install Crypto Software from Unofficial Sources.

Get wallets and apps only from the maker's official site or app store. Never type your seed phrase into an app or website – restore it only in your own official wallet, and on a hardware wallet only on the device's own screen.

Rule	Statement	Why it applies here
GR-001	Never Share Your Seed Phrase	Fake tools exist to capture the phrase.
GR-003	Always Use a Hardware Wallet for Long-Term or High-Value Crypto Storage	Only when bought from the maker and set up with your own phrase.
TSR-002	Assume Your Device Can Be Compromised	Plan as if an extension or app could be reading your activity.
TSR-006	Separate Devices and Accounts for Crypto Use	A clean browser or device limits what a fake tool can see.

Table 4.2: Supporting CSF rules

4.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: exposed seed phrase, installed software, compromised account. Then add the steps for your situation:

If you…	Do this now
entered your recovery phrase into an app, extension or tool	Treat the wallet as compromised. Follow the seed-phrase row from a clean device, and do not create the new wallet in the same app.
set up a hardware wallet with a phrase that came in the box	Treat it as compromised. Move funds to a new wallet whose phrase you generated yourself on a device bought from the maker.

If you…	Do this now
installed a suspicious extension or app	Remove it. Sign out of all exchange sessions from the official app, change passwords from a clean device, and follow the malware row.
logged in to a counterfeit exchange app	Change the password and two-factor settings in the official app, end other sessions and check withdrawal addresses.

Table 4.3: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/scam-apps-browser-extension-crypto-web3/

CHAPTER 5

Malicious Contracts and Approvals

“Every signature deserves suspicion.”

Figure 5.1: Malicious Contracts and Approvals at a glance

In these scams the trap is the smart contract itself. There is no fake brand and no conversation, just a dApp, a bot or a mint page that asks you to approve, sign or send. Once you confirm, the contract does what it was written to do: move your tokens to the scammer.

This chapter explains what you actually give away with each wallet action, the main contract-based scams, and how to limit the damage with approvals management and wallet separation. Phishing pages that copy a real brand are covered in Chapter 3; exploits of legitimate protocols, where users did nothing wrong, are covered in the Hackers guide.

IN THIS CHAPTER

- 5.1 Approvals and signatures in plain English
- 5.2 Malicious contract scams to watch for
- 5.3 Illustrative scenario: the MEV bot tutorial
- 5.4 How to protect yourself
- 5.5 CSF rules for this chapter
- 5.6 If this just happened to you

5.1 Approvals and signatures in plain English

Term	What it means	Why it matters
Approval (allowance)	Permission for a contract to move a specific token from your wallet, up to a set amount.	Unlimited approvals stay active until you revoke them, even after you leave the site.
NFT approval for all	Permission for a contract to move every NFT in a collection.	One click can expose a whole collection.
Signature	A message you sign with your wallet. Some are harmless logins; others authorize transfers.	Permit-type signatures can grant token access without a separate approval transaction.
Blind signing	Confirming a request your wallet cannot fully decode, so you see only raw data.	You cannot know what you are agreeing to.
Revoking	A transaction that sets an approval back to zero.	Stops future use of the permission; does not return what was already taken.

Table 5.1: Approvals and signatures in plain English

5.2 Malicious contract scams to watch for

1. Malicious approval requests

Unknown dApps, games, yield tools or “claim” pages ask for an approval as part of a normal-looking action. The approval is for an unlimited amount, or for a token you did not expect.

Example: A new yield site asks you to approve unlimited USDC “to enable deposits”, then drains the wallet days later.

Red flags

- Unlimited approvals for a simple action.
- Approval for a token unrelated to what you are doing.
- A contract address you cannot verify anywhere else.

How to avoid

- Approve only the amount you need, where your wallet allows it.

- Use a Disposable wallet for unfamiliar dApps.
- Revoke approvals when you are done.

2. Fake trading, arbitrage and MEV bots

Videos and posts offer a “profitable bot”: deploy a contract from a code snippet, fund it, and start it. The code hides a function that sends the funds to the scammer.

Example: A video tutorial shows how to deploy an “arbitrage bot” contract using copied code and fund it with ETH to start trading.

Red flags

- Guaranteed profits from a bot you deploy yourself.
- Code you cannot read, copied from a video or chat.
- Comment sections full of praise.

How to avoid

- Never deploy or fund code you cannot fully read.
- Treat “passive bot income” tutorials as scams.

3. Signature-based drains

Instead of an approval transaction, the site asks you to sign a message. The signature authorizes token transfers, so funds can move later without any further prompt.

Example: A “free mint” asks for a signature that looks like a login but is a Permit-type authorization for your tokens.

Red flags

- Signature requests on sites you have just found.
- Blind-signing or unreadable data.
- A “login” that is not needed for what you are doing.

How to avoid

- Reject signatures you cannot read and explain.
- Keep blind signing switched off unless you need it for a specific trusted app.

4. Unbranded fake mints and claim contracts

Mint and claim pages for projects that do not exist, promoted through ads, replies and airdropped tokens. The mint transaction includes an approval for all your NFTs or tokens.

Example: A page offering a limited free mint asks you to approve your entire NFT collection “for verification”.

Red flags

- Approval for all NFTs to mint one.
- Deadlines and counters showing almost sold out.

How to avoid

- Mint only from projects you have checked independently.
- Mint from a Disposable wallet that holds nothing else.

Type	What you confirm	Key red flag	How to avoid
Malicious approval	Unlimited token approval	More access than the action needs	Limit, separate, revoke
Fake trading or MEV bot	Deploy and fund a contract	Code you cannot read	Never deploy unknown code
Signature drain	A signed message	Unreadable or unexpected signature	Reject what you cannot explain
Fake mint or claim	Mint with approval for all	Approval for all to mint one	Disposable wallet only

Table 5.2: Malicious contract scams to watch for

5.3 Illustrative scenario: the MEV bot tutorial

This is an illustrative scenario, not a specific reported case.

Nina watches a polished video that explains how “MEV bots” earn passive income. The creator shares contract code and a step-by-step guide: paste the code into an online editor, deploy it, send ETH to the contract and press “start”.

Nina follows the steps with 1 ETH. When she presses “start”, the balance in the contract drops to zero. The transaction history shows the ETH went to an address she does not recognize.

What happened

The code contained a hidden address that received the funds when the start function was called. There was never a bot.

Key takeaways

- Profits from code you copy and do not understand are not real.
- The comment section was part of the scam.
- Deploying a contract does not make you its only controller if the code says otherwise.

5.4 How to protect yourself

1. **Separate your wallets.** Keep long-term holdings in a Vault that never connects to dApps. Use a Frequent Use wallet for trusted apps and a Disposable wallet for anything new.
2. **Read before you confirm.** Check the action, the token, the amount and the contract. If your wallet cannot decode it, reject it.
3. **Approve the minimum.** Prefer limited approvals over unlimited ones.
4. **Revoke regularly.** Review your approvals in your wallet or a reputable approval checker and revoke anything you no longer use.
5. **Never deploy or fund code you cannot read.**
6. **Remember what a hardware wallet does.** It protects your keys. It does not make a harmful approval or signature safe if you confirm it on the device.

5.5 CSF rules for this chapter

MAIN RULE · GR-004

Always Revoke Unused Token Approvals After Interacting with New Smart Contracts.

Reject unlimited approvals you don’t need, and use a Disposable wallet for unfamiliar contracts.

Rule	Statement	Why it applies here
SDR-005	Never Connect Your Wallet to Unknown Websites	Every contract scam starts with a connection.
GR-008	Keep Long-Term Holdings in a Vault Wallet. Use a Separate Wallet for DApps, Trading, and Web3	Separation limits what one bad approval can reach.
GR-002	Always Verify the Full URL and Domain Before Connecting Your Wallet to Any Website	Know exactly which site you are connecting to.

Table 5.3: Supporting CSF rules

5.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: connected, approved, signed, sent a transaction. Then add the steps for your situation:

If you…	Do this now
approved a suspicious contract	Revoke the approval from a trusted device. If transfers have already started, move the remaining assets to another wallet you control first.
signed a message you cannot explain	Stop using the wallet for new activity and move remaining assets to another wallet you control.
deployed or funded a bot	Do not send more funds to “unlock” it. Save the contract address and transactions and report them.
minted with an approval for all	Revoke the collection approval and move valuable NFTs to another wallet.

Table 5.4: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/smart-contract-scams-crypto-web3/

CHAPTER 6

Address Poisoning Scams

“The address looked right. Only the middle was wrong.”

Figure 6.1: Address Poisoning Scams at a glance

Crypto addresses are long and hard to read, so most people check only the first and last few characters. Address poisoning exploits exactly that. Scammers create addresses that start and end like one you use, then plant them in your transaction history. The next time you copy an address from your history, you may copy theirs.

It is a short chapter because the scam is simple. It is also one of the easiest losses to prevent, and among the hardest to undo.

IN THIS CHAPTER

- 6.1 How address poisoning works
- 6.2 Variants to watch for
- 6.3 Illustrative scenario: the exchange deposit
- 6.4 How to protect yourself
- 6.5 CSF rules for this chapter
- 6.6 If this just happened to you

6.1 How address poisoning works

1. **Watch.** Scammers monitor the blockchain for wallets that move meaningful amounts.
2. **Copy the look.** They generate an address whose first and last characters match one you send to often.
3. **Poison.** They send a tiny, zero-value or fake-token transfer from that lookalike address, so it appears in your history next to your real transactions.
4. **Wait.** When you next copy an address from your history to send funds, the lookalike may be the one you pick.

The poisoning transfer does not give anyone access to your wallet. Viewing it is harmless. The loss happens only if you send funds to the lookalike address.

6.2 Variants to watch for

Variant	What you see	Key red flag
Zero-value transfers	A transfer of 0 tokens “from” you or to you	Transfers you did not make in your history
Dust transfers	A tiny incoming amount from a lookalike address	Unexpected small deposits
Fake-token transfers	A transfer of a token with the same name and symbol as a real one	A familiar token from an unfamiliar contract
Clipboard swaps	The address changes between copy and paste	Malware on your device; see the Hackers guide

Table 6.1: Address poisoning variants

6.3 Illustrative scenario: the exchange deposit

This is an illustrative scenario, not a specific reported case.

Ben moves savings from his hardware wallet to an exchange every few months. He usually copies the exchange deposit address from his last transaction. This time, the history shows an incoming transfer he does

not remember, from an address that starts and ends exactly like his deposit address.

Ben copies the address at the top of the list, checks the first and last four characters on the device screen, and confirms. The funds never arrive at the exchange.

What happened

The top entry was a poisoning transfer. Ben's check of the first and last characters passed because the scammer had generated an address to match them. The device showed the full address, but he did not compare the middle.

Key takeaways

- Never copy addresses from your transaction history.
- Checking only the start and end is exactly what the scam is designed to beat.
- A hardware wallet shows the full address; compare all of it.

6.4 How to protect yourself

1. **Never copy an address from your transaction history.** Copy it from the source: the exchange's deposit page, a saved contact, or the recipient directly.
2. **Use your wallet's address book** and the exchange's withdrawal whitelist for addresses you use regularly.
3. **Compare the whole address**, not just the beginning and end, on your hardware wallet screen.
4. **Send a small test transaction** before large transfers, then check the full address again for the main transfer: poisoners sometimes react to your test with a new lookalike.
5. **Ignore unexpected transfers** in your history. Do not interact with them.

6.5 CSF rules for this chapter

MAIN RULE · OR-005

Always Verify the Destination Before Sending Crypto.

Never copy addresses from your history. Use your address book and check every character.

Rule	Statement	Why it applies here
GR-006	Always Send a Small Test Transaction Before Transferring Large Amounts of Crypto	A test confirms the route, as long as you re-check the address for the main transfer.
TSR-005	Enable Withdrawal Whitelists on Exchanges	Whitelists stop sending to addresses you have not saved.

Table 6.2: Supporting CSF rules

6.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: sent a transaction, viewed only, installed software. Then add the steps for your situation:

If you…	Do this now
sent funds to a poisoned address	Save the transaction hash and both addresses. Report the address. Act quickly: if the funds reach an exchange, that exchange may be able to freeze them after a report.
see poisoning transfers in your history	Nothing is compromised. Do not interact with them, and copy addresses only from their source from now on.
think the address changed when you pasted it	That points to malware, not poisoning. Follow the malware row.

Table 6.3: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/address-poisoning-scams-crypto-web3/

CHAPTER 7

Giveaway and Airdrop Scams

“Free tokens can become expensive mistakes.”

Figure 7.1: Giveaway and Airdrop Scams at a glance

Airdrops and giveaways are a real part of crypto: projects reward early users and promote new tokens. Scammers copy them to make you connect, sign, pay or share data. The bait is always something free; the price is your wallet.

Legitimate airdrops exist, and some require you to connect a wallet and send a claim transaction with a network fee. So the question is never just “does it ask me to connect?” but **where did I find it, and what exactly am I being asked to approve or pay?**

IN THIS CHAPTER

- 7.1 Giveaway and airdrop scams to watch for
- 7.2 Unexpected tokens in your wallet
- 7.3 Illustrative scenario: the token with a website in its name
- 7.4 How to protect yourself
- 7.5 CSF rules for this chapter
- 7.6 If this just happened to you

7.1 Giveaway and airdrop scams to watch for

1. “Send to receive” giveaways

A famous person, project or exchange appears to promise to send back double whatever you send. Live streams, deepfake videos and replies under real posts are common channels.

Example: A live stream with a well-known founder’s face shows an address and a countdown: send any amount and receive twice as much back.

Red flags

- Any promise to return more than you send.
- Countdowns and live “winner” lists.
- Famous names on accounts that are not their main channels.

How to avoid

- Never send crypto to receive crypto. There are no exceptions.
- Report the stream or post to the platform.

2. Fake airdrop claim sites

Sites that copy a real or invented airdrop and ask you to connect and approve or sign to claim. The approval or signature hands your tokens to a drainer.

Example: A post announces an airdrop for holders of a popular token, with a claim link. The page asks for an approval on your largest token balance.

Red flags

- Claim links in replies, ads or direct messages.
- Approval requests for tokens unrelated to the airdrop.
- Short deadlines.

How to avoid

- Find airdrops only on the project’s official website and main channels.
- Claim from a Disposable wallet.
- Check exactly what you are asked to approve or sign.

3. Pay-to-claim and eligibility fees

You are told you are eligible for a reward but must first pay a fee, “gas deposit” or tax to a specific address before it can be released.

Example: A message says your wallet qualifies for a large airdrop and asks you to send a small amount of ETH to activate the claim.

Red flags

- A fee paid to an address instead of a normal network fee for a transaction you send yourself.
- Eligibility you never applied for.

How to avoid

- A real claim costs only the network fee of your own claim transaction.
- Never send funds to an address to unlock a reward.

4. Data-harvesting airdrops

Forms that ask for personal data, ID documents, wallet details or the recovery phrase to “register” for an airdrop.

Example: A registration form for an upcoming airdrop asks for your email, phone number, a photo of your ID and your wallet’s recovery phrase “to verify ownership”.

Red flags

- Any request for your recovery phrase.
- ID documents for a free reward.

How to avoid

- Never give your recovery phrase to anyone.
- Share personal data only with services you have verified.

5. Fake NFT and token giveaways

Free NFT or token drops that lead to mint or claim pages with hidden approvals, often promoted after a project’s social account is hacked.

Example: A project’s hacked account announces a surprise free mint for loyal holders.

Red flags

- Surprise drops with urgency.
- Announcements that appear only on one channel.

How to avoid

- Check announcements across the project's website and several official channels.
- Mint and claim only from a Disposable wallet.

Type	What you are asked to do	Key red flag	How to avoid
Send to receive	Send crypto first	Promise to return more	Never send to receive
Fake claim site	Connect and approve or sign	Approval unrelated to the airdrop	Official channels, Disposable wallet
Pay to claim	Pay a fee to an address	Fee instead of normal gas	Never pay to unlock rewards
Data harvesting	Fill in a form	Recovery phrase or ID requested	Never share the phrase
Fake NFT or token drop	Mint or claim	Surprise drop from one channel	Verify across channels

Table 7.1: Giveaway and airdrop scams to watch for

7.2 Unexpected tokens in your wallet

Scammers send tokens to many wallets at once. The token name often contains a website address or says something like "claim your reward". The goal is to get you to visit the site, or to try to swap or sell the token, which can trigger a malicious approval.

What you do	Risk
See the token in your wallet	None. Receiving a token does not give anyone access to your wallet.
Hide it in your wallet app	None. Hiding is a display setting.
Visit the website in its name	High. This is usually a claim or drainer page.
Try to sell, swap or transfer it	Possible approval or signature for a malicious contract. Do not interact with it.

Table 7.2: Unexpected tokens: what is safe and what is not

7.3 Illustrative scenario: the token with a website in its name

This is an illustrative scenario, not a specific reported case.

Chris notices a new token in his wallet worth, according to the wallet, several thousand dollars. Its name includes a web address and the words “claim reward”. He visits the site, which explains that he is one of a few holders selected for a bonus.

The site asks him to connect his wallet and approve the token to “activate” the reward. He approves. Within minutes, his stablecoins are transferred out.

What happened

The token was bait with a fake value. The approval he gave was not for the bait token but for his stablecoins, which the drainer moved immediately.

Key takeaways

- Unexpected tokens with websites in their names are advertisements for drainers.
- A displayed value means nothing for a token you did not buy.
- Hiding the token would have been completely safe.

7.4 How to protect yourself

1. **Never send crypto to receive crypto.**
2. **Find airdrops yourself**, on the project’s website and main channels, never through links in replies, ads or messages.
3. **Claim from a Disposable wallet** that holds nothing else, then move what you receive.
4. **Check every approval and signature**: which token, how much, for which contract.
5. **Expect a real claim to cost only network fees** for the transaction you send yourself.
6. **Hide unexpected tokens** and do not interact with them.

7.5 CSF rules for this chapter

MAIN RULE · SDR-005

Never Connect Your Wallet to Unknown Websites.

Find airdrops through official project channels and claim from a Disposable wallet.

Rule	Statement	Why it applies here
SDR-002	Never Send Crypto to Receive Crypto	The core of every giveaway scam.
GR-008	Keep Long-Term Holdings in a Vault Wallet. Use a Separate Wallet for DApps, Trading, and Web3	A Disposable wallet limits what a fake claim can take.
GR-004	Always Revoke Unused Token Approvals After Interacting with New Smart Contracts	Revoke claim approvals once you are done.

Table 7.3: Supporting CSF rules

7.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: viewed only, approved, signed, exposed seed phrase, sent money to a scammer. Then add the steps for your situation:

If you…	Do this now
sent crypto to a giveaway	Stop. It will not come back, and sending more will not help. Report the post or stream.
approved or signed on a claim site	Follow the approve or sign rows: revoke, and move remaining assets if transfers have started.
paid a claim or eligibility fee	Stop paying. Save the address and report it.

If you…	Do this now
shared your recovery phrase on a form	Treat the wallet as compromised. Follow the seed-phrase row now.
only received or viewed an unexpected token	Nothing is compromised. Hide it and do not interact with it.

Table 7.4: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/airdrop-scams-crypto-web3/

CHAPTER 8

Fake Investment Platforms

“Deposits build trust. Withdrawals reveal the truth.”

Figure 8.1: Fake Investment Platforms at a glance

A fake investment platform looks like a real exchange, trading app, mining service or staking program. You deposit, your balance grows on screen, and early small withdrawals may even work. When you try to take out a larger amount, the platform invents a reason you must pay first: a tax, a fee, a “verification deposit”, a minimum balance. Every payment leads to the next demand.

In CSF’s incident collection, this is one of the largest scam categories. Victims often arrive through someone else: a romance contact (Chapter 10), a job or task offer (Chapter 11), an investment group or an ad. This chapter is about the platform itself and the one rule that exposes it: **a legitimate platform never asks you to pay so you can withdraw.**

IN THIS CHAPTER

- 8.1 Fake investment platforms to watch for
- 8.2 The withdrawal trap
- 8.3 Signals that are not proof
- 8.4 Illustrative scenario: the profitable account
- 8.5 How to protect yourself
- 8.6 CSF rules for this chapter
- 8.7 If this just happened to you

8.1 Fake investment platforms to watch for

1. Fake exchanges and trading apps

A website or app that looks like a professional exchange or trading platform, often with live-looking charts, an app download and a support chat. Prices and balances are simulated.

Example: An “AI trading” app recommended in an investment group shows daily profits from automated trades. The app is not in any regulator’s register.

Red flags

- A platform you heard about from a contact, group or ad, not from your own research.
- Unusually high or steady returns.
- An app installed from a link rather than an official store listing.

How to avoid

- Check the platform in your financial regulator’s register and warning lists before depositing.
- Be suspicious of platforms that only accept crypto deposits.
- Search the platform name together with “scam” and “withdrawal”.

2. Mining, staking and “yield” schemes

Services that promise fixed daily returns for cloud mining, staking, liquidity or “arbitrage”. Many are Ponzi schemes that pay early users with later users’ deposits until they collapse.

Example: A cloud-mining site offers a guaranteed 2% per day on any deposit, with higher “VIP” levels for larger amounts.

Red flags

- Fixed or guaranteed returns.
- Bonus levels for depositing more or bringing friends.
- Vague explanations of where the profit comes from.

How to avoid

- Treat guaranteed returns as a scam signal.
- Ask how the profit is made; if no one can explain it, walk away.
- Never chase “VIP” levels with bigger deposits.

3. Copy-trading and signal groups with a platform

Groups on messaging apps run by a “mentor” or “professor” who shares winning trades and recommends a specific platform to follow them. Group members praising their profits are often part of the scam.

Example: A group on a messaging app shares daily signals. The assistant tells new members to open an account on a partner platform to copy the trades.

Red flags

- A mentor who sends you to one particular platform.
- Many enthusiastic members posting screenshots.
- Pressure to deposit before a “big signal”.

How to avoid

- Use only platforms you chose yourself and verified.
- Treat screenshots as marketing, not evidence.
- Leave groups that push a specific platform.

Type	What you see	Key red flag	How to avoid
Fake exchange or trading app	Professional site, growing balance	Not in any regulator register	Check registers and warnings first
Mining, staking, yield	Fixed daily returns	Guaranteed profit	Ask how the profit is made

Type	What you see	Key red flag	How to avoid
Signal group with a platform	Mentor and happy members	Pushed to one platform	Choose platforms yourself

Table 8.1: Fake investment platforms to watch for

8.2 The withdrawal trap

Almost every fake platform ends the same way. When you ask to withdraw, a new obstacle appears:

- a “tax” or “capital gains fee” that must be paid first;
- a “verification” or “anti-money-laundering” deposit;
- a minimum balance, “credit score” or account level you have not reached;
- a frozen account that a “risk department” will unlock for a fee;
- penalties for “irregular trading”.

THE WITHDRAWAL RULE

If a platform asks you to pay before you can withdraw, treat it as a scam and stop. Legitimate platforms deduct their fees from your balance; they do not need new money to release your own. Paying almost never releases funds. It leads to the next demand, and the balance on the screen may not exist at all.

8.3 Signals that are not proof

Fake platforms invest in looking trustworthy. None of the following proves that a platform is legitimate:

Signal	Why it is not proof
A small test withdrawal worked	Many fake platforms allow early small withdrawals precisely to build trust before larger deposits.
A professional website and app	Templates and app builders make convincing platforms cheap to produce.
Company registration documents	Company registration is not a licence, and documents can be forged.

Signal	Why it is not proof
Reviews, testimonials and social media	Reviews can be bought; group members can be accomplices.
Live chat support	Support exists to keep you depositing and to explain away delays.
A registration number from a financial authority	An anti-money-laundering registration (for example a US FinCEN or Canadian FINTRAC “MSB” number) is not a licence or an endorsement – fake platforms often show one. Check for an actual licence and the regulator’s warning list.

Table 8.2: Signals that are not proof

What does help: checking the platform in your national financial regulator’s register of authorized crypto service providers (in the EU, the register of crypto-asset service providers kept under the MiCA regulation), and checking regulator warning lists. Even a registered name can be copied by a clone site, so confirm that the web address matches the one listed in the register.

8.4 Illustrative scenario: the profitable account

This is an illustrative scenario, not a specific reported case.

Tom meets a friendly contact in an online trading group. She shares her results on a platform that looks like a modern exchange. Tom deposits a small amount, sees steady gains, and successfully withdraws a little profit. Encouraged, he deposits his savings.

A month later his balance shows more than double his deposits. When he asks to withdraw, support tells him he must first pay a 20% tax. After he pays, his account is frozen for “unusual activity”, and unfreezing costs another fee.

What happened

The platform was never connected to any market. The balance was a number in a database, and the small early withdrawal was paid to build trust. The “tax” and the “unfreezing fee” were the next stages of the same scam.

Key takeaways

- A successful small withdrawal is not proof of a real platform.

- The first demand to pay before withdrawing is the moment to stop.
- The contact who introduced the platform is usually part of the scheme.

8.5 How to protect yourself

1. **Choose platforms yourself.** Never use an exchange or investment app recommended by someone you met online.
2. **Check the regulator's register** and warning lists before you deposit, and confirm the web address matches.
3. **Apply the withdrawal rule.** Any demand to pay before you can withdraw ends the relationship.
4. **Distrust guaranteed returns.** Real investments go up and down.
5. **Do not chase losses.** Paying more to recover money already deposited is how losses multiply.
6. **Talk to someone you trust** before large deposits. Scammers isolate; a second opinion breaks the spell.

8.6 CSF rules for this chapter

MAIN RULE · SDR-003

Never Pay to Unlock or Withdraw Funds.

If a platform wants a fee, tax or deposit before you can withdraw, stop and report it.

Rule	Statement	Why it applies here
SDR-007	Verify Projects Before Investing	Checks in the regulator register and warning lists come before any deposit.
SDR-001	Never Trust Unsolicited Crypto Contact	Most victims are introduced to the platform by someone who contacted them.
SDR-006	Question Urgency, Hype and Guaranteed Profits	Guaranteed returns and "big signals" are the bait.

Table 8.3: Supporting CSF rules

8.7 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: platform says pay before withdrawing, sent money to a scammer. Then add the steps for your situation:

If you…	Do this now
are being asked to pay before withdrawing	Stop paying and stop depositing. Do not tell the platform you suspect a scam; save everything first.
deposited through an exchange	Contact that exchange with the transaction hashes and the platform address. It may be able to flag or freeze funds still under its control.
paid by bank transfer or card	Contact your bank immediately and ask about recalling the payment.
installed the platform's app	Uninstall it. If it was installed outside an official app store, follow the malware row.
shared ID documents for "KYC"	Watch for identity misuse. Report the loss of the documents where your country offers that, and consider a credit or identity alert.

Table 8.4: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/crypto-exchange-scams/

CHAPTER 9

Token Scams

“Hype isn’t due diligence.”

Figure 9.1: Token Scams at a glance

In a token scam, what you buy is the trap. The token may be a launch or presale that never delivers, a coin pumped by insiders who sell into the buying, a project whose creators pull the liquidity, or a contract that lets you buy but never sell. In every case, the people behind the token control something that buyers do not: the supply, the liquidity, the contract or the promotion.

This chapter brings together three former chapters (token launches, pump and dump, rug pulls) because victims experience them the same way: they buy into hype and are left holding a token that is worth little or cannot be sold. Fake platforms that only show you a balance are covered in Chapter 8.

IN THIS CHAPTER

- 9.1 Token scams to watch for
- 9.2 Signals that are not proof
- 9.3 Illustrative scenario: the community memecoin
- 9.4 How to protect yourself
- 9.5 CSF rules for this chapter
- 9.6 If this just happened to you

9.1 Token scams to watch for

1. Fake launches and presales

A new token is sold before launch through a presale, whitelist or “early access” round. The team collects the money and the token never launches, or launches with most of the supply kept by insiders.

Example: A presale promoted in a chat group promises a fixed launch price and a listing within weeks. After it sells out, the website and team accounts go quiet.

Red flags

- Anonymous teams and vague plans.
- Pressure to buy before a deadline or a price increase.
- Presales paid to a personal wallet address.

How to avoid

- Treat presales as high-risk speculation, not investments.
- Never send funds to an address posted in a chat.
- Assume anything you put into a presale can be lost.

2. Pump and dump

Organizers buy a low-priced token, then promote it through groups, influencers or bots. When outsiders rush in and the price rises, the organizers sell, and the price collapses.

Example: A large chat group announces the “next 100x coin” at a set time. Within minutes the price triples, then falls below where it started.

Red flags

- Coordinated calls to buy at a set time.

- Influencers promoting tokens they hold without saying so.
- Sudden price spikes with no news behind them.

How to avoid

- Do not buy because a group or influencer says now.
- Ask who is selling to you when everyone is buying.
- Check trading activity on a block explorer or market data site before buying.

3. Rug pulls

The creators remove the liquidity that lets people trade the token, mint new tokens to sell, or simply abandon the project after collecting funds. Holders are left with tokens they cannot sell at any meaningful price.

Example: A DeFi project with high advertised yields attracts deposits. Overnight, the creators remove the liquidity and delete their social accounts.

Red flags

- Liquidity that is not locked, or locked only briefly.
- A few wallets holding most of the supply.
- Contracts that let the owner mint tokens or change fees.

How to avoid

- Check holder distribution and liquidity before buying.
- Avoid tokens whose owner can mint or change rules at will.
- Size any position as money you can afford to lose.

4. Honeypot tokens

The token contract allows buying but blocks or heavily taxes selling for everyone except the creators. The price chart looks healthy because nobody else can sell.

Example: A token rises steadily with many buyers and almost no sells. When you try to sell, the transaction fails or loses nearly everything to a hidden fee.

Red flags

- Many buys and almost no sells.
- Unusual sell taxes or failed sell transactions reported by others.

- Unverified or recently changed contract code.

How to avoid

- Check whether other holders have been able to sell.
- Use a token-checking tool as one signal, not as proof.
- Avoid tokens you cannot verify.

5. Fake token migrations and swaps

Holders of a real token are told it is migrating to a new contract, or that they must swap through a special site. The “migration” site takes approvals or the tokens themselves.

Example: A message in a project’s community says the token is upgrading and holders must swap through a link within 48 hours.

Red flags

- Deadlines for migrations announced only in chats or replies.
- Swap sites that are not linked from the project’s website.

How to avoid

- Confirm migrations on the project’s website and several official channels.
- Never rush a migration; real ones allow time.

Type	How you lose	Key red flag	How to avoid
Fake launch or presale	Token never delivers	Presale to a personal address	Treat as speculation; small amounts
Pump and dump	Buy high as insiders sell	Coordinated buy calls	Never buy on a signal
Rug pull	Liquidity removed or minted away	Unlocked liquidity, few holders	Check holders and contract powers
Honeypot	Cannot sell	Buys but no sells	Check that others can sell
Fake migration	Approvals or tokens taken	Deadline in a chat	Confirm on official channels

Table 9.1: Token scams to watch for

9.2 Signals that are not proof

Scam tokens invest heavily in looking trustworthy. None of the following proves that a token is safe:

Signal	Why it is not proof
An audit	Audits can be fake, out of date, limited in scope, or ignore the parts that matter. An audit does not stop a team from selling or pulling liquidity.
Locked liquidity	Locks can be short, partial or on a different pool. Check what is locked, how much and until when.
A listing on a tracker or exchange	Many trackers list tokens automatically. A listing says nothing about the team's intentions.
A doxxed or "KYC'd" team	Identity checks by third parties vary widely in quality, and named people can still walk away.
Followers, holders and community size	Followers, holders and engagement can be bought or farmed.
Influencer support	Promoters are often paid or hold the token themselves.

Table 9.2: Signals that are not proof

9.3 Illustrative scenario: the community memecoin

This is an illustrative scenario, not a specific reported case.

A new memecoin launches with a funny mascot and a large online community. Within minutes of launch the market value climbs fast, and posts about "the next big one" spread across social media. Jamie buys after the first big jump.

Over the next hour the price swings, then drops by more than 80% as several large wallets sell. The project's accounts say everything is fine. Days later, on-chain data shows that a handful of wallets bought most of the supply in the first seconds after launch.

What happened

Insiders or snipers bought early and sold into the wave of buyers that the hype attracted. Jamie, like most buyers, arrived after the people who planned the exit.

Key takeaways

- When a token is everywhere, the early buyers are usually already selling.
- Check holder distribution before buying, not after.
- Memecoins are entertainment-priced risk. Never use money you need.

9.4 How to protect yourself

1. **Find out who holds the supply.** If a few wallets hold most of it, they decide the price.
2. **Check what the contract allows.** Can the owner mint, change fees or block sales? If you cannot tell, do not buy.
3. **Check the liquidity.** How much is there, is it locked, and until when?
4. **Do not buy on a signal.** Coordinated buy calls exist to give insiders someone to sell to.
5. **Treat audits, listings and followers as signals, not proof.**
6. **Use a Disposable or Frequent Use wallet** for new tokens, never your Vault, and revoke approvals afterwards. Wallet separation limits approval risks, but it cannot protect money you choose to invest.

9.5 CSF rules for this chapter

MAIN RULE · SDR-007

Verify Projects Before Investing.

Check who holds the supply and whether liquidity is locked. Audits, listings and followers are signals, not proof.

Rule	Statement	Why it applies here
SDR-006	Question Urgency, Hype and Guaranteed Profits	Hype and deadlines are how token scams find buyers.
SDR-008	Never Trust Social Media Popularity	Followers, holders and influencer posts can be manufactured.

Table 9.3: Supporting CSF rules

9.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: approved, sent money to a scammer, platform says pay before withdrawing. Then add the steps for your situation:

If you…	Do this now
hold a token that collapsed or cannot be sold	Do not buy more to “average down” and do not pay anyone to “unlock” selling. Revoke approvals you gave the token or its sites.
were asked to pay a fee to sell or withdraw	Stop. That is the withdrawal trap from Chapter 8. Save the details and report it.
used a migration or swap site	Follow the approval rows: revoke, and move remaining assets if transfers have started.
think the project was fraudulent	Save the contract address, the project’s posts and your transactions, and report it to the police and the platforms that promoted it.

Table 9.4: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/token-launch-scams-crypto-web3/

CHAPTER 10

Romance Scams

“The relationship is the weapon.”

Figure 10.1: Romance Scams at a glance

Romance scams use a personal relationship to steer the victim. It may start on a dating app, through a social media friendship, or with a “wrong number” message that turns into a friendly chat. Over weeks or months, the scammer builds trust and emotional closeness, then introduces money: an emergency, a gift, or most often an investment opportunity.

The investment version is often called **pig butchering**: the victim is “fattened up” with attention and small early profits on a fake platform, then encouraged to invest everything before the platform blocks withdrawals (Chapter 8). Romance scams cause some of the largest individual losses, and victims are frequently targeted again by recovery scams (Chapter 13).

IN THIS CHAPTER

- 10.1 Romance scams to watch for
- 10.2 The stages of a romance investment scam
- 10.3 Illustrative scenario: the wrong number
- 10.4 How to protect yourself
- 10.5 CSF rules for this chapter
- 10.6 If this just happened to you

10.1 Romance scams to watch for

1. Romance investment scams (pig butchering)

A new friend or partner shares their success trading crypto, often credited to a relative or mentor, and offers to teach you. They guide you to a specific platform or app, where your balance grows quickly, until you try to withdraw.

Example: A match on a dating app moves the chat to a messaging app, talks about their uncle's trading strategy, and helps you open an account on a platform you have never heard of.

Red flags

- A new contact who quickly talks about crypto profits.
- A specific platform or app you must use.
- Early small withdrawals that work, followed by pressure to invest more.

How to avoid

- Never invest on a platform suggested by someone you know only online.
- Keep money and romance separate, always.
- Apply the withdrawal rule: paying to withdraw means a scam.

2. Emergency and gift requests

After building closeness, the scammer faces a sudden problem: a medical bill, a blocked account, travel costs, customs fees for a gift they sent you. Crypto is requested because it is "faster".

Example: A partner you have never met in person is stuck at an airport and needs crypto for a fine before they can travel to see you.

Red flags

- Emergencies that only money can solve, again and again.
- Requests for crypto or gift cards.
- Reasons why they cannot video call or meet.

How to avoid

- Do not send money to someone you have not met in person.
- Talk to a friend or family member before sending anything.

3. “Wrong number” and friendship approaches

A message arrives “by mistake”, or a stranger starts a friendly conversation on social media. Politeness turns into regular chats, then into friendship, mentoring or romance, and eventually into crypto.

Example: A text addressed to someone else apologizes for the mistake, then continues: “Since we’re talking anyway…”

Red flags

- A stranger who keeps the conversation going after a mistake.
- Attractive photos, a successful lifestyle and plenty of free time.
- A quick move from one app to another.

How to avoid

- Do not continue conversations that start by mistake.
- Reverse-search profile photos.
- Be wary of anyone who moves the chat to a private app quickly.

4. Fake identities and catfishing

Scammers use stolen photos, invented life stories and increasingly AI-generated images and video to appear real. Some agree to short video calls using face-swapping tools.

Example: A partner finally agrees to a video call. The picture is blurry, the call is short, and afterwards the requests for money continue.

Red flags

- Profiles with few real connections or recent activity.
- Video calls that are always short, dark or “broken”.

- Stories that change under questions.

How to avoid

- Reverse-search photos and look for inconsistencies.
- Remember that a video call is no longer proof of identity.
- Ask someone you trust to look at the profile with you.

Type	How money is requested	Key red flag	How to avoid
Romance investment	Invest on their platform	A platform you must use	Never invest through an online contact
Emergency or gift	Urgent help or fees	Repeated money emergencies	Never send money before meeting
Wrong number or friendship	Later, through mentoring	Conversation continues after a mistake	Do not continue such chats
Fake identity	Any of the above	Short or poor video calls	Reverse-search; ask someone you trust

Table 10.1: Romance scams to watch for

10.2 The stages of a romance investment scam

Stage	What happens	What you can notice
1. Contact	Dating app match, social media message or wrong-number text.	A stranger who is unusually keen to keep talking.
2. Closeness	Daily messages, shared plans, compliments, moving to a private app.	Speed: intimacy within days or weeks.
3. Introduction	Talk of trading success, a relative or mentor with a system.	Money enters a personal relationship.
4. Small wins	You open an account on their platform; small deposits grow and a small withdrawal works.	The platform came from them, not from your research.

Stage	What happens	What you can notice
5. Big push	A special opportunity, a deadline, encouragement to borrow or sell assets.	Pressure to invest more than you planned.
6. Lock-in	Withdrawals blocked by taxes, fees or “frozen” accounts; the partner urges you to pay.	Pay-to-withdraw: the scam is now certain.
7. Re-targeting	“Recovery” services or authorities offer to get your money back for a fee.	Chapter 13: a second scam.

Table 10.2: Stages of a romance investment scam

10.3 Illustrative scenario: the wrong number

This is an illustrative scenario, not a specific reported case.

Daniel receives a friendly message meant for someone else. He replies politely, and the sender, who says she works in finance, keeps chatting. Over the following weeks they talk every day. She mentions that her uncle has a trading strategy that has made her family comfortable and offers to show Daniel how it works.

She helps him open an account on a professional-looking platform. His first small deposit grows quickly, and a small withdrawal arrives in his wallet. Encouraged, he invests most of his savings. When he tries to withdraw, he is told he must first pay a tax on his profits. She urges him to pay it, and offers to lend him part of the amount.

What happened

The contact, the platform and the “tax” were all part of one operation. The early withdrawal was paid to build trust, and the offer to help with the tax was designed to make him pay.

Key takeaways

- Money and new online relationships do not mix.
- A working small withdrawal is part of the script.
- The partner’s urging to pay the fee is the clearest proof of the scam.

10.4 How to protect yourself

1. **Never invest, trade or send crypto because someone you met online suggests it.**
2. **Never use a platform or app chosen by an online contact.** Use only services you found and verified yourself (Chapter 8).
3. **Do not continue "wrong number" conversations.**
4. **Reverse-search photos** and remember that video can be faked.
5. **Talk to someone you trust** before sending money. Scammers work hard to isolate you; a second opinion breaks that.
6. **After a loss, expect recovery offers** and ignore them (Chapter 13).

10.5 CSF rules for this chapter

MAIN RULE · SDR-006

Question Urgency, Hype and Guaranteed Profits.

Never send crypto or invest on a platform suggested by someone you only know online.

Rule	Statement	Why it applies here
SDR-001	Never Trust Unsolicited Crypto Contact	Every romance scam begins with contact you did not seek.
SDR-004	Verify Identities Outside the Message Channel	A real person can be verified outside the chat; a scammer avoids it.
SDR-003	Never Pay to Unlock or Withdraw Funds	The lock-in stage depends on you paying to withdraw.

Table 10.3: Supporting CSF rules

10.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: sent money to a scammer, platform says pay before withdrawing, someone offers to recover your losses. Then add the steps for your situation:

If you…	Do this now
are being asked to pay before you can withdraw	Stop paying and stop depositing. Do not confront the contact yet; save chats, profiles, platform addresses and transaction hashes first.
sent crypto through an exchange	Contact that exchange with the transaction hashes and the platform's deposit addresses.
sent money by bank transfer or card	Contact your bank immediately.
shared ID documents or personal details	Watch for identity misuse and consider an identity alert where your country offers one.
feel ashamed or are being pressured	You are not to blame: these operations are run by professionals. Talk to someone you trust, and report it to the police.

Table 10.4: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/romance-scams-crypto-web3/

CHAPTER 11

Job and Task Scams

“The opportunity may be real. The employer may not.”

Figure 11.1: Job and Task Scams at a glance

Job and task scams target people looking for work or extra income. Some use a fake job in crypto or Web3 to get you to install malware, share your identity documents or run wallet actions. Others are “task” schemes: simple online work such as rating products or “optimizing” apps, where your earnings grow on screen until you must deposit your own money to unlock them.

The common thread: **a real employer never asks you to pay, deposit crypto or install unknown software to get hired or to get paid.**

IN THIS CHAPTER

- 11.1 Job and task scams to watch for
- 11.2 How task scams trap you
- 11.3 Illustrative scenario: the optimization job
- 11.4 How to protect yourself
- 11.5 CSF rules for this chapter
- 11.6 If this just happened to you

11.1 Job and task scams to watch for

1. Task and “optimization” schemes

You are offered easy paid work: liking posts, rating products, “boosting” apps or completing order sets. A dashboard shows commissions. Then a “combination task” puts your account into a negative balance, and you must deposit crypto to continue and unlock your earnings.

Example: A recruiter on a messaging app offers daily pay for 30 minutes of app “optimization”. After a few days, a special task requires a deposit to complete.

Red flags

- Pay for simple clicks that sounds too generous.
- Earnings you can only see on a dashboard.
- Deposits needed to continue or to withdraw.

How to avoid

- Never deposit money to earn money.
- Treat any work paid through a platform dashboard with suspicion.
- Apply the withdrawal rule from Chapter 8.

2. Fake recruiters and interviews with malware

Recruiters for crypto or Web3 roles ask you to complete a coding test from a repository, install a “meeting app”, or try a game or product during the interview. The software steals wallets, passwords and session data.

Example: A recruiter for a Web3 startup schedules a call and asks you to install a video-meeting app from a link they send, because the usual one “does not work” in their region.

Red flags

- Software to install as part of the hiring process.
- Coding tests that must be run on your own machine.
- Interviews on unusual platforms sent by link.

How to avoid

- Never run test code or install software on a device that holds crypto.
- Use standard meeting apps from official stores.
- Run any coding test in an isolated environment, or decline.

3. Upfront-fee jobs

You are hired, then asked to pay for training, equipment, a work visa, a background check or a “starter package”, often in crypto, with a promise of reimbursement.

Example: A new employer asks you to buy a work laptop from their preferred supplier using crypto and promises to refund you with your first salary.

Red flags

- Paying the employer before receiving pay.
- Equipment bought through their supplier.

How to avoid

- Real employers pay you; you do not pay them.
- Do not buy equipment or training through an employer’s link.

4. Identity harvesting and payment-processing roles

Fake job applications collect ID documents, bank details and selfies. Some “jobs” ask you to receive money or crypto and forward it, which can make you part of money laundering.

Example: A “payment agent” role pays a commission for receiving transfers into your account and forwarding them as crypto.

Red flags

- Requests for ID and bank details before any interview.
- Jobs that involve moving other people’s money.

How to avoid

- Share identity documents only after verifying the employer.
- Never receive and forward money for others. It can have legal consequences for you.

Type	What you are asked to do	Key red flag	How to avoid
Task or optimization	Deposit to unlock earnings	Earnings only on a dashboard	Never deposit to earn
Fake recruiter with malware	Install software or run code	Software in the hiring process	Never on a crypto device

Type	What you are asked to do	Key red flag	How to avoid
Upfront-fee job	Pay for training or equipment	Paying the employer	Employers pay you
Identity or payment agent	Send documents or move money	Moving other people's money	Refuse; verify employer first

Table 11.1: Job and task scams to watch for

11.2 How task scams trap you

1. **Easy start.** Small tasks and small payouts that really arrive, to build trust.
2. **Account upgrade.** Higher commissions if you "upgrade" with a deposit.
3. **Combination task.** A special order puts your balance below zero; you must deposit to clear it.
4. **Lock-in.** Each deposit is followed by another combination task, a fee or a "credit score" problem.
5. **Withdrawal blocked.** Earnings stay on the dashboard; only your deposits are real.

Task scams are fake investment platforms (Chapter 8) dressed up as a job. The same rule ends them: never pay to unlock or withdraw.

11.3 Illustrative scenario: the optimization job

This is an illustrative scenario, not a specific reported case.

Aisha is contacted on a messaging app by a recruiter offering part-time remote work: "optimizing" apps by completing sets of ratings on a work platform. The first days go well. She completes tasks, sees commissions and withdraws a small amount.

Then a "lucky combination order" appears with a higher commission, but it puts her balance into the negative. To finish it, she must deposit crypto. She does, and another combination order appears, larger than the first. Her supervisor in the group chat encourages her to keep going so she does not lose her earnings.

What happened

There was no job. The platform showed invented commissions, the early payout was bait, and the combination orders were designed to require ever larger deposits.

Key takeaways

- A job that needs your money is not a job.
- Early real payouts are part of the script.
- Supervisors and coworkers in the group chat are part of the operation.

11.4 How to protect yourself

1. **Never pay, deposit or buy anything to get a job or to get paid.**
2. **Verify recruiters** through the company's official website and careers page, not through the recruiter's own links.
3. **Keep your crypto device separate.** Never install interview software or run test code on a device that holds wallets.
4. **Be wary of unsolicited job offers** on messaging apps, especially with high pay for little work.
5. **Share identity documents only** after you have verified the employer and the role.
6. **Refuse to move money for others.**

11.5 CSF rules for this chapter

MAIN RULE · SDR-002

Never Send Crypto to Receive Crypto.

Real employers never ask you to deposit, pay a fee or buy anything to get paid.

Rule	Statement	Why it applies here
SDR-003	Never Pay to Unlock or Withdraw Funds	The combination-task trap is a withdrawal trap.

Rule	Statement	Why it applies here
TSR-001	Never Install Crypto Software from Unofficial Sources	Interview software and test code are a common malware route.
TSR-006	Separate Devices and Accounts for Crypto Use	A separate device keeps job-hunting malware away from your wallets.

Table 11.2: Supporting CSF rules

11.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: sent money to a scammer, platform says pay before withdrawing, installed software. Then add the steps for your situation:

If you…	Do this now
deposited money for tasks	Stop depositing. Save the platform address, chats and transactions and report it. Expect recovery offers.
installed software or ran code for an interview	Follow the malware row from a different device. Treat any wallet used on that device as exposed and move funds to a new wallet created on a clean device.
paid an upfront fee	Stop paying and report the employer to the job platform and the police.
shared ID documents	Watch for identity misuse and consider an identity alert where available.
received and forwarded money for someone	Stop immediately, keep all records and contact the police or a lawyer.

Table 11.3: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/web3-crypto-job-scams/

CHAPTER 12

Blackmail and Extortion Scams

“Fear is the attack.”

Figure 12.1: Blackmail and Extortion Scams at a glance

Blackmail and extortion scams use fear to make you pay. The scammer claims to have something that can hurt you: a recording, your personal data, access to your accounts, or the power to cause you trouble. Payment is demanded in crypto because it is fast and hard to reverse.

Most of these threats are bluffs built from leaked data, but some are not. This chapter covers **remote threats**: emails, messages and calls. Physical threats and attacks against crypto holders at home or in person are covered in the Hackers guide.

IN THIS CHAPTER

- 12.1 Blackmail and extortion scams to watch for
- 12.2 Bluff or real? What to check
- 12.3 Illustrative scenario: the old password
- 12.4 How to protect yourself
- 12.5 CSF rules for this chapter
- 12.6 If this just happened to you

12.1 Blackmail and extortion scams to watch for

1. “I hacked your device” sextortion emails

Mass emails claim that your device was hacked and your webcam recorded you, and demand crypto to delete the recording. To look credible, many include an old password or phone number from a data leak.

Example: An email shows a password you used years ago and demands payment within 48 hours, or the “video” goes to your contacts.

Red flags

- An old password or phone number as “proof”.
- No actual evidence of a recording.
- A countdown and a wallet address.

How to avoid

- Do not reply or pay. These emails are sent to thousands of people.
- Change the leaked password wherever you still use it and turn on two-factor authentication.

2. Sextortion with real images

Someone builds a relationship, often posing as a romantic interest, persuades the victim to share intimate images, and then threatens to send them to family or followers unless paid. This version is real and targets adults and teenagers.

Example: A new online contact asks for photos, then sends a list of the victim’s followers and demands crypto within an hour.

Red flags

- Fast intimacy with a new online contact.
- A sudden switch to threats and deadlines.

How to avoid

- Do not pay: payment usually leads to more demands.
- Stop contact, keep the evidence, report the account to the platform and to the police.
- If the victim is under 18, involve a trusted adult and the police immediately; specialist services can help remove images.

3. Leaked-data and doxxing threats

Scammers use personal data from breaches, such as your name, address, phone number or purchase history with a crypto company, to threaten exposure, harassment or “consequences” unless you pay.

Example: A message lists your home address and the hardware wallet you bought, says your holdings are known, and demands payment to keep the information private.

Red flags

- Personal details from a data breach.
- Threats tied to your crypto holdings.

How to avoid

- Do not pay or negotiate. Save the message and report it to the police.
- Review your physical security and keep your holdings private (see the Hackers guide).

4. Fake legal and authority threats

Messages claim you face arrest, a lawsuit, tax penalties or account seizure unless you pay a settlement in crypto. This overlaps with authority impersonation (Chapter 2).

Example: An email that looks like a court notice says you must pay a settlement in crypto to avoid prosecution for “illegal trading”.

Red flags

- Legal threats delivered by email or chat.
- Settlements payable in crypto.

How to avoid

- Courts and authorities do not settle cases in crypto through email.
- Check with the authority directly, using contact details from its official website.

Type	The threat	Key red flag	How to avoid
“Hacked device” email	A recording that does not exist	Old password as proof	Do not reply; change the password

Type	The threat	Key red flag	How to avoid
Sextortion with real images	Sharing intimate images	Fast intimacy, then threats	Do not pay; report; get support
Leaked data and doxxing	Exposure or harassment	Breach data about your crypto	Do not pay; report; review security
Fake legal threat	Arrest, lawsuit, seizure	Settlement payable in crypto	Verify with the real authority

Table 12.1: Blackmail and extortion scams to watch for

12.2 Bluff or real? What to check

Question	If yes
Does the message contain only data that has been leaked before (old password, email, phone)?	Very likely a mass bluff.
Is there specific, verifiable evidence (an actual image you shared, details only one person knows)?	Treat it as real: do not pay, preserve evidence, report to the police.
Is there any threat to your physical safety or your family?	Contact the police immediately.
Does the sender offer to “delete everything” after one payment?	Payment rarely ends it; it marks you as someone who pays.

Table 12.2: Bluff or real: what to check

12.3 Illustrative scenario: the old password

This is an illustrative scenario, not a specific reported case.

Priya receives an email with a subject line containing a password she used years ago. The sender says malware on her computer recorded her through the webcam and threatens to send the video to everyone in her contacts unless she pays in Bitcoin within 48 hours.

She is frightened because the password is real. Instead of paying, she searches the opening line of the email and finds hundreds of people who received the same message.

What happened

The password came from an old data breach. There was no malware and no recording. The same email had been sent to thousands of addresses from the same leaked list.

Key takeaways

- A real old password proves a data leak, not a hacked device.
- Mass extortion emails rely on fear and a short deadline.
- The right response is to change the password, not to pay.

12.4 How to protect yourself

1. **Do not pay and do not negotiate.** Payment rarely ends extortion.
2. **Change leaked passwords** wherever you still use them, use a password manager, and turn on two-factor authentication.
3. **Keep your crypto holdings private.** Do not share balances, purchases or wallet addresses publicly.
4. **Be careful with intimate images** and with new online contacts who push for them.
5. **Keep evidence** and report to the platform and the police.
6. **Take threats to your physical safety seriously** and call the police immediately.

12.5 CSF rules for this chapter

MAIN RULE · GR-005

Never Follow Urgent Support or Security Instructions. Exit the Channel and Re-Enter Through the Official App or URL.

Don’t pay or negotiate. Keep the evidence and report it. If your safety is at risk, contact the police.

Rule	Statement	Why it applies here
SDR-004	Verify Identities Outside the Message Channel	Legal and authority threats must be checked with the real authority.

Rule	Statement	Why it applies here
SDR-001	Never Trust Unsolicited Crypto Contact	Extortion arrives as contact you did not expect.

Table 12.3: Supporting CSF rules

12.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: being threatened or extorted, compromised account. Then add the steps for your situation:

If you…	Do this now
received a “hacked device” email	Do not reply. Change the leaked password everywhere you use it and enable two-factor authentication. Delete or report the email.
are being threatened with real images	Stop contact, do not pay, save the evidence and report the account and the threat to the platform and the police. Talk to someone you trust.
already paid	Stop paying. Further payments usually bring further demands. Report the address and the messages to the police.
are threatened with physical harm	Contact the police immediately and follow the physical security guidance in the Hackers guide.

Table 12.4: Chapter-specific first actions

AFTER A LOSS

Expect follow-up offers to recover your money. They are a second scam. See Chapter 13, Recovery Scams.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/blackmail-extortion-scams-crypto-web3/

CHAPTER 13

Recovery Scams

“The second scam targets the first loss.”

Figure 13.1: Recovery Scams at a glance

After a loss, many victims search for help, post about what happened or file reports. Recovery scammers watch for exactly that. They pose as recovery firms, lawyers, “ethical hackers”, blockchain investigators or even police units, and they promise to trace, freeze or return your crypto. Then they charge fees, ask for wallet access, or both.

Recovery scams hit people at their most vulnerable, and they often take more than the original scam. This chapter explains how they work, what legitimate help looks like, and what to do if you have already paid.

IN THIS CHAPTER

- 13.1 Recovery scams to watch for
- 13.2 What legitimate help looks like
- 13.3 Illustrative scenario: the recovery dashboard
- 13.4 How to protect yourself
- 13.5 CSF rules for this chapter
- 13.6 If this just happened to you

13.1 Recovery scams to watch for

1. Fake recovery companies and “fund recovery” services

Professional-looking websites and ads that claim a high success rate in recovering stolen crypto. After a free “assessment” they ask for an upfront fee, then more fees for “legal costs”, “blockchain tracing” or “release taxes”.

Example: After searching for help, a victim finds a company with testimonials and a recovery guarantee. It asks for 10% of the lost amount in advance to start the case.

Red flags

- Guaranteed or near-guaranteed recovery.
- Fees paid upfront, especially in crypto.
- Testimonials you cannot verify.

How to avoid

- Treat any recovery guarantee as a red flag.
- Never pay upfront to recover crypto.
- Report to the police first; let official processes run.

2. “Ethical hackers” and reply-guy recovery

Accounts reply under posts about losses, or in group chats, recommending a “hacker” who “got my funds back”. Several accounts may vouch for the same contact.

Example: Under a public post about a stolen wallet, three accounts recommend the same “blockchain expert” and share a messaging handle.

Red flags

- Unsolicited recommendations under your post.
- Several accounts praising the same person.
- Claims of hacking scammers or the blockchain to get funds back.

How to avoid

- Ignore and report these replies.
- Remember that no one can hack a blockchain to reverse a transfer.
- Do not share details of your loss publicly with contact information.

3. Fake police, regulators and lawyers

Scammers impersonate police units, international agencies, regulators or law firms. They say they have found your funds or arrested the criminals, and that a fee, tax or deposit is needed to release the money to you.

Example: An email that looks official says a cybercrime unit has recovered your crypto and that you must pay a processing fee to a wallet before it can be returned.

Red flags

- A recovery message you did not request from an “authority”.
- Fees to release recovered money.
- Official-looking documents sent by email or chat.

How to avoid

- Police do not charge victims to investigate a case or to return funds.
- Contact the agency through its official website to check any message.
- If you need a lawyer, find one yourself through your national bar association.

4. Recovery through the original scam

The original platform or contact returns with a new story: a “withdrawal department”, a “compensation program” or a “refund” for victims, each requiring a payment first.

Example: Weeks after a fake platform blocked withdrawals, a “compliance officer” from the same platform offers a refund once a final “clearance fee” is paid.

Red flags

- Contact from the platform or person who caused the loss.
- A refund or compensation that needs a payment first.

How to avoid

- Treat any contact from the original scam as part of it.
- Stop all payments and save the messages for your report.

5. Requests for wallet access

Some recovery scammers ask for your recovery phrase, ask you to connect your wallet to a “recovery tool”, or ask you to install remote-

access software “to trace the funds”. The goal is whatever you still have left.

Example: A “forensic analyst” asks you to connect your wallet to a tracing site so the software can “match your transactions”. The site requests a token approval.

Red flags

- Any request for your recovery phrase.
- Recovery tools that need a wallet connection or approval.
- Remote-access software for “tracing”.

How to avoid

- Never share your recovery phrase or install remote-access software.
- Tracing uses public blockchain data; no one needs your keys to do it.

Type	How it reaches you	Key red flag	How to avoid
Fake recovery company	Search results and ads	Guaranteed recovery for a fee	Never pay upfront
“Ethical hacker”	Replies under your posts	Several accounts vouch for one contact	Ignore and report
Fake police or lawyer	Official-looking email or call	Fee to release recovered funds	Verify through official websites
Original scam returns	Same platform or contact	Refund that needs a payment	Stop all payments
Wallet access request	“Recovery tool” or support chat	Seed phrase, approval or remote access	Never share access

Table 13.1: Recovery scams to watch for

13.2 What legitimate help looks like

A confirmed blockchain transfer generally cannot be reversed. What can sometimes help is official action on funds that pass through regulated services:

Legitimate route	What it can do	What it cannot do
Police or national cybercrime service	Open a case, work with exchanges and other authorities, and in some cases seize funds.	Promise recovery or timelines. They do not charge you to investigate.
The exchange that received the funds	Freeze funds still on its platform after a report, and share data with authorities.	Reverse a blockchain transfer or act on funds that have already left.
A lawyer you choose yourself	Advise on civil claims and work with authorities.	Guarantee recovery. Be careful with anyone who contacted you first.

Table 13.2: Legitimate routes after a loss

Legitimate helpers rarely contact you first – real police sometimes do, so verify any contact through the agency's official website before you reply. They do not guarantee results, do not ask for your recovery phrase or remote access, and do not ask for upfront payments in crypto.

13.3 Illustrative scenario: the recovery dashboard

This is an illustrative scenario, not a specific reported case.

After losing money to a fake trading platform, Sarah posts about it in a forum. A day later she is contacted by a "digital asset recovery" company. It asks for her transaction hashes and soon reports that it has traced her funds.

She gets access to a client dashboard that shows her funds as "recovered" and "pending release". To release them, she must pay a release fee, then a tax, then an "anti-money-laundering certificate".

What happened

The recovery company was run by the same kind of scammers as the original platform, possibly the same people. The dashboard was another fake balance, and each fee was another payment to them. The pattern is the same as the withdrawal trap in Chapter 8.

Key takeaways

- A dashboard showing "recovered" funds proves nothing.
- Pay-to-release is a scam signal, whether the platform calls itself an exchange or a recovery service.

- Unsolicited contact after you post about a loss should be treated as hostile.

13.4 How to protect yourself

1. **Report through official channels first**: police, the exchange involved, the platform where the scam happened.
2. **Never pay to recover crypto.** No fee, tax, deposit or certificate releases stolen funds.
3. **Never share your recovery phrase**, connect your wallet or install software for a “recovery”.
4. **Be careful what you post.** Describe your loss publicly without contact details, and expect scammers to reply.
5. **Find help yourself.** If you want legal advice, look up a lawyer through your national bar association; never use one who found you.
6. **Talk to someone you trust.** Losses hurt, and scammers rely on urgency and shame. A second opinion protects you.

13.5 CSF rules for this chapter

MAIN RULE · SDR-010

Never Pay Anyone to Recover Lost Crypto.

No one can reverse a blockchain transfer for a fee. Report to the police and the exchange through official channels.

Rule	Statement	Why it applies here
SDR-003	Never Pay to Unlock or Withdraw Funds	Recovery dashboards use the same pay-to-release trap as fake platforms.
SDR-001	Never Trust Unsolicited Crypto Contact	Recovery scammers find you after you post or report.
GR-001	Never Share Your Seed Phrase	“Recovery tools” and “analysts” often aim for what you have left.

Rule	Statement	Why it applies here
SDR-004	Verify Identities Outside the Message Channel	Fake police and lawyers must be checked through official websites.

Table 13.3: Supporting CSF rules

13.6 If this just happened to you

First find your situation in the triage table (**Start here**). The rows that usually apply to this chapter are: someone offers to recover your losses, sent money to a scammer, exposed seed phrase. Then add the steps for your situation:

If you…	Do this now
paid a recovery service	Stop paying. Save all messages, invoices and payment details, and add them to your police report as a second offense.
shared your recovery phrase or connected your wallet	Follow the seed-phrase or approval rows now, from a clean device.
installed software for “tracing”	Follow the malware row and change passwords from another device.
were contacted by an “authority” about recovered funds	Do not reply. Contact the agency through its official website and report the message.
are still in contact with a recovery service	Stop contact. Do not announce that you know it is a scam until you have saved everything.

Table 13.4: Chapter-specific first actions

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this scam type:

cryptosafetyfirst.com/recovery-scams-crypto-web3/

CSF Rules Index

These are the CryptoSafetyFirst rules used in this book, with the chapters where they apply. The full rule set, including rules for wallet setup, backups and recovery, is published at CryptoSafetyFirst.com. Rule families: GR = Golden Rules, OR = Operational Rules, SDR = Scam Defense Rules, TSR = Technical Security Rules.

Rule	Statement	Chapters
GR-001	Never Share Your Seed Phrase	2, 3, 4, 13
GR-002	Always Verify the Full URL and Domain Before Connecting Your Wallet to Any Website	3, 5
GR-003	Always Use a Hardware Wallet for Long-Term or High-Value Crypto Storage	4
GR-004	Always Revoke Unused Token Approvals After Interacting with New Smart Contracts	5, 7
GR-005	Never Follow Urgent Support or Security Instructions. Exit the Channel and Re-Enter Through the Official App or URL	2, 12
GR-006	Always Send a Small Test Transaction Before Transferring Large Amounts of Crypto	6
GR-008	Keep Long-Term Holdings in a Vault Wallet. Use a Separate Wallet for DApps, Trading, and Web3	5, 7
OR-005	Always Verify the Destination Before Sending Crypto	6
SDR-001	Never Trust Unsolicited Crypto Contact	1, 2, 8, 10, 12, 13
SDR-002	Never Send Crypto to Receive Crypto	1, 7, 11
SDR-003	Never Pay to Unlock or Withdraw Funds	8, 10, 11, 13
SDR-004	Verify Identities Outside the Message Channel	1, 2, 10, 12, 13
SDR-005	Never Connect Your Wallet to Unknown Websites	3, 5, 7
SDR-006	Question Urgency, Hype and Guaranteed Profits	1, 8, 9, 10

Rule	Statement	Chapters
SDR-007	Verify Projects Before Investing	8, 9
SDR-008	Never Trust Social Media Popularity	9
SDR-009	Verify All Links Before Logging In	3
SDR-010	Never Pay Anyone to Recover Lost Crypto	13
TSR-001	Never Install Crypto Software from Unofficial Sources	4, 11
TSR-002	Assume Your Device Can Be Compromised	4
TSR-004	Use Hardware-Based Two-Factor Authentication	3
TSR-005	Enable Withdrawal Whitelists on Exchanges	6
TSR-006	Separate Devices and Accounts for Crypto Use	4, 11
TSR-007	Slow Down Before Clicking or Installing	1

CSF rules used in this book

Keep Learning

Scams change faster than any book. CryptoSafetyFirst.com keeps this guide alive between editions:

- **A page for every chapter, kept up to date as scams change.**
- **How to report a crypto scam**: country-specific reporting links, kept up to date.
- **The Three-Wallet Model**: a free guide and toolkit for setting up Vault, Frequent Use and Disposable wallets.
- **The User Mistakes and Hackers guides**, for the losses that are not scams.

In crypto and Web3, crossing paths with scams is inevitable. Becoming a victim is not. Knowledge and awareness are your best defense.

cryptosafetyfirst.com