2026 EDITION

THE CRYPTO AND WEB3 USER MISTAKES PREVENTION GUIDEBOOK

DO'S

DON'TS

Avoiding Costly Mistakes: A Practical Guide to Protecting Your Blockchain-Based Assets

JUAN PABLO RENEDO

The Crypto and Web3 User Mistakes Prevention Guidebook

Avoiding Costly Mistakes: A Practical Guide to Protecting Your Blockchain-Based Assets

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 7
How to Use This Book 8
If Something Just Went Wrong 10
Wallet Setup and Custody Choices 14
1.1 Who Holds the Keys 15
1.2 Split Your Funds by Purpose: the Three-Wallet Model® 16
1.3 Setup Mistakes to Watch For 16
1.4 When the Platform Is the Problem 18
1.5 Illustrative Scenario: The Airdrop Wallet 18
1.6 CSF Rules for This Chapter 19
1.7 If This Just Happened to You 19
Seed Phrase and Backups 21
2.1 Seed Phrase, Private Key and Passphrase in Plain English 22
2.2 Seed Phrase Backup Mistakes to Watch For 23
2.3 Backup Methods Compared 24
2.4 Larger Amounts: When One Seed Phrase Is Not Enough 25
2.5 Illustrative Scenario: The House Move 25
2.6 How to Protect Your Seed Phrase Backup 26
2.7 CSF Rules for This Chapter 26
2.8 If This Just Happened to You 27
Passwords, PINs, 2FA and Devices 29
3.1 The Layers of Access Around Your Wallet 30
3.2 Access Mistakes to Watch For 30
3.3 Illustrative Scenario: The New Phone 32
3.4 How to Protect Your Access 32
3.5 CSF Rules for This Chapter 33

3.6 If This Just Happened to You 34
Wrong Address 36
4.1 What Your Wallet Can Catch, and What It Cannot 37
4.2 Address Mistakes to Watch For 38
4.3 Illustrative Scenario: The Address From Last Year 39
4.4 A Send Routine for Every Transfer 40
4.5 CSF Rules for This Chapter 41
4.6 If This Just Happened to You 41
Wrong Network, Token or Memo 43
5.1 Which Mistakes Can Still Be Fixed 44
5.2 Network, Token and Memo Mistakes to Watch For 45
5.3 Illustrative Scenario: The Cheaper Network 46
5.4 Check Network, Token and Memo Before Every Transfer 47
5.5 CSF Rules for This Chapter 48
5.6 If This Just Happened to You 48
Transaction Errors: Fees, Stuck Transactions and Slippage 50
6.1 The Fee and Transaction Terms That Matter 51
6.2 Transaction Mistakes to Watch For 52
6.3 Illustrative Scenario: Paid Twice 53
6.4 Before You Confirm a Transaction 54
6.5 CSF Rules for This Chapter 55
6.6 If This Just Happened to You 55
Updates and Maintenance 57
7.1 One Review Calendar for Your Setup 58
7.2 Maintenance Mistakes to Watch For 58
7.3 Keep It Simple Enough to Use Under Stress 60
7.4 Illustrative Scenario: The Update That Asked for the Words 60
7.5 CSF Rules for This Chapter 61
7.6 If This Just Happened to You 61
Inheritance and Emergency Access 63

8.1 What Your Family Needs – and What They Should Not Hold Yet 64
8.2 Inheritance Mistakes to Watch For 65
8.3 Options for Shared or Delayed Access 66
8.4 A Five-Step Plan 67
8.5 Illustrative Scenario: Two Kinds of Crypto 68
8.6 CSF Rules for This Chapter 68
8.7 If This Just Happened to You 69
Records and Taxes 71
9.1 The Records Worth Keeping 72
9.2 Record-Keeping Mistakes to Watch For 72
9.3 Illustrative Scenario: The Exchange That Closed 74
9.4 CSF Rules for This Chapter 74
9.5 If This Just Happened to You 75
CSF Rules Index 77
Keep Learning 79

About This Edition

The first edition of this guide described eleven common mistakes. Since then, CryptoSafetyFirst has collected and classified real losses reported by crypto users every week – and most of them needed no hacker at all: a lost backup, a wrong network, a missing plan. The 2026 Edition is rebuilt around what that work shows.

What is new

- **Nine chapters in three groups** – access and backups, transactions, maintenance and planning – following the CSF incident taxonomy, so the book, the website and the CSF rules use the same categories.
- **A "Start here" section** for anyone who just made a mistake. It tells you what to do based on what actually happened: wrong network, wrong address, stuck transaction, lost access or a missing backup.
- **New chapters** on wrong network, token or memo – often recoverable – and on records and taxes.
- **CSF rules in every chapter,** with one main rule per mistake and the supporting rules behind it.
- **Corrected and updated advice,** including two offline backups instead of one, 2FA backups that do not depend on one phone, and one review calendar every three months.

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.
- 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.
- Chapter 9 explains which records to keep. It is not tax advice: tax rules differ by country – check the rules where you live or ask a tax adviser.

How to Use This Book

If you…	Go to
just made a mistake – wrong network, wrong address, stuck transaction or lost access	Start here: If Something Just Went Wrong, then the chapter for your situation.
are setting up your wallets	Chapters 1–3, and the Three-Wallet Model guide (free at CryptoSafetyFirst.com). This book uses its terms: Vault, Frequent Use wallet and Disposable wallet.
send crypto regularly	Chapters 4–6: addresses, networks and transactions.
hold crypto for the long term	Chapters 7–9: maintenance, inheritance and records.

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 mistakes to watch for, an illustrative scenario, how to protect yourself, the CSF rules for that mistake, 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. The nine chapters form three groups: Access and Backup Mistakes (1–3), Transaction Mistakes (4–6) and Maintenance and Planning Mistakes (7–9).

Ch	Chapter	Often combined with	Main CSF rule
1	Wallet Setup and Custody Choices	2, 7; Scams guide (fake apps)	GR-008
2	Seed Phrase and Backups	3, 7, 8	OR-002
3	Passwords, PINs, 2FA and Devices	2, 7; Hackers guide (SIM swap)	OR-006
4	Wrong Address	5, 6; Scams guide (address poisoning)	OR-005

Ch	Chapter	Often combined with	Main CSF rule
5	Wrong Network, Token or Memo	4, 6	OR-005
6	Transaction Errors: Fees, Stuck Transactions and Slippage	4, 5	GR-006
7	Updates and Maintenance	2, 3, 8	OR-001
8	Inheritance and Emergency Access	2, 7, 9	OR-007
9	Records and Taxes	8	Key habit

Chapter map: how the mistakes connect

Mistakes rarely come alone. A setup without a plan leads to lost backups; a lost backup leaves heirs locked out; a rushed transfer goes to the wrong network or address. The chapter map shows the most common combinations, so you can read the chapters that belong together.

START HERE

If Something Just Went Wrong

What you should do next depends on what actually happened. Sending on the wrong network is not the same as sending to the wrong address; a stuck transaction is not the same as a failed one; a lost phone is not the same as a lost seed phrase. Some of these can still be fixed – but only if you do not make it worse first.

Find the row that matches what happened. 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 sent crypto on the wrong network, picked the wrong token version or left out a memo or tag	Stop and do not send more. Look the transaction up on the explorer of the network you actually used and save the transaction hash. If you control the receiving address, add that network in your wallet – the funds are often already there. If it went to an exchange, open a ticket through its official app or website with the hash, network and memo. See Chapter 5.	Recovery depends on whoever controls the receiving address. An exchange may refuse or charge a fee; no outside service can do it for you.
You sent crypto to the wrong address	Save the transaction hash. Check whether the address belongs to you (another wallet or account), to an exchange (contact it through its official website) or to a contract. See Chapter 4.	A confirmed transfer cannot be reversed. Nobody can pull it back for a fee.
Your transaction is stuck as pending	Do not send the same payment again. Use “speed up” or “cancel” in the wallet that sent it. If you have no gas left, add a small amount of the network’s native token first. See Chapter 6.	Speeding up or cancelling only works while the transaction is still pending.
A swap returned far fewer tokens, or a failed transaction still cost a fee	Check the slippage setting and the “minimum received” on your next swap. Use the suggested fee and keep a small gas balance. See Chapter 6.	Fees for failed transactions and losses from slippage cannot be refunded.

What happened	What to do now	What this does not fix
Your wallet still opens, but you cannot find the seed phrase	Act now, while the device still works: create a new wallet, write its new seed phrase down twice and keep the copies in separate places, then move your funds to it. See Chapter 2.	If the device fails before you do this, the funds cannot be recovered.
Your phone, computer or hardware wallet is lost, broken or reset	Restore the wallet with your seed phrase – and passphrase, if you set one – on a new or reset device – on a hardware wallet, enter the words only on the device's own screen; for a software wallet, only in its official app. Check that the same addresses appear. See Chapters 2 and 3.	Without the seed phrase, no company can restore a self-custody wallet.
You forgot your PIN, or a hardware wallet reset after wrong attempts	Restore the device from your seed phrase (and passphrase). Then store the new PIN where you can find it. See Chapter 3.	Without the seed phrase, a reset hardware wallet cannot be recovered.
You lost your 2FA phone or cannot log in to an exchange	Use your 2FA backup codes. If you have none, use the exchange's official account recovery – only through its own website or app. Secure your email account first. See Chapter 3.	Official recovery can take days or weeks. Anyone who offers a faster way is a scammer.
Your seed phrase may have been seen, photographed or typed into a website	Treat the wallet as compromised. On a trusted device, create a new wallet with a new seed phrase and move all funds to it now. See Chapter 2.	Changing a PIN or password does not make an exposed seed phrase safe again.
You restored a wallet and it shows an empty balance	Do not panic – the funds are usually still there. Check the passphrase, the wallet app and derivation path, the network, and the exact words and their order. See Chapters 2 and 7.	One wrong word can open a different, empty wallet. Nobody can "find" the funds for you.

What happened	What to do now	What this does not fix
Someone has died or cannot act, and the family needs access	Do not post details publicly and do not pay anyone who offers to recover the funds. Gather the documents. Contact exchanges through their official bereavement or account-recovery process. For self-custody, follow the recovery plan if one exists. See Chapter 8.	Without the recovery information, a self-custody wallet cannot be opened by anyone.
An exchange closed or your transaction history is missing at tax time	Export what is still available, use block explorers for on-chain history, and reconstruct the rest with your bank records. Ask a tax adviser. See Chapter 9.	Lost exchange data usually cannot be recovered. This book is not tax advice.
Someone offers to recover your crypto	Treat it as a scam. Do not pay upfront fees, share your seed phrase or install remote-access software. Report the contact.	No one can reverse a confirmed transfer or recover a lost seed phrase for a fee.

Table 1: What to do next, by what happened

If more than one situation applies

Follow the response for the most serious situation first. For example, if your phone broke and you also cannot find the seed phrase, nothing else matters until you know where the seed phrase is. If your seed phrase may have been exposed, move the funds before you deal with anything else.

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.
- For losses caused by scams or theft: your local police or national cybercrime reporting service. Country links: **cryptosafetyfirst.com/how-to-report-a-crypto-scam/**

BE ALERT FOR RECOVERY SCAMS

After a mistake or a loss, you may be contacted by people who claim they can trace, unlock or recover your crypto. Treat every unsolicited recovery offer as a scam. Do not share your seed phrase or private key, and do not pay anyone who says a fee is needed to release your funds. See **Recovery Scams** in the **Scams Prevention Guidebook**.

What these actions cannot undo

- A confirmed transfer cannot be reversed by anyone.
- Speeding up or cancelling only works while a transaction is still pending.
- A new PIN or password does not make an exposed seed phrase safe again.
- No company can recover a lost seed phrase for a self-custody wallet.

CHAPTER 1

Wallet Setup and Custody Choices

“One wallet, one bad signature – and everything was gone.”

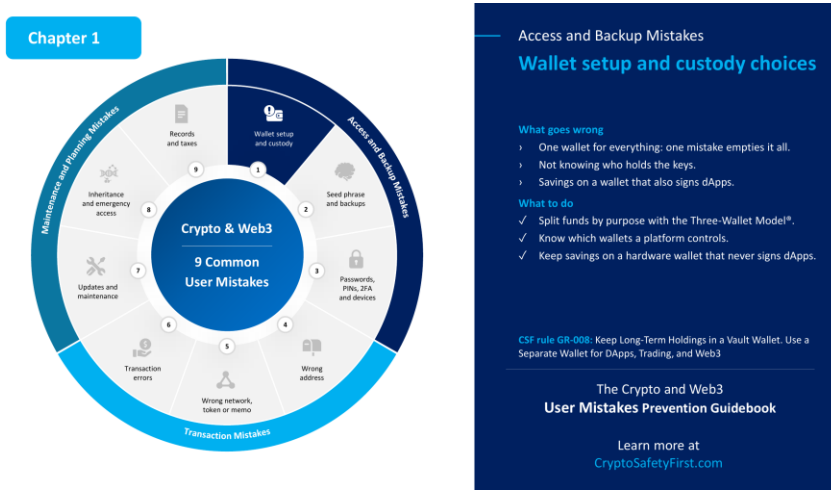

Figure 1.1: Wallet Setup and Custody Choices at a glance

Before any scam, hack or typo, there is a decision most people never consciously make: where their crypto lives, and who controls it. One wallet for everything, savings left on an exchange, or a long-term wallet that also signs every new app – each of these turns a single mistake into a total loss.

This chapter covers the two setup choices that decide how much any later mistake can cost: who holds the keys, and how your funds are split by purpose. The full method is in the free **Three-Wallet Model®** guide; this chapter covers the mistakes.

IN THIS CHAPTER

- 1.1 Who Holds the Keys
- 1.2 Split Your Funds by Purpose: the Three-Wallet Model®
- 1.3 Setup Mistakes to Watch For
- 1.4 When the Platform Is the Problem
- 1.5 Illustrative Scenario: The Airdrop Wallet
- 1.6 CSF Rules for This Chapter
- 1.7 If This Just Happened to You

1.1 Who Holds the Keys

Every place you keep crypto is either a custodial account, where a platform holds the keys, or a self-custody wallet, where you do. Neither is safe by default; they fail in different ways:

Question	Custodial account (exchange, app)	Self-custody wallet
Who holds the keys?	The platform (**custodial wallet**)	You, through your seed phrase (**non-custodial wallet**)
If you lose access	Account recovery with the platform: email, 2FA, identity checks	Only your seed phrase restores the wallet (**Chapter 2**)
Who can block your funds?	The platform: freezes, identity holds, delistings, insolvency	Nobody – but nobody can help you either
What you must back up	Password, 2FA backup codes, the email account (**Chapter 3**)	Seed phrase (and passphrase), wallet details
If the provider disappears	Funds may be frozen or lost in an insolvency	Your seed phrase works in other compatible wallet apps

Table 1.1: Custodial account vs. self-custody wallet

1.2 Split Your Funds by Purpose: the Three-Wallet Model®

The Three-Wallet Model® separates crypto by how it is used, so that the risks of everyday activity never reach your savings. Setup steps and checklists are in the free **Three-Wallet Model® guide** and the **setup post**.

Wallet	Use it for	Rules of thumb
Vault Wallet	Long-term savings	A **hardware wallet** bought from the manufacturer. Rarely used, never connected to dApps, seed phrase backed up offline.
Frequent Use Wallet	Everyday transfers and the apps you trust	Holds only what you need for current activity. Review its approvals regularly.
Disposable Wallet	New dApps, mints, airdrops and anything unfamiliar	Near-zero balance. Replace it instead of letting it grow; retire it when its job is done.
Exchange account	Buying, selling and trading	A transit point, not a home: withdraw what you are not actively trading.

Table 1.2: The Three-Wallet Model® at a glance

1.3 Setup Mistakes to Watch For

1. One Wallet for Everything

Most people start with one wallet app and use it for savings, trading, NFTs and every new app. Each connection and approval adds exposure to all of it. Split your funds by purpose so that a bad signature reaches only the wallet that made it.

2. Not Knowing Who Holds the Keys

An exchange balance, a “wallet” inside an exchange app and a self-custody wallet look similar on screen but behave very differently. Know for each one whether you hold the seed phrase or the platform holds the keys – it decides how you back it up and who can block it.

3. Leaving Long-Term Savings on an Exchange

Exchanges are useful for buying and selling. As a long-term home they add a risk you cannot control: frozen withdrawals, identity holds, delisted coins or an insolvency. Keep on an exchange only what you are actively trading.

4. A Vault Wallet That Signs dApps

The wallet that holds your savings should not connect to new apps, mint NFTs or claim airdrops. Once it signs one malicious transaction or approval, the savings are exposed. Keep the Vault Wallet for rare, deliberate transfers.

5. A Hardware Wallet From the Wrong Source

A hardware wallet from a marketplace, a reseller or a second-hand seller may be tampered with or come with a seed phrase already set – and whoever prepared that phrase controls the wallet. Buy directly from the manufacturer, and create the seed phrase yourself. See **Fake Apps, Extensions and Wallets**.

6. Many Wallets Without a Record

Splitting funds is good; forgetting where they are is not. Wallets from old phones, test setups and airdrops collect small balances nobody watches. Keep one wallet list with each wallet's role, device and backup location.

7. A Disposable Wallet That Grows

A wallet meant for experiments slowly collects tokens, NFTs and approvals until it holds real value. Move anything worth keeping to your Frequent Use or Vault Wallet, and replace the Disposable Wallet instead of letting it grow.

8. Thinking Self-Custody Means Nothing Can Go Wrong

Self-custody removes platform risk, not every risk. Wallet apps can be discontinued – your seed phrase then works in another compatible app – and some wallets use their own recovery methods instead of a standard seed phrase. Know how your wallet is recovered before you put funds in.

1.4 When the Platform Is the Problem

Custodial users lose access in ways self-custody users never see: withdrawals paused for “maintenance”, an identity check that never ends, a coin delisted, or a platform that fails.

- Withdraw what you are not actively trading to your own wallet.
- Turn on a **withdrawal whitelist** so funds can only go to your own addresses.
- Protect the account and its email with a **hardware security key**.
- Download your transaction history regularly – it disappears with the platform (**Chapter 9**).
- In the EU, crypto service providers need authorisation under the MiCA regulation; check a platform in the official register before you deposit.

1.5 Illustrative Scenario: The Airdrop Wallet

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

Daniel keeps his savings and his everyday trading in the same browser wallet. One evening he claims a token airdrop announced on social media and signs what looks like a routine approval. Within minutes, every token in the wallet is gone.

What Happened

The fake airdrop was a scam. What made it a total loss was the setup: the wallet that signed the approval also held his savings. With a Disposable Wallet for the claim, he would have lost almost nothing.

Key Takeaways

- Keep savings in a Vault Wallet that never connects to dApps.
- Use a Disposable Wallet for airdrops and new apps.
- Treat surprise airdrops as suspicious by default.

1.6 CSF Rules for This Chapter

MAIN RULE · GR-008

Keep Long-Term Holdings in a Vault Wallet. Use a Separate Wallet for DApps, Trading, and Web3.

Split funds by purpose so that one mistake can never reach your savings.

Rule	Statement	Why it applies here
GR-003	Always Use a Hardware Wallet for Long-Term or High-Value Crypto Storage	The Vault Wallet keeps its keys off your everyday computer and phone.
TSR-004	Use Hardware-Based Two-Factor Authentication	The exchange account and its email need **phishing-resistant sign-in**.
TSR-005	Enable Withdrawal Whitelists on Exchanges	A **withdrawal whitelist** limits withdrawals to your own wallets, even if the account is taken over.

Table 1.3: Supporting CSF rules

All 32 rules, with what each one prevents: **CSF Crypto Security Rules**.

1.7 If This Just Happened to You

First find your situation in the Start here table at the front of the book. Then add the steps for your situation:

If you…	Do this now
keep long-term savings on an exchange	Set up a Vault Wallet with a hardware wallet bought from the manufacturer, back up its seed phrase offline, send a small test, then move the savings.
use one wallet for savings and dApps	Create a new Vault Wallet for the savings and keep the old wallet only for everyday use – or retire it. Remove old approvals from the old wallet.

If you…	Do this now
signed something suspicious in a wallet with real funds	From a trusted device, create a new wallet with a new seed phrase and move the funds now. Then review approvals on the old one. See **Malicious Contracts and Approvals**.
see an exchange delay or freeze withdrawals	Do not send more funds. Follow only the platform's official announcements, keep your records (**Chapter 9**) and ignore anyone who offers faster withdrawals for a fee. Platforms that demand a fee to withdraw are a scam pattern: see **Fake Investment Platforms**.
bought a used or pre-set hardware wallet	Do not use it for funds, and never use a seed phrase that came with the device. Buy a new one from the manufacturer and set it up yourself.
do not know how many wallets you have	Make a wallet list: name, role, device or app, where the backup is. Retire the ones you no longer need.

Table 1.4: Chapter-specific first actions

AFTER A LOSS

After a drained wallet or a frozen exchange, fake recovery services and fake "support" agents get in touch. Nobody legitimate asks for your seed phrase, remote access or a fee. See **Recovery Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/unsafe-crypto-wallet-setup-risks/

CHAPTER 2

Seed Phrase and Backups

“I wrote it down. I just can’t find where.”

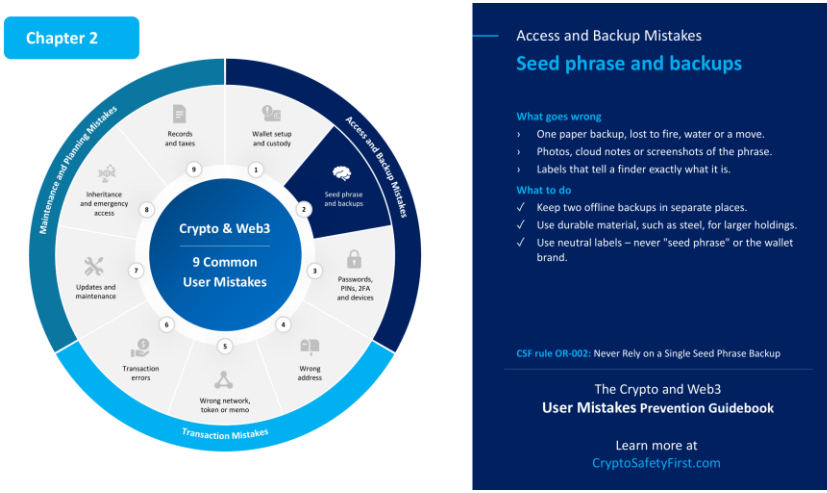

Figure 2.1: Seed Phrase and Backups at a glance

Your seed phrase is the master backup of a self-custody wallet. With it, you can rebuild the wallet on any compatible device. Without it, a lost phone, a broken hardware wallet or a reset app can mean losing everything in the wallet for good. No company, support line or password reset can bring it back.

Most seed phrases are not stolen. They are lost: never written down, written down once and thrown away by accident, saved in a place that later fails, or hidden so cleverly that nobody can find them again. This chapter covers how backups fail and how to build one that still works years from now, for you or for someone acting on your behalf.

IN THIS CHAPTER

- 2.1 Seed Phrase, Private Key and Passphrase in Plain English
- 2.2 Seed Phrase Backup Mistakes to Watch For
- 2.3 Backup Methods Compared
- 2.4 Larger Amounts: When One Seed Phrase Is Not Enough
- 2.5 Illustrative Scenario: The House Move
- 2.6 How to Protect Your Seed Phrase Backup
- 2.7 CSF Rules for This Chapter
- 2.8 If This Just Happened to You

2.1 Seed Phrase, Private Key and Passphrase in Plain English

Your crypto is not stored on your phone or hardware wallet. It sits on the blockchain. Your wallet holds the keys that let you move it.

- **Seed phrase.** A list of 12, 18 or 24 words that your wallet creates when you set it up. It can recreate every key and address in the wallet. Anyone who has it controls your funds; if you lose it, nobody can recreate it for you. See **Seed Phrase** in the CSF Glossary.
- **Private key.** The key for a single address. Your seed phrase generates the private keys of every account created from it, so those need no separate backup. Exception: an account you imported with a private key is not covered by the seed phrase – back that key up separately, or move its funds to an account created from your seed phrase. Do not export them unless you have a specific reason.
- **Passphrase (optional).** Some wallets let you add an extra word or phrase on top of the seed phrase. It creates a completely different wallet. Restore the seed phrase without the exact passphrase and you get a valid but empty wallet, with no error message. If you use a passphrase, it needs its own backup, stored separately from the seed phrase. See **Passphrase**.

One more detail matters when you restore: different wallet apps can use different derivation paths or address types. If you restore a correct seed phrase in a different app and see an empty balance, your funds are usually still there; the app is looking at different addresses. Note the

wallet app or device you used with your backup, and see **Derivation Path** before trying anything else.

A seed phrase looks like a numbered list of plain words: word 1, word 2 … word 24. This guide shows no real example. Seed phrases printed anywhere are watched by automated tools, and people sometimes reuse what they see.

2.2 Seed Phrase Backup Mistakes to Watch For

1. No Backup at All

The wallet offers to show the seed phrase “later”, and later never comes. Months on, a phone reset, a broken device or a deleted app takes the only copy with it. Never put funds into a wallet before the backup is written down and checked.

2. A Digital Copy

Screenshots, phone notes, cloud drives, email drafts, chat messages to yourself and password apps feel safe because they are always at hand. They fail in two ways: the account or device is lost, or someone else gets in. Photos and notes also sync to the cloud on their own. A seed phrase belongs offline only, with no exceptions for encrypted files.

3. A Single Paper Copy

One sheet of paper is one fire, one leak, one house move or one tidy-up away from being gone. Paper also fades and gets misread. Keep at least two copies in separate places, and use durable material for larger amounts.

4. A Backup You Never Tested

A missing word, a misspelling or the wrong order makes the whole backup useless, and you only find out when you need it. The same applies to a passphrase or PIN you forgot to record. Test the backup once, right after you create it, with no funds at risk: on a hardware wallet use its built-in backup check, or restore it on a second hardware wallet; for a software wallet, restore it in the official app on a device you trust. Never type a hardware wallet’s seed phrase into a phone or computer.

5. A Forgotten Place or a “Clever” Hiding Method

A seed phrase hidden in a book, split into a puzzle, written in invisible or UV ink, or encrypted with a key nobody else knows can be lost to time or to your own memory. Invisible inks fade, and your family will not know to look. Simple and documented beats clever: write down where the backups are, in a separate place, without the words themselves.

6. Labels That Tell a Finder What It Is

An envelope marked “seed phrase”, “recovery words” or with a wallet brand is an invitation for anyone who finds it. Use a neutral label that means something only to you and the people in your plan.

7. An Exposed Seed Phrase

Typing the words into a website “to verify” the wallet, showing them to “support”, or reading them aloud on a call exposes them. So does a photo that synced to the cloud. Once a seed phrase may have been seen, treat it as compromised, even if nothing has happened yet.

2.3 Backup Methods Compared

Method	Main risk	Use it for
Single paper copy	Fire, water, fading, thrown away by mistake	Short-term only, until you make a second copy
Two or more paper copies in separate places	Each copy can be read by whoever finds it	Small and medium amounts
Steel or other metal backup	Can still be found and read; cost	Savings and long-term holdings (**how to store a seed phrase on steel**)
Memory only	Forgetting, illness, accidents; nobody else can recover	Never as the only backup
Photo, file, cloud, email or password app	Account loss, device loss, hacking, automatic sync	Never

Table 2.1: Seed phrase backup methods compared

2.4 Larger Amounts: When One Seed Phrase Is Not Enough

For savings you plan to hold for years, a single seed phrase is a single point of failure: one copy found is everything lost, one copy lost may be everything gone. Two setups reduce this, at the cost of more complexity:

- **Multisig:** several keys, each on its own device, with a set number needed to move funds (for example 2 of 3). Losing one key does not lose the funds, and finding one key is not enough to take them – but keep the wallet's configuration file (descriptor) with every key backup, or the keys alone may not restore it.
- **Split backups (Shamir):** the backup is split into several shares, and a set number of shares rebuilds the wallet. Supported by some hardware wallets.

Both add steps that you, and anyone who inherits your crypto, must understand. Set them up only if you will document them clearly and test the recovery. For how this fits your Vault Wallet, see **The Three-Wallet Model®**; for leaving instructions to others, see **Chapter 8: Inheritance and emergency access**.

2.5 Illustrative Scenario: The House Move

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

Mira set up a hardware wallet three years ago and wrote her 24 words on the card that came in the box. She kept the card in a folder with the device's paperwork. During a house move, the folder went into a box of old papers. The box was later emptied into recycling.

Last month the hardware wallet stopped turning on. Mira bought a new device, opened the folder to restore the wallet, and found nothing. The coins are still on the blockchain. Nobody can move them.

What Happened

There was one copy, kept with ordinary paperwork, and never tested or recorded anywhere. The device failing was not the problem; devices fail. The problem was a single copy, filed with ordinary paperwork.

Key Takeaways

- A hardware wallet is only as safe as its backup.

- Keep at least two copies in separate places, away from everyday papers.
- Write down where the backups are, and check them on a schedule.

2.6 How to Protect Your Seed Phrase Backup

- Write the seed phrase down by hand when you create the wallet, before you send any funds to it.
- Keep at least two copies in separate, secure places, so one fire, flood or theft cannot take both.
- Use durable material, such as a **steel backup**, for savings and long-term holdings.
- Keep the seed phrase offline only: no photos, files, cloud, email, chat or password apps.
- Test the backup once with no funds at risk (on a hardware wallet with its built-in backup check), and check it is still readable every three months (review calendar in Chapter 7).
- Record which wallet app or device created it, and any passphrase, separately from the words.
- Use neutral labels. Never write “seed phrase” or the wallet brand on the envelope or container.
- Write down where the backups are, without the words, and include it in your **emergency plan (Chapter 8)**.

2.7 CSF Rules for This Chapter

MAIN RULE · OR-002

Never Rely on a Single Seed Phrase Backup.

Keep at least two offline copies in separate places, and test that they work.

Rule	Statement	Why it applies here
GR-001	Never Share Your Seed Phrase	Anyone who sees the words controls the wallet, including “support” and recovery services.

Rule	Statement	Why it applies here
GR-007	Never Store Your Seed Phrase in Cloud Storage, Email, or Screenshots	Digital copies are lost with the account or found by whoever gets into it.
OR-004	Never Store Seed Phrases Only in Digital Form	A backup that exists only on a device fails when the device does.
OR-001	Test Your Wallet Recovery Before Trusting It	An untested backup can hide a missing or misspelled word for years.
OR-003	Document How Your Wallet Was Created	The wallet app, device, passphrase and derivation path decide whether a restore shows your funds.

Table 2.2: Supporting CSF rules

All 32 rules, with what each one prevents: **CSF Crypto Security Rules**.

2.8 If This Just Happened to You

First find your situation in the Start here table at the front of the book. Then add the steps for your situation:

If you…	Do this now
lost the backup, but the wallet still opens	Create a new wallet, back up its seed phrase properly (two copies, tested), and move all funds to it now. Do not delete or reset the old app until the funds have arrived.
lost the backup and the wallet no longer opens	Search every place it could be, and check for a second device or app where the same wallet is still installed. Without the seed phrase or a working copy of the wallet, nobody can restore it.
think someone saw your seed phrase	Treat it as compromised. Create a new wallet with a new seed phrase and move everything now. Adding an account in the same wallet is not enough.
have a damaged or incomplete backup	Do not type the words into any website or give them to anyone. If the wallet still opens, move the funds to a new, properly backed-up wallet first. A few unreadable words can sometimes be worked out offline with specialised recovery tools – ask only someone you know personally, and never share the words.

If you…	Do this now
restored the right words but see an empty wallet	Check the passphrase, then the wallet app and derivation path before you assume a loss. See **Derivation Path** in the CSF Glossary.

Table 2.3: Chapter-specific first actions

AFTER A LOSS

Expect offers to “recover” your seed phrase or wallet. Nobody can recover a lost seed phrase for a fee, and anyone who asks for your words will take the funds. See **Recovery Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/lost-seed-phrase-crypto-web3/

CHAPTER 3

Passwords, PINs, 2FA and Devices

“The coins were safe. I just couldn’t get to them.”

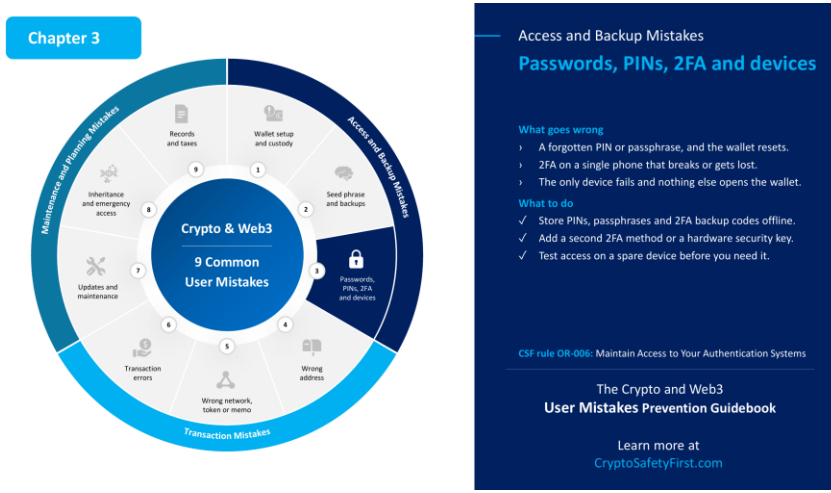

Figure 3.1: Passwords, PINs, 2FA and Devices at a glance

Your seed phrase can be safe, and you can still be locked out. Around every wallet sits a ring of smaller keys: the PIN on a hardware wallet, the password of a wallet app, the login and two-factor authentication (2FA) of an exchange account, the email address that can reset all of them, and the phone or computer they live on.

Lose one of them without a backup, and the result looks the same as a lost seed phrase: funds you can see but cannot move. This chapter covers how people lock themselves out, and the simple backups that get you back in.

IN THIS CHAPTER

- 3.1 The Layers of Access Around Your Wallet
- 3.2 Access Mistakes to Watch For
- 3.3 Illustrative Scenario: The New Phone
- 3.4 How to Protect Your Access
- 3.5 CSF Rules for This Chapter
- 3.6 If This Just Happened to You

3.1 The Layers of Access Around Your Wallet

A seed phrase restores a self-custody wallet. It does nothing for an exchange account, your email or your password manager. Each layer needs its own way back in:

Layer	What locks you out	The backup that gets you back in
Self-custody wallet (app or hardware wallet)	Lost, broken or reset device; forgotten PIN or app password	Your seed phrase (and passphrase, if you set one) – see **Chapter 2**
Exchange or other custodial account	Lost 2FA device, forgotten password, locked email	2FA backup codes or a second security key; access to the account email
Email account	Forgotten password, lost phone number, lost 2FA	Its own recovery codes and a second security key – this account resets the others
Password manager	Forgotten master password, lost device	The written master password or the manager's emergency kit, stored offline
Phone or computer	Loss, theft, damage, a forgotten device PIN	Nothing on the device that exists only there

Table 3.1: The layers of access around your wallet

Malware, keyloggers and remote-access tools can also take over a device. That is an attack, not a mistake, and is covered in the Hackers guide. This chapter is about the access you lose on your own.

3.2 Access Mistakes to Watch For

1. A Forgotten PIN or Wallet Password

Hardware wallets and wallet apps protect your keys with a PIN or password. Many hardware wallets reset themselves after a set number of wrong PINs – check how many your device allows. A reset is harmless if your seed phrase is safe and complete, and final if it is not.

2. A Passphrase Nobody Wrote Down

An optional **passphrase** creates a separate wallet. Forget it, and the seed phrase alone opens an empty wallet. It needs its own written backup, stored separately from the seed phrase (Chapter 2).

3. 2FA on a Single Phone

An authenticator app on one phone is one lost, broken or replaced phone away from a lockout. The same goes for passkeys saved only on that phone. Most services give you backup codes when you switch on 2FA; many people never save them, and a new phone without migrating the codes locks them out.

4. SMS as the Only Second Factor

Text-message codes fail when you change your number, travel or lose your SIM, and they can be taken over in a SIM swap. Use an authenticator app or a hardware security key instead, and keep SMS only as a last fallback where a service insists. See **SIM Swap Scams**.

5. An Email Account That Can Reset Everything

Most exchanges let you reset a password through email. That makes your email the master key to your crypto accounts: lose it and you are locked out of all of them; let someone else in and they can reset them. Protect it with its own strong password and a hardware security key, and keep its recovery codes offline.

6. A Password Manager With No Way Back In

A password manager is a good place for passwords – and a single point of failure if its master password exists only in your head. Write the master password or the manager's emergency kit down and store it offline. A seed phrase does not belong in a password manager (Chapter 2).

7. Everything on One Device

Wallet app, authenticator, password manager and email on the same phone means one theft or one broken screen takes all of them at once. Spread them: a second security key, backup codes on paper, and at least one other device that can log in to your email.

8. A Second-Hand or Pre-Set Device

A hardware wallet bought second-hand, or one that arrives with a PIN or seed phrase already set, may be controlled by someone else. Buy directly from the manufacturer and always create a new seed phrase yourself. Tampered devices are an attack, covered in the **Hackers guide**.

3.3 Illustrative Scenario: The New Phone

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

Tom upgrades his phone and hands the old one in at the shop. A week later he tries to log in to his exchange account. The password works; the 2FA code does not. His authenticator app is on the old phone, and he never saved the backup codes.

The exchange's recovery process asks for an identity check and a waiting period. Meanwhile he cannot sell, withdraw or change settings. A message from "support" offers to speed things up if he installs a remote-access app. He almost does.

What Happened

The authenticator lived on one device, with no backup codes and no second method. The phone change itself was harmless; moving without migrating the 2FA codes was the mistake. The "support" message was a scam aimed at people who are locked out.

Key Takeaways

- Save the backup codes the moment you switch on 2FA.
- Move 2FA to the new phone before you hand in the old one.
- Real support never asks for remote access or your seed phrase.

3.4 How to Protect Your Access

- Save 2FA backup codes on paper when you switch on 2FA, and store them with your other recovery documents.
- Use a **hardware security key** or an **authenticator app** instead of SMS, and register a second key or device as a backup.
- Protect the email account behind your crypto accounts with its own strong password, a security key and offline recovery codes.

- Write down the master password or emergency kit of your **password manager** and keep it offline.
- Record how each wallet was set up: device, wallet app, PIN rules, passphrase (yes or no), and which email each account uses.
- Never let one phone hold everything: keep at least one other device that can log in to your email and exchange.
- Move 2FA to a new phone before you wipe, sell or hand in the old one.
- Buy hardware wallets directly from the manufacturer, and set the PIN and seed phrase yourself.
- Once a year, test that you can get into every account and wallet without your main phone (the review calendar is in **Chapter 7**).

3.5 CSF Rules for This Chapter

MAIN RULE · OR-006

Maintain Access to Your Authentication Systems.

Every PIN, password, 2FA method and email account needs a backup that does not depend on the same device.

Rule	Statement	Why it applies here
TSR-004	Use Hardware-Based Two-Factor Authentication	A security key resists phishing and SIM swaps, and a second key is a ready backup.
OR-003	Document How Your Wallet Was Created	Knowing which device, app, PIN rules and passphrase you used is what makes a restore work.
OR-001	Test Your Wallet Recovery Before Trusting It	A recovery you have practised once will not fail you under stress.
TSR-006	Separate Devices and Accounts for Crypto Use	Spreading wallet, authenticator and email across devices and accounts means one loss is never total.

Table 3.2: Supporting CSF rules

All 32 rules, with what each one prevents: **CSF Crypto Security Rules**.

3.6 If This Just Happened to You

First find your situation in the Start here table at the front of the book. Then add the steps for your situation:

If you…	Do this now
lost the phone with your authenticator app	Log in with your 2FA backup codes or second security key and register a new device. Without them, start the official account recovery of each service; expect identity checks and waiting time.
forgot the PIN of a hardware wallet	Stop after one or two attempts. Check how many tries your device allows before it resets. If it resets, restore it from your seed phrase on the same or a new device.
are locked out of an exchange account	Use only the recovery link inside the official app or website you reach from your own bookmark. Never follow a link or phone number from a message, ad or search result.
lost access to your email account	Recover the email first, using its own recovery codes or security keys. Then check every crypto account that uses that address, and change their passwords.
forgot your password manager's master password	Look for the emergency kit or written master password. Without it, most managers cannot recover the vault; rebuild access account by account.
had a device lost or stolen	From another device, change the passwords of email and exchange accounts, remove the lost device from your accounts, and move funds from any wallet whose seed phrase or app was on it unprotected.

Table 3.3: Chapter-specific first actions

AFTER A LOSS

People who are locked out are a favourite target of fake support and "unlock" services. Nobody legitimate asks for your seed phrase, remote access or a fee to restore access. See **Recovery Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/locked-out-crypto-wallet/

CHAPTER 4

Wrong Address

“The blockchain does exactly what you tell it to – even when you tell it wrong.”

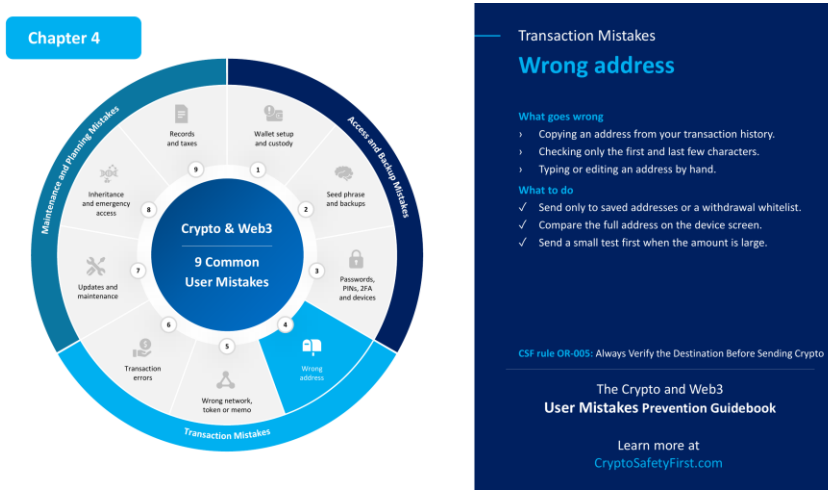

Figure 4.1: Wrong Address at a glance

Sending crypto takes a few seconds. Undoing it is usually impossible. Once a transaction is confirmed, there is no bank to call, no chargeback and no support desk that can pull it back.

Most wrong-address losses are not hacks. They come from small habits: copying an address from your history, checking only a few characters, editing an address by hand, or using an address that is no longer the right one. This chapter covers those habits and the checks that stop them. Sending on the wrong network, token or memo is covered in **Chapter 5**.

IN THIS CHAPTER

- 4.1 What Your Wallet Can Catch, and What It Cannot
- 4.2 Address Mistakes to Watch For
- 4.3 Illustrative Scenario: The Address From Last Year
- 4.4 A Send Routine for Every Transfer
- 4.5 CSF Rules for This Chapter
- 4.6 If This Just Happened to You

4.1 What Your Wallet Can Catch, and What It Cannot

A **wallet address** is a long string of letters and numbers. Wallets check that it is well-formed before they send. That catches many typos, but never a valid address that is simply the wrong one:

The error	Does the wallet catch it?	What happens
A typo in a Bitcoin address	Almost always – the address has a built-in checksum	The wallet rejects it before sending
A typo in an Ethereum-style address written in mixed case	Usually – most wallets check the capital letters as a checksum	The wallet rejects it or warns you
A typo in an Ethereum-style address written all in lowercase	No – lowercase addresses carry no checksum	The crypto goes to an address nobody controls
A valid address of the wrong person	Never	The crypto goes to that person
Your own old address whose seed phrase is lost	Never	The crypto is visible on the blockchain but cannot be moved
The contract address of a token	Sometimes – some wallets warn	The tokens are usually stuck for good

Table 4.1: What your wallet can and cannot catch

Clipboard malware that swaps addresses, and lookalike addresses planted in your history, are attacks, not mistakes. They are covered in the **Hackers guide** and in **Address Poisoning Scams**. The send routine in this chapter protects against both.

4.2 Address Mistakes to Watch For

1. Copying an Address From Your Transaction History

The address you sent to last month sits right there in the history, one tap away. But the history also shows addresses you never meant to use again – and lookalike addresses that scammers plant there with tiny transfers. Copy addresses only from your own saved address book, never from history. How the lookalike trick works: **Address Poisoning Scams**.

2. Checking Only the First and Last Few Characters

Most people check the start and the end of an address. Scammers know it and create addresses that match both. Compare the full address – in groups of four characters, against your saved copy or the address shown on your hardware wallet screen.

3. Typing or Editing an Address by Hand

Bitcoin addresses, and Ethereum-style addresses written in mixed case, carry a checksum, so most typos are rejected. An Ethereum-style address written all in lowercase has none: a single wrong character can create a valid address that nobody controls. Never type an address by hand, never “fix” one by editing it, and never send from an address read out over the phone.

4. Using an Address That Is No Longer Right

Addresses outlive the reason you saved them. A friend moves to a new wallet, an exchange changes your deposit address, an invoice is two years old. Before sending to a saved address you have not used for a while, confirm it with the receiver through a second channel.

5. Picking the Wrong Entry in Your Address Book

An address book only helps if its labels are clear. “Wallet 2” and “Wallet new” look alike on a small screen. Give each entry a clear name, delete

addresses you no longer use, and check the label and the address before you confirm.

6. Sending to a Wallet Whose Seed Phrase Is Gone

Sending to your own old wallet is safe only if you still have its seed phrase. Many people send to an address they used years ago, from a wallet they reset or lost. The funds arrive and stay there forever. Before sending to an old address of your own, confirm you can still open that wallet.

7. Sending Tokens to a Contract Address

Every token has its own contract address, and it often appears on websites and in block explorers next to wallet addresses. Tokens sent to the contract address itself are usually stuck for good. Send tokens to a wallet address, never to the token's own contract.

8. Trusting a Name Instead of the Address

Name services let you send to a readable name instead of a long address. A one-letter typo in the name resolves to someone else's wallet, and expired names can be registered by a stranger. Check the address the name resolves to before you confirm.

4.3 Illustrative Scenario: The Address From Last Year

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

Lena owes her brother money for a shared holiday. She opens her wallet, finds a transfer to him from last year in the history, copies that address and sends the amount. The wallet accepts it; the transaction confirms in minutes.

Her brother never receives it. He had moved to a new wallet months ago and reset his old phone without writing down that wallet's seed phrase. The funds sit at his old address, visible on the blockchain, with nobody able to move them.

What Happened

The address was valid and once belonged to the right person. It was simply no longer in use. Copying from history skipped the one question that mattered: is this still the right address?

Key Takeaways

- Send only to addresses from your own address book, not from history.
- Confirm an address you have not used for a while through a second channel.
- For larger amounts, send a small test and wait for the receiver to confirm it.

4.4 A Send Routine for Every Transfer

- Save each regular address once, in your wallet's address book or an exchange **withdrawal whitelist**, after confirming it with the receiver.
- Copy addresses only from that saved list or from the receiver directly – never from history, chats or old emails.
- Compare the full address in groups of four characters, not just the start and the end.
- On a hardware wallet, compare the address on the device screen before you approve.
- For larger amounts or a new address, **send a small test first**, wait for the receiver to confirm it, then send the rest from your address book again.
- Never type, edit or dictate an address. If the receiver is with you, scan the QR code on their own wallet screen.
- Before sending to an old address of your own, make sure you can still open that wallet.
- Send tokens to wallet addresses only, never to a token's contract address.
- Stop and check again whenever you feel rushed – urgency is when the routine gets skipped.

4.5 CSF Rules for This Chapter

MAIN RULE · OR-005

Always Verify the Destination Before Sending Crypto.

Check the full address against a trusted saved copy, every time, before you approve.

Rule	Statement	Why it applies here
GR-006	Always Send a Small Test Transaction Before Transferring Large Amounts of Crypto	A test proves the address is right and reachable while only a small amount is at risk.
TSR-005	Enable Withdrawal Whitelists on Exchanges	An exchange then sends only to addresses you approved earlier, which also blocks a typo or a pasted wrong address.
SDR-010	Never Pay Anyone to Recover Lost Crypto	People who sent to the wrong address are a main target of fake recovery services.

Table 4.2: Supporting CSF rules

All 32 rules, with what each one prevents: **CSF Crypto Security Rules**.

4.6 If This Just Happened to You

First find your situation in the Start here table at the front of the book. Then add the steps for your situation:

If you…	Do this now
are not sure what happened	Paste the transaction ID into a **block explorer** for that network. Check the status and the destination address character by character.
see the transaction still pending	On some networks a pending transaction can be replaced or cancelled from the same wallet – see **Chapter 6**. Once confirmed, it cannot.

If you…	Do this now
sent to an exchange deposit address that is not yours	Contact that exchange through its official website or app with the transaction ID. Some can help when the address belongs to one of their customers; there is no guarantee.
sent to someone you know, at an old or wrong address	Ask them. If the address belongs to a wallet they still control, they can send it back. If they lost that wallet's seed phrase, nobody can.
sent to an old address of your own	Find the seed phrase of that wallet and restore it in a wallet app – the funds are still there (see **Chapter 2**).
sent tokens to a token's contract address	Contact the project only through its official website. Most projects cannot return them. Never pay anyone who offers to.
noticed the pasted address differs from the one you copied	Stop using that device for crypto. A changed address on paste is a sign of malware – see the **Hackers guide**.

Table 4.3: Chapter-specific first actions

AFTER A LOSS

Nobody can reverse a confirmed transaction or "trace and return" funds for a fee. People who sent crypto to the wrong address are a favourite target of fake recovery services. See **Recovery Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/crypto-wrong-wallet-address/

CHAPTER 5

Wrong Network, Token or Memo

“Right address, wrong network – and suddenly the balance shows zero.”

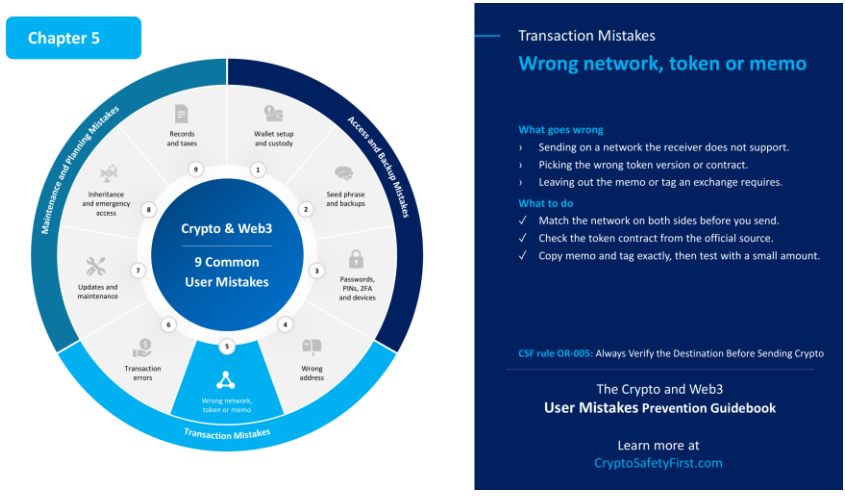

Figure 5.1: Wrong Network, Token or Memo at a glance

You can copy the right address and still lose track of your crypto. The same address format is used on many networks, the same token name exists in several versions, and some exchanges need a memo or tag next to the address to know whose deposit it is.

The good news: many of these mistakes are not final. Crypto sent on the wrong network often sits at an address you or the receiver still control. This chapter shows how the mistakes happen, which ones can be fixed, and the checks that prevent them. Wrong addresses are covered in **Chapter 4**.

IN THIS CHAPTER

- 5.1 Which Mistakes Can Still Be Fixed
- 5.2 Network, Token and Memo Mistakes to Watch For
- 5.3 Illustrative Scenario: The Cheaper Network
- 5.4 Check Network, Token and Memo Before Every Transfer
- 5.5 CSF Rules for This Chapter
- 5.6 If This Just Happened to You

5.1 Which Mistakes Can Still Be Fixed

Unlike a wrong address, a wrong network or a missing memo often leaves the crypto with you or with the exchange. Whether you get it back depends on who controls the receiving address on that network:

What happened	Can it be fixed?	How
Tokens sent on another Ethereum-style network to your own self-custody wallet	Usually yes	Add that network in your wallet. Same seed phrase, same address – the funds appear. You need that network's gas token to move them.
Deposit to an exchange without the required memo or tag	Usually yes	Ticket through the official app or website with the transaction ID. It can take time, and some exchanges charge a fee.
Deposit to an exchange on a network or token version it does not support	Sometimes	Only the exchange can act. Ask its support; there is no guarantee.
Sent to a multisig or smart-contract wallet on a network where it was never set up	Depends on the wallet	Ask the wallet provider through its official website. Some can set up the same address on that network; some cannot.
Tokens sent directly to a token or bridge contract address	Rarely	Contact the project only through its official website. Usually the tokens are stuck.

What happened	Can it be fixed?	How
Wallet shows zero, but the explorer shows the transfer to your address	Nothing is lost	Your wallet is not showing that network or token yet. Add the network or the token contract.

Table 5.1: Which mistakes can be fixed

A fix almost always goes through you (your own wallet and seed phrase) or the official support of the exchange or wallet provider. Never through someone who contacts you, and never by sharing your seed phrase.

5.2 Network, Token and Memo Mistakes to Watch For

1. Picking the Cheapest Network Instead of the Right One

Exchanges offer several withdrawal networks for the same coin, often with the cheapest at the top. The receiving wallet or exchange may support only one of them. Choose the network the receiver names – never by fee alone.

2. Assuming the Same Token Is on the Same Network

USDT on Ethereum, on Tron and on BNB Smart Chain share a name but are different tokens on different networks. A **token standard** such as ERC-20 or BEP-20 tells you which network a token lives on. Always match network and token on both sides.

3. Leaving Out the Memo or Destination Tag

For coins such as XRP, XLM or ATOM, exchanges often use one shared deposit address and a memo, tag or comment to identify you. Without it the deposit arrives but is not credited to your account. Copy the memo exactly, every time; your own self-custody wallet usually does not need one.

4. Sending a Token or Network the Exchange Does Not List

An exchange deposit address accepts only the coins and networks shown on its deposit page. Tokens it does not support may never be credited. Check the deposit page for the exact coin and network before sending.

5. Choosing the Wrong Version of a Token

Many tokens exist in a native and a bridged version on the same network, and fake tokens copy real names and logos. Check the token contract address against the project's official website, not search results or a token list. Fake versions are a scam: see **Token Scams**.

6. Assuming a Multisig Works on Every Network

A normal wallet address works on every Ethereum-style network. A multisig or smart-contract wallet exists only on the networks where it was set up. Funds sent to the same address on another network may be out of reach.

7. Sending Tokens Straight to a Bridge or Contract

Moving tokens between networks goes through a bridge's own app, never by sending tokens to its contract address. Tokens sent straight to a contract are usually stuck. Bridges also carry their own risks, so move only what you need.

8. Thinking Funds Are Lost When the Wallet Just Does Not Show Them

Wallets show only the networks and tokens they have been told about. A transfer on another network can be safe at your address and still show zero. Check the explorer before you panic – panic is what fake recovery services look for. Unexpected tokens you did not send yourself are a different case: do not touch them (**Airdrop Scams**).

5.3 Illustrative Scenario: The Cheaper Network

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

Sam withdraws USDT from an exchange to his hardware wallet. He pastes his Ethereum address, and the exchange offers several networks. BNB Smart Chain is much cheaper than Ethereum, so he picks it. The withdrawal is confirmed, but his wallet shows no USDT.

He posts in a crypto forum. Within minutes, a "support agent" sends him a private message: a "sync tool" can recover the funds if he enters his seed phrase.

What Happened

Nothing was lost. The USDT arrived at the same address on BNB Smart Chain. Once he added that network in his wallet and received a little BNB for fees, he could move it. The forum “agent” was a recovery scam – the only real risk in the whole story.

Key Takeaways

- Pick the network the receiver supports, not the cheapest one.
- Check the explorer before you panic: the funds may be safe at your address.
- Nobody who contacts you can “sync” or recover funds – and never type your seed phrase into a tool.

5.4 Check Network, Token and Memo Before Every Transfer

- Ask the receiver which network and token they accept, or read the exchange’s deposit page – then select exactly that network.
- Compare the network name on both sides: the withdrawal screen and the deposit page must say the same.
- Check the token contract against the project’s official website, not search results or token lists.
- Copy the memo, tag or comment exactly whenever the deposit page shows one.
- Save each regular address in your wallet’s address book or an exchange **withdrawal whitelist** together with its network and memo.
- Send a **small test first** whenever the network, token or memo is new to you.
- Keep a small amount of each network’s gas token where you hold funds on that network.
- Use a bridge only through its own app, and only for what you need to move.
- If the balance shows zero after a transfer, check the explorer before doing anything else.

5.5 CSF Rules for This Chapter

MAIN RULE · OR-005

Always Verify the Destination Before Sending Crypto.

The destination is the address, the network, the token and the memo – check all four before you approve.

Rule	Statement	Why it applies here
GR-006	Always Send a Small Test Transaction Before Transferring Large Amounts of Crypto	A small test on a new network, token or memo shows the setup works before the full amount moves.
TSR-005	Enable Withdrawal Whitelists on Exchanges	A whitelist entry saves the address together with its network and memo, so you choose them once, carefully.
SDR-010	Never Pay Anyone to Recover Lost Crypto	People whose crypto “disappeared” on the wrong network are a main target of fake recovery services.

Table 5.2: Supporting CSF rules

All 32 rules, with what each one prevents: **CSF Crypto Security Rules**.

5.6 If This Just Happened to You

First find your situation in the Start here table at the front of the book. Then add the steps for your situation:

If you…	Do this now
do not know which network you used	Open the withdrawal or transaction details in the app you sent from. Look up the transaction ID on a **block explorer** for that network.
sent to your own wallet on another Ethereum-style network	Add that network in the same wallet (or restore the seed phrase in a wallet that supports it, see **Chapter 2**). Buy or receive a little of that network’s gas token to move the funds.

If you…	Do this now
forgot the memo or tag on an exchange deposit	Open a ticket through the exchange's official app or website: transaction ID, amount, deposit address and your account. Never answer "support" that contacts you first.
sent a token or network the exchange does not support	Ask the exchange through its official support whether it can credit or return the deposit. Do not send anything else to that address.
sent to a multisig or smart-contract wallet on the wrong network	Do not try fixes from forums. Ask the wallet provider through its official website what is possible for that network.
see a zero balance after a transfer to your own wallet	Check the explorer first. If the transfer is there, add the network or the token contract from the project's official website – the funds are not lost.

Table 5.3: Chapter-specific first actions

AFTER A LOSS

Fake "support agents" and recovery services watch forums and social media for people whose funds went missing. No legitimate service needs your seed phrase, remote access or an upfront fee. See **Recovery Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/crypto-sent-wrong-network/

CHAPTER 6

Transaction Errors: Fees, Stuck Transactions and Slippage

“The transaction didn’t vanish. It was waiting – and I paid twice trying to fix it.”

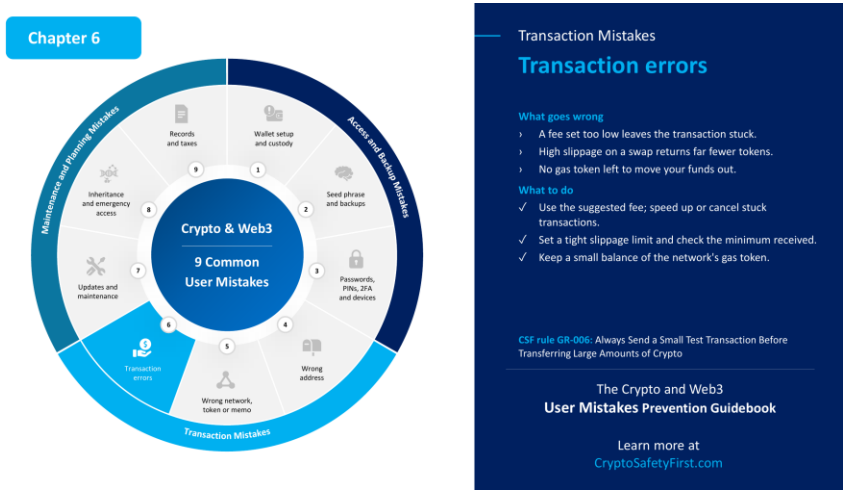

Figure 6.1: Transaction Errors at a glance

Every transaction has a price and a set of settings: the network fee, the amount, and for swaps the slippage you accept. Most of the time the wallet’s suggestions are fine. When they are not, a transaction hangs for hours, fails and still costs the fee, or a swap returns far less than expected.

These mistakes rarely lose everything at once, but they are common, and the panic they cause is what fake “support” looks for. This chapter explains the settings that matter and what to do when a transaction goes wrong.

IN THIS CHAPTER

- 6.1 The Fee and Transaction Terms That Matter
- 6.2 Transaction Mistakes to Watch For
- 6.3 Illustrative Scenario: Paid Twice
- 6.4 Before You Confirm a Transaction
- 6.5 CSF Rules for This Chapter
- 6.6 If This Just Happened to You

6.1 The Fee and Transaction Terms That Matter

You do not need to understand how a blockchain prices its block space. You need to know a handful of terms your wallet shows you – and what each one means when something goes wrong:

Term	What it means	Why it matters
Network fee (gas)	What you pay the network to process a transaction. Wallets usually offer slow, normal and fast.	Too low and the transaction waits; too high and you overpay. See **gas**.
Gas token	The network's own coin that pays the fee: ETH on Ethereum and most of its layer-2 networks, BNB on BNB Smart Chain, POL on Polygon, SOL on Solana.	Without it you cannot move any token on that network.
Pending	Sent, but not yet included in a block.	It can still be sped up or cancelled. Once confirmed, it cannot.
Failed (reverted)	Included in a block, but the action did not happen.	Your funds stay where they were, but the fee is spent.
Nonce (Ethereum-style networks)	The running number of each transaction from your address.	A stuck transaction blocks every later one from the same address until it is confirmed or replaced.

Term	What it means	Why it matters
Speed up / cancel (replace-by-fee)	A new version of the pending transaction with a higher fee.	The safe way to fix a stuck transaction – instead of sending again.
Slippage tolerance	How much worse than the quoted price you accept on a swap.	High tolerance can return far fewer tokens. See **slippage**.
Minimum received	The least the swap may return with your slippage setting.	Read it before you confirm – it is the real worst case.

Table 6.1: Fee and transaction terms that matter

Exchange withdrawals work differently: the exchange sets the fee and sends the transaction itself. You cannot speed up or cancel it – contact the exchange through its official app or website if a withdrawal hangs.

6.2 Transaction Mistakes to Watch For

1. Setting the Fee Too Low

A fee below what the network currently needs leaves the transaction pending – sometimes for hours or days. On Ethereum-style networks it also blocks every later transaction from the same address. Use the wallet's normal or suggested fee unless you know why you need something else.

2. Sending the Payment Again Instead of Speeding It Up

The most expensive reaction to a stuck transaction is to send the same payment again. The first one is still valid and can confirm later – and then you have paid twice. Use "speed up" or "cancel" in the wallet that sent it; they replace the pending transaction instead of adding a new one.

3. Overpaying Without Checking the Fee in Money

Wallets that default to "fast", or a mistyped custom fee, can turn a routine transfer into an expensive one. Before you confirm, read the fee as an amount in your own currency. If it looks wrong, it probably is.

4. Leaving No Gas Token Behind

Sending your whole ETH, BNB or SOL balance with “Max” leaves nothing to pay for the next transaction. The same happens after bridging tokens to a new network without its gas token. The tokens are safe but cannot move. Keep a small balance of each network’s gas token wherever you hold funds.

5. Forcing a Transaction the Wallet Says Will Fail

Many wallets simulate a transaction and warn when it is likely to fail. Confirming anyway usually means a failed transaction and a spent fee. Find out why first: not enough balance, a missing approval, or a price that moved.

6. Setting Slippage Too High

A high slippage tolerance lets a swap go through at a much worse price – and gives trading bots room to take the difference. Keep the default unless a trade keeps failing, and read “minimum received” every time. A token you can only sell with very high slippage is a warning sign: see **Token Scams**.

7. Entering the Wrong Amount

An extra zero, a mix-up between token and fiat display, or a “Max” button you did not mean to tap. Check the amount in both the token and your own currency before you confirm, and on a hardware wallet compare it on the device screen.

8. Approving Unlimited Spending “to Save on Fees”

Unlimited token approvals save one approval fee next time and leave a permission open indefinitely. Approve only the amount you need, and remove old approvals (**approval tools**). How malicious approvals drain wallets: **Malicious Contracts and Approvals**.

6.3 Illustrative Scenario: Paid Twice

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

Mia pays a freelancer in USDC on Ethereum and picks the cheapest fee. An hour later the payment still shows as pending. Worried, she sends the same amount again with a normal fee.

The second payment waits behind the first, because her wallet processes transactions from one address in order. When network fees drop that evening, both confirm. The freelancer has been paid twice and has to be asked to send one payment back.

What Happened

A low fee on its own was only a delay. Sending again turned the delay into a double payment. “Speed up” on the first transaction would have replaced it with a higher fee and kept one payment.

Key Takeaways

- Use the wallet’s normal fee unless you have a reason not to.
- A pending transaction is not lost: speed it up or cancel it, never send again.
- Check the status on a block explorer before doing anything.

6.4 Before You Confirm a Transaction

- Read the fee as an amount in your own currency. If it looks wrong, stop.
- Check the amount twice: in the token and in your currency.
- Keep a small balance of each network’s gas token where you hold funds.
- For swaps, keep the default slippage and read “minimum received” before you confirm (**transaction preview**).
- Take wallet warnings seriously: if it says the transaction will likely fail, find out why first.
- If a transaction hangs, use “speed up” or “cancel” in the same wallet – never send again.
- Approve only the amount you need, and remove approvals you no longer use.
- For a large or unusual transfer, **send a small test first**: it shows the real fee and timing before the full amount moves.

6.5 CSF Rules for This Chapter

MAIN RULE · GR-006

Always Send a Small Test Transaction Before Transferring Large Amounts of Crypto.

A small test shows the real fee, the network and the timing while only a small amount is at risk.

Rule	Statement	Why it applies here
GR-004	Always Revoke Unused Token Approvals After Interacting with New Smart Contracts	Approvals are transactions too. Unlimited approvals “to save fees later” stay open long after the swap.
SDR-003	Never Pay to Unlock or Withdraw Funds	A “gas fee” you must pay first to receive, release or unlock crypto is a scam, not a network fee.
SDR-010	Never Pay Anyone to Recover Lost Crypto	Stuck or failed transactions attract fake support that offers to fix them for a fee or a seed phrase.

Table 6.2: Supporting CSF rules

All 32 rules, with what each one prevents: **CSF Crypto Security Rules**.

6.6 If This Just Happened to You

First find your situation in the Start here table at the front of the book. Then add the steps for your situation:

If you…	Do this now
have a transaction pending for a long time (Ethereum-style network)	In the wallet that sent it, use “speed up” to resend it with a higher fee, or “cancel” to replace it. Do not send a new payment – it waits in line behind the stuck one and both may go through.

If you…	Do this now
have a Bitcoin transaction pending for a long time	If your wallet offers “bump fee”, use it. Otherwise wait: the receiver, or you with the change output, can speed it up with a follow-up transaction, Nodes eventually drop an unconfirmed transaction, but it can still be rebroadcast and confirm later – so re-send only with your wallet’s bump-fee or cancel, which spends the same coins. Never send a second, separate payment.
see a failed transaction	Your funds did not move; only the fee is gone. Read the reason on a **block explorer** (out of gas, price moved, not approved) before trying again.
cannot move tokens because there is no gas token	Send a small amount of that network’s gas token to the same address, from an exchange or another wallet you control.
got far fewer tokens from a swap than quoted	Check “minimum received” and the price impact in the transaction details. It cannot be reversed; lower your slippage setting for next time, and be wary of tokens that only sell with very high slippage.
sent the wrong amount	If the transaction is still pending, cancel it. If it is confirmed, ask the receiver to return the difference.
are told you must pay a “gas fee” to receive or unlock funds	Stop. That is a scam, not a network fee (SDR-003). See **Giveaway and Airdrop Scams**.

Table 6.3: Chapter-specific first actions

AFTER A LOSS

Stuck and failed transactions are a favourite opening for fake support in forums and social media. No legitimate helper needs your seed phrase, remote access or a fee to fix a transaction. See **Recovery Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/crypto-transactions-gas-fees-mistakes/

CHAPTER 7

Updates and Maintenance

“The setup was perfect – in 2021.”

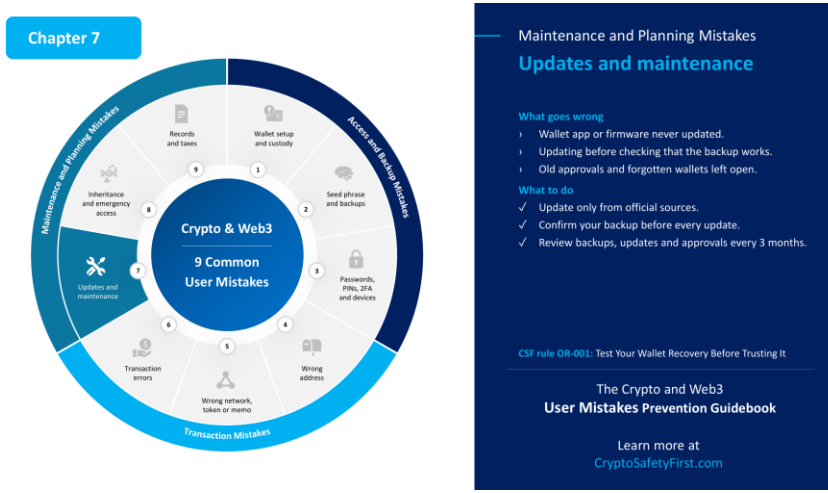

Figure 7.1: Updates and Maintenance at a glance

Most crypto setups do not fail on the day they are created. They fail years later: a backup that faded, a firmware update done without a tested recovery, an approval granted to a project long forgotten, a wallet nobody remembers.

None of this needs technical skill to prevent – only a routine. This chapter covers the update and maintenance mistakes that turn a good setup into a weak one, and gives one review calendar for the whole guide.

IN THIS CHAPTER

- 7.1 One Review Calendar for Your Setup
- 7.2 Maintenance Mistakes to Watch For
- 7.3 Keep It Simple Enough to Use Under Stress
- 7.4 Illustrative Scenario: The Update That Asked for the Words
- 7.5 CSF Rules for This Chapter
- 7.6 If This Just Happened to You

7.1 One Review Calendar for Your Setup

This calendar is the same one the **Three-Wallet Model®Toolkit** uses, and it replaces the different intervals of the first edition. Pick fixed dates – for example the first weekend of each quarter – and the reviews take minutes:

When	Check	Why
Every 3 months	Backups still readable and where they should be · wallet apps, extensions and firmware updated from official sources · token approvals and dApp connections reviewed · Disposable wallets retired when done	Catches faded backups, known security holes and open permissions early.
Every 6 months	Wallet list and labels up to date · each wallet still used for its purpose · new wallets recorded and backed up · emergency information still findable	Keeps your records in line with what you actually use.
Once a year	Full recovery walk-through (hardware wallet: built-in backup check or a second hardware wallet – never type the seed into a phone or computer) · backup locations · access to every account without your main phone (Chapter 3) · inheritance plan (Chapter 8) · old devices and unused wallets retired	Proves the whole setup works when you need it.
Before every firmware or major update	Seed phrase backup complete and readable · passphrase recorded, if you use one	An update that resets the device is harmless only with a good backup.
After any big change	New phone, new wallet, move, new family situation: update records, backups and the emergency plan	Records that no longer match reality fail at the worst moment.

Table 7.1: One review calendar for the whole guide

7.2 Maintenance Mistakes to Watch For

1. Ignoring Updates

Wallet apps, browser extensions, hardware wallet firmware and the phone or computer underneath all receive security fixes. Running old

versions keeps known weaknesses open. Turn on update notifications and check during your three-monthly review.

2. Updating Firmware Without a Tested Backup

Most firmware updates go smoothly. A few reset the device, and then the seed phrase is the only way back. Before every firmware update, check that your backup is complete and readable – and that you know your passphrase, if you use one.

3. Updating From a Link in a Message

Real wallet providers do not send update files by email, text or pop-up. Update only inside the official app, the official app store or the manufacturer's own app for hardware wallets. Fake update messages are covered in **Phishing Scams**.

4. Treating Every Update the Same

Security fixes should go in promptly. Large feature releases and major firmware versions can wait a few days until early problems are known – but not months. Read the release notes in the official app or website.

5. Leaving Old Approvals Open

Every approval you gave a dApp stays valid until you remove it. Projects get abandoned or hacked years later, and an old approval can then be used to take tokens. Review approvals every three months and remove what you no longer use. How approvals are abused: **Malicious Contracts and Approvals**.

6. Forgetting Wallets That Still Hold Funds

Old wallets from airdrops, test setups or a previous phone collect small balances and are rarely watched. If their seed phrase is lost, the funds are lost; if it leaked, nobody notices the theft. Keep a wallet list, and retire wallets you no longer need.

7. Running Wallets on Unsupported Devices

A phone or computer that no longer receives security updates is a weak base, even with an updated wallet app. Move wallets to a supported device, then reset the old one.

8. Never Testing Recovery

A backup is only proven when it has restored a wallet. Test it once with no funds at risk – on a hardware wallet with its built-in backup check or a second hardware wallet, never by typing the seed into a phone or computer – then walk through the full recovery once a year. Do not assume missing words can be “guessed later”: specialists can sometimes test a few missing words offline, but anyone online who asks for your remaining words is after your funds. See **wallet recovery**.

7.3 Keep It Simple Enough to Use Under Stress

Some setups become so complex that their owner cannot follow them in an emergency: seed phrases split across several places, multisig wallets with unclear key holders, encryption tools nobody else understands. A setup that only works on a good day is a risk in itself.

- Can you follow your recovery steps under pressure, without searching?
- Could a trusted person follow them without you?
- Have you tested the full process from start to finish?

Prefer well-documented methods – a hardware wallet and offline paper or steel backups – and add complexity only when you can keep it documented and tested.

7.4 Illustrative Scenario: The Update That Asked for the Words

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

Jonas has not touched his hardware wallet for two years. The official app shows a firmware update, and he installs it. The update stops halfway; the device restarts and asks him to restore from his seed phrase.

His only paper backup is in a drawer. Two words have faded and are hard to read. He finally finds the second copy he made at his parents’ house and restores the wallet.

What Happened

The update did what updates sometimes do. The real risk was a backup that had not been checked in two years. The second copy saved him.

Key Takeaways

- Check your backup before every firmware update.
- Keep a second copy in another place.
- Put backup checks in a fixed review calendar.

7.5 CSF Rules for This Chapter

MAIN RULE · OR-001

Test Your Wallet Recovery Before Trusting It.

Test your backup once – on a hardware wallet with its built-in backup check – and walk through the full recovery once a year.

Rule	Statement	Why it applies here
GR-004	Always Revoke Unused Token Approvals After Interacting with New Smart Contracts	Old approvals are the most common open door in an otherwise well-kept wallet.
TSR-001	Never Install Crypto Software from Unofficial Sources	Updates come only through the official app, store or website – never from a link in a message.
TSR-002	Assume Your Device Can Be Compromised	Old, unsupported phones and computers no longer get security fixes; treat them accordingly.

Table 7.2: Supporting CSF rules

All 32 rules, with what each one prevents: **CSF Crypto Security Rules**.

7.6 If This Just Happened to You

First find your situation in the Start here table at the front of the book. Then add the steps for your situation:

If you…	Do this now
got an update message by email, text or pop-up	Ignore the link. Open the wallet app or type the official address yourself and check there. Fake updates are a scam: see **Fake Apps, Extensions and Wallets**.
have a hardware wallet that reset during an update	Restore it from your seed phrase (and passphrase, if you use one) on the device itself, following the manufacturer's official app. Enter the words only on the hardware wallet's own screen – an app, website or pop-up that asks you to type them is a scam.
found a backup with unreadable words	If the wallet still opens, create a new wallet with a new seed phrase, back it up properly and move the funds now. If it does not, use your second copy (**Chapter 2**). Never share the remaining words with anyone.
found old approvals you no longer need	Remove them from a trusted device with your wallet's approvals view or an **approval checker**. Each removal costs a small network fee.
found a forgotten wallet with funds	Check that you still have its seed phrase. Then move the funds into your current setup, record the old wallet as retired, and keep its backup until it is empty.
use a phone or computer that no longer gets updates	Move your wallet apps to a supported device, then reset or retire the old one so no keys remain on it.

Table 7.3: Chapter-specific first actions

AFTER A LOSS

People with damaged backups or reset devices are a target for fake "recovery" and "repair" services. Nobody legitimate asks for your seed phrase, part of it, or remote access. See **Recovery Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/crypto-wallet-software-mistakes/

CHAPTER 8

Inheritance and Emergency Access

“We knew he had crypto. We just didn’t know where, or how.”

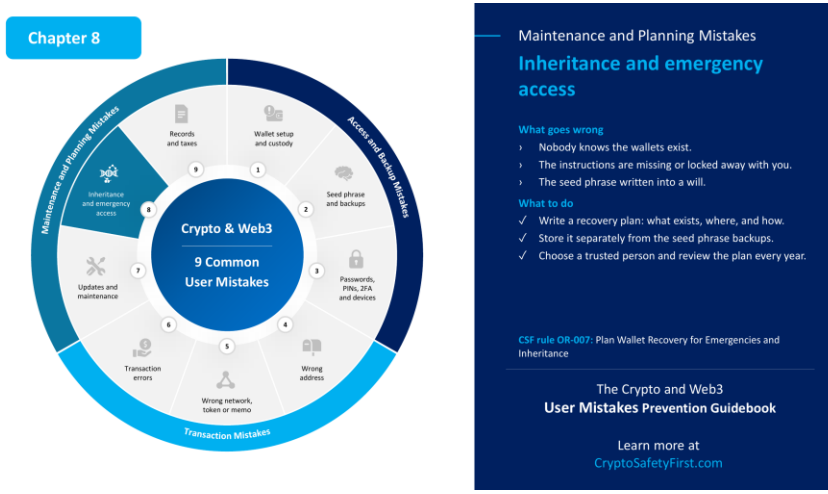

Figure 8.1: Inheritance and Emergency Access at a glance

Self-custody means nobody else can take your crypto. It also means nobody else can unlock it – not your partner, not your children, not a lawyer or a court – unless you have left them a way in.

This chapter is the one place in the guide for inheritance and emergency access: illness, an accident, or simply a time when you cannot act yourself. It shows what your family needs to know, how to keep it safe until then, and the mistakes that leave heirs locked out. It is not legal advice: inheritance law differs by country.

IN THIS CHAPTER

- 8.1 What Your Family Needs – and What They Should Not Hold Yet
- 8.2 Inheritance Mistakes to Watch For
- 8.3 Options for Shared or Delayed Access
- 8.4 A Five-Step Plan
- 8.5 Illustrative Scenario: Two Kinds of Crypto
- 8.6 CSF Rules for This Chapter
- 8.7 If This Just Happened to You

8.1 What Your Family Needs – and What They Should Not Hold Yet

A good plan gives your family a path to follow without handing over the keys today. Think of it in layers:

What	Who knows or holds it	Where it is kept
That crypto exists, and roughly how much	Your trusted person, now	Told in person; mentioned in your will without any keys
Where the recovery plan is	Your trusted person, now	A sealed envelope or the will refers to its location
The recovery plan: wallets, apps, devices, exchanges, step by step	Nobody reads it until needed	Sealed, in a safe place – separate from the seed phrase
Seed phrases (and passphrases)	Nobody but you	Your offline backups, as in Chapter 2 – never in the plan, never in the will
Exchange and email access	Nobody but you	Password manager emergency kit or written credentials, stored offline (Chapter 3)

Table 8.1: What your family needs, and where it is kept

8.2 Inheritance Mistakes to Watch For

1. Nobody Knows the Crypto Exists

Families often know someone “had crypto” but not where. Without at least that knowledge, nobody even starts looking. Your trusted person should know that crypto exists, roughly how much, and where the plan is – without having the keys.

2. No Instructions, or Instructions Only You Understand

A seed phrase and a hardware wallet mean nothing to someone who has never used them. Write plain steps: which device or app, where to download it from, where the backup is, which networks and tokens to expect. Assume the reader has never used crypto.

3. Keeping Instructions and Seed Phrase Together

If the plan and the seed phrase sit in the same envelope, whoever finds it has full access – a burglar as easily as an heir. Keep them in separate places and let the plan say where the backup is.

4. Writing the Seed Phrase Into a Will

Wills are read by lawyers, notaries, family members and sometimes courts, and in some countries become part of official files. Name your crypto in the will and say that a recovery plan exists – never write seed phrases, passphrases or PINs into it. Ask a lawyer or notary how this works where you live.

5. Forgetting Exchange Accounts

Exchange balances can usually be released to heirs, but only if someone knows the account exists. List every exchange and app you use, and the email address behind each account. Records also help heirs with taxes and statements (**Chapter 9**).

6. Everything Behind One Password

If every login, note and recovery code sits in a password manager whose master password exists only in your head, nothing can be opened after you are gone. Store the emergency kit or master password offline, and remember that 2FA on your phone needs its own backup (**Chapter 3**).

7. A Setup Too Complex for Anyone Else

Multisig wallets, split backups and several devices can be good security – and impossible for an heir without guidance. If you use them, document every piece and who holds it, and consider naming a technically capable person your heir can trust.

8. A Plan Nobody Has Checked

Wallets change, backups move and people move house. A plan written five years ago may point to a device that no longer exists. Review it once a year with your other checks (**Chapter 7**) and walk through it with your trusted person.

8.3 Options for Shared or Delayed Access

For most people a sealed plan and a separate offline backup are enough. Larger holdings sometimes justify more – but every extra piece must be documented and tested:

Option	How it works	Watch out for
Sealed plan + separate backup	Instructions in one place, the seed phrase backup in another; your trusted person knows where both are.	Simple and robust. Both places must stay secure, and the plan must be kept current.
Multisig wallet	A **multisig** wallet needs, for example, 2 of 3 keys. You, a trusted person and a backup each hold one.	More moving parts. Losing more keys than the threshold allows – or the wallet configuration file (descriptor) – locks the funds; heirs need clear instructions or help.
Split (Shamir-style) backups	Some hardware wallets split the backup into several shares; a set number of them restores the wallet.	Every share must be recorded and findable. Not every wallet supports it.

Option	How it works	Watch out for
Inheritance or timed-access services	A provider releases access after a waiting period or a confirmed death.	You depend on the provider still existing and being honest. Check who could access your funds, and never hand over a seed phrase.

Table 8.2: Options for shared or delayed access

8.4 A Five-Step Plan

1. List What You Have

Every wallet and its role, every device, every exchange or app, roughly what each holds, and the email address behind each account. The wallet list from the Three-Wallet Model® Toolkit works well for this.

2. Choose Your Trusted Person

A partner, an adult child, a friend or a lawyer. They do not need access now – only to know that a plan exists and where it is.

3. Write the Recovery Plan

Plain steps for each wallet and account: which app or device, where the backup is, whether a passphrase is needed (without writing it into the plan), and who to contact for exchange accounts.

4. Store the Plan and the Backups Separately

For example the plan in a sealed envelope with your important documents and the seed phrase backups in the places from Chapter 2. Mention the plan, not the keys, in your will.

5. Review It Every Year

Update it whenever you add a wallet, change devices or move. Once a year, check it against your setup and walk through it with your trusted person.

8.5 Illustrative Scenario: Two Kinds of Crypto

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

After her father's death, Anna finds emails from a crypto exchange and, in his desk, a small hardware wallet. The exchange asks for a death certificate and the inheritance documents, then releases the balance after a few weeks.

The hardware wallet is another story. Nobody knows its PIN, and there is no seed phrase anywhere – no note, no envelope, no instructions. A stranger in an online forum offers to "unlock" it for a share of the funds.

What Happened

The custodial account had a process; the self-custody wallet had only the seed phrase, and he never left a path to it. The forum offer was a recovery scam – no one can bypass a hardware wallet without its seed phrase.

Key Takeaways

- Tell one trusted person that crypto exists and where the plan is.
- Keep the plan and the seed phrase in separate, known places.
- Never let anyone who contacts you first "unlock" a wallet.

8.6 CSF Rules for This Chapter

MAIN RULE · OR-007

Plan Wallet Recovery for Emergencies and Inheritance.

Leave a written path your trusted person can follow – kept separate from the keys themselves.

Rule	Statement	Why it applies here
OR-003	Document How Your Wallet Was Created	Heirs need to know which wallet app, device and passphrase were used – the words alone may open an empty wallet.
OR-001	Test Your Wallet Recovery Before Trusting It	A plan nobody has walked through is a guess. Walk through it once a year.

Rule	Statement	Why it applies here
SDR-010	Never Pay Anyone to Recover Lost Crypto	Families searching for crypto are a main target of fake recovery services.

Table 8.3: Supporting CSF rules

All 32 rules, with what each one prevents: **CSF Crypto Security Rules**.

8.7 If This Just Happened to You

First find your situation in the Start here table at the front of the book. Then add the steps for your situation:

If you…	Do this now
found a hardware wallet, seed phrase or notes after a death	Keep everything together, private and offline. Look for written instructions and the will first. Do not type words into any website or app, and do not hand them to anyone who offers help.
know there are exchange accounts	Contact each exchange through its official website. Ask for its process for deceased customers; expect to provide a death certificate and proof that you are entitled to inherit.
found words but do not know the wallet	Look for the wallet app on the person's phone or computer, receipts for a hardware wallet, or notes on the setup. The same words can open different wallets depending on the app and on a **passphrase**.
are not technical and the amount is significant	Ask someone you trust personally and who understands crypto to help in person, on your devices. Never accept help from someone who contacts you first.
are planning for yourself	Write down today which wallets and exchanges you use and where the backups are. Tell one trusted person that a plan exists and where it is.

Table 8.4: Chapter-specific first actions

AFTER A LOSS

Families of people who have died are targeted by fake recovery services, fake lawyers and fake officials who “found” the crypto. Nobody legitimate asks for a seed phrase, remote access or a fee to release funds. See **Recovery Scams** and **Impersonation Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/how-to-plan-your-crypto-inheritance-safely/

CHAPTER 9

Records and Taxes

“The exchange was gone, and so were three years of trades.”

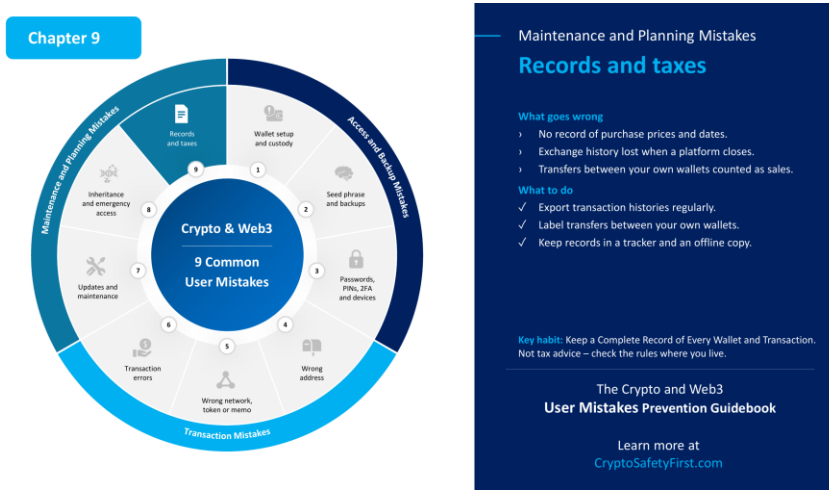

Figure 9.1: Records and Taxes at a glance

In many countries, buying, selling, swapping or earning crypto can have tax consequences. The rules differ from country to country, and this guide does not explain them. What it does explain is the part that is almost the same everywhere: the records you need, and how to keep them before they disappear.

Missing records are a user mistake like a lost backup. An exchange closes, an app shuts down, a laptop dies – and years of history go with it. This chapter is not tax advice. For your own situation, check the rules where you live or ask a tax adviser.

IN THIS CHAPTER

- 9.1 The Records Worth Keeping
- 9.2 Record-Keeping Mistakes to Watch For
- 9.3 Illustrative Scenario: The Exchange That Closed
- 9.4 CSF Rules for This Chapter
- 9.5 If This Just Happened to You

9.1 The Records Worth Keeping

Whatever the **tax rules** where you live, almost every calculation or question starts from the same records:

Record	Why you need it	Where it comes from
Every buy and sell: date, amount, price in your currency, fees	The basis of most tax calculations, and proof of what you paid	Exchange exports and statements; your own notes for private trades
Swaps between tokens	In many countries a swap counts like a sale	Exchange exports; block explorer for your address
Transfers between your own wallets and accounts	Shows that no sale happened	Your own labels; transaction IDs
Income-like receipts: staking rewards, interest, airdrops, payments	Often treated differently from purchases	Exchange exports; wallet history with the value on the day received
Fees paid	May be relevant to the calculation	Exchange exports; block explorer
Losses: theft, scams, failed platforms	Evidence for reports and, where allowed, for tax treatment	Transaction IDs, screenshots, police or platform reports (**how to report**)
Your wallet and account list	So nothing is forgotten – by you or your heirs	The wallet list you keep for Chapters 1 and 8

Table 9.1: The records worth keeping

Keep records for as long as the authorities in your country can ask for them – often several years. Check the period where you live.

9.2 Record-Keeping Mistakes to Watch For

1. No Record of What You Paid

The blockchain shows what moved and when – not the price in your currency. Without purchase records, a later calculation has to guess, and the guess is rarely in your favour. Keep the purchase date, amount, price and fees for every buy.

2. Trusting the Exchange to Keep Your History

Exchanges close, delist coins, leave countries and close accounts. Exports are often available only while you can still log in. Download your full history regularly, not once a year.

3. Not Labelling Transfers Between Your Own Wallets

A move from an exchange to your own hardware wallet is not a sale, but tracking tools and statements may show it as one. Label your own transfers with the wallet they went to, and keep the transaction IDs.

4. Forgetting Income-Like Receipts

Staking rewards, interest, airdrops and crypto payments are easy to overlook because you did not buy them. In many countries they are treated differently from purchases. Record the date and the value on the day you received them.

5. Losing Track of Wallets

Old wallets from previous phones, test setups and airdrops still have histories. If you no longer know they exist, your records are incomplete. Keep one wallet list (**Chapter 1**) and retire wallets you no longer use (**Chapter 7**).

6. Giving a Tracking Tool Too Much Access

Portfolio and tax trackers only need to read. Connect them with your public addresses or a read-only exchange key – never a key that can trade or withdraw, and never your seed phrase. See **portfolio and tax trackers**.

7. Keeping Records in Only One Place

Records only in an exchange account, only on one laptop or only in one app disappear with it. Keep an export in your tracker and an offline copy – and keep records apart from your seed phrase backups, which never belong in the same file or folder (**Chapter 2**).

8. Waiting for the Tax Deadline

Under deadline pressure, missing exports are already gone and memories have faded. Export monthly or quarterly as part of your regular review, and let a tax adviser deal with the rules.

9.3 Illustrative Scenario: The Exchange That Closed

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

Kai traded on a small exchange for three years and withdrew most of his crypto to a hardware wallet along the way. Then the exchange announced it was shutting down. He withdrew the rest – but did not download his transaction history before the site went offline.

When his tax adviser asks for purchase prices, he has only his bank statements and the blockchain history of his hardware wallet. Rebuilding three years of trades takes weeks, and some transfers to his own wallet look like sales.

What Happened

The crypto was safe; the records were not. The exchange was the only place his trades were stored, and his own transfers were never labelled.

Key Takeaways

- Export your exchange history regularly, and immediately when a platform announces changes.
- Label transfers between your own wallets.
- Keep an export in your tracker and an offline copy.

9.4 CSF Rules for This Chapter

KEY HABIT

Keep a Complete Record of Every Wallet and Transaction.

Export histories regularly, label your own transfers and keep an offline copy. This is not tax advice: check the rules where you live, or ask a tax adviser.

Rule	Statement	Why it applies here
OR-003	Document How Your Wallet Was Created	The same wallet list that helps you restore a wallet tells you which addresses belong in your records.

Rule	Statement	Why it applies here
OR-007	Plan Wallet Recovery for Emergencies and Inheritance	Heirs need your records as much as your recovery plan – for the estate and for taxes.
GR-001	Never Share Your Seed Phrase	No tax tool, accountant or tax office ever needs your seed phrase. Public addresses or read-only access are enough.

Table 9.2: Related CSF rules

All 32 rules, with what each one prevents: **CSF Crypto Security Rules**.

9.5 If This Just Happened to You

First find your situation in the Start here table at the front of the book. Then add the steps for your situation:

If you…	Do this now
hear that an exchange is closing or leaving your country	Log in through its official website and download every transaction history, statement and tax report it offers – in more than one format if possible. Then decide what to withdraw.
have an account the exchange has closed	Ask through the official support channel for your full transaction history. Many platforms must keep records for some years and can provide them on request.
are missing records for a wallet	Look up your wallet addresses on a block explorer for each network and export what it shows. Add prices from the exchange or bank side of each purchase.
used many wallets and cannot tell them apart	Make a wallet list now: address, network, wallet app, purpose. The Three-Wallet Model® Toolkit has a template (**Toolkit**).
are asked to pay tax in crypto, or to "verify" your wallet for tax	Stop. Real tax authorities do not collect tax in crypto or ask for wallet access. Contact them through their official website. See **Impersonation Scams**.

If you…	Do this now
received tokens you never asked for	Do not interact with them – some are scams that drain wallets when you try to sell. Note them if your adviser needs it. See **Giveaway and Airdrop Scams**.

Table 9.3: Chapter-specific first actions

AFTER A LOSS

If you lost crypto to theft or a scam, your records are your evidence: keep transaction IDs, screenshots and reports. Nobody can recover the funds for a fee – see **Recovery Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/crypto-tax-records/

CSF Rules Index

These are the CryptoSafetyFirst rules used in this book, with the chapters where they apply. The full rule set, with what each rule prevents, is published at **CSF Crypto Security Rules**. 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, 9
GR-003	Always Use a Hardware Wallet for Long-Term or High-Value Crypto Storage	1
GR-004	Always Revoke Unused Token Approvals After Interacting with New Smart Contracts	6, 7
GR-006	Always Send a Small Test Transaction Before Transferring Large Amounts of Crypto	4, 5, 6
GR-007	Never Store Your Seed Phrase in Cloud Storage, Email, or Screenshots	2
GR-008	Keep Long-Term Holdings in a Vault Wallet. Use a Separate Wallet for DApps, Trading, and Web3	1
OR-001	Test Your Wallet Recovery Before Trusting It	2, 3, 7, 8
OR-002	Never Rely on a Single Seed Phrase Backup	2
OR-003	Document How Your Wallet Was Created	2, 3, 8, 9
OR-004	Never Store Seed Phrases Only in Digital Form	2
OR-005	Always Verify the Destination Before Sending Crypto	4, 5
OR-006	Maintain Access to Your Authentication Systems	3
OR-007	Plan Wallet Recovery for Emergencies and Inheritance	8, 9
SDR-003	Never Pay to Unlock or Withdraw Funds	6
SDR-010	Never Pay Anyone to Recover Lost Crypto	4, 5, 6, 8
TSR-001	Never Install Crypto Software from Unofficial Sources	7

Rule	Statement	Chapters
TSR-002	Assume Your Device Can Be Compromised	7
TSR-004	Use Hardware-Based Two-Factor Authentication	1, 3
TSR-005	Enable Withdrawal Whitelists on Exchanges	1, 4, 5
TSR-006	Separate Devices and Accounts for Crypto Use	3

CSF rules used in this book

Keep Learning

Wallets, networks and apps change faster than any book. CryptoSafetyFirst.com keeps this guide alive between editions:

- **A page for every chapter**, kept up to date.
- **The Three-Wallet Model**: a free guide and toolkit for setting up Vault, Frequent Use and Disposable wallets.
- The **Scams** and **Hackers** guides, for the losses that are not mistakes.
- **Practical safety tools**: what each one prevents and what it cannot do.

Most crypto losses need no hacker. With a plan, a tested backup and a careful send routine, most of them never happen.

cryptosafetyfirst.com