2026 EDITION

THE CRYPTO AND WEB3 HACKS PREVENTION GUIDEBOOK

How to Keep Your Crypto and Digital Assets Safe from Hackers

JUAN PABLO RENEDO

The Crypto and Web3 Hacks Prevention Guidebook

How to Keep Your Crypto and Digital Assets Safe from Hackers

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 You Think You Have Been Hacked 9
How Hacks Usually Start 10
1.1 Hack or Scam? The One Question That Decides 11
1.2 Where Hacks Usually Start 12
1.3 Why Layers Matter 12
1.4 Illustrative Scenario: The Drained Wallet 13
1.5 CSF Rules for This Chapter 14
1.6 If This Just Happened to You 14
Malware and Infostealers 16
2.1 What Malware Wants from a Crypto User 17
2.2 How Malware Gets onto Your Device Today 18
2.3 Warning Signs That a Device May Be Compromised 19
2.4 Illustrative Scenario: The Coding Test 19
2.5 How to Protect Yourself from Malware 20
2.6 CSF Rules for This Chapter 22
2.7 If This Just Happened to You 23
Supply Chain and Wallet Software Flaws 24
3.1 What Supply Chain Attacks Look Like 25
3.2 A Real Case: Implanted Devices from a Reseller 25
3.3 How to Buy and Set Up a Hardware Wallet Safely 26
3.4 Compromised Wallet Software and Libraries 27
3.5 Illustrative Scenario: The Bargain Device 27
3.6 CSF Rules for This Chapter 28
3.7 If This Just Happened to You 29

Account Takeover: Email, SIM Swaps, Passwords and 2FA 30
4.1 Your Email Is the Master Key 31
4.2 SIM Swaps: When Your Phone Number Is Taken 31
4.3 Passwords and Passkeys 32
4.4 Two-Factor Authentication: Not All 2FA Is Equal 33
4.5 Stolen Sessions: Why 2FA Is Not Always Enough 33
4.6 Exchange Settings That Stop a Takeover from Becoming a Loss 34
4.7 Messaging Accounts: Takeovers That Spread to Your Contacts . 34
4.8 Illustrative Scenario: The Night-Time Swap 35
4.9 CSF Rules for This Chapter 36
4.10 If This Just Happened to You 37
Network Attacks and Public Wi-Fi 38
5.1 The Real Risks Today 39
5.2 What Still Matters 39
5.3 Illustrative Scenario: The Airport Login 40
5.4 CSF Rules for This Chapter 40
5.5 If This Just Happened to You 41
Platform Breaches and Insider Attacks 42
6.1 Two Kinds of Platform Breach 43
6.2 Insider Attacks 43
6.3 How to Limit Your Exposure 44
6.4 Illustrative Scenario: The Breach Notice 44
6.5 CSF Rules for This Chapter 45
6.6 If This Just Happened to You 46
Physical Coercion (Wrench Attacks) 47
7.1 How People Become Targets 48
7.2 Privacy: The Best Protection 48
7.3 Setting Up Your Crypto So There Is Little to Take 49
7.4 If It Happens 49
7.5 CSF Rules for This Chapter 50

7.6 If This Just Happened to You 50
Advanced Protection 52
8.1 A Dedicated Device for Crypto 52
8.2 Multisig: More Than One Key 53
8.3 Other Options Compared 54
8.4 Signing Habits That Matter at Any Level 54
8.5 CSF Rules for This Chapter 55
If You've Been Hacked 56
9.1 The First Hour 57
9.2 Find the Likely Cause 57
9.3 Report It 58
9.4 Rebuild Safely 59
9.5 CSF Rules for This Chapter 59
CSF Rules Index 61
Keep Learning 63

About This Edition

The first edition of this guide, published in January 2025 as “How to Keep Your Crypto and Digital Assets Safe from Hackers”, was built around four attack types. Since then, CryptoSafetyFirst has collected and classified real losses reported by crypto users every week. Most hacks against individuals turned out to start on the user’s own device or accounts – not with a broken blockchain. The 2026 Edition is rebuilt around what that work shows.

What is new

- **Nine chapters built around the CSF incident taxonomy,** plus advanced protection and what to do after a hack, so the book, the website and the CSF rules use the same categories.
- **New chapters** on supply-chain attacks, account takeover, platform breaches, physical coercion and what to do after a hack.
- **A clear line with the Scams guide:** this book covers what happens when an attacker gets access. Phishing, impersonation and fake apps are covered in the Scams Prevention Guidebook and linked here.
- **CSF rules in every chapter,** with one main rule per chapter and the supporting rules behind it.
- **Corrected and updated advice,** including what a padlock and an authenticity check really prove, and why a SIM card PIN does not stop a SIM swap.

How examples and data are handled

- Scenarios are illustrative unless clearly stated otherwise. Real cases are described with their month and year, without naming the companies or people involved.
- 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.
- Products and services are not recommended by name. Where a setting is described, check the provider’s official website for the current steps.

How to Use This Book

If you…	Go to
just lost funds and do not know how	Chapter 9: If You've Been Hacked – first-hour checklist.
want to understand where hacks start	Chapter 1.
want to protect your devices and wallets	Chapters 2, 3 and 8, and the free Three-Wallet Model guide.
want to protect your accounts	Chapter 4, then Chapters 5 and 6.
are worried about your personal safety	Chapter 7.

Where to start

How each chapter works

Most chapters follow the same structure: an at-a-glance image, how the attack works, an illustrative scenario, how to protect yourself, the CSF rules for that chapter, and first steps if it just happened to you. Each chapter ends with a link to its page, or to the guide page, on CryptoSafetyFirst.com.

START HERE

If You Think You Have Been Hacked

Move what is left before you investigate. Go to **Chapter 9** now: it lists the first-hour steps in order – new wallet, secure email, lock exchanges, call your mobile provider, revoke approvals – and explains how to find the likely cause afterwards.

BE ALERT FOR RECOVERY SCAMS

After a hack, 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**.

CHAPTER 1

How Hacks Usually Start

“I never shared my seed phrase. How did they get in?”

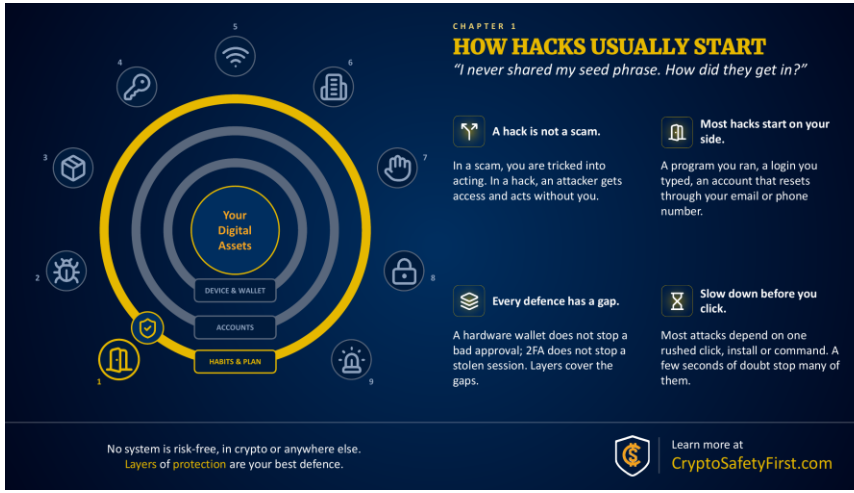

Figure 1.1: How Hacks Usually Start at a glance

No system is free of risk, in traditional finance or in crypto. But crypto holders are more attractive targets than most: funds can be moved in minutes, transfers cannot be reversed, and a single wallet or account often holds a large share of someone’s savings. That is why crypto needs more care than online banking, not less.

The good news is that hacks against individual users follow a small number of patterns. Each one has defences that work, and layered together, they keep one weak point from costing you everything. This chapter explains what counts as a hack, where hacks usually start, and how the rest of this book is organised around them.

IN THIS CHAPTER

- 1.1 Hack or Scam? The One Question That Decides
- 1.2 Where Hacks Usually Start
- 1.3 Why Layers Matter
- 1.4 Illustrative Scenario: The Drained Wallet
- 1.5 CSF Rules for This Chapter
- 1.6 If This Just Happened to You

1.1 Hack or Scam? The One Question That Decides

The CryptoSafetyFirst guides separate losses by one question: **who took the action that moved the funds or opened the account?**

- **A scam:** you were persuaded to act yourself – to send crypto, sign a transaction, connect your wallet or share your seed phrase. Covered in the **Scams Prevention Guidebook**.
- **A hack:** an attacker got access to your device, account or wallet and acted without your approval. Covered in this book.
- **A user mistake:** nobody attacked you; a backup, an address or a setting failed. Covered in the **User Mistakes Prevention Guidebook**.

Many hacks begin with a trick – a fake download, a link, a message – and then continue without you. This book starts where the trick ends: at the moment an attacker gains access.

1.2 Where Hacks Usually Start

Entry point	What the attacker gets	Chapter
A program, extension or command you were persuaded to run	Control of your device, your wallet files and your logged-in accounts	2
A tampered device or a compromised wallet app or library	Your seed phrase or your transactions, before you use the wallet	3
Your email, phone number or passwords	Your exchange and wallet accounts, through password resets and stolen sessions	4
A network you do not control	Redirected traffic and fake login pages	5
A platform that holds your crypto or your data	Your funds on that platform, or your name and address	6
Your home and your public profile	Physical pressure on you or your family	7

Table 1.1: The usual entry points and where this book covers them

Phishing pages, fake support, impersonation and fake apps are the most common first step. They are covered in detail in the Scams guide: **Social Engineering**, **Phishing** and **Fake Apps and Browser Extensions**.

1.3 Why Layers Matter

Every defence in this book has a gap. A hardware wallet does not stop you from approving a bad transaction; 2FA does not stop a stolen session; a strong password does not help if your email is taken over. What works is several layers, so that one failure is not enough:

- **Separate your crypto:** savings in a Vault wallet that never connects to websites, everyday activity in a separate wallet (see **The Three-Wallet Model**).
- **Protect the device:** official software only, a separate device or account for crypto, keys on a hardware wallet (Chapters 2 and 3).

- **Protect the accounts:** a separate email for crypto, hardware-based 2FA, withdrawal whitelists (Chapter 4).
- **Protect yourself:** keep your holdings private, and plan for the day something goes wrong (Chapters 7 and 9).

1.4 Illustrative Scenario: The Drained Wallet

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

Sam wakes up to an empty wallet. He never shared his seed phrase and never signed anything unusual. He changes his password, but the next day his exchange account is emptied too.

What Happened

A “free trading tool” Sam installed weeks earlier was an infostealer. It copied his wallet data and the login session of his exchange. Changing a password on the same infected computer did nothing: the attacker was already inside.

Key Takeaways

- A drain without a signature usually means a compromised device or seed phrase.
- Act from a clean device, and move funds before you investigate.
- Chapter 9 has the first-hour checklist for exactly this situation.

1.5 CSF Rules for This Chapter

MAIN RULE · TSR-007

Slow Down Before Clicking or Installing.

Most hacks depend on one rushed click, install or command.

Rule	Statement	Why it applies here
SDR-001	Never Trust Unsolicited Crypto Contact	Most hacks start with a message, link or file you did not ask for.
SDR-009	Verify All Links Before Logging In	A copied login page hands over your password and 2FA code.
GR-005	Never Follow Urgent Support or Security Instructions. Exit the Channel and Re-Enter Through the Official App or URL	Fake security alerts are a common way to get you to install or log in.
GR-008	Keep Long-Term Holdings in a Vault wallet. Use a Separate Wallet for DApps, Trading, and Web3	A hack of your everyday wallet should not reach your savings.

Table 1.2: CSF rules for the first step of a hack

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

1.6 If This Just Happened to You

If funds have left your wallet or account and you do not know why, go straight to **Chapter 9**: If You've Been Hacked. Act from a clean device, and move what is left before you investigate.

AFTER A LOSS

Expect offers to trace or recover the stolen crypto. Nobody can reverse a confirmed transfer for a fee. See **Recovery Scams** and report the theft: **How to Report a Crypto Scam**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

All chapters, updates and related guides are on the guide page:

cryptosafetyfirst.com/keep-your-crypto-safe-from-hackers/

CHAPTER 2

Malware and Infostealers

“I only ran the setup script for the coding test.”

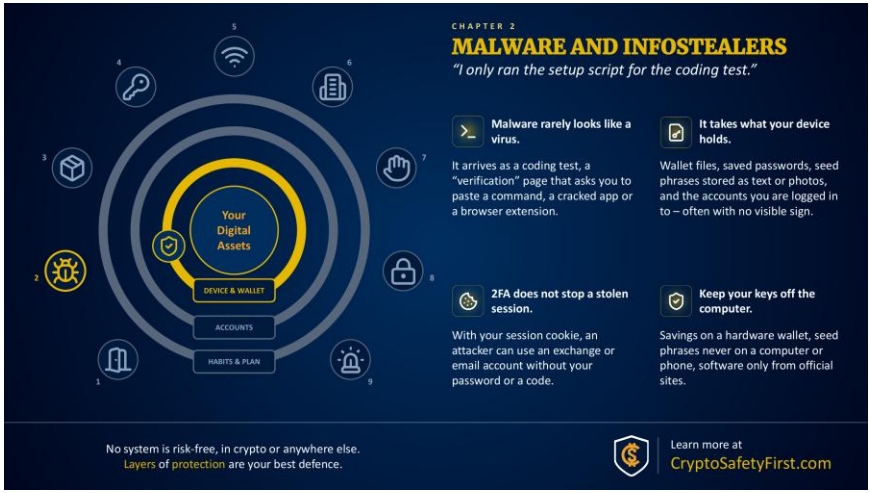

Figure 2.1: Malware and Infostealers at a glance

Most hacks against individual crypto users do not break any encryption. They start on the user’s own device: a program that looks useful, a browser extension, a “verification” step or a file from a new contact. Once malware runs, it can read what you type and store, swap what you paste and use the accounts you are logged in to – often without any visible sign.

This chapter explains what malware takes from crypto users, how it gets onto computers and phones today, the signs that a device may be compromised, and the habits that keep one infected device from costing you everything.

IN THIS CHAPTER

- 2.1 What Malware Wants from a Crypto User
- 2.2 How Malware Gets onto Your Device Today
- 2.3 Warning Signs That a Device May Be Compromised
- 2.4 Illustrative Scenario: The Coding Test
- 2.5 How to Protect Yourself from Malware
- 2.6 CSF Rules for This Chapter
- 2.7 If This Just Happened to You

2.1 What Malware Wants from a Crypto User

Crypto malware does not need to “hack” a blockchain. It goes after whatever on your device can move your funds or open your accounts.

Type	What it takes	Why it hurts
Infostealer	Wallet files and browser-extension data, saved passwords, seed phrases stored as text, photos or notes, and browser session cookies	Session cookies let an attacker use an account you are already logged in to, without your password or 2FA code.
Clipboard swapper	Nothing at first: it waits until you copy a crypto address and replaces it with the attacker’s	The transfer looks normal and confirms. The funds go to the attacker and cannot be reversed.
Remote-access trojan	Control of the whole computer: screen, keyboard, files and open apps	The attacker can act as you, at a time when you are not watching.
Fake wallet app or fake update prompt	Your seed phrase, typed into a window that looks like your wallet software	One typed seed phrase gives away every account in that wallet, on every network.

Table 2.1: What crypto malware takes

Windows PCs are not the only target. Macs are increasingly targeted too, and so are phones: fake wallet apps, apps that read screenshots in your photo gallery, and second-hand phones that come with malware already installed.

2.2 How Malware Gets onto Your Device Today

Malware rarely arrives as an obvious virus. It is usually something you were persuaded to run yourself.

1. Fake Job Interviews and Coding Tests

A recruiter or “Web3 company” offers paid work, then asks you to clone a code repository, run a setup script, install a meeting app or open a project file. The script installs malware. Developers and community managers are the main targets. The job scam side is covered in **Chapter 11 of the Scams Prevention Guidebook**.

2. “Verification” Pages That Ask You to Paste a Command

A page shows a fake CAPTCHA, “human verification” or error message and asks you to press a key combination, paste something into the Run box or Terminal, and press Enter. No real website ever needs this. The command downloads malware with your own permissions.

3. Search Ads, Look-Alike Download Sites and Chatbot Links

Sponsored search results, social media ads and copied download pages offer wallet apps, trading tools or everyday software with malware inside. Links suggested by AI chatbots can point to the same copycat sites. Download software only from the address on the developer’s official website, typed or bookmarked yourself.

4. Browser Extensions and Bookmarklets

Extensions can read and change every page you open, including your wallet and exchange tabs. Some are malicious from the start; others turn malicious through an update after they have built up users. “Trading bot” bookmarklets shared in Discord or Telegram run code inside the page you are logged in to. Fake wallet extensions are covered in **Chapter 4 of the Scams Prevention Guidebook**.

5. Cracked Software, Game Cheats and “Free Tools”

Pirated programs, game cheats, free “AI tools” and mining apps are a common way to deliver infostealers. If something paid is offered for free from an unofficial source, assume the price is your data.

6. Files and Invitations from New Contacts

A contact you met online sends a document, an “encrypted” project file, a game to test on their server or a meeting link that needs a special app. Weeks of friendly conversation are part of the method, not proof of trust.

2.3 Warning Signs That a Device May Be Compromised

Many infections show no sign at all. If one of these appears, stop using the device for crypto and follow the steps at the end of this chapter.

- A pasted address is different from the one you copied.
- Your wallet software suddenly asks you to type your **seed phrase**, “re-verify” the wallet or fix a firmware error. Hardware wallet apps do not ask you to type your seed phrase into a pop-up or “verification” window. A real recovery is something you start yourself, following the manufacturer’s official instructions.
- Extensions, programs or browser settings you did not add, such as a changed proxy or a new default search engine.
- Login alerts, new devices or active sessions in your email or exchange accounts that are not yours.
- Accounts change on their own: messages sent from your social profiles, new API keys, changed withdrawal settings.

The absence of warning signs does not mean the device is clean. An infostealer can copy everything within seconds and leave nothing visible behind.

2.4 Illustrative Scenario: The Coding Test

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

Daniel, a freelance developer, is contacted on a professional network by a recruiter from a Web3 start-up. After two friendly calls, he is sent a repository for a short paid coding test and asked to run the setup script before the next interview.

The script runs in the background while Daniel works on the task. Two days later, his browser wallet is empty and someone has logged in to his exchange account from another country – without his password or 2FA code.

What Happened

The setup script installed an infostealer. It copied his browser wallet data and the session cookie of his exchange login. The attacker did not need to break anything: the computer handed over what it held.

Key Takeaways

- Never run code, scripts or installers sent by someone you met online on the computer you use for crypto.
- A device that runs unknown software is not a place for wallets or exchange logins.
- A hardware wallet would have kept the keys of Daniel's savings off the computer.

2.5 How to Protect Yourself from Malware

- **Install crypto software only from official sources.** Type the developer's website address yourself or use a bookmark; never follow ads, search results, chat links or chatbot suggestions to a download.
- **Keep crypto on a separate device or user account.** Use one computer, or at least one separate account and browser profile, only for wallets and exchanges, with no games, cracked software, test code or random extensions.
- **Keep savings on a hardware wallet.** Its keys never leave the device, so malware on the computer cannot copy them. Check every address and amount on the hardware wallet's own screen before you approve.
- **Never store a seed phrase on a device.** No text files, photos, notes, password managers or cloud drives. Write it on paper or metal (see **Chapter 2 of the User Mistakes Prevention Guidebook**).
- **Never paste a command a website asks for.** Close the page instead.
- **Keep extensions to a minimum.** Remove the ones you no longer use, and be suspicious of any extension that suddenly asks for new permissions.
- **Update your system, browser and wallet apps.** Install updates through the app or system itself, never from a pop-up or a link.

- **Treat security software as a baseline, not a guarantee.** Built-in antivirus helps against known malware; it does not catch everything new. See **Safety Tools** for what each tool covers.

Defence	What it stops	What it does not stop
Hardware wallet	Malware copying your private keys	You approving a malicious transaction or address on its screen
Separate device or account for crypto	An infection from everyday use reaching your wallets	Malware you install on that device yourself
Checking the full address on the device screen	Clipboard swappers	A wrong address you chose yourself
Antivirus and updates	Known malware and known security holes	New malware and anything you run on purpose

Table 2.2: What each defence covers

2.6 CSF Rules for This Chapter

MAIN RULE · TSR-002

Assume Your Device Can Be Compromised.

Check addresses and transactions on the hardware wallet's screen, and keep secrets off the computer.

Rule	Statement	Why it applies here
TSR-001	Never Install Crypto Software from Unofficial Sources	Fake wallets, extensions and trading tools are the most common way malware arrives.
TSR-006	Separate Devices and Accounts for Crypto Use	One infected device should not expose all your crypto at once.
TSR-007	Slow Down Before Clicking or Installing	Almost every infection starts with one rushed install, click or pasted command.
GR-003	Always Use a Hardware Wallet for Long-Term or High-Value Crypto Storage	Keys on a hardware wallet cannot be copied by malware on the computer.
GR-007	Never Store Your Seed Phrase in Cloud Storage, Email, or Screenshots	Infostealers search for exactly these files and photos.

Table 2.3: CSF rules for malware and infostealers

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

2.7 If This Just Happened to You

For the full first-hour checklist, see **Chapter 9**: If You've Been Hacked. The steps specific to malware:

If you…	Do this now
ran a suspicious file, script or command	Disconnect the device from the internet. Do not type passwords or seed phrases on it again. From a clean device, move funds from every wallet that was ever used on it to new wallets with new seed phrases.
see a pasted address change	Do not send. Stop using the device for crypto until it has been wiped and reinstalled.
typed your seed phrase into an app or window	Treat the seed phrase as burned. On a clean device, create a new wallet and move everything now – also from any hardware wallet that uses the same seed phrase.
see logins or changes you did not make	From a clean device: change the email password first, log out all sessions, revoke API keys, check withdrawal whitelists, then change exchange passwords.

Table 2.4: First steps after a malware infection

Wiping and reinstalling comes last, after the funds are safe: a clean system does not make an exposed seed phrase safe again.

AFTER A LOSS

Expect offers to trace or recover the stolen crypto. Nobody can reverse a confirmed transfer for a fee. See **Recovery Scams** and report the theft: **How to Report a Crypto Scam**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/malware-attacks-cryptocurrency/

CHAPTER 3

Supply Chain and Wallet Software Flaws

“It was sealed, it passed the check – at half price.”

Figure 3.1: Supply Chain and Wallet Software Flaws at a glance

A hardware wallet protects your keys from the computer it is plugged into. It cannot protect you from a device that was tampered with before it reached you, or from a wallet app that was compromised at the source. These attacks are rarer than malware, but when they happen, they hit careful users who did everything else right.

This chapter covers the two sides of supply-chain risk – the device you buy and the software you run – and the simple buying and updating habits that remove most of it.

IN THIS CHAPTER

- 3.1 What Supply Chain Attacks Look Like
- 3.2 A Real Case: Implanted Devices from a Reseller
- 3.3 How to Buy and Set Up a Hardware Wallet Safely
- 3.4 Compromised Wallet Software and Libraries
- 3.5 Illustrative Scenario: The Bargain Device
- 3.6 CSF Rules for This Chapter
- 3.7 If This Just Happened to You

3.1 What Supply Chain Attacks Look Like

- **A tampered hardware wallet:** a device modified between the factory and you, most often sold by a reseller or marketplace seller, sometimes below the normal price.
- **A device with a pre-set seed phrase:** a wallet that arrives with a seed phrase already printed on a card, or with instructions to use a supplied phrase instead of creating a new one.
- **A compromised wallet app or update:** the official software, or a code library it uses, is changed by an attacker so that it steals keys or swaps addresses.
- **Leaked customer data:** a breach at a seller exposes buyers' names and addresses, which are then used for phishing, fake "replacement device" mailings and threats (Chapters 6 and 7).

3.2 A Real Case: Implanted Devices from a Reseller

In October 2026, a major hardware wallet manufacturer confirmed that devices sold through a reseller in Southeast Asia, which several manufacturers had listed as authorised, contained an added hardware implant. The implant read the **seed phrase** shown on the device screen during setup and sent it out over a built-in mobile (LTE) connection. Buyers who set up these devices later found their funds drained. Units were reportedly also sold through online marketplaces at around half the normal price. A large European electronics retailer briefly paused sales after a customer report; the manufacturer later said it had found no tampered stock in Europe.

The manufacturer noted that its authenticity check cannot detect an added implant when the original secure chip is intact. In other words: **a genuine check confirms the chip, not the whole device.**

The same month, another hardware wallet maker reported that an attacker had taken customer and shipping data from its online shop, together with the key used by its online device-verification check – which means counterfeit devices could pass that check. The maker announced it would destroy its unsold stock and issue devices with a new key. Seed phrases and private keys were not affected, and devices delivered before the intrusion stayed safe to use.

The lessons from both cases: **a passed authenticity check is not proof on its own, an authorised channel lowers the risk but does not remove it, and after any leak you should expect targeted letters, parcels and messages – even if you bought directly from the maker.**

3.3 How to Buy and Set Up a Hardware Wallet Safely

- **Buy directly from the manufacturer's official store,** typing its address yourself. That is the safest channel. An authorised reseller, listed on the manufacturer's website, lowers the risk but does not remove it.
- **Never buy second-hand, returned, "open box" or unusually cheap devices,** and never accept one as a gift from someone you met online.
- **Check the packaging and the device** against the manufacturer's description. Any sign of opening, a different weight or a loose part: do not set it up.
- **Always create a new seed phrase on the device itself.** A device that arrives with a seed phrase, or that tells you to use a phrase supplied with it instead of creating a new one, has been tampered with.
- **Write the seed phrase on paper or metal only,** never on a computer or phone.
- **Update firmware only through the device's official app,** never from a link, email or pop-up.
- **Test with a small amount first,** then send more.

3.4 Compromised Wallet Software and Libraries

Wallet apps, browser extensions and the websites of decentralised apps are built on shared code libraries. When an attacker takes over one of these – through a stolen developer account, for example – the change can reach many apps at once. Past cases include a code library used by many dApp websites, altered in December 2023, and widely used developer packages altered in September 2025 to swap crypto addresses in browsers.

You cannot audit this code yourself. What you can do:

- Check every address and amount on your hardware wallet's own screen before you approve. A compromised app can show one thing on the computer and send another.
- Avoid blind signing: if the device cannot show what you are approving, do not approve it with your savings.
- When a wallet, extension or dApp you use is reported as compromised, stop using it until the developer's official channel says the fix is out. Check the official website or account, not messages that reach you.
- Keep long-term funds in a Vault wallet that does not connect to dApps at all, so a compromised dApp front end cannot reach it.

3.5 Illustrative Scenario: The Bargain Device

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

Lena wants to move her savings off an exchange. She finds her chosen hardware wallet on a large marketplace for well below the usual price, sealed, with good seller ratings. Setup works, the authenticity check passes, and she moves her savings. Three weeks later, they are gone.

What Happened

The device had been opened and modified before it was resealed and sold. The seed phrase was captured during setup. Nothing Lena did afterwards could have stopped it.

Key Takeaways

- A hardware wallet is only as trustworthy as the place you bought it.
- A low price for a security device is a warning, not a bargain.
- An authenticity check confirms the chip, not that nothing was added.

3.6 CSF Rules for This Chapter

MAIN RULE · TSR-001

Never Install Crypto Software from Unofficial Sources.

The same applies to hardware: buy directly from the manufacturer's official store; an authorised reseller lowers the risk but does not remove it.

Rule	Statement	Why it applies here
GR-003	Always Use a Hardware Wallet for Long-Term or High-Value Crypto Storage	Still the best protection for savings – if the device itself can be trusted.
TSR-002	Assume Your Device Can Be Compromised	Verify addresses and amounts on the hardware wallet screen, not the computer.
GR-008	Keep Long-Term Holdings in a Vault wallet. Use a Separate Wallet for DApps, Trading, and Web3	A compromised dApp or extension cannot reach a wallet that never connects.

Table 3.1: CSF rules for supply-chain risks

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

3.7 If This Just Happened to You

For the full first-hour checklist, see **Chapter 9**. The steps specific to supply-chain risks:

If you…	Do this now
bought a hardware wallet from a reseller or marketplace and have doubts	Do not set it up. Contact the manufacturer through its official website and ask how to confirm it is genuine.
received a device after its maker reported a breach	Check the maker's official notice on whether your device is affected before you set it up.
already use a device from a seller that is reported as compromised	Buy a new device directly from the manufacturer, create a new seed phrase on it, and move all funds to it. Do not reuse the old seed phrase.
use a wallet app or extension that is reported as compromised	Stop using it. Follow the developer's official instructions; if keys may be exposed, move funds to a new wallet with a new seed phrase.
received a letter, parcel or message about a "replacement device" after a data leak	Ignore it and do not enter your seed phrase anywhere. Manufacturers do not send unrequested devices.

Table 3.2: First steps for supply-chain risks

AFTER A LOSS

Expect offers to trace or recover the stolen crypto. Nobody can reverse a confirmed transfer for a fee. See **Recovery Scams** and report the theft: **How to Report a Crypto Scam**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/hardware-wallet-supply-chain-attacks/

CHAPTER 4

Account Takeover: Email, SIM Swaps, Passwords and 2FA

“No service on my phone. An hour later, no funds.”

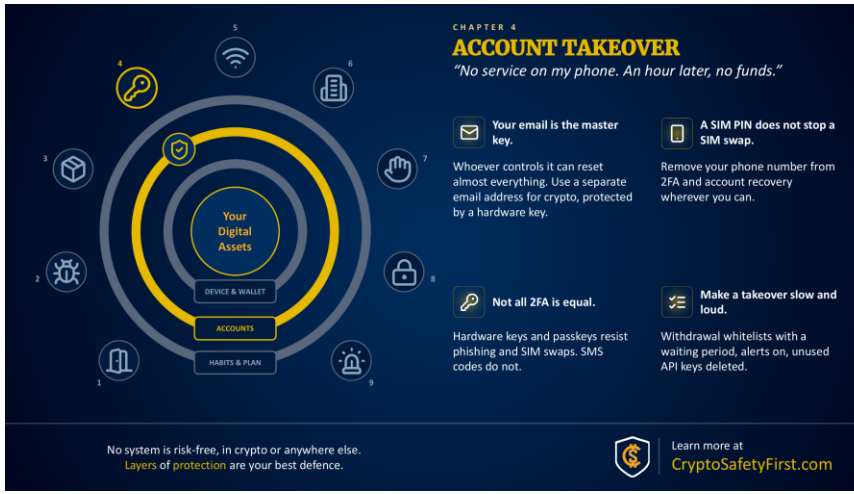

Figure 4.1: Account Takeover at a glance

Your exchange account, your wallet app’s cloud backup and your crypto tax tool are only as safe as the accounts behind them: your email, your phone number and your passwords. Attackers rarely break into an exchange directly. They take over the email that can reset its password, the phone number that receives its codes, or the browser session that is already logged in.

This chapter covers how account takeovers happen – email compromise, SIM swaps, reused passwords, stolen sessions and hijacked messaging accounts – and how to set up your accounts so that one stolen password or code is not enough.

IN THIS CHAPTER

- 4.1 Your Email Is the Master Key
- 4.2 SIM Swaps: When Your Phone Number Is Taken
- 4.3 Passwords and Passkeys
- 4.4 Two-Factor Authentication: Not All 2FA Is Equal
- 4.5 Stolen Sessions: Why 2FA Is Not Always Enough
- 4.6 Exchange Settings That Stop a Takeover from Becoming a Loss
- 4.7 Messaging Accounts: Takeovers That Spread to Your Contacts
- 4.8 Illustrative Scenario: The Night-Time Swap
- 4.9 CSF Rules for This Chapter
- 4.10 If This Just Happened to You

4.1 Your Email Is the Master Key

Almost every account can be reset through email. Whoever controls your email can usually take over everything connected to it. Treat the email behind your crypto accounts as the most important account you have:

- **Use a separate email address only for crypto accounts,** not the one you give to shops, newsletters and social media. It will receive less phishing, and a leak elsewhere does not reveal it.
- **Protect it with a hardware security key or passkey,** and remove SMS as a login or recovery option. Options are on our **Safety Tools** page.
- **Check its settings every three months:** recovery email and phone, forwarding rules, connected apps and active sessions. Attackers often add a forwarding rule and stay quiet.
- **Keep its recovery codes offline,** with your other backups (see **Chapter 3 of the User Mistakes Prevention Guidebook**).

4.2 SIM Swaps: When Your Phone Number Is Taken

In a SIM swap, an attacker convinces your mobile provider – or bribes someone who works there – to move your number to a SIM card or eSIM they control. Your phone suddenly loses service. From then on, every SMS code and every “reset by text message” goes to the attacker.

A SIM card PIN does not protect against this: it only locks the physical card in your phone. What helps:

- **Remove your phone number as a 2FA method and as a recovery option** on email, exchanges and wallet apps wherever the service allows it.
- **Ask your mobile provider for account protection:** a separate account PIN or password, and a block on number transfers and SIM changes without in-person identification, where offered.
- **Keep your phone number private.** Where a service insists on a phone number, use a separate number that you use only for that and never publish.
- **Treat a sudden "No service" as an emergency** if you have not changed anything: call your mobile provider from another phone, and secure your email from another device.

4.3 Passwords and Passkeys

- **Use a different password for every account.** Stolen passwords from one leaked site are automatically tried on exchanges and email providers.
- **Let a reputable password manager create and store them.** Long random passwords or a passphrase of several random words; no personal details. See **Safety Tools**.
- **You do not need to change strong, unique passwords on a schedule.** Change them when a service reports a breach or you suspect a problem.
- **Use passkeys where they are offered.** A passkey cannot be typed into a fake site, so it resists phishing. Make sure you can still log in if you lose the phone or account that stores it.
- **Never store your seed phrase in the password manager.** It is for passwords, not for the keys to your wallet.

4.4 Two-Factor Authentication: Not All 2FA Is Equal

Method	Protects against	Main weakness
Hardware security key or passkey	Password theft, phishing pages, SIM swaps	Losing it without a backup key or recovery codes
Authenticator app	Password theft, SIM swaps	A code typed into a fake site; a lost phone without backup
Email code	Password theft only	Falls with your email account
SMS code	Password theft only	SIM swaps and phished codes

Table 4.1: 2FA methods from strongest to weakest

Use a hardware security key or passkey for **two-factor authentication** on your email and your exchange accounts, with a second key or recovery codes stored separately. Where a service only offers an authenticator app, use that. Keep SMS only where nothing else is available, and never as the recovery route for your email.

4.5 Stolen Sessions: Why 2FA Is Not Always Enough

After you log in, your browser keeps a session cookie so you do not have to log in again. Infostealer malware copies these cookies (see **Chapter 2**). With one, an attacker can use your account as if they were you – without your password and without a 2FA code.

- Log out of exchange and email accounts when you finish, especially on shared or everyday devices.
- Check the list of active sessions and devices in your email and exchange accounts, and end the ones you do not recognise.
- If a device may be infected, end all sessions from a clean device and change passwords there – not on the infected device.

4.6 Exchange Settings That Stop a Takeover from Becoming a Loss

- **Withdrawal whitelist:** funds can only go to addresses you saved in advance, usually with a waiting period before a new address can be used or the whitelist can be turned off. An attacker who controls your email and 2FA can still change it, but the delay gives you time to see the alert and freeze the account.
- **Anti-phishing code:** a word you choose that appears in every genuine email from the exchange.
- **API keys:** create them only for tools you trust, never with withdrawal rights, limited to your IP address where possible; delete keys you no longer use.
- **Alerts:** turn on email or app alerts for logins, withdrawals and security changes.
- **Keep only what you trade on the exchange.** Savings belong in your own Vault wallet.

4.7 Messaging Accounts: Takeovers That Spread to Your Contacts

A taken-over Telegram, WhatsApp, Discord or social media account is used to message your contacts – asking for crypto, sharing a malicious link or a “game to test”. Attackers get in with a stolen login code, a hijacked session or the voicemail on your number, where some services leave a login code when you do not answer.

- Turn on the extra password or PIN these apps offer (two-step verification).
- Set a voicemail PIN or switch voicemail off if you do not use it; ask your mobile provider how.
- Never forward a login code to anyone, even a friend who asks.
- Review active sessions and linked devices in each app.
- If a friend asks for crypto or sends a file, confirm with them on a different channel first.

4.8 Illustrative Scenario: The Night-Time Swap

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

On a Saturday evening, Ana's phone shows "No service". She assumes a network problem and goes to sleep. Overnight, someone resets the password of her email using an SMS code, logs in to her exchange account through "forgot password", and withdraws her balance.

What Happened

Her number had been moved to a new SIM. Her email used SMS as its recovery method, and her exchange relied on that email and on SMS codes. One stolen phone number unlocked every account in the chain.

Key Takeaways

- Never let a phone number be the only thing between an attacker and your email.
- Hardware keys and passkeys cannot be redirected to a new SIM.
- A withdrawal whitelist, with alerts turned on, would have delayed the withdrawal and given Ana time to react.

4.9 CSF Rules for This Chapter

MAIN RULE · TSR-004

Use Hardware-Based Two-Factor Authentication.

A physical security key cannot be redirected to a new SIM or entered on a fake site.

Rule	Statement	Why it applies here
TSR-005	Enable Withdrawal Whitelists on Exchanges	New withdrawal addresses are delayed, giving you time to act before funds leave.
OR-006	Maintain Access to Your Authentication Systems	Backup keys and recovery codes keep you from locking yourself out.
SDR-009	Verify All Links Before Logging In	Copied login pages are the most common way passwords and codes are stolen.
GR-007	Never Store Your Seed Phrase in Cloud Storage, Email, or Screenshots	A taken-over email or cloud account must not contain your seed phrase.
TSR-006	Separate Devices and Accounts for Crypto Use	A separate email for crypto limits what one leak or takeover exposes.

Table 4.2: CSF rules for account takeover

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

4.10 If This Just Happened to You

For the full first-hour checklist, see **Chapter 9**. The steps specific to account takeover:

If you…	Do this now
suddenly have no mobile service	Call your mobile provider from another phone and ask whether your SIM was changed. From another device, secure your email first, then your exchanges.
lost access to your email	Use the provider's official account recovery right away. In parallel, contact your exchanges through their official websites to freeze withdrawals.
see logins, withdrawals or new API keys you did not make	From a clean device: end all sessions, change the password, delete unknown API keys, check the withdrawal whitelist and contact the exchange's official support.
had a messaging account taken over	Recover it through the app, end other sessions, turn on two-step verification and warn your contacts on another channel.

Table 4.3: First steps after an account takeover

AFTER A LOSS

Expect offers to trace or recover the stolen crypto. Nobody can reverse a confirmed transfer for a fee. See **Recovery Scams** and report the theft: **How to Report a Crypto Scam**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/sim-swap-scams-crypto-web3/

CHAPTER 5

Network Attacks and Public Wi-Fi

“The hotel Wi-Fi wanted my email login first.”

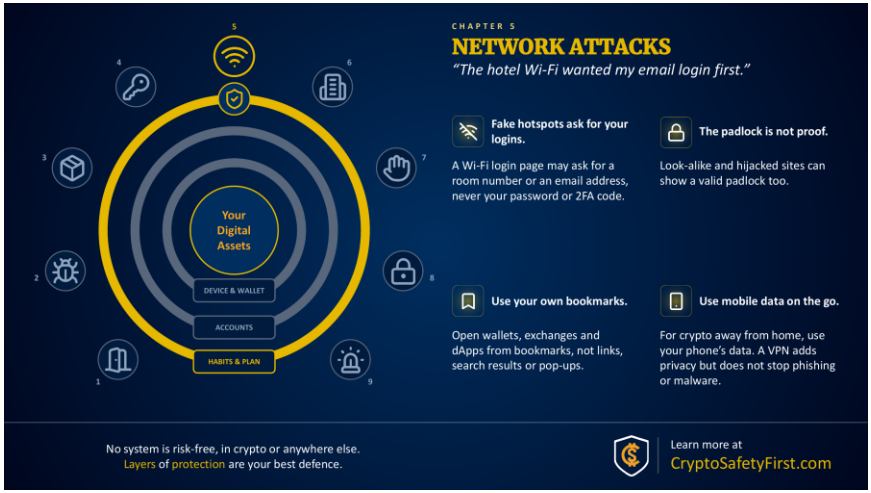

Figure 5.1: Network Attacks and Public Wi-Fi at a glance

Network attacks get a lot of attention, but they cause far fewer losses than malware or account takeover. Most websites and wallet apps now encrypt their traffic, so simply listening on a network reveals little. The real risks today are networks and pages that trick you into typing something – a password, a code or a seed phrase – or that send you to a fake site.

This chapter is short on purpose. It covers what still matters on networks you do not control, and the few habits that make the rest irrelevant.

IN THIS CHAPTER

- 5.1 The Real Risks Today
- 5.2 What Still Matters
- 5.3 Illustrative Scenario: The Airport Login
- 5.4 CSF Rules for This Chapter
- 5.5 If This Just Happened to You

5.1 The Real Risks Today

- **Fake hotspots:** a network with a familiar name, set up by an attacker, whose “login page” asks for your email password or another account login.
- **Fake update or login prompts** shown while you are connected, asking you to install something or sign in again.
- **Redirected websites:** an attacker who controls the network sends you to a look-alike address, or, if a project’s domain has been taken over, to a fake site at the real address. Either can show a valid padlock.
- **Shoulder surfing:** someone watches your screen or keyboard in a café, train or co-working space.

The padlock in the address bar means the connection is encrypted, not that the site is genuine. A fake site can have one too.

5.2 What Still Matters

- **Open wallets, exchanges and dApps from your own bookmarks,** not from links, search results or pop-ups.
- **Never enter a password, 2FA code or seed phrase on a Wi-Fi login page.** A genuine hotspot may ask for an email address, a room number or an access code, but never your email password, 2FA code or seed phrase.
- **Prefer your phone’s mobile data or hotspot** for crypto when you are away from home.
- **Keep your browser and system updated,** and turn on secure DNS in the browser settings if it is not on already.
- **Check transactions on your hardware wallet’s screen,** so that a manipulated page cannot change what you approve.
- **Do large transfers at home,** not in public, where screens can be watched and connections tricked.

A **VPN** adds privacy on networks you do not trust: it hides your traffic from the network owner and moves that trust to the VPN provider. It does not protect you from phishing pages, malware or fake apps, and it is not a reason to relax the habits above.

5.3 Illustrative Scenario: The Airport Login

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

Waiting for a delayed flight, Omar connects to an open network named after the airport. The login page asks him to “sign in with your email account” for free access. He does, then checks his exchange balance. Later that evening his email password is changed.

What Happened

The network was a fake hotspot. Its login page collected his email password, and his email had no hardware-based 2FA. Nothing was intercepted; he typed it in himself.

Key Takeaways

- A Wi-Fi login page never needs your email or exchange password.
- Use mobile data for anything crypto when travelling.
- Hardware-based 2FA would have made the stolen password useless.

5.4 CSF Rules for This Chapter

MAIN RULE · TSR-003

Avoid Public Wi-Fi for Crypto Operations.

Use mobile data or a network you control for logins and transfers.

Rule	Statement	Why it applies here
TSR-002	Assume Your Device Can Be Compromised	Verify on the hardware wallet screen what a page may have changed.
SDR-009	Verify All Links Before Logging In	Bookmarks protect you from redirects and fake login pages.
TSR-004	Use Hardware-Based Two-Factor Authentication	A password stolen on a network is useless without the physical key.

Table 5.1: CSF rules for network risks

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

5.5 If This Just Happened to You

For the full first-hour checklist, see **Chapter 9**.

If you…	Do this now
entered a password or code on a Wi-Fi login page or a page you reached through a public network	From a trusted connection: change that password, end active sessions and check 2FA settings. Start with your email.
installed something a network page asked for	Treat the device as infected: see **Chapter 2**.
typed your seed phrase anywhere online	Treat it as burned: create a new wallet on a clean device and move all funds now.

Table 5.2: First steps after a network-related exposure

AFTER A LOSS

Expect offers to trace or recover the stolen crypto. Nobody can reverse a confirmed transfer for a fee. See **Recovery Scams** and report the theft: **How to Report a Crypto Scam**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/network-based-attacks/

CHAPTER 6

Platform Breaches and Insider Attacks

“The exchange was hacked. Why am I getting calls?”

Figure 6.1: Platform Breaches and Insider Attacks at a glance

Sometimes the weak point is not you but a company you trust: an exchange, a wallet provider, a shop that sold you a device or a service that holds your data. When a platform is breached, two things can be lost – the funds it holds for you, and the personal data it holds about you. The second is often used against you for months afterwards.

You cannot prevent a breach at someone else’s company. You can limit what any one platform holds, and you can recognise the follow-up attacks that come after.

IN THIS CHAPTER

- 6.1 Two Kinds of Platform Breach
- 6.2 Insider Attacks
- 6.3 How to Limit Your Exposure
- 6.4 Illustrative Scenario: The Breach Notice
- 6.5 CSF Rules for This Chapter
- 6.6 If This Just Happened to You

6.1 Two Kinds of Platform Breach

What is breached	What you can lose	What follows
Funds held by the platform (exchange, **custodial wallet**, lending service)	Your balance on that platform, fully or partly	Withdrawal freezes, long recovery processes, fake “compensation” offers
Customer data (names, addresses, phone numbers, balances, order history)	Your privacy – your funds stay where they are	Targeted phishing, fake support calls, fake device mailings, threats and physical targeting

Table 6.1: Fund breaches and data breaches

Real cases show both. In February 2025, an attack on a large exchange took one of the largest amounts ever stolen from an exchange, after attackers compromised the interface of the wallet service it used; customer balances were covered by the exchange. In May 2025, another large exchange disclosed that bribed support contractors had taken customer data, which was then used to impersonate the exchange and persuade customers to send funds.

6.2 Insider Attacks

Insiders are people with legitimate access: platform staff and contractors, but also people around you – a technician, a relative or a housemate who knows where your backup is. Insider cases are rare, and most people around you are trustworthy. The point is not suspicion, but design: set things up so that no single person can take everything.

- At platforms: assume support staff can see your data. Real support never asks for your seed phrase, your password or a transfer “to secure your funds”.
- At home: keep seed phrase backups where only the people in your recovery plan can reach them, and do not leave a hardware wallet with its backup next to it.
- For larger amounts: use multisig, so that one person with one key cannot move funds (Chapter 8).

6.3 How to Limit Your Exposure

- **Keep only what you trade on any platform.** Savings belong in your own Vault wallet (The Three-Wallet Model).
- **Spread risk:** do not keep everything on one exchange or one service.
- **Give platforms as little data as possible,** and use your separate crypto email address (Chapter 4).
- **Expect follow-up attacks after any breach notice:** calls, emails, letters and parcels “from” the platform. Contact it only through its official app or website.
- **After a data leak that includes your address,** review your home security and privacy (Chapter 7).

6.4 Illustrative Scenario: The Breach Notice

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

A week after an exchange reports a data breach, Priya gets a call from its “fraud team”. The caller knows her name, address and balance, and says her account is at risk. To protect her funds, she must move them to a “secure wallet” the team will set up for her.

What Happened

The caller was a scammer using the leaked data. The breach had not touched Priya’s funds; the call was the attack.

Key Takeaways

- Leaked data makes fake calls convincing. Knowing your details proves nothing.
- No real exchange asks you to move funds to a wallet it gives you.

- Hang up and contact the platform through its official app.

6.5 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.

What is not on a platform cannot be lost in its breach.

Rule	Statement	Why it applies here
GR-005	Never Follow Urgent Support or Security Instructions. Exit the Channel and Re-Enter Through the Official App or URL	Fake support calls follow almost every data breach.
TSR-005	Enable Withdrawal Whitelists on Exchanges	Limits what an attacker can do with a taken-over account.
SDR-010	Never Pay Anyone to Recover Lost Crypto	Breach victims are targeted by fake recovery and compensation services.

Table 6.2: CSF rules for platform breaches

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

6.6 If This Just Happened to You

For the full first-hour checklist, see **Chapter 9**.

If…	Do this now
a platform you use reports a hack of funds	Follow only its official announcements. Do not send funds to any “recovery” or “compensation” address. Keep records of your balance and correspondence.
a platform reports a leak of your data	Change that platform’s password, check 2FA, and expect targeted contact. If your address leaked, review **Chapter 7**.
someone calls, writes or sends a parcel “from” the platform after a breach	Do not act on it. Contact the platform yourself through its official app or website.

Table 6.3: First steps after a platform breach

AFTER A LOSS

Expect offers to trace, recover or “compensate” lost crypto. Nobody can reverse a confirmed transfer for a fee. See **Recovery Scams** and report: **How to Report a Crypto Scam**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/crypto-exchange-hacked-what-to-do/

CHAPTER 7

Physical Coercion (Wrench Attacks)

“They found my address from an old screenshot.”

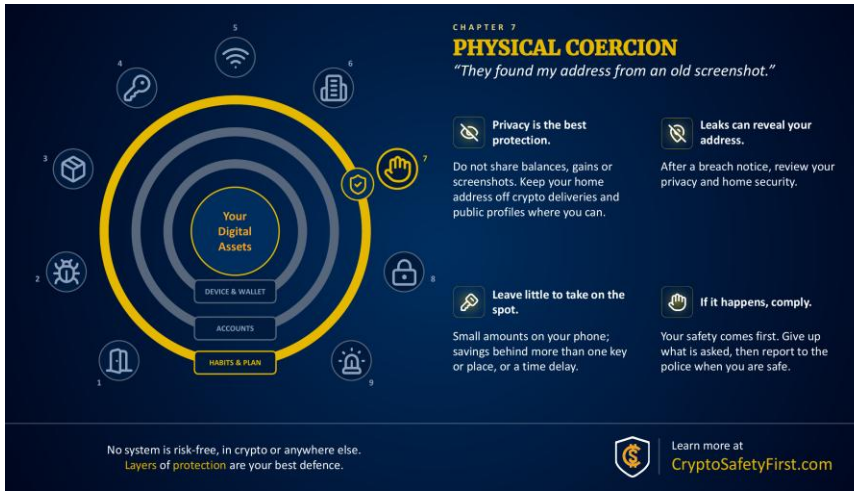

Figure 7.1: Physical Coercion (Wrench Attacks) at a glance

A “wrench attack” is the oldest attack there is: instead of breaking into a device, criminals force a person to unlock it. Robberies, home invasions and kidnappings aimed at crypto holders and their families have been reported in several countries, including a series of cases in France in 2025. They remain rare, but because crypto can be moved in minutes and cannot be reversed, holders are attractive targets.

This chapter is not about fighting back. Your safety and your family’s safety come first, always. It is about not becoming a target, and about setting up your crypto so that, even under pressure, there is little to take on the spot.

IN THIS CHAPTER

- 7.1 How People Become Targets
- 7.2 Privacy: The Best Protection
- 7.3 Setting Up Your Crypto So There Is Little to Take
- 7.4 If It Happens
- 7.5 CSF Rules for This Chapter
- 7.6 If This Just Happened to You

7.1 How People Become Targets

- **Talking about holdings in public:** posts, screenshots of balances or gains, talks at meetups, or a known role in a crypto company.
- **Leaked customer data:** breaches at exchanges, hardware wallet shops and other services have exposed names, phone numbers and home addresses (Chapter 6).
- **Visible signs at home:** hardware wallet boxes in the recycling, delivery labels, or a wallet visible in a video call.
- **Meeting strangers in person** to trade crypto or hardware.
- **People who know:** friends, relatives or contacts who know you hold crypto and may tell others, often without meaning harm.

7.2 Privacy: The Best Protection

- **Do not share balances, gains or screenshots,** online or offline. “I own a bit, like everyone” is enough.
- **Keep your home address off crypto-related accounts and deliveries where you can:** for example a post-office box or a work address for hardware wallet orders.
- **Separate your public identity from your holdings:** a pseudonym for crypto social media, and no wallet addresses linked to your real name.
- **Remove old posts and profiles** that link you to crypto, and ask data broker sites to delete your listing where your country allows it.
- **Talk to your family** about not mentioning crypto to others, and about what to do if someone asks.

7.3 Setting Up Your Crypto So There Is Little to Take

The aim is that nothing you can be forced to do on the spot moves your savings.

- **Keep only small amounts in wallets you can open with a phone or a single device,** and nothing large on an exchange app you can unlock with your face or fingerprint.
- **Put savings behind more than one key:** with multisig, the keys are stored in different places, so funds cannot be moved from one location or by one person (**Chapter 8** and **The Three-Wallet Model**).
- **Add delay:** some setups and services allow time-locks or withdrawal delays, so a large transfer cannot happen immediately.
- **A decoy wallet:** a hardware wallet passphrase can open a second, separate wallet. A small balance behind the main wallet and savings behind a passphrase is one option some holders use to have less at risk. A decoy is a way to have less at risk, never something to defend.

7.4 If It Happens

Comply. Your life and your family are worth more than any amount of crypto. Do not resist, do not bargain, do not try to trick the attackers. If you are asked about a hidden wallet or passphrase, give it up. If your setup means you cannot move funds on the spot, say so calmly and truthfully.

- When you are safe, call the police, and tell them crypto was involved.
- Record the time, what was taken and any transaction details you can see later on a block explorer.
- Move any remaining funds to new wallets with new seed phrases, because the attackers may have seen your backups or devices.
- Expect follow-up contact, including fake recovery offers. Use the reporting steps in **Chapter 9**.

7.5 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.

Savings in a Vault wallet away from your phone – ideally behind more than one key or a delay – are much harder to take on the spot.

Rule	Statement	Why it applies here
GR-003	Always Use a Hardware Wallet for Long-Term or High-Value Crypto Storage	Keeps savings off the phone in your pocket.
OR-007	Plan Wallet Recovery for Emergencies and Inheritance	Your family needs a plan that does not depend on you being free to act.
SDR-001	Never Trust Unsolicited Crypto Contact	Targets are often researched through contact that seems harmless.

Table 7.1: CSF rules for physical safety

There is no CSF rule specific to physical coercion yet; it is a candidate for the next version of the rules. All 32 rules: **CSF Crypto Security Rules**.

7.6 If This Just Happened to You

Get to safety and call the police first. Then follow the steps in “If It Happens” above and the first-hour checklist in **Chapter 9**, from a device the attackers did not have.

AFTER A LOSS

Expect offers to trace or recover the stolen crypto. Nobody can reverse a confirmed transfer for a fee. See **Recovery Scams** and report: **How to Report a Crypto Scam**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/crypto-wrench-attacks/

CHAPTER 8

Advanced Protection

“One device failing should never be enough.”

Figure 8.1: Advanced Protection at a glance

The habits in Chapters 2 to 7 protect most people well. This chapter is for larger holdings, or for anyone who wants their savings to survive even a compromised device, a tampered wallet or a stolen backup. Every option here adds steps – and every extra step is something you, and anyone who inherits your crypto, must understand. Choose what you will actually maintain.

IN THIS CHAPTER

- 8.1 A Dedicated Device for Crypto
- 8.2 Multisig: More Than One Key
- 8.3 Other Options Compared
- 8.4 Signing Habits That Matter at Any Level
- 8.5 CSF Rules for This Chapter

8.1 A Dedicated Device for Crypto

The simplest advanced step is a computer or phone used only for crypto: no email, no games, no browsing, no test code, only the official apps of

your wallets and exchanges. Malware usually arrives through everyday use, so a device without everyday use has far less exposure.

A live Linux system started from a USB stick – downloaded from the official site and checked against its published signature – is a cheaper alternative for occasional use. It helps against malware on your normal system. It does not help against compromised hardware or firmware, and it does not make it safe to type a seed phrase: **never type a seed phrase into any computer, even a clean one.**

8.2 Multisig: More Than One Key

A **multisig** wallet needs several keys to move funds – for example 2 of 3. Each key is on its own hardware wallet, ideally from different manufacturers, and stored in different places.

- **What it protects against:** one compromised or tampered device, one stolen backup, or one person forced or tempted to act alone.
- **Why 2 of 3 and not 2 of 2:** with 2 of 2, losing one key locks the funds for good. With 2 of 3, you can lose one key and still recover.
- **What it costs:** every key needs its own backup, and you must also back up the wallet configuration (often called the descriptor), which records how the keys work together. Without it, two seed phrases alone are usually not enough to recover the funds. Keep a copy of the configuration with each key backup: it cannot move funds, but it reveals your balances, so store it privately. The risk moves from hackers to your own record-keeping.

For how multisig fits your Vault wallet, see **The Three-Wallet Model**. For backups, see **Chapter 2 of the User Mistakes Prevention Guidebook**.

8.3 Other Options Compared

Option	What it adds	Trade-off
Passphrase on a hardware wallet	A second secret: the seed phrase alone does not open the passphrase wallet	Forget it and the funds are lost; it must be backed up separately
Air-gapped signing device	Never connects to a computer; transactions move by QR code or memory card	Slower to use; still needs a trusted source and careful setup
Multisig across vendors	No single device, place or person can move funds	More backups, more steps, harder inheritance
MPC wallet	Key shares are held in several places, often including a provider; no full key exists	You depend on the provider's security and continued service where it holds a share
Smart-contract wallet	Spending limits, delays and recovery contacts	Relies on contract code; setup and recovery differ by network

Table 8.1: Advanced options and their trade-offs

8.4 Signing Habits That Matter at Any Level

- **Verify on the device screen:** the full address and amount, not just the first and last characters.
- **Avoid blind signing** for anything that touches your savings: if the device cannot show what you approve, do not approve it.
- **Revoke approvals you no longer need** on wallets that still hold funds.
- **Test the recovery** of any advanced setup before you rely on it, and again after any change.

8.5 CSF Rules for This Chapter

MAIN RULE · TSR-006

Separate Devices and Accounts for Crypto Use.

One infected device or breached account should never expose all your crypto at once.

Rule	Statement	Why it applies here
TSR-004	Use Hardware-Based Two-Factor Authentication	Protects the accounts around your advanced setup.
TSR-005	Enable Withdrawal Whitelists on Exchanges	New withdrawal addresses are delayed, giving you time to act.
GR-003	Always Use a Hardware Wallet for Long-Term or High-Value Crypto Storage	The base of every advanced setup.
GR-004	Always Revoke Unused Token Approvals After Interacting with New Smart Contracts	Old approvals bypass any wallet hardening.
OR-001	Test Your Wallet Recovery Before Trusting It	A complex setup you cannot restore protects nobody.
OR-003	Document How Your Wallet Was Created	Multisig and passphrases are useless without a clear record.

Table 8.2: CSF rules for advanced protection

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

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/advanced-security-practices-cryptocurrency/

CHAPTER 9

If You've Been Hacked

"I kept watching the explorer instead of acting."

Figure 9.1: If You've Been Hacked at a glance

Finding a wallet or account emptied is a shock, and the first reaction is to find out how it happened. That can wait. In the first hour, what matters is stopping further losses: anything an attacker could reach once, they can usually reach again.

This chapter gives the first-hour checklist, a way to find the likely cause, and what to do in the days after – including how to avoid the recovery scams that follow almost every loss.

IN THIS CHAPTER

- 9.1 The First Hour
- 9.2 Find the Likely Cause
- 9.3 Report It
- 9.4 Rebuild Safely
- 9.5 CSF Rules for This Chapter

9.1 The First Hour

Do the steps that apply, in this order, from a device you trust – ideally one that was never used with the affected wallet or accounts. If an exchange account is being emptied right now, contact its official support to freeze it at the same time as step 1.

1. Move what is left. Create a new wallet with a new seed phrase – on a new hardware wallet, or temporarily on a clean device – and move remaining funds from every wallet that shares the affected seed phrase or device. Include tokens and NFTs that can still be moved. If the seed phrase or key is compromised, do not send new coins into the wallet to pay fees: automated “sweeper” bots usually take them within seconds. Move only what the balance already there allows, and treat the rest as lost unless the wallet’s or token’s official support describes a safe method.

2. Secure your email. Change its password, end all sessions, remove unknown forwarding rules and recovery options, and turn on a hardware key or passkey.

3. Lock your exchanges. End sessions, change passwords, delete unknown API keys, check withdrawal whitelists, and contact official support to freeze withdrawals if needed.

4. Call your mobile provider if you lost mobile service or received unexpected SIM or number messages.

5. Revoke token approvals on wallets whose keys are not compromised and that still hold funds, using a trusted approval checker (see **Safety Tools**) opened from your bookmarks.

6. Stop using the affected device for crypto until it has been wiped and reinstalled – after the funds are safe.

Do not send funds to the attacker’s address, reply to them, or pay anyone who offers to get the funds back.

9.2 Find the Likely Cause

Knowing how it happened tells you what else is exposed. Look at the transactions on a block explorer and at your account activity.

What you see	Likely cause	What else is exposed
Funds left your wallet without any signature from you	Seed phrase or **private key** exposed: malware, a digital copy, a tampered device or someone who saw it	Every wallet created from the same seed phrase; any other secret on the same device
Tokens left through a contract after you connected to a site	A token approval or signature you gave (a scam – see the **Scams guide**)	Other approvals on the same wallet
Exchange withdrawal you did not make	Account takeover: password, email, SIM swap or stolen session	Your email and every account that resets through it
A transfer went to an address you did not choose	Clipboard swapper or a manipulated app or page	The device you used
Everything happened right after setting up a new device	Tampered or pre-set device	Anything set up on that device

Table 9.1: Signs and likely causes

Sometimes the cause cannot be found. Treat everything that touched the wallet – devices, backups and accounts – as exposed, and rebuild from scratch.

9.3 Report It

- Report the theft to your local police or national cybercrime reporting service. Country links: **How to Report a Crypto Scam**.
- Report to the exchanges involved, including the exchange that may receive the stolen funds, with transaction hashes and times.
- If stablecoins were stolen, report the transaction hashes quickly to the stablecoin issuer through its official website; issuers can sometimes freeze them.
- Keep a record: transaction hashes, addresses, screenshots of messages and account activity, dates and times.
- If a wallet app, extension or device was involved, report it to the developer or manufacturer through its official website.

Reports rarely bring funds back quickly, but they help investigators connect cases, and some funds are frozen when they reach regulated exchanges.

9.4 Rebuild Safely

- Wipe and reinstall affected devices, or replace them.
- New wallets with new seed phrases, written on paper or metal, backed up in two places.
- A separate email for crypto with a hardware key; no SMS recovery.
- Review the Three-Wallet Model, so the next problem cannot reach your savings.

9.5 CSF Rules for This Chapter

MAIN RULE · TSR-002

Assume Your Device Can Be Compromised.

After a hack, act from a clean device and treat every secret on the old one as exposed.

Rule	Statement	Why it applies here
SDR-010	Never Pay Anyone to Recover Lost Crypto	Unsolicited recovery offers are scams; nobody can reverse a confirmed transfer for a fee.
GR-004	Always Revoke Unused Token Approvals After Interacting with New Smart Contracts	Old approvals can keep draining a wallet after the first loss.
SDR-001	Never Trust Unsolicited Crypto Contact	Fake helpers contact victims within hours of a loss.

Table 9.2: CSF rules after a hack

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

AFTER A LOSS

Expect offers to trace or recover the stolen crypto – in comments, messages and even fake “law firm” letters. Nobody can reverse a confirmed transfer for a fee. See **Recovery Scams**.

CONTINUE ON CRYPTOSAFETYFIRST.COM

Read the full chapter post for this topic:

cryptosafetyfirst.com/crypto-wallet-drained-what-to-do/

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-003	Always Use a Hardware Wallet for Long-Term or High-Value Crypto Storage	2, 3, 7, 8
GR-004	Always Revoke Unused Token Approvals After Interacting with New Smart Contracts	8, 9
GR-005	Never Follow Urgent Support or Security Instructions. Exit the Channel and Re-Enter Through the Official App or URL	1, 6
GR-007	Never Store Your Seed Phrase in Cloud Storage, Email, or Screenshots	2, 4
GR-008	Keep Long-Term Holdings in a Vault wallet. Use a Separate Wallet for DApps, Trading, and Web3	1, 3, 6, 7
OR-001	Test Your Wallet Recovery Before Trusting It	8
OR-003	Document How Your Wallet Was Created	8
OR-006	Maintain Access to Your Authentication Systems	4
OR-007	Plan Wallet Recovery for Emergencies and Inheritance	7
SDR-001	Never Trust Unsolicited Crypto Contact	1, 7, 9
SDR-009	Verify All Links Before Logging In	1, 4, 5
SDR-010	Never Pay Anyone to Recover Lost Crypto	6, 9
TSR-001	Never Install Crypto Software from Unofficial Sources	2, 3
TSR-002	Assume Your Device Can Be Compromised	2, 3, 5, 9
TSR-003	Avoid Public Wi-Fi for Crypto Operations	5
TSR-004	Use Hardware-Based Two-Factor Authentication	4, 5, 8
TSR-005	Enable Withdrawal Whitelists on Exchanges	4, 6, 8
TSR-006	Separate Devices and Accounts for Crypto Use	2, 4, 8
TSR-007	Slow Down Before Clicking or Installing	1, 2

CSF rules used in this book

Keep Learning

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

- **A page for every chapter**, kept up to date.
- The **Scams** and **User Mistakes** guides, for the losses that start with a scam or a mistake.
- **The Three-Wallet Model**: a free guide and toolkit that keeps one compromised wallet or device from reaching your savings.
- **Practical safety tools**: what each one prevents and what it cannot do.

cryptosafetyfirst.com