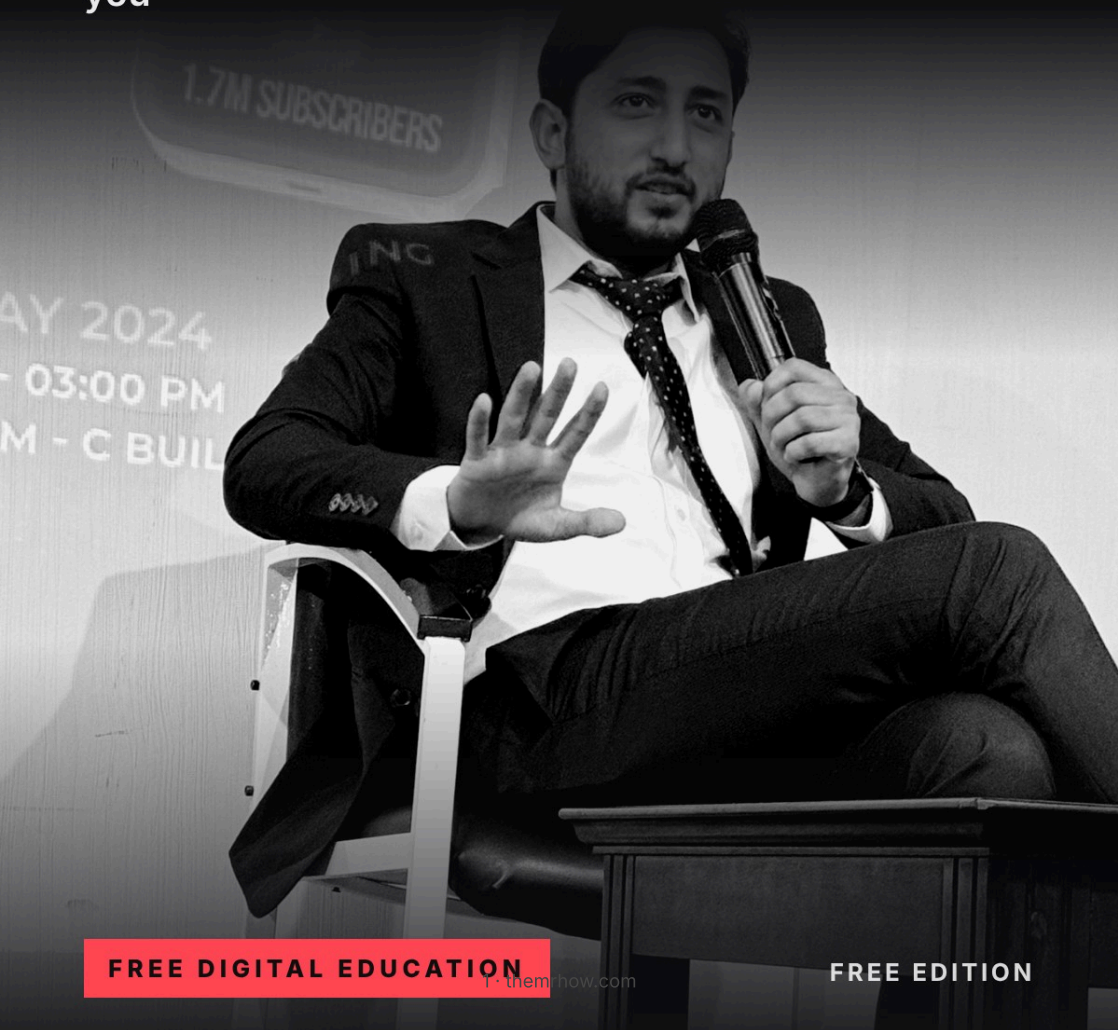
Never Get Scammed

Spot every online trap before it catches you



FREE DIGITAL EDUCATION

1 · themrhow.com

FREE EDITION

Never Get Scammed

Spot every online trap before it catches you

By Mr How

Contents

Why this book exists

Chapter 1. How scammers think

Chapter 2. The golden rules

Chapter 3. Fake earning apps and websites

Chapter 4. Binary trading and "investment" schemes

Chapter 5. Crypto scams

Chapter 6. Phone, SMS and WhatsApp scams

Chapter 7. Job, course and freelancing scams

Chapter 8. Shopping and social media scams

Chapter 9. When scammers use Mr How's name

Chapter 10. Protect your accounts like an engineer

Chapter 11. If you have been scammed

Chapter 12. Case files: ten scams, dissected

Chapter 13. Teaching your family

The 10-second checklist

Little dictionary

A message from Mr How

Why this book exists

In 2025, YouTube terminated my channel. It had 2.1 million subscribers and five years of free lessons. It was taken down after a wave of complaints that followed my videos exposing more than fifty scams, led by the binary trading app Binomo, and the people who promoted them to young Pakistanis.

A few months later, in August 2025, Pakistan's National Cyber Crime Investigation Agency declared Binomo and 45 other apps illegal and asked PTA to block them. I had been right. But being right did not return the money that thousands of students, shopkeepers and housewives had already lost.

That is why this book exists. Scams are not a problem of "stupid people". I have met engineers, bankers and teachers who lost lakhs. Scams work because they are designed by professionals who study human psychology the way a doctor studies the body. To beat a professional, you need to understand the design.

This book takes you inside that design. You will learn how scammers think, the patterns behind every major scam in

Pakistan today, how to protect your accounts like a security engineer, and exactly what to do if the worst happens. Read it, and then teach it to the people you love, especially the ones who are new to smartphones.

The stories in this book are examples built from real patterns. Names and details are changed. Laws and agency names are current as of November 2026.

Chapter 1. How scammers think

A scam is a product. It has a target customer, a marketing funnel, a sales script and a "conversion rate". The people who run large scams often work in organised teams with managers, scripts and targets, just like a call centre. Understanding this changes how you see every suspicious message. It is not a random person trying their luck. It is a system designed to move you from curiosity to payment.

The six levers

Almost every scam pulls on one or more of six psychological levers. Learn their names. When you can name the lever, its power over you drops.

1. **Greed.** "Earn Rs 3,000 a day from home." The promise is bigger than what honest work would give. The bigger the promise, the louder the alarm should ring.
2. **Fear.** "Your bank account will be blocked in 2 hours." "Your son has been arrested." Fear switches off careful thinking and switches on panic.

3. **Urgency.** "Offer ends tonight." "Only 3 seats left." Urgency stops you from asking anyone else for advice. Real opportunities can wait one day.
4. **Authority.** The message claims to be from the bank, PTA, FIA, NCCIA, a famous creator or a government programme. People obey authority without checking it.
5. **Social proof.** Screenshots of other people's "profits", WhatsApp groups full of happy members, fake reviews. If everyone else is doing it, it feels safe. Many of those "members" are the scammers themselves.
6. **Reciprocity and trust.** The scammer gives you something first: a small payout, a gift, helpful advice, weeks of friendly chat. Then they ask for something much bigger.

The funnel

Most modern scams follow the same five steps:

Stage	What the scammer does	What you feel
1. Hook	An ad, a message, a reel, a "wrong number"	Curiosity
2. Trust	Friendly chat, small free task, a small real payout	"Maybe this is real"
3. Commitment	A small deposit, an upgrade, a "test" investment	"It's only a little"
4. Escalation	Bigger deposits to "unlock" earnings, fees to withdraw	"I can't lose what I've put in"
5. Exit	The app disappears, the number blocks you	Shock and shame

Notice stage 4. Once you have put money in, a powerful bias called the **sunk cost fallacy** keeps you putting more in, because stopping means accepting the loss. Scammers know this. The most important skill in this book is the ability to stop at stage 2 or 3, before the escalation.

Why smart people fall

Scams do not target intelligence. They target situations: a person who needs money urgently, a person who is lonely, a person who is new to technology, a person who is tired at midnight. Everyone is in one of these situations sometimes. That is why the best defence is not "being smart" but having

fixed rules that you follow even when you are tired, scared or excited.

Exercise

Think of the last suspicious message you received. Which of the six levers did it pull? Write them down. Do this for every suspicious message for one week, and you will start seeing the levers instantly.

Chapter 2. The golden rules

Rules beat intelligence because rules work even when your brain is under pressure. Here are ten rules. Learn them until they are automatic.

1. **Money flows to you in real work.** If you must pay first to earn, it is a trap.
2. **No one can promise fixed profit.** Fixed daily or monthly returns are the signature of a Ponzi scheme.
3. **Never share codes.** OTPs, verification codes, PINs, passwords and seed phrases are never needed by a real bank, platform, employer or creator.
4. **Hang up and call back.** If someone calls claiming to be your bank or an agency, end the call and call the official number yourself.
5. **Type the address yourself.** Never log in through a link in a message. Open the app or type the website address.
6. **Slow down urgency.** Any message that says "right now" gets a 24-hour wait and a second opinion.

7. **Verify the person, not the profile.** Profile photos, names and blue ticks can be faked. Verify through a different channel.
8. **Screenshots prove nothing.** Profit screenshots and payment proofs are trivially easy to fake.
9. **Small wins are bait.** A first payout does not prove an app is real. It proves the scammer can afford bait.
0. **Talk to someone.** Scammers want secrecy. Telling a friend or family member breaks the spell.

> **If you remember only one thing**
>
> Scammers can fake everything except your patience. Time and a second opinion defeat almost every scam.

Chapter 3. Fake earning apps and websites

This is the scam I have exposed most, because it targets the people with the least: students, the unemployed and families looking for a little extra income. The apps change names every few months, but the machinery is always the same.

The common types

- **Watch-ads and click apps.** You are paid tiny amounts to watch ads or click links. Then you are told to buy a "level" or "VIP package" to earn more. The higher-level earnings are paid from the deposits of new users.
- **Task and order-grabbing scams.** You "complete orders" or "boost products" in an app, and earn commission. Soon an order needs you to top up your balance. Each new task needs a bigger top-up, and you can never withdraw.
- **Like-and-subscribe tasks.** Often starting on WhatsApp or Telegram: you are paid Rs 100 to like videos. After a few

genuine small payments, you are moved into a "premium" group that requires deposits.

- **Investment "plans" with daily profit.** Deposit Rs 5,000, get Rs 300 daily. Early users are paid from later users' money until the inflow slows and the site vanishes.
- **Multi-level referral schemes.** Your earnings depend mainly on recruiting others who also pay to join. When recruitment slows, the bottom layers lose everything.

Why the first payment arrives

Victims often say: "But it paid me! I withdrew Rs 800!" That is the bait from Chapter 1. Paying a few hundred rupees to thousands of people is a marketing cost. It creates screenshots, trust and word-of-mouth. The real business is the deposit you make after you trust it.

A quick maths lesson: the Ponzi curve

Suppose an app promises 3% daily on deposits. To pay that, it needs new money equal to 3% of all existing deposits every single day. That is roughly doubling the money inside every 24 days. No real business grows like that. When new deposits slow even slightly, the app cannot pay, so it invents "withdrawal fees", "tax clearance", "system upgrades", and then disappears. The collapse is not bad luck. It is built into the maths.

Red flags checklist

☐ Income that is high compared with the work involved

☐ Any deposit, recharge, level or upgrade

☐ Earnings visible as a balance in the app but hard to withdraw

☐ Pressure to bring friends and family

☐ App available only as a downloaded file, not from the official app store

☐ Customer support only on WhatsApp or Telegram

☐ No real company name, address or registration you can verify

> **Story**
>
> Sana, a teacher in Faisalabad, joined an "online shopping task" app on a friend's recommendation. For two weeks she earned Rs 200 to Rs 400 a day and withdrew it easily. Then a "lucky combo order" appeared, worth Rs 18,000, which needed her to top up her account first. She paid. Then another combo, Rs 45,000. She borrowed. When she tried to withdraw, she was told to pay 20% "tax". The app vanished a week later. Her friend had lost money too; she had been paid a small referral bonus for inviting Sana. Both were victims.

Chapter 4. Binary trading and "investment" schemes

Binary options apps were among the most damaging scams in Pakistan, and they are still promoted under new names. This chapter explains exactly how they work, so that no marketing video can fool you again.

What binary options are

In a binary option, you predict whether a price will go up or down within a short time, often 60 seconds. If you are right, you win a fixed percentage, perhaps 80% of your stake. If you are wrong, you lose your whole stake. That is the entire product.

Look at the payout carefully. Win: +80%. Lose: -100%. Even if you guessed right exactly half the time, you would lose money steadily. To break even, you must be right about 56% of the time on what is essentially a coin flip over 60 seconds. The house always has the edge. This is not trading. It is a casino with charts.

Why it looks like trading

The apps show professional-looking charts, indicators and "signals". Promoters show screenshots of big wins and luxury lifestyles. Some apps let you practise on a demo account where winning feels easy. Then real money behaves differently. In many unregulated apps, the platform itself is the other side of your trade, which means your loss is literally their profit.

The legal position

In August 2025, NCCIA declared 46 betting, forex and binary trading apps illegal, including Binomo, Quotex, Pocket Option, IQ Option, Deriv, Olymp Trade and OctaFX, and asked PTA to block them. Using a VPN to reach a blocked app does not make it legal or safe. If your money is stuck inside one of these apps, there is usually no Pakistani regulator who can help you recover it.

"Signal groups" and "account managers"

A common variation: a Telegram or WhatsApp group shares "VIP signals" for a monthly fee, or an "account manager" offers to trade for you and share the profits. Some show fake profit screenshots; others really do trade your money in the same losing products. Either way, the person selling signals earns from your subscription, not from trading.

Other investment traps

- **Fixed-return "business partnerships"** where you invest in a shop, a car rental or a property scheme with guaranteed monthly profit and no paperwork.
- **Forex "fund management"** by individuals promising 10% to 30% monthly.
- **Gold or commodity schemes** sold through WhatsApp with no licensed company behind them.

> **The test**
>
> Ask: "Who regulates you, and where can I verify your licence?" Then verify it yourself on the regulator's own website, not through a link they send. In Pakistan, securities and investment companies fall under the SECP, and crypto service providers fall under PVARA. If there is no licence you can verify, walk away.

Chapter 5. Crypto scams

Crypto is a real technology, explained in Book 4 of this series. But because transactions are fast, global and hard to reverse, it is a favourite tool for scammers. Most crypto scams do not attack the blockchain. They attack the person holding the keys.

Fake exchanges and fake apps

A website or app looks like a real exchange, shows your balance growing, and lets you deposit easily. Withdrawals fail or need "fees". Always download exchange apps from the official app store, check the developer name, and remember: as of November 2026, no crypto platform holds a full PVARA licence in Pakistan. Any app claiming to be "PVARA licensed" is lying. You can check any platform with the free checker on themrhow.com.

"Pig butchering" (relationship investment scams)

It starts with a "wrong number" message or a friendly stranger on social media. Weeks of warm conversation follow. Then the new friend mentions they make money on a special crypto

platform, and offers to teach you. Your first small investment shows great profits. You invest more. When you try to withdraw a large amount, you are asked for taxes and fees, and then the friend disappears. The name comes from the idea of "fattening the pig before the slaughter". The friendliness is the weapon.

P2P fraud

- **Fake payment proof.** A buyer sends an edited screenshot of a bank transfer and asks you to release crypto. Always check your actual bank account, not a screenshot.
- **Third-party payments.** Money arrives from a name different from the buyer's account. That money may be stolen, and your bank account can be frozen during an investigation.
- **Chargeback and reversal tricks.** Payments made by methods that can be reversed after you release the crypto.

Seed phrase and wallet attacks

Your seed phrase (12 or 24 words) is the master key to a self-custody wallet. Anyone who has it owns your crypto. Scammers ask for it as "wallet validation", "sync", "airdrop claim" or "support verification". No real support team will ever ask for it.

"Wallet drainers" are fake websites that ask you to connect your wallet and sign a transaction to claim a free token. The

signature gives the website permission to empty your wallet. Never sign transactions on websites you reached through ads, DMs or comments.

Rug pulls and pump-and-dumps

A new token is promoted heavily, often by paid influencers, its price rises as people buy, and then the creators sell everything at once, crashing the price to almost zero. If a token's main selling point is "it will go 100x", treat it as a trap.

Fake giveaways and fake support

"Send 0.1 ETH and get 0.2 back" is always a scam, even if it appears to come from a famous person. Fake "support agents" reply to your public complaints on X or in Telegram groups and guide you to fake help pages. Contact support only through the official app.

> **The three crypto commandments**
> Never share your seed phrase. Never sign what you do not understand. Never send crypto to "double" it.

Chapter 6. Phone, SMS and WhatsApp scams

Your phone number is connected to your bank, your mobile wallet and your WhatsApp. That makes it one of the most valuable things a scammer can attack.

Fake government and prize messages

SMS and WhatsApp messages claim you have won a prize, a lucky draw, or money from a government support programme such as BISP. They ask you to call a number, share your CNIC details, or pay a small "processing fee" to receive a large amount. Real government programmes do not ask beneficiaries to pay fees to strangers. Check official programme information only through their official channels.

"Your account will be blocked"

A caller claims to be from your bank, JazzCash, Easypaisa or PTA. They say your account or SIM will be blocked unless you "verify" right now. They already know your name and some details, which makes them sound real. Then they ask for the

code that just arrived on your phone. That code is the key to your account. Hang up.

WhatsApp account hijacking

You receive a six-digit WhatsApp code you did not request, followed by a message from a friend's number: "Sorry, I sent my code to you by mistake, please send it back." Your friend's account is already hacked, and now they want yours. Sending the code hands over your WhatsApp. Turn on **two-step verification** in WhatsApp settings today; it adds a PIN that stops this attack.

The family emergency

"Your son has been in an accident and needs money for the hospital." "Your nephew was arrested; pay now to avoid an FIR." Sometimes the caller even imitates a crying voice. With AI voice cloning, it may sound like the real person. Agree on a family code word that only your family knows, and always call the person directly on their known number before sending anything.

Delivery and courier scams

"Your parcel is held, pay Rs 150 to release it" with a link. The link steals your card or wallet details. Check delivery status only in the courier's official app or website.

Do this today

Turn on WhatsApp two-step verification. Hide your profile photo and "last seen" from people not in your contacts. Agree on a family code word. These three steps take ten minutes and block some of the most common attacks.

Chapter 7. Job, course and freelancing scams

People looking for work are under pressure, and pressure is what scammers love. These scams are especially cruel because they take money from people who have very little.

Overseas job scams

An "agent" offers a job in Dubai, Saudi Arabia or Europe, with a visa, high salary and free accommodation. You pay for "processing", "medical", "protector fee", "ticket" and "visa", often in parts. The job never appears. Before paying anyone, verify that the agency is licensed through the official Overseas Employment authorities, and never pay large fees in cash or to personal accounts.

Fake remote jobs

A "recruiter" contacts you on WhatsApp or LinkedIn with a well-paid remote job and a very quick interview by chat. You are hired immediately, then asked to buy a laptop, software or training from a specific vendor before you start, with a promise

of reimbursement. The vendor is the scammer. Real employers do not make you buy equipment from their chosen seller with your own money.

"Course plus guaranteed job"

A paid course promises guaranteed income or a job afterwards. Some teach a little; many teach nothing you could not learn free. The guarantee is the lie. No honest training provider can guarantee income, because income depends on the market and on you.

Account renting and selling

"Give us your verified Fiverr or Upwork account and we'll pay you monthly." "Open a bank account in your name and we'll use it, you get a commission." This is not passive income. Your identity becomes the face of whatever the renter does, which can include fraud and money laundering. When the account is banned or investigated, the name on it is yours.

Freelancer-targeted tricks

Overpayment refunds, fake escrow emails, giant "free tests" and off-platform payment pushes were covered in Book 1, *My First Dollar Online*. The defence is always the same: keep work and payment inside the platform, and never send money back to a "client".

Chapter 8. Shopping and social media scams

Fake online stores

An Instagram or Facebook page sells branded shoes, phones or clothes at unbelievable prices, with professional photos stolen from real stores. You must pay in advance; cash on delivery "is not available for this deal". After payment, you are blocked. Prefer cash on delivery for new sellers, check how old the page is, read comments from real-looking accounts, and be wary of prices that are far below the market.

Giveaway impersonation

A fake account copies a popular creator's name and photo and comments: "Congratulations, you won our giveaway! DM to claim." You are then asked to pay "delivery charges" or share card details. Real giveaways never require you to pay. Check the account's handle letter by letter.

Account takeover

Your Instagram or Facebook gets hacked, often through a fake "copyright violation" or "verification badge" message that leads to a fake login page. The hacker then uses your account to scam your friends. Turn on two-factor authentication and never log in through links in messages.

Sextortion and blackmail

A stranger builds an intimate chat or video call, records it, and then threatens to share it unless you pay. This is a serious crime. Do not pay, because payment leads to more demands. Stop responding, save evidence, report the accounts on the platform, and report to NCCIA. Talk to someone you trust. You are the victim, not the criminal.

Chapter 9. When scammers use Mr How's name

Because millions of Pakistanis trust my videos, scammers regularly create fake accounts using my name, photos and even edited videos. They offer "personal classes", "VIP groups", "account management" or "investment plans" in my name. Here is the truth, stated plainly:

- I never charge learners. No paid courses, no personal classes, no paid groups.
- I never take money to trade or invest for anyone.
- I never message learners first to offer earning opportunities.
- I do not have assistants or managers who contact learners about money.

My only official accounts are listed on themrhow.com, on the Scam Alert page, which also has a free tool to check any account, link or number. If anyone asks you for money in my name, it is a scam. Please report the account on the platform and warn the people around you.

Deepfakes and edited videos

AI can now create videos and voice clips that look and sound like real people. You may see a video of a famous creator, a news anchor or even a politician recommending an investment app. Treat any video that promotes an investment, a giveaway or a "secret platform" with deep suspicion, especially if it arrives as an ad or a forwarded message. Check the creator's official channels. If it is not there, it is not real.

Chapter 10. Protect your accounts like an engineer

Most people protect their accounts like a house with the key under the doormat. Security engineers think in layers: even if one layer fails, the next one holds. Here is a practical, layered setup that anyone can do in one evening.

Layer 1: Passwords

- Use a different password for every important account: email, bank, wallets, social media.
- Make passwords long rather than complicated: a phrase of four or five random words is stronger and easier to remember than "Ali@123".
- Use a trusted password manager so you do not have to remember them all.
- Your email password is the most important of all, because email is used to reset every other account.

Layer 2: Two-factor authentication (2FA)

Turn on 2FA everywhere it is offered, especially email, social media and exchanges. An authenticator app is safer than SMS codes, because SMS can be stolen through SIM swaps. Save your backup codes somewhere safe and offline.

Layer 3: Your SIM and phone

- Set a screen lock with a strong PIN, not a simple pattern that others can see over your shoulder.
- Install apps only from the official app store. Never install banking or wallet apps from links or APK files.
- Keep your phone and apps updated. Updates fix security holes.
- Be careful with apps that ask for permission to read your SMS or control your screen. Screen-sharing apps have been used to empty bank accounts during "support" calls.
- Check how many SIMs are registered on your CNIC through PTA's official service, and block any you do not recognise.

Layer 4: Your behaviour

- Never log in through a link in a message.
- Never share codes, ever.
- Use separate accounts or wallets for daily use and for savings.

- Be careful on public Wi-Fi; avoid logging into banking apps on networks you do not trust.

Layer 5: Your family

Your security is only as strong as the least protected person in your family WhatsApp group. Spend one evening setting up 2FA and two-step verification on your parents' phones, and teach them the golden rules. It may be the most valuable hour you spend this year.

Account	Minimum protection
Email	Unique long password, authenticator-app 2FA, recovery phone updated
WhatsApp	Two-step verification PIN, profile hidden from strangers
Banking and wallets	Official app only, strong PIN, never share OTP
Social media	2FA on, login alerts on, unknown sessions logged out
Crypto	2FA, withdrawal whitelist, seed phrase offline and never shared

Chapter 11. If you have been scammed

If it has happened to you, first: you are not stupid, and you are not alone. Scammers are professionals, and shame is part of their plan, because ashamed victims stay silent. Now act quickly, because the first hours matter most.

Step 1: Stop all payments

Do not send any more money, no matter what you are told: "release fee", "tax", "account unfreezing", "final step". Every new payment is lost too.

Step 2: Contact your bank or wallet immediately

Call your bank's or wallet provider's official helpline and report the fraudulent transaction. Ask them to block the receiving account if possible. Speed matters; banks can sometimes act before money is withdrawn.

Step 3: Save all evidence

Take screenshots of chats, profiles, website addresses, phone numbers, transaction IDs, dates and amounts. Do not delete the conversation, even if you feel embarrassed. Evidence is what makes a complaint actionable.

Step 4: Report to the authorities

Report cybercrime and online fraud to the National Cyber Crime Investigation Agency (NCCIA) through its official online complaint portal at nccia.gov.pk, or call its helpline, 1799. For SIM and calling scams, you can also complain to PTA through its official complaint portal. Include all your evidence.

Step 5: Secure your accounts

If you shared a password or code, change your passwords immediately, starting with email, and turn on 2FA. If you installed an app at the scammer's request, uninstall it, and consider resetting your phone.

Step 6: Warn others

Report the fake account or app on the platform where you found it, and warn your friends and family. Your story may stop the next victim.

Beware the recovery scam

After you lose money, you may be contacted by "recovery agents", "hackers" or even fake officials who promise to get your money back for an upfront fee. This is the second scam, aimed at people who were just scammed. Official complaint channels are free.

Chapter 12. Case files: ten scams, dissected

These case files are built from patterns reported repeatedly by Pakistanis. For each one, notice the levers from Chapter 1 and the stage of the funnel where the victim could have stopped.

Case 1: The "Daraz review" job

Hook: a WhatsApp message offers Rs 2,000 a day for reviewing products. **Trust:** the first three tasks are free and pay Rs 150 each. **Escalation:** "merchant tasks" require buying products with your own money for a refund plus commission. **Exit:** after a Rs 25,000 task, the group disappears. **Stop point:** the first request to pay. Rule 1.

Case 2: The crypto mentor

Hook: an attractive profile messages "by mistake" on Instagram. **Trust:** weeks of friendly chat, never asking for anything. **Commitment:** the friend shows profits on a "special exchange" and offers to teach. **Escalation:** growing deposits,

then "tax" to withdraw. **Stop point:** any investment platform suggested by an online stranger.

Case 3: The bank security call

Hook: a caller with your name and CNIC digits says your account is being misused. **Fear and authority:** "Your account will be blocked in 30 minutes." **Ask:** "Tell me the code we just sent to confirm it's you." **Exit:** the account is emptied. **Stop point:** any request for a code. Hang up and call the bank's official number.

Case 4: The overseas visa agent

Hook: a job in Saudi Arabia with a high salary, advertised on Facebook. **Commitment:** Rs 30,000 for "file processing". **Escalation:** medical, protector, ticket and visa fees. **Exit:** the office closes. **Stop point:** verifying the agency's licence through official overseas employment authorities before paying anything.

Case 5: The binary "teacher"

Hook: a reel shows a young man earning Rs 50,000 in ten minutes on a trading app. **Commitment:** a referral link and a small deposit. **Escalation:** "VIP signals" for a monthly fee. **Exit:** the account is wiped; the teacher earned referral commissions

on the losses. **Stop point:** recognising binary options as gambling, and the NCCIA ban.

Case 6: The WhatsApp code

Hook: a message from a cousin's real number: "Sent you my code by mistake, please send it back." **Exit:** your WhatsApp is taken over and used to ask your contacts for money. **Stop point:** never sharing codes, and turning on two-step verification.

Case 7: The Instagram iPhone

Hook: a page sells the latest iPhone at 40% below market price. **Social proof:** thousands of followers and "customer reviews". **Ask:** full advance payment, no cash on delivery. **Exit:** blocked. **Stop point:** a price that is too good, and refusal of cash on delivery.

Case 8: The fake creator giveaway

Hook: a comment from an account copying a famous creator's name: "You won!" **Ask:** "Pay Rs 1,500 delivery charges." **Stop point:** real giveaways never charge winners, and the handle was different by one letter.

Case 9: The recovery agent

Hook: after posting about losing money, a "cyber expert" offers to recover it for a 20% advance fee. **Exit:** a second loss. **Stop point:** official complaint channels are free; anyone charging upfront to recover money is a scammer.

Case 10: The "Mr How VIP group"

Hook: a Telegram group using my name and photos offers personal mentorship and signals. **Ask:** a membership fee or an investment. **Stop point:** I never charge learners. Check the official accounts list on themrhow.com.

Chapter 13. Teaching your family

Your parents, grandparents and younger siblings may be more at risk than you. Older family members are often new to smartphones and trust official-sounding calls. Younger ones are targeted with games, giveaways and "easy earning". Here is how to protect them without lectures that they will ignore.

Five rules for the family WhatsApp group

1. Nobody in this family ever shares a code that arrives by SMS or WhatsApp.
2. If anyone calls about an emergency, we hang up and call the person directly.
3. We have a family code word for real emergencies.
4. Before sending money to anyone new, we ask one other family member.
5. No one pays to earn, and no one invests for fixed profit.

A one-evening setup

☐ Turn on WhatsApp two-step verification on every family phone

☐ Hide profile photos and "last seen" from unknown numbers

☐ Turn on screen locks and app store-only installs

☐ Save official bank and wallet helpline numbers in each phone

☐ Show them three real scam messages and explain the levers

Make it safe to admit mistakes

The biggest danger is shame. If a family member fears being scolded, they will hide a scam until it is too late. Tell them clearly: "If you ever get tricked, tell me immediately. I will help, not shout." Speed saves money.

The 10-second checklist

Before you pay, click, install or share anything, ask:

☐ Am I being asked to pay to earn?

☐ Is someone promising a fixed or very high profit?

☐ Is someone asking for a code, PIN, password or seed phrase?

☐ Is there pressure to act right now?

☐ Did this reach me through a link, an ad or an unknown number?

☐ Can I verify the person or company through an official channel?

☐ Would I be comfortable telling my family about this payment?

If any answer worries you: stop, wait a day, and ask someone you trust.

Little dictionary

- **2FA:** two-factor authentication, a second step to log in besides your password.
- **Deepfake:** AI-generated video or audio that imitates a real person.
- **Phishing:** fake messages or websites that trick you into giving details.
- **Ponzi scheme:** a scheme that pays old investors with new investors' money.
- **Seed phrase:** the 12 or 24 words that control a self-custody crypto wallet.
- **SIM swap:** when a criminal moves your number to their SIM to receive your codes.
- **Sunk cost fallacy:** continuing to invest because you have already lost a lot.

A message from Mr How

Exposing scams cost me a 2.1 million subscriber channel. I would do it again. Every family that did not lose its savings because someone watched a video is worth more than any number of subscribers.

Now you know the patterns. Please do not keep them to yourself. Teach your parents, your younger siblings and your friends. Scams spread through WhatsApp groups; so can protection.

Stay alert. Mr How