

THE PRACTICAL FAMILY REFERENCE

THE SCAM DEFENSE HANDBOOK

64 DOCUMENTED SCAM PATTERNS



**Recognize the request. Check the story.
Protect your money. Help your family.**

EXPANDED FIRST EDITION / SEPTEMBER 2026

A REFERENCE FOR REAL LIFE

Keep your money. Keep your say.

Why this book exists

A suspicious call rarely arrives when you have a quiet hour to investigate it. It arrives while dinner is cooking, a bill is due, or someone you love sounds frightened. This handbook gives you a place to start: identify the request, check it outside the conversation, and choose the next useful action.

Who it is for

This U.S.-focused edition is written for adults, families, and people helping someone else sort out a troubling request. You do not need to be a technology expert. You do need permission to pause, ask questions, and bring another person into the conversation.

What documented means here

The 64 profiles describe patterns covered in official consumer alerts or enforcement-related reporting. Each profile links to its sources. The expanded situations are original illustrations, not verified accounts of named victims. The artwork is illustrative and AI-generated, not evidence of an incident.

A dated reference, not a guarantee

Scams overlap and change. This is a broad first edition, not a registry of every scam or case ever reported. Information was checked for this edition on September 18, 2026. Use the linked agencies for current procedures. This is general education, not individual legal, financial, or medical advice.

START HERE

Is something happening right now?

Someone may be in physical danger

Call 911 for an immediate emergency in the United States. A threatened abduction or a person at the door deserves appropriate emergency help. Do not travel to a place chosen by a suspicious caller or attempt to confront a courier.

You are still in the conversation

Stop giving information, stop installing software, and do not send another payment. Leave the call or chat. Use a separate, trusted route to reach the person, bank, company, or agency involved. If you cannot verify the claim, do not treat silence as confirmation.

Money has moved

Contact the bank, card issuer, payment app, wire service, or other provider you actually used. Explain exactly what happened and ask what can be stopped, recalled, disputed, or otherwise addressed. Act promptly. Available remedies depend on the facts, payment method, and timing; recovery is not guaranteed.

Someone has access to your device or account

If an unknown person has remote access, disconnect the affected device from the network. Use another trusted device to contact financial providers and secure accounts. Get help from a technician you independently choose. Preserve relevant messages and transaction information.

Then make a record

Write down the time, claimed identity, contact method, money or information shared, and the case numbers from your real providers. Report fraud through the appropriate official channels. Do not pay an unsolicited recovery specialist. See the payment guide and printable incident log.

SOURCES: FTC: What to do if you were scammed / FBI: Altered proof-of-life media in virtual kidnapping / FTC: Tech support scams / FTC: Refund and recovery scams

THE PAUSE PLAN

Four moves that give you room to think.

1 / Leave the pressure

An unexpected demand does not earn immediate access to your money. End the conversation long enough to check it. A request for secrecy is a reason to involve a trusted person, especially if the caller says your usual helpers are compromised.

2 / Find a separate route

Use the number on your card, a statement you already have, a saved contact, or an official website you reach independently. A callback number, transferred supervisor, link, or second participant supplied by the same caller is still part of the same information chain.

3 / Verify the underlying event

Ask the real person or organization about the specific claim: the accident, charge, account change, overdue bill, or payment instructions. Do not stop at confirming that a company exists. A real company can be impersonated, and a real invoice can contain false payment details.

4 / Choose the next action

If the claim checks out, use the genuine organization's normal process. If it does not, stop the transaction and report it as appropriate. If you cannot reach anyone, keep checking instead of treating the lack of an answer as proof of an emergency.

A phrase you can use

I do not make payments or share account information during an unexpected call. I will contact the organization myself. You do not need a clever argument or a confession from the caller to leave the conversation.

SOURCES: FTC: How to avoid a scam / FTC: Fake family emergencies / FBI: Business email compromise

01 Grandparent emergency

The caller wants your help before you can check.

WHAT THIS SCAM IS

Someone pretends that a loved one is in trouble and needs money immediately. The emergency supplies the fear; a second caller may supply the apparent authority. The goal is to collect your money before you verify the story.

AN ILLUSTRATIVE EXAMPLE - NOT A REPORTED CASE

A grandmother answers the phone. A young man calls her Grandma and says he has been in a car accident. Before she can find out much, he passes the call to a supposed attorney.

The attorney says her grandson needs money for release. He tells her to keep the matter quiet and says someone can collect cash from her home. She begins thinking about how to get the money, although she has not spoken to her grandson on his usual number.

In this example, the emergency is invented. The two callers support the same false story. A person arriving for the envelope would not prove that the grandson was arrested.

WHY IT CAN FEEL CONVINCING

The first caller draws on a real relationship. The second makes the request sound organized and official. Secrecy keeps another family member from questioning it, while urgency makes checking feel like a delay that could hurt someone you love. [1, 2]

Knowing a name or sounding familiar is not proof of identity. Personal details can be gathered elsewhere, and a voice can be imitated or cloned. You do not have to identify the technology: check the claimed emergency through a contact route you already trust. [1, 2]

The key question: Have I checked with my actual family, or only with people introduced by the caller?

See where the story leads.

One illustrated route through the scam - other versions vary.



BREAK THE CHAIN

End the call. Contact your family using a number you already know.

CHECK THE STORY

1. Call your relative yourself.
Use their saved number, not one the caller supplies.
2. If there is no answer, call another trusted relative.
An unanswered phone does not establish an emergency.
3. Resist the secrecy demand.
Check with family before sending money or arranging a pickup. [1, 2]

IF YOU ALREADY PAID

Contact the bank, payment service, or gift-card issuer immediately. Explain the fraud and ask whether the payment can be stopped or recovered. Recovery is not guaranteed.

If you mailed cash, contact the delivery service promptly. Save messages and payment records. Report the scam at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) and [IC3.gov](https://www.ic3.gov). [2, 3]

SOURCES / GUIDANCE CHECKED SEPTEMBER 18, 2026

1. [FTC: Fake family emergencies](#)
2. [FBI/IC3: Grandparent scams and couriers \(2023\)](#)
3. [FTC: What to do if you were scammed](#)

08 Bank safe-account scam

The supposed rescue is the transfer that causes the loss.

WHAT THIS SCAM IS

A fake fraud alert leads to instructions to move your savings into a supposedly safer account. The destination is controlled by the scammers. What is presented as protecting your money is actually the step that gives someone else control over it.

AN ILLUSTRATIVE EXAMPLE - NOT A REPORTED CASE

A text alerts a man to a purchase he does not recognize. He calls the number in the message. A person claiming to work in his bank's fraud department says criminals have access to his account and his savings must be moved.

The caller supplies a different account and calls it a temporary safe account. The man is told to describe the transfer as personal if anyone asks, because the bank is supposedly investigating its own employees. He thinks he is protecting his money, not giving it away.

In this example, the destination is controlled by the scammers. The false fraud alert brought him into a conversation where every instruction came from the same source.

WHY IT CAN FEEL CONVINCING

The scam reframes the loss as a protective action. Words such as safe, secure, and investigation do not change who receives the money. Coaching someone to mislead bank staff cuts off an important chance for an independent check. Stop before transferring or withdrawing funds. [1, 2]

The demand may change from a transfer to cash, gold, or a cryptocurrency machine. The central claim remains that surrendering money will somehow keep it safe. [1, 2]

The key question: Who controls the destination, and has my actual bank verified this instruction?

See where the story leads.

One illustrated route through the scam - other versions vary.



1. THE FRAUD ALERT

A message claims your money is at risk.



2. THE FALSE RESCUE

A caller gives instructions to protect it.



3. THE TRANSFER

Your money goes to a destination they control.

BREAK THE CHAIN

Stop the transfer. Call the number printed on your bank card.

CHECK THE STORY

1. Hang up and use the number printed on your bank card or a statement you already possess.
2. Ask the real bank whether there is a problem, whether any transfer has occurred, and what protective steps it recommends.
3. Do not move money to a new account, buy gold, or hand over cash because an unexpected caller says it will protect your savings. [1, 2]

IF MONEY HAS MOVED

Contact your real bank immediately. Explain the deception, identify the transfer and ask about a recall or reversal. Recovery is not guaranteed.

Tell the bank if you also disclosed passwords or security codes. Keep destination details and messages. Report the fraud at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud). Do not pay someone who promises to recover the money for a fee. [1, 3]

SOURCES / GUIDANCE CHECKED SEPTEMBER 18, 2026

1. FTC: Move-money impersonation scams

2. FTC: Refund and recovery impostors

3. FTC: What to do if you were scammed

09 Tech support pop-ups

The warning and the proposed helper can be the same trap.

WHAT THIS SCAM IS

A fake warning claims your computer is infected and directs you to a supposed support technician. The warning may be only a web page, not a diagnosis. Calling its number can lead to demands for remote access, payment, or financial information.

AN ILLUSTRATIVE EXAMPLE - NOT A REPORTED CASE

A woman browsing on her laptop sees a warning that her files are at risk. Familiar security colors surround a telephone number. The message makes her afraid to close the window.

She calls. A supposed technician requests remote access to inspect the computer. Once connected, he points to unfamiliar information on screen and says it proves a serious infection. He demands payment to fix it.

In this example, the warning was bait. The caller has not provided a trustworthy diagnosis. Granting access let a stranger control the device; it did not prove he was qualified or honest. Even a legitimate support tool can be misused.

WHY IT CAN FEEL CONVINCING

The screen creates the problem and supplies its own solution. Technical language makes the caller seem more knowledgeable than the person asking for help. Once you grant access, activity on your own computer may look authoritative even though someone else is directing it. [1, 2]

Some versions move from a device warning to a claim that your bank account is in danger. An introduction to a second supposed expert does not independently verify the first caller. A tech-support conversation should not require you to move your savings. [1, 2]

The key question: Did I choose a trusted support service, or did the warning choose it for me?

See where the story leads.

One illustrated route through the scam - other versions vary.



1. THE POP-UP

A screen claims your computer is in danger.



2. THE FAKE HELPER

The supplied number reaches an impostor.



3. THE ACCESS

Remote control or payment is requested.

BREAK THE CHAIN

Do not call the pop-up number or grant the caller access.

CHECK THE STORY

1. Do not use the telephone number or links in the warning. Close the page; get trusted help if it will not close.
2. If you suspect a real device problem, open your installed security software and run a scan.
3. Choose support through a company or technician you already trust, not the pop-up or an unverified advertisement. [1, 2]

IF YOU GRANTED ACCESS

End the remote session and seek help from a technician you independently trust. Update your security software and run a scan.

Change exposed passwords from a device you trust, including reused passwords. Contact your bank if financial information or money was involved. Keep evidence and report the scam at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud). [1, 3]

SOURCES / GUIDANCE CHECKED SEPTEMBER 18, 2026

1. FTC: Tech support scams

2. FTC: Recognizing a tech support scam (illustrated)

3. FTC: What to do if you were scammed

25 Fake investment platforms

The balance that keeps growing

WHAT THIS SCAM IS

The platform can display invented profits and allow an early payout to build confidence. It may not hold the investments it claims. A demand for more money to release a balance is not evidence that the balance exists.

AN ILLUSTRATIVE EXAMPLE - NOT A REPORTED CASE

A retiree opens an account on a platform recommended by an online acquaintance. The dashboard shows steady gains. A small withdrawal reaches his bank, giving him confidence that the service works.

He adds more money. When he later wants to withdraw the balance, support demands a separate tax or verification deposit. The screen still shows his profits, so he believes another payment will unlock money already belonging to him.

In this example, the displayed balance is not proof of assets. The early payout helped establish trust but did not authenticate later claims. Sending more money would increase his exposure without proving that anything can be withdrawn.

WHY IT CAN FEEL CONVINCING

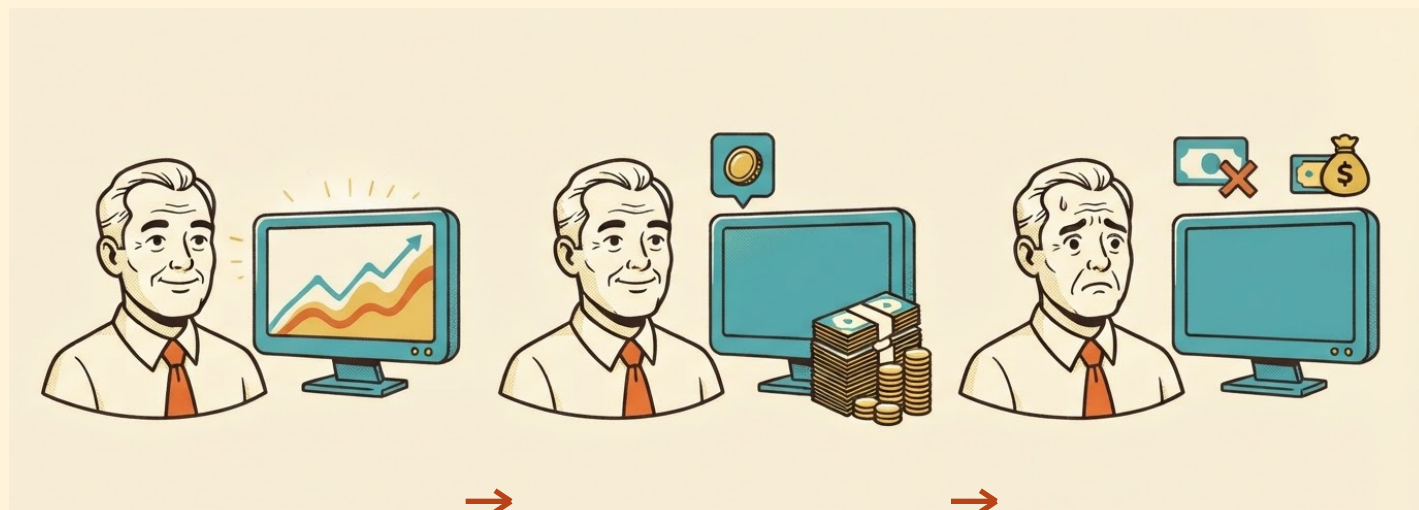
A working website and a successful small transaction can feel like a test of the whole business. They are not. The operator may control the figures, the support conversation, and the release conditions. Evidence supplied by that operator needs independent confirmation. [1, 2]

Claims of taxes or fees should be checked outside the platform. Do not assume a large on-screen balance exists merely because paying a smaller sum might release it. [1, 2]

The key question: What evidence of the investment exists outside this platform's own screens?

See where the story leads.

One illustrated route through the scam - other versions vary.



1. THE DISPLAY

An account appears to earn steady profits.

2. THE TRUST

A small payout encourages a larger deposit.

3. THE LOCK

A new fee blocks the requested withdrawal.

BREAK THE CHAIN

Stop adding money and verify the provider and claimed assets independently.

CHECK THE STORY

1. Check the firm and professional through Investor.gov and relevant regulators.
2. Understand custody, fees, risks, and withdrawal terms before funding.
3. Consult an independent professional with no connection to the pitch. [1, 2]

IF THIS HAPPENED

Stop adding funds. Preserve wallet addresses, transfer records, website addresses, and messages. Report suspected fraud to IC3 and the appropriate securities or commodities regulator.

Contact the relevant provider promptly. Save messages, agreements, and payment records. Recovery is not guaranteed. [3]

SOURCES / GUIDANCE CHECKED SEPTEMBER 18, 2026

1. FTC: Investment scams

2. FTC: How to avoid a scam

3. FTC: What to do if you were scammed

39 Ticket resale fraud

The seat that belongs to someone else

WHAT THIS SCAM IS

Tickets can be nonexistent, duplicated, or transferred in a way that is not valid for the event. A screenshot and a plausible story are not proof that the seller can provide a usable ticket.

AN ILLUSTRATIVE EXAMPLE - NOT A REPORTED CASE

A fan finds scarce tickets through a social-media seller. The seller sends a screenshot showing seats and a barcode. It looks like the ticket the fan expects to receive, and the price seems reasonable.

The seller asks to leave the platform and pay immediately because another buyer is waiting. The fan cannot independently confirm that a valid transfer will occur. The screenshot becomes the main reason for trusting the deal.

Here, an image is being mistaken for control of admission. A ticket may be copied, nonexistent, or transferred in a way the event does not accept. Seeing a plausible barcode does not establish that you will be able to enter.

WHY IT CAN FEEL CONVINCING

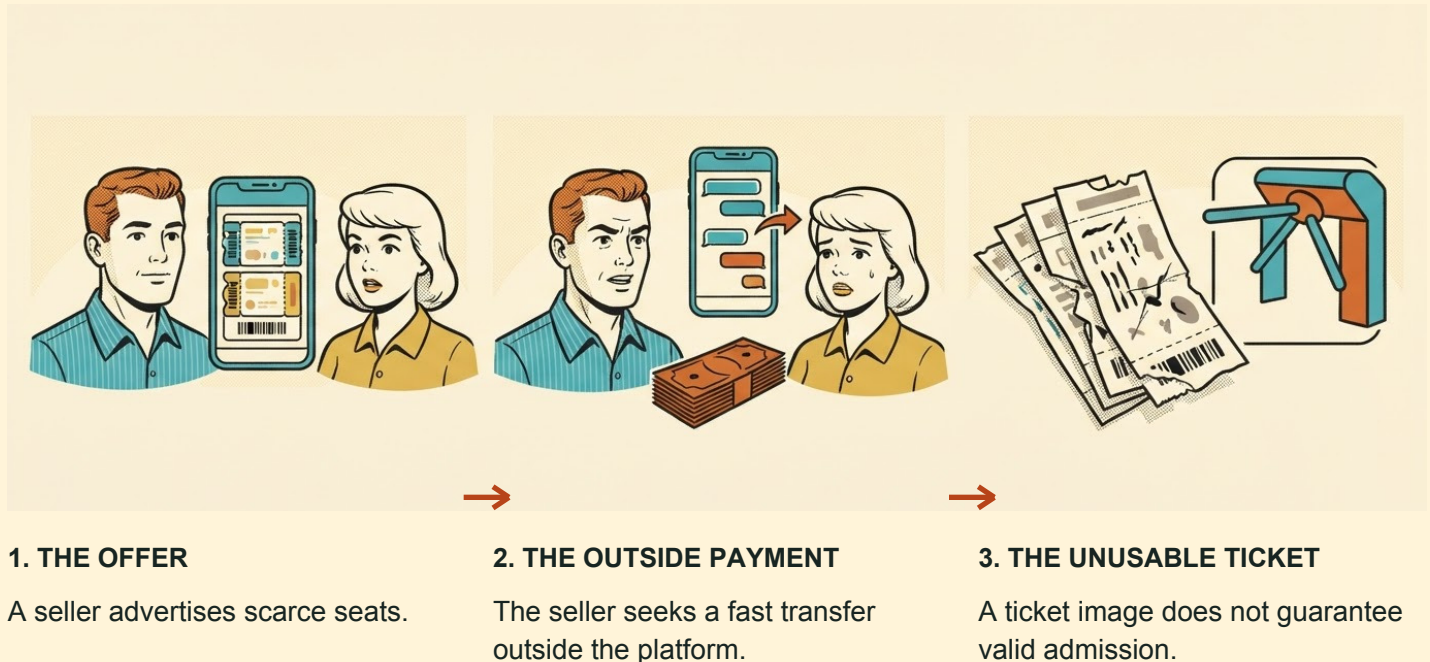
Demand for a particular event makes delay feel expensive. Detailed seat information can create confidence without proving ownership. Moving payment outside the original service may also remove protections that influenced the buyer's decision to use that service. [1, 2]

Different venues have different transfer rules. Verify them through the event or authorized ticket provider and evaluate what happens if the promised admission is not delivered. [1, 2]

The key question: Will this transaction give me a valid ticket under the event's actual rules?

See where the story leads.

One illustrated route through the scam - other versions vary.



BREAK THE CHAIN

Use a verifiable ticket transfer and understand the payment protection.

CHECK THE STORY

1. Start with the venue or event's official ticket information.
2. Check which resale and transfer methods it recognizes.
3. Understand the seller protection, refund terms, and payment method before buying. [1, 2]

IF THIS HAPPENED

Save the listing and payment records. Contact the seller platform and payment provider promptly. If already at the venue, ask its box office about the ticket rather than paying an unknown person for a replacement.

Contact the relevant provider promptly. Save messages, agreements, and payment records. Recovery is not guaranteed. [3]

SOURCES / GUIDANCE CHECKED SEPTEMBER 18, 2026

1. Pennsylvania Attorney General: Ticket scams

2. FTC: How to avoid a scam

3. FTC: What to do if you were scammed

64 Check washing and mail theft

The ordinary check with a new payee

WHAT THIS SCAM IS

Stolen checks can be altered or reproduced for fraudulent deposit. This begins with a real payment instrument, unlike a fake check sent to you. The bank's check image and the intended recipient's records can help establish what changed.

AN ILLUSTRATIVE EXAMPLE - NOT A REPORTED CASE

A household mails a check to pay a routine bill. Later, the bank record shows a different payee or an altered amount. The check may have been stolen from the mail and changed before being deposited or otherwise misused.

The household initially assumes the intended recipient received the payment. Only a late notice or review of the cleared-check image reveals the mismatch. The legitimate bill may still be unpaid while the account has already lost money.

In this example, the original payment was real, but the physical instrument became the attack point. Prompt review and reporting matter. The customer should contact the bank about the altered check and the intended recipient about the actual bill, using trusted contact information.

WHY IT CAN FEEL CONVINCING

Checks contain useful account information and can move through places the sender cannot monitor. A transaction appearing in the bank history may look like proof that the correct bill was paid. The cleared-check details can tell a different story. [1, 2]

Mail theft can also lead to other forms of check fraud. Safer payment and mailing choices reduce exposure, but no single ink type or mailing habit guarantees protection. [1, 2]

The key question: Do the cleared-check payee and amount match what I actually wrote?

See where the story leads.

One illustrated route through the scam - other versions vary.



BREAK THE CHAIN

Contact the bank promptly and report suspected mail theft to USPS.

CHECK THE STORY

1. Review paid-check images and statements.
2. Use secure mailing and payment options appropriate to the bill.
3. Confirm receipt with the intended payee when a payment is missing. [1, 2]

IF THIS HAPPENED

Notify the bank promptly and report mail theft or check washing to USPS. Preserve the check image and mailing details. Ask the bank how to address the original unpaid obligation without duplicating a disputed payment unnecessarily.

Contact the relevant provider promptly. Save messages, agreements, and payment records. Recovery is not guaranteed. [3]

SOURCES / GUIDANCE CHECKED SEPTEMBER 18, 2026

1. USPS: Check washing

2. FTC: How to avoid a scam

3. FTC: What to do if you were scammed

PRINTABLE TOOL 01

The pause card

I WILL CALL YOU BACK.

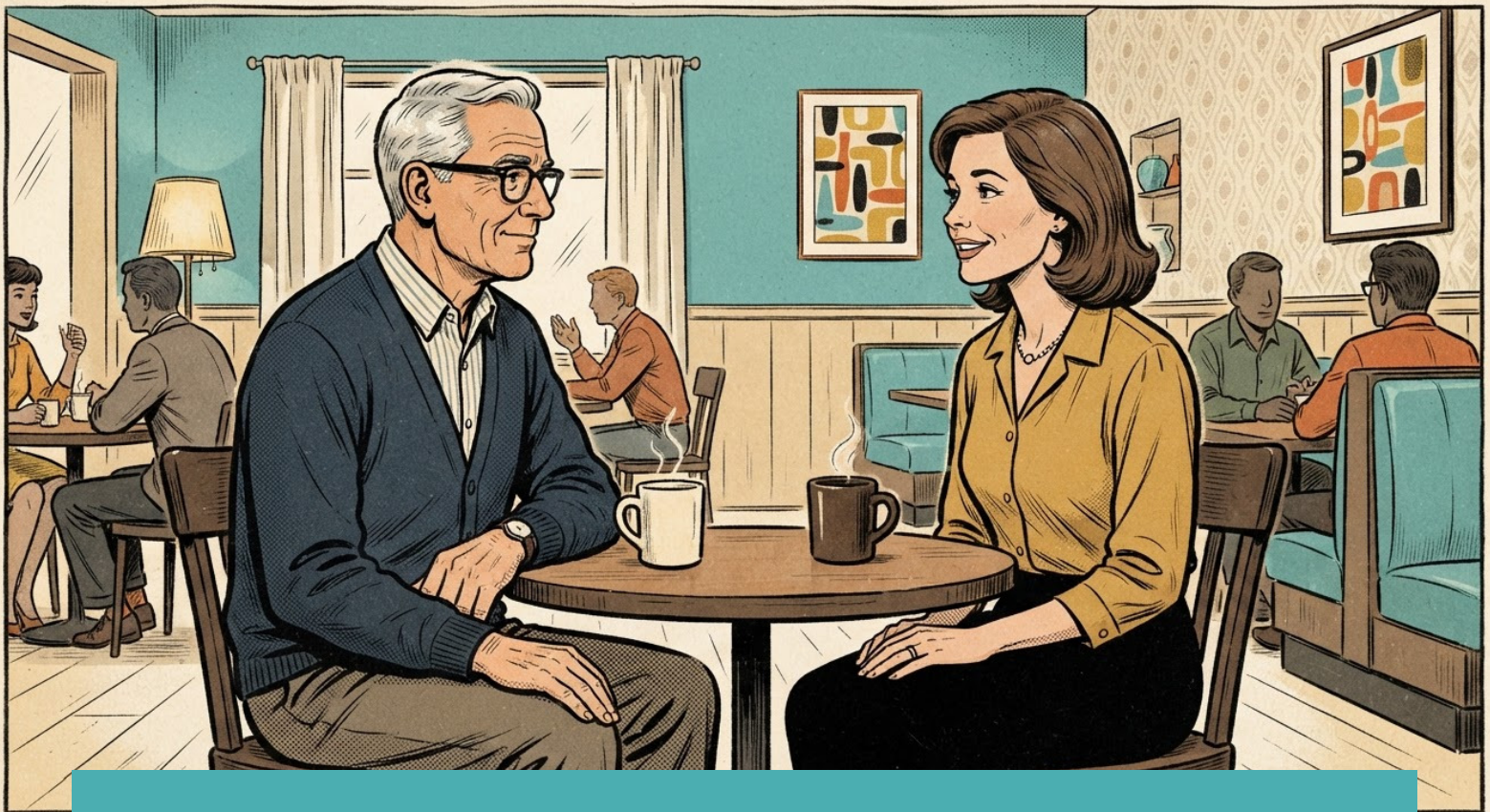
**Use a number you already know or find independently.
Verify the event before sending money, codes,
documents, or access.**

AN UNEXPECTED CALL DOES NOT SET YOUR DEADLINE.

Keep this by the phone. If someone may be in immediate danger, call 911. For a suspicious payment, contact the real bank or provider promptly. Three unanswered calls do not confirm an emergency.

KEEP THIS WITHIN REACH

You do not have to solve it alone.



A familiar voice. An impressive title. A frightening deadline.

You can still pause and check separately.

FREE SAMPLE / Full edition includes 64 profiles and the printable kit.