TECHNITEA BOOKS · EVERYDAY SAFETY

Spot the Scam

A plain-English guide to online and phone fraud, for you and the people you love.



Technitea

technitea.com

Spot the Scam

A plain-English guide to online and phone fraud, for you and the people you love.

Spot the Scam
A plain-English guide to online and phone fraud, for you and the people you love.
First edition, November 2026

Written and edited by the Technitea editorial team.

Published by Technitea.
PT Arena Karya Nusantara, Tuban, East Java, Indonesia.
technitea.com

© 2026 PT Arena Karya Nusantara. All rights reserved. No part of this book may be reproduced, shared or resold in any form without written permission from the publisher, except for brief quotations in reviews. Your purchase licenses one reader. The worksheets may be printed for your own use.

Illustrations generated with AI image tools under art direction. Statistics are taken from the U.S. Federal Trade Commission and the FBI's Internet Crime Complaint Center, cited at the back of the book.

Statistics and advice were checked against the sources listed at the back as of November 2026. This book gives general information, not legal or financial advice. Scam tactics change quickly; check the official sites listed at the back for current guidance. If you are in immediate danger, call 911. The publisher accepts no liability for losses arising from the use of this book.

Contents

	Before you start
01	Every scam runs the same play
02	The pause that beats most scams
03	Imposters: who's really calling?
04	Texts, emails and the urge to click
05	Money that can't come back
06	Love, friendship and investment scams
07	Jobs, shopping and selling online
08	Fake voices, faces and messages
09	Lock the doors before anyone knocks
10	If it happens: the first hour and after
A	The scam-spotting card
B	Where to report and get help

Before you start

In 2024, people in the United States told the Federal Trade Commission they had lost more than **$12.5 billion** to fraud. That was up 25% from the year before. The number of reports barely changed, at about 2.6 million. What changed was how often people lost money: 38% of the people who reported a scam had paid something, up from 27% a year earlier.

The FBI's Internet Crime Complaint Center (IC3), which counts cybercrime separately, received just over **one million complaints in 2025**, with reported losses of almost **$20.9 billion**. People aged 60 and over reported about $7.7 billion of that.

Those are only the losses people reported. Many never do, out of embarrassment or because they don't know where to go.

The scammers behind these numbers are not geniuses. Most are working from scripts, the same few scripts, rewritten for whatever is in the news this month. Once you can see the script, the costume stops working. That is what this book teaches.

Who this book is for

- Anyone who has ever got a strange text about a package, a toll or a bank account and wasn't sure what to do with it.
- Adult children worried about a parent, and parents worried about a teenager.

- People who have already been scammed, and want to make sure it never happens again. If that's you: it was not because you're foolish. These schemes are designed by professionals to catch smart, busy, kind people at a bad moment.

How to use it

Chapters 1 and 2 are the core. They explain how almost every scam works and the single habit that defeats most of them. If you only read two chapters, read those. Chapters 3 to 8 walk through the scams people actually meet, grouped by how they reach you. Chapter 9 shows how to make yourself a harder target, and Chapter 10 is what to do if money or information has already gone.

At the back you'll find a one-page **scam-spotting card** to print and stick by the phone, and a list of **where to report** every kind of scam.

> NOTE
>
> Every statistic in this book comes from U.S. government sources: the Federal Trade Commission's Consumer Sentinel data and the FBI's IC3 annual reports. Full references are listed at the back. Advice about what to do is based on guidance from the FTC, the FBI and the consumer agencies named in each chapter.

CHAPTER

01

Every scam runs the same play



IN THIS CHAPTER

- The four signs the FTC says almost every scam shares
- Why scammers aim at your feelings, not your intelligence
- How to recognize a script no matter what costume it wears

A scam can look like a bank alert, a job offer, a soldier who wants to talk, or your grandson in trouble. Underneath, the plot hardly changes. Learn the plot once and you'll recognize it in every costume.

1.1 The four signs

The Federal Trade Commission, the U.S. agency that collects fraud reports from the public, sums up almost every scam in four signs. They're worth memorizing, because together they cover the vast majority of what reaches your phone and inbox.

1. **They pretend to be someone you know or trust.** A government agency, your bank, a delivery company, a tech company, a family member, a charity.
2. **They say there's a problem or a prize.** Your account is locked. You owe back taxes. Your grandson is in jail. You won a sweepstakes. Your computer has a virus.
3. **They pressure you to act right now.** Before you can think, check or talk to anyone.
4. **They tell you to pay in a specific way.** Usually a way that's fast and hard to reverse: gift cards, a wire transfer, a payment app, cryptocurrency, or cash handed to a courier.

You don't need all four to be suspicious. Any one of them is a reason to slow down. Two or more together is a scam until proven otherwise.

WORKED EXAMPLE

Spotting the signs in a real-looking message. Here's a text of the kind millions of people received in 2024 and 2025:

"STATE TOLL SERVICES: Our records show your vehicle has an outstanding toll balance of $6.99. To avoid a late fee of $50.00 and suspension of your registration, pay by today at the link below."

- **Pretend:** "State Toll Services" sounds official but names no real agency.
- **Problem:** an unpaid toll.
- **Pressure:** "by today," a late fee, a threat to your registration.
- **Pay:** through a link in a text, which leads to a fake page that collects your card number.

The amount is small on purpose. Nobody thinks hard about $6.99. The real goal is your card details, which can then be used for much larger charges.

1.2 They aim at feelings, not intelligence

People often assume scam victims are naive. The data says otherwise. Fraud happens to doctors, engineers, police officers and accountants. What scammers target isn't a lack of intelligence. It's a moment when strong feelings crowd out careful thinking.

The feelings they use most:

- **Fear.** Your account is compromised. You're under investigation. Your computer is infected.
- **Love and loyalty.** A family member needs help. Someone you've been talking to online needs money to visit you.

- **Hope.** A great job, a sure investment, a prize.
- **Shame and secrecy.** "Don't tell anyone, or it'll make things worse." Scammers often instruct victims not to talk to family or bank staff, because they know a second person usually breaks the spell.
- **Helpfulness.** You want to fix the problem, help the caller, be a good customer.

Notice that most of these are good qualities. Scammers turn your best instincts against you.

> TIP
>
> When you notice a strong feeling while reading a message or talking on the phone, especially fear or urgency, treat the feeling itself as a warning sign. Real problems can wait the ten minutes it takes to check.

1.3 The script under the costume

Most scams follow the same five steps, whatever the story:

1. **Contact.** A call, text, email, social-media message or pop-up reaches you. It looks like it comes from someone legitimate.
2. **Story.** You're told about a problem or a prize. The details are specific, which makes them feel true.
3. **Isolation.** You're kept on the phone, told the matter is confidential, or warned not to trust bank staff.
4. **Urgency.** A deadline, a threat, or a limited window. You must act now.

5 **Payment.** You're steered toward a payment method that's fast and hard to undo, or asked for details (passwords, codes, card numbers) that let them take the money themselves.

Once you see this pattern, you'll start noticing it everywhere, including in the news reports of new scams. The technology changes. The script doesn't.

1.4 How they reach you

According to the FTC's 2024 data, people who reported fraud most often said the scammer first reached them by **email**. That was the case for the second year in a row. **Phone calls** were second and **text messages** third.

That matters because each channel has its own tricks, and Chapters 3 and 4 cover them in turn. But the rule for all of them is the same: **a message reaching you is not proof of who sent it.** Caller ID can be faked. A sender's name in an email can be anything. A text can claim to be from your bank. You can't tell who someone is from how they contacted you, only from contacting them yourself through a route you already trust.

CHAPTER SUMMARY

- The FTC's four signs: scammers **pretend** to be someone you trust, say there's a **problem or prize**, **pressure** you to act now, and want you to **pay** in a specific way.
- Scams target feelings (fear, love, hope, shame, helpfulness), not intelligence.
- Most scams follow one script: contact, story, isolation, urgency, payment.
- Email, phone calls and texts were the most common first contact in 2024. None of them proves who is on the other end.

NEXT

You know the play. Chapter 2 gives you the one move that defeats most of it.