



Free guide · 50+ Edition

Spot AI Scams & Stay Safe Online

A calm way to check a worrying call, message, or offer before you act.

Inside: realistic practice situations, clear next steps, a personal contact plan, and trusted places to get help.

No AI account or special software required.

Free edition 1 · October 10, 2026

Delta 3 Core Tech LLC · Carrboro, NC · delta3coretec.ai

You do not have to prove it is fake.

You only need a safe way to check before sharing information, giving access, or sending money.

AI can help a scammer sound convincing. A familiar voice, polished message, or realistic picture can make a request feel trustworthy. You do not need to become an expert at spotting edited media. Focus on the request and check it through a route you choose. [1, 2]

If something is happening now: stop responding. For a possible payment or account loss, turn to page 10. For immediate physical danger, contact emergency services: 911 in the United States, or your local emergency number elsewhere. [9]

Choose your path

- **Three minutes:** learn the pause-and-check routine on page 3.
- **Ten minutes:** read the situation closest to yours on pages 4 to 7, then try the practice on page 8.
- **One useful habit:** fill in your personal contact plan on page 12 while you are calm.

Examples in this guide are invented teaching situations. They are not reports about real people or businesses. The reporting directory is for the United States; readers elsewhere should use their own official local services.

Sources [1], [2], [9]. Numbered references are on page 13.

Pause. Leave. Check. Decide.

Keep this routine beside your phone. A request can wait while you check who is asking.

- 1 Pause the action.**
Do not send money, share a code, install software, or open a link just because someone says it is urgent.
- 2 Leave that conversation.**
End the call or stop replying. You do not owe an unknown sender an explanation.
- 3 Check through your own route.**
Call a number you already trust, open the company's usual app, or use an official website you know. Do not use contact details supplied in the suspicious message.
- 4 Decide after the check.**
If you still cannot confirm the request, keep it on hold and ask a trusted person or the helpline on page 11.

A SENTENCE YOU CAN USE

"I will check this independently and contact the organization myself."

Pressure, secrecy, frightening threats, and demands for unusual payment are reasons to pause. A professional-looking message does not cancel those warning signs. [3]

Routine adapted from FTC scam-avoidance guidance [3].

“It's me. I need help now.”

INVENTED SITUATION

A caller sounds like your nephew. He says he has had an accident, needs money immediately, and does not want you to tell anyone. Another person takes the phone and gives payment instructions.

A voice can be copied. Caller ID, personal details, and an emotional story do not establish who is on the line. The FTC advises checking with the person using a number you already know. [2]

Take a separate route

1. End the call. Do not follow payment instructions while checking.
2. Call your nephew using the saved number you used before this incident.
3. If he does not answer, contact another trusted relative or friend who may know where he is. Silence does not confirm the caller's story.

Prepare together: agree on a private family word or phrase. Keep it out of public posts and AI chats. Treat it as an extra check, not the only proof of identity. A correct answer does not replace a separate callback. [1]

If there is a credible immediate threat to someone's safety, contact emergency services directly rather than relying on the caller's instructions. [9]

Sources [1], [2], [9].

Check the account, not the message.

A delivery problem, unpaid bill, or account warning can be used to rush you onto a fake website.

INVENTED SITUATION

"Your parcel is on hold. Pay the small redelivery fee today." The text contains a link. You are expecting a parcel, so the story feels plausible.

Your safer next move

Leave the text alone. Open the delivery company's usual app or use the tracking information from your original order. If something needs attention, handle it there. The fact that you are expecting a parcel does not authenticate this message. [4]

- **Attachments:** do not open an unexpected file to "see what it is."
- **QR codes:** treat an unexpected code like an unexpected link. A code can send you to a fake sign-in page. [5]
- **Branding:** a familiar logo and good spelling are not proof. AI can help produce polished messages. [1]

Keep the choice simple: you do not need to study a long web address under pressure. Use a saved bookmark, your existing app, or a known contact instead.

Sources [1], [4], [5].

A warning is not a verified helper.

INVENTED SITUATION

Your screen displays an alarming message with a number to call. A “technician” says your accounts are exposed and asks to control your computer. A second caller says to move your savings to protect them.

Fake support warnings and follow-on government impersonation can be part of the same scam. Real security pop-up warnings do not ask you to call a phone number. [6]

Keep control of the next step

- Do not call the number in the warning or give an unexpected caller remote access.
- Close the page if you can. If it will not close, seek help from someone you already trust rather than pressing buttons in the warning.
- For an account concern, use the number printed on your bank card or statement, or the bank's established app.
- Do not move money at the caller's direction. A supposed government official saying to transfer money to protect it is a scam warning. [6, 7]

Search carefully: scammers also advertise fake support services. A prominent search result is not an endorsement. [6]

Sources [6], [7]. Already gave access or sent money? See page 10.

Look at the request behind the picture.

AI-made or altered media can imitate a person. A real person's photo can also be stolen and reused.

The FBI describes fraud involving generated profiles, fake endorsements, copied voices, and fabricated video. A live-looking call or realistic image is not enough to verify an identity. [1]

INVENTED SITUATION

An account sends friendly messages for several weeks. It then invites you into an exclusive investment group and promises that a celebrity's "AI system" will make money for you.

Separate the story from the action

- Write down exactly what the account wants you to do: send money, share account details, install an app, or keep the arrangement secret.
- Avoid treating a face, voice, badge, or screenshot as the final check.
- Do not let an online relationship or a claimed endorsement replace independent checks with sources you choose.

You do not need a verdict on the technology. A request can be unsafe whether AI helped create it or not. A strange-looking image is not proof of fraud, and a convincing image is not proof of safety.

Source [1]. This guide does not assess investments or recommend financial products.

What would you do next?

These are invented practice situations. Choose the safest next action, not whether you can prove someone used AI.

1. The new phone number

"Hi, it's your daughter. My phone broke. Please pay this bill for me now."

- A. Reply and ask for a photograph.
- B. Call your daughter's existing number or another trusted contact.
- C. Pay because the message uses her usual greeting.

2. The account warning

A text says your account will close today unless you sign in through its link.

- A. Open your normal app separately and check there.
- B. Enter your password quickly to meet the deadline.
- C. Ask the text sender whether the link is genuine.

3. The confident chatbot

You summarize a suspicious offer for an AI assistant. It replies, "This looks legitimate."

- A. Treat the answer as an identity check.
- B. Ask it to make the payment.
- C. Keep the request on hold and verify through an independent route.

One extra question: what would change your next action? Look for information obtained independently, not more reassurance from the same sender.

Answers and explanations are on page 9.

Use AI to organize, not authenticate.

An AI assistant can help you slow down and make a list. Its confident answer does not establish who sent a message.

Practice answers

- 1: B.** A separate contact route checks the story without relying on the new sender's evidence.
- 2: A.** Opening your existing app avoids the message's sign-in link.
- 3: C.** A chatbot's impression is not proof of identity or legitimacy.

Before using an assistant

Describe the situation in your own words. Leave out names, addresses, contact details, passwords, codes, account numbers, and private documents.

Do not upload suspicious attachments or ask an assistant to visit the sender's links.

OPTIONAL PROMPT WITH A MADE-UP EXAMPLE

Help me list safe ways to verify this request independently. Do not decide whether the sender is genuine or open any links. Situation: someone claiming to be a relative asks for an urgent payment from a new number. Give me three checks that do not involve replying to that sender.

This prompt is an original practice aid, not a scam detector. Check its suggestions against the routine in this guide. It cannot verify a caller, guarantee safety, or recover money.

Practice applies the independent-check principles in sources [2] and [4].

Take the next useful step.

Being deceived is not a reason to stay silent. Stop further contact and get help promptly.

1. **Money or card details:** contact the bank, card issuer, payment service, or gift card issuer immediately through a trusted route. Explain what happened and ask whether the payment can be stopped, reversed, or refunded. Recovery is not guaranteed. [7]
2. **Password or account access:** use another trusted device if yours may be compromised. Change affected and reused passwords through the real service. Turn on multi-factor authentication, an extra sign-in check, where available. Use official recovery if locked out. [7]
3. **Remote access or a suspicious download:** if someone has remote access, disconnect the affected device from the internet: turn off Wi-Fi and unplug any network cable. Use another trusted device to contact your bank or secure accounts. Get trusted technical help, then update security software and run a scan. [6, 7, 11]
4. **Keep a record:** save dates, messages, receipts, and transaction references you already have. Do not reopen a risky attachment or contact the sender again to collect evidence. [9]

Beware of a second scam: an unsolicited “recovery specialist” who promises your money back for an upfront payment can cause another loss. Use the official resources on page 11. [8]

If personal information was exposed, visit [IdentityTheft.gov](https://www.identitytheft.gov) for situation-specific recovery steps. Immediate danger requires emergency services, not an online report. [7, 9]

Sources [6], [7], [8], [9], [11].

Places to report and ask for help

Type the address yourself or use these links from your own saved copy. Avoid links sent by the suspicious contact.

ReportFraud.ftc.gov

<https://reportfraud.ftc.gov/>

Report scams and fraud to the Federal Trade Commission. A report is not a promise of individual recovery. [3, 7]

FBI Internet Crime Complaint Center

<https://www.ic3.gov/>

Report internet-enabled crime. Keep records; the FBI cannot guarantee a response to each report. IC3 warns that impostors may falsely offer recovery help. [9]

AARP Fraud Watch Network Helpline

877-908-3360 · Monday to Friday, 8 a.m. to 8 p.m. Eastern

aarp.org/money/scams-fraud/helpline/

Free guidance and support for members and nonmembers. It is not an investigation, recovery service, or emergency line. [10]

Identity information: IdentityTheft.gov provides recovery guidance. **Immediate danger:** call 911 in the US. Outside the US, use official local reporting services and the local emergency number. [7, 9]

Resources checked October 10, 2026. Services and hours can change; confirm on the official sites. Sources [3], [7], [9], [10].

My pause-and-check plan

Prepare this now. Keep it somewhere you can find easily, away from public view.

A trusted person I can call when a request worries me

Their number, checked with them in advance

A second trusted contact if the first is unavailable

Where I keep my bank's official contact details

My three commitments

- ☐ I can end a worrying conversation and check independently.
- ☐ I will not send money or share a code while someone is pressuring me.
- ☐ I will ask for help if I am uncertain or have already acted.

Keep secrets off this sheet: do not write passwords, payment details, one-time codes, or your family verification phrase here. Do not upload the completed sheet to an AI assistant.

A phrase to practice: "I do not act on urgent requests until I have checked them myself."

Read more from the original sources

Official resources checked October 10, 2026. This guide summarizes practical precautions; the agencies do not endorse this publication.

[1] FBI IC3: Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud

December 3, 2024. Examples of AI-assisted impersonation.

ic3.gov/PSA/2024/PSA241203

[2] FTC: Scammers use AI to enhance their family emergency schemes

March 2023. Voice cloning and independent callbacks.

consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes

[3] FTC: How To Avoid a Scam

consumer.ftc.gov/articles/how-avoid-scam

[4] FTC: How To Recognize and Avoid Phishing Scams

consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams

[5] FTC: Scammers hide harmful links in QR codes to steal your information

December 2023.

consumer.ftc.gov/consumer-alerts/2023/12/scammers-hide-harmful-links-qr-codes-steal-your-information

[6] FTC: How To Spot, Avoid, and Report Tech Support Scams

consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[7] FTC: What To Do if You Were Scammed

consumer.ftc.gov/articles/what-do-if-you-were-scammed

[8] FTC: Refund and Recovery Scams

consumer.ftc.gov/articles/refund-and-recovery-scams

[9] FBI IC3: Home, reporting guidance, and frequently asked questions

ic3.gov · ic3.gov/Home/FAQ

[10] AARP: Fraud Watch Network Helpline

aarp.org/money/scams-fraud/helpline/

[11] FBI Chicago: Local technical support scam warning

fbi.gov/contact-us/field-offices/chicago/news/press-releases/fbichicago-warns-of-local-technical-support-scam

You can pause before you act.

Choose one person for your contact plan today. Practice making an independent check before you need it.

What this guide can do: help you recognize risky requests, slow the situation down, and find a trusted route for checking or reporting.

What it cannot do: prove a person's identity, identify every scam, guarantee recovery, or replace help for a real emergency.

Your free-use license

© 2026 Delta 3 Core Tech LLC. All rights reserved. This free guide is licensed to each reader for personal use. You may save and print a copy, and copy, adapt, and use its prompts and templates for your own purposes, including at work. Share the download page at www.delta3coretec.ai/free/spot-ai-scams so others can get their own copy. The guide itself may not be redistributed, republished, resold, or included in another product. ChatGPT, Claude, Perplexity, and other product names are trademarks of their respective owners; this is an independent publication and is not affiliated with or endorsed by them. AI output can be inaccurate; verify anything important, and never share passwords, bank or card numbers, or government ID numbers. Nothing in this document is medical, legal, or financial advice.

About this publication

Prepared by Delta 3 Core Tech LLC, Carrboro, North Carolina.

Free edition 1 · October 10, 2026 · AI-13

For a problem with this download, contact support@delta3coretec.com. The publisher is not a fraud-reporting or emergency service. Use page 11 for those resources.

www.delta3coretec.ai