Free printable · For US readers

AI Scam Safety Checklist

AI lets scammers fake voices, faces, websites and chat. The trick is new; the ask is old: send money fast, in a way that is hard to undo.

Three habits that stop most of these

1. **Slow down.** A real emergency can wait five minutes for a callback.
2. **Check on a channel you already trust:** a number saved in your phone, the official app, the number on your card.
3. **Never pay by gift card, wire, crypto or crypto ATM because someone contacted you.** The FTC says only scammers demand payment in cryptocurrency.

Scam	What it looks like	Red flags	What to do
Deepfake calls and video	A call, voice note or video chat that sounds or looks like a relative, your boss or a famous person.	It is urgent and secret. It asks for money, codes or a payment. Video lags or lips don't match the words.	Hang up. Call back on a number you already have. Ask for your family safe word.
Fake support bots	A chat window, search ad or social account posing as your bank, an app store or tech support.	You reached it through an ad or a message, not the company's own app. It wants passwords, one-time codes, remote access, or money moved "to keep it safe."	Close it. Use the company's official app or the number on the back of your card.
Fake AI trading bots	Ads, influencers or group chats selling a bot that "uses AI" to trade for you.	Guaranteed or very high returns, a "100% win rate," bonuses for signing up friends, a fee to withdraw your own money.	Send nothing. AI can't predict markets (CFTC). Look up the company and get a second opinion from someone you trust.
AI phishing	Emails and texts that read perfectly, use your name and mention real details about you.	An unexpected link, "your account is locked," a short deadline, a sender address that is slightly off.	Don't click. Type the site address yourself or open the app. Turn on two-step sign-in.
Wallet drainers	Fake "claim," airdrop or mint sites that ask you to connect a crypto wallet and sign.	Free tokens you didn't expect, a signature you don't understand, a request to "approve" spending.	Don't connect or sign. Do crypto experiments in a separate small wallet, never your main one.
Fake tokens and coins	A new coin pushed on social media, often with a fake celebrity video or an "AI" label.	A countdown, a celebrity "endorsement," a promise it will multiply. Some can be bought but never sold.	Skip it. Celebrities are not messaging you, and only scammers guarantee profits (FTC).

In 2025 the FBI's Internet Crime Complaint Center received more than 22,000 complaints with AI-related information, with reported losses above $893 million (FBI IC3 2025 Annual Report).

Set these up this week

- [ ] Pick a family safe word and share it in person. The FBI recommends a secret word or phrase.
- [ ] Save the real numbers for your bank, card company and close family in your phone.
- [ ] Turn on two-step sign-in for email, bank and your phone carrier.
- [ ] Make social accounts private and limit public clips of your voice and face (FBI tip).
- [ ] Put AI subscriptions and any AI shopping on a capped virtual card, not your main card.
- [ ] Keep crypto experiments in a separate small wallet.
- [ ] Never read out or type in a one-time code someone asked you for.
- [ ] Tell older relatives about voice cloning. Give them a copy of this page.

If it already happened

1. **Stop sending money.** Paying again to “unlock” or “recover” funds is usually part of the scam. Ignore anyone who offers to get your money back for a fee.
2. **Call your bank or card company** on the number on your card. Ask them to stop or reverse the payment. The FTC says the sooner you act, the better.
3. **Lock things down.** Change passwords, turn on two-step sign-in, and if you gave someone remote access, disconnect that device from the internet.
4. **Save the evidence:** screenshots, phone numbers, website addresses, wallet addresses, receipts and dates.
5. **Report it** to the FBI at **ic3.gov** and the FTC at **ReportFraud.ftc.gov**. For crypto or trading-bot fraud, the CFTC also takes reports at **cftc.gov/complaint**.
6. **Tell someone you trust.** Scammers count on you keeping it secret.

> **Quick test for any message, call or ad:** Did they contact me first? Are they rushing me? Do they want money, a code or access? Two yeses: stop and check through a channel you trust.

Sources

FBI IC3 2025 Annual Report, ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
FBI IC3 PSA I-120324-PSA (Dec 3, 2024), ic3.gov/PSA/2024/PSA241203
FTC, “What To Know About Cryptocurrency and Scams,” consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams
FTC, “Scammers Use Fake Emergencies To Steal Your Money,” consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money
CFTC Customer Advisory, “AI Won’t Turn Trading Bots into Money Machines,” cftc.gov/LearnAndProtect/AdvisoriesAndArticles/AITradingBots.html

General information, not financial or legal advice. More plain guides: agentlane.net