AI Scam and Deepfake Warning Checklist

Version 1.0 — May 2026

AI has made some scams easier to personalize and harder to spot. This checklist is not here to make you paranoid. It is here to give you a pause button.

If something feels urgent, emotional, secret, or money-related, slow down.

The big rule

Do not act on an urgent request until you verify it through a separate trusted channel.

That means you do not use the phone number, link, email address, or instructions in the suspicious message.

Instead:

- Call the person using a number already saved in your contacts.
- Call the organization using the number on an official card, statement, or website.
- Text the person separately in an existing conversation.
- Ask another trusted family member or coworker.
- Log in by typing the website address yourself, not by clicking the link.

If it is real, it can wait long enough for verification.

Common warning signs

Be extra careful if the message, call, image, or video includes any of these:

- “You must act right now.”
- “Do not tell anyone.”
- “Send money immediately.”
- “Buy gift cards.”
- “Move money to protect it.”
- “Your account will be closed today.”
- “Your grandchild/friend/coworker is in trouble.”
- “This is law enforcement / the IRS / your bank / tech support.”
- “Click this link to fix the problem.”
- “Download this file.”
- “Install this app so I can help you.”
- “Share your screen with me.”
- “I need your password or verification code.”
- “This is confidential.”
- “I changed my number.”
- “I cannot talk long.”

• “Please do not call me back.”

Scammers use pressure because pressure makes people skip verification.

Voice call checklist

A voice can be faked or imitated. Caller ID can also be misleading.

Before trusting a surprising or urgent call, ask:

• Is the caller pushing urgency?
• Are they asking for secrecy?
• Are they asking for money, gift cards, wire transfers, crypto, or payment apps?
• Are they asking for a password, code, PIN, or account number?
• Are they refusing to let you hang up and call back?
• Are they asking you to install a remote access app or share your screen?
• Does the situation seem dramatic but vague?
• Does the voice sound close enough to someone you know, but the request feels wrong?

What to do:

1. Hang up.
2. Call the person or organization using a known trusted number.
3. If it involves a family member, call another family member too.
4. Do not send money until you verify.

A useful sentence:

“I need to verify this separately before I do anything.”

Text and email checklist

Be careful with messages that:

• include suspicious links
• ask you to log in through a link
• claim a delivery, bank, tax, or account problem
• include an attachment you were not expecting
• use strange grammar or unusual tone
• look almost right but not quite
• come from a new number claiming to be someone you know
• ask for a verification code
• ask you to reply with private information

What to do:

• Do not click the link.
• Do not download the attachment.

• Do not reply with private details.
• Do not install remote access apps or share your screen because of an unexpected message.
• Go to the official website yourself or use the company's official app.
• Contact the person or company through a trusted channel.

Photo and video checklist

AI can create fake images and videos. Some are obvious. Some are not.

Be careful when an image or video:

• seems designed to make you angry or afraid
• shows a public figure saying something shocking
• shows a person in a situation that seems out of character
• comes from an account you do not recognize
• has no reliable source attached
• is being shared with "Can you believe this?" energy
• appears during a crisis, election, disaster, or breaking news event

Look for:

• weird hands, teeth, glasses, shadows, or reflections
• unnatural blinking or mouth movement
• distorted background text or signs
• mismatched lighting
• strange edges around the face or hair
• a source that traces back only to reposts

But do not rely only on visual clues. AI fakes are getting better.

Better check:

• Is a reliable news source reporting it?
• Did the person or organization post it on an official account?
• Are multiple trustworthy sources confirming it?
• Could this be old footage with a new false caption?

Money request checklist

Stop and verify before any request involving:

• gift cards
• wire transfers
• crypto
• payment apps
• bank transfers
• cash pickup
• "refund" overpayments

• moving money to a “safe” account
• emergency bail, hospital, travel, or accident stories
• a boss or coworker asking for a secret purchase

Real banks, government agencies, and law enforcement do not need you to buy gift cards to solve a problem. That is scam territory.

Family emergency checklist

If someone claims a relative is in trouble:

1. Slow down.
2. Ask where they are and who is with them.
3. Hang up.
4. Call that relative directly.
5. Call another family member.
6. Use a family code word if your family has one.
7. Do not send money based only on a voice, text, photo, or video.

If your family has older relatives, consider agreeing on a simple verification phrase for emergencies. It does not need to be fancy. It just needs to be something a scammer would not know from social media.

Work or organization checklist

If a boss, pastor, board member, vendor, or coworker seems to ask for unusual money movement or private information:

• Do not act only by email or text.
• Verify by phone or in person using a known number.
• Follow normal payment approval steps.
• Be suspicious of “I am in a meeting and cannot talk” messages.
• Be suspicious of “keep this confidential” requests that bypass normal process.

Scammers love pretending to be authority figures.

The pause script

Use these words if you feel pressured:

“I do not handle urgent money or account requests without verifying separately.”

“I am going to hang up and call the official number.”

“I need to check this with another family member first.”

“I do not give passwords, codes, or payment information over unexpected calls.”

You do not have to win an argument. You just have to stop the scam from moving forward.

If you already clicked or paid

Do not panic, but act quickly.

Depending on what happened:

- Contact your bank or credit card company using the official number.
- Change passwords on affected accounts.
- Turn on multi-factor authentication if available.
- Report the scam to the platform, bank, or relevant agency.
- Tell a trusted person so you are not handling it alone.
- If workplace information was involved, notify the right person at work immediately.

Do not let embarrassment keep you quiet. Scams work because they are designed to work.

Educational-only note

This checklist is general educational information. It is not cybersecurity, fraud-prevention, legal, financial, or law-enforcement advice. It cannot guarantee that something is or is not a scam. When money, accounts, safety, or legal issues are involved, verify through official channels and seek qualified help as needed.