BUILD SAFELY · START HERE · 10 MIN READ

Stay safe from AI-powered scams

Spot phishing, fake voices and deepfakes, and lock down your accounts with a password manager, multifactor sign-in and updates.

Pass the check (4 of 5) online to earn the “Scam Spotter” badge:
https://digitalbuilders757.com/university/study/stay-safe-from-ai-scams

AI makes scams more convincing

Scammers use AI too. It writes polished messages with no spelling mistakes, copies a company's style, and can clone a voice from a short clip posted online. The US Federal Trade Commission warns about calls that sound exactly like a family member in trouble asking for money. The good news: the same few habits beat almost all of them.

The warning signs

- Urgency or fear: 'act now', 'your account will be closed', 'I'm in trouble, don't tell anyone'.
- Unusual payment: gift cards, wire transfers, cryptocurrency or payment apps to someone new.
- Requests for codes, passwords or remote access to your computer.
- Links or attachments you weren't expecting, even from a name you know.
- A voice or video that seems slightly off, or a caller who won't let you call back.

Stop, check, then act

Pause; scams depend on panic. Don't trust the voice or the caller ID: hang up and call the person back on a number you already have, or check with another family member. Agree a family 'safe word' for emergencies. Go to websites by typing the address or using your own bookmark, not the link in a message. Never share a one-time code with anyone who contacts you. In the US you can report scams at ReportFraud.ftc.gov.

Lock down your accounts

- Use a password manager to create a long, unique password for every account.
- Turn on multifactor authentication (MFA), starting with email, banking and social media.
- Keep your phone, computer and apps updated (turn on automatic updates).
- Think before you post voice and video clips publicly, and keep private details off public profiles.

Key terms

Phishing
A fake message (email, text, call or DM) that tries to get you to click, pay or share a password or code.

Deepfake
Fake AI-made media of a real person, often used to mislead.

Two-factor authentication (2FA)
A second check at sign-in, like a code from an app, on top of your password.

Voice cloning
AI that imitates a specific person's voice; needs that person's permission.

Password manager
An app that creates and remembers a long, unique password for every account.

Social engineering
Tricking people (not computers) into giving access, money or information, often with urgency or fear.

Try it: A 20-minute safety check

1. Turn on multifactor authentication for your main email account.
2. Install a password manager and change your most reused password to a unique one.
3. Agree a family safe word and tell the people who'd call you in an emergency.
4. Paste a suspicious message (with personal details removed) into an AI assistant and ask it to list the warning signs, then decide for yourself.

KNOWLEDGE CHECK

Stay safe from AI-powered scams

5 questions. Circle one answer for each; 4 or more correct passes. Answers are at the back.

1. You get a call that sounds exactly like your cousin, panicking and asking you to send gift cards. Best move?

A. Buy the gift cards quickly, it's an emergency
B. Ask the caller to prove it's them by telling you their home address and birthday
C. Send half now and half later
D. Hang up and call your cousin back on a number you already have

2. Which is a common sign of phishing?

A. Urgent pressure to click a link or your account will be closed
B. A message you were expecting from a friend about plans you made together
C. A receipt for something you actually bought, sent to your usual email address
D. Your bank's app showing your balance

3. Someone messages: 'I sent you a code by mistake, can you read it to me?' What do you do?

A. Read it to them, since they explained it was sent by mistake
B. Never share it; it's likely the key to your account
C. Share only the first half
D. Post it publicly so they can find it

4. Why use a password manager?

A. So you can use one easy password everywhere
B. It stops all spam calls
C. It creates and remembers long, unique passwords for every account
D. It's required to use AI tools

5. What does multifactor authentication (MFA) add?

A. Faster sign-in, because you no longer need to type a password at all
B. A backup copy of your files, saved to the cloud every night
C. A way to share your account safely with family members or coworkers
D. A second check, so a stolen password alone isn't enough

Official sites

FTC: Family emergency scams (including voice cloning): https://consumer.ftc.gov/scams/family-emergency-scams
CISA: Recognize and report phishing: https://www.cisa.gov/secure-our-world/recognize-and-report-phishing
CISA: Turn on multifactor authentication: https://www.cisa.gov/secure-our-world/turn-mfa

Last reviewed 2026-11-25. AI tools change fast; check each tool's own site for current features, plans and prices.

ANSWER KEY

Stay safe from AI-powered scams

1. D: Hang up and call your cousin back on a number you already have
Voices can be cloned. Call back on a known number; gift cards are a classic scam payment.

2. A: Urgent pressure to click a link or your account will be closed
Urgency plus a link is the classic pattern. Go to the site yourself instead of clicking.

3. B: Never share it; it's likely the key to your account
One-time codes are for you only. Sharing one can hand over your account.

4. C: It creates and remembers long, unique passwords for every account
Unique passwords mean one leaked site can't unlock your other accounts.

5. D: A second check, so a stolen password alone isn't enough
Even if a scammer gets your password, they still can't pass the second step.