

AI SCAM & DEEPFAKE SAFETY CHECKLIST



STOP IF SOMEONE —

- ☐ Asks for gift cards
- ☐ Asks for cryptocurrency
- ☐ Requests a password or security code
- ☐ Sends an unexpected login link
- ☐ Creates an artificial deadline
- ☐ Tells you to keep something secret
- ☐ Claims a family emergency
- ☐ Says you've unexpectedly won money
- ☐ Asks you to remotely install software
- ☐ Asks you to move the conversation off a trusted platform

PHOTOS & VIDEO: CHECK THREE THINGS

Source — who posted it?

Search — is a credible outlet reporting it?

Date — is this actually current?

FIVE QUESTIONS BEFORE CLICKING

Do I know who sent this?

Why are they creating urgency?

Are they asking for money or information?

Can I verify this another way?

What happens if I don't click?

WHEN IN DOUBT: STOP, VERIFY, CALL SOMEONE YOU TRUST.

THE FAMILY EMERGENCY PROTOCOL

A scammer needs only a few seconds of recorded voice to clone a child or grandchild. The defense is not technical. It is a plan your family agrees to before the call comes.

STEP ONE – AGREE ON THIS TODAY

CHOOSE A FAMILY SAFE WORD.

A word or phrase only close family members know. Not a pet's name, not a birthday, not anything posted online. If somebody calls claiming an emergency, ask for it.

WRITE IT HERE (THEN KEEP THIS PAGE PRIVATE)

STEP TWO – WHEN THE CALL COMES, IN THIS ORDER

- 01 ASK FOR THE FAMILY WORD.
- 02 HANG UP.
- 03 CALL THE PERSON DIRECTLY.
- 04 CALL ANOTHER FAMILY MEMBER.
- 05 NEVER SEND MONEY UNDER TIME PRESSURE.

THE FIVE SENTENCES THAT SHOULD END THE CALL

"Don't tell anyone."

"Send it right now."

"I'm in jail."

"I need gift cards."

"I can't talk long."

