AI SCAMS & DEEPFAKES

Quick Safety Guide

STOP

Don't respond right away.

VERIFY

Contact the person or organization another way.

DON'T CLICK OR PAY

Avoid suspicious links and urgent payment requests.

REPORT

Alert the real company, bank, platform, or a designated reporting service.

COMMON SCAM RED FLAGS

- Urgency
- Secrecy
- Unexpected requests for money, gift cards, wires, or crypto
- Requests for codes or personal information
- Pressure to click a link or attachment
- A silent and/or unusual call from an unknown number

AI FAKES MAY INCLUDE

- A loved one's cloned voice or fake video call
- Fake bank, support, or work messages
- Images or videos with odd hands/teeth, strange text, mismatched lighting, off lip-sync

PROTECT YOURSELF

- Turn on two-factor authentication and use unique passwords
- Share less online, and be careful with sensitive details
- Pause and verify unexpected/unknown messages, calls, or videos before trusting them

VERIFY ANOTHER WAY

- Hang up and call back using a number you trust, or wait for them to call you again
- Use contact information from the official company website
- Ask something only the real person would know
- Use a family code word or safety question
- Reverse search suspicious images

WHERE TO REPORT/GET HELP

FTC — All Scams:
reportfraud.ftc.gov | 1-877-FTC-HELP

FBI IC3 — Internet/Cybercrime:
ic3.gov

AARP Fraud Watch:
aarp.org/fraudwatch | 1-877-908-3360

Identity Theft:
identitytheft.gov

AI Literacy For All | ailiteracy-forall.netlify.app | ailiteracyforall@gmail.com