AI THREATS: A FAMILY GUIDE

Practical defenses against scams, fakes, and fraud you can put in place today

DO THIS TODAY: Set a family safe word: Pick a word no one would guess and that doesn't appear on any social media. If anyone calls in distress asking for money or urgent action — even if it sounds exactly like them — ask for the word. No word, no action. Hang up and call back on a number you already have saved.

Voice cloning

10–30 seconds of audio (TikTok, voicemail, webinar) is enough to clone a voice. Scammers use it for fake "grandchild in trouble" calls. Defense: the safe word, plus always call back on a known number.

AI phishing

Typos and bad grammar are gone. AI writes clean, personalized emails using details scraped from social media and breaches. New rule: verify the channel, not the content. Banks, the IRS, and your boss never need action in 10 minutes — urgency is the tell.

Romance & friendship scams

AI chatbots run long-con relationships at scale — months of daily messages, real-looking photos, eventually a crisis requiring money. The signal isn't "this feels fake." It's: never met in person or on a live unscheduled video call, and money or crypto eventually comes up.

Deepfake images & video

Anyone can generate fake explicit images of a real person from ordinary social media photos. Tell kids: it isn't your fault if it happens — tell me, you're not in trouble. Also: shocking videos of public figures or family aren't evidence. Wait for confirmation from a second source.

The information firehose

AI-generated articles and images flood social feeds. Slow down before sharing anything that makes you angry. If a story only exists on one site you've never heard of, it's probably not real. Reverse-image-search photos that seem too perfect.

Account security is the entry point

Most attacks succeed because email gets compromised first. Use a password manager (every account unique) and turn on two-factor authentication using an authenticator app or hardware key — not text messages. Email is the master key to your life; protect it accordingly.

FIVE FAMILY RULES

- **Safe word.** Required for any urgent request involving money or action.
- **Call back on a known number.** Never the number in the message. Never the link in the email.
- **Pause before sharing or reacting.** Anything emotionally charged deserves a second source first.
- **Two-factor everything.** Email and banking first. Authenticator app or hardware key, not SMS.
- **Tell each other.** If something feels off — a strange message, a new online relationship, an image of you online — say so. No judgment, no blame.

When in doubt: slow down, hang up, verify through a channel you already trust.