AI-Related Scams

Deepfake Technology

💭 Picture this

A user received a phone call where the caller's voice sounded exactly like a beloved family member — anxious, breathless, and right off the bat asking for help and money. The person who received the call felt their heart pounding and was about to reach for their credit card, but then they remembered a family rule they had previously agreed upon. The call recipient hung up the unsolicited call, then contacted their family member as usual, laughing with relief when they answered calmly, reassuring them they were fine.

This type of trick is becoming more common because, whereas previously creating compelling fakes required specialists and expensive equipment, now easily accessible apps can rapidly mimic voices or swap faces—replacing one person's face with another in a photo or video—with just a few clicks.

Let's review the definitions of "AI" and "Deepfake."

Artificial Intelligence, or AI, is software that analyzes large sets of data, learns the patterns within them, and then applies those patterns to perform tasks that usually require human thought, such as understanding language, recognizing images, making predictions, or generating text and speech. In simple terms, AI identifies patterns across many examples and uses that knowledge to deliver effective results, all without needing a person to create each detail.

What is a Deepfake?

It is a fake image, voice, or video created by a specific type of AI called “deep learning.”—This kind of AI can analyze a wide range of real photos, videos, or voice recordings to learn how a person looks or sounds, then uses that knowledge to produce a strong imitation of an individual. In other words, a deepfake is a synthetic (not real) piece of media designed to make it seem as if someone said or did something they did not.

Despite this, “Deep Learning” has demonstrated itself as revolutionary when used for positive purposes, such as:

- In medical image diagnosis, it helps doctors identify problems in X-rays, CT scans, and MRIs by quickly and accurately highlighting abnormalities, so issues can be detected earlier and treatment can begin sooner.
- In systems like phone transcription, voice assistants, and real-time translation, deep learning is employed to convert spoken words into text and facilitate natural responses, making devices more accessible for people with diverse needs.

When Voices and Faces Lie

Humans naturally rely on sight and sound as quick signals of truth. When we hear familiar voices or see familiar visuals, our instinct is to trust and respond, even in unfamiliar or strange situations. Deepfakes exploit this by producing voices and images that match our expectations, which weakens our instinctive doubt of **“does this feel right?"**

Where Do Deepfakes Get Their Information From?

It draws on references from real people collected from different sources.

- **Publicly shared content:** photos and videos people post on social media profiles, video sites, and forums.
- **Broadcast and published media:** news clips, interviews, podcasts, and TV or movie footage.
- **Open datasets and archives** that researchers and companies share so others can study or build computer programs.
- **User-provided samples:** short voice clips or photos that someone uploads to online services or that a scammer gathers directly from their targets.

What Happens Next? The AI software then processes the available content in three stages.

1. **Gathering Examples,** the system needs a lot of media showing different angles, expressions, and speech so it can see the usual ways people look, talk, and communicate.
2. **The AI looks for patterns in the data it has collected:** how a smile widens, how voice pitch varies, or what typical word sequences look like. It learns by identifying consistent rules across the many references it has been trained on.
3. **Create imitations.** Once the patterns are learned, the AI can combine them to generate new content that follows the same rules—creating an image that looks real or audio that sounds just like a person's voice, even if it is artificial.

AI-Voice Cloning Scam

It can produce a highly convincing replica of someone's voice from just a short recording. From harmless prank calls to elaborate frauds that mimic friends, family, or officials. These scams are usually carried out through phone calls or VoIP (Voice over Internet Protocol), which is internet-based calling that works like a phone but doesn't depend on traditional landlines.

Impersonated Family Emergency Call

A persuasive call or voicemail from someone who sounds like a family member, close friend, or trusted contact mentions an urgent matter—jail bail, hospital bills, or travel costs.

—Highest emotional leverage; people tend to respond quickly to family distress, making this approach very effective.

Protective Steps

- **Shared-detail check:** Agree on two simple facts beforehand. Example: the last thing you did together and the color of the streetlight outside their house. If someone calls claiming to be that person, ask for both facts. If they can't provide them exactly, don't trust the call.
- **Callback validation:** Tell the caller you'll call back, then ring the person using the saved number in your phone. If they don't answer, contact another trusted relative before sending money. Do not use any number the caller provides.
- **Two-hour delay rule**: Make a household rule to wait at least two hours before sending money for any urgent request. Use that time to check facts and call other family members.

Fake Bank/IRS Verification Call

The attacker mimics a bank rep or financial advisor to claim suspicious activity or overdue taxes, then asks for account numbers, PINs (Personal Identification Numbers), or transfer authorization "to a safe account."

—**Leverages authority** and fear of legal/financial consequences to extract credentials.

Protective Steps

- **Secure verification for official-sounding callers:** Ask for a reference number, then call the bank or agency yourself using the phone number from official mail or the organization's website. Record the reference number and confirm the call was legitimate before acting.
- **Require written follow-up:** Insist that any urgent notice be sent to your known physical address or your account email before you respond. Do not act on voice claims alone.
- **Two-person confirmation:** Require a second independent person to confirm requests about accounts or taxes—example: spouse, financial advisor, or trustee.
- **Micro-test question:** Ask for a small, non-sensitive detail only the real institution would know, e.g., the last four digits of an account you hold with them. If the caller hesitates or answers incorrectly, escalate and stop the request.
- **Official-channel rule:** Only use the bank's official voice-authentication system or secure messaging app for sensitive actions. Do not complete transactions if the communication did not happen through that official channel.

Recorded-Consent Wire Transfer Trick

A trusted contact's voice is used to persuade the individual to approve a payment or confirm a code verbally; the recording is then employed to convince banks or payment services that consent was granted, enabling fraudulent transfers.

—**Directly converts voice cloning into actionable authorization;** exploits institutions that accept verbal consent.

Protective Steps

- **Voice passphrase for callers:** Require a pre-agreed verbal passphrase that includes the full date and a token. Example: “April 21 — blue tulip.” If the caller refuses or the recording is unclear, cancel the request. Do not act on incomplete or muffled passphrases.
- **One-time authorization codes:** Require a bank-generated, single-use code sent to the account holder’s device before any transfer is made. Never read or give out the code during a call. Treat spoken codes as insecure.
- **Transaction limits and written confirmation:** Set a small daily transfer limit and request written confirmation, such as email or text, from the verified account holder for amounts over a certain threshold, like $200. Do not process large transfers without this written approval.
- **Hold-and-verify for suspicious transfers:** Ask your bank to place suspicious transfers on temporary hold for 48 hours after voice authorization.

AI-Generated Face Swapping Scam

Face-swapping is a technique that replaces one person's face in a photo or video with another person's face, making it look like the second person is the one pictured or speaking. Scammers and creators use it to make someone appear in scenes they were never in; it can be done to still images, edited video clips, or live video.

Community Leader Video

Social Post from a Trusted Public Figure

A short video featuring a local pastor, club president, or neighborhood organizer is shared in a group on platforms like Facebook or sent via text messages, appealing for urgent support, event funding, or personal assistance.

Protective Steps

- **Verify through a trusted group member by contacting someone else in the group, not the group admin.** Choose someone you know is on the mailing list or receives the group's messages, and ask if they saw it and what they think of the request.
- **Request a time-stamped public gesture.** Ask the person "in question" to send a photo or a short video of themselves holding a piece of paper with today's date and the group name.
- **Escalate to group moderators:** Alert the group admin or moderators with a short message. Say something like — Possible impersonation — please verify and ask the platform to review the post.

Healthcare-Provider Video

Telehealth App or Social Clip Shared by a Doctor or Nurse

A recorded or live video, where you can see and hear people instantly (with a slight delay), shows a physician, clinic staff, or home-care worker referencing urgent medical tests, prescription payments, or insurance actions that need to be completed quickly.

Protective Steps

- **Verify clinic messages through official channels:** Only accept instructions or billing links sent through the clinic's patient portal or their official secure email. Ignore requests that arrive via direct messages on social media, texts from unknown numbers, or unfamiliar links.
- **Ask for official paperwork:** Request a scanned note on clinic letterhead when they mention something is urgent. A legitimate clinic can scan and send its own notes.
- **Confirm videos or codes by phone:** Call the clinic using the phone number on your appointment card or your insurer's provider directory. Read the exact words or numbers shown in the video and ask the staff if they recognize or generate them.
- **Hold payments and prescriptions until confirmed:** Ask the pharmacy or clinic to delay charging or filling a prescription if something seems sudden or questionable. Request a mailed statement or written confirmation before making any payment.

Home-Service Worker Video

Messages from Contractors, Utility Workers, or Delivery Drivers

A face-swapped clip in an app or messages from someone claiming to be your utility company, cable technician, or delivery person, saying service will stop unless you pay now or give access.

Protective Steps

- **Demand dispatcher confirmation:** Request to be transferred to the company dispatcher, then verify the worker's name, badge number, and job order before allowing them entry or making payment.
- **Use single-use appointment codes:** Coordinate with regular service providers to issue one-time codes that workers must display on their devices; contact the company to verify the code in real time.
- **Check a live close-up of ID:** Request a close-up video of the company ID card (not just their face) and call the company number on your bill to verify the badge number.
- **Refuse remote access without an in-person tech:** Never unlock doors or give remote access—control of a device over the internet—based solely on a video request. Always ensure a technician is pre-scheduled and a written work order is in place before allowing entry or access.

AI-voice cloning and face-swapping videos may appear realistic, but often contain subtle inconsistencies that can reveal manipulation. Use these clues to quickly identify altered audio or video.

Spotting Deepfakes

General Visual Cues 🔍

- ➔ *Unusual blinking or mouth movements. Eyes blink too slowly.*
- ➔ *Stiff or floating head. The head or face looks slightly disconnected from the background, or moves unnaturally.*
- ➔ *Blurry edges around the face. The hairline or jaw looks smudged or as if it were cut out from somewhere else and pasted into the video.*
- ➔ *Lighting mismatches. The face is lit differently from the rest of the scene, either too brightly or with odd shadows.*
- ➔ *Watch for quick flickers or tiny stutters in the face—like a brief jump or a split-second change.*

Visual Content Clues

—Look at what the video actually shows

Polished but seemingly out of place: Highly smooth, dramatic, or cinematic videos from a private account or direct messages—especially if they don't match the person's usual tone.

Mouth and sound out of sync: You notice a word being spoken before the lips move, or see the lips move without an accompanying sound.

Minor background details like props, badges, paperwork, or signs that seem slightly off—such as misspelled names, incorrect logos, inconsistent fonts, or layout errors (like cut-off images or misplaced buttons)—can reveal that the scene has been edited.

Audio and Speech Clues

—Listen carefully to the small, odd sounds in the voice; they can tell you if a clip is fake.

Mechanical or hollow sound: the voice may seem thin, tinny, or as if it's coming through a speaker instead of a real person.

Unnatural breaks, repeated words, sudden pauses, awkward hesitations, or the reuse of the same short phrase can indicate editing.

Words that don't fit the person: if their tone, choice of words, or level of formality feels different from how they are used to express themselves (e.g., using unfamiliar slang or a different accent).

Context and Social Media Account Clues

—Look at the bigger picture around the message

Watch for sudden changes in who's contacting you online. If a friend's account that usually shares family photos starts posting urgent pleas or money requests, treat it with caution — scammers often take over accounts or make lookalike profiles to ask for help.

Be extra careful with brand-new profiles that have very few followers but post polished videos, as these are commonly fake.

Pay close attention to how the person asks you to respond. If they push you to use a new payment link, a different app, or an unfamiliar message thread instead of your usual means of communication, pause and verify by calling them on the phone number you already have.

Deepfake Detection Tools

Think of these tools as a quick "second opinion" you can use whenever a video, call, or message seems off.

Trend Micro Check
This application has over 2000 ratings and is rated 4.6 out of 5 stars in app stores. Users praise its ability to block scam calls, filter suspicious texts, and check links, images, and even fake video calls.

What it does: Helps you check if news, images, or videos are real or fake.

How to use it: Download the free app from the App Store (iPhone/iPad) or Google Play Store (Android). Copy and paste a link, or upload a suspicious image or video.

Why it's useful: Gives a quick "real or fake" style answer, so you don't have to guess.

Resemble AI – Voice Deepfake Detector
It is not available as a mobile app; it operates directly through their website. It's widely cited in cybersecurity circles for detecting fake voices.

What it does: Detects fake voices in phone calls or recordings (like scam calls pretending to be a family member).

How to use it: Go to their website, upload or record the audio, and the tool will analyze it.

Why it's useful: Protects against one of the most common scams targeting older adults—fake emergency calls.

📌 Key Resources for Staying Updated

In the U.S., you can trust organizations like AARP, the National Council on Aging (NCOA), and the FBI's Internet Crime Complaint Center (IC3) to stay informed about AI and deepfake scams.

1. **AARP Fraud Watch Network**
   https://www.aarp.org/money/scams-fraud/ai-scams/
   It consistently issues alerts about new scam methods, including AI-driven fraud. Their 2024 survey revealed that adults aged 50 and older are very concerned about AI scams but often lack a clear understanding of how they operate

2. **National Council on Aging (NCOA)**
   https://www.ncoa.org/article/understanding-deepfakes-what-older-adults-need-to-know/
   It offers detailed instructions on how to respond if you believe you've been targeted.

3. **FBI Internet Crime Complaint Center (IC3)**
   https://www.ic3.gov/
   It monitors national scam trends, including AI-enabled fraud. Their 2023 report recorded $3.4 billion in elder fraud losses, a 14% rise from the previous year. Likewise, in this portal, users can submit complaints directly, aiding law enforcement in identifying patterns.


Connecting Generations
Cyber-Seniors™


be well
ILLINOIS


aetna


BEYOND
FORCE


trail
TOTAL RETIREE ADVANTAGE ILLINOIS

DEFINITIONS

***Apple App Store** and **Google Play Store** are online marketplaces on iPhones/iPads and Android devices where you can browse, download, buy, and update apps and games. They also offer reviews, ratings, app descriptions, and developer information to help you choose safe, compatible software.

- **Android** is a Google-made operating system for smartphones and tablets, managing apps, settings, and features. It allows app downloads from Google Play. Brands like Samsung and Pixel use Android.
    - **Operating system** (OS) is the main software that runs a computer, phone, or tablet. It manages apps, files, and hardware (like screen, keyboard, and Wi-Fi) so the device works and you can use programs easily. Examples: Windows, macOS, Android, iOS.

***Broadcasting** is sending the same audio, video, or data from one source to many recipients at once.

***Content** is any information you create or see online — words, photos, videos, audio, posts, or files.

***Cut-off image** is a picture where part of it is missing or not shown because it's been cropped, sized too small, or positioned so the edges are outside the viewing area.

***Cybersecurity** is the practice of keeping computers, phones, and online accounts safe from theft, damage, or unwanted access.

***Data set** in artificial intelligence is a collection of examples that a computer uses to learn. Each example is a piece of information—like a photo, a line of text, a number, or a label (e.g., "cat" or "not cat"). The dataset shows the AI many instances, so it can recognize patterns and make predictions.

***Forum** is an online message board where people post questions, share information, and reply to each other—organized into topics or threads so conversations stay grouped and easy to follow.

***Layout error** is a problem with how text, images, or elements are arranged on a screen, page, or document that makes it look wrong or hard to use—examples: overlapping text or columns that don't line up.

***Live video** is a video you watch as it happens—like a video call or livestream—so you see and hear events in real time (usually with a short delay), not a pre-recorded clip.

***Mechanical sound** (in video context) is any noise from machines or moving parts recorded on a video — e.g., clicks, whirrs, motor hums, or rattles from cameras, props, fans, or nearby appliances — that can distract from dialogue or the intended audio.

***Mobile app** is a small program you download and use on your phone or tablet to do things like message friends, check the weather, shop, or watch videos.

***Phone transcription** is turning the words spoken on a phone call into written text so you can read what was said.

***PIN** is a short code or number (often 4–6 digits) you use to unlock an account, phone, or card—keeps access secure.

***Podcast:** is a series of audio episodes you can listen to on demand, usually focused on a theme or host conversation.

***Prop** in video creation is any physical object an actor holds or uses on screen (like a phone, book, or cup) that help tell the story or make the scene look real.

***Real-time translation** is when spoken words are translated into another language instantly, so you can understand someone who speaks a different language during a conversation or live event.

***Social media** are websites and apps that let people create, share, and interact with posts, photos, videos, and messages—connecting friends, communities, and the public in real time. Common examples are:

- **Facebook** — staying in touch with family and seeing photos.

- **WhatsApp** — sending messages and voice clips to friends.
- **YouTube** — watching how-to videos and news.
- **Instagram** — viewing family photos and short videos.
- **Nextdoor** — neighborhood news and local recommendations.

***Social media post** is a message, photo, video, or link you share on a website or app (like Facebook or Instagram) so friends, followers, or the public can see and respond.

***Token** is a small digital key or code used to prove your identity or allow access to an account or service, like a one-time code from an app or device you enter to log in securely.

***Voice assistance** is a tool you talk to (like Siri or Alexa) that listens to your voice and answers questions, follows commands, or helps with tasks.

***Voice clip** is a short audio recording of someone speaking, saved as a file you can play, send, or share.

***Video sites** are websites or apps where people watch, upload, and share videos (examples: YouTube, Vimeo).

- **Website** is a collection of pages on the internet you visit with a browser (like Chrome or Safari) to read information, see photos or videos, use services, or contact people.

- **Upload** means sending a file (like a photo, video, or document) from your device (phone or computer) to the internet or another person's device so others can see or use it.

***Wire transfers** electronically move money between accounts. You provide the recipient's details, and the bank sends the funds directly. They are usually final and irreversible, so they should only be used with verified recipients.