

SPOTTING AI DEEPFAKES: PRACTICAL GUIDELINES AND RED FLAGS



Use this job aid to learn more about common giveaways that can alert you to the presence of a deepfake, and some ways to check.

Detecting AI deepfakes, especially when used for scams, requires vigilance and attention to detail. Typical giveaways are anatomical, sociocultural, or functional implausibility, such as extra fingers, unusual positions or activities, and unlikely interactions. For videos, movements will typically be unnatural, with mouth or eye movements that don't align with the audio. Stylistically, AI-generated images and videos are often hyper-realistic in the fore and backgrounds. There is a lack of dimension.

COMMON GIVEAWAYS THAT CAN ALERT YOU TO THE PRESENCE OF A DEEPFAKE

- **Visual anomalies**

- Facial inconsistencies: Look for unnatural facial movements, like blinking too little or too much, inconsistent lip-syncing, or awkward expressions.
- Lighting issues: Check for inconsistent lighting or shadows on the person's face compared to the background.
- Blurriness or artifacts: Deepfakes may display subtle blurring around the edges of the face, hair, or other areas, especially during fast movements.
- Unnatural eye movements: The eyes might appear misaligned or fail to track properly in the context of the video.
- Skin texture or flickering: AI-generated faces may have overly smooth skin, flickering patches, or unnatural transitions in texture.

- **Audio clues**

- Speech cadence: Listen for unnatural pauses, robotic intonations, or inconsistencies in speech patterns.
- Background noise: Deepfake audio might lack natural background noise or have mismatched acoustics compared to the setting shown in the video.

- Emotionless voice: The voice might sound flat or lack genuine emotion, especially in emotional or high-stakes situations.
- **Behavioral red flags**
 - Unusual requests: Be cautious if the person in the video/audio is asking for sensitive information, money, or urgent action, especially if it's out of character.
 - Inconsistent context: Does the video or audio seem out of place for the person's usual style, tone, or typical communication method?
- **Metadata and file analysis**
 - File properties: Check the file's metadata for inconsistencies, like unusual creation dates or suspicious editing software.
 - Low quality: Deepfakes are often produced with intentionally low video or audio quality to hide imperfections. A video or audio file with unusually low resolution or quality might be a red flag.

WAYS TO CHECK IF A VIDEO OR AUDIO FILE IS REAL

- **Cross-verify information**
 - Contact the source directly: If the video or audio appears to be from a known person, confirm it through a separate communication channel.
 - Check for inconsistencies: Verify details like names, dates, locations, or facts mentioned in the video/audio.
- **Use AI detection tools**
 - Use deepfake detection tools and software. These tools analyze videos or audio for signs of manipulation. Examples include Microsoft Video Authenticator, Deepware Scanner, and Sensity AI.