HOW TO PROTECT YOURSELF FROM DEEPFAKE ATTACKS

Verify requests with other channels

If you receive an unusual request through video, audio, or phone calls—especially involving financial transactions or sensitive actions—always verify it through a second method, such as a phone call to the person or an official company email.

Look for signs of manipulation

Deepfakes, while highly realistic, may still show subtle signs of tampering. Watch for mismatched lip movements, unnatural facial expressions, or audio that doesn't quite match the speaker's mouth movements.

Use multi-factor authentication

To protect against deepfake impersonation attacks, ensure that any critical actions, such as money transfers or accessing sensitive systems, require multi-factor authentication. MFA adds an extra layer of security beyond verbal or video confirmation.

Establish verification protocols

Create robust steps or processes that help you validate legitimate communications, especially for critical transactions. These protocols help ensure that impersonation attempts fail.

Limit availability of voice & video data

Reduce the amount of publicly available video and audio of key executives or employees to limit what attackers can use to create deepfakes. Avoid unnecessary public speeches or recordings that could be misused.

Use deepfake detection tools

Deepfake detection tools can help identify whether a video or audio file has been manipulated. These tools analyse visual and auditory cues to flag content that may be artificially created.

QUICK TIPS

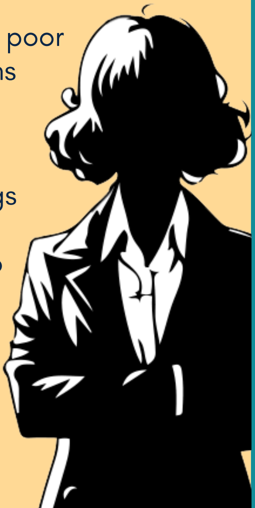
Verify through multiple channels—double-check all video or audio requests by contacting the person through a known, trusted method.

Use MFA—require additional verification, especially for financial or high-stakes actions.

Watch for signs—subtle issues like poor lip-syncing or odd facial expressions can be indicators of deepfakes.

Limit public voice/video data—reduce publicly available recordings of executives or key employees to limit material that could be used to create deepfakes.

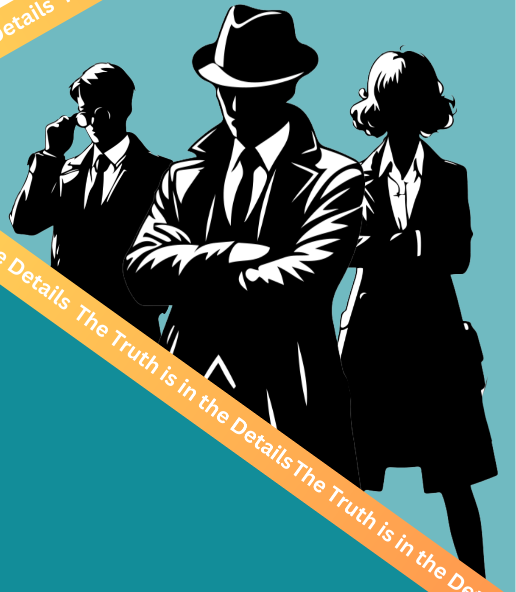
Establish code words—use internal security measures like code words for verifying important requests.



Cyber Security Awareness Month 2024

Look Closer.
Think Smarter.

The Truth is in the Details The Truth is in the Details The Truth is in the Details The Truth is in the Details



The Truth is in the Details The Truth is in the Details The Truth is in the Details The Truth is in the Details

Protect Yourself from Deepfake Threats

WHAT ARE DEEPFAKES?

Deepfakes are synthetic media—video, audio, or images—created using artificial intelligence to mimic real people.

By using deep learning algorithms, attackers can generate convincing fake videos or audio that appear to show someone saying or doing something they never did. Deepfakes are increasingly being used for fraud, misinformation, and impersonation.

Common types of deepfake attacks

Deepfake Audio

Attackers clone a person's voice using AI and use it in phone calls or audio messages to impersonate them. This can trick victims into transferring money, sharing confidential information, or granting access to systems.

Deepfake Video

Cybercriminals create realistic videos of someone, typically a public figure or executive, to spread false information, damage reputations, or manipulate business decisions.

Deepfake Impersonation

Attackers may impersonate executives or business leaders to deceive employees into making wire transfers, sharing sensitive information, or performing critical actions.

Social Media Misinformation

Deepfakes can be used to spread false or misleading information on social media platforms. These videos can manipulate public opinion by making it appear that someone said or did something inflammatory or controversial.

REMEMBER

Deepfakes are becoming increasingly sophisticated, but by using verification protocols, multi-factor authentication, and deepfake detection tools, you can protect yourself and your organisation from falling victim to these deceptive tactics.

Stay vigilant and always verify suspicious communications, especially those involving critical decisions or sensitive information.

RED FLAGS OF DEEPFAKE ATTACKS

- **Unusual or urgent requests** from high-level executives that deviate from normal communication patterns.
- **Audio or video** that seems slightly "off," such as mismatched timing between audio and lip movement.
- **Emails or calls** with poor grammar or odd phrasing, even if the video/audio appears to come from a legitimate source.
- **Requests** for financial transactions or sensitive data that seem out of place or overly urgent.