How to identify Deepfakes Cheat Sheet

Deepfakes are fake videos, audio, or images made using AI to look and sound like real people. They can make anyone appear to say or do things they never actually did.

How to Spot a Deepfake

Look for Weird Movements

Watch for unnatural facial expressions, awkward blinks, or odd lip-syncing. These subtle glitches are common in deepfakes.

Check the Lighting and Shadows

Real videos have natural lighting and shadows. Deepfakes often have lighting that doesn’t match the background or other objects

Audio Mismatches

Is the voice slightly off? Does the person’s mouth not match the words? These are signs of deepfake audio manipulation.

Too Good to be True?

If a video seems shocking, scandalous, or too sensational, take a step back. Deepfakes are designed to provoke strong emotions.

How to Protect yourself from Deepfakes

Verify the Source

Don’t trust videos just because they’re viral. Check if the content comes from a reliable, trustworthy source.

Cross-Check the Information

If you see a controversial or surprising video, search for it on multiple trusted platforms to see if it’s reported elsewhere.

Report Suspicious Content

If you suspect a video is fake, report it to the platform you found it on (YouTube, Facebook, etc.). Help stop the spread of misinformation.

Protect Your Digital Identity

Use strong passphrases and enable Multi-Factor Authentication (MFA) on your accounts to prevent unauthorised use of your data for deepfake creation.

Cyber Security Awareness Month 2024

Look Closer. Think Smarter.

e Details The Truth is in the Details The Truth is in the Details The Truth is in th

How to identify Deepfakes Cheat Sheet

Deepfakes are fake videos, audio, or images made using AI to look and sound like real people. They can make anyone appear to say or do things they never actually did.

Protecting Yourself from Being Deepfaked

Be Cautious with Your Digital Presence

Limit the personal content (photos, videos, and audio) you share online, especially in public forums or social media. This helps prevent cybercriminals from collecting enough data to create a deepfake using your likeness.

Strengthen Your Security

Enable Multi-Factor Authentication (MFA) on your accounts to add extra layers of protection in case someone tries to use a deepfake to gain access.

Use Strong Passphrases: Avoid simple or predictable passwords. Use longer passphrases and change them regularly to prevent unauthorised access.

Monitor Your Online Presence

Periodically check the internet for mentions of your name or images using tools like Google Alerts or other identity monitoring services to see if your likeness is being misused.

Educate Yourself and Others

Stay informed about new developments in deepfake technology. Educating yourself and spreading awareness in your community or workplace can help prevent deepfake scams.

Tips for the Workplace

Verify Video Calls

Before responding to sensitive requests on a video call (especially financial or security-related), double-check the identity of the caller, even if they look and sound familiar.

Implement Strict Verification Policies

For critical actions like approving transactions or sharing sensitive information, consider implementing voice or video verification procedures that are difficult to manipulate, even by deepfakes.

e DetailsThe Truth is in the Details The Truth is in the Details The Truth is in the Details The Truth is in th

Cyber Security Awareness Month 2024

Look Closer. Think Smarter.