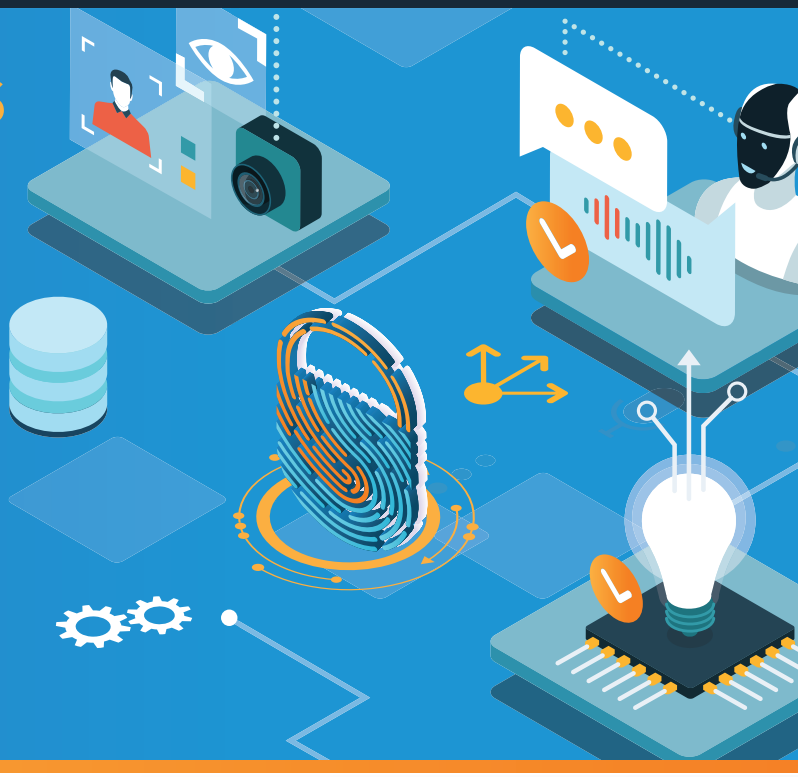
DEEPFAKE: FUNNY PRANKS OR DISRUPTIVE FRAUD?

Deepfakes are altered images, audio recordings and videos that have been constructed to make a person appear to say or do something that they never said or did.

While fake or "doctored" images have a long history, technology today helps fraudsters create deepfake video and audio that are very difficult to detect. And because social media provides a large platform for this to reach huge audiences, it is often portrayed as breaking news by duped media. Learn about this type of fraud and how it can impact you.



HOW IT WORKS

The word "deepfake" is a mash-up of the words "deep learning," which is associated with machine learning and artificial intelligence (AI), and an old-fashioned reference to something being "fake."

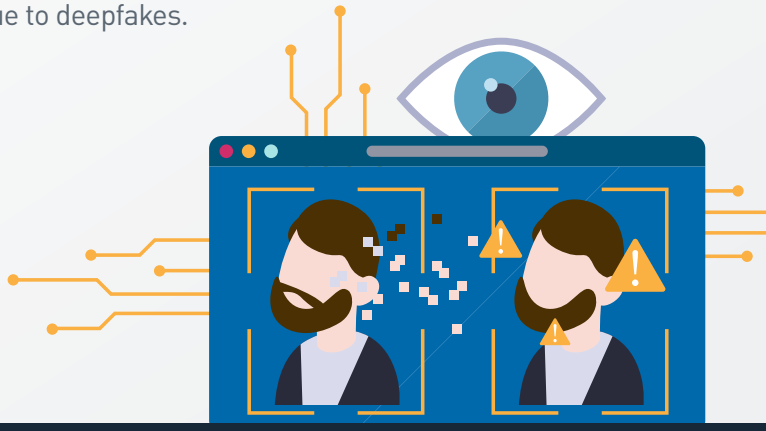
Fraudsters start by taking advantage of an abundance of content available of a specific individual for free from online news outlets and social media, including consumer-generated video and photos. The fraudster manipulates that content into a new image or voice recording with the subject saying or doing something that they never did or that is out of character for them.

The process itself is very technical: Deepfakes are generated by neural networks, using artificial intelligence and machine learning algorithms to imitate real humans. However, an advanced degree is not required to create deepfakes thanks to readily available software that enables people with basic computer skills to become deepfake creators. Quality of the final product may reflect skill level, but may also improve over time due to machine learning, not necessarily human learning.

WHO GETS HURT

Those most often victimized are politicians, celebrities and high-level business executives, due in part to the availability of images, videos and audio recordings of them on the internet. Sometimes the goal of the fraudster is a funny prank that drives social media engagement. But other times the goal is to spread misinformation, ruin reputations or inflict financial harm.

Don't assume you won't be impacted by deepfake if you are not a Hollywood or Washington, D.C., socialite. An internet search on deepfakes highlights a wide array of fraud. For example, workers at corporations have been duped into taking inappropriate actions when instructed by a deepfake of their CEO instructing them to do so, sometimes resulting in significant costs and job losses. At a minimum, you may be misinformed about an important topic or person due to deepfakes.



HOW TO DETECT

Deepfake images, audio and video can be so well done that it is very difficult to determine a fake. Because deepfakes are synthesized using high tech, detecting them with high tech and algorithms is key. In general, here are a few things to be on the lookout for:

- Poorly synced sound and video, especially with lip movement
- Blurriness where the face meets the neck, hairline or blurry teeth
- Box-like shapes or other cropped effects around the mouth, eyes and neck
- Face discolorations
- Irregular blinking or no blinking
- Asymmetries or inconsistencies in clothing, glasses, jewelry, ears and fingers
- Movements that are unnatural
- Exaggerated, unrealistic or not in-character behavior
- Changes in the background and/or lighting, including monotone or out-of-focus backgrounds
- Lower-quality sections in the same video

ACTIONS YOU CAN TAKE

Challenge what you see and hear, especially if the message is highly unusual for the person.

Be cautious about video and photos that you share via social media.

Confirm the authenticity of the message, especially before taking action.

Do not deviate from routine controls. If you receive a phone call from a superior with a highly unusual request, follow company protocols to double-check the order before executing.

TAKE ACTION

CON PDF 0820-084

PNC BANK