V.F. McNeil INSURANCE
Since 1886

The right insurance from day one®
www.vfmcneil.com

Cyber Bytes: What Is a Deepfake?

Deepfake technology is advancing at a rapid rate. The applications are changing how people work, play, shop, learn, travel, interact, do business and care for themselves. Learn about good and bad deepfakes, and ways to avoid falling into a deepfake trap.

What is a deepfake?

According to the U.S. Government Accountability Office, "deepfake" is a term combining artificial intelligence (AI) "deep learning" and "fake."

Deepfakes are realistic images, sounds and movements created using artificial intelligence and machine learning. Deepfake creators use technology to replace an actual person's image or voice with an artificial likeness or voice.

There are many websites dedicated to deepfake productions and the deepfake technology used to make them, some of which are on the dark web.

This technology, more broadly known as synthetic media, can have positive applications. But as with any benevolent artificial intelligence, a malignant fake is never far behind.

The good	The bad
Nonplayer characters orient, entertain and inform gamers.	Nonplayer characters seem helpful but trick users into giving out personal information.
Virtual reality presentations use a historical character's likeness for immersive learning.	Virtual reality presentations use the likeness of a character to spread misinformation.
Videos acted in real time deliver an interactive conversation with a historical or present-day figure to create unique learning.	Videos acted in real time deliver political messaging designed to mislead voters or spread disinformation.
AI chatbots offer Q&As for instant tailored information about a product or service.	AI chatbots pose as Q&A sessions but they're hosted by threat actor websites. The chatbots trick consumers into giving personal information.
AI generates voice-overs in your voice to narrate and edit typed presentations.	AI generates voice-overs in your voice to fake and spoof your identity.
AI creates synthetic data about how to drive vehicles autonomously or test products without harming animals or humans.	Threat actors corrupt synthetic data for autonomous vehicles or product testing to skew results or create chaos.
AI-generated personal avatars replicate your voice and likeness for meeting, working or socializing in the digital space.	AI-generated personal avatars hack your voice and likeness to scam others or defame people in the digital space.
Biometric security, like facial and voice recognition, uses AI to secure and validate personal data.	AI voice and face generators bypass security measures using deepfake technology to hack personal data.
HR can use AI-generated simulation to train employees on safety, workplace harassment and other topics.	AI-generated simulation can be used to fake an interview with HR to get hired and access confidential data and systems.

What can you fake?

Anything that has data associated with it can be faked. This includes:

- Voices
- Videos
- Photos
- Text
- Art

Deepfakes can be automated using various technologies such as:

- 3D face tracking
- Video
- Voice and sound recording
- Animation
- Decoders
- Computer graphics
- Image capturing and rendering
- Deep mirror networks

Some AI applications can complete stories and engage in interactive texts. Other AIs can generate images based on text suggestions.

And what used to be a complex process to fake a video image is now an automated process, achieved by a single individual and a computer.

An algorithm does most of the heavy lifting, automating the process to render a fully formed deepfake character. With enough images of a person from random directions under different lighting conditions, a fully fabricated avatar can be generated.

Dealing with a suspected deepfake

Not everything you see or hear is real. Here are some red flags to watch out for:

- Be on the lookout for glitchy or overly produced videos, voices or texts that don't look or feel right.
- If an individual or company unexpectedly contacts you with a request and you cannot verify their identity confidently, end the call. Then contact them through a trusted method.
- Be wary of videos that appear glitchy or pixelated. Mismatched lips, eyes, hairlines and chin lines can expose a fake.

- Look out for coughing or sneezing that appears out of sync with on-screen visuals.
- Exercise caution when sharing information digitally. Scammers won't like it if you ask to call them back and might even pressure you to act immediately, creating a sense of urgency.
- Watch out for robocalls. These targeted voice, text and messaging scams trick you into giving information using scare tactics or by spoofing a trusted product name.
- If you suspect a scam, end contact immediately. Go directly to the source to validate if the contact person or company is legitimate.
- Don't be scared or embarrassed to end contact. Scammers who use a deepfake against you count on your trust or fear of being rude to keep you on the line.
- Always do background checks and verify personal information before hiring someone.

Fake-detecting technology

In response to malignant deepfakes, new security solutions and scam alert technologies are rising. A good example is Deepware, a service that allows you to scan a suspected deepfake video. Companies are also adding features and enhanced security questions to validate the authenticity of videos, posts and audio snippets.

The Federal Communications Commission helps consumers identify robocalls and suspected roboscams using a caller ID authentication technology called STIR/SHAKEN. The technology protects consumers by validating calls and displaying ID text when there's a possible scam call. Phone providers must enact the system by June 30, 2023.

Deepfake and national security concerns

Deepfake technology has advanced since its early days of glitchy animation effects. Some deepfake technology is so realistic that it's becoming impossible to detect. In response to a growing deepfake threat, the U.S. government introduced the Deepfake Task Force Act, saying:

"As the software underpinning these technologies becomes easier to acquire and use, the dissemination of deepfake content across trusted media platforms has the potential to undermine national security and erode public trust in our democracy, among other nefarious impacts. The threat that deepfakes could pose if used in misinformation campaigns is well known and well-documented."

Deepfakes that made the news

Deepfaking a U.S. president

In 2018, film director Jordan Peele showcased deepfake technology featuring the likeness of former president Barack Obama; Peele is actually controlling the movements and speech.

The illusion is not 100% convincing, but security experts' concerns remain. Would you dismiss the video if it was delivered on a trusted platform or by a major news outlet? What if it came from someone you thought you knew?

Bank heist by phone

In 2020, a Hong Kong bank manager got a call from a company client. The call was from the director, an individual he'd talked to many times before with a familiar voice. According to a Forbes report, the director asked him to transfer $35 million to bank accounts for an acquisition deal.

The lawyer, the escrow accounts and (most importantly) the voice seemed legitimate, so the bank manager transferred the $35 million. It was an elaborate scam involving 17 people and it was all kicked off by one event — a deepfake voice call.

Political spoofing and misinformation

On March 16, 2022, NPR reported that hackers posted a manipulated video of Ukrainian President Volodymyr Zelenskyy telling Ukrainians to surrender. The video circulated on social media and made it to a news site before being removed and debunked. Even if the quality was low, the damage was done.

Hiring spoofing and data theft

On June 28, 2022, the FBI Internet Crime Complaint Center issued a statement warning employers about increased deepfakes involving job applicants. Malignant hackers had been using stolen personal information to apply for remote jobs.

Deepfakes included videos, images and voice recordings impersonating individuals applying for information technology, computer programming, database entry and software jobs. They suspect the criminals wanted internal access to customer and financial data, corporate IT databases and proprietary information.

Deepfake incidents are on the rise

Malignant deepfakes are increasing to meet demands, and this is facilitated by a rise in easy-to-use technology. Social media sites are a treasure trove of images, videos and audio files. It doesn't take much to create a fully formed deepfake persona from hacking the average person's social media account.

Other times, deepfakes are cruel retaliations like revenge or crush porn, created by someone known to the victim. If these images or videos are shared, they can go viral or live in the cloud forever. These kinds of deepfakes can be particularly traumatic, damaging a person's life, sense of safety and livelihood.

But prosecuting a deepfake perpetrator is challenging since laws haven't kept up with technology. For example, many states have laws against nonconsensual pornography, but because a deepfake is a likeness that uses your face and not your body, most laws don't apply. Law enforcement has to work within state laws to find a way to prosecute these criminals. These laws are meant to address:

- Cyberstalking
- Bullying
- Harassment
- Credible or false impersonation

- Defamation

Report suspicious activity and stay vigilant

Deepfakes shake the core of how we trust — seeing can no longer be the basis for believing, at least not in the digital world.

If you suspect you've encountered a deepfake, report it to the FBI Internet Crime Complaint Center. Your information helps the authorities stay on top of the cybercriminals and their latest scams.

Cybersecurity and cyber liability insurance can help you offset the aftermath of a malicious deepfake, but nothing is foolproof. Use your good judgment and check your insurance coverage to prepare for what's next.

V.F. McNeil Insurance

(203) 481-2684
phandy@vfmcneil.com

V.F. McNeil Insurance
500 East Main St
Suite 200
Branford, CT 06405
www.vfmcneil.com