OUCH! March 2022

Learn a New Survival Skill: Spotting Deepfakes

What Are Deepfakes?

The word "deepfake" is a combination of "deep learning" and "fake." Deepfakes are falsified pictures, videos, or audio recordings. Sometimes the people in them are computer-generated, fake identities that look and sound like they could be real people. Sometimes the people are real, but their images and voices are manipulated into doing and saying things they didn't do or say. For example, a deepfake video could be used to recreate a celebrity or politician saying something they never said. Using these very lifelike fakes, attackers can spin up an alternate reality where you can't always trust your eyes and ears.

Some deepfakes have legitimate purposes, like movies bringing deceased actors back to life to recreate a famous character. But cyber attackers are starting to leverage the potential of deepfakes. They deploy them to fool your senses, so they can steal your money, harass people, manipulate voters or political views, or create fake news. In some cases, they have even created sham companies made up of deepfake employees. You must become even more careful of what you believe when reading news or social media in light of these attacks.

The FBI warns that in the future deepfakes will have "more severe and widespread impact due to the sophistication level of the synthetic media used." Learn to spot the signs of a deepfake to protect yourself from these highly believable simulations. Each form of deepfake — still image, video, and audio — has its own set of flaws that can give it away.

Still Images

The deepfake you may see most often is the phony social media profile picture. The image below is an example of a deepfake from the website thispersondoesnotexist.com. Below the image are five different clues that this could be a deepfake. You will notice that these clues are not easy to spot and can be hard to identify:

1. Background: The background is often blurry or crooked, and may have inconsistent lighting such as pronounced shadows pointing in different directions.

2. Glasses: Look closely at the connection between the frames and the arms near the temple. Deepfakes often have mismatching connections with slightly different sizes or shapes.

3. Eyes: Deepfake photos currently used for fake profile pictures appear to have their eyes in the same spot in the frame, resulting in what some call the "deepfake stare."

4. Jewelry: Earrings may be amorphous or strangely attached. Necklaces may be embedded into the skin.

5. Collars and shoulders: Shoulders may be misshapen or unmatching. Collars may be different on each side.

Video

Researchers at the Massachusetts Institute of Technology, MIT, developed a question list to help you figure out if a video is real, noting that deepfakes often can't "fully represent the natural physics" of a scene or lighting.

1. Cheeks and forehead: Does the skin appear too smooth or too wrinkly? Is the age of the skin similar to the age of the hair and eyes?
2. Eyes and eyebrows: Do shadows appear in places that you would expect?

3. Glasses: Is there any glare? Too much glare? Does the angle of the glare change when the person moves?
4. Facial hair: Does the facial hair look real? Deepfakes might add or remove a mustache, sideburns, or beard.
5. Facial moles: Does the mole look real?
6. Blinking: Does the person blink enough or too much?
7. Lip size and color: Do the size and color match the rest of the person's face?

Audio/Voice

Researchers say technologies like spectrograms can show when voice recordings are fake. But most of us do not have the luxury of a voice analyzer when an attacker calls. Listen for a monotone delivery, odd pitch or emotion, and lack of background noise. Voice fakes can be hard to detect. If you receive an odd call from a legitimate organization, you can verify if the call is real by first hanging up then calling the organization back. Be sure to use a trusted phone number, such as a phone number you already have in your contact list, a phone number printed on a bill or statement from the organization, or the phone number on the organization's official website.

Conclusion

Be aware that attackers are actively using deepfakes. They can make fake accounts on social media to connect with or create fake videos to influence public opinion. Some are even selling their services on the dark web so other attackers can do the same. We don't expect you to become a deepfake expert, but if you arm yourself with the basics of identifying the fakes, you'll be far better at defending yourself. If you suspect you have detected a deepfake, report it to the website or source that is hosting the content.

Guest Editor

Kerry Tomlinson (@KerryTNews) is a cyber news reporter at Ampere News and a certified SANS Security Awareness Professional. Her mission is to translate what is happening in the digital world for people of all knowledge levels with compelling, insightful news stories, and compelling presentations.

Resources

Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Can you spot the fake? (Ampere News): https://www.amperesec.com/news/can-you-spot-the-fake
MIT's deepfake detection test (MIT): https://detectfakes.media.mit.edu/
Spot the deepfake: https://www.spotdeepfakes.org/en-US

Translated for the Community by::