INSIGHTS

Cyber made simple.

DEEPFAKES ARE GETTING BETTER

BY JAY BORDEN

What are deepfakes? Wikipedia defines deepfakes this way:

“Deepfakes (portmanteau of "deep learning" and "fake"[1]) are synthetic media[2] that have been digitally manipulated to replace one person's likeness convincingly with that of another. Deepfakes are the manipulation of facial appearance through deep generative methods.”

Many people think they can spot deepfakes and not be fooled. Experience shows otherwise. In simple examples people are shown two photos, one real and one a deepfake. They do not score well at identifying the deepfake.

As the use of Artificial Intelligence, AI, and Machine Learning, ML, by cybercriminals increases the deepfakes get better and harder to spot.

In a recent scam employees of an international company received an email inviting them to a internal videoconference meeting. An employee suspected that the email was a phishing attempt. But he joined the videoconference and saw people he knew, including the Chief Financial Officer. That made him believe it was real. He was instructed to carry out secret transactions. He followed those instructions and sent out about $25 million to five different bank accounts.

Needless to say, the entire episode was fake. The original email was phishing and the “participants” in the videoconference, including the CFO, were deepfakes. The money was sent to accounts owned by cybercriminals.

The level of detail and the use of a faked videoconference with participants known to the victim including a company executive, show the planning and effort the cybercriminals will go to. But then again, $25 million is a good return for the effort. This is just one example.

DEEPFAKES ARE GETTING BETTER

Continued

Deepfakes are becoming popular as a way to spread false “news” or conspiracy theories on social media. In these examples a celebrity appears to deliver the message. As celebrities are often spokespersons for different causes it is believable. Except they are deepfakes.

Here is an example https://www.youtube.com/watch?v=oxXpB9pSETo

This one is from about 2 years ago and the technology has advanced significantly since then making the deepfakes harder to detect.

Another recent use has been to show deepfakes of celebrities in compromising positions. Taylor Swift is one of the latest to be exploited this way.

Tools to create deepfakes are proliferating and coming down in price making it easier to create them and needing less technical know-how.

While there are no assured ways of spotting deepfakes, there are things that may help. If it is a videoconference or other “live event” ask the person to turn their face sideways. This is a view that may not have been captured from the real person and will look less real than a full face view.

If you are basically just an observer and don’t really interact with the other participants it is a red flag. Interact means more than just being asked questions and you responding. You need to be able to ask questions and get responses or have a conversation with the other participants. This applies if it is a phone call and not a videoconference.

If possible use a high resolution monitor and enlarge the view to zoom in on the person’s face. This can show portions of the face that are faked.

It isn’t even necessary to break into a corporate network or security system to get the images used for the deepfake. The video for the money transfer mentioned above used footage that is publicly available.

Nor is it necessary to have vast amounts of video or audio of a person to create the deepfake. A Chinese company has a commercial service that can create deepfakes that are high resolution and realistic using just three minutes of live action video and 100 spoken sentences of the person to be faked.

DEEPFAKES ARE GETTING BETTER

Continued

With the success of deepfakes and the ease in creating them, deepfakes are being viewed as the new spear phishing delivery mechanism. The more believable they become, the easier it will be to get people to fall for them and perform compromising actions such as clicking links, sharing credentials, or other private information, or as in the example above, initiate money transfers.

Alerting your employees at all levels about deepfakes is a first step in improving cyber safety.

To learn all the ways we can help make your company safer, visit onebrightlycyber.com and contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920