INSIGHTS

Cyber made simple.

one brightly cyber

PROTECTING AGAINST DEEPFAKES

BY JAY BORDEN

Let's begin with a definition of deepfake. According to Merriam-Webster it is:

> "an image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said"

Sounds clever. So why is it so dangerous?

Not long ago deepfakes needed strong technical skills and powerful computers. Now the new AI technology has made it very easy to create deepfakes that are much more believable and no longer need technical skills or massive computing power.

We have written before about how successful phishing and Business Email Compromise are for cybercriminals. Now imagine voice calls that sound exactly like an executive from your company telling you to do something right now! Such as initiate a wire transfer of other form of money transfer. Or the head of HR saying there has been a problem with their systems and in order to process your payroll, they need your username and password, Social Security number and bank account number.

To make even more real, it is a video call where not only can you hear this executive but see them. Makes it very real doesn't it?

In today's world where everyone is overloaded and overwhelmed, how many people will take to the time to confirm the authenticity of the call? Even without deepfakes who would call the head of HR or the CEO to ask if they really called?

Remember, with deepfakes it is their voice and image you are seeing. It's just that they didn't say those words.

onebrightlycyber.com
(888) 773-1920

INSIGHTS

Cyber made simple.

PROTECTING AGAINST DEEPFAKES

Continued

In another example, imagine a video of the CEO of a company on social media or a video call giving a glowing report about the financial performance of the company. The report isn't just words, there are graphs and tables of the financial results with all the supporting data.

Of course, it's all deepfake, the words, video, and the financial reports. But convincing enough to get individuals and professional investors to invest.

Not only investors can be fooled, but regulatory authorities can also be fooled. So much for the oversight designed to protect investors.

What can you do?
Educate users at all levels and in all disciplines about deepfakes and how convincing they will appear. Teach them to be extra cautious of any communication asking for questionable actions.

As the old saying goes "trust but verify" or even don't trust but verify. Let them know that all company executives want them to take the time to reach out using known phone numbers to confirm instructions before initiating a money transfer, sending private information or any other potentially risky action. Require additional approvals before any monetary transaction is processed, especially to a new receiver.

Inform your customers or clients to report any suspicious emails, voicemails, or any other communication appearing to come from your company asking for private information or money transfers.

Teach your executives to be wary about creating videos, posting pictures of themselves or doing presentations where their full face is visible. If only a profile or side view of a person's face is available to cybercriminals it is more difficult to create a convincing deepfake of the person.

We have emphasized before that people are the cause of a high percentage of cyberbreaches. Education is essential as tools will not catch everything.

Deepfakes only serve to emphasize this.

Need help or guidance? Learn how we can help you in so many ways.

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.