The Reality Of Non-Reality: Deepfakes And The Workplace

Insights
5.29.20

It's Monday morning. Your employee receives a phone call from the Chief Revenue Officer (CRO) asking them to immediately wire funds to an off-shore bank account. That phone call is followed by an email and a text message from the CRO's cell phone asking for the status of the request. The employee complies with this somewhat unusual but urgent instruction.

Only later do you realize that the voice requesting the wire transfer wasn't the CRO. By then, your company's money is long gone. The person who spoke to your employee was a cybercriminal using artificial intelligence to imitate the CRO's voice.

This might sound like a scene from a James Bond movie – but it isn't. In 2019 alone, at least three companies were attacked using variations of the scheme detailed above, resulting in millions of dollars being transferred to cybercriminals. This is the "reality of the non-reality," otherwise known as deepfakes. Employers, now more than ever, need to get acquainted with this developing technology to ensure that the right processes and systems are in place to guard against cybercriminals wielding deepfakes.

What Are "Deepfakes"?
Deepfake is a term used to refer to artificial intelligence generated synthetic media. Deepfakes are created by using software that leverages complex algorithms to mimic voice, mannerisms, facial expressions, and lip movements to create a close or nearly discernable match to the likeness of a person or object. In other words, this technology can be used to make people believe something is real, when it is not.

When used successfully, it can create video clips of events that never happened and sound clips of statements never made. What's more alarming? Any individual with access to the internet and a willingness to explore the technology can produce a deepfake.

Deepfake Technology As A Business Threat
When we think of deepfake technology, we often think of its impact on social media, politics, and the like. Perhaps less talked about is the impact of such technology on the workplace. Many of us are familiar with spearfishing. Spearfishing is the technological ability to have individuals complete a manual task such as sending physical documents or buying a gift card for the cybercriminal. Spearfishing can be difficult to detect as most spearfishing communications mask themselves as

individuals you know. Sophisticated employers tend to be hyper-aware of spearfishing threats and, in most cases, train their employees on how to identify and report such threats.

Deepfake technology is a supercharged version of spearfishing. What do we mean by that? Well, remember that employee who wired your company's money to an off-shore account? You may be wondering how could that employee have possibly thought that request was legitimate. Let's provide some additional context.

That employee had previously spoken to the CRO on multiple occasions and knew the sound of the CRO's voice. That same employee also had the CRO's personal cell phone number and often texted with the CRO outside the workplace. Fast-forward to the day the employee wired company funds to an off-shore account: The employee recognized the CRO's voice and the follow-up text and email came from the CRO's mobile number and email account. This is the reach of deepfake technology.

In addition to the threat of fraud at the hands of cybercriminals, businesses should also be concerned about the threat deepfakes pose to a company's reputation and hiring practices. At the House Intelligence Committee Hearing on Deepfake Videos held in June 2019, Professor Danielle Citron theorized the havoc that a well-timed deepfake could cause for businesses. A deepfake of a company's CEO speaking negatively about the company's value posted to social media on the eve of an IPO could destroy the IPO and the company's reputation.

What's worse is that once a deepfake goes viral, the market will respond quicker than that deepfake can be identified and discredited. This so-called "cheapfake" (a less sophisticated, low-budget form of altered media) of House Speaker Nancy Pelosi went viral on social media, generating millions of views before it was debunked. Adding insult to injury, these attacks can leave a negative impression about targets even after they have been identified as false and discredited. At present, the security industry has not put forth any email filters or other technologies to defend against deepfakes.

Deepfake Regulation (Or Lack Thereof)

Whether it's the use of deepfakes to steal millions of dollars from unsuspecting companies, discredit the health of a political opponent, or generate nude photographs of unwilling women – there can be no doubt that the misuses of deepfakes are concerning. Adding to the potential for misuse of this technology is the fact that, as with most forms of artificial intelligence, it is largely free from government oversight and regulation.

Despite bills proposed by the House and Senate, the federal government's only foray into legislation involving deepfakes was contained in the 2020 National Defense Authorization Act. The Act commissioned a report on deepfake technology and foreign weaponization of deepfakes. It also established a program to award prizes to companies or individuals creating technology to automatically detect deepfakes.

On a state basis, only three states have enacted legislation addressing the potential misuse of deepfakes. Thus far, deepfake regulation on the state level can be divided into two distinct categories

deepfakes. Thus far, deepfake regulation on the state level can be divided into two distinct categories – laws outlawing the use of deepfakes in pornography and those prohibiting the use of deepfakes to influence elections. Neither category provides much protection for employers when it comes to workplace concerns.

Prepare For Deepfake Attacks

We'd be willing to bet that most of your employees don't know what a deepfake is, let alone the potential danger they can pose to your company. With deepfakes becoming more and more prevalent online and easily available to cybercriminals, the first step companies should take is to provide across-the-board training on deepfakes. Currently, there is no software that filters deepfake media and identifies it as altered or synthetic. Because of this, the strongest tool is knowledge paired with common sense. To that end, employers should update cybersecurity training in order to educate employees about the existence and dangers of deepfakes.

Training provided to employees should include a brief explanation of deepfake technology. This should include the various types of deepfakes that can be generated using artificial intelligence, which include: voice cloning, "puppet-master," face-swap, and artificial portraits. Puppet master deepfakes are created using already existing media. Oftentimes these types of deepfakes use an impersonator to change the language contained in a video clip. Face-swap deepfakes take the face of one individual and place it on the face of another. A good example is this face-swap of Kate McKinnon and Elizabeth Warren. Both face-swap and puppet master deepfakes use artificial intelligence to alter the speaker's lip movements and facial expressions to make the deepfake look more realistic.

Even employees and human resource professionals trained on the existence and types of deepfakes may not be immediately aware of the extent of the threat they pose. Employees should be warned about the various possible uses of deepfakes. Many of the viral news stories involving deepfakes have centered on videos. However, thus far, deepfake audio has posed the greatest risk to companies.

Employees should be warned that any request or communication that comes without notice or verification could be a deepfake. Training should encourage employees to seek confirmation for any suspicious or urgent requests that are made without prior notice. Employers should expect that cybercriminals wielding deepfake technology will create deepfakes of high level company officers. Because of this, employees should be informed that seeking to verify a request from a high-level company employee will not result in disciplinary action. Training should also include tips on identifying deepfakes and perhaps go as far as designating an employee or department responsible for receiving and reviewing potential deepfake activity.

You should also consider developing a role at your company for a media professional to monitor your company's social media and online presence. This person should be trained on the identification and response to deepfakes that could be used to tarnish your company's reputation or spread false information. Quick identification of and action against deepfakes targeting your company may stop a viral scandal.

In addition to guarding against the threats posed by deepfakes, human resources employees need to be specially trained in considering the possibility of deepfakes for all employee discipline based on media that is susceptible to manipulations or deepfake technology.

Conclusion

Deepfake technology is constantly evolving. Deepfakes that may not have been convincing even a year ago are now more realistic and easier to make – and the technology is going to keep improving. Creating a deepfake cybersecurity policy and training employees on the dangers of deepfakes may save your company significant costs and loss of reputation.

Remember the employee that wired company funds to an off-shore account? With proper training, that employee would have been better equipped to question whether that request was a deepfake. If he had sought independent verification of the request, he could have saved the company millions of dollars. Don't let your company be the next deepfake cautionary tale.

For more information, contact the authors here or here.

Related People

Kelsey E. Schiappacasse
Partner
610.230.2184
Email

Service Focus

Counseling and Advice