Courtesy of
Universal Group LTD.

CYBERRISKS&LIABILITIES_

Deepfakes Explained

Deepfakes refer to sophisticated forgeries of an image, video or audio recording. Deepfakes have been around for years—you can even find a version of them in social media applications. For instance, with Snapchat, face-changing filters take real-time data and feed it through an algorithm to produce a synthetic image.

However, as the technology has evolved, deepfakes are now able to alter media so well that it's often difficult to detect that any manipulation has occurred at all. Through the use of artificial intelligence (AI) technology, deepfakes leverage existing audio and video of an individual—all while continuously learning how to produce a more convincing forgery.

Deepfakes have been used to believably impersonate influential political figures. They can even be used to alter both real-time or recorded media. Deepfakes are so sophisticated that they can deceive the general public into thinking a person has said or done something they normally wouldn't. And, in the hands of a malicious party, deepfakes can be incredibly devastating.

The Risk of Deepfakes for Businesses

Through the use of phishing and "fake president" scams, cybercriminals have long tried to deceive businesses into giving up sensitive information. Often, these scams are executed using fraudulent email accounts, which, in some cases, can be easy to spot. However, using deepfakes, cybercriminals now have the power to fool even the most careful and perceptive organizations.

With deepfakes, cybercriminals can make a person in a video look and sound like a target company's CEO, tricking employees into wiring money or sharing sensitive data, among other compromising actions. Specifically, deepfakes can be used to execute social engineering scams or sway public opinion**:**

- **Using deepfakes in social engineering scams**—Put simply, social engineering is when a malicious party takes advantage of human behavior to commit a crime. Social engineers can gain access to buildings, computer systems and data simply by exploiting the weakest link in a security system: humans. For example, social engineers could steal sensitive documents or place key loggers on employees' computers at a bank—all while posing as fire inspectors from a nearby fire department. Social engineers don't need to have expert knowledge of a company's computer network to break into a business—all it takes is for one employee to give out a password or allow the social engineers access to an area they shouldn't be in. And because deepfake technology has become less expensive and more accessible, the prospect of tricking an employee to perform a malicious action through social engineering tactics is that much easier. This is especially true given how realistic deepfakes can be.
- **Using deepfakes to sway public opinion**—By deepfaking a company's CEO or figureheads, a malicious party can easily spread false or potentially damaging information. Through deepfakes, criminals can make key stakeholders say or do just about anything. They could have a CEO share false information, say or do socially unacceptable things or attempt to influence consumer behavior. All of these actions can harm a business's reputation, sometimes irreparably.

Given the potential harm of deepfakes, it's crucial that businesses are prepared to protect themselves.

UNIVERSAL
Group, LTD.

Guarding Against Deepfakes
When it comes to protecting your business from deepfake schemes, consider:

- **Training employees**—To protect your organization against deepfakes, employee training is critical. Employees should be educated on deepfakes, including what they are and how they may be used against the business. Simply by raising awareness of deepfakes, employees will be better equipped to spot them, allowing your business to respond quickly and swiftly.
- **Utilizing detection software**—While AI is used to make deepfakes better and more effective, it can also be used to help detect potential deepfakes. In fact, large corporations such as Facebook and Microsoft use AI and similar software to detect and remove deepfake videos from their platforms. When it comes to deepfakes, the earlier you detect one, the better. This allows you to act quickly to reduce potential harm.
- **Establishing a response strategy**—If and when your organization is the target of a deepfake-driven attack, it's crucial to have a response strategy in place. Such a strategy should center around crises mitigation. This includes outlining individual responsibilities, determining escalation practices and communicating response best practices.

For more information on various cyber exposures, contact Universal Group LTD. today.