beazley

Article

Deepfakes: The latest weapon in the cyber security arms race

Melissa Collins • October 04, 2024

Artificial Intelligence (AI) and new so called ‘deepfake’ tools are being deployed by cyber criminals to defraud companies out of significant amounts of money. A recent example of this new phenomena in action occurred in May this year. News of an elaborate deepfake scam broke. UK engineering group, Arup, suffered a US$25m loss, when a member of its finance team based in Hong Kong became a victim of a sophisticated deepfake con[1]. Cyber criminals successfully cloned Arup’s Chief Financial Officer’s (CFO) image and voice, and invited a member of the finance team to listen in to a video conference call, along with other ‘purported’ employees (who were also fakes)[2]. The employee’s initial suspicions were allayed by seeing and hearing the firm’s CFO and other colleagues, discussing the opportunity and he transferred funds to various bank accounts based in Hong Kong as instructed by the deepfake CFO on the call[3].

Today seeing is not believing

New AI technology allows cyber criminals to refine existing techniques, such as phishing emails, while also giving rise to new types of attacks. Deepfakes represent a new weapon in cyber criminals’ arsenals. The Arup example is, unfortunately, just the opening salvo.

It is now almost impossible to detect synthetic voice. Readily available AI tools can create video likenesses and develop text which mirrors the styles of specific individuals. This threat will only increase. Our Risk & Resilience research data shows that Canadian business executives feel exposed to the growing cyber threat, with over a quarter (28%) of business leaders seeing cyber as the biggest threat they face this year. Yet concerningly, 15% believe that their organisation does not have adequate protections in place.

Deepfakes are not the only new weapon for hackers. AI enhanced social engineering tools are also providing a shot in the arm for hackers on the backfoot as cyber defences steadily improve. Social engineering

involves the manipulation of people to transfer money or unwittingly share sensitive data. While businesses are investing in cyber security, and over a quarter (26%) of the Canadian executives we surveyed plan to do so this year, ensuring employees are aware of the increased risks and are well-placed to spot attacks is by no means an exact science. Although businesses can hold training sessions, human error will always be a possibility, particularly when emails and phone and video conference calls appear legitimate.

Continuous innovation

AI, is enabling traditional hacking techniques and social engineering to become easier and more effective to execute. As an example, AI can now be trained to draft phishing emails using its natural language processing capabilities[4]. Authentication is becoming increasingly problematic. Hackers can circumvent multi-factor authentication (MFA), which traditionally provided businesses with a solid layer of security. While MFA once represented the gold standard for cyber security defences, the pendulum has swung again. In doing so, businesses can no longer rely on MFA to repel hackers, protect sensitive data and provide peace of mind for key stakeholders.

Deepfakes mark a clear departure from pre-existing hacking techniques and, despite being a relatively recent innovation, are already highly sophisticated. Their ability to blur the distinction between reality and manipulation is unparalleled. The ability of hackers to replicate the human voice and face, with such efficiency that employees can be deceived into thinking they are speaking with a colleague on a video call, poses a real danger to businesses.

Deepfakes pose a particular threat from a ransomware perspective. With technology, and its associated threats, moving at such speed, lawmakers are racing to update existing legislation. For example, only in April this year did it become illegal in the UK to create sexually explicit deepfake images without consent[5]. Concerningly, there is a growing trend of school students being targeted by such deepfakes, with the perpetrators typically demanding ransom payments to prevent the images from being published[6].

This being said, deepfakes do have some limitations. For example, cyber criminals are not yet able to use deepfakes to have real-time conversations with employees of a company, posing as their boss or senior colleague. Also, while a deepfake technology may accurately recreate someone’s appearance and voice, the tone of language it employs may not reflect that typically used by the victim, which can sometimes give the scam away. However, given the speed of innovation in this space, it will not be long before solutions are found for these shortcomings.

How can businesses protect themselves?

With social engineering and deepfake technology becoming increasingly effective, businesses must place greater emphasis on internal controls to protect against human error. Deepfakes have highlighted the need for businesses to have strict structures in place to govern, for example, the authorisation of payments to third parties.

Businesses must invest in employee training to ensure their staff are well-placed to recognise potential deepfake scams. As cyber criminals become increasingly sophisticated and scams harder to detect, instilling a culture of vigilance and good practice is crucial. Encouragingly, our research found that over a quarter (26%) of Canadian businesses plan to invest in cyber security measures this year.

Insurance can also play an important role, forming part of a wider risk mitigation strategy. Insurers can provide tailored, specialist support to help spread awareness of the latest threats and boost preparedness. Considering the fast-evolving threat landscape, insurers can serve as important partners to many businesses. As deepfakes are often excluded in cyber insurance policies, it is incumbent on insurers to work with brokers and insureds to help them understand the cover on offer.

Melissa Collins

Claims Focus Group Leader – Third Party Liability Cyber & Tech

BZSL 235.

[1] Arup lost $25mn in Hong Kong deepfake video conference scam (ft.com)

[2] Arup lost $25mn in Hong Kong deepfake video conference scam (ft.com)

[3] Arup lost $25mn in Hong Kong deepfake video conference scam (ft.com)

[4] Can AI Write a More Convincing Phishing Email Than Humans? - Unite.AI

[5] Creating sexually explicit deepfakes to become a criminal offence - BBC News

[6] Real Teenagers, Fake Nudes: The Rise of Deepfakes in American Schools - The New York Times (nytimes.com)

beazley