News article

Mar 2024

AI Deep Fake Used In Social Engineering Attack

Hong Kong Police are investigating a social engineering attack that targeted a multinational organisation that is believed to be the first cyber-attack to use video deepfakes.



What Happened?

The attack, which took place over a week, began with traditional social engineering techniques - threat actors sending emails to an employee within the finance department, and impersonating the organisation's Chief Financial Officer (CFO). The phishing email requested that the employee carry out a secret transaction on behalf of the UK-based CFO. While the employee was initially sceptical of the request due to the unusual nature of the secret transaction and believed it to be a phishing email, the threat actors invited them to join a video call, supposedly with the CFO, to discuss the request and put their mind at ease.

When the employee joined the video call, they were met with sophisticated deepfake representations of key company officials, including the CFO, which convincingly replicated their appearance, voices, behaviours and mannerisms. This video call and the conversation that took place convinced the employee that the request was legitimate, and they subsequently authorised 15 separate financial transactions, totalling approximately £20 million.

Wider Implications

This incident highlights how AI is enhancing existing social engineering techniques making them harder for employees to identify. While this incident appears to be the first that has utilised AI deepfakes in a video call to aid a social engineering attack, it is unlikely to be the last. As more advanced AI tools are made available to the public, voice and video deepfakes will likely become more common, requiring organisations to continue evolving their controls to reduce the risk of advanced social engineering attacks.

Organisations Should

- Consider investing in an advanced email security solution that uses machine learning to develop a picture of the email relationships within an organisation and its suppliers. This can help customise security to an organisation's specific needs, identifying emails sent from unusual senders or using unusual language.

- Ensure that all processes to carry out sensitive actions such as financial transactions have a formal and auditable process that must be followed at all times. Social engineering attacks (using AI or not) will usually ask users to carry out actions that do not follow normal operations. It is essential organisations develop processes that cannot be bypassed to increase the number of people involved in the decision, and therefore a concern being raised.

- Ensure employees receive regular cyber awareness training on how to identify the latest threats, including AI enhanced social engineering attacks and deepfakes. Employees should also be made aware of the importance of following formal procedures related to any sensitive actions linked to their day-to-day work.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430