30.04.2024

CEO fraud 2.0

With classic cases of CEO fraud, employees of a company receive an e-mail, supposedly from their boss, instructing them to immediately initiate a payment. The Bundesamt für Cybersicherheit has now been notified of a case which goes a step further.

The case the Bundesamt für Cybersicherheit (BACS) was notified of is one that stands out from all other known attacks so far. Unlike the usual approach, the victim was not stopped from contacting his boss at all. Instead, an employee with direct authorisation to initiate payments received a call, supposedly from a solicitor, inviting him to attend a video conference with his boss. Once the employee dialled into the conference, he could actually see his alleged boss on the screen and talk to him as well. In the course of the conversation, this "boss" then tried to convince him to initiate a financial transaction.

This fake video of his boss was created using Artificial Intelligence (AI). It is not clear from where the criminals obtained the materials to create this. However, it is suspected that publicly available video materials were used to produce this so-called "deepfake video".

Another option, in particular in order to copy a voice, is to make some telephone calls beforehand. In this regard, several companies reported that persons unknown obtained information about the company via telephone calls. Such information could then be used for targeted attacks. Using the recorded voice of someone's boss, it is then possible to copy this using AI and deepfake options.

This incidence shows that criminals increasingly abuse the possibilities offered by Artificial Intelligence (AI), even if they have not quite perfected its application just yet. In the current case, this fraud was discovered. The fraudsters focused on merely manipulating the face of this boss. The way he was dressed did not conform to his usual habits, and the imitation of his voice was not a particularly good one either.

This is how you recognise a deepfake:

- Lips don't move in time with the spoken text
- Pronunciation errors
- Strange wordings
- Bad video quality
- Material used from a different context

Further information on CEO fraud and in particular also on how you can protect yourself can be found under: www.ebas.ch/ceofraud (http://www.ebas.ch/ceofraud)

The original BACS article can be found here (https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/wochenrueckblick_14.html) .

Copyright – All rights reserved. Lucerne School of Information Technologies