nccgroup

shutterstock illustration ID: 1464098960

Mar 27, 2020 00:19 GMT

Deepfake attack threat during Covid-19

In these unprecedented times many companies are in business continuity mode so the unusual has become both prioritised and normalised.

Many are making unusual purchases at short notice to facilitate their migration to increased or full remote working and fiduciary financial due diligence rules such as ‘four eyes’ checks and verification may be relaxed as finance teams are pushed to work remotely. This changes the threat landscape and affords threat actors new opportunities for attack which they will be characteristically quick to exploit.

Several of our clients had already seen an increase in the use of deepfakes to

support Business Email Comprises (BECs) prior to the current Covid-19 crisis. Some stories have been covered in the press[1]. These attacks are often in the form of voicemails in support of an email (or sometimes alone) apparently from a CEO asking a CFO or finance colleague to make a transfer to a new customer or an existing one with changed payment details. Given the change in working practices brought about by the Covid-19 crisis and the natural human desire to help the business in the difficult times the additional use of deepfake voicemails could tip many finance colleagues into making the transfer.

Deepfakes are now relatively easy to make provided the threat actors have some samples of the victim's voice. Many CEOs have active social media profiles replete with audio and video recordings so this is a straightforward matter. Technologies such as Lyrebird[2], Wavenet and Adobe VoCo[3] demonstrate the current state of the art and create a trickle-down effect bringing the technology within easy reach of the cyber criminals. Anyone who has seen my talk on 'Managing Cyber Risk in a Fake World' will be aware of how easy this is becoming. My colleague Matt Lewis covers many of the technologies in his excellent 44con talk[4].

The solution is education, awareness and process. Make sure all your finance colleagues are aware of the increased threat and seek to replicate your 'four eyes' checks even if your entire finance function is working remotely.

[1]https://www.scmagazineuk.com/ai-mimics-ceo-voice-scam-uk-energy-firm-200k/article/1595277

[2]https://faculty.ai/

[3]https://www.youtube.com/watch?v=I3l4XLZ59iw&feature=youtu.be&t=120

[4]https://youtube.com/watch?v=HoYZG1JpZbg

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted

by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970