SENT 02-11-2020.
ATTACHMENTS: 0

View this email in your browser


SANDBOX TECHNOLOGIES

# Information Security Alert

## Cyber Criminals Now Using Artificial Intelligence to Falsify *Verbal* Financial Instructions

If you feel the topic of this notification beggars belief, you're in good company. When it first hit the radar of our EGP Secure® team, our reaction was similar. As surreal as it would seem however, the threat is genuine, and based on reports from The Wall Street Journal and The Washington Post, the first widely-publicized incident appears to be credible.

Given the number of our clients conducting business within the financial services industry, we have elected to send this alert now, prior to the official launch of our new information security practice. In the future, should you wish to no longer receive these notifications, simply reply to this message with the word "UNSUBSCRIBE" in the subject.

### Threat Summary

Cyber-criminals are reportedly now using the controversial "Deepfake" technology that's been receiving much media attention as of late to commit financial fraud. The perpetrator(s) are alleged to have created a very believable copy of a real person's voice, which was then used to initiate a live telephone conversation during which the caller instructed an unwitting subordinate to transfer €220,000 to an account controlled by the perpetrator(s).

For businesses that routinely initiate wire transfers at the instructions of celebrity clients or other high-profile parties, this is particularly concerning, given the public availability of audio samples that could easily be used to create and fine-tune artificial voice copies.

## Recommendations

As we continue to actively monitor the development of this threat, our initial recommendations to clients are:

- Disseminate this information to all relevant staff and financial services clients;
- Always call back requestors at a legitimately known contact number to obtain a second live confirmation before taking any action;
- When a call-back is not possible, require that all verbal instructions be given directly to someone with intimate knowledge of the requestor and the ability to engage in conversation that confirms the caller's identity beyond any shadow of doubt;
- Implement a simple system of numeric, one-time use codes that the client or executive requestor must provide whenever a request is made. To minimize inconvenience, codes can be stored in encrypted, password-protected mobile applications, or printed onto discreet, wallet-size cards containing no other information and laminated.

Of the above, the use of call-backs and codes are the preferred approaches, as other methods of confirming identity can be overcome if a party's email has been breached, providing perpetrators an opportunity to familiarize themselves with intimate details about the person they're impersonating.

For more information about this emerging threat, clients are encouraged to visit the links below.

https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#766a453d2241

https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/?noredirect=on

https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

As always, if you have questions, please feel free to contact any member of our technical services team.

Sincerely,

Oliver Fox
Chief Operating Officer and Interim CIO
Sandbox Technologies, Inc.

*Copyright © 2019, Sandbox Technologies, Inc. All rights reserved.*

**Our mailing address is:**
4111 West Alameda Ave., Suite 605 Burbank, CA 91505

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list.