



What are deepfakes?

Deepfakes are synthetic media that effectively mimic someone else's appearance/or voice.

They are created using artificial intelligence techniques. They involve manipulating or replacing someone's face or voice in a video or image with that of another person, making it appear as though the second person is actually saying or doing things they never did.

Deepfake Phishing

In deepfake phishing attacks threat actors manipulate their targets by exploiting their trust and bypassing traditional security measures as they do with traditional phishing attacks.

New technological advancements make it possible for anyone with a computer to create deepfakes, resulting in more sophisticated attacks.

Threat actors are weaponizing deepfake phishing attacks in different ways including:

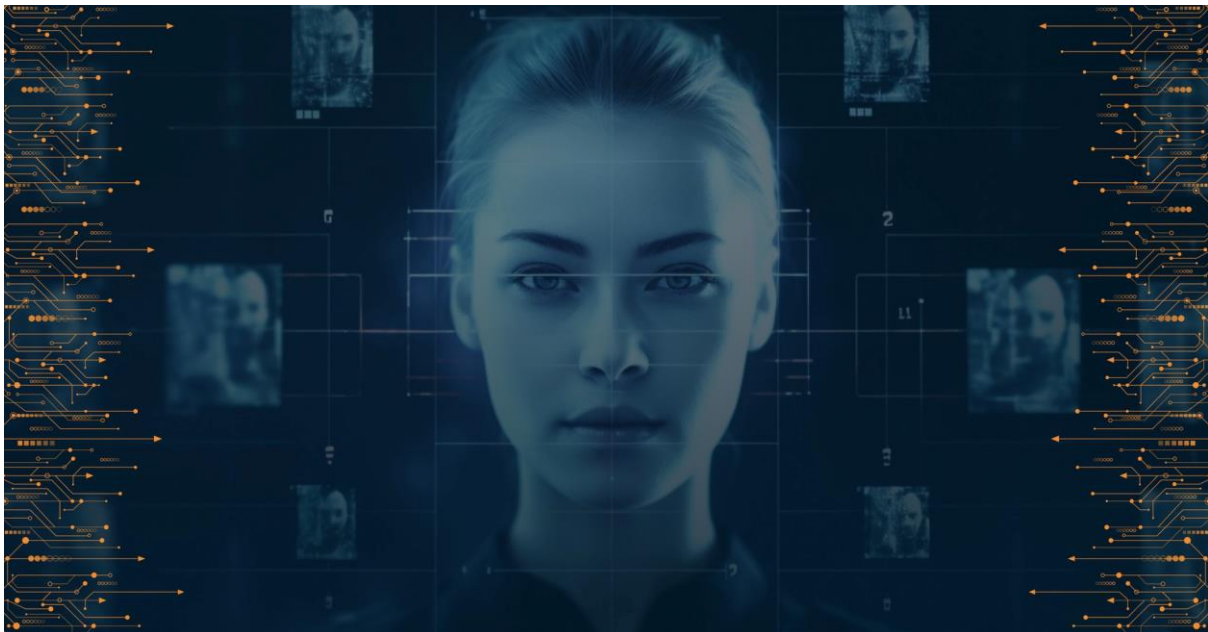
- E-mail
- Video calls
- Voice messages
- Fraudulent internet posts
- Financial and legal documents fraud

Why are deepfakes so concerning?

- They are evolving quickly
- They are highly personalized
- They can be extremely difficult to detect

How can you help protect the organization?

1. Be skeptical and cautious. If you handle financial transactions, be on high alert and follow the company's internal processes.
2. Verify the credibility of the source over a trusted channel that you initiate (ex. Microsoft Teams Chat)
3. Report all suspicious messages in Outlook by clicking the '**Report Message**' button and selecting '**Phishing**' from the dropdown.
4. Report any text message phishing, voice call phishing and deepfake video phishing by e-mailing cyberteam@company.com with a description of the incident and screenshots.



Recent, Real-life Examples

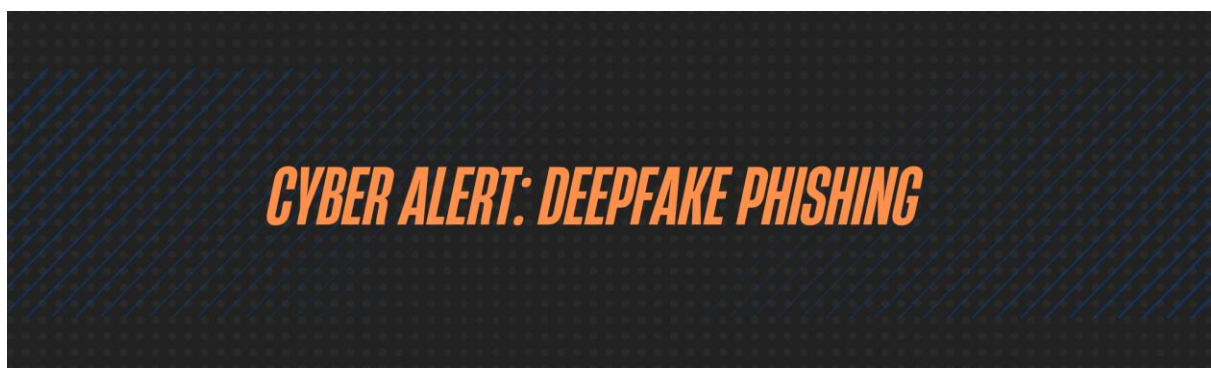
In February of 2024, a finance worker in Hong Kong paid \$25M after a deepfake call with the “CFO”. The worker was duped into attending a video

call with what he believed to be other members of staff, but they were all deepfake recreations.

Early 2024, a peer company experienced an attack in which a threat actor used WhatsApp to send deepfake audio messages of the company's CEO to attempt to trick finance employees into making payments on a fake court order following a civil case. The threat actors went as far as to create fake court documents and other material on demand when asked. Their team thought the audio was remarkably convincing down to the accent and word choice.

In May 2024, a Big 4 firm experienced a deep fake of their CEO. The video and voice were convincing. What tipped the team was that the CEO didn't talk as much as they usually do in such a meeting.

In May 2024, a Pharma Board Member was victim of a deep fake. They believed they were speaking to the CEO of another pharma company via a video call. The communication slipped in and out of English and French fairly effectively. The suspected intent was to gather voice and video data from the Director for future deep fake exploitation.



Did you know that deepfake phishing is one of the most dangerous forms of AI cybercrime?

Deepfakes are media, such as images, audio, or video, that is manipulated using generative AI-powered neural networks. Threat actors are increasingly

using deepfakes, endangering companies' security, finances, brands, and reputations.

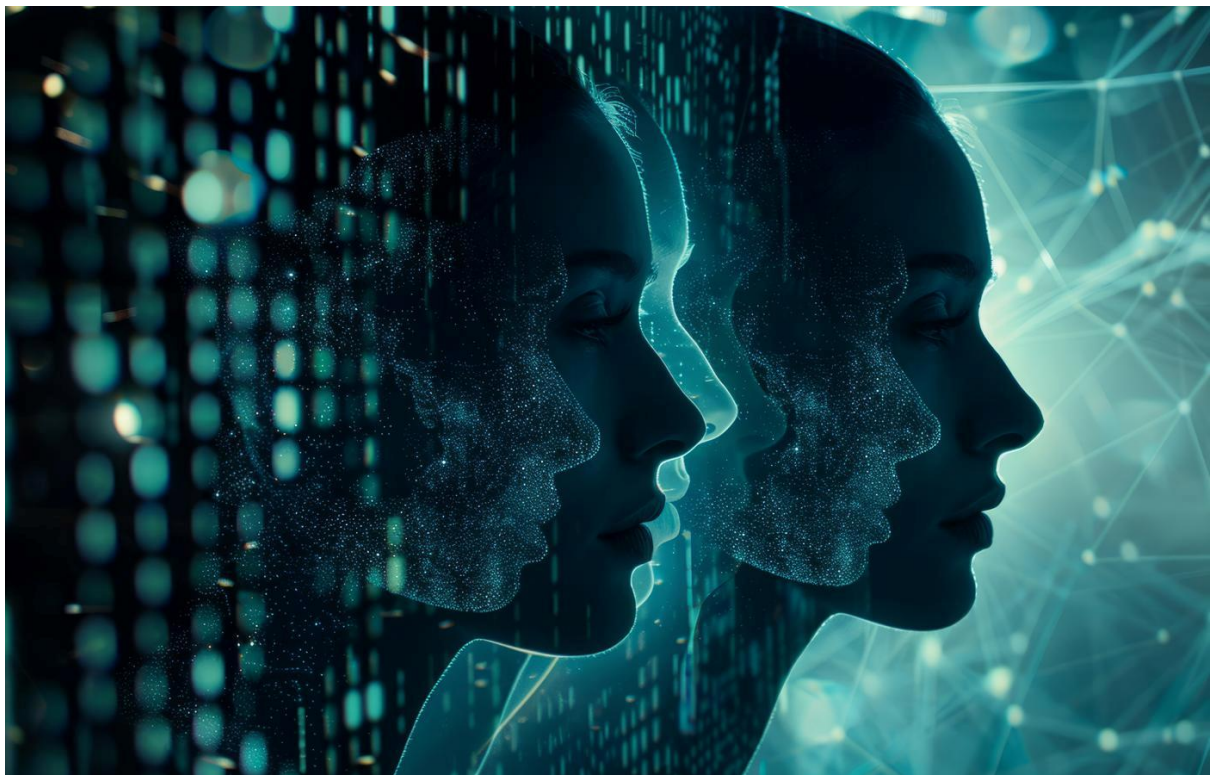
Threat actors are weaponizing deepfake phishing attacks in different ways:

- Email or messaging attacks
- Video calls
- Voice Messages
- Fraudulent Internet posts
- Financial and legal document fraud

Deepfakes often impersonate employees and partners.

If you are contacted by someone who claims to be a company employee, consultant or third-party partner, you should verify the individual's identity in the company whitepages before providing any information.

Tips to Spot Deepfakes



- Glasses may disappear or reflect differently.
- Features are positioned incorrectly or move.
- The hair and skin of the person looks blurry - or perfect,
- The audio doesn't match the video.
- The background does not make sense.
- The lighting looks unnatural or strange.
- The subject does not use language or mannerisms consistent with the person you know (e.g., can talk either too much or too little).

Tip: Ask the participant to turn 90 degrees and wave their hand in front of their face. While they will follow the cue, you can see the manipulation.

Deepfakes are evolving quickly, highly personalized, and extremely difficult to detect.

Stay vigilant!

