AI deepfake attacks and how to prevent them

AI is rapidly advancing, and we are encountering new issues every day. With AI technology being widely used by the public and regulations still being developed, AI-related crimes are on the rise. This month's newsletter focuses on AI deepfakes, the significant problems they are causing and how we can avoid becoming victims of an AI crime.

What is an AI deepfake?

AI deepfakes are AI-generated fake images, videos and audio recordings that look and sound just like real ones. These tools use real images and videos to create realistic-looking content for malicious purposes.

Recent deepfake attacks

$25-million-dollar heist

A Hong Kong corporation recently lost $25.6 million dollars to a deepfake scam. The scam began with a phishing attack: an email that appeared to be from the CFO was sent to an employee in the finance department. The email asked the employee to carry out a confidential transaction.

The employee became suspicious. However, he was asked to join a video conference call where everyone on the call seemed familiar. They asked him to carry out the transaction, which involved making fifteen transfers to five different banks.

Even after the transfers and approvals, the employee was still unsure about the transaction's legitimacy. Eventually, he contacted the company's head office, and they confirmed that it was a scam.

Everyone in that meeting? Scammers. They used deepfake technology to impersonate the CFO and other executives. In this case, the employee couldn't even trust the evidence of his eyes or ears.

Cricket star targeted

Indian cricket player Sachin Tendulkar was seen promoting a sports betting app. However, it was later revealed that the video was a deepfake — an AI-generated video that looked and sounded like the famous cricketer.

Deepfake videos like these are highly damaging to a person's reputation. The fake Tendulkar in the video was seen endorsing the betting app and even claimed that it had helped his daughter financially. He went to social media to express his concern: "It is disturbing to see rampant misuse of technology."

UMass Boston

Don't let them scam you

You get a call from what sounds to be like a family member. They've been in an accident or they're in jail, and they need you to send money as soon as possible. This is alarming ... but it should also be suspicious. Scammers now use audio clips from social media and voice cloning programs to impersonate individuals and request money over the phone.

If you receive such a call, **do not immediately trust the voice on the other end.** Be wary if they ask for money via wire transfers, cryptocurrency or gift cards. These are common methods used by scammers.

To avoid falling victim to such scams, **it is essential to slow down and verify the caller's identity through a reliable means of communication.** For instance, you can contact the individual in question through their official phone number or another trusted family member.

If you suspect you are or have been scammed, **do not hesitate to report it**. It is always better to share your suspicions with authorities or individuals who can help.