AI and deepfakes present new risks for internet relationships

June 6 2022

Credit: Pixabay/CC0 Public Domain

People looking for genuine relationships via the internet will need to become a lot more savvy about new technologies which expose them to romance fraud at an "entirely new level of risk," warns QUT internet fraud researcher Associate Professor Cassandra Cross.

Romance scams, which netted criminals $131 million from Australians in 2020 alone, are likely to get harder to detect as perpetrators are moving into using AI (artificial intelligence) and deepfake technology to deceive their victims.

With deepfake technology, offenders can not only use readily available images of another person and create a fake profile image, but they can also create an entirely synthetic image and corresponding profile without having to lift one from another person's social media or the internet.

Professor Cross, from QUT School of Justice, said the public had become aware of romance scams and had been advised to use detection methods such as a reverse image search on images sent to them in order to determine if the sender was who they claimed to be.

"This means fraud prevention campaigns will need to be revised to make people aware of this sophisticated and not easily detected method of deception," Professor Cross said.

"AI and deepfakes render reverse image searches virtually obsolete. There is a critical need to improve the technological response to AI and the fraud potential of deepfakes as there are limited means of detection available."

Professor Cross said many media reports had already documented the use of AI and deepfakes to deceive romance fraud victims.

"For example, a US woman sent multiple sums of money to a man she believed was a US Navy official. In this case, the offender manipulated publicly available images and recordings of a US Naval officer to create deepfake videos of the genuine person under a different identity," she said.

"As well as enabling offenders to lift images of living people and create realistic profiles, deepfake software can create an entirely believable but fictitious image and profile.

"The ability of technology to generate unique images for use in social media profiles has the potential to change how romance fraud and other deceptive online practices (such as catfishing) are perpetrated."

Professor Cross said deepfakes had evolved to encompass voice recordings and were a powerful tool when used with other fraudulent behaviors.

"For example, in business email compromise (BEC) fraud, offenders can use fake audio recordings to impersonate CEOs and other authoritative figures and target lower-level employees with urgent requests to transfer funds on their behalf.

"Clearly, prevention messaging needs to be targeted at the people who use dating platforms and social media platforms to form relationships and at the very least alert the public to the risks AI and deepfakes pose in these areas of their lives."

The paper was published in *Crime Prevention and Community Safety*.

More information: Cassandra Cross, Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging, *Crime Prevention and Community Safety* (2022). DOI: 10.1057/s41300-021-00134-w

Provided by Queensland University of Technology

Citation: AI and deepfakes present new risks for internet relationships (2022, June 6) retrieved 7 May 2024 from https://techxplore.com/news/2022-06-ai-deepfakes-internet-relationships.html