AI fuelling dating and social media fraud, EU police agency says

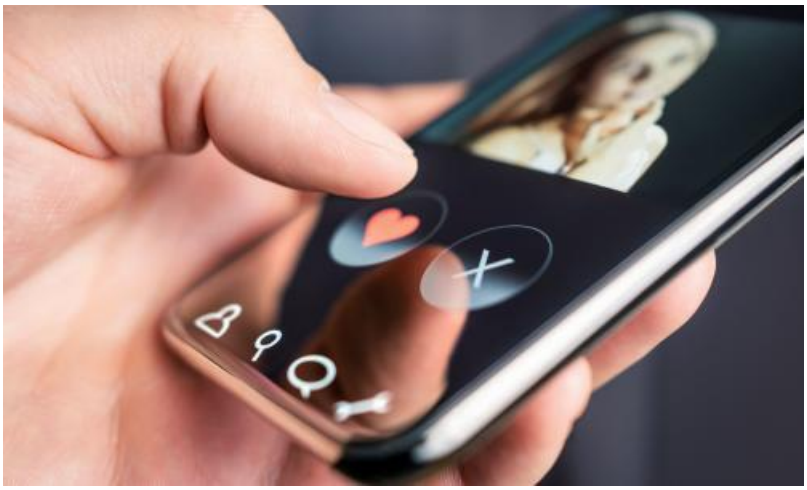
Publication Date: 2024-01-09

Author: Lisa O'Carroll

Section: Technology

Tags: Artificial intelligence (AI), Computing, Scams, Consumer affairs, Dating, Social media, Digital media, news

Article URL: https://www.theguardian.com/technology/2024/jan/09/ai-wars-dating-social-media-fraud-eu-crime-artificial-intelligence-europol



Artificial intelligence, combined with wars in Ukraine and the Middle East, is fuelling a boom in fraud on dating and social media apps, officials at Europol have said. Speaking to the Guardian, the agency's top financial crime experts said scripts generated by artificial intelligence enable criminals to target multiple victims at once. Sebastian Bley, the head of the Europol economic crime team in The Hague, said: "There is a trend of more and more cases of people saying 'I'm a doctor in a war zone' and asking for funds to be transferred out of that zone. They say they also need to get the family out." Burkhard Mühl, the overall head of the financial and economic crime unit at Europol, said: "It can involve tens of thousands of euros in one case." They also warned of a rise in "bogus boss" scams, with fraudsters spinning an elaborate web of fake websites, fake CVs and investor profiles to target a gamut of victims ranging from personal investors to tax authorities. The impact can be devastating, resulting in the loss of life savings and in some cases suicide. The EU's law enforcement agency, whose mission is to prevent and combat international and organised crime, analyses trends in fraud. It said AI is making it easier for scammers to increase their success rate, and there is an increase of "abuse using large language tools like ChatGPT," Mühl said. "With large language tools you can write thousands of tailored messages in different languages with different targets, different stories, and you can do that with your laptop from wherever," he added. The rise in dating fraud comes less than two years after a Netflix documentary, The Tinder Swindler, brought global attention to a man who posed as the son of a wealthy diamond mogul and conned several women out of money, one losing nearly €250,000 (£215,000) in loans. No matter how compelling their story is, "never send money to a person you haven't personally met", Mühl said. Bley and Mühl spoke of the devastating consequences and in some cases "revictimisation", when fraudulent financial advisers offered help to get money back. "People sometimes lose the life savings, investing in all kinds of products. We don't have statistics really drilling into those questions in detail but we hear from our investigators about cases that are quite dramatic – people jumping out of the window because they lost pension savings in investment schemes," Mühl said. The best solution is reporting the crime to the police, Bley and Mühl said, but they believe investor fraud is underreported because of the shame people feel. "It's not only the financial damage that hits the victims. It is also psychological damage," Mühl added. General investor fraud through text message scams is said to have risen by 40% in the UK since the launch of ChatGPT, according to British authorities. AI is bringing previously unseen economies of scale to the world of fraud, Bley said. He added that traditional fraud takes a lot of time to make things up and lure victims into a drawn-out narrative until they establish trust. AI can cut this out, with industrial-scale fishing for victims possible. "If you personally meet somebody, you

have to invest a lot of time making things up and to find the right victim," Bley said. "Online, it's easier to target a lot of people once you have feedback from somebody on the platform, something to continue with engagement. If you see it's not going to go anywhere you just turn to the next one. It's much easier to approach people." Europol said it believed Europe was being targeted by criminals operating outside the EU because of the "high standards of living" and because "people have money to invest". Last year authorities in India busted a bitcoin racket being operated out of a call centre in Delhi that was targeting Austrians. Fraudsters posed as Interpol investigators and called Austrians to advise them they were the subject of police investigations but if they went to a bitcoin ATM to exchange cash the inquiries would end. In a recent "bogus boss" case, criminals managed to steal €50m from a variety of companies and "major corporations that you would not consider to be victims", Mühl said. The criminals were "very clever", learned about company structures, set up fake websites and somehow were able to get in touch with investors, offering them "discount" shares.