Scamming the scammers: Using AI-created fake victims to disrupt criminal business model

June 26 2023, by Fran Molloy

Keep talking: Professor Dali Kaafar, pictured, and the cyber security team hope their new scam-fighting bots will keep scammers on the line for up to 40 minutes and also help identify the latest phone scams so banks can warn customers. Credit: Macquarie University

Macquarie University cyber security experts have invented a multi-lingual chatbot designed to keep scammers on long fake calls and ultimately reduce the huge number of people who lose money to global criminals every day.

A new AI-driven system has created convincing fake victims in the form of multi-lingual chatbots who waste the time of scam callers, in a quest to put a dent in the estimated $55 billion people lose each year to thieves.

Named Apate, after the Greek goddess of deception, the system will 'scam the scammers," using convincing voice clones to conduct conversations with real scammers.

"Phone scams are run by organized crime groups and currently only a tiny fraction of the criminals are caught, and the money is rarely recovered," says Professor Dali Kaafar, Executive Director of Macquarie University's Cyber Security Hub.

The idea came to Professor Kaafar while having lunch with his family, when a scammer called. He put on an entertaining pretense, keeping his kids laughing—and keeping the scammer on the line for 40 minutes.

"I realized that, while I had wasted the scammer's time so they couldn't get to vulnerable people, which was the point—that was also 40 minutes of my own life I wouldn't get back," Professor Dali says.

"Then I started thinking about how we could automate the whole process, and use Natural Language Processing to develop a computerized chatbot that could have a believable conversation with the scammer," he says.

Professor Kaafar says his team now has patents pending for this highly-effective technology.

"We are excited about the potential for this new technology to actively break the scam-calling business model and make it unprofitable," he says.

The hugely lucrative global phone scam trade is growing each year, and the ACCC estimates Australians lost over 3.1 billion to scammers in 2022.

Chipping away at easy profits

Professor Kaafar says despite telecommunications providers blocking well over half a billion scam calls since 2020, Australians are still flooded with these calls—and the tiny fraction that get through can wreak havoc on victims.

Phone scams are on the rise globally for a few reasons, he says.

Technology like voice-over-internet protocol (VOIP) makes it easy and cheap for cyber-criminals to mask their location, pretending to call from any number.

Meanwhile on the technology front, it is hard and expensive to update the telecommunications infrastructure and protocols to improve authentication of the calls.

"Financially, it's a high-gain, low-cost ratio for scammers, the practice is very lucrative and a relatively low-risk criminal activity—and it's pretty hard for victims to recover this money."

These conditions attract growing numbers of scammers who specialize in playing on human emotions and fears.

"The business model of scammers relies on making a large profit from a small number of victims; only a small percentage of the thousands of calls they make each week are successful," says Professor Kaafar.

"Our model ties them up, wastes their time and reduces the number of successful scams," he says. "We can disrupt their business model and make it much harder for them to make money."

How APATE was created

The team from the Macquarie University Cyber Security Hub began by analyzing scam phone calls and pinpointing the social engineering techniques scammers use on their victims, using machine learning techniques and natural language processing to identify typical scam "scripts."

They then trained chatbots on a dataset of real-world scam conversations from recordings of scam calls to transcripts of scam emails, and chat logs from social media platforms so the bot can generate its own conversations resembling those of real-world scam calls.

Professor Kaafar says advances in Natural Language Processing (NLP) and AI human voice cloning have allowed them to develop AI agents that are capable of fluent speech, and can adopt a particular persona and stay on track in a conversation, being convincingly consistent in their responses.

"The conversational AI bots we have developed can fool scammers into thinking they are talking to viable scam victims, so they spend time attempting to scam the bots," Professor Kaafar says.

These bots can be trained in any language or accent and because phone scams are a global challenge, this technology can be deployed anywhere in the world.

Live scam call trials

The team is now trialing the chat bots on live scam calls, redirecting calls intended for victims to their testing prototype, an "always-on honeypot" with a wide range of personas.

"We've put these 'dirty' numbers all around the internet, getting them into some spam apps, or publishing them on webpages and so on, to make them more likely to receive scam calls," Professor Kaafar says.

"We found the bots react pretty nicely to some tricky situations that we were not expecting to get away with, with scammers asking for information that we didn't train the bots for—but the bots are adapting, and coming up with very believable responses.

"The bots are continually learning how to drag the calls out to meet their primary objective: keeping scammers on the line longer. "

The current deployment of Apate bots are already averaging five minutes, and the aim is to get them to 40 minutes.

The scam-fighting bots also contribute to threat intelligence—timely information that is gathered about current phone scams and their targets; this helps organizations such as major banks, retailers and government bodies warn customers.

Professor Kaafar says the team is in conversation with a number of telecommunications providers and says they are open to a number of commercial partnerships.

"Partnering with communications providers will be the key to making this really effective," Professor Kaafar says.

"We see this as having huge potential globally; if we can redirect many of those spam calls that providers are currently blocking, and send the scammers to Apate bots, tying up their time as much as we can, the whole industry will no longer be viable.

"I suggest the ultimate meta-scenario might see scammers adopting AI themselves, training their own scam chatbots—which are then diverted into speaking to chatbots owned by the telecommunications providers.

"If scam chatbots end up talking to scam-defending chatbots instead of stealing money from real people—I'd take that as a big win."

Provided by Macquarie University

Citation: Scamming the scammers: Using AI-created fake victims to disrupt criminal business model (2023, June 26) retrieved 8 May 2024 from https://techxplore.com/news/2023-06-scamming-scammers-ai-created-fake-victims.html