FRANKON FRAUD

11 FRAUDS AND SCAMS SUPERCHARGED BY AI

AI will create new and in most cases better versions of old frauds and scams

THE DEEPFAKE CEO BEC FRAUD

Leveraging realtime video and audio cloning, fraudsters will engage in super realistic BEC attacks deepfaking CEO's and other executives to con employees to sending out wire transfers.

AI ENABLED EXTORTION SCAMS

AI generated sexually explicit images or even video are generated by scammers on victim targets and are then used to extort those targets of money with the promise that images won't be released.

PERFECT ROMANCE SCAMS

Realtime Deepfake video cloning and applications like Xpression Camera allow scammers to pull off incredibly real catfishing attempts against victims to convince them they are real.

FRAUD VENDOR AI ATTACKS

AI Bots are trained to attack retailers in "swarm attacks" to exploit the fraud solutions those retailers use. The bots can self learn and adapt the transaction patterns to exploit gaps in controls.

AI AUTOMATED CREDIT AND FRAUD DISPUTES

AI enabled software allows first and third party fraudsters to automate and perfect the dispute process including writing realistic handwritten dispute letters that fool banks and lenders.

AI GENERATED PHISHING ATTACKS

Using AI, CyberAttackers create highly personalized phishing emails that evade spam filters and are more likely to get clicked by targets. AI is then used to adapt and fine tune future attacks based on whether the user clicks the links or not.

AI GENERATED DOCUMENT FORGERIES

AI generated paystubs, bank statements and even identification cards will be created instantly with near perfect imagery and content, giving fraudsters the ability to create near perfect undetectable forgeries.

CHILD IN DANGER RANSOM OR BAIL VOICE CLONING SCAMS

Near perfect voice clones are created by scammers and then used to contact parents or family members to convince them their relative is in trouble and they must pay ransom or bail to get help them get free.

AI GENERATED MALWARE

CyberAttackers use AI to create autonomous malware trained to adapt to changing environments so it evades detection and evolves over time. Malware can be constructed by someone with no programming experience.

AI CONSTRUCTED FAKE RETAILER AND HARVESTING SITES

Using Generative AI, fraudsters will create fake online retailers with realistic products, photos, and services to harvest card details or engage in sophisticated triangulation scams.

AUTONOMOUS AI SCAM BOTS

AI Scam Bots are trained and released into the wild to interact with victims in human like chats, building relationship up slowly until they are primed to send money. Human scammers step in and engage in the final stages of the scam to extract funds from victim.