

Artificial Intelligence

AI (artificial intelligence) is using computer systems to perform tasks or produce emails, text or phone calls that would normally require a person. It has transformed scamming. Scammers exploit AI to increase their chances of success.

DEEP FAKE AND VOICE CLONING

Scammers use AI to create deep fake videos and images and voice cloning. Scammers use voice cloning to impersonate family, friends, or executives – such as in an emergency scam.

Deepfake videos or images use AI to generate the likeness of a real person. Scammers can use these to impersonate a public figure to promote a fake investment scheme, a family or friend to financial accounts.

Mary sees an ad on Facebook where the Prime Minister of Canada is urging residents to invest \$250 into a Federal Government program with the promise of making a huge profit. THIS IS A SCAM!

Scammers use AI to create messages with correct grammar and tailored content. This makes 'fake' emails and other messages much harder to detect.

CHATBOTS

Chatbots are a software app or web interface that converses through text or speech. Scammers use AI-powered chatbots to engage in long-lasting, emotional, and personalized conversations for romance scams via messaging and phone.

FAKE IDENTITY

Using AI, scammers combine real data (e.g. SIN) with fake info to create a 'new identity'. They use this made-up person to open bank accounts, apply for loans, and build credibility over time to maximize gains.

AI PAYMENT OPTIONS

Scammers favour cryptocurrency, digital wallets, money transfer apps, and other instant, non-reversible payment options. These are very hard to trace and make it impossible to recover funds.

FAKE PROFILES

Scammers use social media to create fake profiles or bots (automated apps) to build trust and gather information. They use these tools to impersonate friends, celebrities, or public officials; to trick people into sending money and personal or financial info.

SPOOFING

Spoofing is when the scammer changes the number on the displayed caller ID to make it look like it's from a trusted number, with a local area code – from a legit business, government agency, family member, or friend. Scammers use these apps or bots to disguise their identity and robocall many people at once.

OTHER AI METHODS

SIM card swapping, porting, and call forwarding are all legitimate services. Scammers use them to take over a mobile phone and control accounts. Banks and other entities often use one-time passcodes to authenticate the user. If the scammer has access to the phone, they can intercept the passcode, pose as the person, and start scamming.

Scammers use virtual private networks (VPNs) to hide their internet address. They use botnets to automatically attack a large number of people at the same time. A botnet is a network of internet-connected devices infected with malware.

Fake mobile apps and quick response (QR) codes may use legitimate names or brands. Scammers use these to steal personal info, intercept payments, or install malware to get control of devices and gadgets.

