C&N

Commercial Services Security Newsletter

March 2024 | CSN – Q1 - 2024

FS-ISAC

Reducing Risk When Using Artificial Intelligence

Artificial Intelligence (AI) is a term used almost everywhere. What is it? Is it right for your business?

The term "artificial intelligence" or "AI" has the meaning outlined in 15 U.S.C. 9401(3): *a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments* as defined in the 30 October 2023, Executive Order of the Biden-Harris Administration.

AI and Small Businesses

There are benefits of using AI in small business areas such as marketing and sales, drafting business plans, financial management, and human resources.

Forbes featured an article about a report on AI produced by the Small Business and Entrepreneurship Council (SBEC) that revealed a large percentage of small businesses are using AI tools. For some, AI is not a matter of if, but when you incorporate it to enhance your customer experience.

If you are planning to adopt AI into your business, there are several items you should consider such as in-house or outsourced development, compliance and privacy risks, and fraud scams.

The Survey Says:

- 75% of the surveyed small businesses (507 out of 676) utilize AI tools in their operations.
- 41% have used AI to redirect their own time and employee time to higher-value work
- 39% have invested in AI tools for innovative solutions for customer engagement and retention
- 34% have used cost savings to pursue growth opportunities for their business

- *SBEC*

Build, Buy, or Outsource

Whether you build your own AI or acquire software, remember the code being used is only as good as the human coding it. An internet search will yield numerous leads for free software, coding applications, or companies who do the work for you. Ensure you fully understand what you will be introducing into your business and any exposure to your customers. Important factors include compliance and privacy, governance, operational guidelines and training, security, and third-party management. *Forbes* shares an informative article that goes into discussing these in depth.

Additionally, the Cybersecurity Infrastructure and Security Agency (CISA) collaborated with international agencies to produce Engaging with Artificial Intelligence - joint guidance, led by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), on how to use AI systems securely. The guidance provides AI systems users with an overview of AI-related threats, as well as steps that can help them manage AI-related risks while engaging with AI systems. CISA also encourages developers of AI systems to review the recently published Guidelines for Secure AI System Development.

Cyber Risks

On 4 January 2024, the National Institute of Standards and Technology (NIST) released a paper titled Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations that identifies types of cyber attacks that manipulate the behavior of AI systems. This document is a result of an extensive literature review, conversations with experts from the area of adversarial machine learning, and research performed by the authors in adversarial machine learning.

AI systems can malfunction when exposed to untrustworthy data, and attackers are exploiting this issue. No foolproof method exists as yet for protecting AI from misdirection, and AI developers and users should be wary of any who claim otherwise.

AI and Fraud

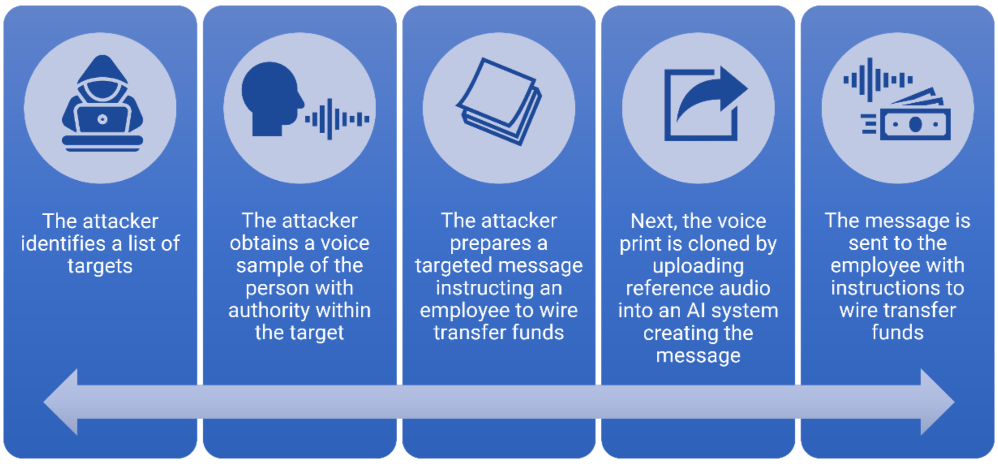
Criminal groups are already using AI in fraud attacks involving synthetic voice identification scams.

Comply Advantage said in its State of Financial Crime 2024 report, "AI is being deployed by criminals to perpetrate fraud, launch attacks against individuals and corporations, and gain access to the international financial system. AI has been linked to inciting terror attacks, generating deepfakes for ransom, extortion, and fraud, carrying out corporate espionage, and carrying out online account takeover fraud for profit."

DataBreach Today reports, "Fraudsters used deepfake technology to trick an employee at a Hong Kong-based multinational company to transfer $25.57 million to their bank accounts. Hong Kong Police said Sunday that the fraudsters had created deepfake likenesses of top company executives in a video conference to fool the worker."

Figure 1 reveals how the scammer can obtain a sample voice print.

Think about it - voicemail recording, electronic eavesdropping… How much talking do you do, and where are you having conversations? It's a lot to consider, and it's very concerning.



The attacker identifies a list of targets

The attacker obtains a voice sample of the person with authority within the target

The attacker prepares a targeted message instructing an employee to wire transfer funds

Next, the voice print is cloned by uploading reference audio into an AI system creating the message

The message is sent to the employee with instructions to wire transfer funds

Figure 1 Synthetic voice fraud example.

Prevention Tips

- AI can successfully be used to detect and prevent payments (card) fraud, but can also create fake accounts, execute account takeovers, and other types of fraud. AI also learns and grows the more it is used. Be aware of what AI programs are doing in your instance.
- Social fraud can be addressed through training – incorporating secondary controls that require another human to review and approve high-risk transactions, such as wire transfers.
- Protect your client's data with encryption during transmission and at rest.
- Adopt an AI framework and policy[1] for your customer's review and ensure that you can do what you place in writing. Outline how permissive or stringent you are with the data.
- When outsourcing AI to a company, perform your due diligence as a critical vendor. Ensure that thorough risk management is performed and obtain adequate insurance.

If You Think You've Been Scammed

If you suspect your business has fallen victim to a scam:

- Contact [YOUR INSTITUTION NAME HERE] immediately so we can act and provide recommendations
- Report suspicious activity to the Internet Crime Center, www.ic3.com, and/or your local law enforcement agency.

[1] FS-ISAC Framework of an Acceptable Use Policy for External Generative AI https://www.fsisac.com/hubfs/Knowledge/FrameworkOfAnAcceptableUsePolicyForExternalGenerativeAI.pdf?hsLang=en