From Nigerian Princes to AI Agents: How Scams Are Evolving in the Age of Artificial Intelligence

KISSIMMEE, FL, UNITED STATES, June 9, 2025 /EINPresswire.com/ -- The original email scam—often mockingly called the "Nigerian Prince" scam—was simple, crude, and surprisingly effective. Today, it has evolved. But instead of a desperate prince, you are now getting emails or texts from hyper-intelligent AI agents pretending to be investors, co-authors, family members, or even auditing officials claiming you're owed millions. And they're much harder to spot.

We are entering an era of AI-enhanced deception—and the threats are not only more convincing but also scalable, relentless, and increasingly integrated into business, politics, and society. We already had a tough time with all the nation-state sponsored criminal and hacking activities – now we must deal with any criminals that have figured out how to use ChatGPT or any LLM. Maybe the tech execs building them are right – buy land in the Midwest without utilities, build a bunker, and you will be fine. For all of us that do not have AI bunker money, here are some things to look out for.

Welcome to the Age of AI-Powered Scams

The AI revolution has empowered not just businesses and developers—but adversaries, fraudsters, and nation-state actors. Here are the most common and concerning forms of AI-driven scams and misuse:

1. Conversational AI Scams

AI-powered phone scams can now hold entire conversations with victims. These voice agents never get tired, never miss a beat, and never call in sick. Some have been used to impersonate executives, law enforcement, or even relatives in distress—convincing targets to wire money or disclose sensitive information. With the voice sampling and ability to conduct open-source intelligence on just about anyone – you should be aware that you should never answer the phone or respond to a text unless you really know who is on the other side of that phone. Not to mention many of these scammers use emails before the calls so they can show up on your phone as someone you might know...

2. Hyper-Realistic Phishing & Fake Websites

With tools like generative image editors and AI web copiers, attackers can now create fake websites that mirror legitimate businesses with near pixel-perfect precision. You might think you're logging into your bank, healthcare portal, or even a trusted vendor—when you're actually handing over credentials to a hostile AI. Don’t just click the hyperlink – go directly to the browser and type the name of the organization or bank in…

3. Email and Message Manipulation

Modern LLMs like GPT can generate personalized, persuasive phishing emails based on publicly available information (LinkedIn, social media, press). These aren’t the typo-filled spam messages of yesterday. These are well-written, targeted communications engineered to trick you. If it sounds too good to be true or you don’t recognize the person or even the way they are reaching out – ignore them or call them directly and ask – especially before you leak any information or try to pay for anything.

4. Zero-Day AI Attacks

AI can now analyze defenses in real-time and create adaptive phishing or malware payloads. These are attacks your antivirus won’t recognize and your firewall won’t catch—because the code morphs each time it’s generated. Zero-Day attacks were already an issue when we had humans and some code logic to uncover them. Now this is simply and AI vs AI war – if your provider does not employ AI, you really have zero chance here.

5. “Fake AI” Startups

In the investor gold rush, many companies are claiming to be “AI-first”—but they’re really just layering ChatGPT or any LLM over a simple UI. Some don’t even bother with that – I have met AI companies that are literally just using ChatGPT. It's a vaporware with a pitch deck. Others go so far as to raise money on claims of proprietary models that don’t exist or worse ask the AI in front of you to answer their ridiculous claims. Tech experts do not run these companies they seem to mostly run by people jumping on the AI wave that have never surfed in the tech waters before.

6. Full-Blown Information Operations

From deepfake videos and synthetic voice impersonations to AI-generated evidence, entire nation-state campaigns are now leveraging AI to sway elections, manipulate public discourse, and undermine trust in truth itself. You have seen the “fake news and disinformation” but now

instead of recruiting a bunch of followers – these campaigns are deploying AI agents that build trust, respond to your posts, and slowly but surely real you into their side of the story....

The ZeroTrusted.ai Response

At ZeroTrusted.ai, we saw this coming. That is why we built a model-agnostic AI security and governance platform—to monitor not just your data, but your AI agents, prompts, APIs, and even the reliability and ethics of model outputs. Our AI HealthCheck and AI Judge systems identify anomalies, detect misuse, and help organizations enforce boundaries in an increasingly boundary-less world.

You cannot stop AI from being used by criminals or becoming SkyNet. But you can stop your AI systems from being exploited by them—or worse, becoming them.

Final Thought: Be Skeptical, Be Secured

If you receive a message offering you millions out of nowhere, ask yourself: Is this a scam?
In 2025, it might not be a prince. It might be an AI agent, trained to say exactly what you want to hear.

The only difference? This one speaks better English, knows your background, and sounds completely real.

Catie Moore
Lifestyles CFL
+1 407-449-2022
email us here