

AI is affecting security in every part of the communications infrastructure. Research and advisory firm Metrigy found that collaboration security incidents are up 300% since 2021, while a report from TransUnion finds that 70% of telecom fraud incidents are now occurring through online channels. Rounding out the picture is a report from security vendor Pindrop, which found that fraud in contact centers now occurs in one of every 599 incoming calls, representing a 26% increase year over year and a 100% increase when compared to 2021.

Here are four ways that AI is weaponizing vulnerabilities in communications infrastructures today.

1 Identity Spoofing

In the context of unified communications, identity spoofing can take the form of caller ID spoofing, sending realistic SIP requests that wreak havoc on the system; phishing; vishing; toll fraud or endpoint identity spoofing. Hackers do this by manipulating identifiable information to impersonate a legitimate source, and enter the system by manipulating network or email protocols.

“If I can capture a snippet of your voice, I can pretty much create a voice bot or real-time translation to impersonate you using AI” explained Irwin Lazar, president and principal analyst at Metrigy. “We see it on the consumer side to hack into bank accounts, and we see it in enterprises where people might impersonate someone to call into an IT service desk and gain credentials.”

The situation has gotten so bad that some companies have stopped using voice biometrics for user validation altogether, since they are so easy to impersonate. In the past few months, both AWS and Google have ended support for their voice biometrics solutions, and Microsoft is headed in the same direction.

Part of the solution, Lazar said, is to rely more heavily on network APIs. “We’ve seen companies like Ericsson and Nokia working on the ability to send out a network API call that would determine where the phone is located, if it has been jailbroken, if it has the original SIM, etc.,” he said.

There are also systems, he said, that will help authenticate inbound contact center calls by establishing secure, private connections.

A growing area of identity spoofing is malicious avatars, which use AI-based facial recognition, 3D rendering and deepfake technology to create hyper-realistic avatars for real people.

Scott Murphy, a consultant at Data Perceptions and an expert in the field, has seen this first-hand.

“I was talking to the CEO of a company, or I thought I was, when the actual CEO cut into the meeting and asked how it was going,” Murphy said. “That shows how avatars could easily replace a person in a meeting and depending on how it’s programmed, mislead people.”

The best way to stop them, Murphy said, is by employing federated and central authentication services. Today, he said only about 50% of companies are authenticating properly and effectively.

2 Hyper-Personalized Phishing

Like identity spoofing, hyper-personalized phishing is intended to trick someone into performing an action or trusting the sender. But hyper-personalized phishing takes it further, using AI to collect personal data from a variety of sources and social engineering to create a sense of urgency or false familiarity. It often uses techniques like deepfake voice and video, along with AI-powered tools for content generation. These campaigns tend to be highly targeted and customized, focusing on a specific person or small group.

To fight hyper-personalized phishing, Murphy suggested using some type of verifiable credential identity protocol that issues digital, tamper-proof credentials verifying that a person is who they say they are.

3 Adaptive Malware

Adaptive malware is malicious software imbued with AI, empowering it to continuously adapt by modifying code, changing attack vectors and customizing payloads, all with the goal of circumventing security defenses. AI-based adaptive malware can show up in the form of ransomware, botnets or social engineering.

“If you think about the vulnerabilities typically associated with unified communications, it could be someone registering a client who shouldn’t have the ability to connect into a system,” Lazar explained. “If I could connect a softphone, I could connect to some other software client that I’ve hacked and get into your system that way. Then I could inject a link into a conversation so that somebody clicks on it and then that installs malware on their machine.”

The best way to fight adaptive malware is by using AI itself, in the form of a tool that could identify vulnerabilities, Lazar said. That would help ensure that those vulnerabilities were fixed before being exploited.



4 AI-Driven Bots Coordinating Massive DDoS Attacks

During the first quarter of 2025, Cloudflare reported a 358% year-over-year increase in DDoS attacks. Much of that was undoubtedly caused by AI-driven bots. AI and machine learning enable bots to quickly analyze a target's defenses and weak points, and shift attack patterns in response. These bots also can mirror legitimate user traffic, making them more difficult to pinpoint. It's also easier than ever for less experienced hackers to get in the game, using tools like FraudGPT and WormGPT to generate scripts and automate responses.

"Some of these AI bots are very well-written and do a good job of getting in," Murphy said. "Contact centers could be a target, because they could tie up all of your SMS queues, web chat queues and phone queues, bringing the business to a halt."

The only way to get ahead of these AI-driven bots is by using AI itself, he said. "There is so much data coming into most security systems that if you try to review all those incidents and the alerts manually, it won't be fast enough. It's more effective to use AI to weed through all of that noise and find the real stuff."

It's also critical to make sure DNS is set up properly, with the proper security. "You'd be surprised how many organizations don't even use two-factor authentication, have the proper configurations for email, or have DMARC [Domain Message Authentication Reporting] and DKIM [Domain Keys Identified Mail] set up properly," Murphy said. "And even if they do, often they aren't integrated from a security detection and response perspective."

It's also important to keep policies updated to ensure that the right people have the right permissions—and that others don't, Lazar added. Finally, it's important to understand exactly what technology the company is using, including what software people may have procured without permission. Without that information, it's very difficult to have visibility into AI risks. A recent report from BigID brought the point home, finding that 64% of organizations lack visibility into their AI risks.



Thank you for reading.

For more resources like this, visit our [Knowledge Hub](#).

