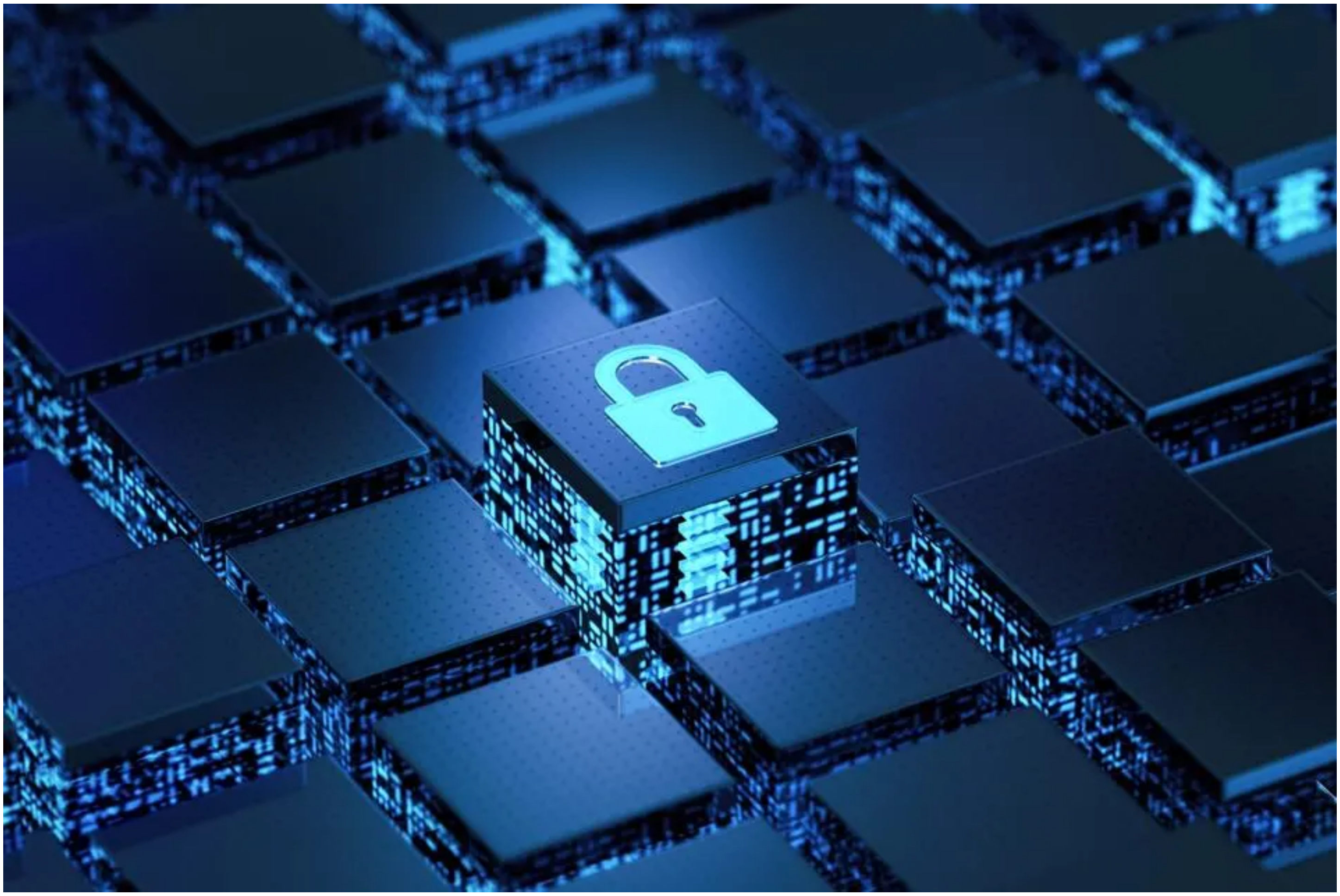
Cybersecurity Threats: How To Fight AI With AI

Christophe Van de Weyer

Christophe Van de Weyer is the Chief Executive Officer of Telesign.



getty

The promise of AI to enhance and scale human work is stunning. But unfortunately, it holds the same promise for those with ill intent. When GenAI applications began rolling out nearly two years ago, fraudsters were among the early adopters.

The best example is how GenAI is used for phishing. As CNBC reports, “Since the fourth quarter of 2022, there’s been a 1,265% increase in malicious phishing emails, and a 967% rise in credential phishing, according to a new report by cybersecurity firm SlashNext.” Phishing emails, often posing as if they are sent from someone at a financial institution, trick a person into providing their credentials. According to StationX and others, it’s the culprit in over one-third of data breaches. It also has an evil cousin: “smishing,” when a user is tricked by a legitimate-looking text (also known as SMS) message.

Generative AI allows users with criminal intentions to write very convincing copy at scale. We used to be able to detect phishing from the poor grammar and syntax in the messages, the telltale signs that it’s not actually your bank but someone in another corner of the world who has a poor grasp of your language. This is no longer the case. GenAI can write a scam message in the language of the target and in the tone of a financial institution.

GenAI is also being used to create more convincing social engineering via the creation of synthetic identities, which mix legitimate and artificial data to create fake profiles, complete with AI-designed profile images. It's being used to mimic human voices in scam-motivated phone calls. It's used to write malicious computer code and to automate attacks. One lesson companies should take from the rise of AI-infused fraud is not to neglect their own use of AI to bolster defenses.

Infuse Authentication With AI

The front door is the best place to stop a digital intruder. Fraudsters understand this well, which is why they invest in creating fake accounts or stealing credentials. The great news is that machine learning (ML), the function of AI that absorbs data and learns from it at lightning speed, never sleeps. It possesses the incredible ability to constantly learn how fraudsters behave and compare it to how typical, legitimate users act. The best cybersecurity vendors leverage it for exactly this purpose.

For example, AI can analyze the typical use patterns of billions of devices and phone numbers used to log in to critical accounts, such as email or bank accounts, to find unusual behavior. For instance, if a device that pinged from San Jose, California 30 minutes ago is suddenly signaling it is in Prague, in the Czech Republic, something is likely amiss.

The same goes for signals from a device being used to log into an email account or a ping from a mobile device to a cell tower. AI runs data analysis that helps you understand geographic and other behaviors and determine when additional caution is needed. These are among the ways AI can risk-score instances of devices attempting to log in, such as a mobile phone or a PC with a passkey system, and tailor the number of authentication steps accordingly. A device showing more potential fraud signals means more friction, whereas a lower-risk device sails through faster.

How AI Stops Other Forms Of Fraud

Another growing threat is SIM swaps. Here's how it works: First, a criminal who has found some of your personal information on the dark web tricks your mobile phone service into transferring your phone number. Now, with a mobile phone associated with your phone number, they start requesting password resets via a one-time password (OTP). They might first reset your email password before moving on to your bank or retirement accounts.

Using this process, a fraudster can literally turn a person's life upside down within a single day. The great news is that AI can detect signals that a customer has potentially been the victim of a SIM swap by recognizing that baseline patterns have changed—the person who stole your phone number is typically in another city if not another country—and automatically increase the friction required before a transaction goes through. This increases protections for customers from having their accounts infiltrated after a SIM swap and ramps up safeguards against fraudsters infiltrating your digital ecosystem.

“Toll fraud,” or its longer name, International Revenue Sharing Fraud (IRSF), is also an area in which AI is helpful. Toll fraud is a scheme that blasts a company with requests to send SMS, one-time-passcodes to phone numbers that charge a fraudulent fee**.** Think of toll fraud as forcing a company to use the numbers over and over for SMS communication.

You can guard against fraudsters hijacking routine business processes and committing digital theft. Machine learning can analyze phone number behavior and, for example, alert you to phone numbers with a history of sending giant batches of SMS messages in a short period of time—a telltale sign of IRSF attacks.

Assess How Cybersecurity Vendors Leverage AI

Many established vendors, including CISCO, IBM, OKTA and others, allow their customers to use AI to fight a plethora of other kinds of attacks, including those that come from malicious IP addresses and malware.

There are also innovative startups using AI for cybersecurity in new ways. BioCatch, for example, uses ML to analyze human digital, physical and cognitive behavior. Its AI platform allows financial and other institutions to risk-score sessions—which often include transactions—when anomalies suggest account takeover or other kinds of fraud.

Look for vendors who leverage AI and machine learning to understand how fraudsters think and behave compared to everyone else. This allows you to risk-score transactions, logins, sessions and more. This information can help differentiate legitimate intentions from fraudulent ones and inform your decisions about other security steps required before that online process can continue.

The bottom line: Whether you are considering a legacy cybersecurity provider or a startup, look seriously at how they leverage AI to fight AI-powered fraud.