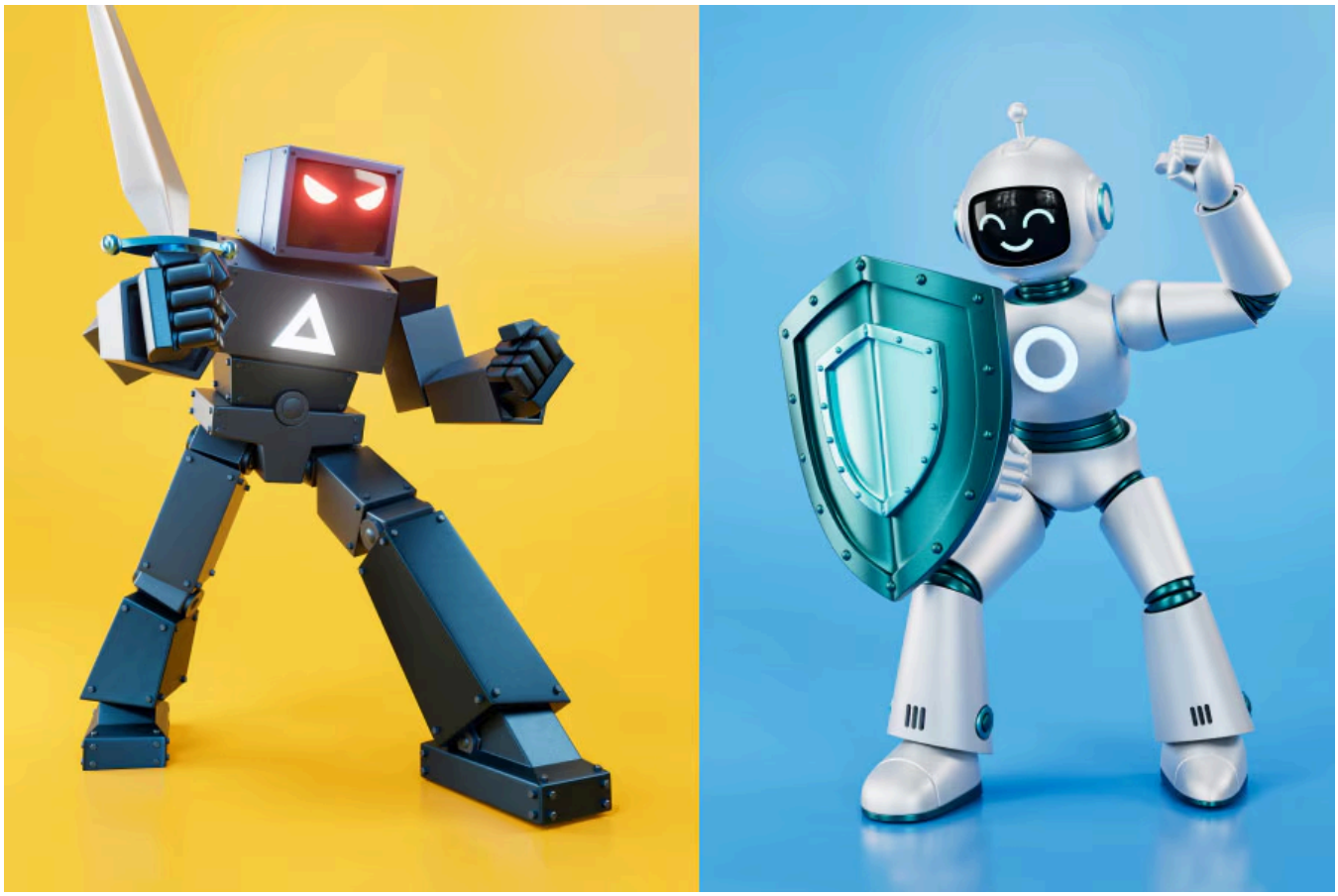
FRAUD PREVENTION >

The Evolution of AI Fraud: Offense and Defense

Artificial intelligence (AI) is making cyberscams easier to execute and more convincing. But financial institutions like Schwab are using the same tools to combat AI fraud.

June 5, 2026



When it comes to your finances, artificial intelligence (AI) is both a threat and a powerful defense.

On the one hand, targeted communications fueled by information AI has collected about *you* are replacing one-size-fits-all robocalls and generic spam. "We're seeing fraud that feels more personal, incorporates real information, and creates a sense of believability and urgency," says Kim Bailey, a senior manager on Schwab's Financial Crimes Risk Management team.

On the other hand, "we're using AI, too," says Zack Rosebrock, director of eCrimes Research & Detection at Schwab, noting that Schwab is investing in AI-powered detection systems that can identify patterns and unusual behaviors at a scale impossible for human monitoring to achieve.

"Bad actors collaborate and evolve quickly, so responsible institutions must do the same to protect their clients and the broader financial ecosystem," says Kim, who observes that individuals, too, have a part to play.

Here's what to know about the current threat posed by AI—and how to help protect you and your loved ones.

The current threat landscape

Despite consistent technological advances, AI can't orchestrate financial fraud on its own. For the time being, at least, criminals must still build networks, develop tactics, and actually implement their schemes. But AI makes all of this far easier to do at scale—and helps fraudsters improve their scams by identifying potential victims, testing their defenses, and adjusting tactics based on their responses *in real time*.

Common scams that rely on AI include:

- **Deepfake videos** designed to imitate a real-life person or situation. In Hong Kong, for example, a finance worker at a multinational firm was tricked into paying $25 million to fraudsters after attending a videoconference call that impersonated the company's chief financial officer and other recognizable staff members.
- **Fake personas** that pretend to be renowned financial experts or other public figures, often with false documents or other materials to establish their bona fides or bolster their claims. "As financial institutions have improved their defenses, criminals are attempting to manipulate clients into providing access themselves—

often by impersonating people within the very institutions designed to protect them," Zack says.
- **Voice cloning**, in which a scammer uses a specialized app or program to recreate the voice and speech patterns of a colleague or loved one with just a few seconds of recorded audio—usually found in interviews, social media videos, or voicemails. The FBI released guidance on such scams, known as vishing, when fraudsters impersonated government officials last year.

"Identity theft has always been a risk, but AI has made it more persuasive and difficult to detect," says Zack. "And we've seen that criminals are actively refining their methods."

Want to learn more about financial fraud?

See the latest content

Warning signs

Gone are the days of obvious grammatical errors or awkward phrasing in an email. Today's AI-generated content often sounds natural and looks professional, using real company logos, email addresses, and phone numbers—a tactic known as spoofing. A call, email, or text may look like it's coming from a trusted financial institution—your phone may even identify it as such—but that doesn't mean it's really from them.

"I almost fell for one," says Jill A., a Schwab client from Florida. "It was so realistic. I can see how we're all vulnerable now."

Kim says to watch out for three red flags that are common to fraudsters but virtually unheard of among well-established financial institutions:

- **Pressure to act immediately**, particularly when it comes to moving money. "No reputable financial institution will rush you," Kim says.
- **Requests for login credentials**. Legitimate organizations will never call, text, or email asking for your login and password. "Sharing those credentials is like giving a thief your house keys," Zack says.

- **Unexpected investment opportunities** that promise high or guaranteed returns. If it seems too good to be true, it probably is.

Of course, the most powerful defense remains what Zack calls actual intelligence. "AI can make people say things they've never said, but when the target knows the person supposedly speaking, the deception usually falls apart," he says. "We're still smarter than the computer. Be aware, take a breath, and ask yourself, *Does this make sense?*"

If you feel uncomfortable for any reason, hang up and contact the person or institution at a known or publicly listed telephone number to confirm the previous call's legitimacy. "If you realize you have indeed fallen victim to a scam, time is of the essence," Zack says. "Alert your financial institution immediately and preserve the communications to report the incident to authorities."

It's also important to share these strategies in order to protect the identities and finances of your family members of all ages.

"These scams can be especially convincing to the vulnerable," says Mark G., an investor from California. "I worry about my in-laws, who suffer from dementia and Alzheimer's."

Kim recommends several proactive steps:

- **Openly discuss the threat landscape**, including any recent scams you may have read about in the news.
- **Designate a trusted contact for financial accounts**, which authorizes your financial institution to consult someone of your choosing under specific, limited circumstances—if they are unable to reach you or suspect possible financial exploitation, for example. "A trusted contact serves as an extra layer of security for your account but does not have the authority to access your account, make decisions, or execute transactions on your behalf," Kim says.
- **Establish personal verification methods**, such as a password or phrase family and friends can use to easily authenticate their identity. "Our family has a special code word to prove we are talking to the actual person," says Mayer L., a Schwab client from Florida.

Add or review trusted contacts for your Schwab accounts.

AI as a force for good

While much of the conversation around AI and fraud focuses on the problems created by the technology, artificial intelligence can also be part of the solution. For example, Kim notes that some AI programs can identify synthetic voices, which can help if an impostor calls the company using AI to impersonate a client.

"Voices are like fingerprints—no two are alike. While it can be difficult for humans to pick up on the tiny tells that indicate AI-generated audio, these tools can help us detect fakes trying to game the system," Kim says.

Intercepting synthetic voices

With the rise of AI-enabled fraud, it's natural to worry that a digital mimic could compromise your accounts. However, while deepfakes may be good at tricking the *human* ear, they're no match for sophisticated technology—which is what makes Schwab Voice ID so secure.

When you enroll, the system creates an encrypted digital voiceprint—*not* a recording—based on hundreds of elements that are unique to your voice and speech patterns, including cadence, frequency, pitch, and tone. During a call, it not only analyzes information about the carrier, device, network, and more, but it also monitors background noise to help distinguish a live environment from a synthetic recording.

"Our systems are continuously updated to adapt to emerging threats like deepfakes and synthetic voices," says Mike Uhlenkamp, director of voice products at Schwab. "So even if a spoofed call sounds like you, the technology knows it's not."



Learn more about Schwab VoiceID.

Other ways that AI can help uncover and prevent fraud include:

- **Anomaly detection**: AI can analyze millions of data points in seconds and recognize patterns associated with fraud. For example, an AI-enabled system may be able to

spot a transfer to an account that has been flagged as potentially fraudulent, block the transaction, and send an alert to the account owner.

- **Behavioral biometrics**: AI can track how you typically swipe, type, and navigate apps, assembling a profile that distinguishes you from bots attempting to take over your account.
- **Document checks**: Computer vision (CV)—the same technology behind everything from self-driving cars and facial recognition to medical diagnostics—can also verify invoices, pay stubs, personal IDs, and other records by comparing them against a database of validated documents and pinpointing possible tampering.
- **Network analysis**: By mapping interconnected systems, AI can differentiate between legitimate relationships among accounts, devices, and merchants and those of bad actors seeking to exploit the complex global financial system.

Rather than rely on digital defenses alone, many financial institutions—including Schwab—take a layered approach to fraud prevention, combining technology with education and human oversight. This involves enhanced monitoring for unusual activities, stronger verification processes for higher-risk actions, and clear, timely communications—especially at moments when risk is highest.

What's more, Schwab works closely with other financial firms, law enforcement, and information-sharing groups to identify emerging threats.

However, for all the technological advances, awareness and human judgment are still our strongest defenses against fraud. "AI has forever altered the threat landscape, but there's no substitute for common sense," Kim says. "When something seems off, don't hesitate to slow down, verify the details, and ask for help from someone you trust. That moment of pause could be the difference between protection and loss."