

Tech Fix – NY Times

A.I. Is Making Scams Hard to Spot. Here's How to Protect Yourself.

A criminal could be masquerading as a celebrity, web store or family member asking for your money.

Detecting scams requires a new approach.



By [Brian X. Chen](#)

Brian X. Chen is the author of [Tech Fix](#), a weekly column about the tech we use.

- May 28, 2026

An email riddled with typos. A customer service agent with a thick accent. A blurry Craigslist photo.

Those used to be telltale signs of internet scams. But today, thanks to generative artificial intelligence, those red flags have mostly vanished. Low-cost chatbots, image generators and voice-cloning tools make it simple for criminals to produce pristine copy, create seemingly legitimate websites and even replicate identities.

A.I.-powered internet scams have become so convincing that I confess I almost fell for one. While mindlessly scrolling through TikTok videos, I came across an ad for a pair of Hoka sneakers marked 80 percent off. When I tapped on it, a website loaded that looked like an authentic clearance outlet for the shoe brand.

But after I added the shoes to the shopping cart, my Spidey sense went off. A quick web search revealed that users on Reddit had been scammed by this site; Hoka had even published a [warning about a surge of fake web stores](#) masquerading as its brand.

These look-alike websites are one of several A.I.-fueled internet scams that have recently been on the rise, security experts say. The F.B.I. reported last month that cybercriminals had defrauded Americans of nearly \$21 billion last year, with about [\\$893 million in losses linked to A.I.](#)

Because A.I. makes it effortless to build websites and digital avatars, we may have to rethink our approach to protecting ourselves from online fraud.

“Instead of looking for indicators of what’s bad, now you need to be verifying if it’s good,” said Mark Beare, a general manager for Malwarebytes, an internet security firm. “It’s not a Nigerian prince anymore. It’s a look-alike site for REI or eBay or any one of those known, reputable brands.”

Scam ads have been so rampant that legal complaints against the social media giant Meta are mounting. Last month, the Consumer Federation of America, a nonprofit advocacy group, [filed a complaint](#) accusing Meta of misleading users about its efforts to combat scams. The complaint cited examples including scam ads for baby gear and free phones. California’s [Santa Clara County filed a similar lawsuit against Meta](#) this month.

In response, [Meta said that last year, it removed 159 million scam ads](#) and took down nearly 11 million accounts on Facebook and Instagram associated with known producers of scams. It added that it was investing in new technology to combat scams.

A TikTok spokeswoman said that the company prohibited deceptive practices and misleading content in ads, and that attempts to defraud users were not allowed on the platform. She added that in the fourth quarter of 2025, 97 percent of violating spam content that TikTok removed was taken down before users reported it.

Other than fake stores, scammers have used A.I. to pretend to be someone close to their victims, including family members and old flames. To put it another way, A.I. has made it possible for criminals to tailor their attacks to be more personal than ever before.

Here’s what to know about the most common A.I. scams and what to do.

A.I. Cat Fishers and Impersonators

Everyone is familiar with the text message coming from an unknown number saying something along the lines of “It’s been a long time. How have you been?” Engaging with the sender could end with a phone conversation and the scammer asking for cash. Today, that conversation is likely to shift to a video call because fraudsters have discovered they can use A.I. [tools that digitally transform them](#) into someone else.

“It’s very easy and very cheap to do a real-time Zoom call with whole body replacement and voice changing in a way that’s completely realistic,” said Andrew Yoon, a researcher at CivAI, a nonprofit that teaches people about A.I.’s capabilities.

This scheme could take on different forms depending on the victim’s interests and weaknesses. A lonely male may be tricked into believing that an attractive woman from his past is hoping to reconnect. A job seeker could be duped by a phony A.I. interviewer into doing work for a bogus company.

And because phone numbers are easy to fake and the names and contact information for our relatives are publicly available online, the scams can get much more personal. A mother could receive a fraudulent text message from her son’s phone number and eventually get on a video call with an A.I. simulation of him, where the impersonator asks for money.

Mr. Yoon suggested a low-tech antidote: Have conversations with family members, especially any older relatives inexperienced with tech, to discuss the possibility that they might get a call from an impersonator. Establish a secret safe word that can be used to test whether someone is real, whenever in doubt.

The Fake Celebrity

Since the arrival of instant video generator apps like OpenAI’s Sora, [social media has been flooded with A.I.-fabricated slop](#). Fake videos featuring Hollywood celebrities and high-profile business executives are widespread because so many images and videos of them are available on the web to help A.I. models generate near-perfect imitations.

Some scammers have tried to exploit celebrities by using their star status to market nonexistent products. Deepfake videos of the chef Gordon Ramsay, for instance, circulated on social media in the last few years endorsing a cookware giveaway; victims who thought they were paying a small shipping fee for free frying pans were handing their credit card numbers to criminals.

Abusers also generated deepfake videos of Richard Branson, the founder of the Virgin Group, to lure his fans into making phony investments. It

happened so often, he posted an Instagram video educating his followers [on how to spot these types of scams](#).

Mr. Branson's advice was spot on. Trust only information from official sources — for example, in the case of Mr. Branson, a webpage published on Virgin.com. Blue checkmarks on social media sites are not foolproof indicators that people are who they claim to be, so don't let them lure you into shady get-rich-quick schemes.

The Cloned Store Brand

Ads that direct you to A.I.-generated scam sites, like the sneaker shop that almost tricked me, are prolific on social media. The ads may be directly relevant to your personal interests — for instance, if you encounter a fake store selling a bicycle.

That's because the scammers pay for ad space on TikTok and Instagram to leverage the same tools that real marketers use to target ads at people with relevant interests, said Mr. Beare of Malwarebytes. Criminals can afford to spend those dollars on ad-targeting because — unlike real brands — they have no product to ship.

There are ways to quickly determine whether an online store posing as a brand is fake. A simple method is to do a Google search for the store's web address and see what people are saying about it on sites like Reddit.

For more thorough scam detection, you can also ask an A.I. chatbot for help. Malwarebytes recently teamed up with [OpenAI](#) and [Anthropic](#) to connect its free scam-detection app to the ChatGPT and Claude chatbots. You can paste a web address and screenshots into the chatbots and ask Malwarebytes to run an analysis on whether a site is legitimate.

If that sounds like too much work, there's one age-old piece of conventional wisdom that is still true in the era of A.I.: If something seems too good to be true, it probably is.