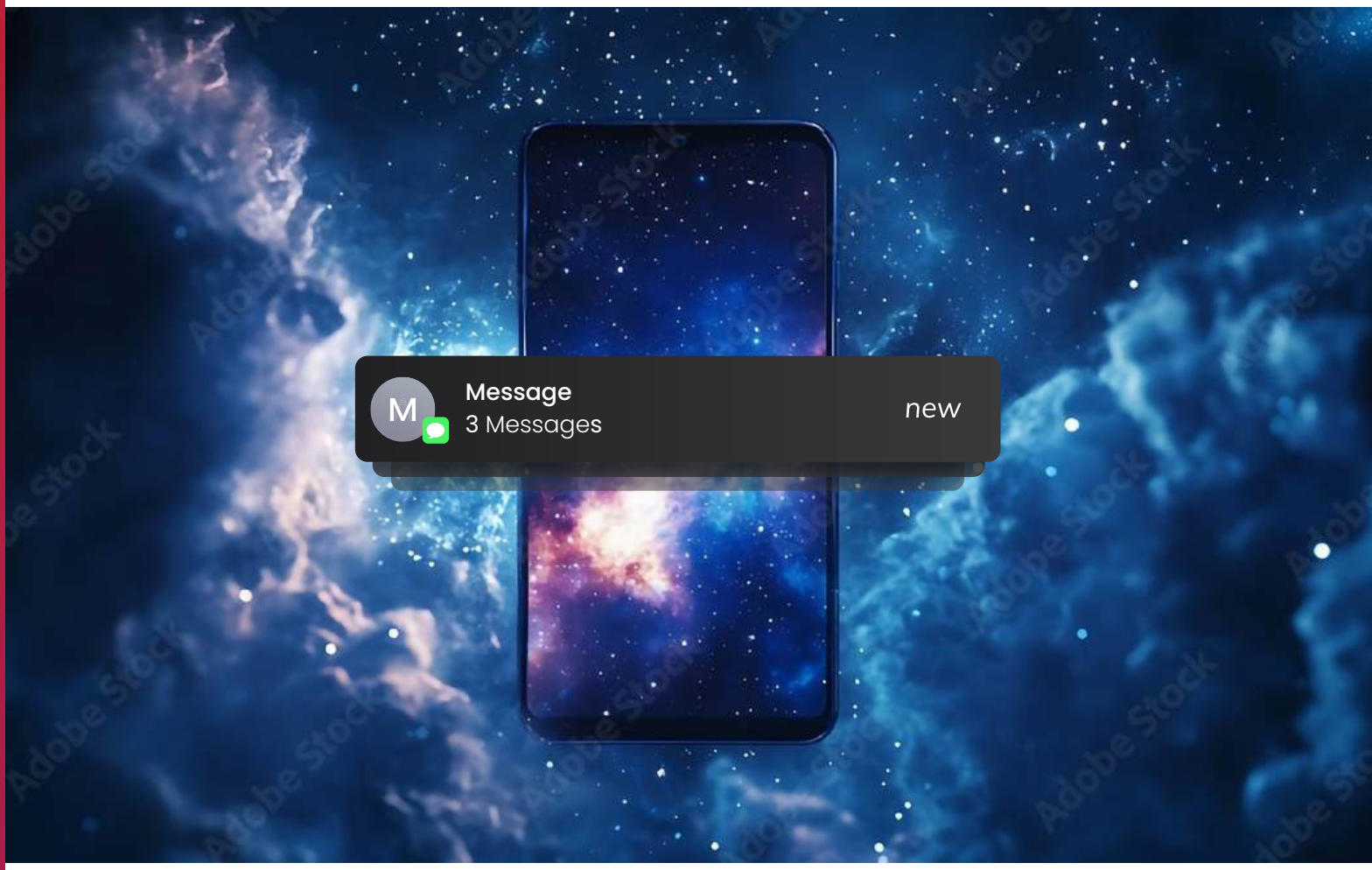
REPORT

The State of the Scamiverse

A surge in text and email scams, $5 and 10 minutes to deepfake deception

January 2025



REPORT

Table of Contents

Summary

For the price of a latte and in less time than it takes to drink it, a scammer can create a convincing deepfake video of your mom, your grandchild, your boss, or your coworker.

Tools for creating these kinds of scams are readily available and easy to use. For example, a study of 17 different deepfake-creation tools, by McAfee Labs, found that for just $5 and 10 minutes of setup time, scammers can create powerful, realistic-looking deepfake video and audio scams.

These are just some of the tools powering the Scamiverse: The ever-growing world of scams and frauds facing everyone online today.

Scams are surging, even as people's awareness of them is growing. McAfee's December 2024 survey of 5,000 adults found that, globally, the average person sees 12 scams per day — and the average American is targeted by more than 14 scams every day, including an average of 3 deepfake videos.

These scams cost people money, time, and their sense of well-being. One-third of those who fall victim to scams globally lose $500 or more, and over a third of people say falling for an online scam caused moderate to significant distress. Worldwide, the average person spends over 83 hours a year reviewing text, email, or social media messages to figure out which ones are fake — and for Americans, it's almost 94 hours a year.

Scams are on the rise worldwide. Detected deepfakes surged tenfold globally in the past year, with North America alone experiencing a 1,740% increase. Social media users shared over 500,000 deepfakes in 2023. Two-thirds of people admit they're more worried about falling victim to scams than ever before, according to a separate McAfee survey of more than 7,000 adults in November 2024.

As scammers embrace sophisticated AI tools, consumers face new risks, including personalized text and email scams, hyper-realistic deepfakes, evolving identity theft tactics, and more.

A combination of AI-powered technology and education is key to outsmarting the Scamiverse. McAfee recommends consumers practice good cyber hygiene, embrace the latest in online protection, and cast a skeptical eye on the content they consume — whether that's in text messages, or on email or social media.

Highlights

$5 Cost to create a new deepfake scam using AI-powered tools

10 mins Time to create a convincing deepfake video

59% Percentage of people globally who say they or someone they know has been a victim of an online scam

87% Percentage of those targeted by a scam who say they lost money

33% Percentage of people who lost $500 or more

1 hour or less Time it took a scammer to cheat their target of money or information, in 64% of survey respondents

The Scamiverse is evolving rapidly, and this study makes it clear just how much of an impact it's having. Knowing what techniques scammers are using is the first step to protecting yourself.

Survey data: Deepfakes have gone mainstream

Online scams are no longer an exception — for most of us, scams are an everyday fact of online life. Three-fifths of people worldwide (59%) say they or someone they know has been a victim of an online scam, according to McAfee's December 2024 survey. For those aged 18-24, that rises to 77%.

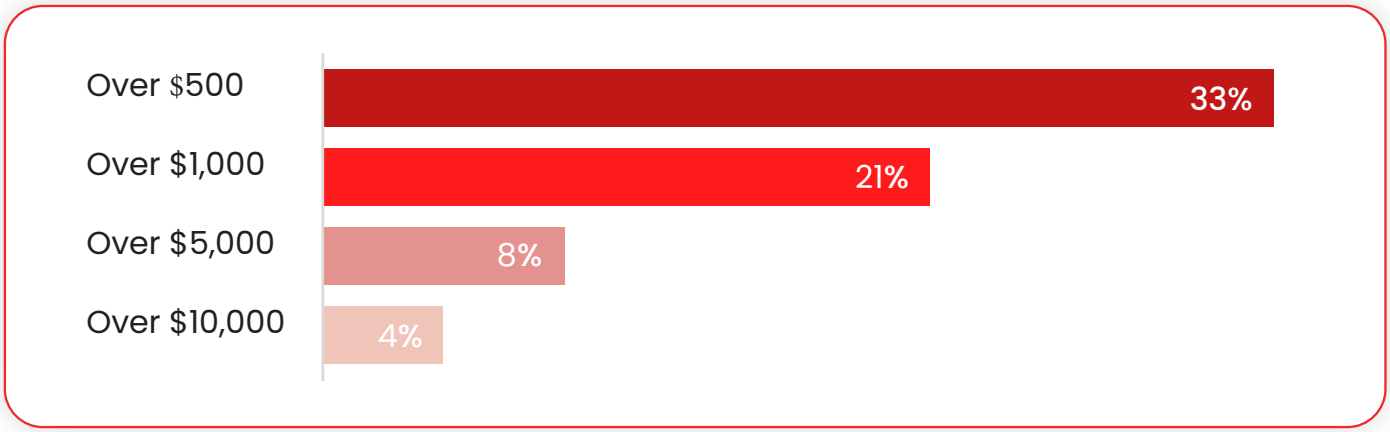
These scams are everywhere, and despite a relatively high level of awareness about them, people are still getting fooled – because they are more personalized and realistic than ever.

Scammers also depend on speed and surprise to be effective, and these techniques are working. More than half of the targets (56%) realized they were being scammed in less than an hour, but financial losses or theft of personal information happened just as fast: In 64% of the cases, it took less than an hour for the scammers to do damage.

The losses can be huge. Eighty-seven percent of people targeted by a scam say they lost money, with losses exceeding $500 in one-third of those cases — and almost one in ten lost over $5,000.

Scam losses

Of those targeted by a scam, 87% said they lost money. How much?



In addition to monetary damages, online scams take an emotional toll. Thirty-five percent of people globally said falling for an online scam caused them moderate to significant distress.

It takes time to recover from a scam — and to avoid the scam artists in the first place. According to our survey, people who fell for a scam spent an average of 1.3 months trying to resolve scam-related issues afterward. There's also significant time spent before a scam ever occurs: the average person globally spends 1.6 hours per week reviewing, verifying, or deciding whether a message sent through text, email, or social media is real or fake. That's 83.2 hours every year — and for Americans, it's 93.6 hours per year!

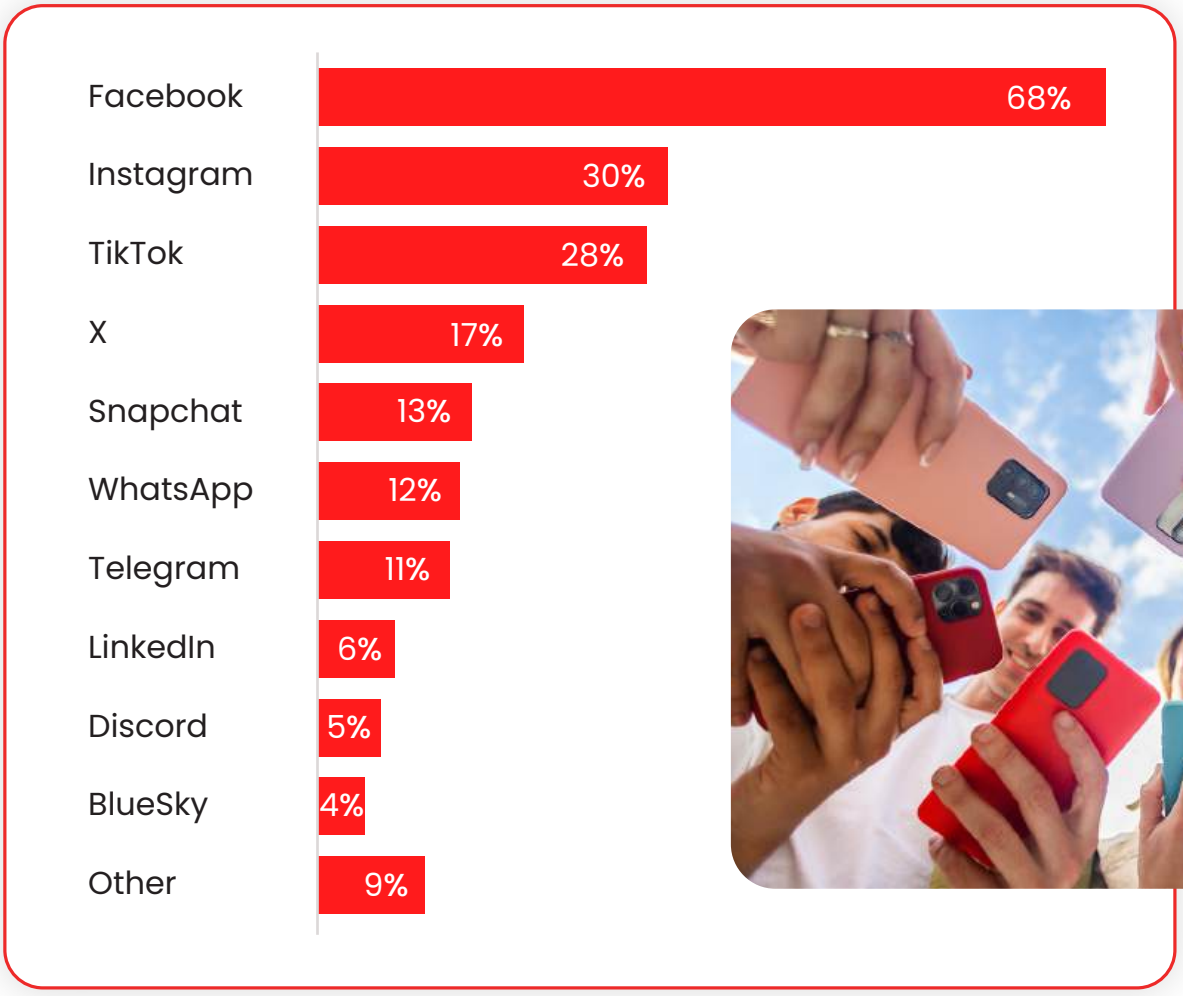
Scammers are using an increasingly powerful array of scam software available, as we will see in the next section. The results? It's hard to go online without running into scams everywhere you turn.

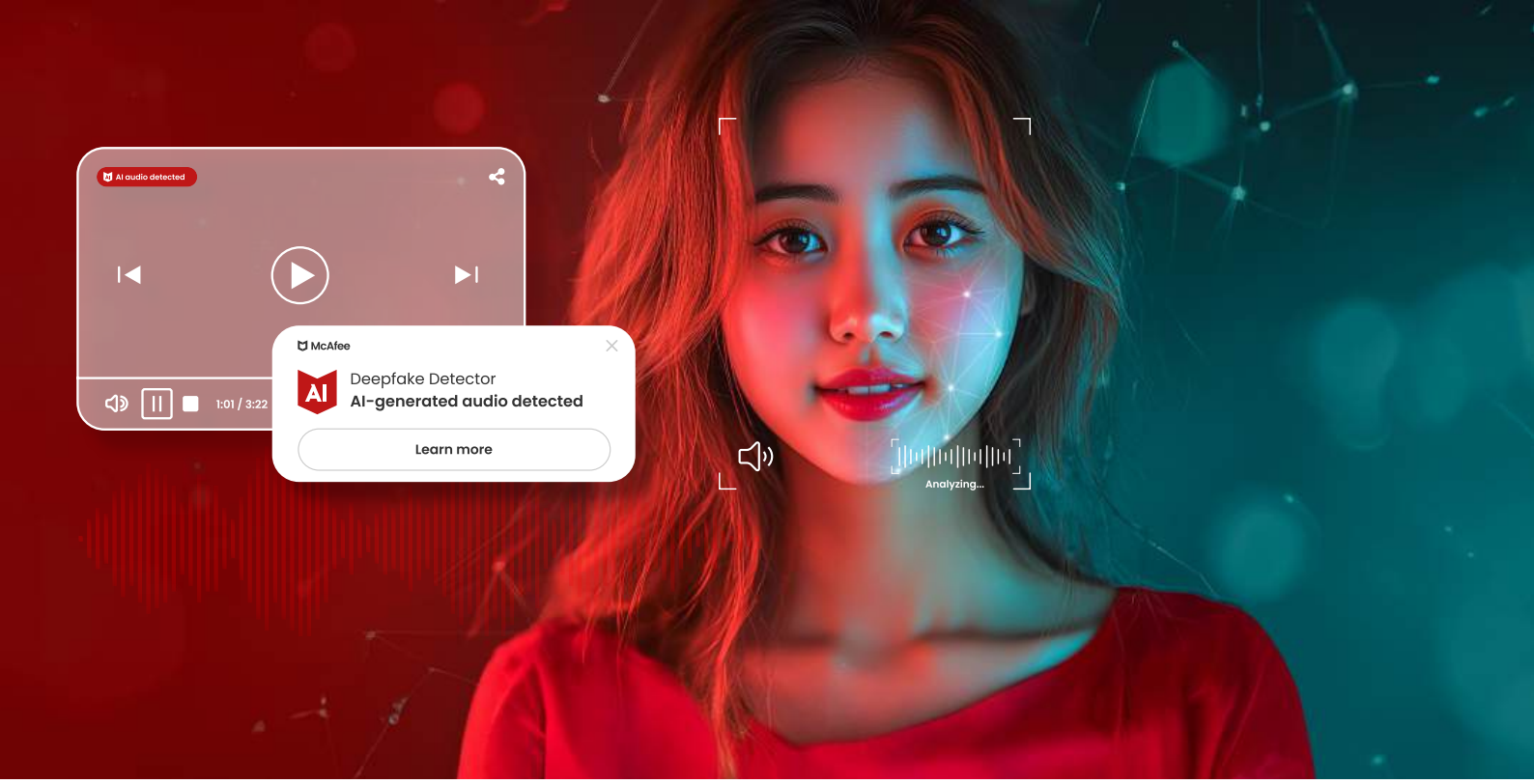
The average American sees an average of over 14 scam messages and deepfakes every day. These scams show up via text message, on email and social media, and as deepfake videos. Americans see about three of these per day in each medium except for email, where people encounter an average of five scams every day. And if you thought deepfake videos were something that was "coming in the near future," guess again. On average, Americans see nearly 3 deepfake videos every day.

Not all deepfake videos are scams, but many are: Most Americans estimate that between 25% and 75% of the deepfakes they see are scams. And social media platforms are minefields for this type of content.

Deepfake platforms

The percentage of Americans reporting deepfakes on each social media platform





Younger people run into deepfake videos more often, on the whole: People in America aged 18-24 see 3.5 deepfake videos daily, while people over 65 see just 1.2 such videos per day.

But older Americans are more likely to see deepfakes on Facebook: 79% of those aged 55–64 and 81% of those 65+ say they've encountered deepfakes on this social media platform. For younger folks, they're more likely to see deepfakes on Instagram or TikTok.

In addition to monetary losses, McAfee's State of the Scamiverse survey showed that falling victim to scams causes people emotional distress and impacts their self-esteem. This is a price that people shouldn't have to pay simply for going online.

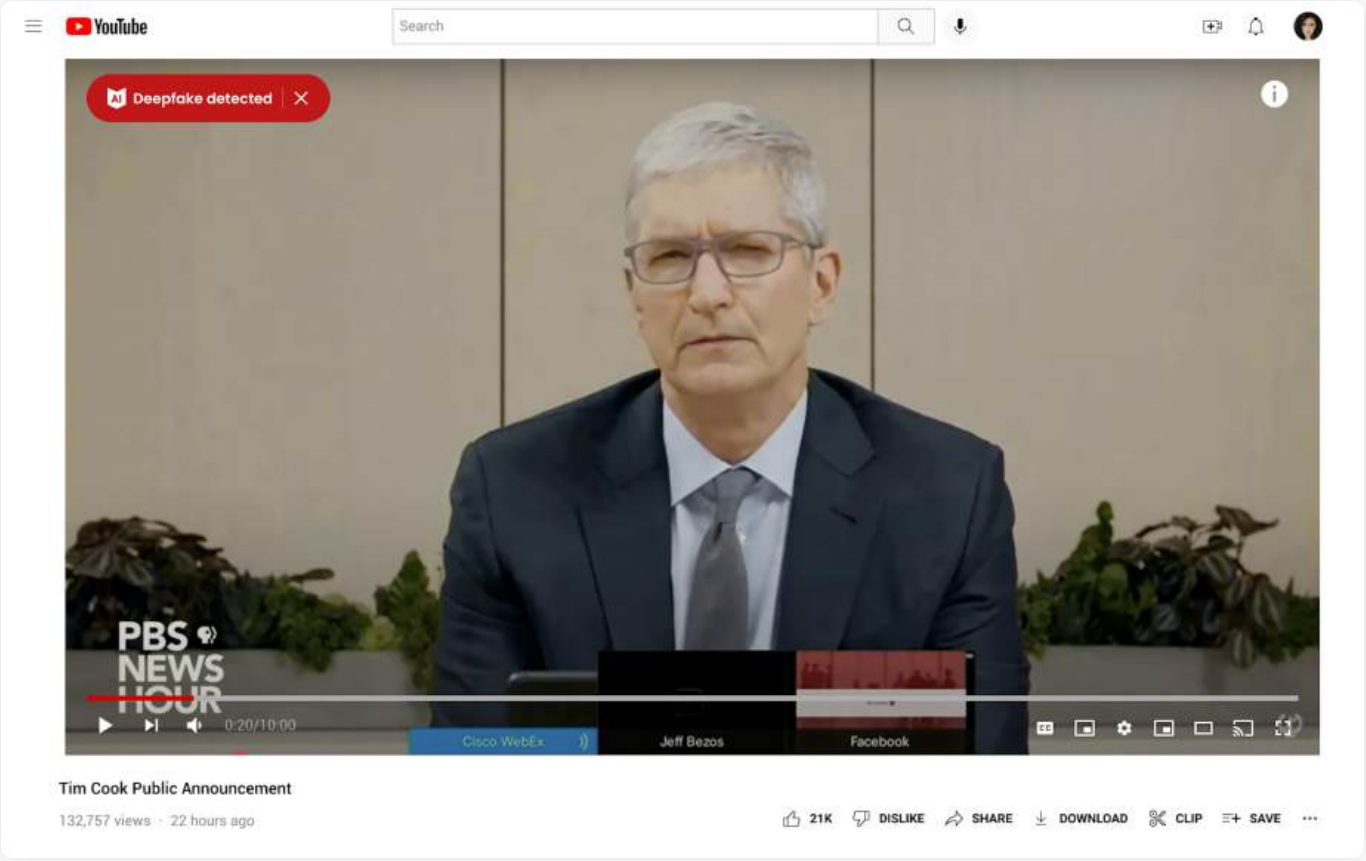
Anatomy of a deepfake

How did deepfakes get to be such a big deal?

Let's start with the basics. Deepfakes are highly realistic fake videos or audio recordings created with generative artificial intelligence (GenAI) technologies. Scammers are now using deepfakes to impersonate real people — and not just famous people, but your friends, relatives, and coworkers.

Deepfake technology is now advanced enough that it can sometimes be very hard to tell if that video of your mom really did come from her — or if it's a fake created from a snippet of online video.

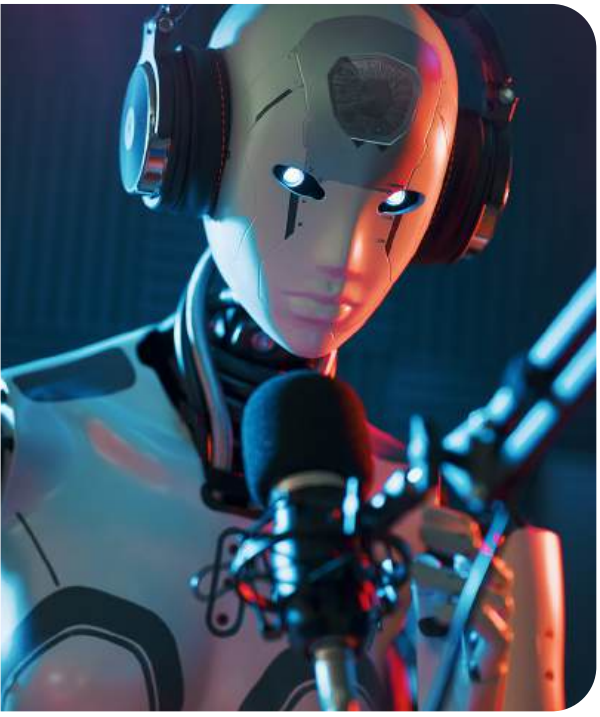
Deepfakes gained attention over the past two years due to popular memes that got a lot of news coverage. Videos featuring fake, AI-generated versions of Taylor Swift, Elon Musk, Mark Zuckerberg, Tim Cook, and other celebrities showed the world how powerful this tech could be.



Deepfake audio and video played a darker role in elections around the world in 2024, with impersonations of major candidates. But most of these videos were also identified as fakes relatively quickly.

It's different now. Scammers are using readily available deepfake tech to create extremely persuasive audio and video impersonations of people known to the victims.

It only takes a few seconds of sampled audio or video to create a convincing scam, and many of the deepfake tools now work in real time, as we discuss in the next section, overlaying the impersonated person's face and voice over the scammer's.



This allows the scammers to impersonate people interactively, through chat apps or video and voice calls, answering the target's questions in real time.

For example, an Arizona mom received a terrifying phone call that sounded like her daughter being kidnapped. The scammer tried to extort a $1 million ransom. It was only after calling 911 and talking with other moms on her daughter's ski trip that she confirmed the entire conversation was faked. "It was completely her voice," the mother said later. "It was her inflection. It was the way she would have cried."

The FTC has reported that scammers can pretend to be Apple or Microsoft, saying there's a problem with your computer; Amazon, saying there's a problem with your order; or even your grandchild, saying they're in trouble and need you to send them money. All of these are fakes that sound convincingly real.

Other scams recorded by the FTC include impersonations of people's bosses calling to ask for bank account numbers.

People targeted by voice cloning scams have reported to McAfee that the caller "sounded just like my granddaughter" or grandson. "It frightened the hell out of me," one target said.

> "Deepfakes have moved out of science fiction and entertainment into everyday life. As our research shows, most people are seeing more of these than ever." — Steve Grobman, Chief Technology Officer, McAfee

REPORT

Deepfake tools: $5 and 10 minutes to deception

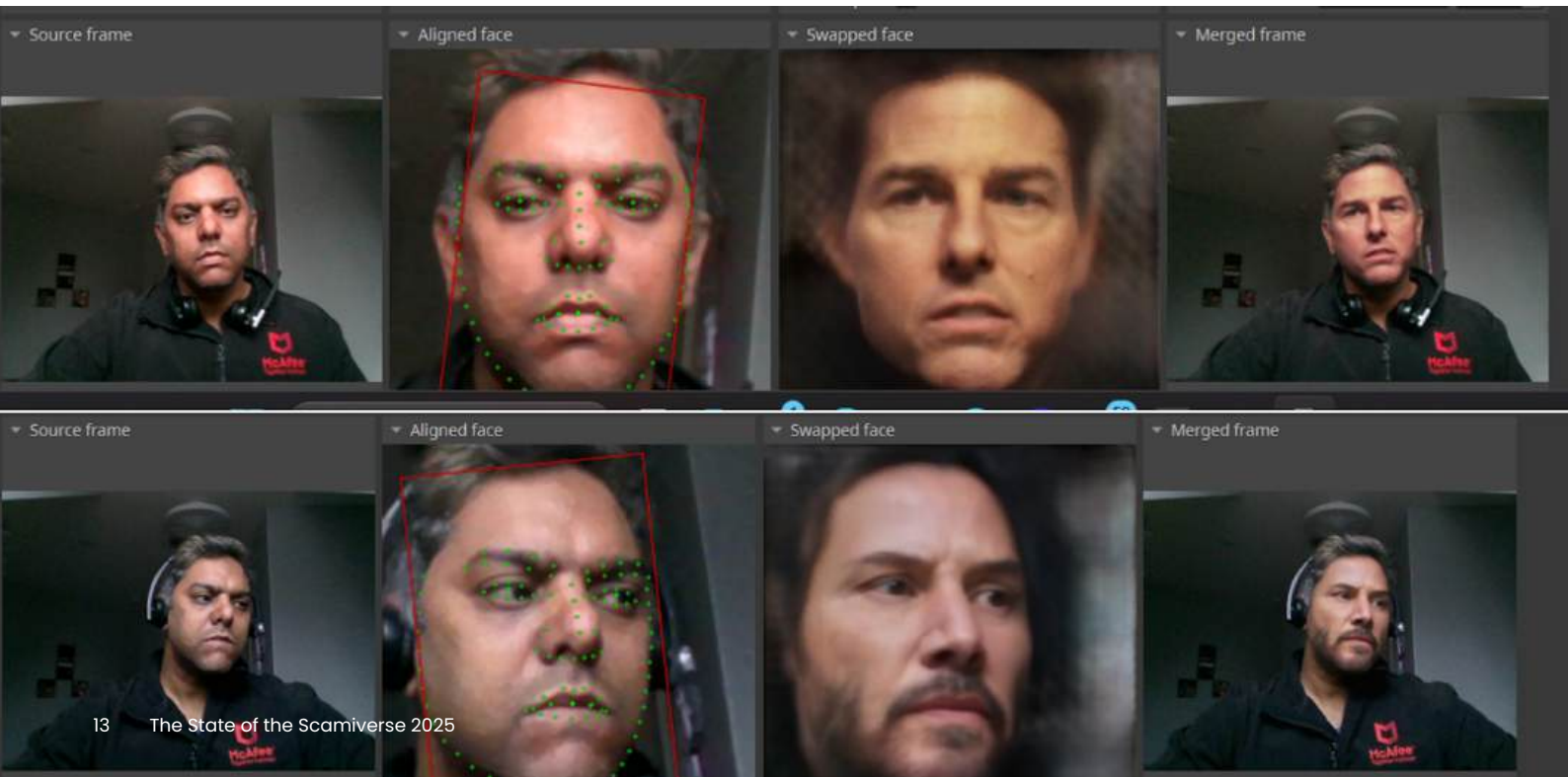
A major reason these scams are getting so common is that scammers have a wide variety of inexpensive, easy-to-use deepfake tools available to use. Such tools are readily available for download online or as services provided through a website. Many offer free trials that let you create a limited number of deepfake videos or phony audio impersonations.

Some of these tools are marketed as "entertainment," aimed at people who want to call a friend on WhatsApp or another platform while pretending to be a famous actor.

But others are clearly intended for use by scammers — and the makers of these tools are, in some cases, putting a lot of effort into making them usable and powerful.

McAfee Labs tested 17 of these tools and found that the quality varies wildly, but some are remarkably effective and easy to set up.

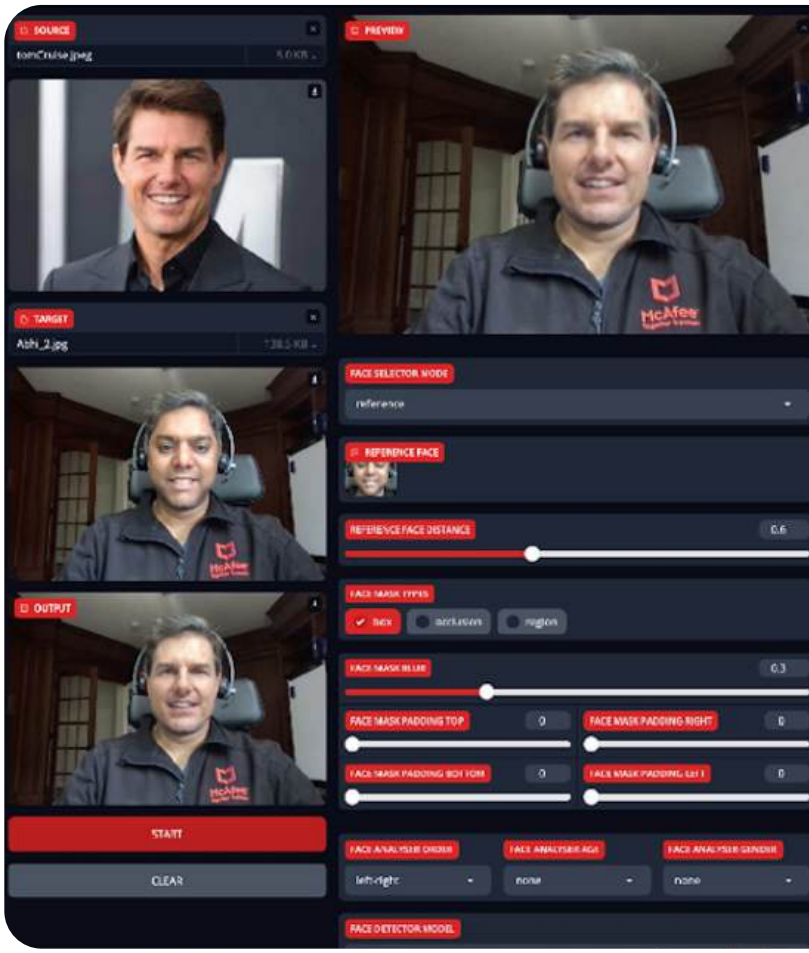
In fact, for as little as $5 and 10 minutes of setup time, the McAfee Labs team created convincing, real-time avatars that made us look like Keanu Reeves, Tom Cruise, and other famous actors.



What once required experts weeks to produce, we were able to achieve for as little money as it costs to buy a latte — and in less time than it takes to drink it. Beginner-friendly tools, with simple drag-and-drop interfaces, allow even newcomers to create realistic fake audio and video.

Additionally, open-source libraries provide tutorials and pre-trained models, allowing scammers to bypass complex setups entirely.

Our tests also revealed that these tools often require the attacker to have a powerful computer system and a good graphics card, although that is not a high barrier as such systems generally cost under $1,000 – a small investment given the potential return.



As noted previously, 87% of the people targeted by scams globally lost money, and one-fifth of those lost over $1,000. So it only takes a few successful scams for a scammer to earn back the cost of a very powerful PC.

> "The thing that blew me away about doing these tests was just how easy it was to create a deepfake video that let me pretend to be anyone I wanted to be, from Keanu Reeves to my best friend. These tools are incredibly powerful." — McAfee Labs

The kinds of scams we're seeing

The kinds of scams reported by respondents in McAfee's December 2024 survey run the gamut from the most frequent (a fake shipping notification) to tech support scams and family emergency scams.

Knowing what kinds of tricks scammers are using is the first step toward not getting fooled. So take a look at this list of scams and ask yourself whether you've ever seen one of these in your inbox, instant messenger, or social media platform.

Note: We've highlighted the six types of scams that frequently involve deepfake video or audio in bold. Keep in mind that deepfake technology is rapidly evolving, so deepfakes may start to show up in many other types of scams in the very near future.

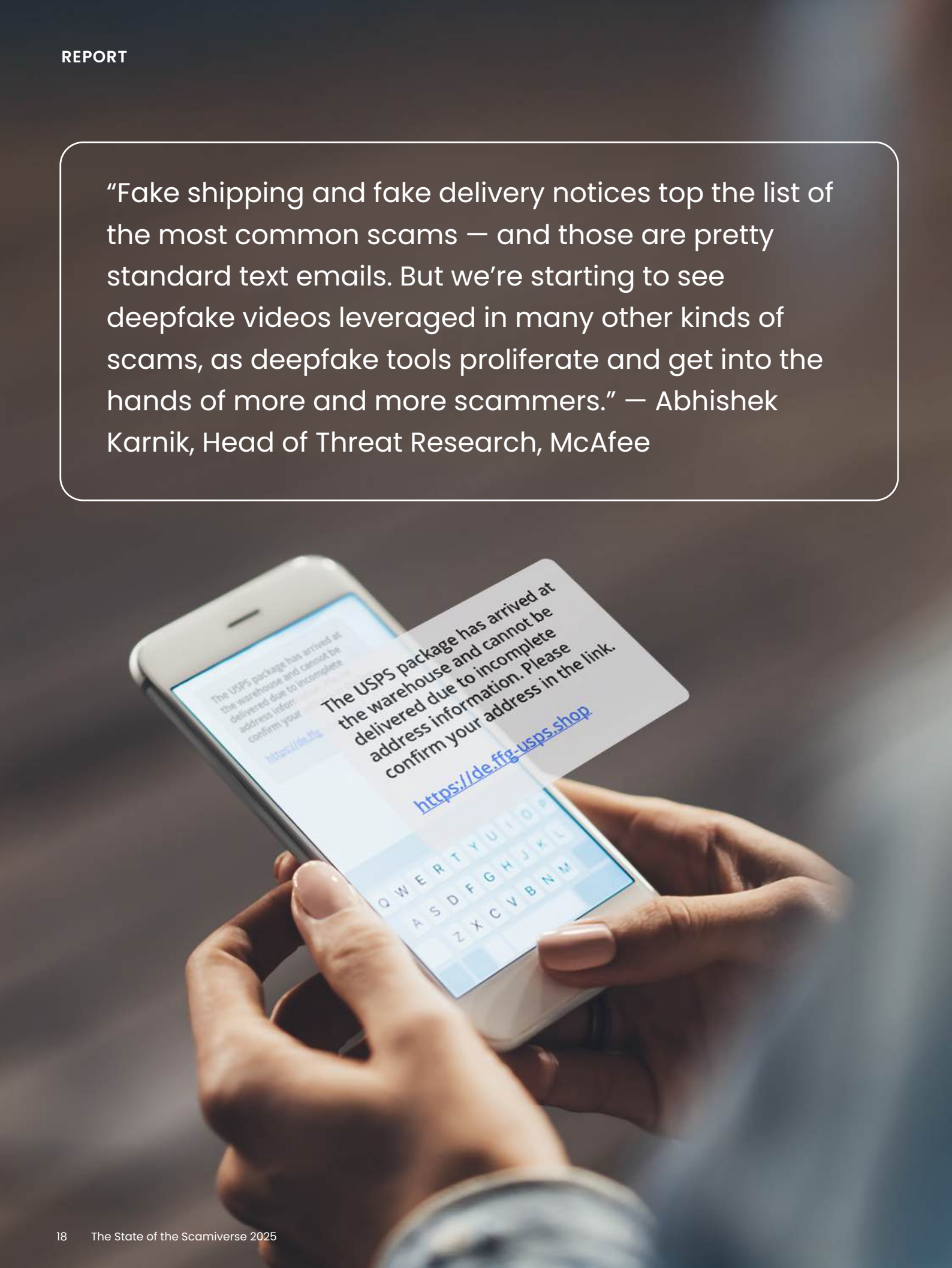
Types of scams reported by survey respondents

Survey respondents reported 25 different types of scams. Here's what percentage of respondents saw each type. **(often involves deepfake video or audio.)**

Scam	Percent reporting	Description
Fake shipping notification	36%	Claims a package is delayed or undeliverable, with a link to "resolve" the issue
Fake delivery notice	34%	Claims you have a missed package and prompts you to click a link to "reschedule delivery"
Account verification scam	29%	Claims your account (e.g., Google, PayPal) will be suspended unless you click a link and enter your details
Special offer scam	24%	Promises massive discounts or freebies but contains links to phishing sites
Fake invoice	21%	Sends invoices for products or services you didn't order, pressuring you to pay
Fake news videos	**21%**	**Spreads fabricated news stories asking for donations or personal support**
Friendly text scam	18%	A stranger sends a friendly text, and after engaging in conversation, they ask for money through a fake investment or romance scam
Subscription renewal scam	20%	Asks you to update payment details for a subscription (e.g. streaming services or antivirus software)
Lottery or prize scam	23%	Claims you've won a prize but asks for payment or personal information to claim it
Loan or financial services scam	16%	Offers fake financial advice or services through polished AI-generated videos
Account verification scam	17%	Pretends to be from platforms like Facebook or Instagram, asking you to verify your account

Scam	Percent reporting	Description
Bank imposter scam	22%	Poses as your bank, warning of suspicious activity and requesting login details or personal information to “secure” your account
Job offer scam	14%	Promises high-paying remote jobs but asks for personal information, payment for training, or other upfront costs
Celebrity endorsement scam	18%	**Shows a fake video of a celebrity endorsing a product or hosting a giveaway to steal payment details**
Car warranty scam	9%	Falsely claims your car warranty is expiring and pressures you to extend it
Tech support scam	16%	Pretends to be from a tech company, warning about security breaches or viruses and requesting remote access or payment to “fix” the issue
Fake survey scam	13%	Offers a reward for answering a survey but asks for credit card details to claim the prize
Cryptocurrency deepfake scam	16%	**Uses deepfake videos of public figures promoting "guaranteed" returns to lure victims into investing in fake schemes**
Tax refund scam	19%	Claims you're owed a tax refund and asks for your details to process it
Donation or charity scam	11%	Falsely claims to represent a charity or relief effort, asking for funds, often in response to a recent disaster or tragedy
Impersonation video scam	11%	**Fake live or recorded video of someone you know asking for money or sensitive information**
Business email compromise	10%	An email that pretends to be your boss or colleague, asking for wire transfers or sensitive data
Utility scam	12%	Threatens to cut off electricity or water unless you pay immediately
AI voice cloning scam	10%	**Simulates a loved one's voice in a video to make fake emergencies more convincing**
Family emergency scam	12%	**Text messages, videos, or calls claiming a loved one is in trouble and needs money urgently**

"Fake shipping and fake delivery notices top the list of the most common scams — and those are pretty standard text emails. But we're starting to see deepfake videos leveraged in many other kinds of scams, as deepfake tools proliferate and get into the hands of more and more scammers." — Abhishek Karnik, Head of Threat Research, McAfee



Conclusion

AI-powered technology has reshaped the Scamiverse, transforming how online scams, identity theft, and disinformation take shape. We now live in an environment where deception spreads at lightning speed. It's harder than ever to tell the difference between what's real and what's AI-generated.

Scams are getting smarter, faster, and harder to detect. AI is giving scammers easy access to tools that once required a high degree of expertise. Even the most advanced of these AI-powered scam tools are now available to anyone for as little as the cost of a latte.

AI-powered scam technology is no longer a novelty; it's a weapon cybercrooks use to exploit people at every level, every day. And the impact is real, costing people money, time, and emotional distress.

But there's hope. By staying informed and aware, you can protect yourself and your loved ones. Knowing how to identify deepfakes and scams can help keep you from falling victim to them. And using cybersecurity tools aimed at protecting you can help keep you safe.

"The scams cybercrooks are creating are developing quickly, with the help of AI, but the tools we have to protect ourselves are evolving just as fast. With preparation and the help of AI-powered online protection technology, we can keep ourselves safe and feel confident online – even in today's Scamiverse." — Abhishek Karnik, Head of Threat Research, McAfee

How to protect yourself

Don't become a victim! Knowing what kinds of scams are out there is the first step. Protecting yourself from online scams also requires being savvy about what you click on, where it's coming from, and what it looks like.

In McAfee's December 2024 survey, 53% of people globally and 56% of Americans said they are confident they can spot deepfake video scams because the scams are very obvious. But the rest were not so confident, because these videos are getting more sophisticated all the time.

Some of the most common giveaways cited by people who were able to identify a deepfake video were over-the-top claims or distorted imagery.

How to spot a deepfake video

The most common techniques for identifying deepfakes, and the percentage of respondents who have used each one

40%	Over-the-top claims, such as unrealistic discounts, benefits, or results
35%	Products or people looked distorted, with unusual textures or backgrounds
35%	Website links looked suspicious or didn't match an official domain
33%	Images or videos that seemed too perfect to be true
28%	Audio that was overly generic, robotic, or didn't align with the video
28%	Audio not synced with lip movements, or the tone sounded unnatural
26%	Low-quality or mismatched branding

> A small group of people — just 17% globally — were able to spot a deepfake because they did a reverse image search and found the original.

Incredibly, experience does not always make us wiser. Twenty-six percent of people globally who fell victim to an online scam say that they fell victim to another online scam within 12 months. So there's always more you can learn and do to stay safe.

Here are some more tips to protect yourself from deepfakes and other online scams:

Watch for video glitches.

Look for slight inconsistencies in content. Is there unnatural blinking, odd eye movements, or unusual-looking hands or teeth? Does the audio not quite match the speaker's lips or have a distorted quality? Do parts of the background look odd or inconsistent?

Be cautious of distorted images.

Fabricated images and videos often aren't perfect. If you look closely, you can often spot the difference between real and fake. For example, AI-created art sometimes adds extra fingers, creates faces that look blurry, or creates background objects that don't quite match up.

Listen for robotic voices

AI voices often make awkward pauses, clip words short, or put unnatural emphasis in the wrong places.

Use your judgment

If someone is saying or promoting something unexpected via video or audio, especially a celebrity, pause and question whether it's legit. Also, pay attention to content that heavily appeals to emotion rather than fact, as it is often designed to bypass rational analysis and provoke an immediate reaction.

Think before you click

If you receive an email or text message asking you to click on a link, even if it's a great-sounding deal or indicates it'll provide useful information such as a package delivery update, it's best to avoid interacting with the message altogether. Always go directly to the source and interact directly with the company you trust. In other words, don't just click a link in an email: Open a new tab, type in the name of the company, sign in, and check for the deal or delivery notification.

Engage with caution

On social media, avoid sharing or engaging with content that hasn't been verified. Even commenting on a post or clicking on a link makes you more susceptible to scams and misinformation.

Stay vigilant

Phishing emails and texts are a common tactic used by cybercriminals to trick travelers into revealing sensitive information or downloading malware onto their devices. Be wary of unsolicited messages claiming to be from airlines, hotels, or financial institutions, especially if they ask for personal information or prompt you to click on suspicious links.

Press pause on emotionally charged content

Scammers play on people's emotions. If you receive a message or see a post or "news report" that makes you incredibly angry, sad, or frightened, take a moment to assess the message context, source, and legitimacy. Phishing emails, fake news reports, and scams all urge you to act without thinking. Your best defense is to take a few minutes to think it through.

Validate sources

Social media is a breeding ground for disinformation and scams. According to our December 2024 survey, 47% of people globally and 44% of Americans say they are not confident they can spot a deepfake scam, because these videos are getting so sophisticated. So approach any content with a healthy sense of skepticism. If you come across shocking or dubious claims, validate them through reliable news sources and sites that do fact-checking.

Invest in holistic online protection

Use products that provide maximum identity, privacy, and device protection. Help keep yourself and your family safe online with protection that detects and protects against suspicious links and sites, so you can browse online with greater confidence. Consider using modern AI-powered tools designed to detect deepfakes — so you can use AI to fight AI.

"Educating yourself about the state of the Scamiverse is a crucial step to staying safe. Knowing more about deepfakes makes it much easier to identify them when they pop up on your screen." — German Lanconi, Chief Data Scientist, McAfee

Survey Methodology

The McAfee State of the Scamiverse survey, which focused on the topic of deepfakes, text and email scam messages and the impact of these scams on consumers, was conducted online in December 2024. Survey participants included 5,000 adults, age 18+, In 7 countries (US, Australia, India, UK, France, Germany, Japan).

About McAfee

McAfee is a global leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com