REPORT

State of the Scamiverse

New research shows scams have become so realistic that most consumers don't realize they've been targeted until after the damage is done.

January 2026

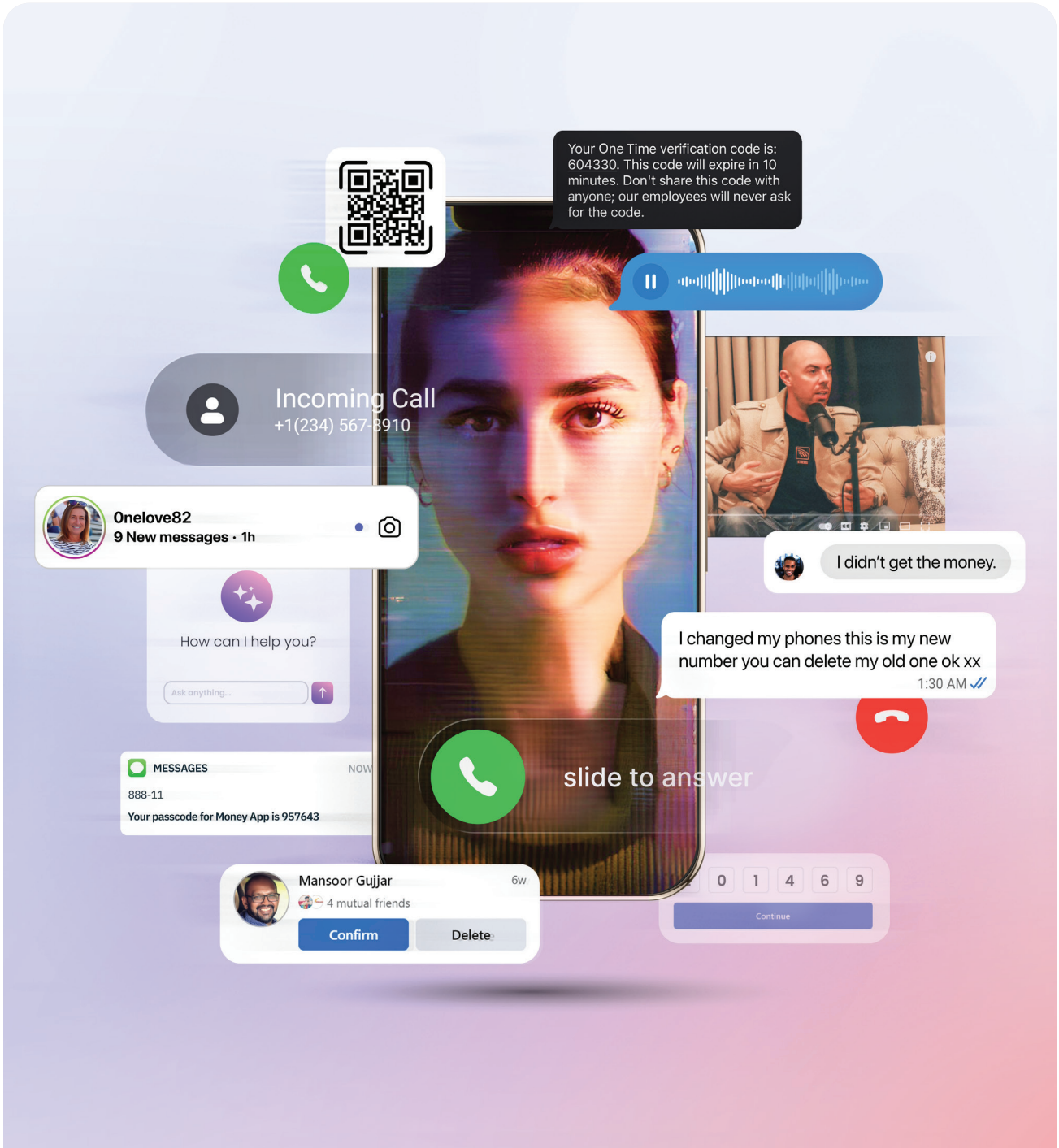
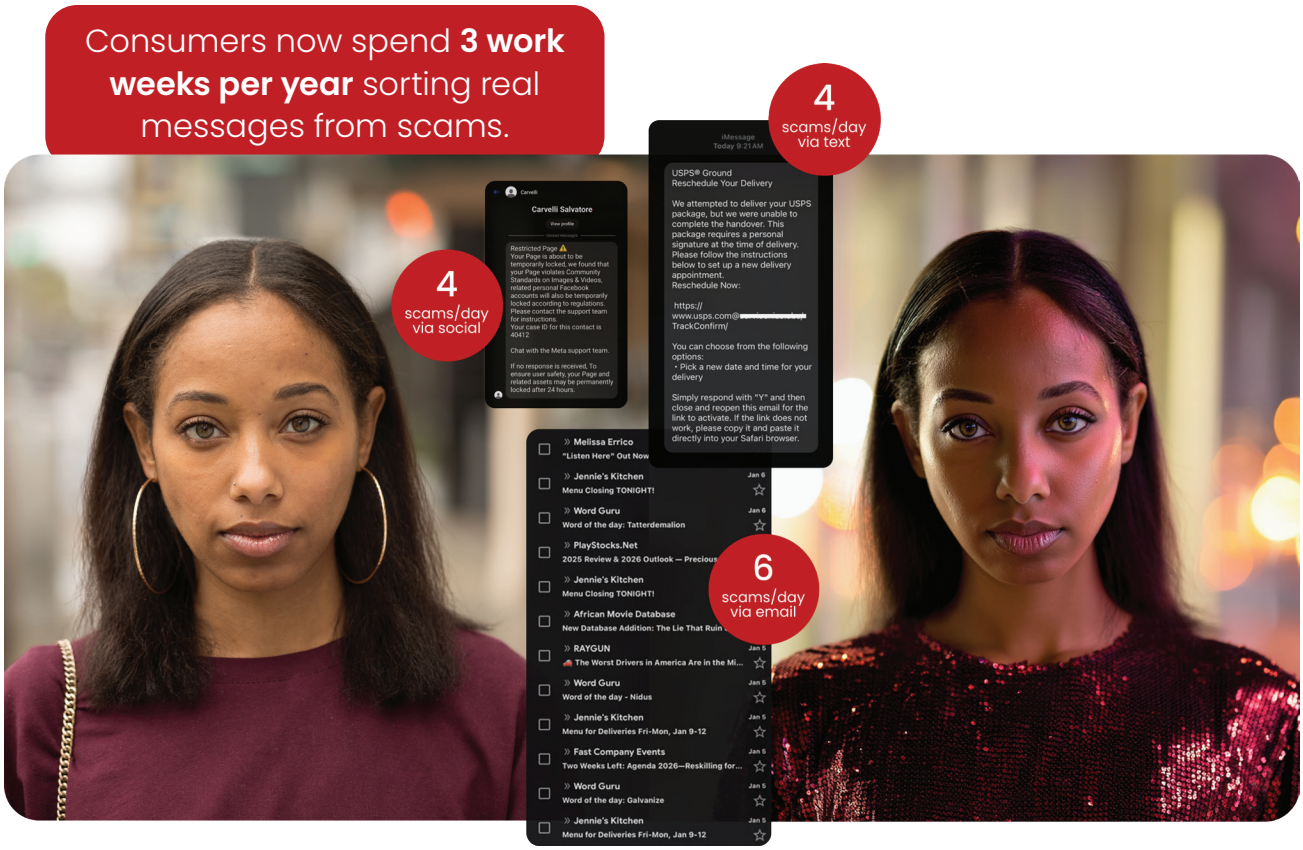


Table of Contents



Summary

One in three Americans surveyed (33%) say they feel less confident spotting scams than they did a year ago, and the data shows why. **Americans now receive an average of 14 scam messages every single day,** scattered across text, email, social media, phone calls, and even QR codes. And the scams look and sound more realistic than ever.

In fact, scams have become so ubiquitous in everyday digital life that, according to our survey, **the average person spends 114 hours a year trying to determine between what's real or fake online.** That's nearly three full workweeks of time lost.

More than half of Americans (55%) surveyed say they had a social media account compromised in the last year, underscoring why so many feel the traditional signs used to spot scams, such as poor grammar or obvious impersonation, no longer work.

Scammers increasingly use professional language, polished branding, and believable scenarios: fake delivery notices, account verification requests, subscription renewals, tax messages, job offers, charity appeals, and bank alerts that closely resemble legitimate communications. They layer in deepfake videos and voice calls, and hide malicious sites behind QR codes that appear on menus, parking meters, posters, and emails that otherwise look innocuous.

People are trying to adapt, **82% of Americans surveyed by McAfee say they're now more cautious about opening messages from unknown senders,** and 75% have made an effort to educate themselves. Compare that to 2024, when just 43% of respondents to our survey said they were more cautious about opening messages from unknown senders. Even with an increase in self-education and vigilance, the gap between what people feel prepared for and what scammers are able to trick them into continues to widen.

One thing our research clearly highlighted is that the 2026 State of the Scamiverse is evolving to outpace even the most vigilant users. Scams have grown more realistic, leading people to grow less confident in who and what to trust.

Research Highlights:
Scam Signs Are Harder to Spot

Over the past year, artificial intelligence has become part of everyday internet culture. AI-generated content now appears everywhere, from politics and celebrity impersonations to surreal viral clips like bunnies jumping on trampolines, dogs hosting podcasts, and bears caught on backyard cameras. This low-effort "AI-generated slop," named Merriam-Webster's 2025 Word of the Year, fills many social feeds. Much of this content is harmless entertainment. Some of it is not.

The constant exposure to harmless AI-generated content can have a subtle effect, lowering people's guard and making it harder to recognize when similar tools are being used with malicious intent. And that's dangerous as scammers are increasingly borrowing the same AI tools and techniques to make their schemes more convincing.

Phishing scams have upped their game, with scammers able to quickly and easily craft a malicious site that looks almost identical to a legitimate company or carry on a conversation that feels real, luring recipients into a false sense of security.

As technology and AI tools continue to advance and become more accessible, scam content is becoming both more prolific and realistic making it challenging to identify. The traditional hallmarks people have relied on to spot scams, such as strange links, odd grammar, and bizarre requests, are no longer enough.

The data shows how quickly this happened:

Fast facts from our survey of 7,500 consumers:

14 — **Number of scam messages per day**—a time tax of 114 hours or three workweeks per year.

26% — **More than 1 in 4 people say suspicious social messages now contain no link at all,** nothing to hover over, no URL to question.

44% — **Percentage of people who reply to those linkless DMs,** often triggering the scam's next step.

55% — **Percentage of Americans who say their social account was compromised** in the past year.

1 in 10 — **Number of Americans who encountered a suspicious QR code,** and **18% of those people landed on a dangerous page** after scanning one.

38 — **The number of minutes the typical scam takes to play out,** among people who ended up harmed by a scam.

3 — The **average number of deepfakes** people see **every day.**

76% — **Percentage** of Americans who say they've personally **experienced/encountered an online scam.**

1 in 3 — **Number of Americans (33%)** who say they've **lost money to a scam.**

$1,160 — Americans who lost money to a scam reported **losing an average of $1,160.**

We haven't just seen more scams. We've seen familiar scam tactics become far more convincing.

The structure of a scam message is now often indistinguishable from the structure of a normal message. And that's dangerous.

Deepfakes 2.0:
When Anyone's Face or Voice Can Be Faked

Just a few years ago, deepfakes were easy to spot. They had telltale glitches: extra fingers, strange lighting, stiff expressions, or that unmistakable uncanny-valley shimmer. Today, they're more lifelike than ever, and they increasingly show up in ordinary digital spaces, not just viral videos or political misinformation.

According to our survey findings, **Americans see three deepfakes per day on average,** often mixed seamlessly with real content. And as the technology improves, one of the clearest signs people used to trust, "does this look or sound real?" no longer works.

That erosion of confidence is reflected in the data, as **more than a third of Americans surveyed by McAfee say they aren't confident they can identify a deepfake scam,** and a similar share say they don't feel confident protecting themselves if a deepfake targets them.

Consumers report seeing deepfakes, not necessarily scams, but AI-generated videos, everywhere: **most commonly on Facebook (59%),** but also across **YouTube (36%), TikTok (34%), Instagram (33%),** and **X (19%)**. Among consumers who encounter deepfakes, most believe a significant share are tied to scams.

One in three say about half of the deepfakes they see are deceptive, and another **20% believe most or nearly all deepfakes they see are scams.** Even private messaging and community spaces aren't immune. WhatsApp, Snapchat, Telegram, Reddit, Discord, and LinkedIn all surfaced in consumer reports. Deepfakes are no longer a niche phenomenon. They're part of the social fabric.

For many, the threat feels personal: **one in ten Americans surveyed by McAfee say they have already experienced a voice-clone scam.** These scams come in a variety of forms, from mimicking a celebrity to impersonating a loved one's voice. They often generate a sense of urgency that pushes victims for a quick transfer of money or personal information before there's time to verify the situation.

Figure 1. Real examples of celebrity deepfake scams. All of these images come from AI-generated scam videos made without the stars' consent.

Deepfakes also introduce a different layer of risk. Not all deepfakes are scams, and many are created for entertainment or creative expression. However, as AI-generated video becomes more common in everyday online content, people grow more accustomed to seeing it and less confident in their ability to question it. **More than one in three Americans (35%) in our survey say they are not confident they can spot deepfake scams,** and that familiarity can lower skepticism, making scam-related impersonations and deceptive content easier to believe. Bad actors leverage this false sense of security along with a sense of urgency to anchor their scams:

- A recruiter whose intro video looks exactly like a real HR rep
- A bank agent who appears on a video call to discuss an account issue
- A celebrity endorsing an investment that never existed
- A distressed family member asking for urgent help
- A government or service agent with an ai-generated voice and callback number

The result is a confluence of manipulating a recipient's mindset and creating a digital environment where scams feel plausible before the victim has a chance to feel suspicious, leaving people to navigate confusion in real time.

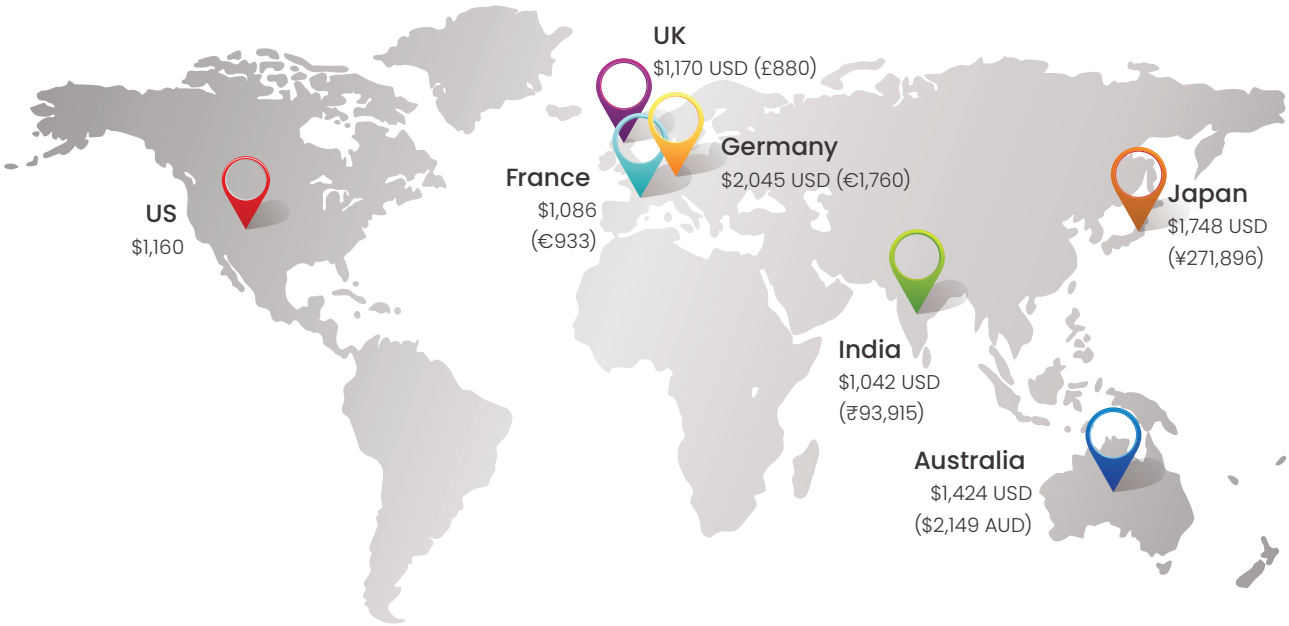
Scam Economics:
Losses, Time Costs, and Emotional Toll

The financial impact of scams is rising, but the currency of those losses is changing. Scams today span everything from high-dollar investment fraud to everyday impersonation messages that steal personal information and drain time, attention, and emotional bandwidth.

Together, they form a scam economy that is both more expensive and more exhausting for consumers to navigate.

World Map of Scam Losses Yearly

(according to our consumer survey data)



Investment scams remain the most financially devastating category.

According to reports submitted to the FTC, **Americans lost nearly $4 billion in investment scams in 2025, with a median loss of $10,800.** These scams increasingly mimic legitimate financial platforms, customer support interactions, or crypto opportunities, making them harder to dismiss as obvious fraud.

Government impersonation scams surged at unprecedented speed.

Reports of **DMV and toll-related scams also rose in 2025, according to FTC Consumer Sentinel data.** In 2024, there were just over 12,000 toll-road scams total reported to the FTC, totalling $1.64 million in losses. Compare that to 2025, which saw over 154,330 such incidents reported to the FTC, with a total of $14.16 million in known losses. These scams often succeed because they resemble routine government notices: short, transactional messages designed to blend into everyday digital life. Importantly, these numbers reflect reports to the FTC, not total scam incidents nationwide.

Scams cost more than just money. They cost time.

According to McAfee's survey, Americans now **lose 114 hours per year** simply trying to determine whether a message, alert, call, or notification is real.

That's **nearly three full workweeks** spent evaluating everyday digital interactions. Instead of a one-off event, scams have become an ongoing time tax embedded into modern life.

The emotional toll is also rising.

In the same survey, one in three Americans (33%) reported that they had lost money to a scam, and **15% of those victims were targeted again within a year.** Younger adults report the highest recurrence rates, underscoring that scams affect all age groups, not just seniors, as many may assume.

Beyond financial harm, scams introduce anxiety, hesitation, and second-guessing into everyday tasks, from opening messages to checking account alerts. **Nearly two-thirds of Americans (62%) believe their personal information is more at risk today** than a year ago, and one in three say they feel less confident spotting scams.

The result is an economic picture defined by more than monetary loss. It includes an erosion of time, trust, and confidence.

15% victims hit again within a year

Types of scams reported by study respondents

Study respondents reported the types of scams they've encountered. Here are 10 of the most common scams:

Percent reporting	Scam
31%	Fake delivery/shipping notice (missed package, delayed parcel)
27%	Social platform "verify your account" request
27%	Account verification (e.g. PayPal "will be suspended" without verification)
26%	Fake invoice for goods/services you didn't order
22%	Fake survey/reward requiring payment card details
22%	Pressure to extend car warranty coverage
21%	Subscription renewal payment update request
21%	Bank alert/bank impostor asking to "secure" your account
21%	"Security breach" message from a tech brand
20%	"Hey, how are you?"/wrong number that turns into romance or investment ask

The Future of Scams:
What Our Research Tells Us About 2026

Scams are moving past one-off messages and becoming systems that are longer, more coordinated, and designed to blend into the digital routines people complete every day. McAfee Labs research shows several patterns from 2025 that point directly to how scams are likely to evolve in 2026, especially as scammers mimic the workflows people trust most.

Everyday online storage impersonation scams: the next major frontier

One of the clearest signs of this shift was the rise in cloud storage and account-notice impersonation. Millions of consumers use cloud storage services, such as Google Drive, iCloud, or Dropbox to store and share everything from important documents to cherished family photos, making it a target-rich environment for scammers to exploit.

In October and November of 2025, McAfee Labs observed a significant increase in scams mimicking cloud service providers. These messages appeared very similar to the real thing and were designed to instill a sense of urgency with a need for immediate action:

- "Your account storage is full"
- "Your password expired"
- "A new device signed in"
- "A file has been shared with you"

They succeed because they resemble the routine notifications people handle every day. Cloud services are so embedded in modern life—email, photos, authentication, documents—that people rarely pause to question whether an alert is legitimate.

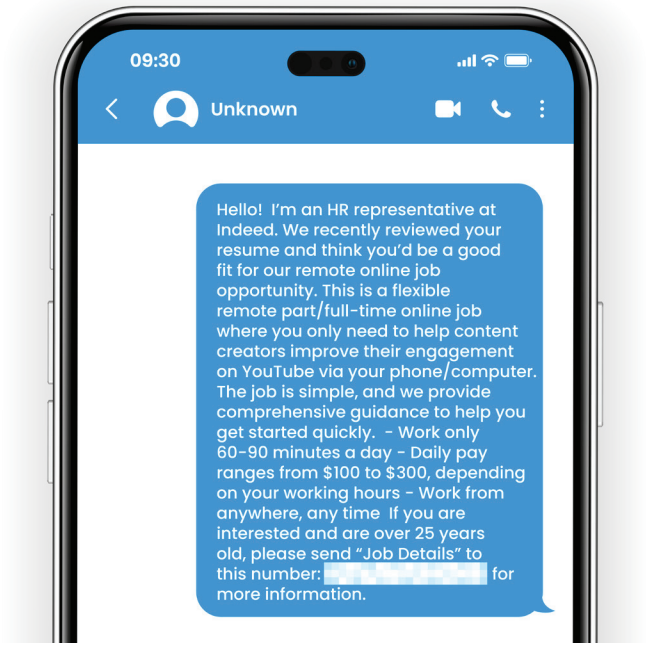
In 2026, we expect these scams to become multi-step impersonations, not one-off notifications. Instead of prompting one action, scammers may try to replicate a normal cloud workflow: an account warning —> a login request —> a two-factor authorization (2FA) -style prompt —> a document preview.

Each step feels ordinary on its own and, in fact, the complexity can make the process seem official, which is exactly why consumers may overlook subtle signs of fraud.

Other patterns that point to future risks

Government impersonation will broaden.

- In 2025, reports submitted to the FTC showed dramatic growth in DMV and toll-related impersonation scams. Based on this pattern, similar tactics may expand into taxes, licensing, and benefits, all areas where official communication already feels complex and urgent.



Job scams will grow more personal.

- Job scams accelerated sharply in 2025, with FTC-reported losses rising nearly 40% year over year, from $543 million in 2024 to $752 million in 2025. McAfee Labs analysis shows these scams are also becoming more targeted, with fraudsters tailoring outreach to specific roles, industries, and career stages. Labs identified increasingly tailored job scams in 2025. In 2026, scammers may use AI tools to customize postings, onboarding steps, and even contracts to mirror a victim's real background or industry. As the job market grows more competitive, "hustle" job scams will become a real risk to job seekers.

Malicious ads are poised to climb.

- Deepfake ads and synthetic celebrity endorsements are already widespread, and their quality is improving. These can be used to drive people toward fraudulent investment platforms, fake downloads, or credential-harvesting pages.

A long-con that begins as a simple conversation may become more common.

- Scammers now run relationship-based scams that unfold over days or weeks, starting with simple messages like “hi” or “how are you?” instead of urgent warnings. Once a victim replies, iOS and Android treat that number differently than an unknown sender, moving it into a more trusted message state and making future scam messages more likely to reach the main inbox. This allows scammers to maintain context, build trust, and later introduce links, requests for codes, or financial asks that feel like part of an ongoing conversation rather than a cold scam.

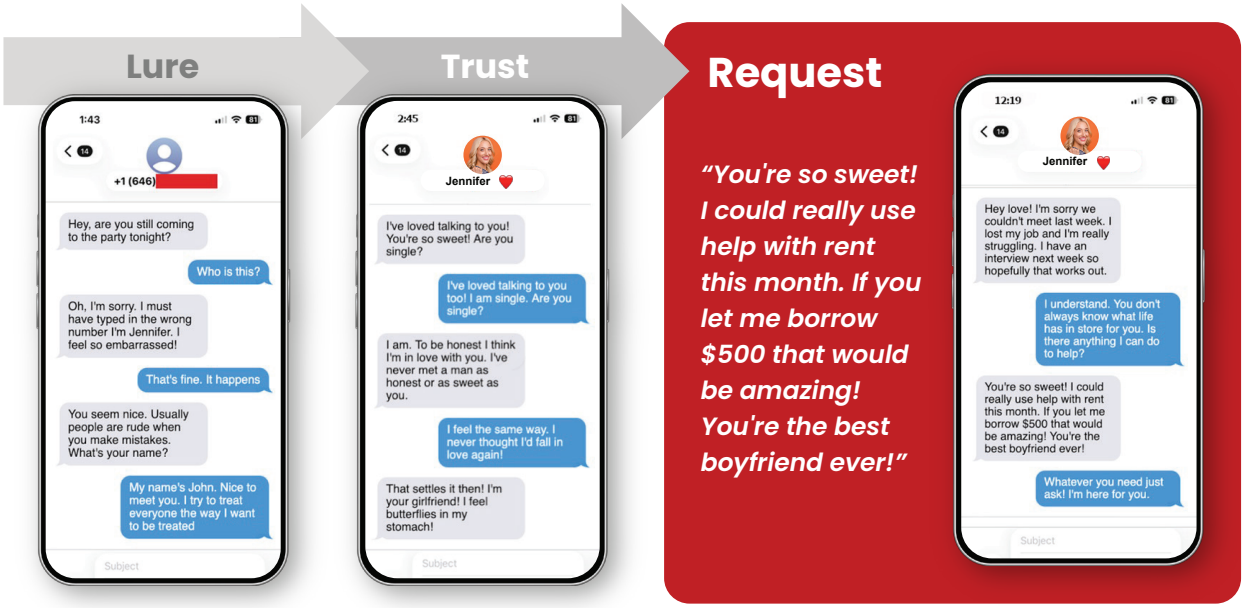


Figure 2. Scams don’t need links to work. 44% of consumers replied to a suspicious message that didn’t contain a link.

Targeting will continue to sharpen.

- AI tools make it easier to scrape public social content and build detailed profiles based off photos, posts, and information shared online. This enables more convincing impersonation, more relevant outreach, and scams that feel tailored to a person’s habits.

Crypto and financial scams are likely to intensify.

- Periods of market volatility traditionally create openings for investment fraud. Fake crypto platforms, fraudulent trading apps, and misleading financial ads may increase as scammers exploit economic uncertainty.

VPN misuse will create new scam entry points.

- VPNs remain an important privacy tool, and a trusted VPN is critical, particularly on untrusted networks. However, recent age-verification laws tied to adult content have driven spikes in VPN use as consumers attempt to bypass local restrictions. This increased demand creates opportunities for scammers to promote fake or malicious VPN apps, browser extensions, and look-alike download sites.

What these trends mean for consumers

Scams are becoming **systemic, adaptive, and embedded** in the tools people use every day. Instead of relying on obvious warning signs, consumers are increasingly asked to evaluate alerts, messages, and prompts that look and behave like the real thing.

The takeaway for 2026 is simple: scams will become harder to recognize as they increasingly resemble the trusted digital workflows people use without thinking twice.

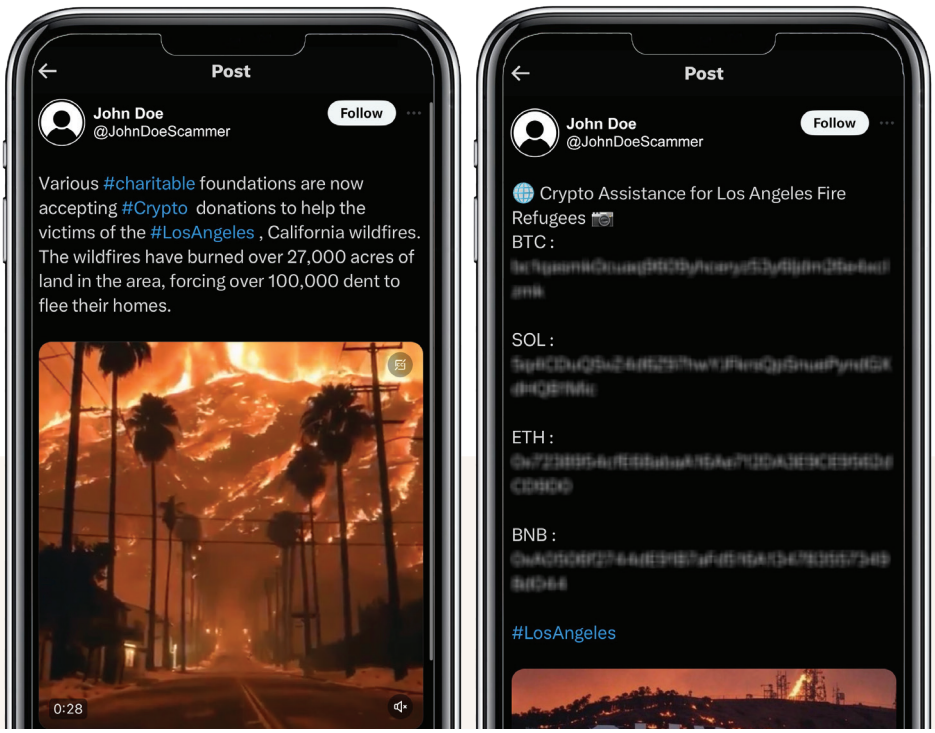


Figure 3. AI-generated images linked to the 2025 Los Angeles fires were used to promote fake cryptocurrency charities online. Shown here are real examples.

How to Protect Yourself When Scams Get Harder to Spot

As scams become more realistic and blend into everyday digital life, protection shifts from only looking for traditionally clear red flags to also picking out the subtle giveaways that indicate the content may not be legitimate. Protection in 2026 is less about looking for bad grammar, spelling mistakes, and poorly designed imitation websites; it requires a combination of **personal skepticism** and **automated protection** that is capable of spotting even minute idiosyncrasy across multiple platforms.

Because modern scams operate across email, text, social media, calls, and QR codes, consumers increasingly rely on cybersecurity tools that provide **real-time scam detection, identity monitoring, account takeover protection, and AI-driven analysis.** These layers go beyond what the human eye can catch, especially when the scam blends in.

That's not to say that the traditional indicators of a scam are obsolete. They're still a good first line of defense, and many traditional scams are still out there, and the traditional hallmarks make a good first pass, but increasingly, they can't be the only pass.

What Not To Do in 2026

- **Don't** assume "no link" means safe; linkless scams are now common
- **Don't** act on urgency alone; pressure is the scam
- **Don't** scan random QR codes; especially in public spaces
- **Don't** trust caller ID, photos, or voices; all can be faked
- **Don't** click account alerts from messages; go directly to the official site
- **Don't** share login or verification codes—ever
- **Don't** reuse passwords across accounts; one breach can unlock everything
- **Don't** assume you're "too smart" to be fooled; modern scams are built for that confidence

Smart Habits + Smarter Protection

1. Before you reply to any message

- ✓ Confirm you know who it's from, even if it looks familiar.
- ✓ Don't respond to unexpected "verification" or "urgent" requests.
- ✓ Treat linkless messages as suspicious if they appear out of context.
- ✓ Avoid engaging in communications with unknown and untrusted senders.

2. Before you click or scan anything

- ✓ Preview QR codes with a trusted QR scanner.
- ✓ Make sure QR codes aren't a sticker covering a legitimate QR code.
- ✓ Avoid scanning codes from flyers, parking lots, restaurant tables, or random screens.
- ✓ Don't click login or payment links in DM notifications.

3. When setting up your accounts

- ✓ Use separate passwords for every account and consider a password manager.
- ✓ Where possible, set up 2FA on your accounts for an added layer of protection.

4. Before you share personal information

- ✓ Never give codes, passwords, or 2FA approvals to anyone.
- ✓ Verify government notices through official websites, not by the message you received.
- ✓ Call your bank or service provider using the number on the company's website, not the one given in a message.

5. Before you trust a face or voice

- ✓ Be skeptical of "urgent" calls from family members asking for money.
- ✓ Hang up and call back using a known number.
- ✓ Don't rely on appearance or audio alone—deepfakes can mimic both.

6. Review your social media privacy settings

- ✓ Turn on 2FA across key accounts.
- ✓ Use strong, unique passwords.
- ✓ Enable alerts for new logins, password changes, and account recovery attempts.

7. Choose security software that can

- ✓ Detect unsafe texts, emails, and DMs, even without visible links.
- ✓ Scan QR codes for malicious redirects.
- ✓ Flag deepfake audio/video in suspicious interactions.
- ✓ Monitor for identity leaks, breached credentials, and account takeover attempts.
- ✓ Provide real-time warnings across SMS, email, social platforms, and browsers.

Conclusion

Scams continued to change in 2025. They became more realistic, more routine, and harder to distinguish from the messages people already trust. Alerts, account notices, job leads, delivery updates, and even familiar faces and voices now have credible imitations.

The shift continues: Scams have become part of the noise

As scammers automate, personalize, and move across every platform, people are facing more threats with fewer reliable signs to guide them. Confidence is dropping, time spent verifying messages is rising, and instinct alone isn't enough.

Staying safe in 2026 comes down to three essentials: awareness, skepticism, and protection that can detect risks in real time. Consumers shouldn't have to navigate this alone, and with McAfee, they don't have to.

Methodology

McAfee Labs Data Sources

Insights in this report draw from McAfee Labs' ongoing monitoring and analysis of global scam activity across email, SMS, social media, cloud platforms, and emerging AI-driven vectors. Labs data incorporates:

- U.S. Federal Trade Commission Consumer Sentinel Network
  - Fraud and scam reports (https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts)
  - Government impersonation trends (https://public.tableau.com/app/profile/federal.trade.commission/viz/GovernmentImposter/Infographic)
  - General consumer complaint patterns (https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic)
- McAfee internal telemetry and research
  - Scam detection signals across email, browsing, mobile interactions, and social platforms
  - Brand impersonation patterns analysed through McAfee's threat detection systems (https://www.mcafee.com/blogs/security-news/the-most-impersonated-brands-in-holiday-shopping-ranked/)

This combined dataset enables cross-validation of consumer-reported experiences with observed threat activity in the wild.

Consumer Survey Methodology

In addition to Labs research, McAfee commissioned a global consumer survey to assess attitudes, behaviors, and real-world experiences related to online scams.

- **Fieldwork:** November 2025
- **Method:** Online survey
- **Sample size:** 7,592 adults (age 18+)
- **Countries surveyed:** United States, Australia, India, United Kingdom, France, Germany, and Japan
- **Focus areas:**
  - Frequency and types of scams encountered
  - Self-reported victimization and financial impact
  - Confidence in recognizing scams and deepfakes
  - Emerging behaviors (QR codes, linkless scams, impersonation attempts)

Findings reflect consumer-reported experiences combined with real-time threat intelligence from McAfee Labs, providing a comprehensive view of how scams evolved in 2025 and what to expect in 2026.

About McAfee

McAfee is a worldwide 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.

www.mcafee.com

For more information about online protection, visit us at mcafee.com/blogs

McAfee

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

JANUARY 2026 C478-25_rp-state-of-the-scamiverse_0126