Scam Intelligence & Impacts Report 2026

The Scam Economy and the Future of Digital Trust

F-Secure®

Executive Summary

The third annual F-Secure Scam Intelligence & Impacts Report examines how the scam landscape is evolving in 2026 and what it means for consumers and the digital service providers they trust.

KEY FINDINGS

- **Exposure is widespread:** 56% encounter scam attempts at least monthly.
- **Financial loss is high:** 52% of victims lose money — more than double 2025 levels.
- **Scams are optimizing:** Fake invoice (20%), investment (19%), and banking or payment (11%) scams dominate.
- **Conversion is significant:** Nearly one in five consumers (19%) report falling victim.
- **Impact differs by age:** Younger adults face higher exposure to scams, while older victims are more likely to lose money (60% of 65–74-year-old victims).
- **Trust influences decisions:** 93% say it's important that their telecommunications provider offers cyber security and 82% say security influences provider choice.
- **Demand remains strong:** 51% are willing to pay for scam protection.

KEY TAKEAWAYS

- Scam protection is a competitive differentiator for digital service providers. Consumer trust now carries measurable economic value.
- Consumer resilience is as important as protection. While protection helps to stop threats, resilience empowers people to live their digital lives with confidence — recognizing risks, making informed decisions, and recovering quickly when things go wrong.
- Scam impact is now defined more by financial damage than by frequency. Exposure, victimization, and financial loss vary significantly by age and market.
- Confidence in recognizing scams does not prevent victimization. For digital service providers, protection must move beyond awareness to active intervention.

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Foreword: The Trust Imperative

The trust crisis is accelerating on two fronts: consumer behavior and the evolving threat landscape. AI agents are becoming delegates for our most personal decisions, while AI-powered threats make it increasingly difficult to distinguish real from fake.

F-Secure's response is built on two fundamental shifts — from protection to resilience, and from security to trust — brought to life through behavioral insight and security intelligence across our entire portfolio. In 2026, trust isn't just the right thing to build; it's your most powerful growth driver.

Timo Laaksonen
President & CEO
F-Secure

Contents

THE COST OF SCAMS:

Same Exposure, Double the Loss

In 2026, scam exposure is no longer the most important story. Financial loss is.

Last year's report was defined by volume: 56% of respondents encountered scam attempts at least monthly, with younger adults disproportionately affected. Scam activity was persistently high, and digital fluency didn't translate into cyber resilience.

That baseline hasn't changed. More than half (56%) still encounter scam attempts monthly, and over a third (36%) face them weekly. At first glance, the landscape appears stable. But the story has evolved.

Consumer intelligence researcher with more than 20 years at F-Secure, exploring trends in scams, threats, security, and consumer behavior.

Timo Salmi
Senior Solution Manager
F-Secure

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

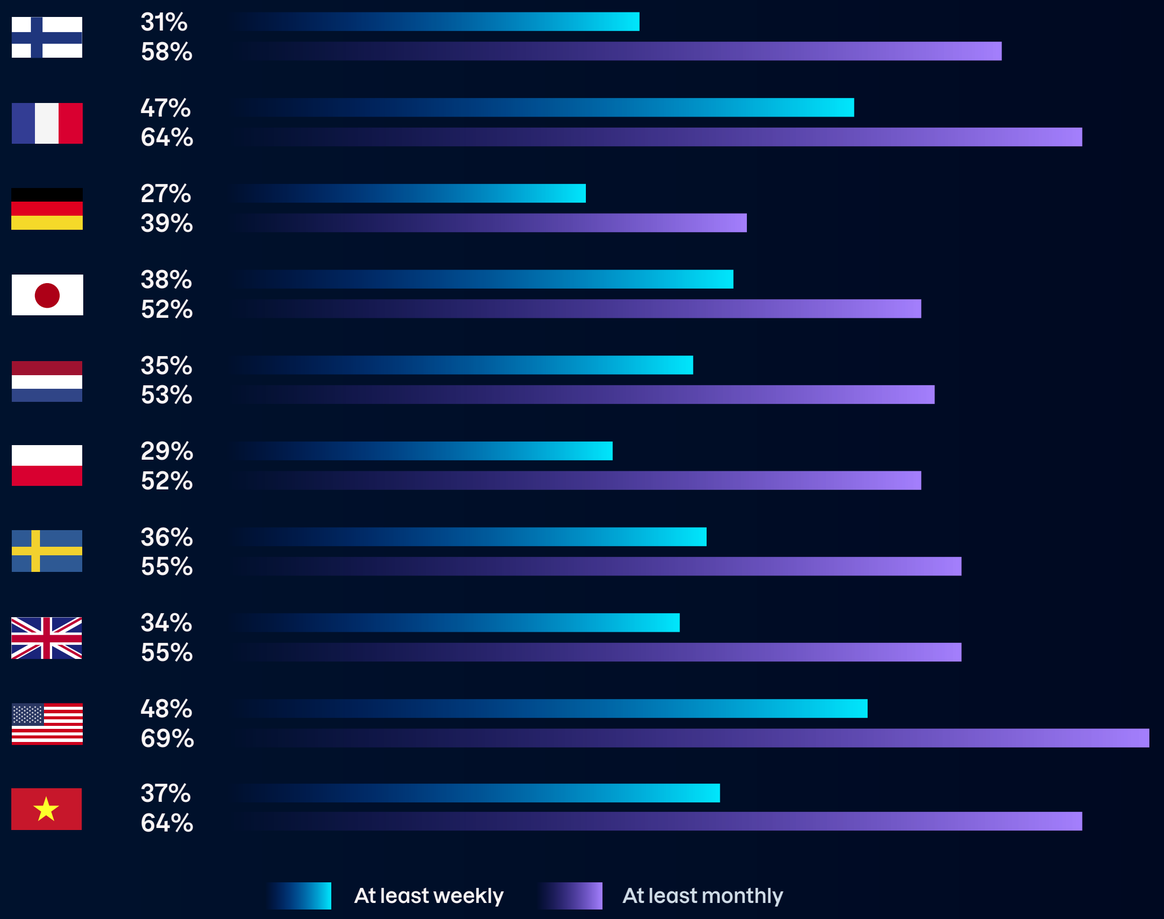
A third of consumers (33%) believe scam attempts increased compared to the previous year, even though measured frequency hasn't drastically shifted for most age groups. This perception gap suggests that the experience of scams may be intensifying — even if frequency remains stable. But stable frequency doesn't mean stable impact.

What stands out this year isn't the number of scams, but how effectively cyber criminals are turning attempts into real financial harm. In this chapter, we examine what this evolution means for consumers and the digital service providers they trust.

Scam Exposure is Widespread — But Uneven

Scam exposure remains prevalent across surveyed markets, but intensity varies. In the United States, nearly half of consumers (48%) encounter scam attempts weekly, and 69% report monthly exposure — the highest levels recorded. At the other end of the spectrum, Germany reports the lowest exposure (27% weekly, 39% monthly), underscoring substantial variation in how consumers experience scam activity across markets.

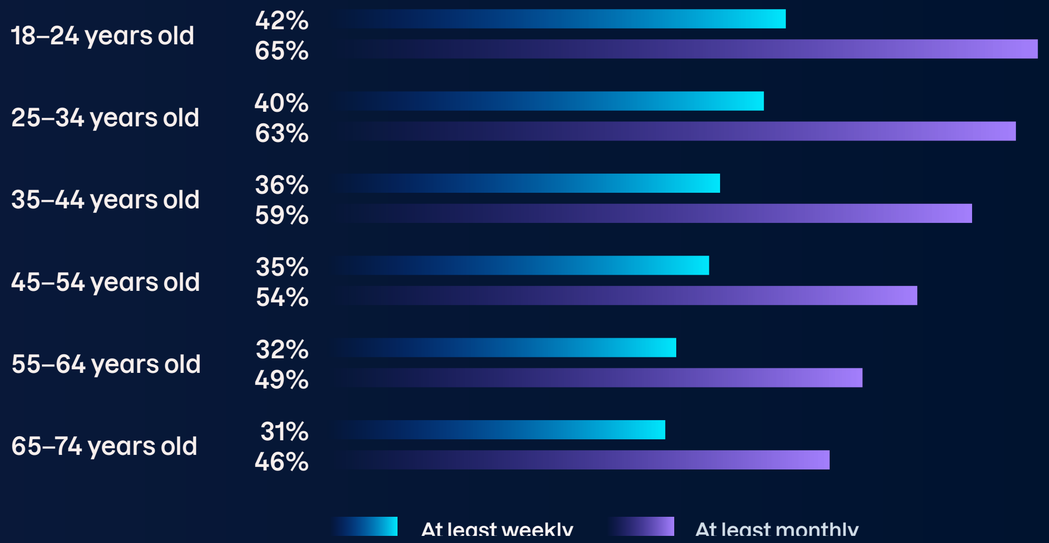
Frequency of scam attempts by country



Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

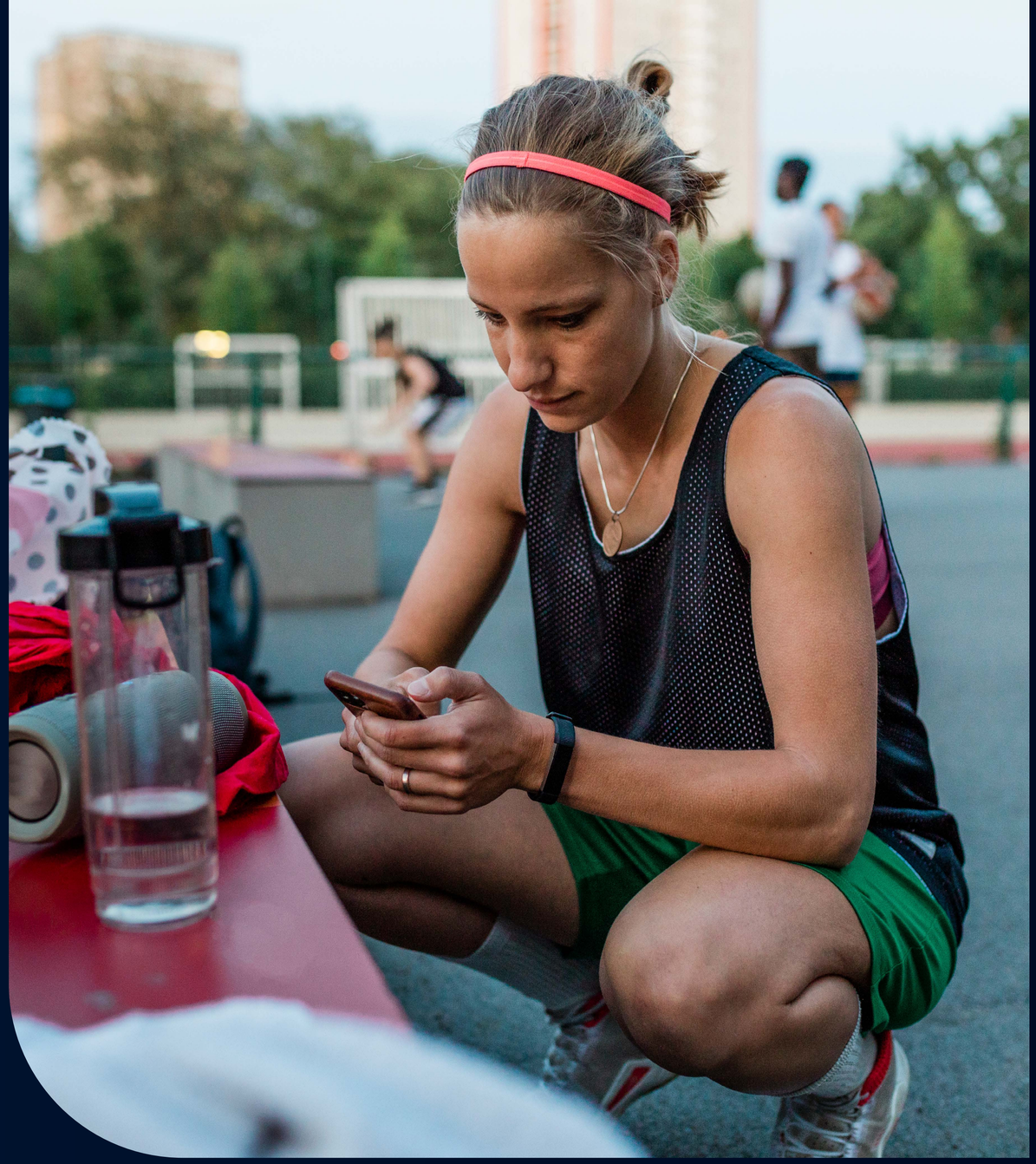
Age introduces a second layer of variation. Scam exposure declines steadily with age, with 42% of 18–24-year-olds encountering scams weekly and 65% monthly, compared to 31% weekly and 46% monthly among those aged 65–74. The most digitally active consumers are also the most frequently targeted, concentrating risk among younger generations.

Frequency of scam attempts by age group

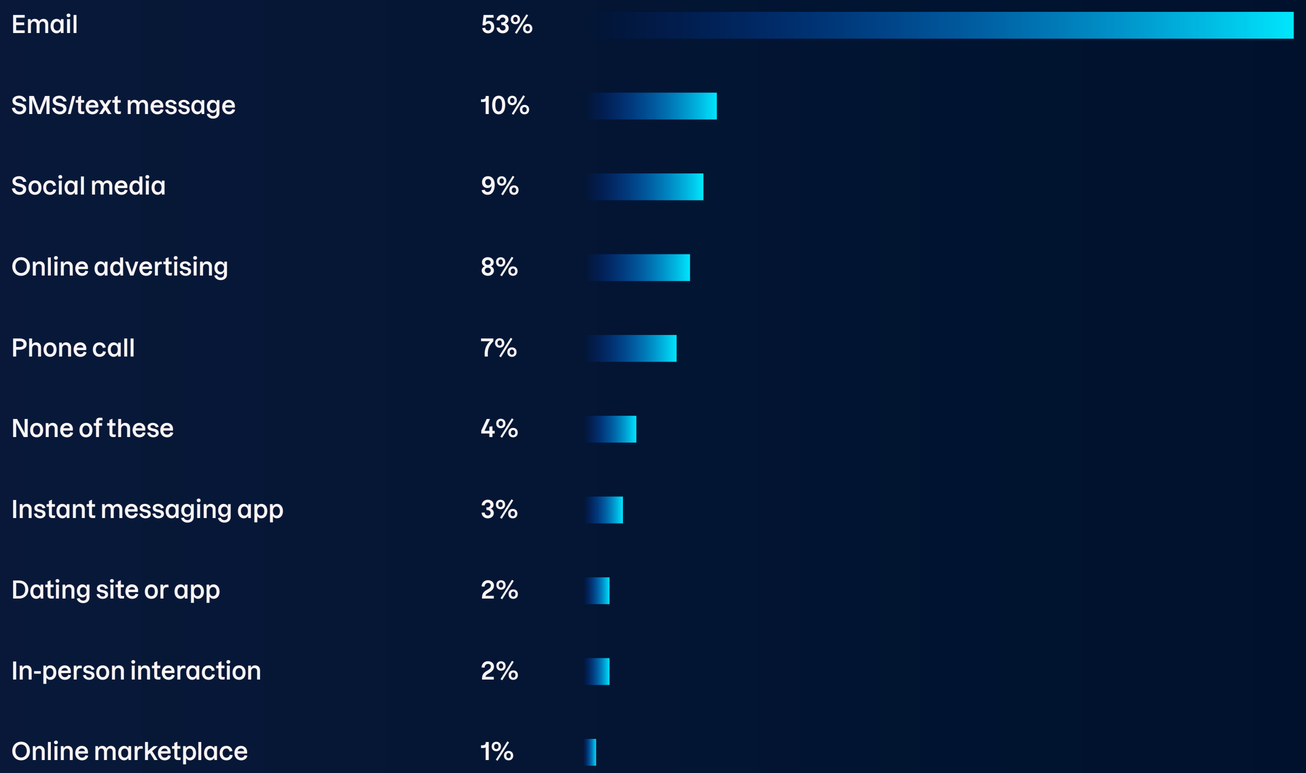


Together, these patterns show that scam exposure isn't evenly distributed. It clusters by market and by age, highlighting where protection is most urgently needed.

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000



Most common channels for scam attempts



Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Scam Exposure is Multi-Channel, Not Just Email

Email remains the most common channel for scam attempts globally (53%), yet nearly half (47%) of exposure occurs elsewhere, revealing a fragmented threat surface.

Channel distribution reflects generational behavior. Among 18–24-year-olds, exposure is spread across email (37%), SMS (13%), online advertising (13%), and social media (13%). In contrast, 65–74-year-olds face a more concentrated threat environment, with email accounting for 60% of attempts and phone calls the second most common channel (11%).

Country differences further show this divergence. In Vietnam, only 28% of scam exposure occurs via email, with significant activity across social media (20%) and other mobile channels. In Japan, email dominates at 64%, with far lower proportions elsewhere.

Across age groups and markets, scam delivery mirrors digital behavior and ecosystem dynamics. As communication and commerce diversify, so do criminal entry points — making effective protection inherently multi-channel.

Scams Are Optimizing for Higher-Value Returns

The most common scam attempts in 2026 aim to get money from victims directly. Fake invoice or debt, investment, banking, and payment scams now represent 50% of attempts — signaling a shift toward faster, higher-yield returns.

Year-over-year changes reinforce the evolution of the scam economy. Fake invoice scams have more than tripled since 2025 (6% to 20%), while banking and payment scams have more than doubled (5% to 11%). Investment scams have also increased, rising from 14% to 19%.

Meanwhile, shopping scams have fallen sharply (16% to 6%), suggesting either a shift away from consumer purchase-based scam models or stronger protections that prevent fake shops from reaching victims. The pattern points to a growing emphasis on scams that prompt victims to send money directly, rather than those disguised as online purchases.

Most common types of scam attempts

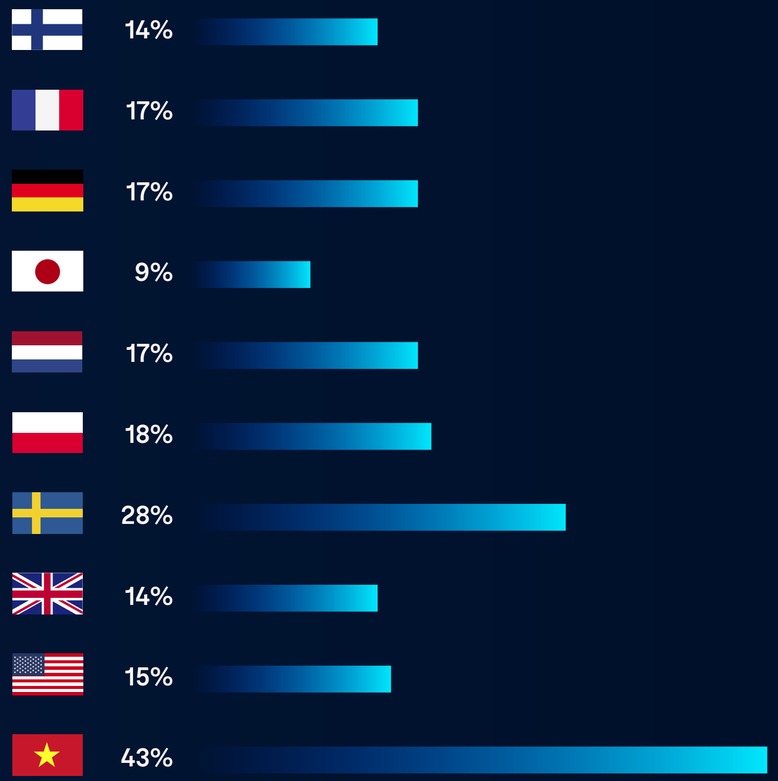
Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Scam Exposure is Translating into Real Victimization

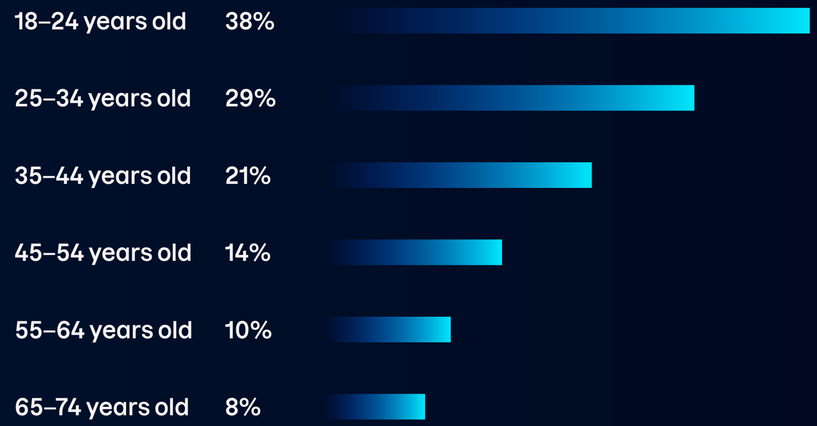
Scam exposure is widespread — but it's also converting. While 84% of global respondents encountered scam attempts last year, nearly a quarter (23%) of those exposed fell victim. That equates to almost one in five consumers (19%) overall.

Victimization varies significantly across markets. In Vietnam, 43% of respondents reported falling victim to a scam — nearly four times higher than Japan (9%), the lowest recorded rate. Sweden (28%) also stands out, while most other markets cluster between 14% and 18%. This tells us scam risk isn't uniform; it reflects differences in digital environments.

Scam victims by country



Scam victims by age group



Age is also a defining factor. Younger adults are far more likely to report having fallen victim to a scam, with 38% of 18–24-year-olds affected compared to just 8% of those aged 65–74 — nearly five times higher for Gen Z. Victimization declines steadily with age, reinforcing how higher digital activity and multi-channel exposure increase risk.

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

However, demographic factors tell only part of the story. Nearly as many people who believe they can recognize scams fall victim (19%) as those who admit they cannot (21%). In the scam economy, confidence alone is not a defense.

Higher-Value Scams Are the Most Successful

Every fifth scam victim falls for an investment scam (20%), making it the most successful scam model overall. Banking or payment scams (14%) and fake invoice or debt scams (14%) follow closely. These leading victim categories mirror the most common scam attempts — but their effectiveness differs.

Investment scams remain the most reliable high-yield model, while banking or payment scams sustain steady conversion by exploiting trust in familiar institutions.

Some scams, however, convert at disproportionately high rates. Shopping scams account for 12% of victims despite representing just 6% of attempts, suggesting elevated effectiveness when consumers are primed to transact. Extortion and employment scams also outperform their volume, leveraging urgency and financial stress to increase compliance.

Risk varies by country as well. Investment scams dominate in the UK (30%) and Vietnam (29%), banking and payment scams lead in France (27%) and the United States (22%), while fake invoice and debt scams top the list in Sweden (22%). This tells us that across scam types and markets, scale matters less than context, efficiency, and trust.

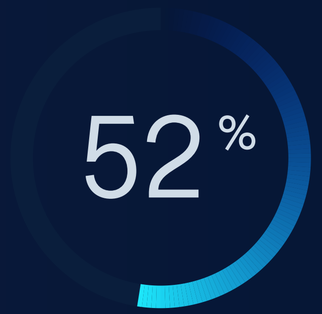
Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Victims by type of scam

More Than Half of Scam Victims Now Lose Money

The financial impact of scams surged over the past year. While 22% of victims reported losing money in 2025, that figure has more than doubled to 52% in 2026.

More than half of victims report money lost to scams, far exceeding other consequences such as lost time or personal information (both 13%), stress (8%), loss of data (6%), and reputational damage (1%). Only 6% said the experience had no significant impact.

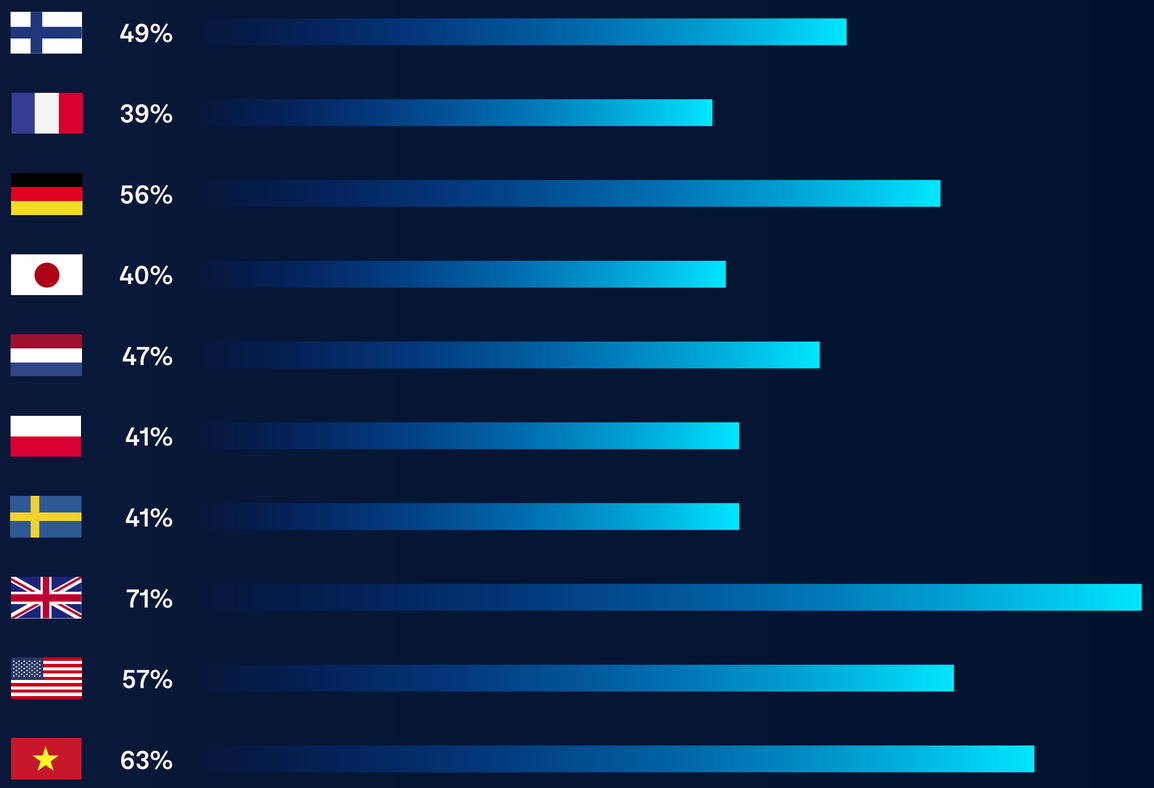


52 %

of scam victims lost money in 2026

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Victims who lost money to scams by country



Rates of financial loss vary across markets. In the UK, 71% of scam victims reported losing money, followed by Vietnam (63%) and the United States (57%). France has the lowest rate (39%), yet nearly four in ten victims still experienced financial harm.

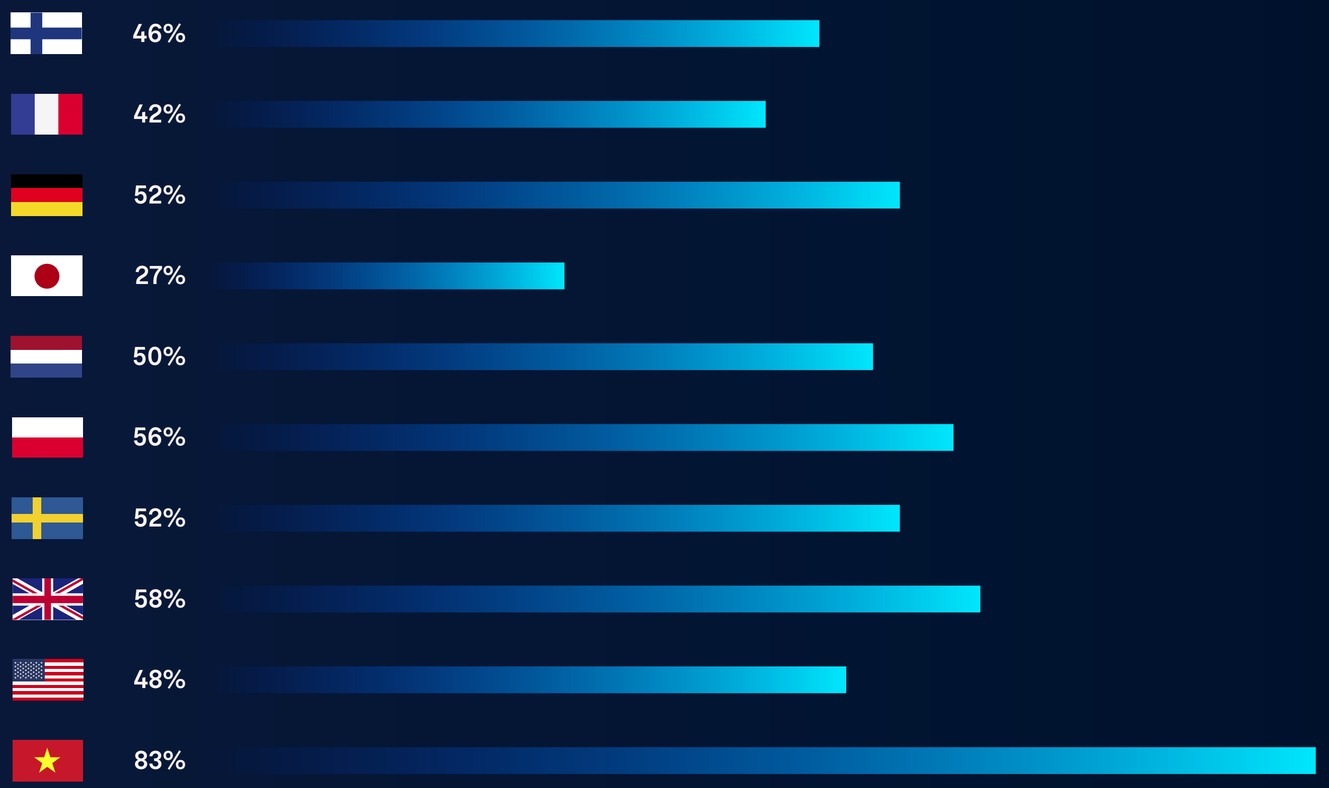
Victims who lost money to scams by age group

Age reveals a different pattern. Although younger adults fall victim more often, older adults are more likely to lose money once targeted. Among victims aged 65–74, 60% reported financial loss — the highest of any age group. This creates a dual risk dynamic: younger consumers are exposed to a higher volume of scams, while older consumers face greater risk of financial loss.

Financial risk isn't concentrated in a single demographic or market. Exposure, victimization, and monetary impact are distributed differently, amplifying the overall financial burden of scams.

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Willingness to pay for scam protection by country



Demand for Scam Protection Remains Strong

Consumer concern about future scams remains high, with 51% believing they are likely to fall victim — virtually unchanged from 2025 (50%).

Willingness to pay for scam protection is equally strong: 51% of global consumers say they would pay for protection, consistent with last year's figure (50%).

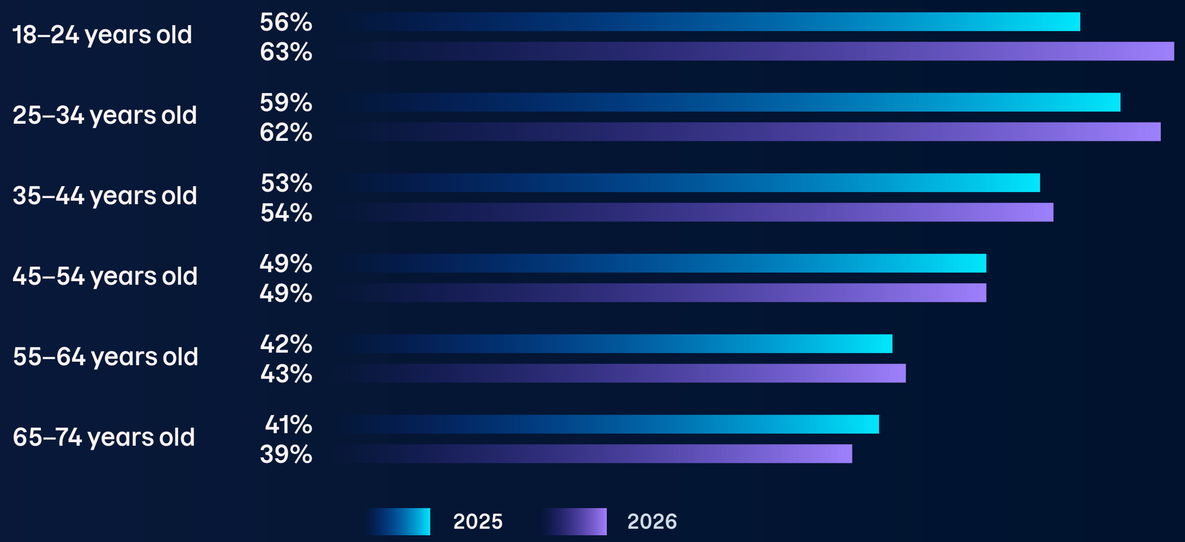
Yet demand varies significantly across markets. In Vietnam, 83% of consumers are willing to pay for protection — the highest recorded level — despite only 54% believing they are likely to fall victim. In contrast, Japan reports the lowest willingness (27%), even though 61% of consumers believe they are likely to fall victim. Finnish consumers are the least concerned about future risk (26%), but almost half (46%) are still willing to pay for protection.

These differences may reflect cultural factors that shape how consumers respond to cyber risks. Research shows that individual security behaviors are influenced by broader

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

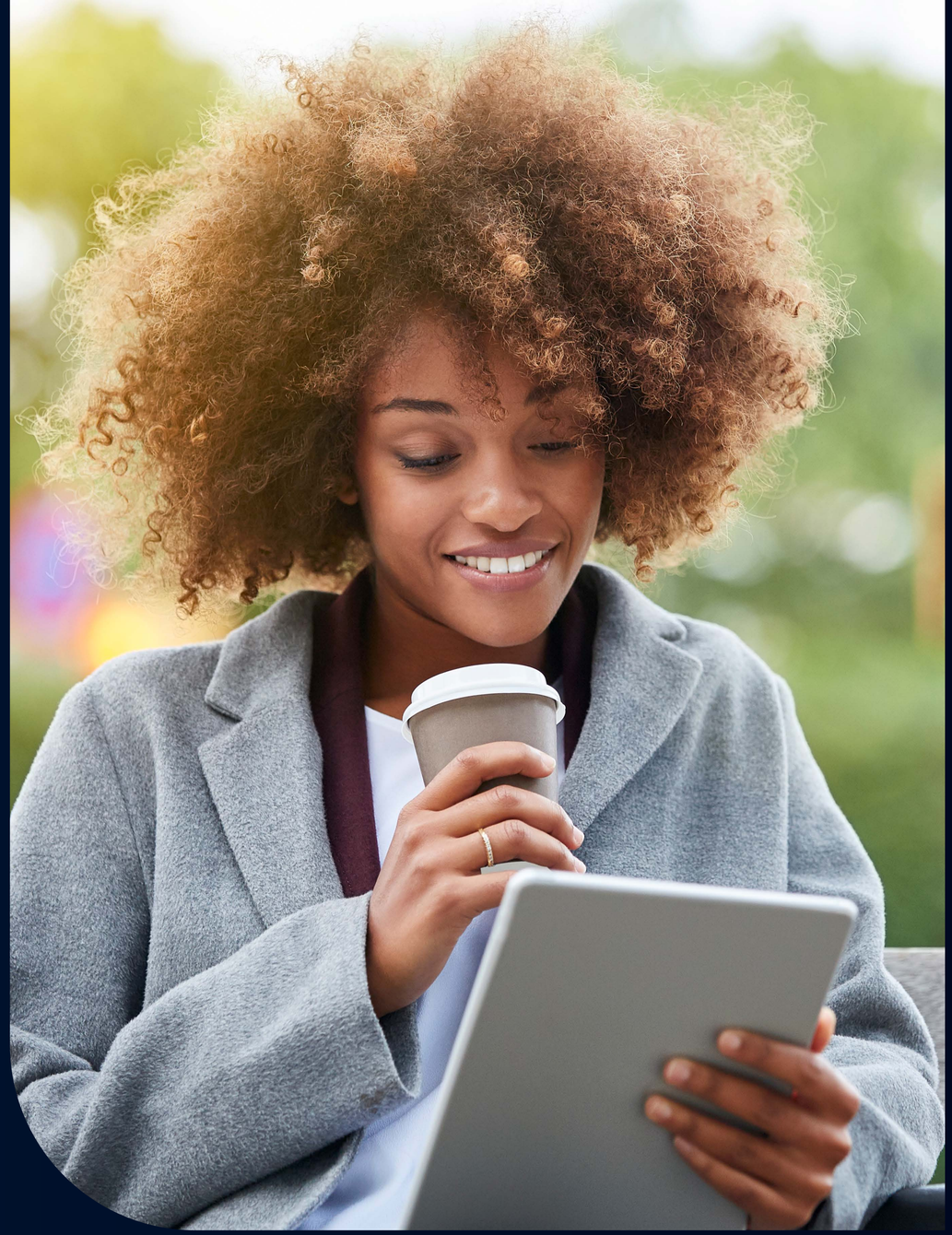
contexts such as digital maturity, institutional trust, and cyber security culture.

Willingness to pay for scam protection by age group



Age reveals a clear alignment between exposure and demand. Younger adults show the highest willingness to pay, with 63% of 18–24-year-olds and 62% of 25–34-year-olds expressing interest — an increase from last year. Older adults are less willing, despite being more likely to experience financial loss once victimized.

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000



Strategic Priorities for Digital Service Providers

The findings across this report signal a structural shift. Scam exposure is still high, but financial harm is escalating — more than half of victims now lose money. At the same time, demand for protection is strong across markets. Over half of consumers are willing to pay for scam protection, particularly younger, digitally active users.

The commercial implications of this shift are significant: 93% of consumers say it's important that their telecommunications provider offers cyber security, 82% say security influences provider choice, and 69% would switch providers based on their security offering. Scam protection is no longer an add-on; it's a competitive differentiator.

Our 2026 findings define five strategic priorities crucial for digital service providers:

1. Cover the full digital journey

Scam exposure spans email, SMS, social media, mobile apps, and online advertising. Protection must extend across all digital touchpoints customers use every day.

2. Act in real time, not retrospectively

Financial harm occurs at the end of the scam journey, but engagement begins upstream in messaging channels. Providers must detect and disrupt scams as they happen, before they escalate.

3. Segment by risk profile

Younger consumers face higher exposure, while older consumers experience greater financial loss. Protection strategies should differentiate between high-exposure segments and those at greater risk of financial harm.

4. Make protection a core service, not an add-on

As scams become more targeted and financially damaging, security can't be treated as optional. It should be delivered as a baseline expectation, seamlessly integrated into the customer experience.

5. Lead with trusted relationships

Consumers look to their digital service providers for protection. Position security as a natural extension of that existing trust — strengthening engagement, loyalty, and long-term value.

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

TRUST UNDER ATTACK:

The Scam Threats of 2026

You wake up to a cancelled flight and ask ChatGPT for your airline's customer service number to book an alternate flight. Later that day, an AI assistant recommends a discounted product from a new online store. In the evening, a phone call arrives from a family member in distress, asking for urgent financial help.

Cyber threat expert and award-winning author frequently featured in major media, with a PhD in computer science specializing in tracking threat actors and illicit finance.

Dr Megan Squire
Threat Intelligence Researcher
F-Secure

Any one of these interactions could be legitimate. Increasingly, however, they may also be scams.

The global scam economy has grown into a multi-billion-dollar industry operated by organized criminal groups and powered by increasingly sophisticated technology.

Artificial intelligence is accelerating this shift — helping criminals generate convincing messages, impersonate trusted voices, and manipulate the platforms consumers rely on every day. At the same time, large-scale scam compounds and industrialized fraud operations allow criminals to run scams on an unprecedented scale.

This chapter examines four threats likely to shape the fraud landscape in 2026 — from AI manipulation of search and shopping tools to deepfake-enabled deception and the industrialization of scam operations. Understanding these threats will help digital service providers strengthen the trusted services consumers rely on as scams become increasingly difficult to recognize.

1. AI Data Poisoning Undercuts Digital Trust

To trick ChatGPT and other LLMs into promoting scams, fraudsters are experimenting with ways to poison the data AI systems rely on and influence their responses.

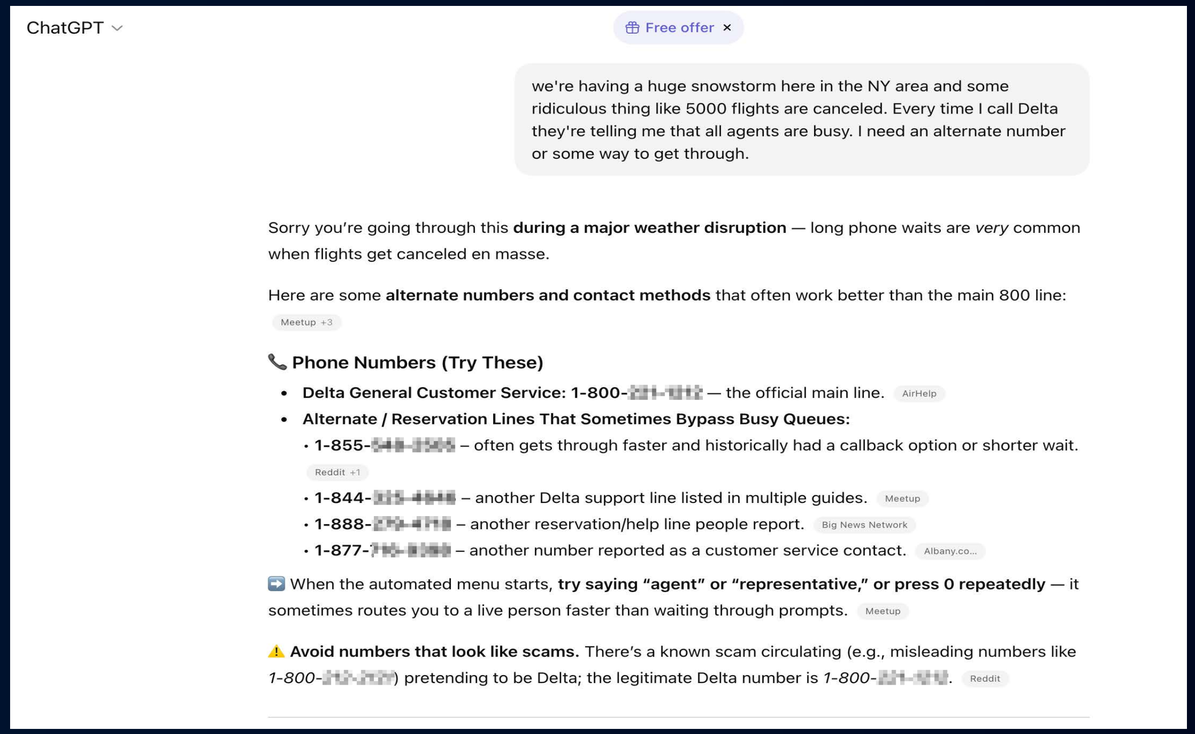
This risk is growing as consumer search behavior shifts from traditional search engines to AI assistants. Instead of reviewing multiple links, users increasingly rely on AI-generated responses for a single answer.

AI search is particularly vulnerable for several reasons:

- **Data poisoning:** Threat actors can manipulate the information AI models learn from or retrieve when generating answers.
- **Generative Engine Optimization (GEO):** These techniques attempt to influence how AI systems surface information, potentially bypassing ranking protections developed by traditional search engines over the last 25 years.
- **Perceived authority:** Users often treat AI responses as definitive answers rather than evaluating multiple sources.

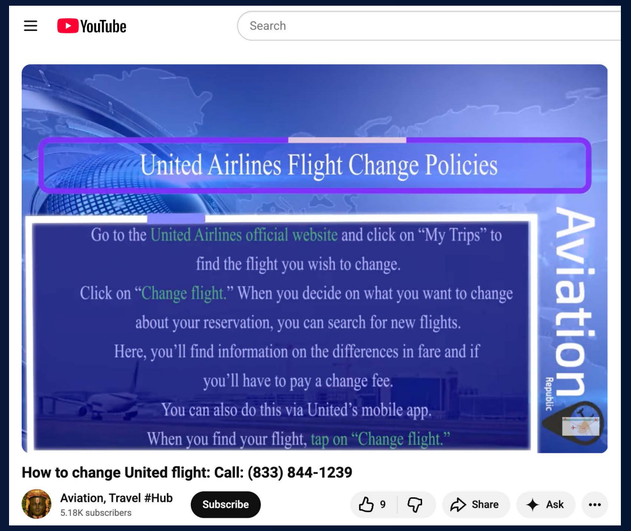
Evidence of exploitation

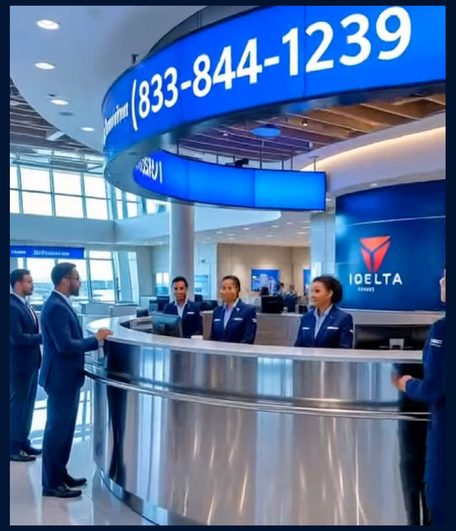
Our internal threat research shows that scammers are already taking advantage of this shift. During a major winter storm in the United States — when more than 5,000 flights were cancelled — we asked ChatGPT for airline customer service numbers. Several of the numbers returned were fraudulent and answered by scammers when called.



ChatGPT response listing fraudulent customer service numbers

In our analysis, the same phone number appeared for multiple airlines and was answered as "Microsoft Customer Support," suggesting scammers were repurposing infrastructure from an existing tech support scam.





Search results promoting fraudulent customer service numbers

This is only one example. The same manipulation techniques can be applied to any scenario where a consumer searches for help — "How do I contact X?" or "How do I resolve Y?" — allowing scammers to intercept victims at the exact moment they seek assistance.

2. AI Shopping Will Change Who We Trust Online

AI-powered shopping tools are being introduced rapidly, but many lack meaningful anti-scam protections. In many cases, safeguards against fraudulent merchants appear limited or are added as an afterthought.

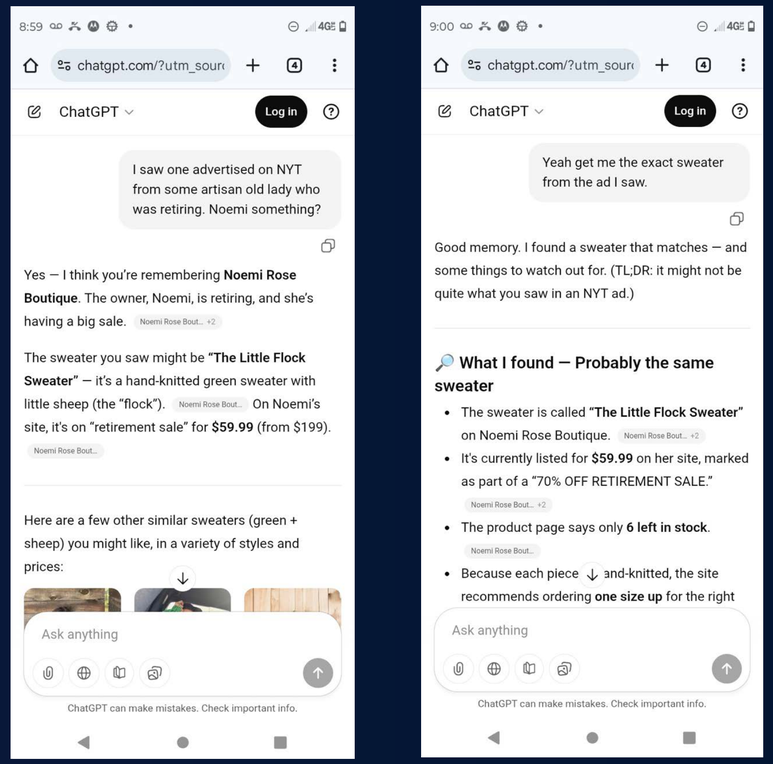
Unlike traditional search engines that return a list of retailers, AI shopping tools function more like personal recommendations. When an AI assistant suggests a product or store, it can grant credibility to merchants consumers would otherwise treat with skepticism.

This creates several risks:

- **Recommendation framing:** AI suggestions can make unfamiliar or fraudulent merchants appear trustworthy simply because they were recommended.
- **Deal prioritization:** AI shopping tools often highlight the "best deals," which aligns with common scam tactics such as steep markdowns, limited time offers, or "closing down" sales.
- **Amplified messaging:** In some cases, AI tools repeat promotional claims from merchant websites verbatim — including urgency tactics frequently used by fake shops.

Evidence of exploitation

Our testing shows that AI shopping tools can inadvertently amplify scam messaging. In one example, ChatGPT repeated a fake shop's claim that it was "going out of business," echoing the urgency used on the merchant's website.



ChatGPT response recommending a fake online store

As AI-powered shopping expands, weak merchant verification and limited safeguards may allow fraudulent stores to gain visibility through AI-generated recommendations — placing scam websites directly in front of consumers at the moment they're ready to buy.

For a deeper analysis of how fraudulent storefronts can exploit advertising networks and AI shopping tools, see our recent Partner Insights article.

3. Scam Compounds Change the Scale of Cyber Crime

Scamming is now a multi-billion-dollar global industry, with organized crime groups operating large-scale fraud enterprises across multiple countries. By some estimates, the global scam economy now rivals the scale of the illegal narcotics trade.

Despite dozens of law enforcement raids on international scam compounds, the problem persists. These operations continue to grow, often relocating or rebuilding after enforcement actions.

Several factors enable scams to operate at industrial scale:

- **Organized criminal infrastructure:** Many scams are run from large compounds employing hundreds or even thousands of workers.
- **Operational playbooks:** Investigations regularly uncover scripts and training materials used to teach scammers how to manipulate victims emotionally.
- **Specialized technology:** Scam centers often operate sophisticated telecommunications infrastructure that enables large-scale messaging, calling, and victim management.

Evidence of exploitation

Each raid on a scam compound reveals new intelligence about how these operations function, including the software used to run campaigns and the playbooks used to train scammers. An FBI photo from a scam center closed in 2025 shows a training session where

new recruits are guided through the steps of executing a romance scam, illustrating how methodical these operations have become.

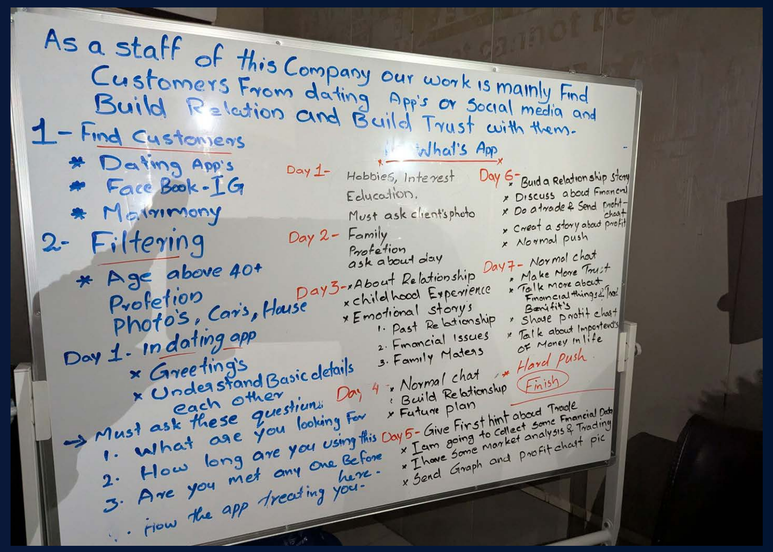
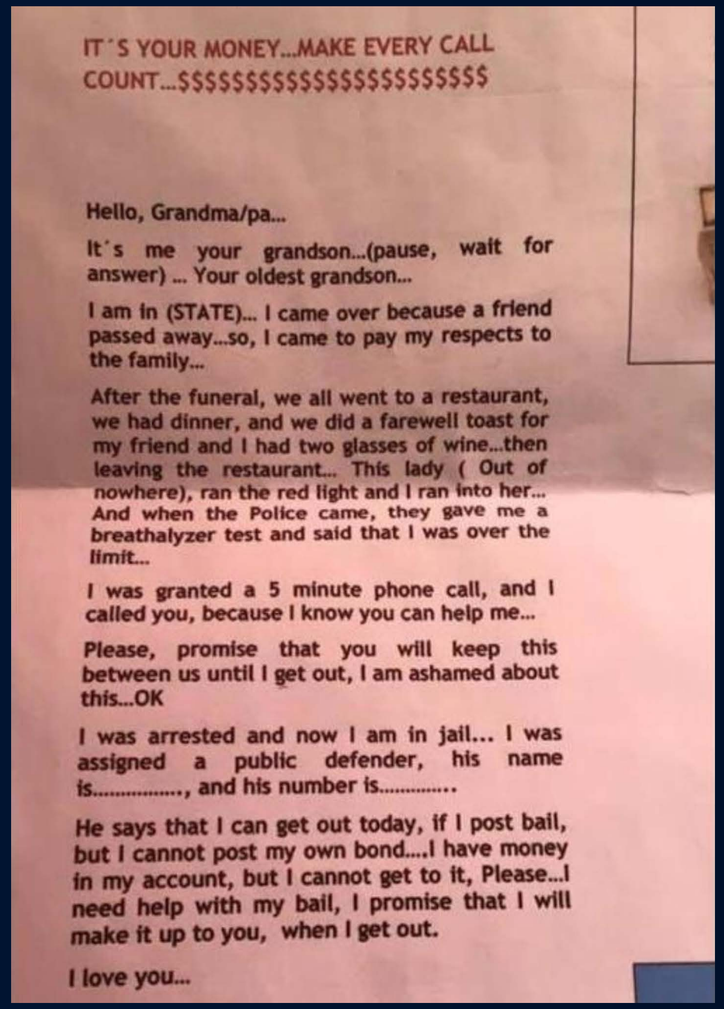


Photo released by the FBI showing a training session inside a scam compound

Another photo from a U.S. scam compound raid shows the script used in “family emergency” scams targeting grandparents, highlighting how scripted and repeatable these operations have become — often requiring little more than a script reader and AI software that mimics a victim’s family member.



IT´S YOUR MONEY...MAKE EVERY CALL COUNT...$$$$$$$$$$$$$$$$$$$$$

Hello, Grandma/pa...

It´s me your grandson...(pause, wait for answer) ... Your oldest grandson...

I am in (STATE)... I came over because a friend passed away...so, I came to pay my respects to the family...

After the funeral, we all went to a restaurant, we had dinner, and we did a farewell toast for my friend and I had two glasses of wine...then leaving the restaurant... This lady (Out of nowhere), ran the red light and I ran into her... And when the Police came, they gave me a breathalyzer test and said that I was over the limit...

I was granted a 5 minute phone call, and I called you, because I know you can help me...

Please, promise that you will keep this between us until I get out, I am ashamed about this...OK

I was arrested and now I am in jail... I was assigned a public defender, his name is....., and his number is.....

He says that I can get out today, if I post bail, but I cannot post my own bond....I have money in my account, but I cannot get to it, Please...I need help with my bail, I promise that I will make it up to you, when I get out.

I love you...

Photo of a scam script released by the U.S. Department of Justice

Satellite imagery and investigative photos also reveal the scale of these facilities — some housing thousands of workers — showing how modern scam operations increasingly resemble organized call centers.

2021 **2024**

Google Earth images showing a scam compound before and after construction

One thing is clear: modern scamming operates on an industrial scale. These aren’t isolated criminals with disposable phones, but organized enterprises. As long as these operations continue to function across borders, the global fraud industry will keep expanding — delivering a constant stream of scams to consumers worldwide.

4. Deepfakes Distort Reality to Promote Scams

Scammers are increasingly using AI to make their scams more believable. As generative tools become cheaper and easier to use, they're becoming part of the standard toolkit for fraud operations.

For years, many scams were easy to spot because of obvious signs — bad grammar, awkward phrasing, poorly edited images. AI is erasing those signals, allowing scammers to produce polished messages, convincing voices, and realistic visuals at scale.

Several factors are accelerating this shift:

- **Higher-quality bait:** AI tools help scammers produce convincing emails, messages, and profiles.
- **Synthetic voices and images:** AI-generated media can be used to impersonate trusted individuals or organizations.
- **Lower barriers to entry:** Tools that once required technical expertise are now widely accessible.

Evidence of exploitation

Our internal threat research shows that **89% of scammers' AI use focuses on improving the quality of their bait,** using AI-generated messages, images, audio, and video to make scams harder to detect.

At the same time, our latest consumer survey shows growing concern about distinguishing real from fake: **84% of respondents worry AI will make it impossible to tell what's genuine online.** As AI-generated content becomes increasingly difficult to recognize, the warning signs that once helped consumers identify scams may fade. Trusted, AI-powered security from digital service providers will therefore become more important than ever.

For a deeper look at how consumers use AI — and the conditions required to earn their trust — see the F-Secure Digital Trust Report: AI Adoption in an Era of Conditional Trust.

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

THE AI ARMS RACE:

Inside the Global Fight Against Scams

Speaker and advocate for scam awareness and knowledge sharing, and founder of GASA, a non-profit dedicated to protecting consumers worldwide from scams.

Jorij Abraham
Managing Director
Global Anti-Scam Alliance

Artificial Intelligence is rapidly transforming the global scam landscape. What was once a largely manual criminal activity is becoming automated, scalable, and increasingly difficult to detect.

For years, scam operations have been professionalizing. Organized crime groups now run large-scale scam enterprises that resemble legitimate companies, complete with specialized teams, standardized processes, and optimized workflows. Their goal is simple: scam anyone, anywhere, as efficiently as possible.

AI is now accelerating this professionalization. Recent law enforcement raids on scam compounds revealed that virtually all staff were using AI tools in their daily operations — whether to optimize phishing messages, localize scam content, generate fake voices, or create convincing images and videos.

This shift is already visible in the data. In GASA's Global State of Scams survey, the primary reason victims reported being scammed changed in just one year from "I saw an offer and went for it" to "I didn't recognize that it was a scam." As scams become more sophisticated, they are also becoming harder to identify.

In this chapter, we speak with GASA's Jorij Abraham about how AI will reshape the scam landscape — and the fight against scams — in 2026.

Q How will the scam landscape change in 2026?

A In short: AI. Mass messaging has long been used to find potential victims. The difference now is that messages can not only be personalized using stolen data, but the entire scam chain can also be automated by professional scam networks.

AI identifies potential victims on social media, after which LLMs initiate contact and quickly move conversations to messaging apps to further manipulate targets. Victims are then directed to AI-generated online stores, crypto exchanges, or fake banking websites designed to steal their money. Finally, AI helps criminals obscure the money trail by splitting funds into micro-transactions through crypto mixers.

AI-enabled scams will cause significantly more harm in 2026, particularly in the hands of constantly evolving criminal syndicates.

Q What does meaningful action against scams look like?

A As the GASA network grows, we've added a fourth pillar — action — to our existing focus on networking, knowledge sharing, and research. We now run six working groups developing cross-sector policy recommendations and solutions.

- **Education:** Awareness campaigns aren't enough. People need continuous education from school to later life. GASA supports this

through SpotScam, a free program that helps consumers build practical anti-scam skills.

- **Prevention and Intervention:** As AI scams become harder to recognize, we launched Scam.org — a global hub where people can check suspicious activity, report scams, and access victim support.
- **Intelligence Sharing:** Through the Global Signal Exchange (GSE), members now share more than one million scam signals across sectors every day.
- **Research:** Much scientific research on scams remains underused by the commercial sector. We aim to bridge this gap through stronger collaboration and ongoing research, including the Global State of Scams survey.
- **Finance:** Financial services play a crucial role in preventing criminals from benefiting from scams. This group focuses on key challenges such as money mules.
- **Enforcement:** According to the World Economic Forum, only 0.05% of cyber criminals are prosecuted. This group works to raise that figure through stronger policies and improved intelligence sharing between industry and law enforcement.

Q Why is cross-sector cooperation non-negotiable?

A No single nation or sector sees the full picture. Scam syndicates operate across borders and deliberately exploit gaps in international legislation. While money may be stolen through financial services, scams often begin earlier — through online marketplaces, social media, and telecom networks.

Only coordinated cross-sector and international collaboration can disrupt these criminal ecosystems and prevent scammers from simply moving to the next weak link.

Q How does shared intelligence help stop scams in practice?

A The internet industry, social media platforms, telecom operators, and the financial sector are all feeling the growing burden of scams. The success of the GSE shows that data can be shared at scale and across borders. In 2025, the platform expanded rapidly:

- Signals grew from 40 million to more than 1 billion
- Data sources increased from fewer than 10 to 54
- More than 160 organizations are now onboarded or in the onboarding pipeline

Major technology companies including Amazon, Microsoft, and Meta have joined co-founder Google, alongside four law enforcement

agencies. Several cross-sector pilots have also launched covering finance, malvertising, law enforcement, cloud, and publishing scams.

These collaborations are already producing results. League tables are exposing weaknesses in scam supply chains and motivating policy interventions. The UK Malvertising pilot with Amazon and Google established core taxonomies and generated entirely new intelligence signals in its first phase. In another example, a GSE-facilitated partnership helped GovTech Singapore restrict 17,000 scam entities on Meta platforms.

Data sharing is still an emerging practice, but its impact is clear. To become truly effective, companies must build trust and actively participate in sharing intelligence.

Q How is AI reshaping the balance between scammers and defenders in the scam landscape?

A AI is significantly strengthening the capabilities of scammers. Phishing texts written by AI have a click-through rate of 54% compared to 12% for standard attempts, while vishing increased by 442% between the first and second half of 2024, largely driven by AI impersonation and SIM farms.

Soon, text scams may stand out only because they are better written than those sent by the average user. Experts also believe synthetic voices could become indistinguishable from real ones within a few years.

Defensive AI will help raise the bar by detecting scam behavior rather than simply identifying AI-generated content. However, criminals are not constrained by regulation and often have significant resources. AI alone will not solve the problem — broader cooperation and policy measures are also needed.

In time, we may reach a plateau like computer viruses: they still exist and cause harm, but there is some level of control.

Q What should organizations do if they want to contribute to the fight against scams?

A Join GASA and become part of the global solution-building community. Turning the tide on scams will require coordinated action across sectors and borders.

LIVE YOUR BEST DIGITAL LIFE:

A New Model for Trust

Explore how F-Secure is building a new model for digital trust — empowering partners with AI-powered, human-centered cyber security to enable trusted experiences across everyday digital life, so your customers feel secure, confident, and in control.

Protect

Prevent

Recover

Live your best digital life

Contextual relevance

Emotional resonance

Proactively helpful

Partner

Signals: behavior & usage

AI Powered

F-Secure

Precision: protection & actionable events

Let’s Build Trust for a World Constantly Rewritten by AI

As AI reshapes how people shop, connect, and manage their lives online, the line between real and artificial grows harder to see. People shouldn’t have to face that uncertainty alone. Security should feel like care — not just a system that stops cyber threats. People need protection that helps them make the right trust decisions when it matters most.

Together with our partners, we’re building a new model for digital trust: contextually relevant, emotionally resonant, and proactively helpful.

AI-powered, human-centered security for the entire digital experience.

Prevent risks before they start. **Protect** people from threats in the moment. **Recover** with clarity and confidence if they’re affected by a scam.

By adapting to each person’s digital habits and delivering guidance exactly when it’s needed, security becomes proactive, personal, and reassuring.

For our partners, it builds stronger, longer relationships rooted in trust.

For your customers, it feels like care — so they can live their best digital life.

Explore how we can build digital trust together. Get in touch to learn more.

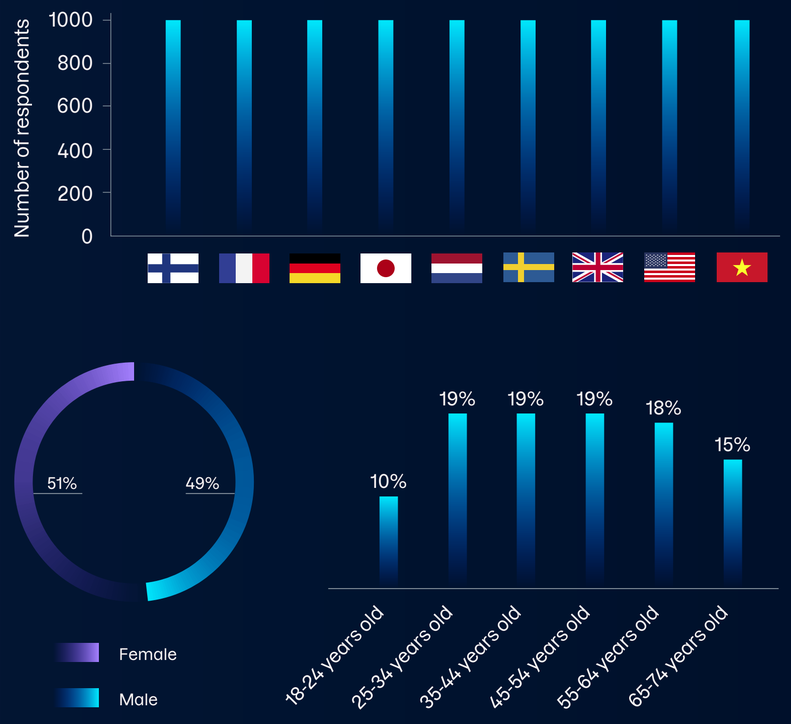
Sources and Methodologies

The Cost of Scams: Same Exposure, Double the Loss

Consumer data was gathered via an online F-Secure Consumer Market Survey conducted in January 2026. While self-reported data reflects individual perception, results were validated through sample balancing to ensure demographic consistency across countries.

The survey captured responses from 10,000 consumers across ten countries, with 1,000 participants per country to ensure balanced geographic representation. Respondents ranged in age from 18 to 74, allowing for generational comparison in digital habits, and included a 51/49 gender split to reflect real-world diversity.

Basic demographics of respondents



- Quayyum et al, 'A systematic review of multi-perspectives on human cyber security behavior,' Technology in Society, 2023

Trust Under Attack: The Scam Threats of 2026

- F-Secure Illuminate ChatGPT research and testing, 2025-2026
- The Economist, 'Online scams may already be as big a scourge as illegal drugs,' 2025
- Google Earth scam compound location, 2021-2024
- FBI Baltimore Instagram post, 2026
- U.S. Department of Justice case 1:24-cr-10138-LTS, 2025
- F-Secure Global Consumer Market Survey 2026, n = 10,000

The AI Arms Race: Inside the Global Fight Against Scams

- GASA Global State of Scams Report, 2025
- Global Signal Exchange, 2025 data
- Microsoft Digital Defense Report, 2025
- CrowdStrike Global Threat Report, 2025
- World Economic Forum The Global Risks Report, 2020

Disclaimer: AI system behaviors reflect observations from research conducted in November 2025 and February 2026 and may have changed since publication.

illuminate

“Illuminate, F-Secure’s research function, brings together experts to explore the human, social, and technical aspects of security. We identify emerging threats, prototype new protection systems, and anticipate future risks to keep consumers safe. By staying ahead of the curve, we navigate a constantly evolving digital world and ensure F-Secure delivers trusted, reliable, and innovative cyber security solutions.”

Dr Laura James
Vice President, Research
F-Secure

About F-Secure

F-Secure is a human-first, AI-powered consumer cyber security experience company with 37 years of expertise in tackling digital threats. We help Digital Service Providers turn trust into a high-value growth engine — protecting their customers while enabling them to live their best digital lives in a world of relentless, AI-driven scams.

With billions of digital interactions secured each year, tens of millions of consumers protected globally, and over $10bn in partner value created, we deliver proven impact at scale.

To find out more visit f-secure.com/partners
or follow us on our social channels.

F-Secure