US Scam Intelligence & Impacts Report 2025

Uncovering the human cost of scams—overconfidence, stigma, and silence.

F-Secure®

Executive Summary

The second annual F-Secure US Scam Intelligence & Impacts Report looks beyond statistics to examine scams through a human lens. As fraud becomes more manipulative, its toll is not just financial, but psychological, social, and systemic.

US data and behavioral insights reveal a paradox: most people trust their ability to spot scams—yet nearly a third still fell victim. This overconfidence leaves them emotionally exposed, digitally unprepared, and often too ashamed to speak out. Blame and stigma reinforce the silence, making scams one of the most underreported crimes today.

KEY FINDINGS

- **Confidence ≠ Resilience:** 80% of people believe they can spot a scam—but 60% of them still fell victim in the past year.
- **Victimization is Rising:** Scam rates in the USA doubled from 31% in 2024 to 62% in 2025.
- **Young Adults Are Most Exposed:** Individuals aged 18–24 are 1.6 times as likely to experience cyber crime than adults aged 55–74.
- **Underreporting is Widespread:** Only 2.6% of scams are reported in the US, largely due to victim blaming and feelings of shame.
- **US Consumers Want Protection:** 86% are likely to choose a carrier based on the security offered, and 55% are willing to pay for it. Yet 60% are unaware whether their carrier provides such protection.

A CALL TO ACTION FOR SERVICE PROVIDERS

Service providers are uniquely positioned to lead the fight against scams. With frequent customer touchpoints, they can embed protection into everyday services—shifting from one-off campaigns to ongoing education around behavior and emotion, not just red flags.

To address the human cost of scams, we must shift from blame to building resilience. That means empowering consumers to advocate for scam protection, fostering human connection at every customer touchpoint, and strengthening empathy towards victims.

Sources: F-Secure Consumer Market Survey, January 2025 (US data); GASA analysis of multiple data sources, 2024; F-Secure US Consumer Market Survey, July 2025

Contents

2025 US SCAM LANDSCAPE:

How Overconfidence Leaves Consumers Vulnerable

Scams don’t just exploit gaps in knowledge—they prey on overconfidence. Based on new market survey findings, this chapter unpacks the paradox of modern cyber crime: the more confident consumers feel, the more vulnerable they become.

Consumer intelligence researcher focusing on scams and security experiences.

Insights lead and owner of the F-Secure Consumer Market Survey (January 2025).

Over 20 years at F-Secure exploring trends in consumer behavior and cyber threats.

Timo Salmi
Senior Solution Marketing Manager
F-Secure

The Overconfidence Effect

In today's hyperconnected world, consumers are more likely than ever to fall victim to scams. But not all see it that way—many believe they're equipped to recognize and avoid them. This confidence offers a sense of control, but it can also be their greatest weakness.

According to US data from the F-Secure Consumer Market Survey (January 2025), **80% of Americans believe they know how to spot a scam**. Yet **60% of those confident individuals still fell victim** in the past 12 months. This is the overconfidence effect in action—a cognitive bias where people overestimate their own knowledge or ability, leaving them blind to real risk.

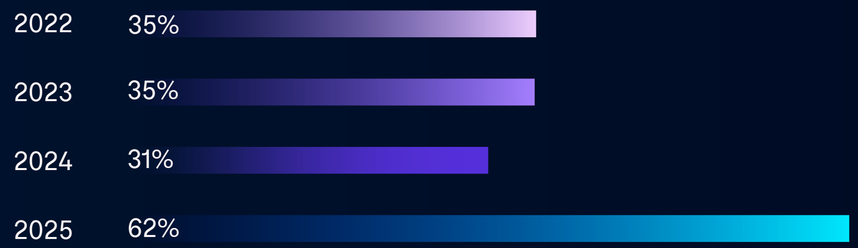
of Americans believe they know how to recognize an online scam

of those individuals also reported falling victim to a scam in the last year

Scam Victimization Is Rising Drastically

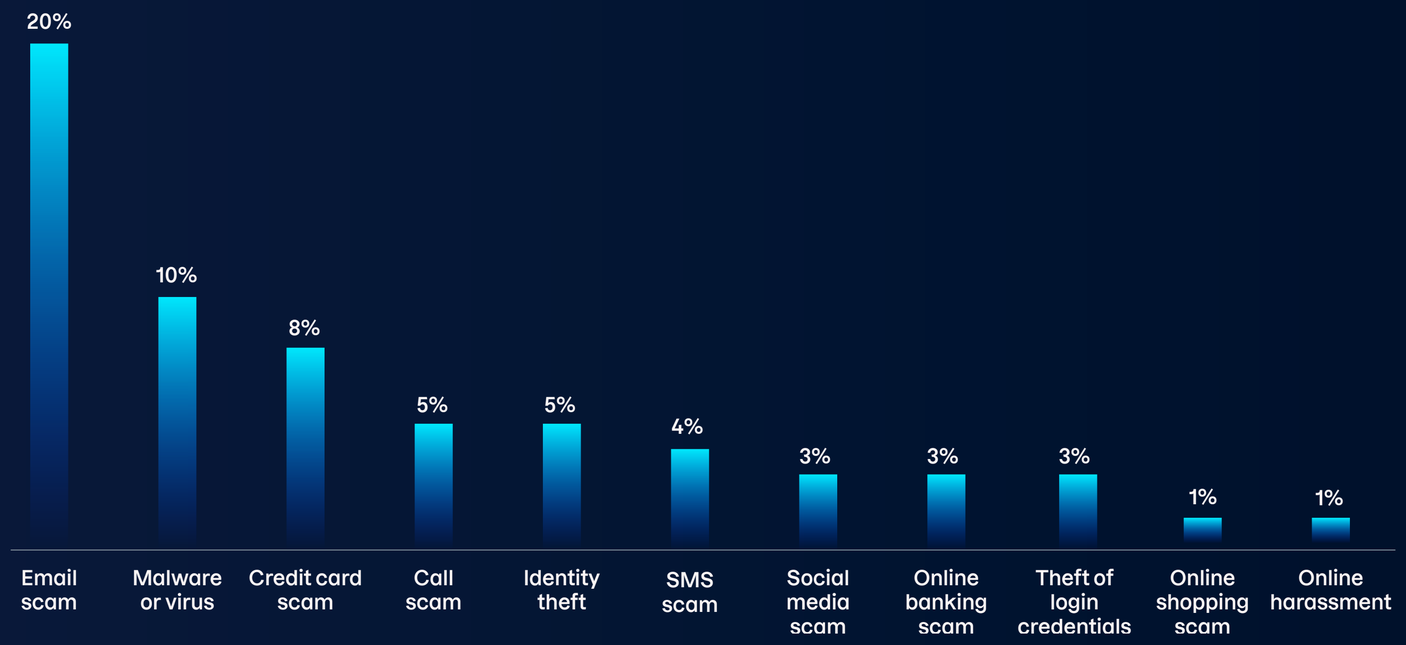
Scammers are quick to exploit these cognitive blind spots, using tactics like urgency and authority to override rational thinking. Our research shows that **scam victimization in the United States has doubled in just 12 months**, climbing from 31% to 62%.

Percentage of US respondents who fell victim to cyber crime (2022–2025)



Source: F-Secure Consumer Market Survey, January 2025 (US data)

Types of cyber crime US respondents fell victim to in the past 12 months



Overall, **62% of US respondents reported falling victim to cyber crime in the past 12 months**. The data shows no single dominant scam type—instead, threats are spread across a wide range of categories and channels. Email scams lead at 20%, followed by malware or virus attacks at 10%, credit card scams at 8%, and call scams and identity theft at 5% each.

Smaller but still significant numbers experienced SMS scams, social media scams, online banking scams, and online shopping scams. This variety underscores how cyber criminals are diversifying their tactics to target consumers in multiple ways, across every digital touchpoint.

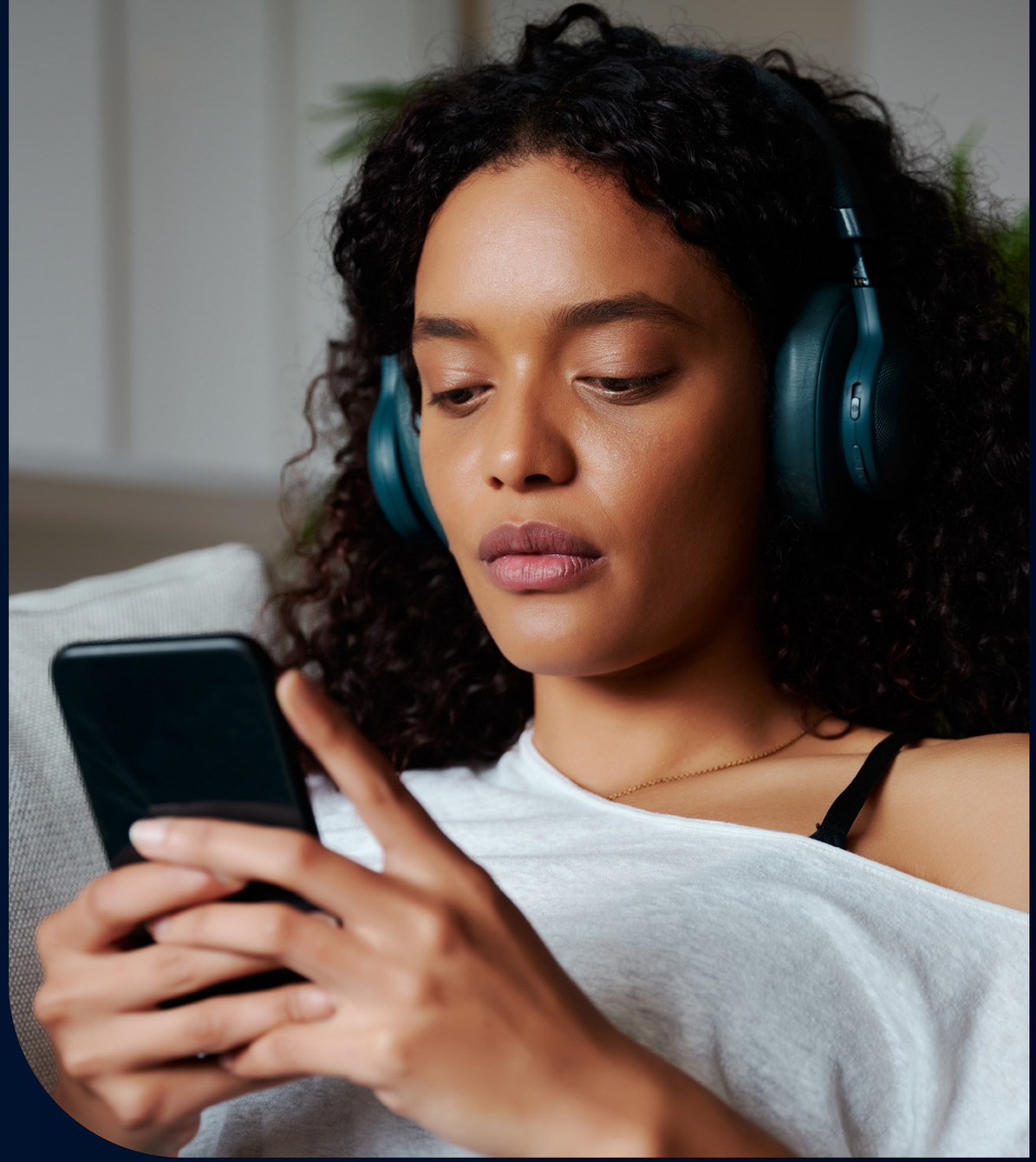
Source: F-Secure Consumer Market Survey, January 2025 (US data)

Digital Natives Are Most at Risk

Younger demographics—the very group seen as most tech-savvy—face the highest exposure to scams. **Adults aged 18 to 24 are about 1.6 times as likely to experience cyber crime (77%)** compared to those aged 55 to 74 (49%). A larger digital footprint, frequent online activity, receptiveness to new technology, and trust dynamics shaped by online influencers and parasocial relationships all increase exposure.

Cyber crime victimization by age group

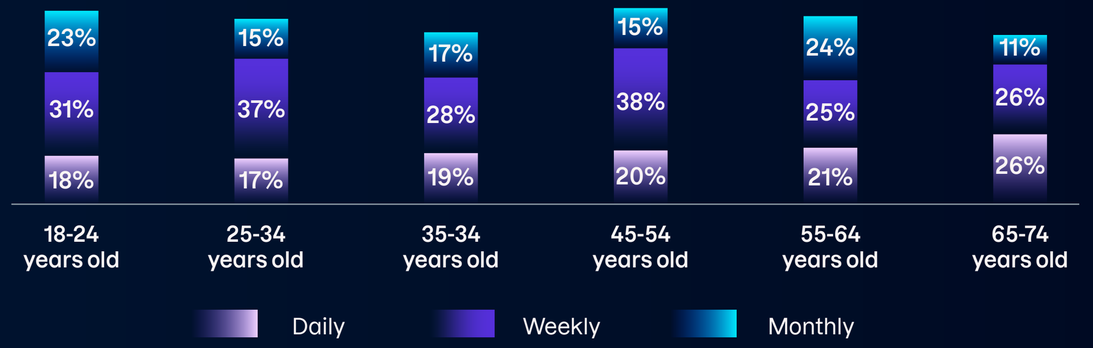
Source: F-Secure Consumer Market Survey, January 2025 (US data)



While 68% of Americans encounter scam attempts at least monthly, that rate rises to 72% among 18–24-year-olds. Reported exposure remains consistently high—ranging from the low 60s to low 70s—showing that scams are a constant threat across all ages, though the type of scam shifts over time. The pattern is uneven: exposure peaks among young adults, dips in midlife, rises again for older adults, and then falls among seniors.

Seniors may face fewer scam attempts, but they often suffer far greater losses. According to FTC consumer protection data, adults over 60 reported a sharp rise in impersonation scam losses last year. From 2020 to 2024, reports of older adults losing $10,000 or more to these scams increased more than fourfold. Even more striking, losses of over $100,000 surged eight-fold—from $55 million in 2020 to $445 million in 2024. While younger adults also reported losses, the financial toll was disproportionately higher for seniors.

Frequency of scam attempts by age group



Source: F-Secure Consumer Market Survey, January 2025 (US data)

Scam exposure is highest among younger adults (18–34), who are more connected and often more confident than cautious, making them prime targets for phishing. Cost-of-living pressures also leave them vulnerable to “get-rich-quick” scams. Exposure then dips for middle-aged adults (35–44), likely reflecting greater stability—settled financial routines and increased caution from parenting responsibilities.

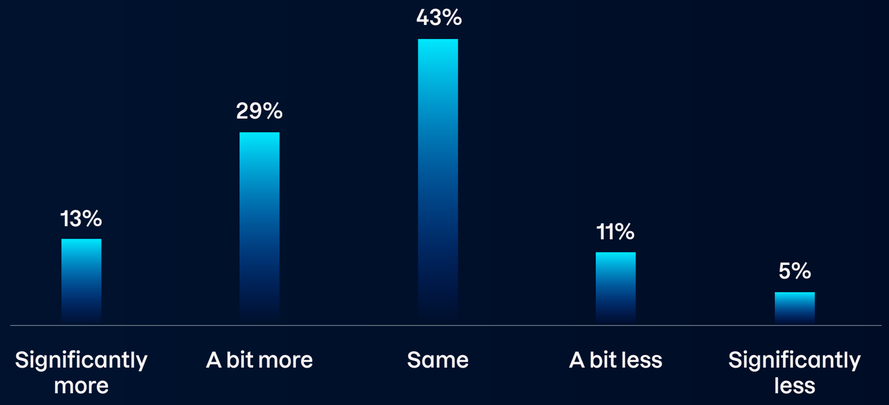
The curve rises again for older adults (45–64), who often manage complex finances such as mortgages, retirement planning, and healthcare costs, making them attractive targets for investment, IRS, or Medicare scams. Seniors (65–74) show lower exposure, likely due to reduced online activity, yet remain highly at risk when targeted.

Scams Are a Constant Threat

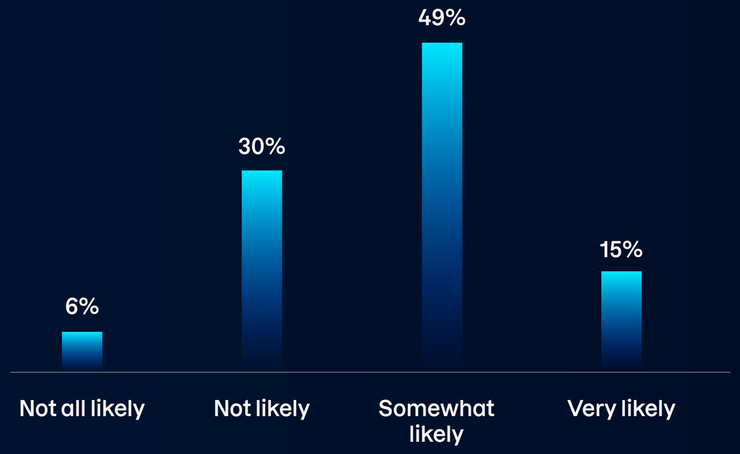
Scam attempt volumes are rising. While 43% of respondents reported receiving the same number as last year, nearly as many (42%) noticed an increase, and only 16% experienced a decline. This helps explain why **64% of US consumers consider themselves at risk of falling victim to scams or other cyber crime in the future.**

Source: F-Secure Consumer Market Survey, January 2025 (US data)

Percentage of US respondents who experienced scam attempts in 2024 vs 2023

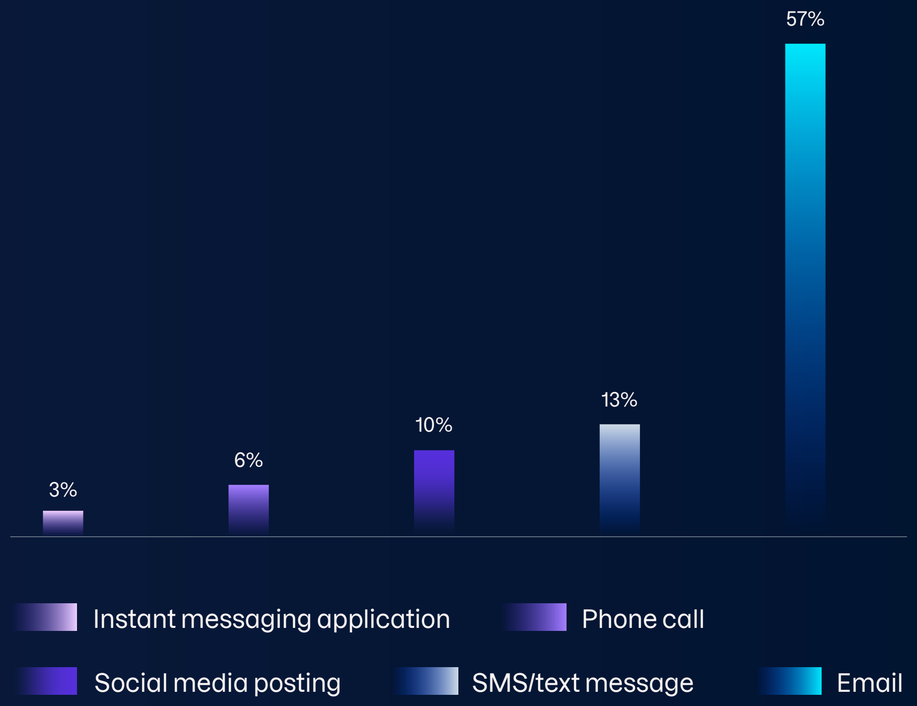


Perceived likelihood of falling victim to scams or cyber crime in the future



Email remains the top delivery channel by far at 57%. Yet despite its dominance, many still underestimate the sophistication of scams delivered through familiar channels like email and SMS. This perception-reality gap leaves US consumers unprepared.

Channels used for scam attempts in the past 12 months

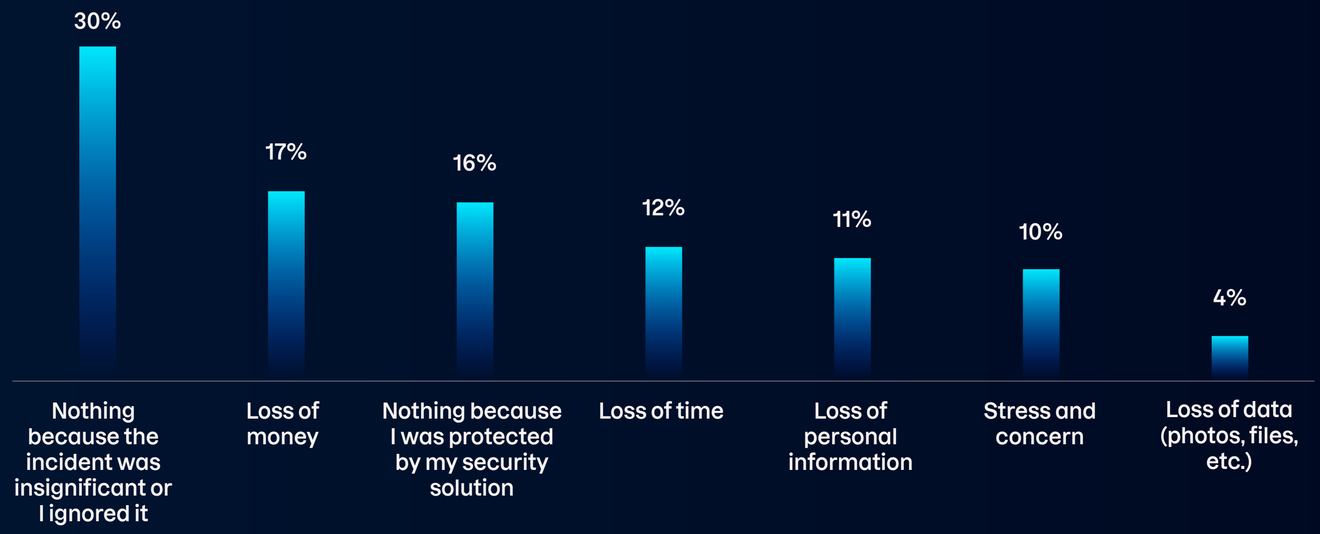


The Real-World Impact of Scams

Scams don't just cause momentary disruption—they have real consequences. Among victims, 17% lost money, 12% lost time, and 11% lost personal information. Others reported stress (10%) and data loss (4%).

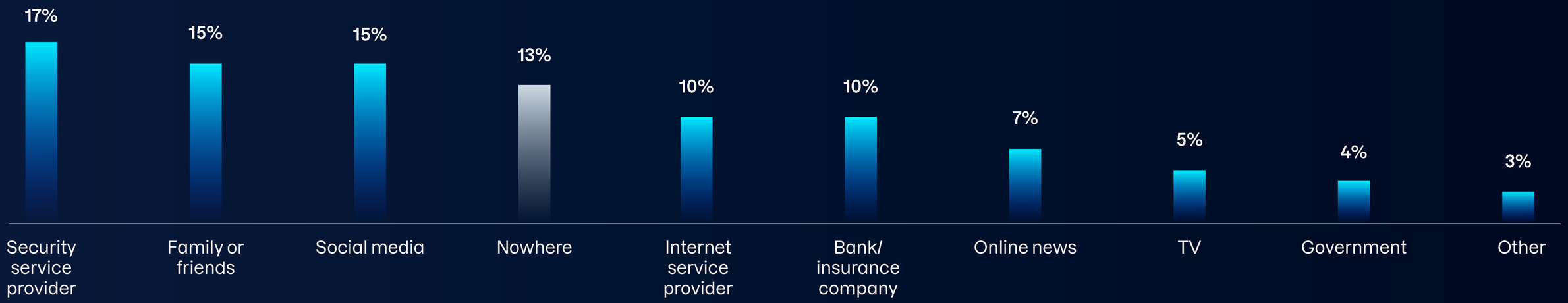
Yet 30% downplayed or ignored the incident—likely due to feelings of shame or embarrassment, growing desensitization from repeated scam exposure, or the belief that they should have known better. This avoidance reflects the overconfidence effect: "I should've seen that coming" becomes a reason to stay silent.

Consequences experienced as a result of cyber crime



Source: F-Secure Consumer Market Survey, January 2025 (US data)

How people stay informed about trending scams and online threats



A Fragmented Information Landscape

One reason overconfidence persists is the lack of centralized, trusted information about online threats. When asked where they learn about scam trends, 17% cite a security service provider, 15% turn to social media, 15% speak to friends or family, 10% rely on their carrier, bank, or insurer, and 13% admit they don't get scam information from any source at all.

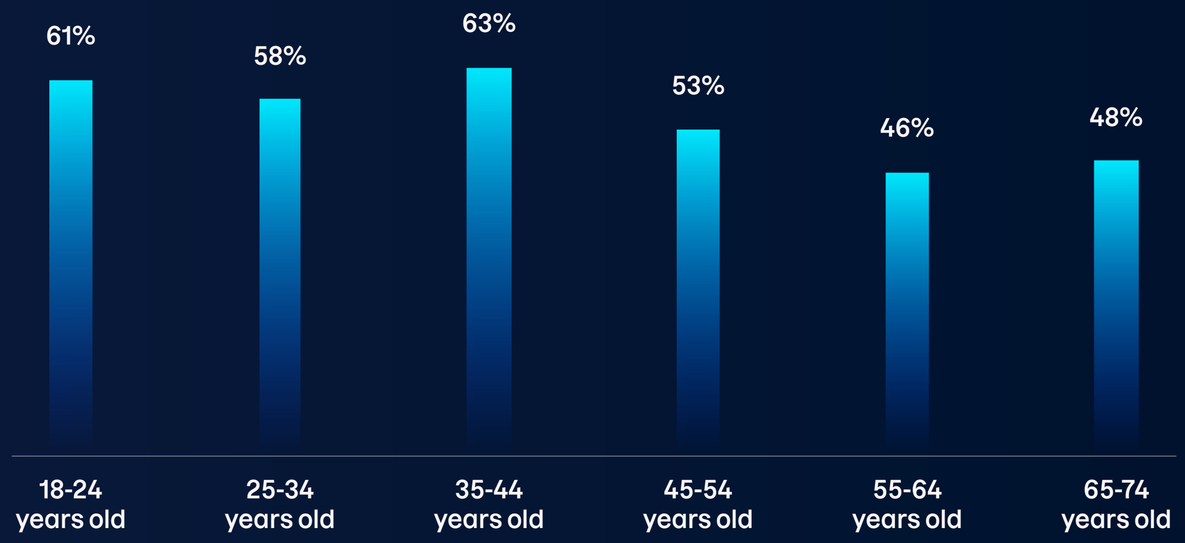
This fragmented landscape leaves consumers vulnerable to misinformation, outdated advice, and emerging scam tactics that often go undetected until harm is done.

Source: F-Secure Consumer Market Survey, January 2025 (US data)

Rising Willingness to Pay for Protection

Despite blind spots and gaps in awareness, consumers are beginning to recognize the limits of self-reliance: **55% of US respondents now say they are willing to pay for scam protection.**

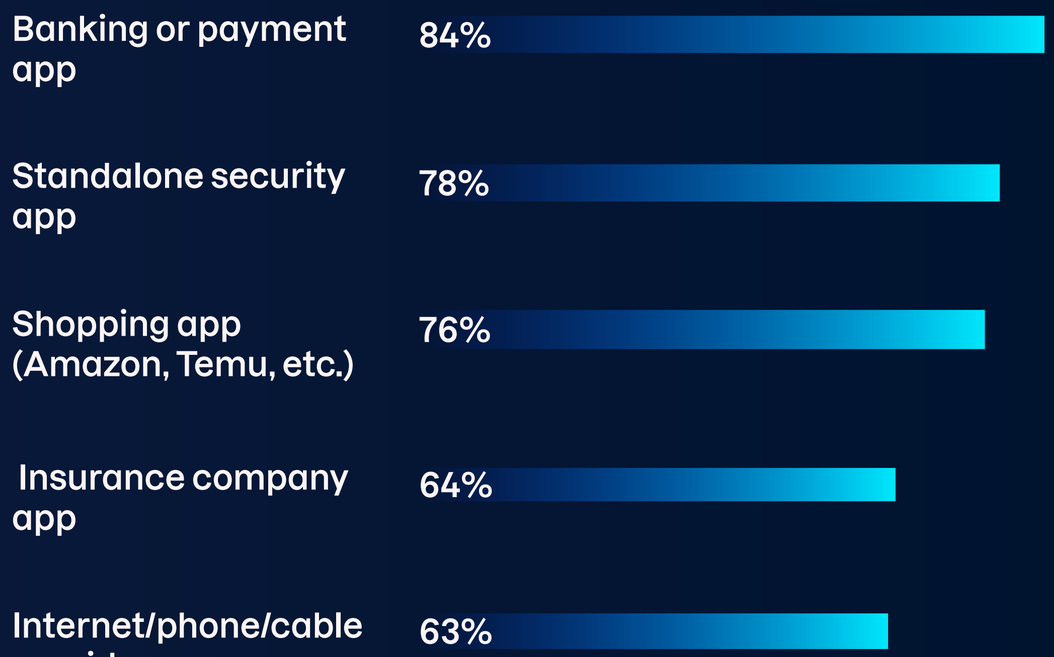
Willingness to pay for scam protection per age group



Younger adults (aged 18 to 44) are the most willing to invest, reflecting their greater exposure to scams and higher likelihood of falling victim. Crucially, consumers want protection from the brands they already trust. They expect banks, insurers, carriers, and other digital service providers to safeguard not only their money or connectivity, but their online security as a whole.

Source: F-Secure Consumer Market Survey, January 2025 (US data)

Which apps US consumers are open to for providing security



As scams become more personalized and persistent, consumers need more than instinct or isolated advice. They need seamless, always-on protection embedded in the services they already rely on.

Looking Ahead: Reframing Scam Education

It's not just a lack of knowledge that scammers exploit—it's misplaced confidence. That's why scam education must shift from information-sharing to behavior-shaping.

1. **Shift from awareness to resilience.** Reframe "Here's how scams work, learn the red flags" to "Even if you know the red flags, you can still be emotionally manipulated. Let's normalize hesitation as a safety tool."

2. **Focus on emotional triggers, not just scam tactics.** Rather than asking "What do scams look like?" ask: "When are you most emotionally exposed?" This reframes scam recognition as emotional literacy, not just pattern recognition.

3. **Empower consumers as advocates.** Instead of saying "You know the signs," prompt: "Do your loved ones?" Reframing personal awareness as community protection makes education more meaningful—and more effective. Especially during times of stress or emotional challenges brought on by major life changes.

Source: F-Secure Consumer Market Survey, January 2025 (US data)

HUMANIZING SCAMS:

“How Could You Be So Stupid?” —A Victim’s Story

Media personality sharing her experience as a victim of a prolific investment and romance scammer.

Author of the empowering true crime memoir The Last Victim.

Public speaker delivering keynotes on topics including scams, trust, shame, and financial security.

Tracy Hall
Author, Speaker, and Advocate

Some scams make headlines but leave deeper scars than the public sees. In this chapter, Author, Speaker, and Advocate Tracy Hall recounts being the final victim of con man Hamish McLaren, revealing how he manipulated her trust and underscoring the need to put people at the center of scam prevention and recovery.

“How could you be so stupid?”

I’ve asked myself this question about 2,649 times in the last eight years. I’ve also wondered how many others thought the same after hearing my story. I’ve come to accept it’s natural to go there—but I’ve also learned it’s unhelpful and deeply inaccurate.

In 2017, my world came crashing down when I woke up to a Crime Stoppers video of my boyfriend of almost 18 months being arrested outside his Bondi Beach apartment for swindling 15 Australian victims out of $7.6 million.

My boyfriend, Max Tavita—a Chief Investment Officer for a Family Office—was really Hamish McLaren, one of Australia’s most notorious con men. He stole my life savings ($317,000) and, it’s fair to say, my ability to trust.

A Match Made in Deception

We met in early 2016 on a dating app. I’d been separated from my husband for over a year, was working in a demanding marketing role at eBay, and adjusting to single parenting a five-year-old. I wasn’t looking for another husband—just company. Someone with similar interests, values, and humor. I matched with ‘Max’ and our relationship grew slowly. He was athletic and had a down-to-earth lifestyle, even though his work was anything but.

Over months, we had hundreds of detailed conversations about his work, investments, world economies, political impacts on global stock exchanges, financial opportunities, and much more. It was convincing. He shared weekly reports, had Bloomberg monitors that he tinkered on, and spent late nights watching the global markets.

When it came time to discuss my superannuation (pension scheme) and investments, I was so convinced he was exactly who he claimed—a skilled finance professional—that I didn’t even question it. I believed he could help me build my financial future and independence. And I was in love. So, I entrusted him with $317,000.

The Day His Lies Collapsed

Hamish was arrested in July 2017. He was sentenced to 16 years in prison for his crimes against 15 Australian victims, later reduced to 12 on appeal. He will be eligible for parole in July 2026.

The story hit the media in 2019 when The Australian released hit podcast *Who the Hell Is Hamish?* Through his investigations, journalist Greg Bearup uncovered that Hamish had likely stolen $60–$100 million globally over three decades.

I was his last victim and didn’t even know his real name when he was arrested. Everything about my life with him had been a complete fabrication. At 42, a single mother, I had to start over—financially, emotionally, and psychologically.

The True Price of Trust

The human cost of financial crime is rarely discussed. We focus on money lost, the technology required to detect scams, and regulatory frameworks—but not the human toll. The lives devastated by the greed of others. Some who never recover.

The emotional aftermath of a scam can often be more damaging than the financial losses. It erodes self-trust, corrodes confidence, and lingers far longer than people realize. For me, the price of trust was years of recovery and rebuilding. Learning how to trust the world and myself again after such betrayal has been one of my greatest challenges.

Scammers Hack People, Not Just Systems

I've thought a lot about how Hamish managed to manipulate me so successfully. What I've come to realize is that it's surprisingly easy to manipulate human behavior—the most dangerous weapon in a scammer's toolkit isn't software, it's psychology.

Scammers manipulate our brain biases—the mental shortcuts we use to make quick decisions. They exploit the primitive instincts that help us survive, like trust, love, loyalty, fear, and reciprocity, with clinical precision. In my case, Hamish manipulated me using multiple strategies and psychological tactics.

He Created a False Persona Matching My Values

Psychological exploitation: Mirroring and halo effect

Hamish crafted an identity that reflected my passions, ambitions, and emotional needs. He claimed to care about the same things and fabricated trauma to manufacture intimacy. This disarmed my critical thinking and created a false sense of familiarity and trust.

He Flooded Me with Financial Jargon and Urgency

Psychological exploitation: Cognitive overload, scarcity bias, and authority bias

He bombarded me with investment lingo and unique “opportunities,” making it difficult to dismiss or ignore. He positioned himself as a financial expert, using jargon and props to imply authority, while subtly investigating my personal financial position.

He Exploited My Trust and Weaponized Compassion

Psychological exploitation: Emotional manipulation and reciprocity bias

Hamish portrayed himself as a victim of past betrayals and injustices, making me feel emotionally protective of him. He told me his parents died to engender compassion as I too had lost a parent. It was emotional grooming: he turned my empathy into a weapon for his own gain.

He Used Gradual Commitment to Erode My Boundaries

Psychological exploitation: Foot-in-the-door technique and normalization

He didn’t ask for large sums up front—he started small. A rare investment opportunity, how much he was making for clients. It built a false sense of reliability and safety. Over time, he pushed the boundaries of what felt “normal,” until I was unknowingly in too deep.

He Isolated Me Emotionally

Psychological exploitation: Gaslighting and isolation tactics

He subtly avoided interactions with others. Friends and family were positioned as an inconvenience getting in the way of us spending time together. He created a psychological fortress around the relationship, and I was emotionally alone before I realized it.

“Why Don’t You Just Get Over It and Move On?”

I’ve spent eight years turning something devastating into something useful—writing *The Last Victim* to show how insidious and layered these crimes are, and speaking worldwide on victim narratives, trust, scam psychology, resilience, and rebuilding. Not because it’s easy, but because it’s essential.

Ultimately, the weakest link in the scam ecosystem is humans—you, me, colleagues, parents, kids. If there’s one thing I want people to understand, it’s this: the most intelligent thing we can do is to humbly accept that fraud could happen to anyone.

Looking Ahead: People Must Be the Priority

- We must design solutions and long-term recovery with humans in mind, supporting victims beyond reimbursement, as psychological and emotional impacts often outweigh the financial.
- Education needs to be harder-hitting—desensitization leaves consumers less vigilant, and phishing warnings no longer grab attention. Stories are powerful.
- Language matters. Victim-blaming increases stigma and shame, reduces reporting, and stops people from seeking help.
- Victims need a single, simple reporting and support pathway, guided by someone who can help them navigate the system. The current system is difficult to deal with, especially when you’re experiencing the impact of trauma and loss.

Product marketing leader specializing in launching innovative tech solutions.

Leads the go-to-market strategy for F-Secure's embedded security portfolio.

Holds an Executive Certificate from MIT and an MBA from the University of Georgia.

Bill Lott
Head of Marketing, Embedded Solutions
F-Secure

AWARENESS GAP:

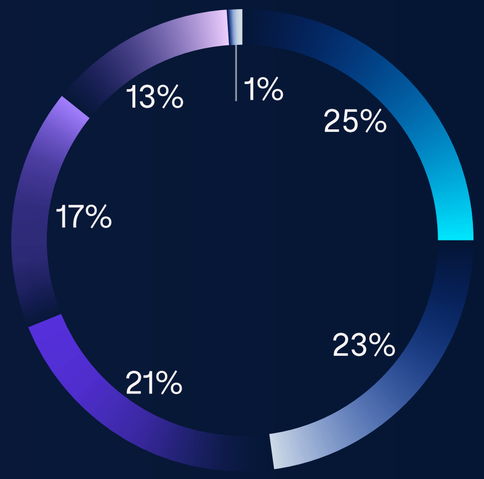
75% Expect Security—Yet 60% Don't Know Their Carrier Offers It

US consumers expect scam protection from their carrier, but most don't realize if it's available. Drawing on new consumer research, this chapter highlights where carriers are meeting expectations—and where they're missing out.

The Impact of Scams is More Than Lost Dollars

In our latest F-Secure Consumer Market Survey, which focused specifically on the US, respondents revealed just how pervasive digital scams have become. **One in four Americans reported losing money to scams in the past year,** with more than a quarter of those victims parting with serious amounts—ranging from $500 to over $5,000. But the impact of scams goes far beyond financial loss.

Emotional impact of scams on victims



25% were angry or frustrated

23% felt embarrassed or ashamed

21% feared for their safety or the financial consequences

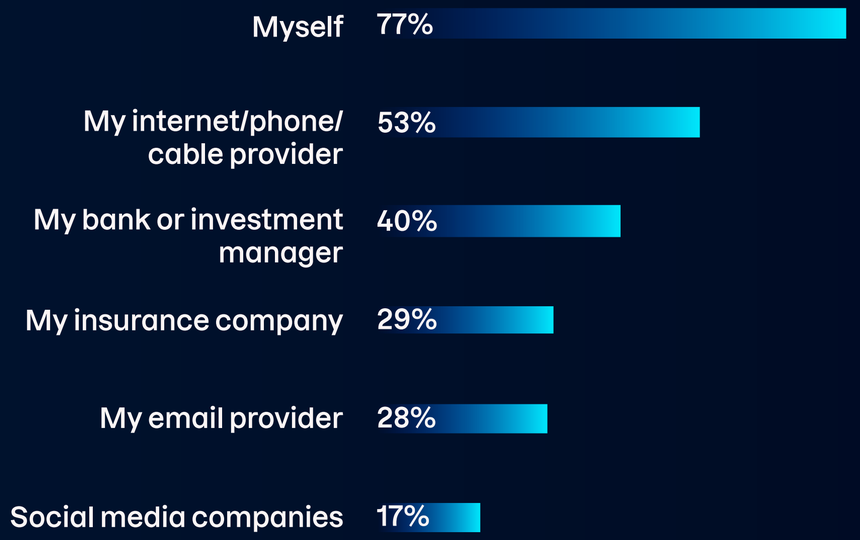
17% describe it as an invasion of their privacy

13% felt inconvenienced

1% had no strong feelings

Among those who fell victim, **anger and frustration (25%)** were the most common reactions, followed by embarrassment or shame (23%), fear for personal safety or financial consequences (21%), feeling violated (17%), and inconvenience (13%). These varied emotional responses reflect the broader psychological toll of scams, fueling anxiety, mistrust, and hesitation in everyday digital life.

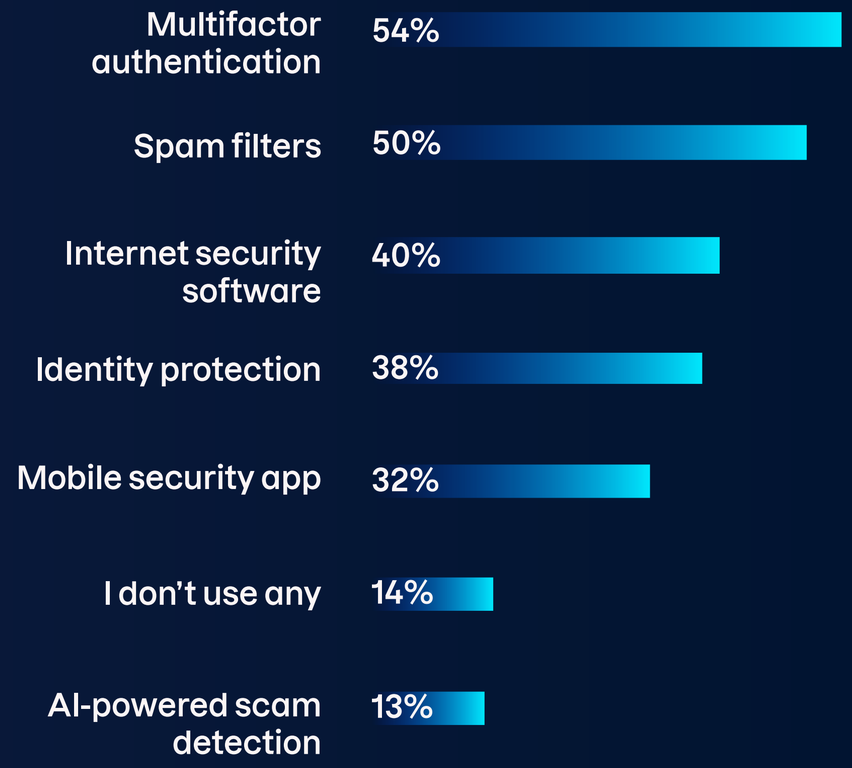
Who do you trust to protect you from digital scams?



Source: F-Secure US Consumer Market Survey, July 2025

Despite the growing threat landscape, **more than three quarters of consumers say they trust themselves most** to stay safe from online scams. But when it comes to the tools they actually use, the data tells a different story.

Which tools do you use to protect yourself from digital scams?



Only 54% use multifactor authentication, and fewer than half rely on tools like spam filters (50%) or internet security software (40%). Interestingly, 1 in 7 (14%) report using no security tools at all. This disconnect reveals a critical insight: **while consumers may trust themselves in theory, many are under-protected in practice.**

Why might this be the case? Several factors contribute:

- **Limited awareness:** Many are unfamiliar with scams and the protections available to them.
- **Perceived complexity:** 60% of US consumers consider cyber security too complicated.
- **Lack of trust:** 71% of Americans report not knowing who to trust online.

Encouragingly, consumers also show openness to external support: **more than half (53%) trust their internet, phone, or cable provider to protect them from digital scams.**

A Powerful Opportunity for Carriers

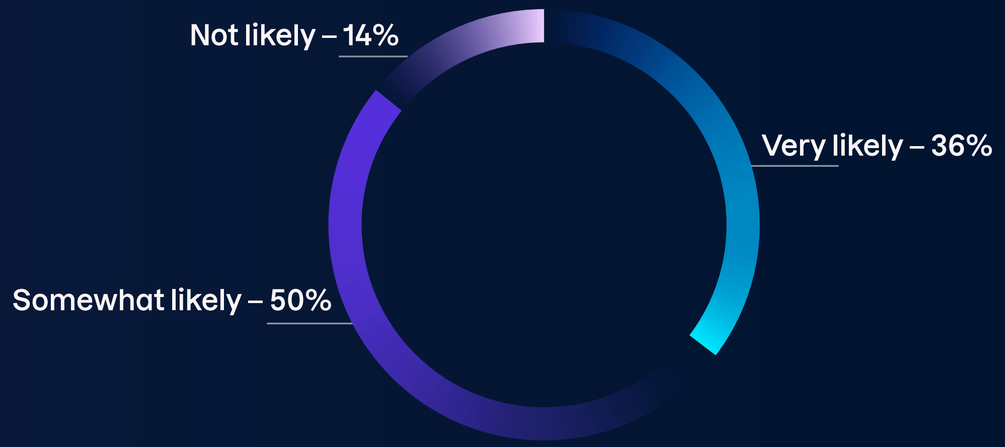
This presents a clear opportunity for carriers to close the trust–action gap by delivering built-in, easy-to-use protection that meets

Sources: : F-Secure US Consumer Market Survey, July 2025; F-Secure Consumer Market Survey, January 2025 (US data)

consumers where they are—not as IT experts, but as everyday people seeking relief from constant worry.

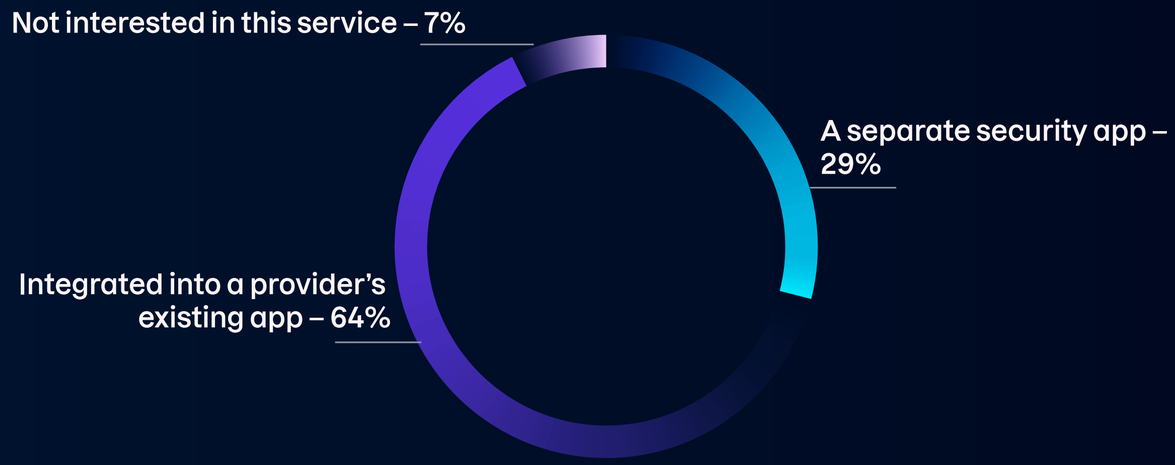
That peace of mind matters: **86% say they're likely to choose a carrier based on the security protections offered**, making cyber security not just a value-add, but a true differentiator.

Likelihood of choosing a carrier based on scam protection services



In addition, consumers aren't looking for another app to manage. **Nearly two-thirds (64%) prefer scam protection to be integrated into their provider's existing app**, reinforcing that convenience and seamless experience are key drivers of adoption.

Preferred way to access cyber security and scam protection



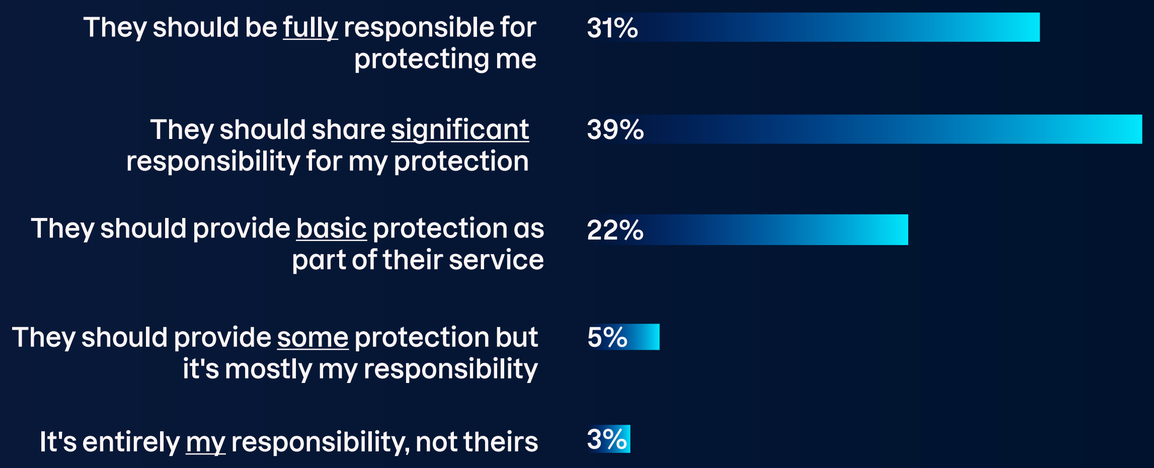
Source: F-Secure US Consumer Market Survey, July 2025

Scams Aren't Just a Consumer Burden

US consumers aren't just worried about scams, they expect help. In fact, **75% say they expect their internet, phone, or cable provider to keep them safe from digital crime.**

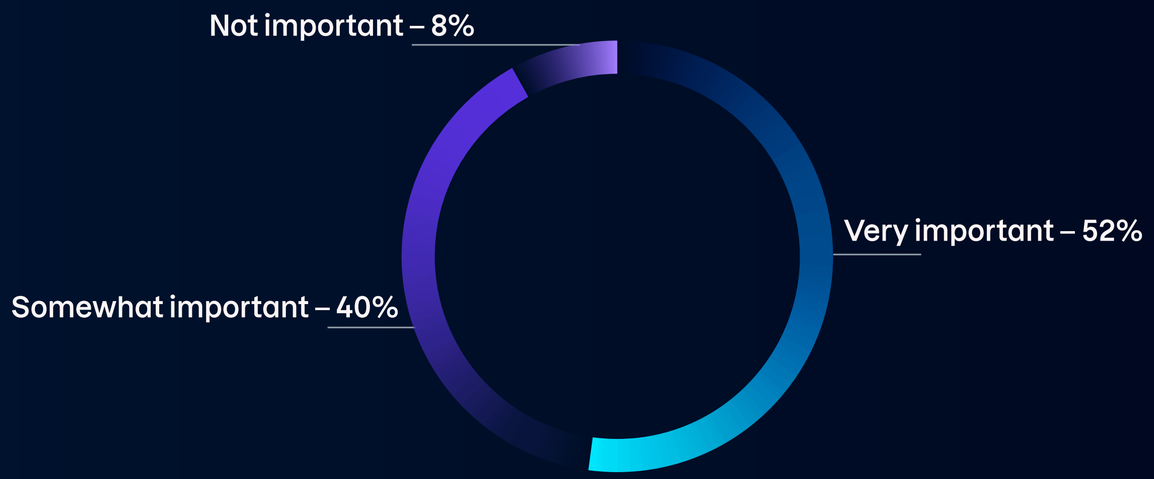
This reflects an overwhelming belief that digital safety isn't just a personal task. Only 8% of consumers think it's mostly or entirely up to them to protect themselves from scams and cyber threats, while **70% say their provider should be fully or significantly responsible.**

Perceived responsibility of carriers in digital scam and cyber threat protection



It's clear that cyber security is no longer seen as a do-it-yourself effort. It's now a service expectation. So it's no surprise that a substantial **92% of consumers consider it important for their provider to offer scam and cyber protection services**.

Importance of cyber security and scam protection from carriers



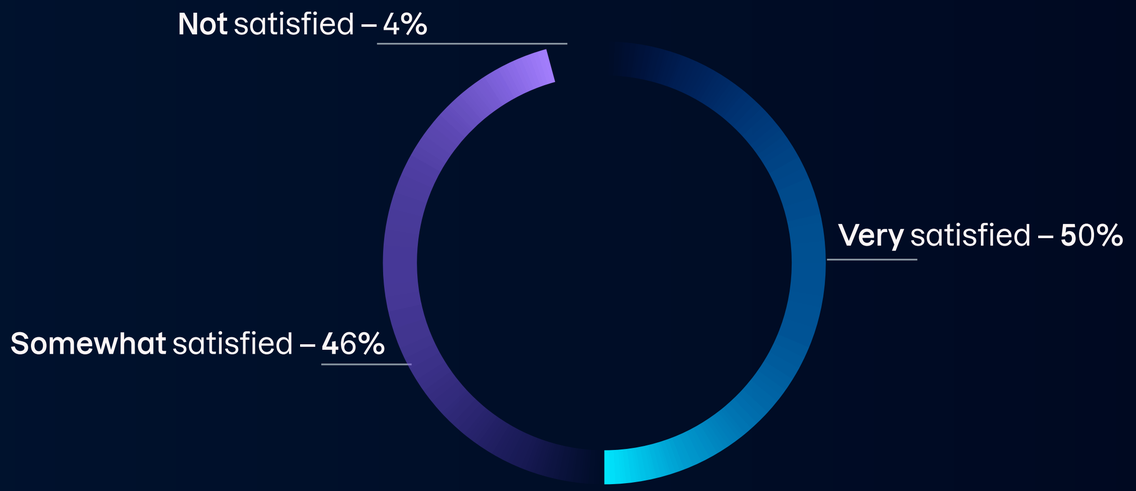
Source: F-Secure US Consumer Market Survey, July 2025

Untapped Marketing Opportunities

While demand for scam protection is high, **60% of consumers are unaware of any such services** offered by their provider. Yet among the 40% who are aware, **96% report being satisfied**—highlighting a marketing and communication gap, not a product one.

Are you aware of any scam or cyber security services offered by your current carrier?

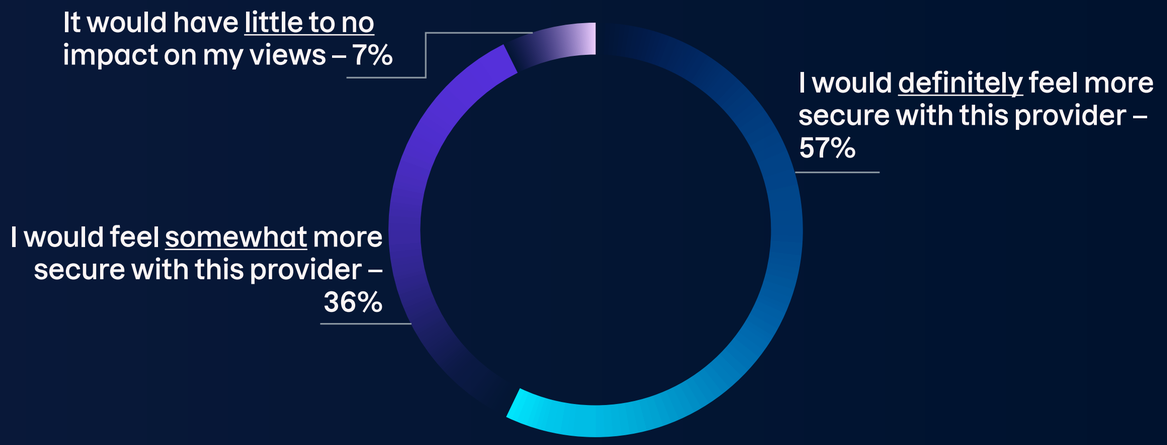
If you are aware, how satisfied are you with their scam or cyber security services?



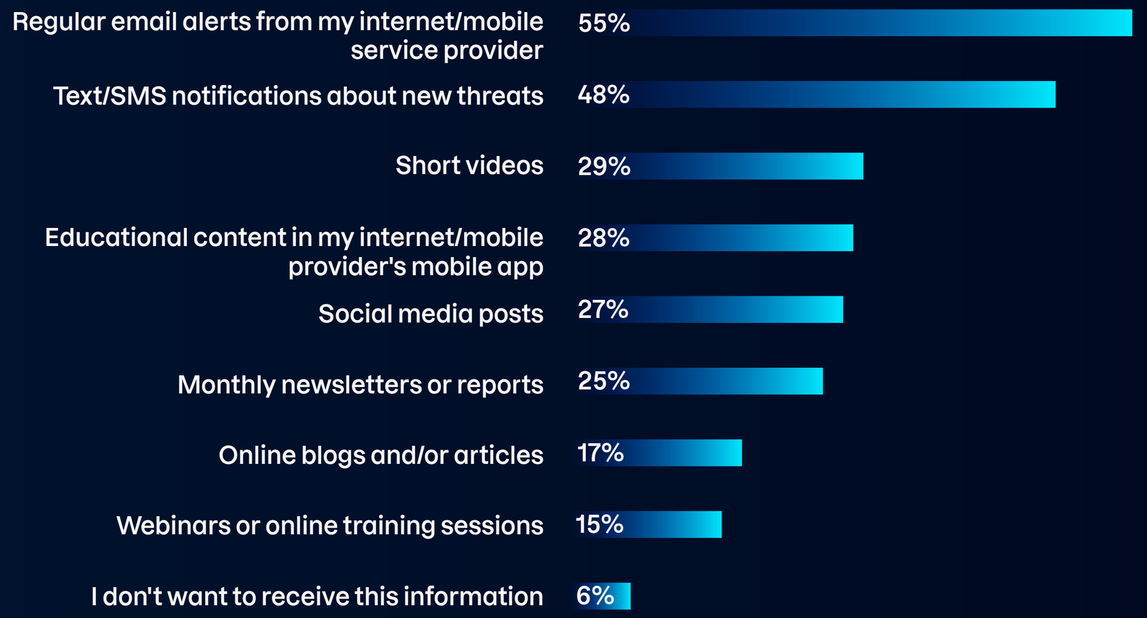
This represents a strong opportunity: **93% of Americans say they'd feel more secure with a provider that offers education about emerging scams**, while 90% are interested in receiving ongoing information about cyber threats. For marketing and communications teams, this is a pathway to transform security into a loyalty-driving value proposition.

Source: F-Secure US Consumer Market Survey, July 2025

How would your opinion of your carrier change if they offered education about emerging digital scams and cyber threats?



Preferred channels for scam and cyber threat education



But consumers aren't looking for occasional updates. **More than half (55%) want regular emails from their carrier about scams**, while 48% want SMS notifications about new threats, and more than 1 in 4 would like to see educational content in their provider's app. Only **6% aren't interested**—a clear sign that demand is strong and disengagement is rare.

Source: F-Secure US Consumer Market Survey, July 2025

Looking Ahead: Strategic Takeaways for Carriers

- US consumer survey results confirm that cyber security can no longer be treated as an optional upsell. Americans need it to be a core part of their service bundle.
- Providers who communicate clearly about scams, educate consistently on cyber threats, and protect their customers proactively will win on loyalty.
- Scam protection has evolved from a defensive feature into a growth engine. Carriers that lead in cyber security will redefine how digital value is delivered.

THE AI SCAM BOOM:

4 Ways Scammers Are Using AI in 2025

This year, AI is fueling a new wave of scams—helping threat actors scale faster and appear more convincing. This chapter breaks down how they're putting AI to work and explores the human cost of these increasingly sophisticated attacks.

Computer science PhD specializing in tracking threat actors and illicit finance.

Author of two books and 40+ peer-reviewed articles, with Best Paper Awards in data science and cyber security.

Cyber threat expert featured in major media iNew York Times and PBS-Frontline.

Dr Megan Squire
Threat Intelligence Researcher
F-Secure

How Scammers Are Using AI in 2025

Our comprehensive analysis of documented AI-driven scams in 2025 reveals four distinct categories of AI application in fraudulent activities:

1. **Target Selection** – AI is used to identify and profile potential victims.
2. **Infrastructure Development** – AI builds the digital tools needed for attacks.
3. **Content Generation** – AI improves the personalization and credibility of scam bait.
4. **Victim Communication** – AI enables scammers to engage directly with targets.

We found that in **89% of our sample of AI-enhanced scams, AI was used for content generation**. The vast majority of these involved enhancing phishing emails or impersonating people using voice cloning and deepfake video technology.

Category	Percentage
AI-enabled Victim Targeting	
• Using AI to locate victims	**5.5%**
AI-enabled Content Generation	
• Using AI to generate scam bait	**13%**
• Using AI to improve the credibility of bait, including:	**76%**
◦ AI-generated text	
◦ AI-generated photos	
◦ AI-generated audio/voice cloning	
◦ AI-generated video/deepfake video	
AI-enabled Victim Contact	
• Using AI to contact and engage with victims	**5.5%**

Note: Our sample was derived from news media reports, industry analysis, and other external and internal intelligence sources

Making Scam Bait More Convincing

In most cases we documented, scammers used AI tools to enhance the customization and credibility of the bait used to deceive victims. Voice cloning, for example, requires only a brief audio sample to build a replica of someone's voice. This enables scammers to deliver emotionally charged messages that appear to come from relatives in crisis.

These scams—often called "family emergency" or "grandparent" scams—once relied on muffled or garbled messages to impersonate a loved one in distress, claiming to be kidnapped or in urgent need of bail money.

Hear a voice cloning scam in action

Now, with just a few seconds of audio, AI can generate longer, highly convincing messages in the target's own voice. Victims consistently report that the recordings sound indistinguishable from their relatives or friends.

Deepfake Videos and Fake Endorsements

AI video generation tools are also being used to fabricate celebrity endorsements—promoting questionable products and fake investment schemes.

Social media platforms are flooded with deepfakes purporting to be public figures like Elon Musk, Al Roker, Jamie Lee Curtis, Keanu Reeves, and many others. In July, The Hollywood Reporter detailed how several frequently impersonated celebrities have turned to AI detection firms to find and remove fake content featuring their likeness.

Policy Responses to Crime Using Deepfakes

The marked increase in deepfakes used for deceptive, inauthentic content has prompted two new pieces of legislation in the US:

- **The TAKE IT DOWN Act** – Passed in Congress with overwhelming bipartisan support, criminalizing non-consensual intimate deepfakes.
- **The DEFIANCE Act** – Advanced in Congress and could be passed soon, creating a civil right to sue over this type of deepfake forgery.

While these laws address specific types of harm, our analysis shows that victims of financial fraud still lack adequate protection against deepfakes used for impersonation and scams.

AI for Phone Calls and Messaging

While deepfakes and voice cloning are being actively exploited by scammers, we found limited evidence of threat actors using AI to initiate phone calls or send SMS messages directly. However, as AI-based chatbots and agents become more reliable, this type of automated contact is likely to become increasingly prevalent.

Building Victim Target Lists with AI

In some cases, AI is being used to analyze previously scraped social media data to identify potential victims and build more effective target lists.

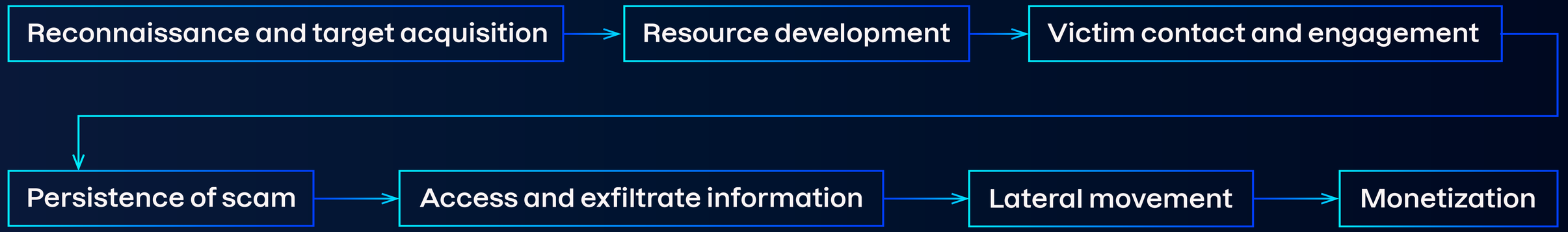
For example, The Financial Times reported that British insurance firm Beazley and ecommerce platform eBay have warned about scammers using AI to craft fraudulent emails by extracting and analyzing victim details from social media profiles.

A Moving Target for Scam Defenses

Scammers are expected to continue applying AI across the broader scam kill chain, making fraud detection and prevention a constantly shifting challenge for the scam protection industry. Our research highlights two emerging areas of concern:

- **Reconnaissance and target acquisition:** Using AI to analyze data and prioritize high-value targets.
- **Persistence of scam:** Deploying AI chatbots to handle the time-consuming psychological manipulation involved in long-term romance or investment scams.

How the F-Secure Scam Kill Chain Has Evolved



Since its launch earlier this year, the F-Secure Scam Kill Chain— our comprehensive knowledge base detailing both high-level scam tactics and specific techniques—has evolved to offer improved readability, accessibility, and a greater range of techniques.

Each scam tactic now includes a clearly defined goal describing what the scammer aims to achieve. For example, the goal of the 'reconnaissance and target acquisition' tactic is to identify potential victims based on factors including available data, personal interests, demographics, and overall suitability for the scam. This tactic is then broken down into techniques, such as manually building target profiles or using automated data collection.

The Human Cost of AI-enhanced Scams

There's no question that AI-powered scam tactics are evolving rapidly. And while detection tools and defensive measures are improving in parallel, consumers remain at risk—unwittingly caught in an arms race between scammers and those working to stop them.

As scams grow more frequent and convincing, many individuals will begin to doubt their own ability to tell real from fake—leading to a broad erosion of trust in digital spaces. Others will face scam fatigue: overwhelmed by the constant stream of threats, they become desensitized and more likely to overlook red flags.

Looking Ahead: The Role of Human Connection

- Research shows that one of the most effective ways to help people navigate the AI-enabled fraud landscape is to **emphasize genuine human connections**.
- Whether through peer education as a prevention mechanism, or by encouraging the verification of suspicious communications via trusted human channels, fostering personal connections creates a powerful circuit breaker in the fraud cycle.
- In an era where seeing is no longer believing, our most powerful tool against AI-enabled fraud may be the very thing machines can’t replicate.

Founder of GASA, a non-profit dedicated to protecting consumers worldwide from scams.

Speaker and advocate for scam awareness and knowledge sharing.

Educator with a focus on developing scam prevention strategies.

Jorij Abraham
Managing Director
Global Anti-Scam Alliance

THE SILENT TOLL OF SCAMS:

Breaking the Cycle of Shame and Inaction

Drawing on US and global insights from the Global Anti-Scam Alliance (GASA), this chapter explores the deeper human toll of scams—from victim shaming to silence driven by stigma—and why awareness alone isn't enough.

Virtual Crime Hits Harder Than Expected

Online scams don't just empty bank accounts—they damage trust, dignity, and personal wellbeing. In fact, growing research suggests that the emotional trauma caused by virtual crimes can actually exceed that of physical ones.

A study by the Dutch police found that victims of digital crime often report higher levels of peritraumatic stress than those affected by physical incidents, including burglary and even sexual assault. Because there's no physical interaction, people tend to underestimate the impact of online scams. The emotional damage, however, is real and lasting.

Blame's Role in Silencing Victims

One of the most damaging aspects of online scams isn't the scam itself—it's how society responds to victims. While those affected by physical crimes are often met with sympathy, **victims of online fraud are frequently dismissed, ridiculed, or shamed.**

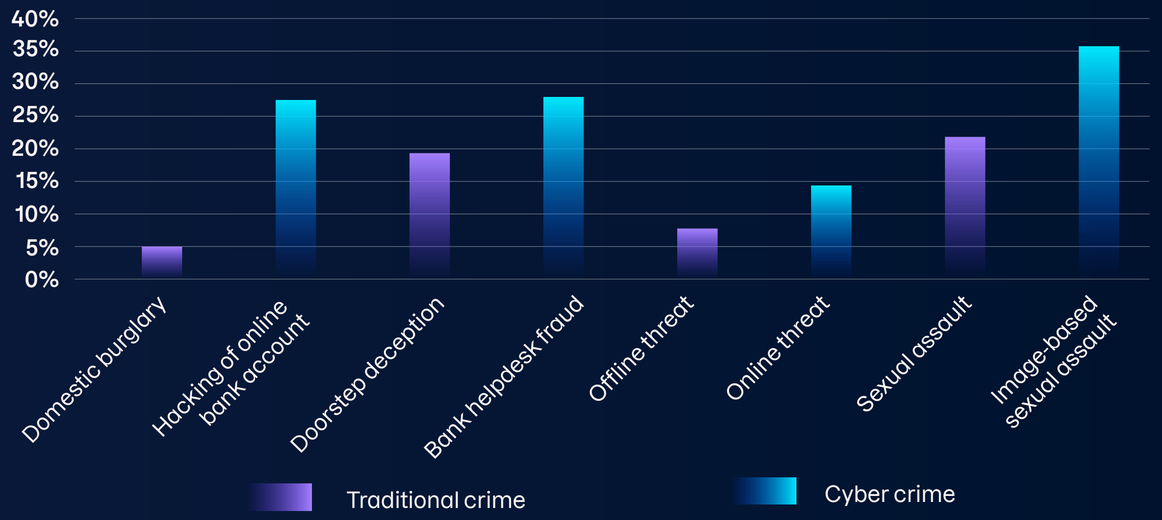
Instead of empathy, they're met with blame: "How could you be so stupid?" Public shaming is even common on professional platforms like LinkedIn, where one user told a scam victim, "Even my 90-year-old mother wouldn't fall for that."

Peritraumatic stress levels: Traditional crime vs cyber crime

Source: The Impact, Needs and Reporting Experiences of Cyber Crime Victims, Jildau Borwell, 2024

This culture of judgment deepens the emotional toll, fueling shame and silence. And data supports this trend: just 5% of burglary victims experience victim blaming, compared to 27% of individuals whose online bank accounts have been hacked. The numbers are even more troubling when it comes to sexual crime, with 22% of sexual assault victims reporting blame, versus 36% of those subjected to image-based sexual abuse.

Victim blaming rates: Traditional crime vs cyber crime

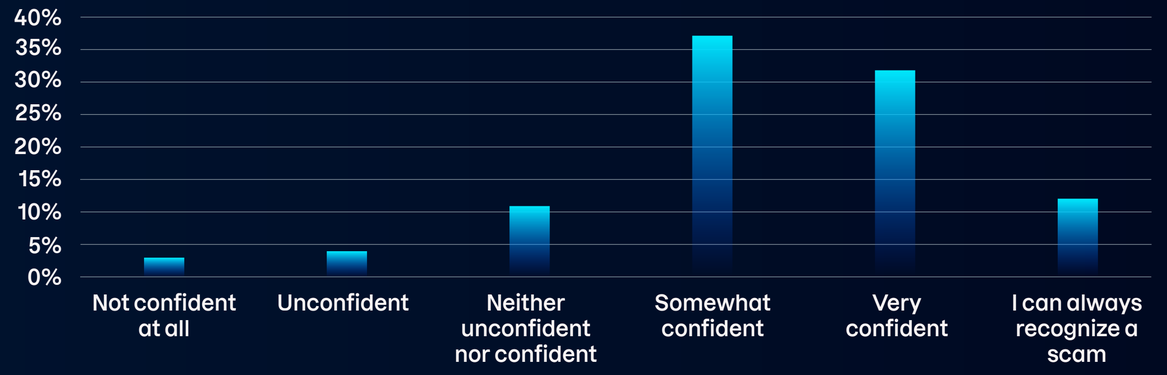


Overconfidence Fuels Victim Blaming

A key driver of victim blaming is overconfidence: the belief that "I'd never fall for that," and anyone who does must be naïve.

According to GASA's research, **81% of Americans feel confident in their ability to spot a scam**. But this confidence often collapses when deception hits, leading to shame often reinforced by the judgment they've seen or expressed themselves. This mindset doesn't just deepen the emotional impact—it also discourages victims from reporting.

Percentage of US respondents confident in their ability to spot scams



Sources: The Impact, Needs and Reporting Experiences of Cyber Crime Victims, Jildau Borwell, 2024; GASA State of Scams in the United States of America, 2025

The Silent Epidemic of Underreporting

2.6% of scam victims report the crime

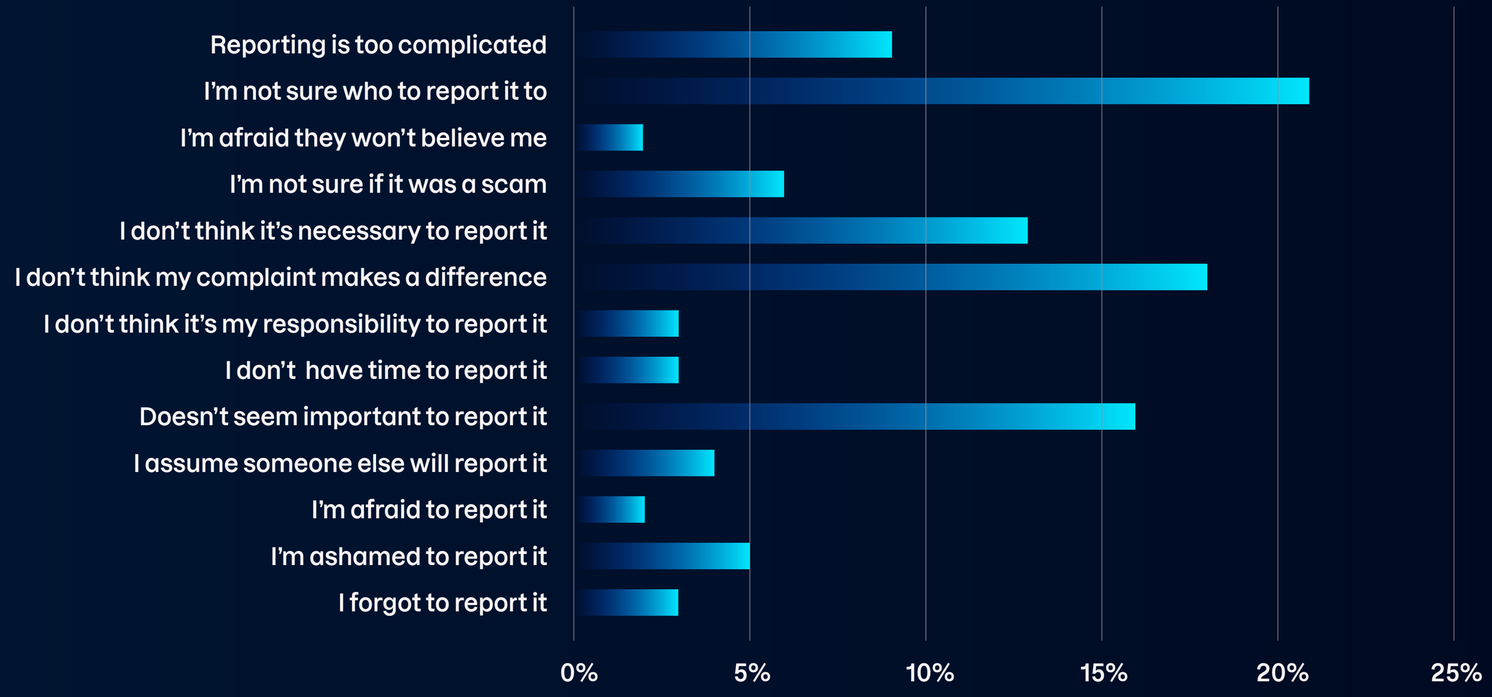
In the US, only around 2.6% of scams are reported to the authorities. Why don't more victims come forward? Most simply don't believe reporting will make a difference. And too often, they're right.

In most cases, victims are told the amount lost is too small, the scammer is overseas, and the chance of recovering the money is minimal. It's a response that, while honest, does little to encourage future reporting.

A Fragmented Reporting System

Even when victims are willing to report, the process is so fragmented and complex that it becomes a barrier. A fifth (21%) don't know where to turn, and when they do try, dense forms and unclear processes often shut them down. Reflecting this frustration, 18% of US consumers believe that reporting a scam wouldn't make a difference.

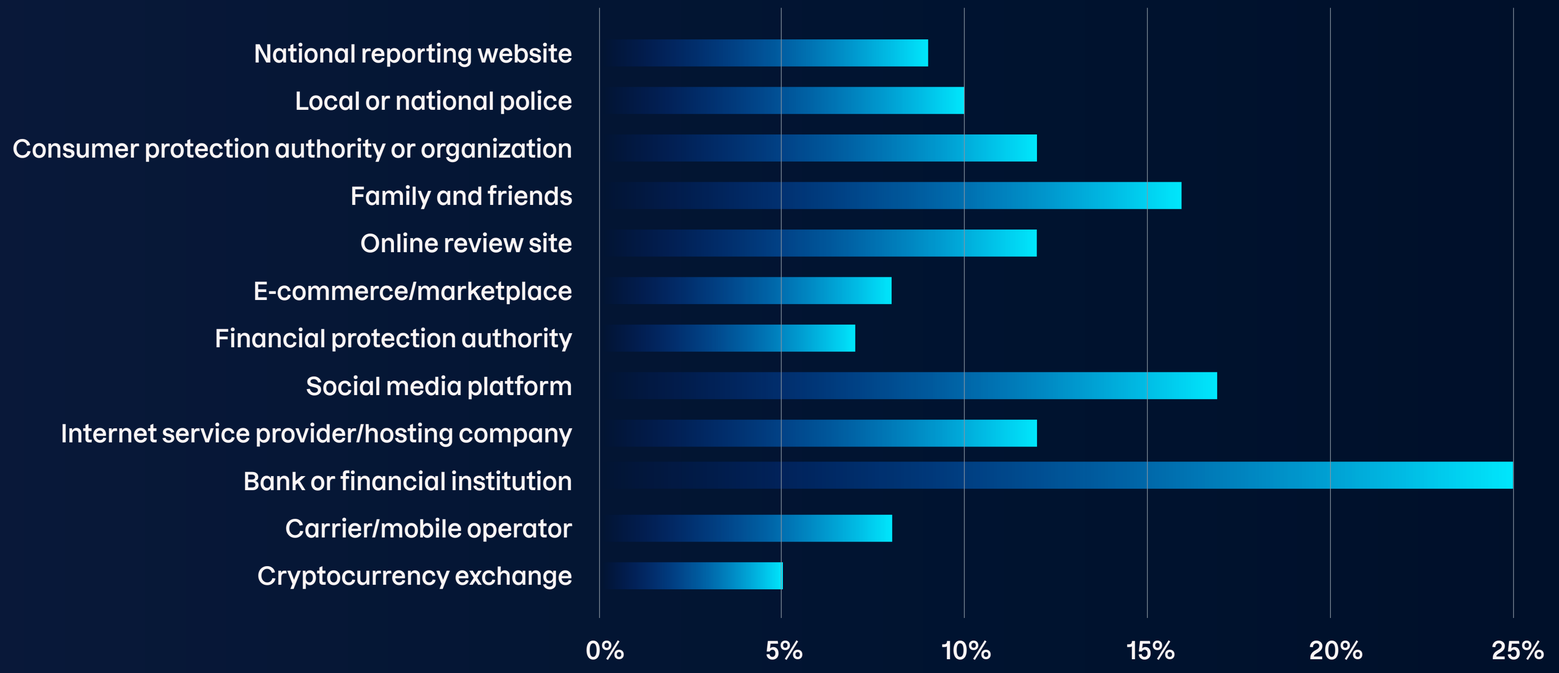
Reasons US respondents might choose not to report a scam



Sources: GASA analysis of multiple data sources, 2024 ; GASA State of Scams in the United States of America, 2025

GASA's findings highlight the extent of reporting confusion: 25% of Americans say they would turn to their bank, 17% to a social media platform, and 16% to family and friends, while just 10% would report a scam to the police. With such a scattered system, victims are left uncertain—and many scams go unrecorded.

Who US respondents would report a scam to if deceived



Local law enforcement is under-resourced. Despite scams being common, officers often focus on traditional crime and lack the tools to investigate cyber fraud. Directing victims to police departments that aren't equipped to respond is a broken model. What's needed is a single reporting channel known to authorities in each country, such as the UK's Action Fraud.

Why Awareness Campaigns Are Falling Short

Governments and organizations spend millions on scam awareness campaigns, yet their impact is often short-lived. Humorous ads may grab attention, but the message fades quickly. Many still rely on outdated advice, like checking for spelling errors or looking for secure website connections. But today's scammers use AI to craft flawless messag-es and easily obtain SSL certificates, making these tips largely ineffective.

Source: GASA State of Scams in the United States of America, 2025

To address this, GASA is advocating for long-term, systemic education that starts in early childhood and continues throughout every stage of life. Children playing Roblox already face scammers targeting their parents' payment details. Students encounter fake loan offers. Pensioners are lured by fraudulent investment schemes. Every demographic is targeted year-round, so education must be continuous and relevant.

Education Alone Isn't Enough

While education is essential, it can't be the only line of defense. Consumers can't be expected to remain alert 24/7. That's why automated tools—such as those offered by F-Secure—are critical, especially when scams are too advanced for human detection.

This also is where service providers like banks, telcos, and insurers have a unique opportunity. With regular customer engagement, they can integrate scam protection directly into their services. Instead of one-off campaigns, they can deliver short, recurring micro-trainings that steadily build awareness and reduce risk.

Looking Ahead: It Takes a Network to Stop Scams

- Education and awareness are not silver bullets. Combating scams requires a coordinated effort, with cyber security experts, governments, law enforcement, educators, and service providers all working together.
- Scammers operate around the clock, which is why real progress depends not just on tools and policies, but also on moving beyond victim blaming.
- If your organization interacts with customers online, you're on the frontline of scam prevention. Don't just warn—empower. Don't just inform—protect. Now is the time to embrace your role and invest in smarter tools, ongoing education, and integrated solutions that truly make a difference.

Computer science PhD specializing in tracking threat actors and illicit finance.

Author of two books and 40+ peer-reviewed articles, with Best Paper Awards in data science and cyber security.

Cyber threat expert featured in major media including the New York Times and PBS-Frontline.

Dr Megan Squire
Threat Intelligence Researcher
F-Secure

2025 FINANCIAL THREATS:

Top 3 Banking Scams Targeting Americans

Banking scams continue to rank among the most significant digital threats in the United States. This chapter outlines the top three methods targeting consumers and the key factors that drive their effectiveness.

Fraud Is Escalating Year Over Year

In 2024, fraud cost American consumers $12.5 billion, as cyber criminals exploited weaknesses in US consumer protection laws and outdated banking infrastructure.

To understand how these attacks work, the following analysis examines the scam kill chain of the three most prevalent banking scams targeting Americans—focusing on the psychological manipulation and systemic vulnerabilities that enable their success.

1. Bank Impersonation Scams

This sophisticated scam typically begins with a fake fraud alert SMS: "Bank of America: Suspicious transaction of $2,500. Reply NO if this wasn't you."

When victims respond, they receive a call from someone claiming to be from their bank's fraud department, often with a spoofed caller ID matching the bank's real number.

The scammer creates urgency, warning that the victim's account is being drained. They instruct the victim to open their banking app and "reverse" the fraudulent transaction by sending money to a "secure holding account" via Zelle or Bitcoin payments. In reality, the funds go directly to the scammer.

Why It Works

- **Irreversible payments:** Wire transfers and cryptocurrency payments settle instantly and can't be reversed. Once sent, the money is gone.
- **Limited reimbursement:** Banks often deny refunds for these scams, citing that the payment was "authorized," even though the victim was deceived. A 2024 Senate report found that major banks reimbursed victims of authorized payment scams just 38% of the time.
- **Exploiting trust in Zelle:** Scammers target Zelle because it combines the speed of modern payment apps with the perceived safety of being integrated into banking apps—yet lacks the dispute protections of credit card transactions.

2. Romance and Investment Scams

Romance scams remain among the most financially devastating frauds, often draining victims' life savings. These scams typically start on dating apps or social media, where scammers build emotional connections over weeks or months.

Once trust is established, a financial angle emerges—ranging from a medical emergency to a cryptocurrency investment. The "pig butchering" variant is especially cruel: scam-

mers use fake apps to show fabricated investment returns, encouraging victims to invest more and more money.

Why It Works

- **Emotional manipulation:** These scams are psychologically sophisticated. Scammers create convincing personas, share fake photos, and engage in long-term conversations that build genuine emotional trust with victims.
- **Gradual escalation:** Financial requests begin small and grow steadily, often tied to promises of real-life meetings and shared future plans.
- **Irrecoverable losses:** Funds sent via wire transfer, gift cards, or cryptocurrency are virtually untraceable. Victims rarely recover their money—and the emotional toll, coupled with feelings of shame, often prevents them from reporting the crime or seeking support.

3. Check Overpayment Scams

Despite being outdated in many countries, paper checks remain widely used in the US, creating opportunities for fraud. These scams exploit the confusing delay between funds appearing in an account and the actual clearing of a check.

Scams typically begin with fake job offers, housing rentals, or online marketplace listings. The scammer sends a check for more than the agreed amount—say, $1,500 for a $500 item—and then claims it was a mistake, asking the victim to return the difference via Zelle, wire transfer, or gift cards.

Why It Works

- **Clearing confusion:** Banks make deposited funds available within days, but it can take weeks to fully verify a check. Victims see the money in their account, assume the check has cleared, and send the “overpayment” to the scammer.
- **Delayed reversal:** When the check is ultimately flagged as fraudulent, the bank withdraws the full amount—leaving the victim out of pocket.
- **Systemic gaps:** In the US, checks are still common for rent payments and even government disbursements. The delay in fraud detection makes recovery nearly impossible, and banks aren’t legally required to reimburse victims who sent money voluntarily, even if deceived.

Looking Ahead: Breaking the Scam Cycle

Banking scams continue to thrive by exploiting both technical vulnerabilities in the US banking system and human psychology.

- Until regulation and infrastructure catch up with modern scam tactics, prevention will depend on consumer vigilance and proactive intervention from service providers.
- Consumers should never send money to “reverse” fraud and should always verify unexpected financial requests through official channels.
- Legitimate banks and employers will never ask for repayment via Zelle, cryptocurrency, or gift cards.

THE FUTURE OF SCAMS:

What the Next 5 Years Could Bring

Scams are adapting fast—and the next wave could be more personal than ever. This chapter explores what might come next, from AI agents and all-in identity theft to moments of trust that open the door to deception.

Sarogini Muniyandi
Head of Scam Research &
Defense Engineering
F-Secure

Trust Triggers: Scammers Are Hacking Human Behavior

Over the past decade, scams have evolved far beyond suspicious links and malicious files. As devices and security systems become more resilient, scammers have shifted their focus—not to vulnerabilities in code, but to vulnerabilities in people. Today, trust, emotion, and behavioral patterns are the new attack surface.

Modern scams increasingly target 'money moments': key interactions when people move or manage money online, like paying bills, transferring funds, applying for loans, or hiring services through social media. These aren't random attacks; they're engineered to strike when emotional pressure is high, and attention is low.

AI now enables scammers to hijack conversations, mimic voices, and craft messages that feel personal and urgent. A fake vendor demanding a deposit. A deepfake voice message from a loved one asking for a favor. The pressure to act fast creates the perfect opening for manipulation.

As cyber security grows stronger, the human layer is becoming—and will remain—the primary attack surface. Scam protection must evolve to recognize behavioral risks, detect emotional manipulation, and intervene before a costly decision is made.

> **In a world where scams begin with trust, the question is no longer what users click, but why, and when, they click it.**

Joel Latto
Threat Advisor
F-Secure

All-In Identity Theft: The Next Frontier for Scammers?

Identity theft isn't new, but it's always evolving. As outlined in the F-Secure Scam Kill Chain, most scams begin with basic personal details: a name, address, phone number, or email address. While not enough to commit fraud directly, this data enables phishing attacks, impersonation, or account recovery abuse.

Next, I expect to see the emergence of something deeper: all-in identity theft. Instead of stopping at surface-level details, scammers could assemble full digital personas.

It begins with common personal data, then adds stronger identifiers like passports or Social Security numbers. Public social media posts, breached health records, and even audio or video clips to create deepfakes can round out the profile. In some cases, scammers may collect biometric data like fingerprints to bypass advanced security.

This kind of comprehensive identity theft isn't common—yet. Most scams succeed with less effort. But as with phishing kits and malware-as-a-service, the barrier to entry is dropping. Semi-automated tools may soon build 'identity packages' from multiple sources. And biometric data could be key to that shift—you can only change your fingerprint scan nine times, then you're out of options.

> **Once all-in identity theft becomes profitable at scale, scammers won't need much incentive to take it further.**

Laura Kankaala
Head of Threat Intelligence
F-Secure

AI Agents: A Future Tool for Scammers—But Not Yet

AI agents are designed to do more than answer questions—they can act on our behalf. That sounds promising for users, but also for scammers.

In theory, scammers could harness AI agents to automate spam campaigns, carry out convincing conversations with victims, or even commit financial theft. They could also use them to validate stolen data, like login credentials or credit card details, without the manual effort usually required.

In the consumer cyber security space, there's plenty of speculation about what AI agents could do. But here's the reality: scammers aren't using them today.

Why not? For one, scams already rely on simpler forms of automation that are cheaper and easier to deploy. AI agents, by contrast, remain costly to operate and too niche for widespread use in the cyber crime ecosystem. While generative AI is already helping scammers create convincing content or translate phishing messages, AI agents aren't yet practical.

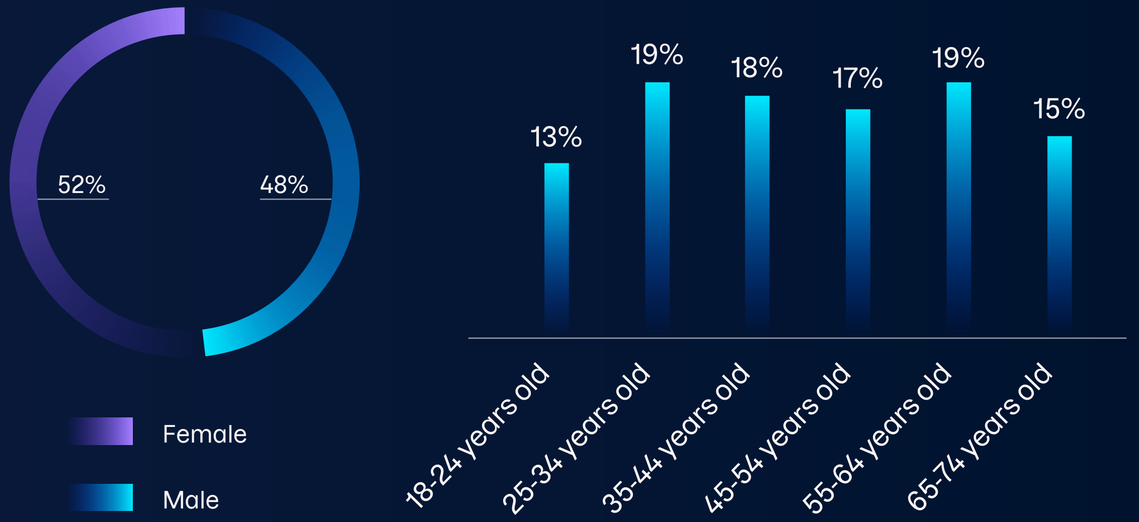
> **It will take another breakthrough—one that makes AI agents significantly more accessible and affordable—before scammers are likely to adopt them at scale. Whether that tipping point arrives in the next few years remains to be seen.**

Sources and Methodologies

2025 US Scam Landscape: How Overconfidence Leaves Consumers Vulnerable

US consumer data was gathered via an online F-Secure Consumer Market Survey conducted in January 2025. While self-reported data reflects individual perception, results were validated through sample balancing to ensure demographic consistency.

The survey captured responses from 1,000 consumers across the United States. Respondents ranged in age from 18 to 74, allowing for generational comparisons in digital habits, and reflected a 52/48 gender split consistent with the US population.

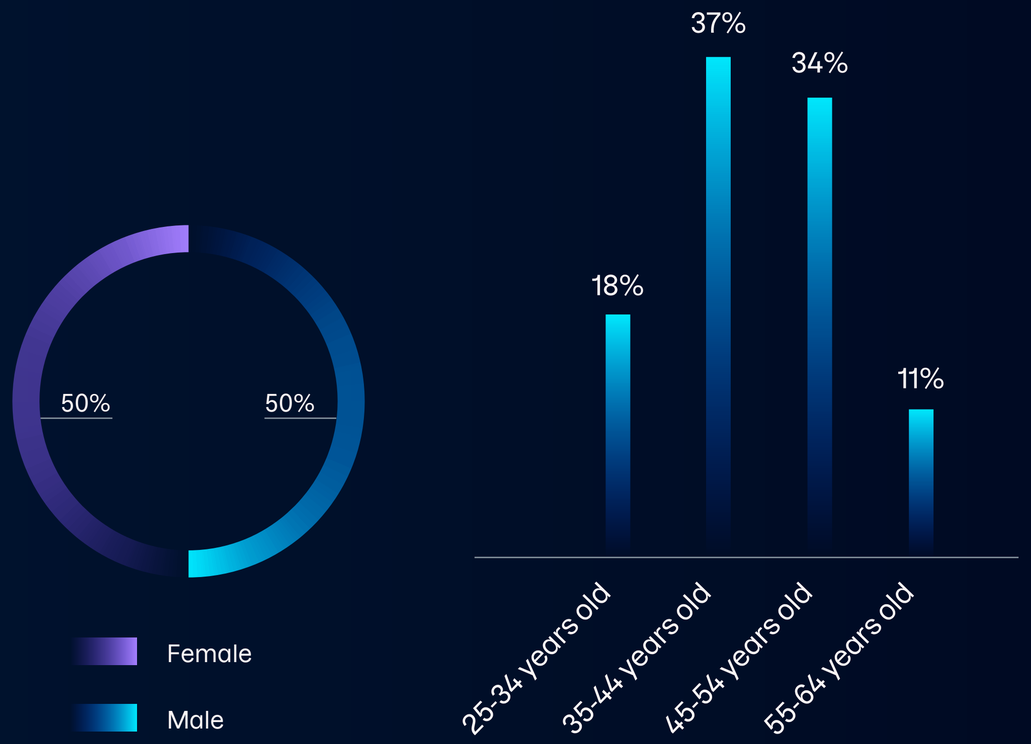


- FTC Consumer Protection Data Spotlight, 2025

Awareness Gap: 75% Expect Security—Yet 60% Don't Know Their Carrier Offers It

Consumer data was gathered via an online F-Secure US Consumer Market Survey conducted in July 2025. While self-reported data reflects individual perception, results were validated through sample balancing to ensure demographic consistency.

The survey captured responses from 1,022 consumers across 48 US states. Respondents ranged in age from 25 to 65 and included a 50/50 gender split to reflect real-world diversity.



The AI Scam Boom: 4 Ways Criminals Are Using Artificial Intelligence in 2025

- AI application in fraudulent activities sample derived from news media reports, industry analysis, and other external and internal intelligence sources, 2025
- People: 'Woman Conned Out of $15K After AI Cloned Her Daughter's Voice in Terrifying Scam', 2025
- KWCH: 'Wichita mother nearly duped by AI voice cloning scam', 2025

- Hollywood Reporter: ‘This Is Not Keanu: Inside the Billion-Dollar Celebrity Impersonation Bitcoin Scam’, 2025
- Axios: ‘Scoop: Momentum builds for AI deepfake bills’, 2025
- F-Secure: ‘US Congress Builds a Deepfake Defense, But Forgets Some Victims’, 2025
- Financial Times: ‘AI-generated phishing scams target corporate executives’, 2025
- F-Secure Scam Kill Chain, 2025

The Silent Toll of Scams: Breaking the Cycle of Shame and Inaction

- GASA State of Scams in the United States of America, 2025
- GASA analysis of multiple data sources, 2024
- The Impact, Needs and Reporting Experiences of Cyber Crime Victims, Jildau Borwell, GASA Meetup, 2024

2025 Financial Threats: Top 3 Banking Scams Targeting Americans

- F-Secure Scam Kill Chain, 2025
- Federal Trade Commission: ‘New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024’, 2025
- United States Senate: ‘A Fast and Easy Way to Lose Money: Insufficient Consumer Protection on the Zelle Network’, 2024

illuminate

Shaping the Future of Digital Confidence

At F-Secure, research is not simply about tracking today's threats—it's about anticipating tomorrow's digital challenges. Through **Illuminate**, our multidisciplinary research initiative, we combine technical innovation with social science to redefine how cyber security enables digital confidence.

- We use **foresight and systems thinking** to navigate uncertainty and anticipate changes—from the degrading information environment to evolving trust dynamics.
- By combining **behavioral science and technical expertise**, our approach sees consumers as whole individuals, designing protection that aligns with real behaviors and psychology.
- Our research moves beyond a purely defensive approach to **actively creating positive online experiences**. We explore trust in AI and reimagine cyber security as a foundation for digital confidence and resilience.

About F-Secure

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 200+ partners.

For more than 35 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For the latest news and updates visit f-secure.com or follow us on our social channels.

F-Secure