# Scam Intelligence & Impacts Report 2025

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

F-Secure®

# Executive Summary

The second annual F-Secure 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.

Global data and behavioral insights reveal a paradox: most people trust their ability to spot scams—yet nearly half 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:** 69% of people believe they can spot a scam—but 43% of them still fell victim in the past year.
- **Victimization is Rising:** Scam rates doubled in the USA from 2024 to 2025. In Vietnam, 90% of respondents were scammed last year.
- **Young Adults Are Most Exposed:** Individuals aged 18–34 face more than double the scam risk of adults aged 65–74.
- **Underreporting is Widespread:** Only 7% of scams are reported globally, largely due to victim blaming and feelings of shame.
- **Consumers Want Protection:** 50% are willing to pay for scam protection—especially younger adults who expect it from service providers.

## 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.

# Contents

2025 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 F-Secure Consumer Market Survey data, **69% of people believe they know how to spot a scam**. Yet **43% 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 people believe they know how to recognize an online scam**

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

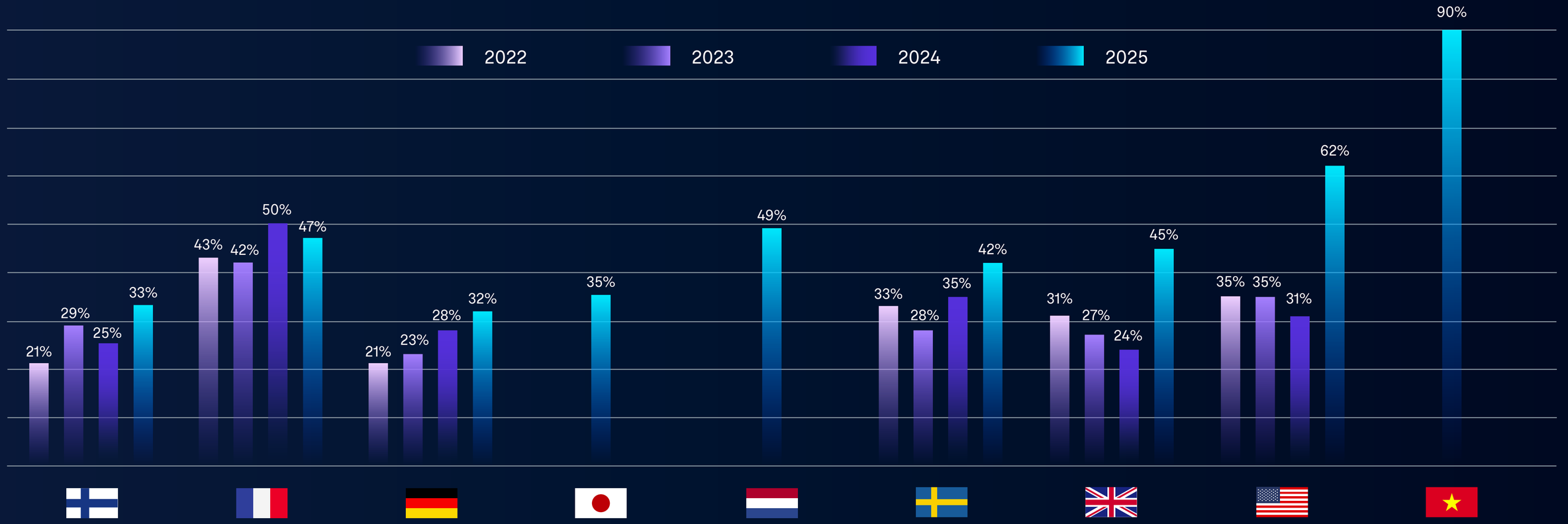
## Scam Victimization Is Rising Drastically

Scammers are quick to exploit these cognitive blind spots, using tactics like urgency and authority to override rational thinking. Our research shows that, compared to the previous year, scam victimization is accelerating across nearly all surveyed markets:

- USA: 31% → **62%**
- UK: 24% → **45%**
- Finland: 25% → **33%**
- Sweden: 35% → **42%**
- Germany: 28% → **32%**

Source: F-Secure Consumer Market Survey, January 2025

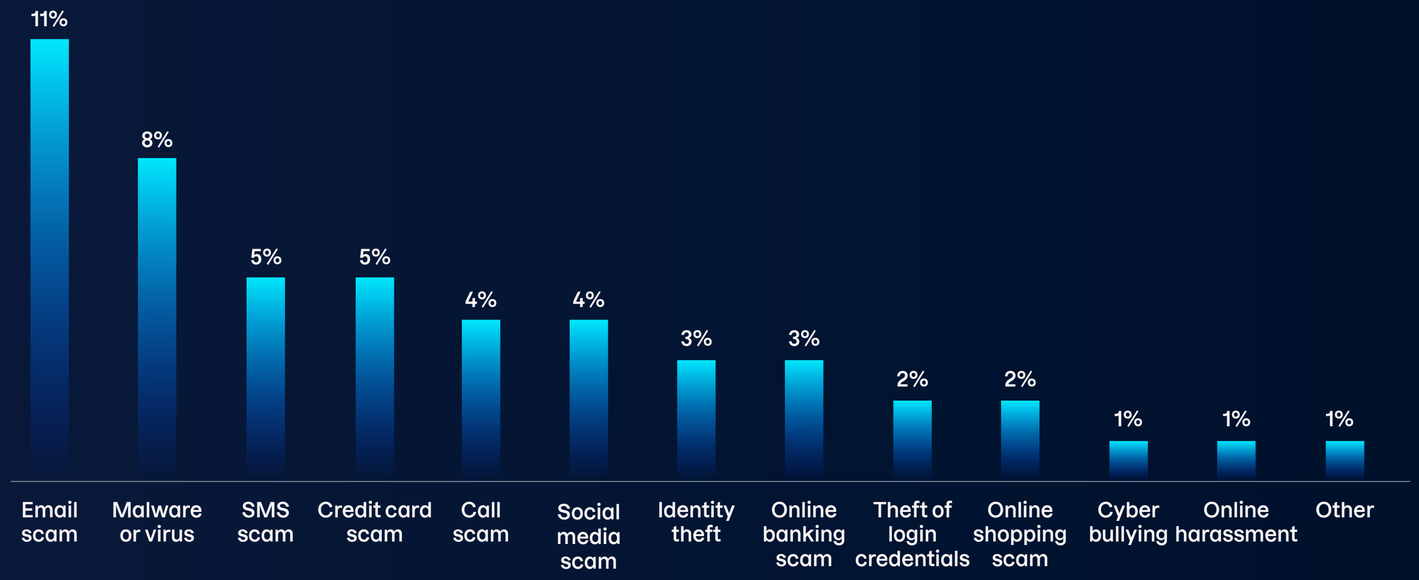
# Percentage of respondents who fell victim to cyber crime by country (2022–2025)




Vietnam, newly included in this year's survey, stands out with a staggering **90% of respondents reporting victimization** —the highest rate observed in any market.

Source: F-Secure Consumer Market Survey, January 2025

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




Overall, **48% of global 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 11%, followed by malware or virus attacks at 8%, and SMS scams and credit card scams at 5% each.

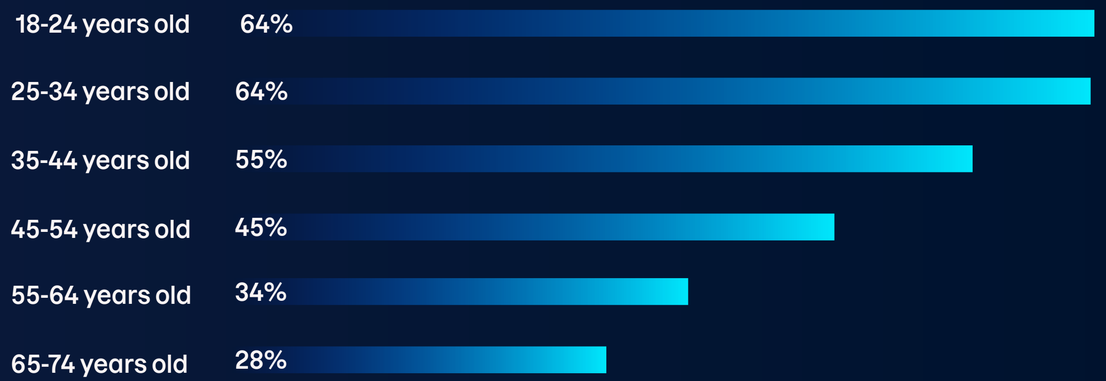
Smaller but still significant numbers experienced call scams, social media scams, online banking scams, and online shopping scams. This variety underscores how cyber criminals are diversifying their tactics to target consumers in multiple ways, across every digital touchpoint.

Source: F-Secure Consumer Market Survey, January 2025

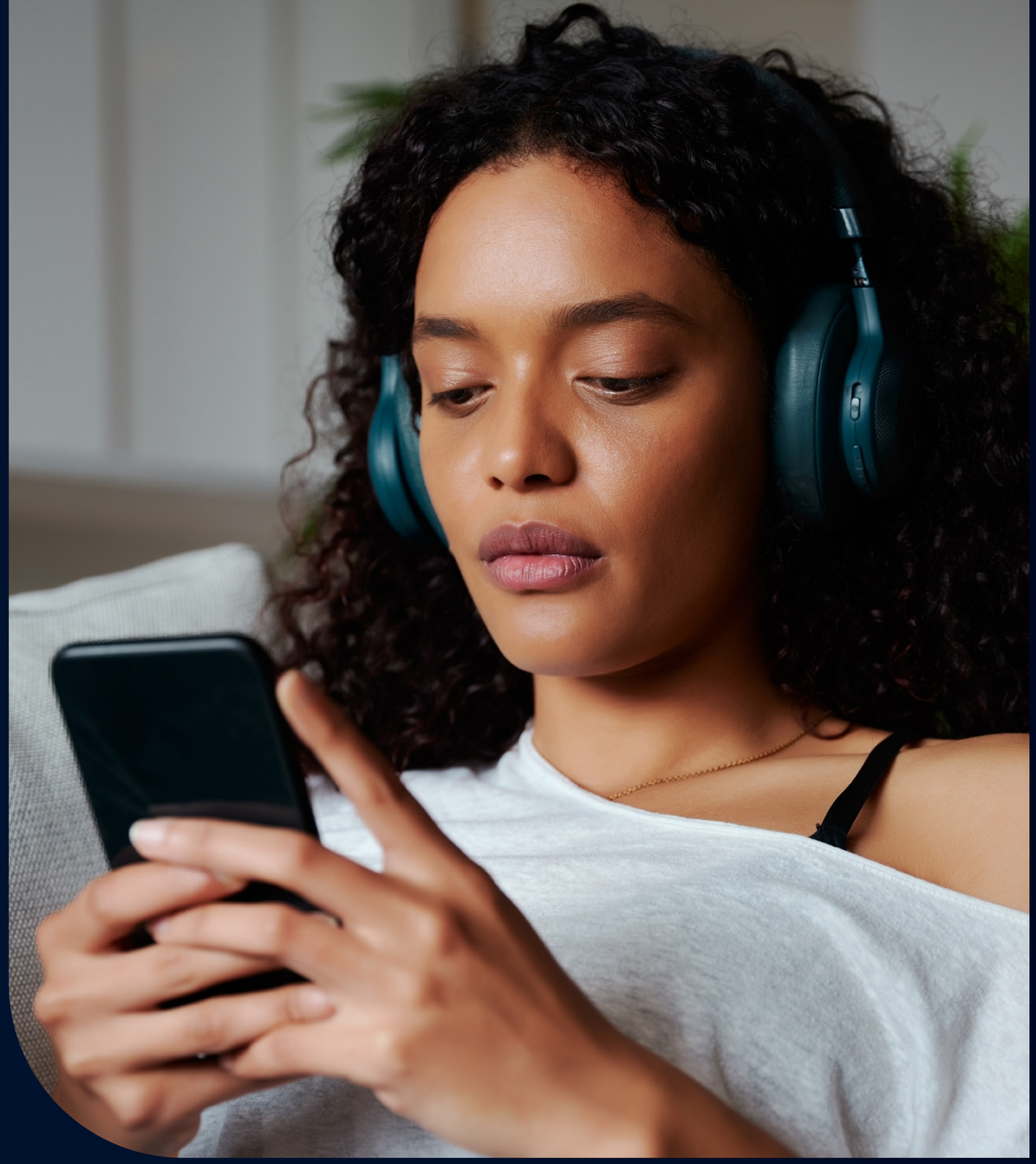
## Digital Natives Are Most at Risk

Younger demographics—the very group seen as most tech-savvy—face the highest exposure to scams. **Adults aged 18 to 34 are more than twice as likely to experience cyber crime (64%)** compared to those aged 65 to 74 (28%). 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



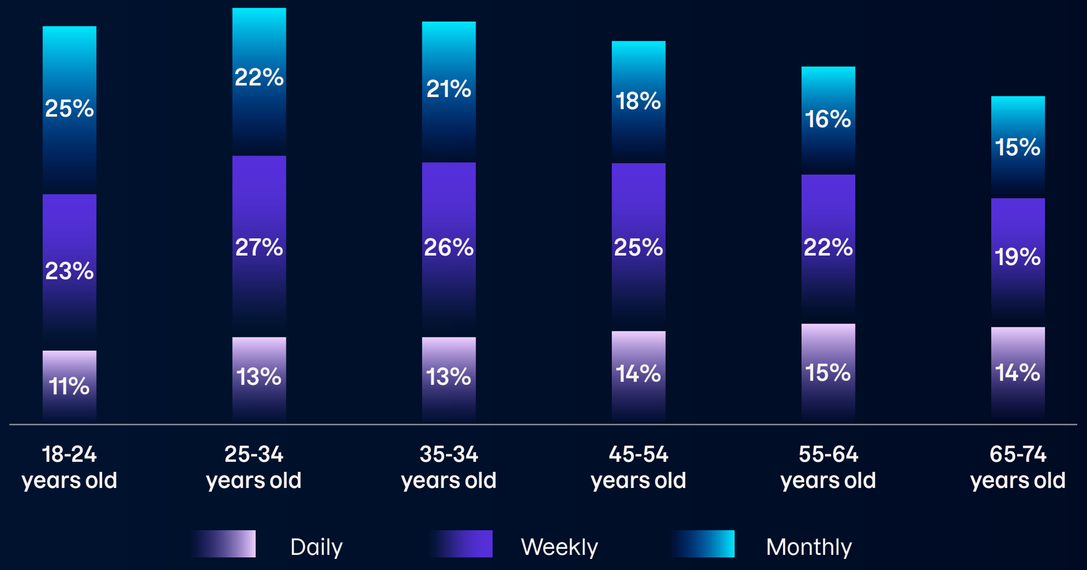

Source: F-Secure Consumer Market Survey, January 2025



While **56% of people overall encounter scam attempts at least monthly**, this rate rises to 59% for 18–24-year-olds, 62% for 25–34-year-olds, and 60% for 35–44-year-olds. In contrast, only 48% of those aged 65–74 report the same—highlighting a key truth: digital fluency does not equal cyber resilience.

Younger adults are more connected, more exposed, and often more confident than cautious. They're also more likely to encounter situations that make certain scams effective—for example, cost-of-living pressures can leave them more vulnerable to crypto scams and "get-rich-quick" schemes.

## Frequency of scam attempts by age group

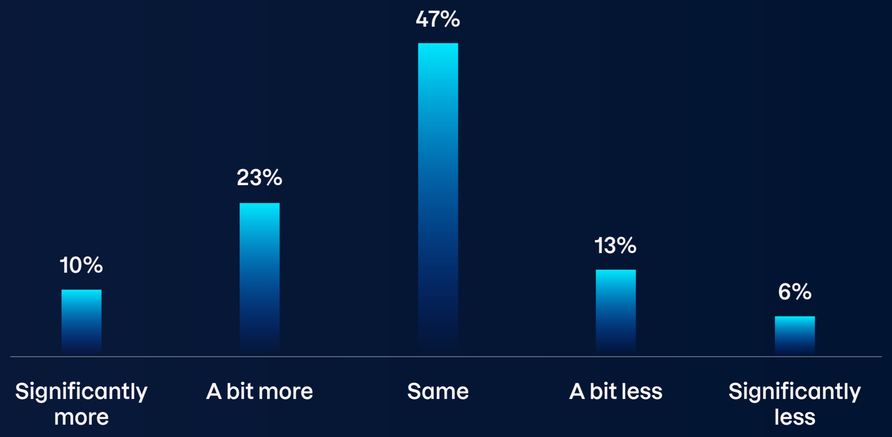



Source: F-Secure Consumer Market Survey, January 2025

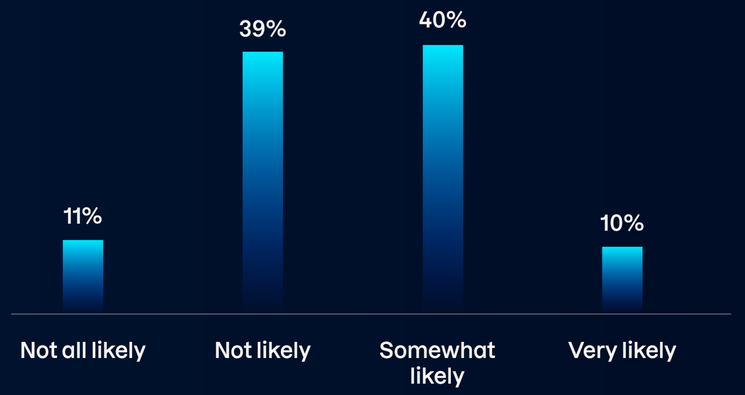
## Scams Are a Constant Threat

Scam attempt volumes have remained relatively stable since the previous survey year: 47% of respondents reported receiving about the same number, while 33% noticed an increase. Still, perceived risk is rising—**50% of consumers now believe they're likely to fall victim to scams or other cyber crime in the future.**

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



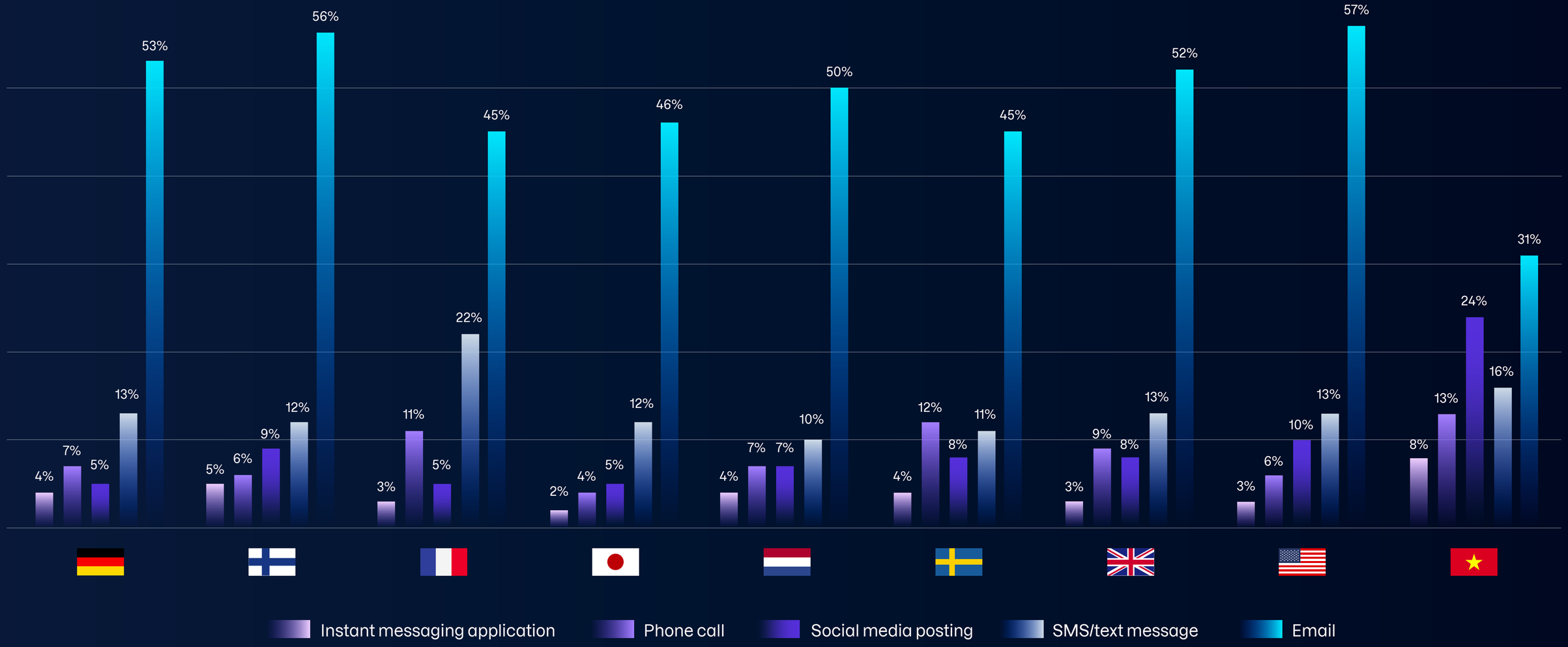

## Perceived likelihood of falling victim to scams or cyber crime in the future




Email is still the top delivery channel (48%), though its prominence varies. In mobile-first markets like Vietnam, it plays a smaller role (31%) compared to 57% in the USA or 56% in Finland. Despite this, many still underestimate the sophistication of scams, especially when they arrive via familiar channels like email and SMS. This perception-reality gap leaves many unprepared.

Source: F-Secure Consumer Market Survey, January 2025

# Channels used for scam attempts in the past 12 months



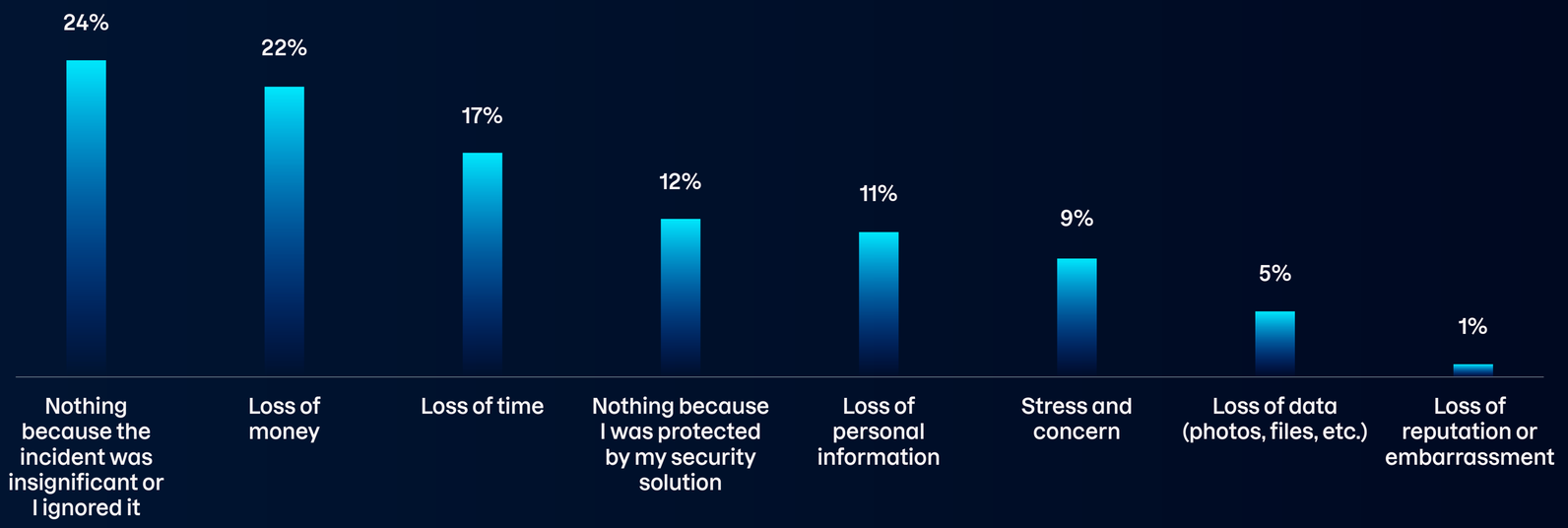

Source: F-Secure Consumer Market Survey, January 2025

## The Real-World Impact of Scams

Scams don't just cause momentary disruption—they have real consequences. Among victims, 22% lost money, 17% lost time, and 11% lost personal information. Others reported stress (9%), data loss (5%), and reputational damage (1%).

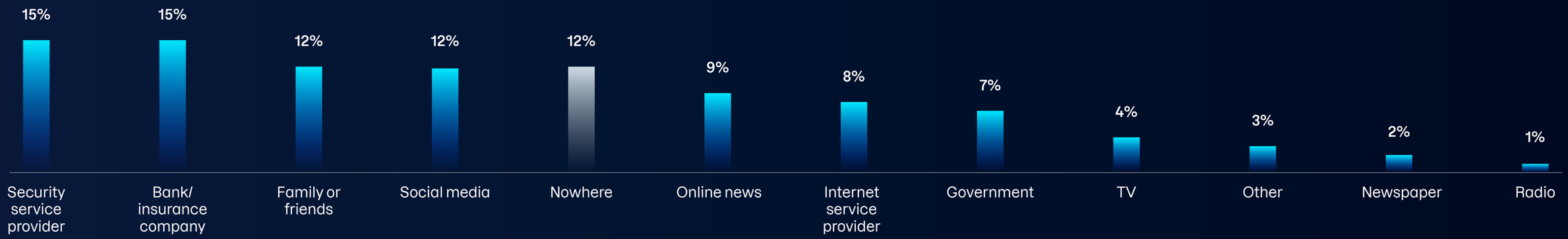
**Yet 24% downplayed or ignored the incident**—likely due to feelings of shame or embarrassment, growing desensitization from repeated scam exposure, or the belief that they should have known better. This avoidance reflects the overconfidence effect: "I should've seen that coming" becomes a reason to stay silent.

## Consequences experienced as a result of cyber crime




Source: F-Secure Consumer Market Survey, January 2025

# 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, 15% cite a security service provider, 15% turn to their bank or insurer, 12% speak to friends or family, 12% rely on social media, and 12% admit they don't get scam information from any source at all.

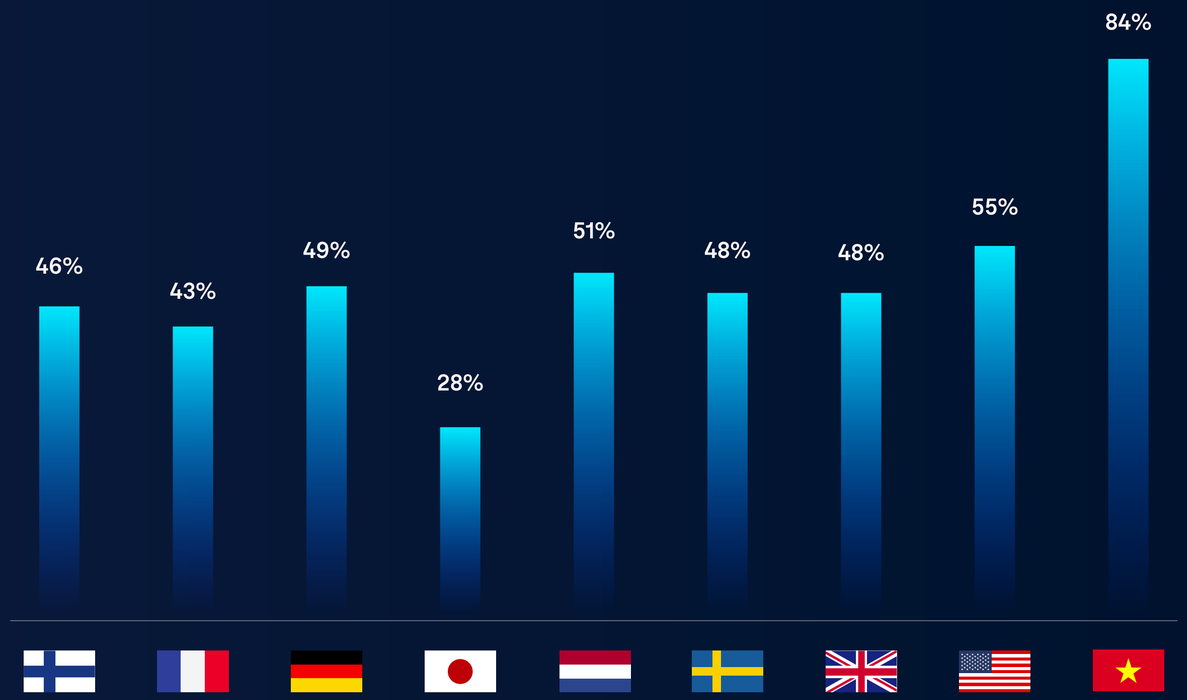
This fragmented landscape leaves consumers vulnerable to misinformation, outdated advice, and emerging scam tactics that often go undetected until harm is done.

Source: F-Secure Consumer Market Survey, January 2025

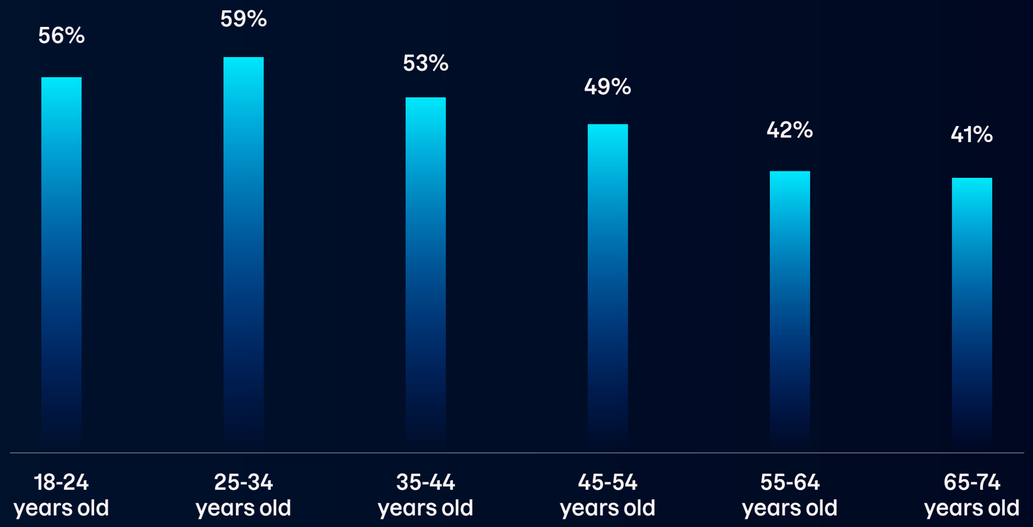
## Rising Willingness to Pay for Protection

Despite blind spots and gaps in awareness, consumers are beginning to recognize the limits of self-reliance: **50% of global respondents now say they are willing to pay for scam protection**. In Vietnam, that figure climbs to 84%.

## Willingness to pay for scam protection per country



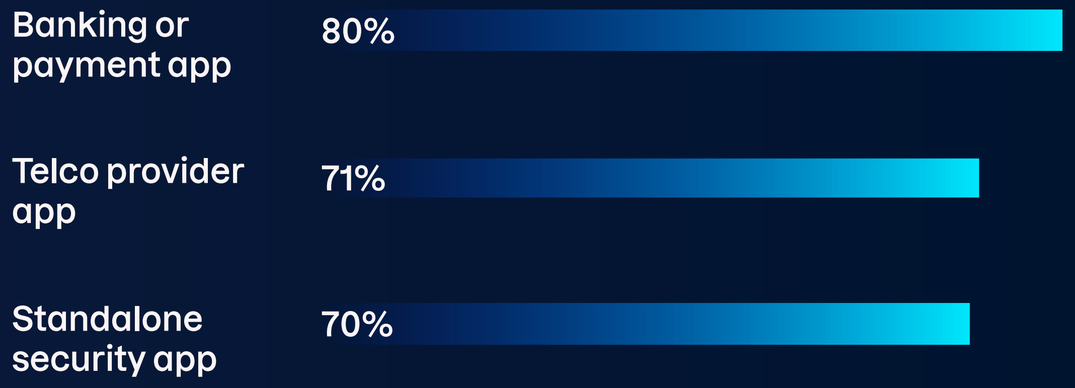

## Willingness to pay for scam protection per age group




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, telcos, 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

## Which apps 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

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.

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 including The New 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.

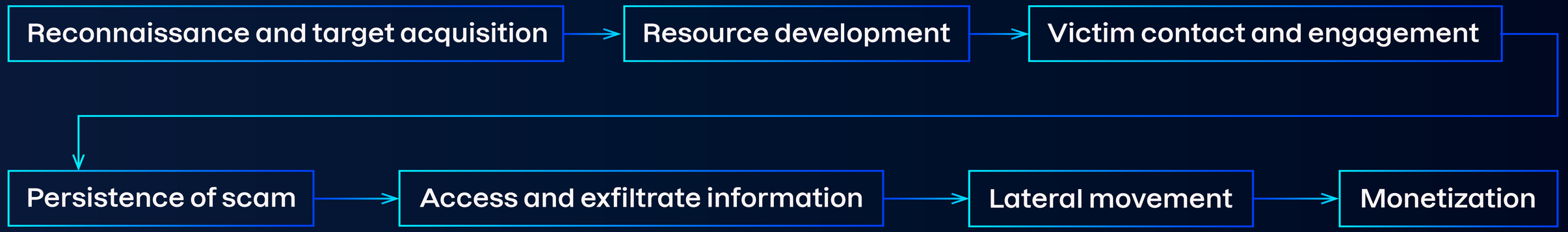
For example, The Financial Times reported that British insurance firm Beazley and ecommerce platform eBay have warned about scammers using AI to craft fraudulent emails by extracting and analyzing victim details from social media profiles.

## 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.

THE SILENT TOLL OF SCAMS:

# Breaking the Cycle of Shame and Inaction

Drawing on 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.


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

## 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.**

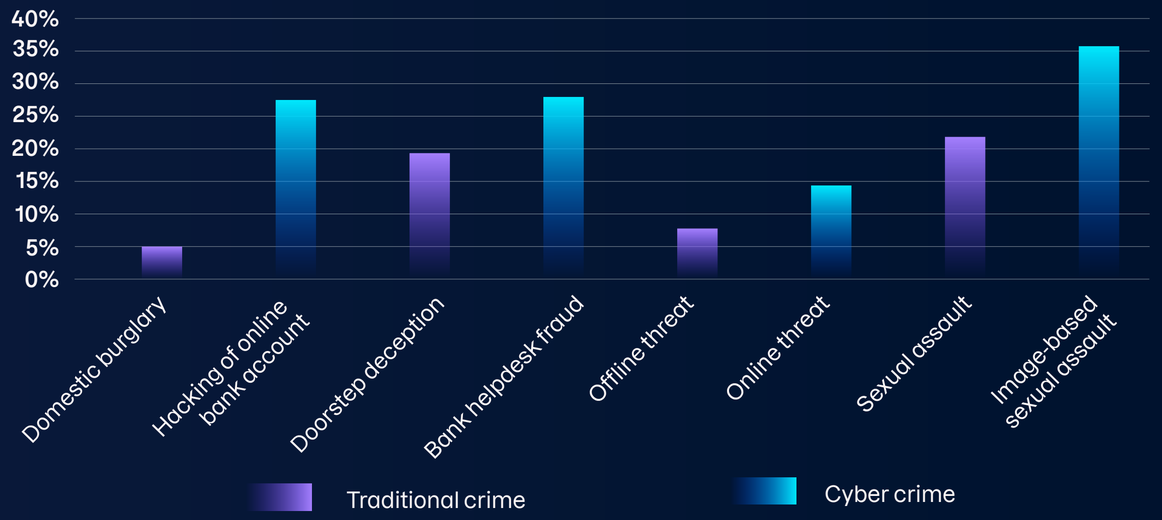
Instead of empathy, they're met with blame: "How could you be so stupid?" Public shaming is even common on professional platforms like LinkedIn, where one user told a scam victim, "Even my 90-year-old mother wouldn't fall for that."

## 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

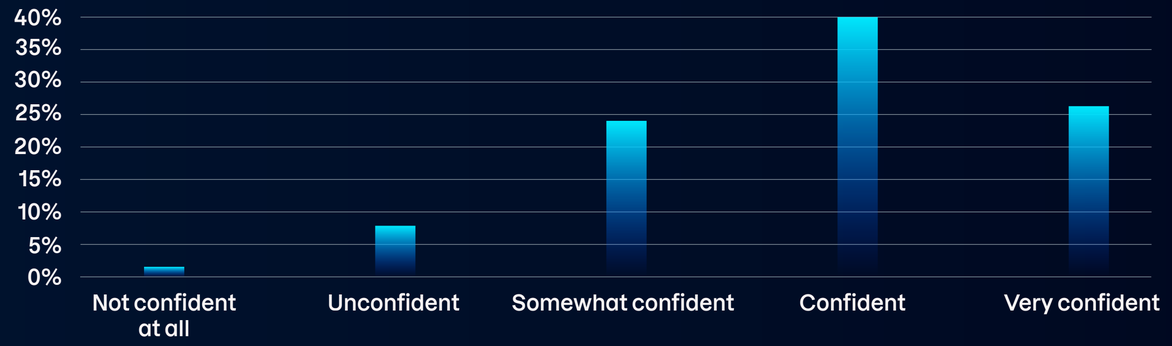



## Overconfidence Fuels Victim Blaming

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 global research, 67% of people believe they can 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 respondents confident in their ability to spot scams

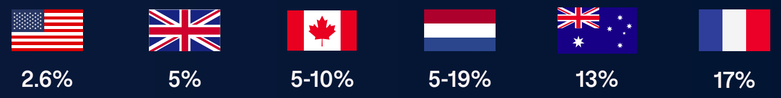



Sources: The Impact, Needs and Reporting Experiences of Cyber Crime Victims, Jildau Borwell, 2024; GASA Global State of Scams, 2024

## The Silent Epidemic of Underreporting

Globally, only around **7% of scams are reported to authorities**. In some countries, the numbers are even lower—just 2.6% in the United States and 5% in the UK. In the Netherlands, reporting estimates range from 5% to 19%, highlighting how hard it is to measure underreporting.

## Scam reporting rates by country

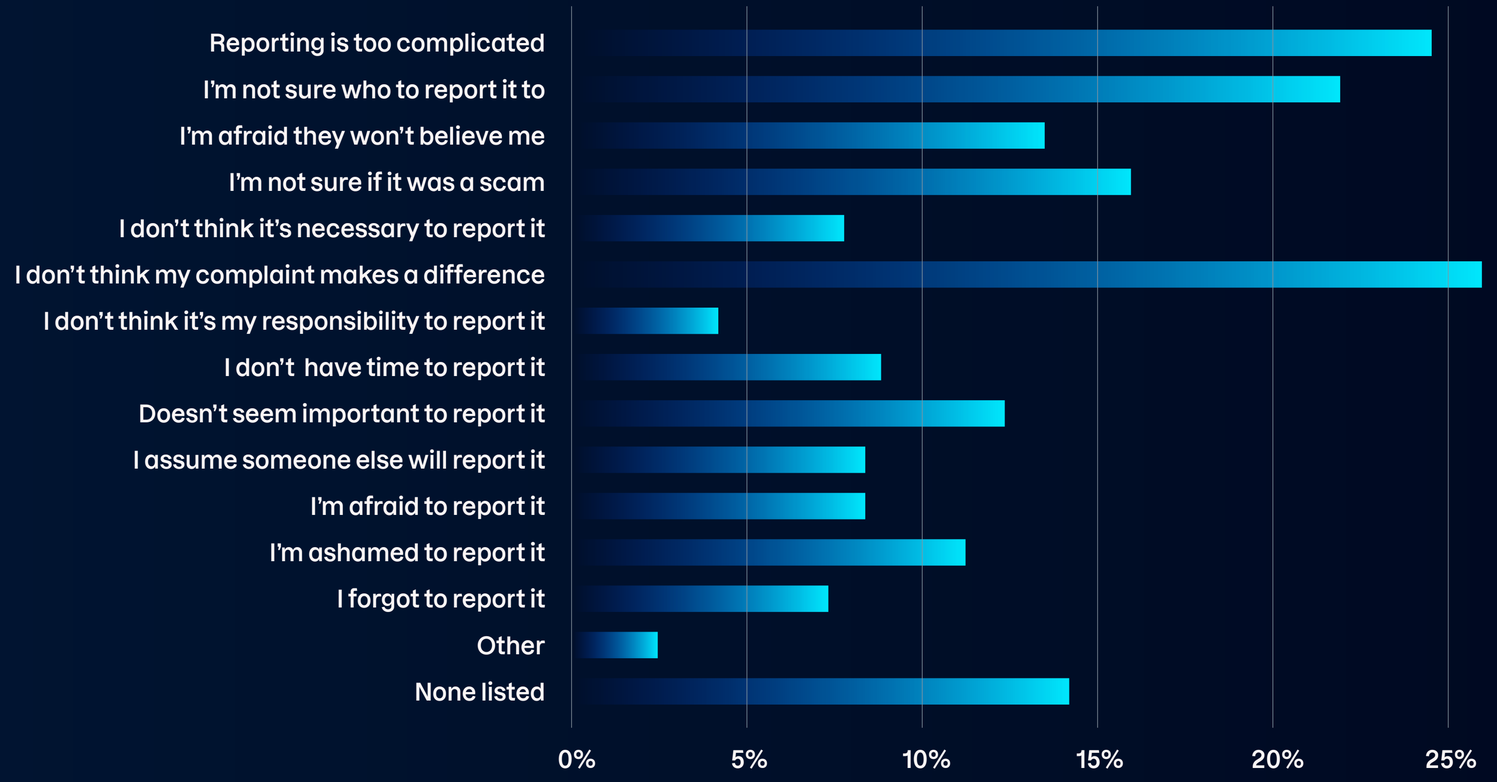



Why don’t more victims come forward? Most simply don’t believe reporting will make a difference. And too often, they’re right. In most cases, victims are told the amount lost is too small, the scammer is overseas, and the chance of recovering the money is minimal. It’s a response that, while honest, 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. Many don’t know where to turn, and when they do try, dense forms and unclear processes often shut them down.

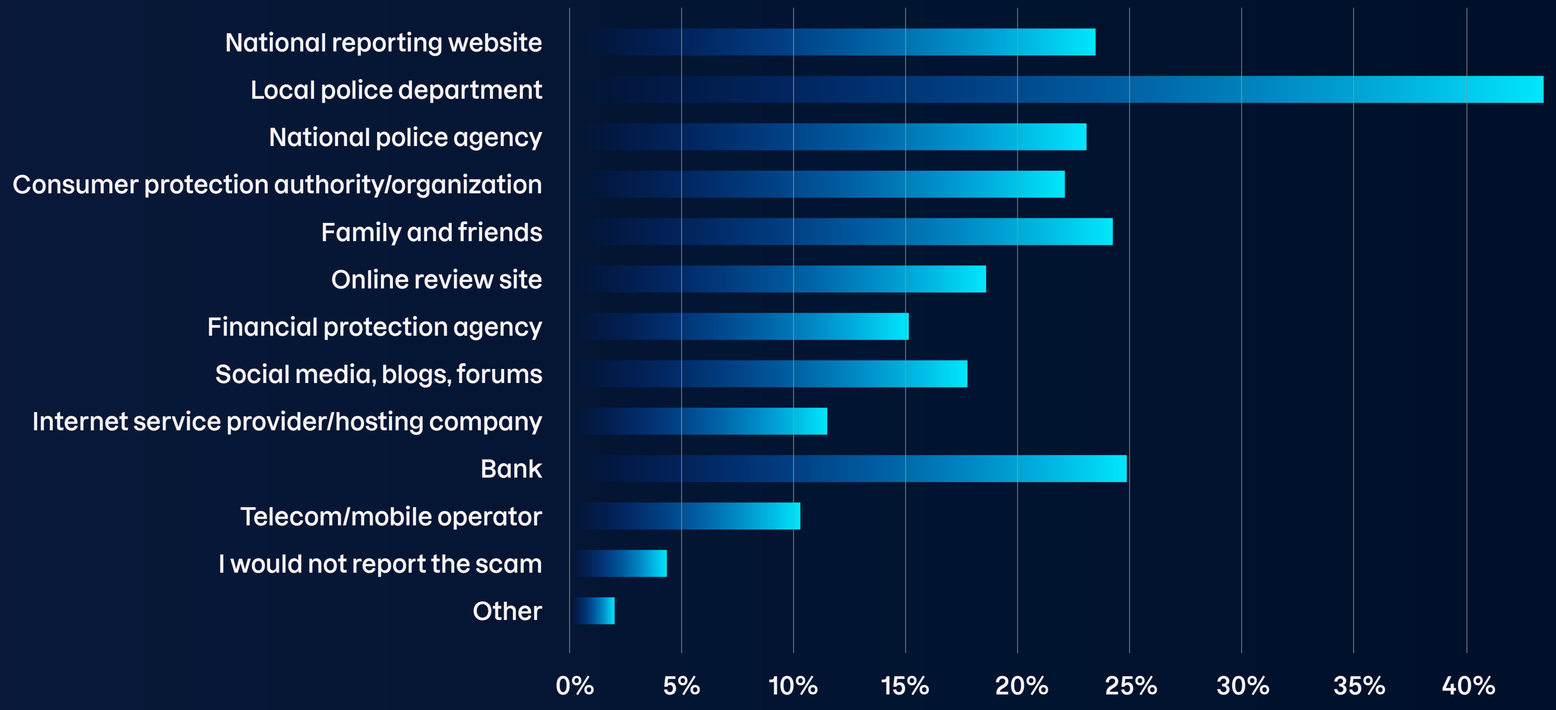
## Reasons respondents might choose not to report a scam




Sources: GASA analysis of multiple data sources, 2024 , GASA Global State of Scams, 2024

GASA's data illustrates this confusion clearly: 44% of people say they would report to local police, 25% to their bank, 24% to friends or family, and 23% to a national agency. With such a scattered system, victims are left uncertain—and many scams go unrecorded.

## Who 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 Global State of Scams, 2024

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.

RISK VS REALITY:

# Crypto Feels Dangerous—But Is Fear Justified?

From crypto hype fueling consumer anxiety to billion-dollar scam networks, this chapter demystifies the threat landscape and explores how everyday users can protect themselves in a system built for speed, not safety.

Threat researcher and ethical hacker specializing in information security.

Active keynote speaker, including a TEDx Talk on the dangers of stalkerware.

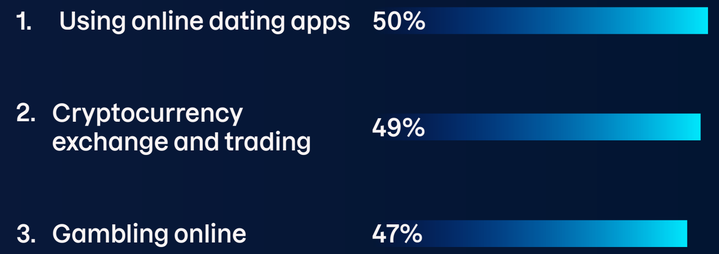
Podcaster and Finnish TV personality, educating audiences on cyber threats.

**Laura Kankaala**
Head of Threat Intelligence
F-Secure

## A Leading Driver of Digital Anxiety

What people perceive as dangerous online often doesn't align with what is actually risky. Our consumer market research shows that unfamiliar online activities—or those amplified by media attention, like cryptocurrency (crypto) trading—tend to trigger the most fear. But why is that, and are those fears truly justified?

## Online activities that worry consumers the most




As highlighted in the F-Secure Digital Perception–Reality Gap Report, **there's a stark disconnect between perceived threats and real cyber risks.** Familiar, everyday activities such as messaging via SMS or WhatsApp, making voice calls, or banking online are among the most common entry points for cyber crime, yet they provoke the least concern among consumers.

Meanwhile, crypto trading is widely seen as high-risk—even though the actual threat, in terms of likelihood and reach, is relatively lower. The potential for monetary loss, however, is significant and multifaceted: investing is inherently risky, and individuals can lose money either through scams or legitimate but poor investments.

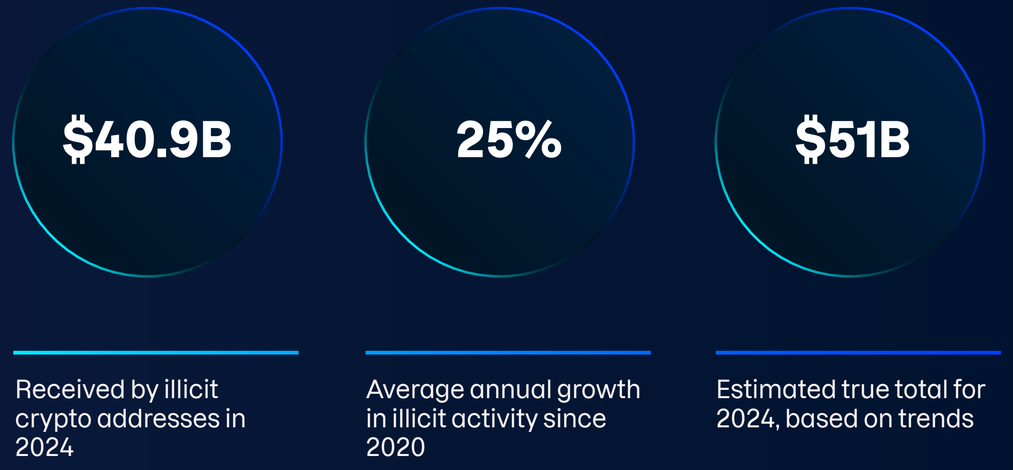
## Illicit Crypto Activity is Worth Billions

In addition to legitimate trading of cryptocurrencies, the financial impact of illicit crypto activity is substantial and continues to grow.

Chainalysis estimates that illicit cryptocurrency addresses—used for a range of illegal activities, from ransomware to the trade of illicit goods—received $40.9 billion in 2024. This figure is expected to rise as more addresses are identified, and historical activity is taken into account.

Since 2020, annual estimates of illicit crypto activity have increased by an average of 25%. If that trend holds, the true total for 2024 could approach $51 billion.

Sources: F-Secure Consumer Market Survey, January 2025, Chainalysis 2025 Crypto Crime Report




According to the Chainalysis 2025 Crypto Crime Report, this rise is likely driven by a growing number of illicit organizations and crime networks using cryptocurrency with increasing levels of professionalization and operational complexity.

## The Role of Cryptocurrency in Cyber Crime

To fully grasp the dynamics of crypto-related cyber crime, it's important to first understand how cryptocurrency works and why its unique characteristics have made it an appealing tool for fraud and financial exploitation.

## How Cryptocurrency Works

Cryptocurrency is a form of digital money that can be bought with traditional (fiat) currencies like dollars or euros. Unlike fiat currencies, it operates outside the control of central banks and isn't backed by physical assets or regulatory institutions.

Most cryptocurrencies run on decentralized blockchains that publicly record all transactions. Crucially, crypto transactions are irreversible, unlike bank transfers which can often be reversed in cases of fraud. While primarily used as a volatile investment, some retailers—both online and in-store—now accept crypto as payment.

## Why Scammers Use Cryptocurrency

Despite their public ledgers, cryptocurrencies offer more anonymity than traditional financial systems. Although every transaction is visible on the blockchain, identifying the real person behind a crypto wallet can be difficult, especially if they use platforms that don't require strong identity verification or if users have registered accounts with fake information. Crypto is also easy to transfer across borders without the oversight of banks.

Unlike traditional payments, and depending on the currency and mechanism used for transfer, crypto transactions often lack built-in fraud

protections. Once cryptocurrency is sent, it's impossible to recover. While there have been rare cases of law enforcement recovering stolen crypto assets, so-called "crypto recovery services" are scams themselves—often preying on people who have already been defrauded.

## Bitcoin and the Rise of Memecoins

Bitcoin remains the most well-known cryptocurrency, but it's just one of thousands, each with its own value proposition and underlying mechanisms.

In recent years, memecoins—tokens inspired by internet trends or memes—have surged in popularity, with examples like Dogecoin and $TRUMP. Their hype-driven nature makes them especially vulnerable to scams such as pump-and-dump schemes, where bad actors artificially inflate a coin's price before selling off their holdings. The price then crashes, leaving others with worthless tokens.

This wave of speculative crypto has opened the door to scams that prey on emotional triggers, social trust, and user inexperience. Whether through financial manipulation or social engineering, the goal is the same: to separate victims from their money.

## Prevalent Cryptocurrency Scams in 2025

1. **High-Yield Investment Scams** – Promise of fast, guaranteed returns through fake crypto investment platforms, often using fabricated testimonials.
2. **Romance Scams** – Scammers build trust over time, often through online romance or friendship, before convincing victims to invest in fraudulent crypto schemes.
3. **Rug Pulls** – Developers suddenly withdraw all liquidity or abandon the project, causing the token's value to collapse and investors to lose their funds.
4. **AI-Powered Sextortion** – Cyber criminals use threats, such as AI-generated nude deepfakes or stolen images, to blackmail victims into sending cryptocurrency.
5. **Crypto ATM Fraud** – Romance scam or helpdesk scam victims are coerced into transferring funds via physical crypto ATMs by scammers posing as love interests, authorities, or financial institutions.

# Staying Secure While Investing in Cryptocurrency

As crypto continues to attract new investors, education remains the strongest line of defense. The following guidance outlines key practices to help users avoid falling victim to scams.

## How to Vet an Investment Opportunity

- Research the investment, platform, and individuals involved. Search for the name of the cryptocurrency online and look for scam alerts, negative reviews, or user complaints—both before investing and on an ongoing basis.
- Exercise caution with memecoins, especially in their early stages. Investigate who created the coin, whether it has undergone audits, and how it's being promoted. Scam memecoins often rely on hype on social media platforms.
- Users should only invest what they can afford to lose. Cryptocurrency is inherently volatile, and lesser-known coins carry an even greater risk. There are no guaranteed returns.

## Common Warning Signs of a Crypto Scam

- Unsolicited contact promising high returns. This is especially concerning when it targets individuals through online dating platforms or unexpected social media interactions.
- Celebrity-endorsed ads on social media. These are often AI-generated and designed to lend false credibility to fraudulent crypto schemes, making them appear legitimate to users.
- Offers to recover lost cryptocurrency—for a fee. Scammers frequently re-target victims by posing as recovery services, further exploiting individuals who have already suffered losses.
- Pressure, threats, or extortion demands. Any attempt to coerce users into sending cryptocurrency, especially under duress, is a serious red flag.

THE FUTURE OF TRUST:

# Reckoning with an Increasingly Unreliable Digital World

Grounded in new foresight research, this chapter explores how consumer coping behaviors are evolving in response to an increasingly untrustworthy internet—and how protection must adapt in parallel.

Research engineer specializing in complex, sustainable technologies and systems.

Extensive experience in deep tech startups and researching and shaping policy for socio-technical systems.

University of Cambridge alumna with a PhD in engineering.

**Dr Laura James**
Vice President of Research
F-Secure

## Exploiting What Makes Us Human

Scams are a deeply human threat. They exploit trust, convincing people to believe the wrong thing or to question the right one. As scams grow more personal and emotionally manipulative, we're choosing to dig deeper into what makes people vulnerable and how we can better understand them.

This is the focus of F-Secure's research function, Illuminate. As the rules of engagement change, so must our understanding of how digital threats exploit our human tendencies. That's why we're applying social science: to explore how human behavior shapes risk and test new approaches to helping people stay safe online.

## A Glimpse into the Future of Trust

To anticipate what lies ahead, we recently conducted a foresight study exploring how trust will evolve over the next three to five years—identifying key global shifts that are reshaping the consumer threat landscape:

**Deteriorating information environment.** As misinformation and AI-generated content spread, it's becoming harder to tell what's real online.

**Economic instability.** Growing financial anxiety leaves people more desperate, uncertain, and emotionally vulnerable, making them easier targets for scams.

**Unreliable internet infrastructure.** We're moving toward a future marked by outages, glitches, and unpredictable failures. This isn't just about evolving threats, it's about a changing internet.

## How People Are Learning to Cope Online

After more than two decades online, many of us have developed coping mechanisms to navigate digital spaces. But as the threat landscape evolves, those strategies are starting to break down. Even confident, tech-savvy users are now being scammed in growing numbers—proof that past experience is no longer enough to stay safe.

To better understand this shift, we identified several emerging patterns of behavioral adaptation. Shaped by risk appetite, digital confidence, culture, values, and behaviors, they reveal how people are trying to regain control in an environment that feels increasingly unpredictable. The following examples represent just a few of the broader set of patterns.

**Scam Taxpayer:** A busy individual who accepts minor fraud losses as just another cost of modern digital life.

**Exhausted Influencer:** A content creator who is shrinking their online presence after repeated negative experiences.

**Confident Outrunner:** Someone who thinks they're too smart to be targeted by scammers.

Together, these patterns help us navigate the future digital behavior landscape, showing not just what people do online, but how they feel, cope, and adapt. This perspective helps identify gaps between threat exposure and user response that traditional models overlook and enables the design of protection that accounts for human emotion, not just digital function.

## Designing Protection That Builds Trust

Building on this work, we're developing future consumer archetypes shaped by one of the most important forces in online behavior: trust dynamics.

Take two examples: Gretchen and Vivienne. Each reflects a distinct mix of digital confidence, social behavior, motivation, and risk exposure. These patterns reveal where protection is most needed—and what form it should take.

### Gretchen

Strong parasocial connections

Content creator, priortizes reputation

Empathy

Trusts on instinct

Susceptible to flattery

### Vivienne

Strong relationships locally

Trusts family and friends

Seeks advice when she needs it

Easily trusts people she doesn't know well in lightweight interactions, such as small online purchases and participating in many group chats

## Rethinking Consumer Segmentation

The internet is changing. Traditional segmentation based on age, location, or device no longer captures the full picture. To truly understand our users, we need to look at how they trust, how they feel, and how they live.

This gives us something powerful: a framework to design protection that's personalized, not one-size-fits-all. It's how we stay ahead of tomorrow's threats and fight back against the scam pandemic.

## Looking Ahead: Illuminate's Research Vision

F-Secure Illuminate is exploring approaches to protection that work with human psychology—not against it. Our work examines cognitive styles and identifies ways to help people build resilience before, during, and after security incidents, focusing on:

- **Detecting Unseen Scam Risks** – Beyond the reach of today's app-based security, using network signals and behavior patterns.
- **Understanding How Consumers Build Trust in AI** – To design protection that's transparent, personal, and aligned with real behaviors.
- **Reframing Security as Empowerment** – Not just defense, but a source of positive value, enabling digital confidence and control.
- **Connecting Threats with Human Behavior** – So we can design protection that works in the real world, not just in the lab.

Threat researcher and ethical hacker specializing in information security.

Active keynote speaker, including a TEDx Talk on the dangers of stalkerware.

Podcaster and Finnish TV personality, educating audiences on cyber threats.

**Laura Kankaala**
Head of Threat Intelligence
F-Secure

INSIDE SCAM CENTERS:

# The Dual Realities of Privilege and Exploitation

From designer-clad employees to trafficked workers forced into scams, this chapter exposes the dual realities behind global scam operations—and why service providers must move beyond stereotypes to protect consumers.

## Scammers, Stereotypes, and Blind Spots

When most people picture scam operations, two familiar stereotypes come to mind: a buzzing underground call center in India filled with young men cold-calling victims, or a shadowy criminal syndicate led by mafia-style kingpins with unlimited technological prowess.

These tropes, shaped by media narratives and cultural bias, contain fragments of truth. But when we reduce scammers to caricatures, we overlook the deeper mechanisms—and the often desperate or coercive circumstances—that lead people to commit cyber crime.

Oversimplifying how scams operate creates blind spots in prevention. And glamorizing scam culture risks desensitizing the very people we need to reach. These misconceptions matter. Reframing these assumptions isn't just a PR exercise; it shapes how we understand modern day crime and helps consumers respond to threats.

## What Modern Scam Centers Actually Look Like

Many operations today more closely resemble commercialized cyber crime enterprises than backroom hustles, mirroring legitimate businesses with onboarding processes, sales scripts, performance quotas, and structured shifts.

But not all scam centers operate alike. Some are profit-driven enterprises, fueled by ambition and status. Others are far more sinister, powered by coercion, violence, and modern slavery—making fraud not just a financial threat, but a human rights emergency.

To understand the full spectrum of these operations, let's examine two real-world examples at opposite ends of the scam ecosystem.

### Operation A:

Lavish Lives of a Scam Center (p.44)

### Operation B:

Forced Labor in Scam Farms (p.45)

## Operation A: The Lavish Lives of a Georgian Scam Center

At one end of the scam spectrum lies a culture of conspicuous wealth: young scammers flaunting designer clothes, luxury cars, and exotic holidays on social media, proudly claiming it was all paid for with stolen money.

A standout example is the Georgian investment scam center exposed by the Organized Crime and Corruption Reporting Project (OCCRP). Staffed by 85 young, university-educated individuals, the operation posed as financial advisors serving global clients.

In reality, they stole $35.3 million from more than 6,100 victims in under three years. The structure was simple: 'conversion' teams contacted ad leads, while more experienced 'retention' teams worked to extract as much money as possible.

Operating as a registered telemarketing firm, the scam center resembled a modern tech startup—but its performance reviews revealed a darker reality: employees were evaluated on their ability to lie and manipulate. Internal messages were even more disturbing, with one scammer writing: "I will make their mother cry, I promise."

Since the OCCRP exposé, digital traces tied to the group have started disappearing. They once believed that the internet made them untouchable, but their digital footprints may ultimately be their downfall. Once something is online, it's never truly gone.

*Illustrative example of a scam center setup, not the actual facility*

## Operation B: Forced Labor in Southeast Asia's Scam Farms

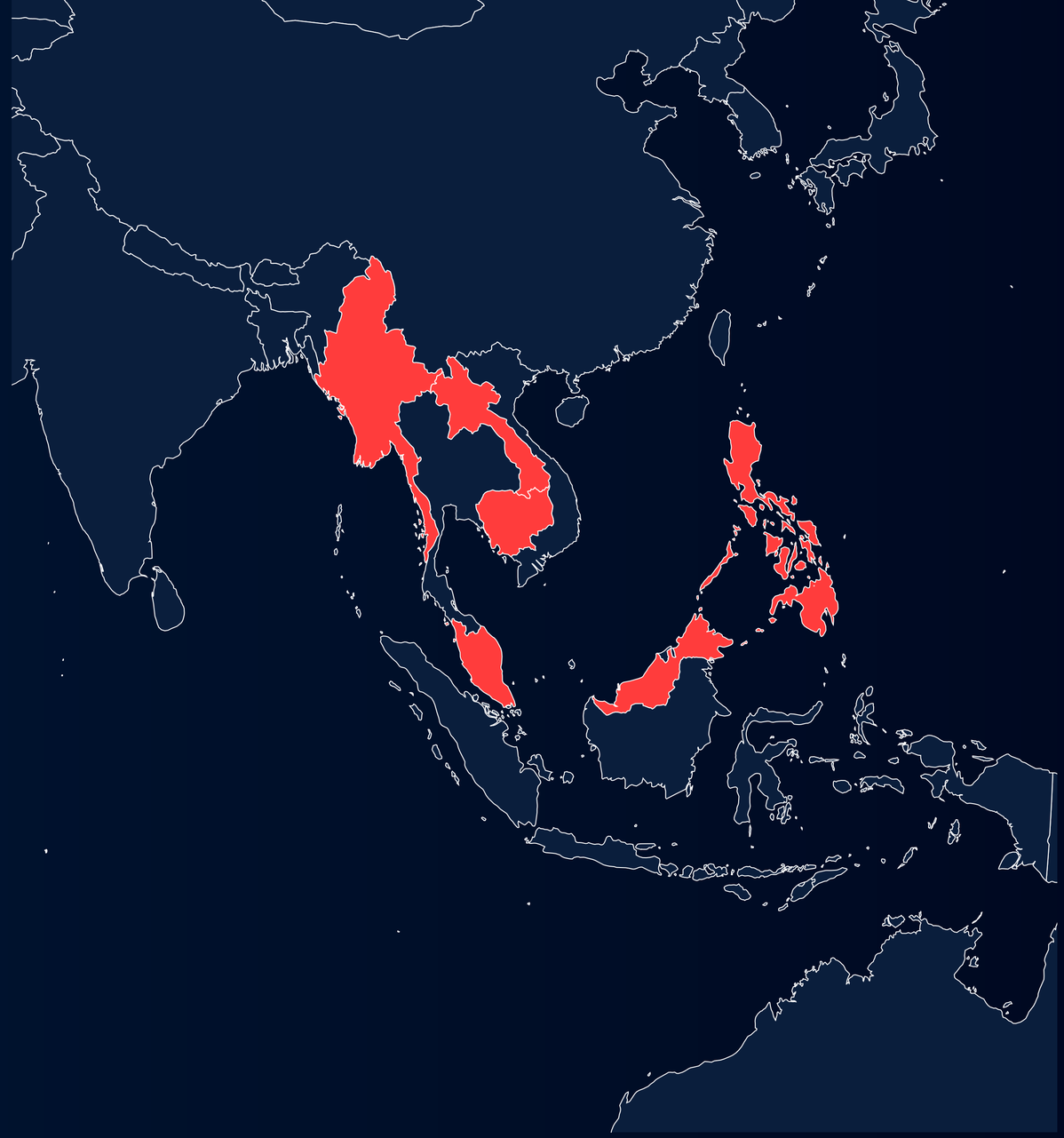
At the other end of the scam spectrum, a human rights crisis is unfolding. Hundreds of thousands of trafficked individuals are forced into scam farms across Southeast Asia, held in cramped conditions with little food, water, or medical care.

These underground operations often recruit victims from around the world—kidnapped, sold, or tricked with false promises, then held until their families pay a ransom. Escape attempts are met with torture or death, often overlooked by corrupt officials.

One such scam compound in the Philippines, shut down in 2024, was found to have 700 workers living inside, fenced off from the outside world. Workers who failed to meet their "daily quota" of money scammed from victims were tortured as punishment.

In another case reported this year, 176 Filipinos were trafficked into Myanmar scam centers after being lured by fake job ads. Promised roles in customer service, they were instead smuggled into conditions described as harrowing: they were held against their will, subjected to physical abuse, denied medical care, and forced into criminal activity.

And these are only a few examples. Scam compounds remain active across Southeast Asia. UN experts warn that governments must address the root drivers of forced cyber crime: poverty, poor access to education, work, and healthcare, and limited legal migration options—all pushing vulnerable people into this exploitative system.



*Scam farm hotspots in Southeast Asia*

## Looking Ahead: Turning Insight into Action

- Understanding scam operations is essential to disrupting them. This goes beyond filtering calls or flagging suspicious activity. It demands a multi-layered response: sharing threat intelligence, monitoring risks in real time, delivering timely in-app warnings, and equipping call centers to respond with clarity and compassion.
- But technical controls alone aren't enough. Scam centers thrive in the shadows of public misconception. When consumers underestimate the sophistication, scale, or human cost of scams, they're more likely to fall victim. And while some scammers profit, others are trapped in the very system they appear to control.
- That's why service providers must play an active role in reshaping public understanding—challenging outdated stereotypes, raising awareness of how scams operate, and preparing consumers for the tactics they're likely to face.
  By closing the gap between perception and reality, service providers can strengthen trust, reduce harm, and take the lead in protecting their customers from scams.

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.

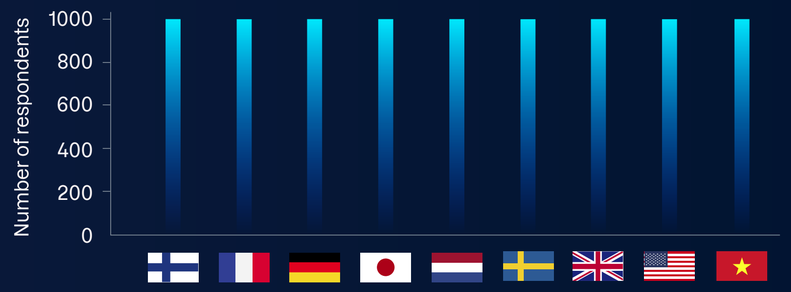
> **It will take another breakthrough—one that makes AI agents significantly more accessible and affordable—before scammers are likely to adopt them at scale. Whether that tipping point arrives in the next few years remains to be seen.**

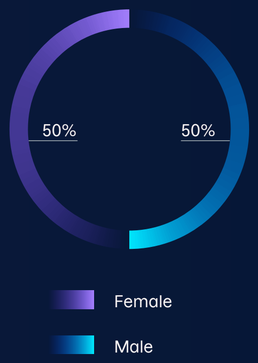
# Sources and Methodologies

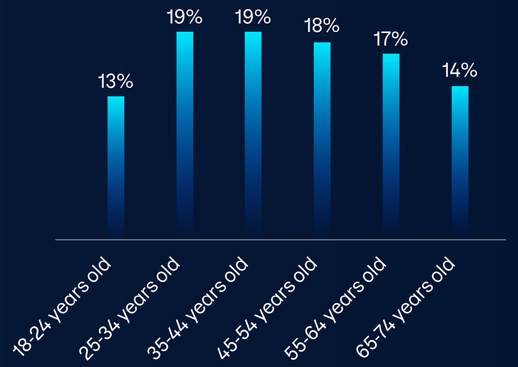
### 2025 Scam Landscape: How Overconfidence Leaves Consumers Vulnerable

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 across countries.

The survey captured responses from 9,000 consumers across nine 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 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 Global State of Scams Report, 2024
- The Impact, Needs and Reporting Experiences of Cyber Crime Victims, Jildau Borwell, GASA Meetup, 2024

### Risk vs Reality: Crypto Feels Dangerous—But Is Fear Justified?

- F-Secure Consumer Market Survey, January 2025
- F-Secure Digital Perception–Reality Gap Report, 2025
- Chainalysis 2025 Crypto Crime Report, 2025

### The Future of Trust: Reckoning with an Increasingly Unreliable Digital World

- F-Secure Illuminate Foresight Study: Evolution of Trust in 3–5 Years, 2025
- F-Secure Illuminate Patterns of Behavioral Adaptation Study, 2025
- F-Secure Illuminate Trust Dynamics Study: Future Consumer Archetypes, 2025

### Inside Scam Centers: The Dual Realities of Privilege and Exploitation

- Organized Crime and Corruption Reporting Project: 'Diamonds, Dior and Dubai Vacations: The Luxurious Lives of Georgia's Call-Center Scammers', 2025
- Office of the United Nations High Commissioner for Human Rights: 'UN Experts Urge Immediate Human Rights-based Action to Tackle Forced Criminality in Southeast Asia Scam Centers', 2025
- Organized Crime and Corruption Reporting Project: 'Philippine Rights Commission: Dozens of Filipinos Trafficked into Scam Centers in Myanmar', 2025

illuminate
By F-Secure

# 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