Cyber Threats Guide 2025

Actionable insights to help service providers navigate emerging consumer scams and other critical online threats.

F-Secure®

Executive Summary

The third annual F-Secure Cyber Threats Guide provides an in-depth analysis of the cyber threats consumers will face in 2025. Tailored for service providers, it offers critical insights into the evolving landscape of scams, personal data theft, and other emerging online risks. Leveraging the expertise of renowned F-Secure threat intelligence specialists, the guide delivers actionable insights and strategic recommendations to help businesses protect their customers from the latest cyber threats.

KEY FINDINGS

- Cyber threats in 2025 are more sophisticated than ever, driven by AI advancements, evolving scam tactics, and shifting geopolitics. Scammers continue to prey on human emotions, using deepfakes and social engineering to deceive consumers.
- The F-Secure Scam Kill Chain—a proprietary framework—offers a deep understanding of cyber criminal tactics and techniques and serves as a foundation for building effective defenses against evolving scam threats. Additionally, our latest consumer data reveals attitudes towards and experiences with scams in 2025.
- Data privacy is under threat, as exploiting personal data can lead to significant financial gains. We expose how personal data reaches illegal online marketplaces and reveal the black market prices for social media logins, PayPal accounts, and more.
- Looking beyond 2025, we forecast the next frontier of cyber threats and defense strategies—from the disruptive potential of quantum computing to AI's role as a 'trusted companion' in defending consumers against scams.

FINAL THOUGHTS

As cyber threats evolve in complexity and scale, the need for vigilance has never been greater. Scammers are adapting rapidly, capitalizing on AI and exploiting global events and vulnerabilities to target consumers and businesses. To stay ahead, service providers must take a proactive stance—embracing new technologies, strengthening consumer education, and pooling resources. The future of cyber security hinges on innovation, cross-industry collaboration, and an unwavering commitment to protecting digital spaces.

Contents

The Battle for Data Privacy in the Cyber Wild West

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 look at how modern-day outlaws exploit digital loopholes to hold our personal data hostage. Are privacy laws enough to stop scammers and protect consumer data?

Delaware, Nebraska, Iowa, New Hampshire, New Jersey, Maryland, Minnesota, and Tennessee—what do these US states have in common? They have all implemented, or will implement, privacy laws in 2025. While specifics vary by state, these laws aim to ensure that businesses and organizations processing or controlling personal data do so with consumer consent, greater transparency, and the possibility of fines for non-compliance.

Data is a Critical Asset in 2025

Data is really what makes most companies tick today. Even if collecting and processing data isn't the core of the business, as it is for data brokers, for instance, there is still plenty of data that needs to be collected and processed simply to pay the bills or deliver services to consumers. While computers have made businesses more efficient compared to the era of pen and paper, they've also made them more vulnerable.

What do I mean by 'more vulnerable'? Data has always been important, even though it hasn't always been stored in servers or in cloud services. When providing any kind of service, you'll need to know different kinds of things about your customers—their name, address, phone number, birthday, Social Security number, preferences, background. Data is a very multi-faceted term, but when talking about data referring to a living and breathing individual, it means information that can be used to identify them.

The True Value of Personal Data

Personal data is widely used on the internet for various purposes, from targeting ads and tailoring content to enabling companies to make data-driven decisions about individuals. While targeted content and decision-making can sometimes lead to unfair treatment of consumers, the collection of personal data also carries an even darker side.

Data is valuable because it reveals a lot about us—sometimes even more than we know of ourselves. When large amounts of data are analyzed, trends and patterns emerge, grouping us by our interests and backgrounds. This is what makes data so valuable, but also what makes it vulnerable when it falls into the wrong hands—it can be leveraged for social engineering and extortion.

Our data can be obtained by threat actors—individuals or groups who exploit technology and the internet with malicious intent. For example, data brokers, whose sole business is selling data, have operated relatively unregulated, leaving a significant gap in individual privacy protections.

Can Privacy Laws Protect Data?

Privacy is a crucial building block for protecting everyday citizens as it steers companies to operate responsibly. Without regulations and laws governing data collection, companies can exploit data for profit through unfair or unethical practices. They might also collect excessive personal data and store it insecurely, leaving it vulnerable in databases or storage systems that can be easily hacked.

With a background in ethical hacking, I'm often asked: What's the difference between privacy and security? Privacy refers to the rules and practices that govern how companies handle our data. An added benefit is that privacy regulations often lead to improved security. Security, on the other hand, involves the practical measures used to protect data

such as strong password policies, regular updates, and a defense-in-depth approach.

But here's the thing: scammers and cyber criminals don't care about laws the way legitimate businesses do. They know they aren't running lawful operations, and they have no intention of being caught or facing consequences. Instead, they leverage online platforms, hide behind aliases, and creatively advertise their services to build an ecosystem where sellers of illicit goods or services can connect with buyers.

Laws Fail to Deter Cyber Criminals

Threat actors don't care about your privacy or security practices. They're not concerned with how many boxes you tick on a security checklist. What matters to them is data—and how to get their hands on it. Even in the criminal world, data is a lucrative business.

Imagine a rogue data broker hacking into a legitimate data broker's system, stealing background checks or criminal records, and then selling them on illicit online marketplaces or directly to shady buyers. There's no oversight or regulation of sold data when criminals are doing the selling.

Cyber criminals are also creative in how they gain access to data. They might exploit weak processes, such as buying data directly from a legitimate data broker. Alternatively, they could take advantage of a software bug or exposed databases to secretly copy valuable data.

The Internet is Full of Loopholes

As a security professional and ethical hacker, I see a cyber landscape littered with loopholes. These vulnerabilities in our systems make it possible for cyber outlaws to rob a person without ever meeting them. Privacy policies and security promises are meaningless if your stolen medical records are being used to extort money from you or to threaten you.

I'm skeptical that any law will ever fully close these loopholes, as laws are designed for the law-abiding. That's not to say laws aren't important—at their best, laws and regulations establish a solid baseline and motivate companies to keep data safe. And this is crucial. Keeping data secure means keeping consumers and societies safe.

But we can't rely solely on laws to protect people online. Laws are slow to pass, and new technologies and possibilities for threat actors emerge constantly. We must do more—go the extra mile and work every day to ensure that people and their data remain safe.

How the Online Scam Landscape is Evolving in 2025

Speaker and advocate for scam awareness and knowledge sharing.

Educator specializing in the development of scam prevention strategies.

Managing Director of ScamAdvisor, a service that develops website trust scores.

Jorij Abraham
Managing Director
Global Anti-Scam Alliance

F-Secure × GASA Global Anti-Scam Alliance

F-Secure is a Foundation Member of GASA, collaborating with industry leaders and sharing cyber threat intelligence to help set the global standard for scam protection.

Staying up to date with the fast-moving online scam landscape is crucial for protecting consumers, building trust, and delivering positive experiences. Here's what you need to know.

Scams are a significant challenge for just about everyone in today's digital age. In our shared efforts to combat this growing threat, we spoke with Jorij Abraham, Managing Director of the Global Anti-Scam Alliance (GASA), whose mission is to protect people from the financial and emotional harm caused by scams.

Abraham explains that GASA works by "bringing together governments, law enforcement, consumer protection organizations, financial services, telcos, social media, and cyber security companies like F-Secure to share knowledge and define joint actions to protect consumers from scams".

Worldwide Cost of Scams

The scale of online scams is staggering. “Nearly $1.026 trillion was lost by consumers worldwide last year,” explains Abraham. “In our global study, 78% of participants experienced at least one scam in the last 12 months. However, 59% didn’t report the scam to authorities—24% believed reporting it wouldn’t make a difference”.

It’s understandable why they hold that belief: “According to the World Economic Forum, only 0.05% of all cyber criminals are prosecuted. Scammers can go free because they can operate globally, while law enforcement operate locally, regionally, or nationally”.

Masterfully Exploiting Trends

This immense cost is fueled by scammers’ adaptability and their ability to exploit timely events. As Abraham explains: “If there’s a flood, scammers launch charity scams. A military threat? Fake arms shops appear. A Taylor Swift concert? Fake tickets. Scammers are, unfortunately, great marketers”.

Beyond financial losses, scams erode trust—an essential foundation for service providers. According to F-Secure data, 77% of people worry about their online safety, with 7 in 10 unsure whom to trust. And there’s good reason for this: GASA found that 45% of people experienced more scams in the last 12 months than the year before.

Cultural Differences in Scamming

Scams affect people worldwide, but some regions face greater risks. “People in developing countries are scammed far more than citizens of wealthier nations,” explains Abraham. “The rapid adoption of digital platforms during the Covid-19 pandemic left many in these countries more vulnerable due to a lack of cyber security awareness programs”.

Cultural differences also influence the types of scams that emerge. As Abraham notes: “In India, fake employment scams are rampant, while Southeast Asia struggles with fake gambling websites. Scams often ‘migrate’—a successful scam in one country is refined and exported to others or sold as a service to other scammers”.

Top Channels for Scams

While email-based phishing remains the top channel for scammers, they are increasingly using fake text messages to exploit public trust. Posing as trusted entities such as healthcare, taxation, and government services, these scams aim to panic recipients with urgent language or threats of financial or legal consequences. Victims are then directed to malicious websites to pay fictitious invoices, resolve supposed tax issues, or address fabricated fines.

Trending Scam with a Twist

GASA has observed a sharp rise in romance scams globally, often combined with

Sources: GASA Global State of Scams 2024 , F-Secure Digital Moments Survey 2025

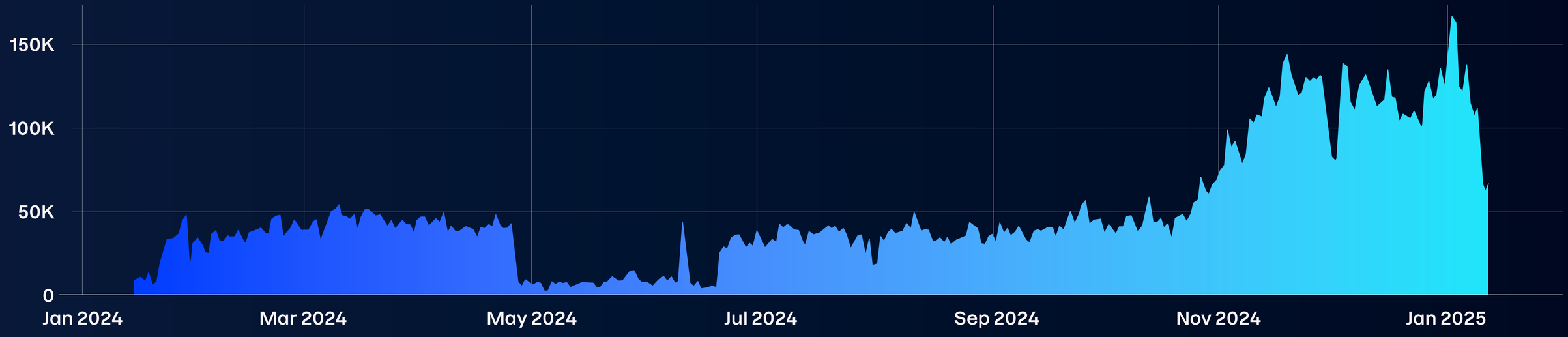
investment scams. As Abraham explains, “Scammers build relationships with victims through dating apps or social media. Once trust is established, they ask for money—usually to solve emergencies or to meet in person”.

The scam kill chain is constantly evolving. “Nowadays, we see victims lured to fake investment websites and convinced to invest,” Abraham continues. “These platforms appear highly professional, mimicking real trading systems. Victims can initially even withdraw profits, but the trap snaps shut once they make a significant investment. These scams hurt victims in two ways: they lose their savings and often experience heartbreak”.

Rise in Fake Online Shops

Shopping scams use fake offers, counterfeit websites, and fraudulent order confirmations to target online consumers. Scammers mimic trusted retailers, offering huge discounts to steal personal and payment details or sell items that never arrive.

F-Secure data reveals a spike in blocked scam sites late last year, underscoring the need for vigilance during peak shopping periods. This also highlights an opportunity for service providers to educate consumers on safe online shopping practices during these times.



Scam shopping sites blocked by F-Secure

AI is Ruling the Scamscape

As forecasted in last year's guide, scammers have rapidly adopted generative AI to create more sophisticated scams. "Scammers use AI to send personalized phishing emails, chat with victims via WhatsApp and Telegram, and create fake product photos or deepfake videos of well-known individuals," explains Abraham.

This technological leap makes it increasingly difficult for consumers to identify scams. In one case, scammers used AI to convince a victim for over a year that they were in a relationship with Brad Pitt, ultimately defrauding them of €830,000 for 'hospital expenses'.

Despite this rising threat, Abraham remains optimistic about AI's defensive potential: "Cyber security companies like F-Secure are using AI for good. In a few years, AI could fully protect us—reading our emails, answering our calls, and monitoring our video meetings for scam signals".

Global Responses to the Scam Pandemic

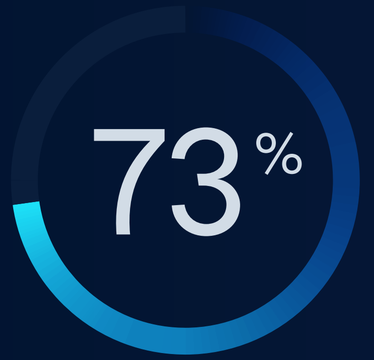
Abraham emphasizes the need for systemic solutions: "Consumers need extra protection as scams become harder to recognize, and infrastructure-level efforts have already proven effective in reducing scams".

"One successful initiative is the Belgium Anti-Phishing Shield project, where 20,000 phishing emails are analyzed daily and blocked at the network level by internet service providers," he continues. "Another is in Singapore. The Anti-Scam Command works closely with police, banks, operators, and social media platforms to take direct action".

Device-Level Scam Protection

"These initiatives are excellent, but device-level protection, such as anti-scam software, is equally critical," Abraham concludes.

F-Secure shares this view, having launched Scam Protection functionalities in 2024 to cover online shopping, banking, SMS scams, phishing links, harmful ads, and more. These functionalities offer effortless security, each day performing 700,000 AI-driven detections to block suspicious behavior and securing over 1 million banking transactions worldwide.



of people don't know who to trust online

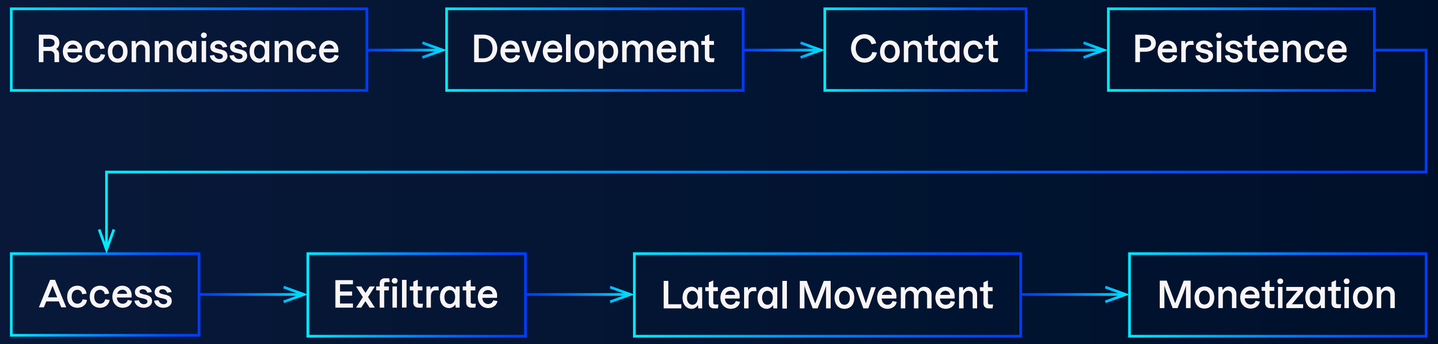
of people don't know if their devices are secure

Source: F-Secure Digital Moments Survey 2025

FROM HOOK TO HEIST:

Inside the Scam Kill Chain

To effectively defend against scams, we must first understand how they operate. That's why we developed the F-Secure Scam Kill Chain—a detailed breakdown of modern scamming strategies.



The borderless internet is saturated with scammers targeting vast numbers of consumers daily. Yet, until now, no framework has comprehensively described how scammers operate. The goal of the F-Secure Scam Kill Chain is to offer that deep understanding of various types of scams, breaking down both high-level tactics and specific techniques. By doing so, we aim to build a rich, detailed knowledge base that serves as a formal foundation for researching and developing effective defenses against scams.

How Scams Are Executed in Eight Key Stages

Every scam follows a series of building blocks, which we've broken into eight key stages. Each stage represents a tactic aligned with scammers' goals, building on the previous one to ensure success. 'Techniques' are the specific methods scammers use to achieve these goals.

This work is inspired by the MITRE ATT&CK® Matrix for Enterprise; however, instead of mapping cyber security threats to organizations, it focuses on threats to consumers' online accounts, devices, and data.

Stage 1: Reconnaissance

The scammer gathers information about potential victims to use in later stages of the scam. This phase involves both identifying victims and collecting their personal data for future exploitation. The scammer's goal is to identify as many victims as possible—or a targeted group—and gather extensive information about them. Techniques range from manually collecting details from social media or using automated data collection, to phishing via SMS and phone calls or purchasing data from illegal online marketplaces.

Stage 2: Development

The scammer establishes resources that form the foundation of the entire scam. These resources support later tactics in the Scam Kill Chain and may include creating, purchasing, or compromising resources to aid in targeting victims. Resources can be both physical (e.g. computing devices and human scammers) and virtual (e.g. websites, social media accounts, and malware) infrastructure used in the scam.

Stage 3: Contact

Once potential victims are identified and their information is gathered, the scammer makes contact. They may employ various manipulative techniques, including interactive contact (e.g. phone calls, email, SMS, and social media), non-interactive contact (e.g. online ads), or a mix of both. Victims may even contact scammers unintentionally, such as by searching for pirated software. The goal of this tactic is to provoke a response, either by directing the victim to a malicious site or getting them to reveal sensitive information.

Stage 4: Persistence

As a scam progresses, the likelihood of discovery increases. At this stage, the scammer has already invested time and effort into building and launching the scam. Now, they must prolong it by any means necessary. The scammer may use several techniques, but the focus remains on building trust. This could involve misleading the victim about the scam's intent, convincing them to make small payments under the false belief of earning rewards, or shifting conversations to different platforms to avoid detection.

Stage 5: Access

The scammer attempts to access the victim's devices with the goal of stealing private information, either with or without gaining a foothold on the device. Scammers are typically interested in data they can use directly or sell, rent, or ransom later. This includes personally identifiable information, credit card details, and bank account information. The victim's information may be accessed through theft, direct sharing by the victim, or malware. The goal of this tactic is to actively access and control the victim's information.

Stage 6: Exfiltrate

Accessing the data alone isn't enough, as it could be denied or revoked at any time. The scammer must now take possession of it. In this tactic, the scammer transfers the stolen data from the victim's device or saves the information entered by the victim on the scammer's hosted service. Exfiltration techniques can be automated or manual and may require interaction with the victim, while others can be carried out covertly.

Stage 7: Lateral Movement

Typically, the success of a scam grows with the number of victims, and scammers exploit this to increase their profits. In this tactic, the scammer spreads the scam to as many people as possible using the initial victim's environments. This can occur in several ways, such as by abusing the victim's social media accounts to reach their contacts, posting scam messages in victim-related groups, or using one account to access others. This proliferation also makes it harder for new victims to identify the true perpetrator.

Stage 8: Monetization

Scamming is a business, and profit is at the core of nearly every scammer's motive. All previous tactics lead to this point, but the scammer must take steps to avoid detection. For example, direct money transfers can be traceable, and cash transactions may be impractical. As a result, scammers often use multiple forms of monetization, including actual money, cryptocurrency, selling valuable data, assuming another person's identity, or taking advantage of premium memberships to services such as Steam without paying.

Dive deeper into the full framework here.

Research engineer specializing in complex, sustainable technologies and systems.

Non-executive board member at the Green Web Foundation, working towards a fossil-free internet.

University of Cambridge alumna with a PhD in engineering.

Dr Laura James
Vice President of Research
F-Secure

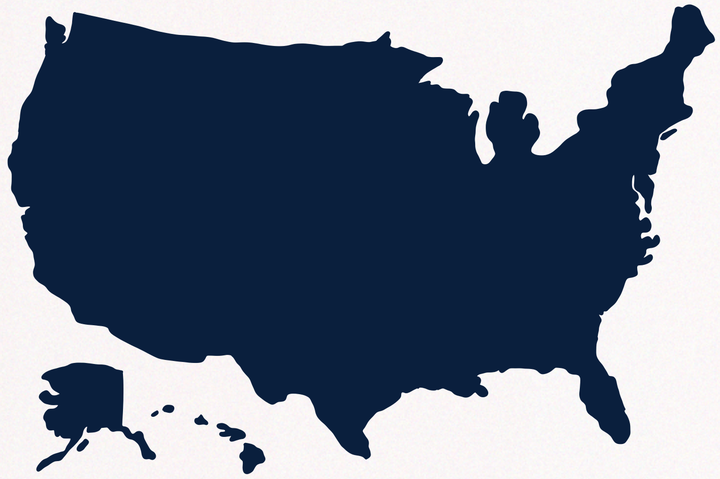
The Impact of Shifting Geopolitics on Global Cyber Crime

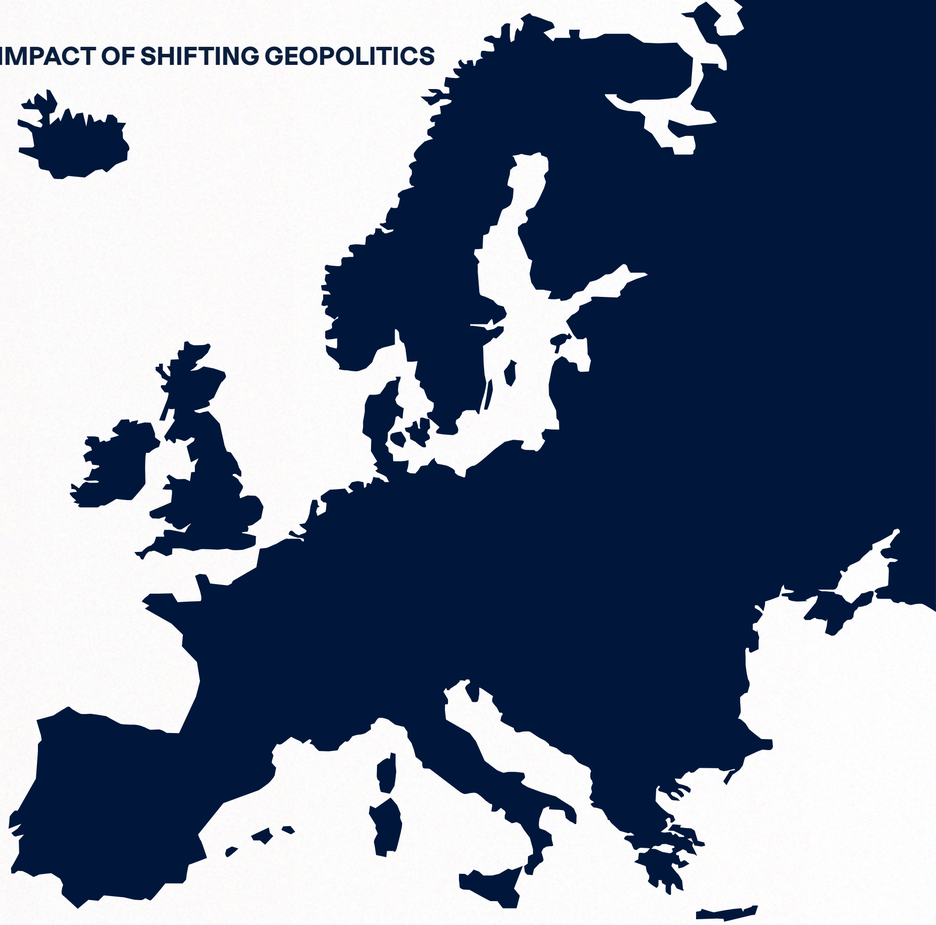
Exploring how a shifting geopolitical landscape influences scams and cyber crime—from the cost-of-living crisis to international tensions and the rise of right-wing governments.

United States

Consumer protection and financial crime enforcement are undergoing major changes in the US. The Consumer Financial Protection Bureau, an independent agency that has safeguarded consumers in the financial industry since 2011, recently lost its funding under the new administration. Meanwhile, the Internal Revenue Service (IRS) is facing budget cuts, weakening its ability to enforce financial crime laws. It remains the only federal agency authorized to investigate money laundering, currency violations, and terrorist financing.

Coupled with the growing enthusiasm for cryptocurrencies, including 'memecoins', this marks a significant shift away from consumer protections and toward a higher-risk environment. Scams may become harder to detect, recourse more difficult to find, and enforcement increasingly weakened. As a result, we can expect more scams, greater harm to victims, and less support for recovery.





Europe

In 2025, more European countries will likely roll out and adopt electronic and digital IDs, with a mandated digital wallet set to launch in January 2026. These advancements will strengthen the digital identity space, making it more secure against fraud, synthetic identities, and other forms of impersonation commonly used in scams. While challenges remain, this signals a glimmer of hope in the fight against online fraud and scams.

Critical Geopolitical Factors Driving Cyber Crime

1. Global cost of living crisis

The rising cost of living, driven by inflation in many countries, is pushing more people toward crime—including scamming others. This can create a snowball effect: once someone gets away with a scam, they're likely to try again. When others see these successful schemes, they may be more inclined to follow suit.

A secondary factor contributing to this trend is the high levels of government debt in many countries, leading to cuts in public services and benefits. As more people slip into poverty, or even just relative poverty, the temptation to engage in small-scale fraud and scamming becomes greater. Unfortunately, increasing poverty also heightens vulnerability to scams. Those who are struggling financially are more likely to seize opportunities that seem too good to be true, including scams that promise money, opportunity, affection, or hope.

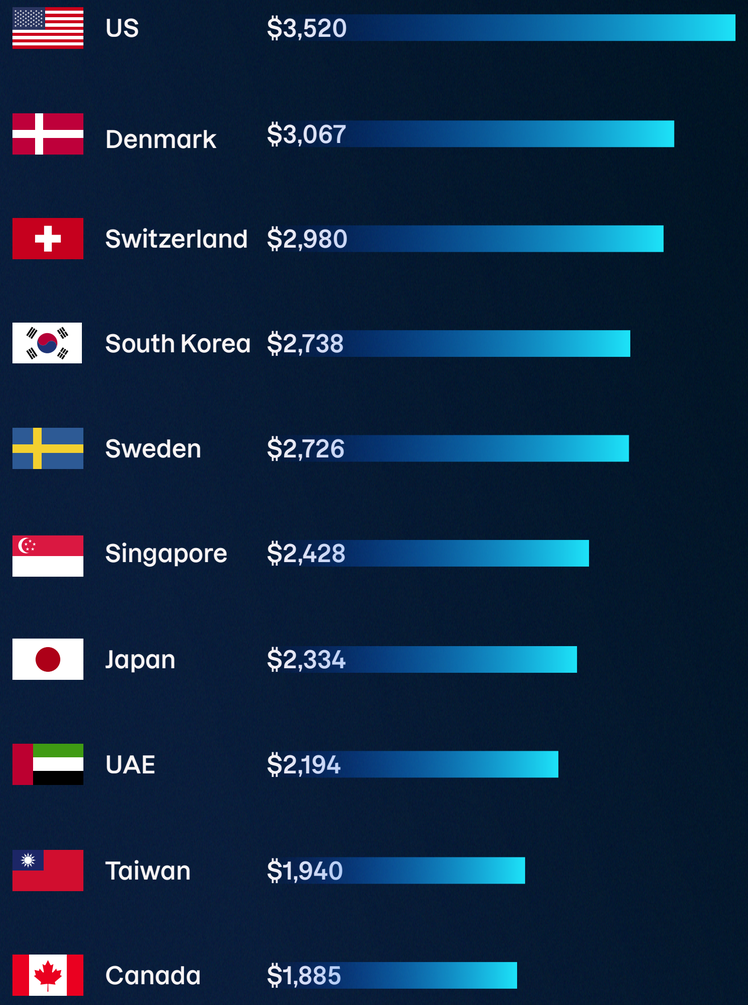
Additionally, poverty creates an increased cognitive burden. Living with limited resources is inherently stressful, and money worries can affect cognitive function. Tasks that may seem straightforward for wealthier individuals—such as shopping around for low prices or navigating complex Social Security or benefits paperwork—become time-consuming and mentally taxing for those with fewer resources. This added cognitive load makes it easier for scammers to exploit vulnerable individuals.

2. International conflicts and chaos

Global uncertainty and geopolitical tensions are at a high, with conflicts and trade wars on the rise. There is also increasing evidence of hybrid warfare—subtle 'grey-zone' attacks that exert pressure on rival states, such as disrupting economies through cyber attacks, disinformation, economic sanctions, and support for aggressive non-state actors.

Physical and cyber attacks on supply chains are becoming more common, as seen with

Average loss per victim to scams last year



Source: GASA Global State of Scams 2024

the Houthi attacks on shipping that disrupted the transport of consumer goods and components, leading to shortages. Additionally, there's some overlap in the tools used by national actors and cyber criminals, but their motivations are vastly different. For example, Russia, Iran, and China are leveraging AI to generate content for their influence operations, enhancing both reach and effectiveness.

These global stresses affect individuals in various ways. The changing information landscape, where truth and propaganda often blend, makes it harder for people to discern what's real and what's fake. This creates new vulnerabilities, making individuals more susceptible to scams.

As international tensions grow, criminal opportunities also increase. Conflicts, social unrest, and shortages create fertile ground for criminal organizations to profit. For instance, shortages of popular consumer items make people more likely to purchase from unfamiliar sources or pay inflated prices, increasing their risk of falling victim to scams.

3. Rising populist and authoritarian governments

The rise of right-wing parties is evident across multiple countries. Populist and authoritarian politicians often erode or damage critical institutions that support a healthy information environment, such as independent journalism and democratic bodies that publish essential data. Nationalist policies can also reduce international cooperation by limiting the influence or funding of organizations like the United Nations. Recent examples, such as the US pulling out of the UN Human Rights Council, illustrate this trend.

Institutions like these have traditionally helped people determine what information to trust. As they weaken without adequate replacements, informal sources step in to fill the gap—often spreading misinformation or disinformation with political or criminal intent. This makes it harder to verify facts and know which information is reliable, creating greater vulnerabilities to scams.

4. Communities under threat from disasters

The 2020s are on track to see more wars than recent decades, with conflicts rising from an average of 45 per year in the 2010s to 56 today. At the same time, climate-driven extreme weather—flooding, violent storms, unprecedented winds, landslides, and wildfires—is disrupting communities worldwide. When disaster or conflict strikes, the effects can last for weeks, months, or even permanently displace entire populations. In these moments of crisis, scammers exploit confusion, desperation, and the urgent need for assistance.

Recent events illustrate just how severe these disruptions can be. In September 2024, Hurricane Helene caused widespread flooding in North Carolina and East Tennessee, damaging infrastructure and forcing evacuations. Just a month later, Hurricane Milton followed, leaving more than 3 million homes and businesses in the US without power.

Meanwhile, in Spain, record-breaking floods hit Valencia in October and November, delivering a full year's worth of rain in just a few hours and killing more than 200 people. That same month, Canada faced one of its worst wildfire seasons on record, with more than 13.29 million acres burned across 5,000 separate fires, producing massive smoke clouds that severely impacted air quality in Canada and parts of the US.

Beyond the immediate destruction, disasters like these take an immense psychological toll. When people are in distress, they have less time and mental capacity to critically assess situations, making them more vulnerable to scams. Losing or damaging a home often means losing crucial identity and financial documents, while limited or unreliable internet access makes it harder to verify information. Scammers capitalize on this, preying on those urgently seeking help—whether from loved ones, businesses, or government agencies—by offering fraudulent assistance that only deepens their hardship.

Key Considerations:

- The shifting geopolitical landscape is undeniably fueling the growth of cyber crime on a global scale. Economic hardship, international conflicts, the rise of authoritarianism, and climate disasters all contribute to an environment where cyber attacks thrive.
- However, there's still room for optimism—as cyber threats evolve, so do our defenses. Governments, organizations, and individuals are becoming more aware of digital risks and investing in stronger cyber security measures.
- International cooperation in cyber security is also growing, with nations working together to counter cyber threats and dismantle criminal networks.
- Additionally, education and awareness initiatives across the world are empowering people to recognize scams and protect themselves.
- While the challenges of geopolitical instability are significant, resilience, innovation, and collective action remain powerful tools in the fight against cyber crime.

SCAM CSI:

5 Biggest Consumer Threats in 2025

An in-depth analysis of the five most significant scam threats currently affecting consumers, their implications, and strategies to proactively mitigate risks. Plus, a look at consumer attitudes to scams in 2025.

Threat researcher with a particular focus on scams and social media.

Regular contributor to cyber threat reports, including F-Secure's F-Alerts.

Collaborated with Laurea University of Applied Sciences to educate the public on cyber crime.

Joel Latto
Threat Advisor
F-Secure

1

Deepfakes

As generative AI advances, the skill and cost barriers to entry are rapidly decreasing—an opportunity cyber criminals are eager to exploit for scamming. Throughout 2025, AI-driven scams, including simulated phone calls and deepfake audio and videos, are expected to rise exponentially, posing a significant global threat.

Problem: AI Scales Up Scams

Criminals have long used multi-stage social engineering schemes involving direct interaction. For instance, a scammer might call a victim about a loan application and then transfer them to another person posing as a bank worker to steal banking details. These scams succeed because victims trust they are speaking with genuine, helpful people, making them more susceptible under pressure.

Previously, the scalability of such scams was limited by the scammers' ability to handle only a finite number of interactions. Now, AI is overcoming these limitations, enabling automated and highly scalable simulations of human conversations in multiple languages.

Deepfake technology allows scammers to create highly realistic and deceptive video or audio content. Using voice cloning, scammers can impersonate trusted individuals to extract money or personal information. For example, a finance worker at a multinational firm was tricked into transferring $25 million after fraudsters used deepfake technology to impersonate the company's CFO during a video conference. Believing they were speaking with colleagues—each a deepfake recreation—the worker released the funds to the scammers.

Solution: Adapting and Educating

To counter these evolving threats, consumers and service providers must adapt their defenses. Blocking call-forwarding malware, detecting suspicious numbers, and employing advanced audio analysis to identify deepfakes are essential measures. Equally important is educating individuals about common scam warning signs.

In an era dominated by AI, maintaining skepticism is critical. Consumers should always verify unexpected requests for money or personal information—even if they seem to come from trusted sources. When in doubt, they should reach out to the person directly (ideally through an alternative channel or in person) to confirm the authenticity of the request.

2

SMS Scams

Although instant messaging apps with group chats and end-to-end encryption have become the norm for many, SMS remains a favored channel for scammers. Text messages have an open rate of around 98%—far higher than emails at just 20%—and their simplicity and brevity make it easier for scammers to craft convincing fake messages compared to emails.

Problem: SMS Scams Are Versatile

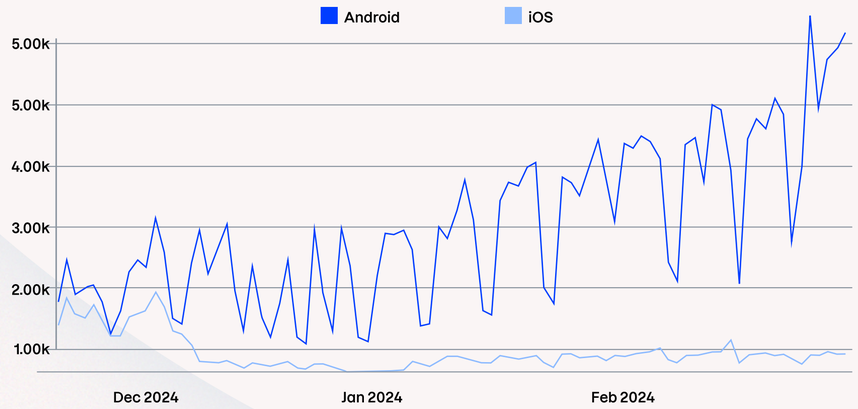
During the Covid-19 pandemic and the online shopping boom, various types of delivery scams became increasingly common. Among these, text message scams stood out due to their versatility. These scams employ a wide range of tactics, from smishing (SMS phishing) for credit card details with "failed payment" messages to impersonating banks with requests to log in to "verify your account" or "review suspicious activity".

Scammers can also spoof sender IDs in SMS spam, a problem that's harder for consumers to detect compared to email scams. Without safeguards in place (e.g. regulations in some countries requiring sender IDs to be registered to prevent others from using them), fake messages can appear in the same conversation thread as legitimate texts from banks or other organizations. Even when this doesn't occur, it's often difficult to verify the authenticity of a sender based on the sender ID alone.

Solution: AI-Enabled Messaging Protection

Banks, insurers, and telecom operators should provide information on their websites about the types of text messages they send to customers and whether those messages include links. Consumers are also strongly advised to use advanced security that understands the full context of a message, rather than just blocking known malicious URLs. Malicious text messages are an everyday problem, and F-Secure's technology blocks thousands of them daily.

Malicious messages blocked on Android and iOS by F-Secure Total



Source: Sender SMS Marketing Open Rate Statistics 2024

3

Shopping Scams

It's no surprise that shopping scams were the most common type of fraud consumers encountered last year. Cyber criminals have become increasingly sophisticated, launching realistic social media pages for fake shops, purchasing ads to appear in search engine results, and creating functional, imitation web stores complete with fake reviews. At every stage of the scam kill chain, they continue to refine their tactics, making it harder than ever to identify fraudulent shops.

Problem: Scams Hide in Plain Sight

During peak shopping periods like Black Friday or Christmas, it can be frustrating to distinguish genuinely good deals from outright scams. This uncertainty negatively impacts sellers as well—especially when well-meaning consumers mistakenly label them as scammers and start 'warning' others in the comments on social media posts.

To make matters worse, many scammers use tactics that mimic normal marketing methods—but dialed up to eleven. Most of us have seen messages like "Only 2 items left in stock!" or "Sale ends in 10 minutes!" flashing across our screens while shopping online. Impulse purchases are a goldmine for scammers, so the best defense for consumers is to pause, take a deep breath, and research the seller before buying.

Solution: Research and Verify Shops

Consumers should check a shop's URL and social media accounts before making a purchase. Do they look legitimate? Are there reviews beyond just glowing 5-star ones? Does the Terms of Service page clearly state where the shop is based and how to contact customer support? Ultimately, however, the simplest solution for consumers is to use a security app that notifies them in real time when they enter a suspicious website.

27M

shopping websites blocked by F-Secure on Windows in 2024

Source: F-Secure Digital Moments Survey 2025

4

Banking Scams

The final stage in the F-Secure Scam Kill Chain is ‘Monetization’, and some scammers waste no time targeting victims’ bank accounts to get there. While dedicated malware like infostealers once posed the biggest threat in this area, scammers are now increasingly relying on less technical—but equally effective—social engineering strategies.

Problem: Ever-Evolving Scam Techniques

Scammers often target potential victims—especially senior citizens—by posing as bank representatives and claiming that the victim must log in to their online banking and transfer funds to a ‘safe account’ to prevent fraud. Another common scam is advance fee fraud, where the scammer asks for a small upfront payment (for shipping, taxes, or documentation) before sending goods or fulfilling a promise. Banking scams may also involve phone calls from scammers pretending to be law enforcement or tech support, claiming that someone has gained illicit access to the victim’s account and requesting they download a remote access tool for assistance.

Many banking scams might seem obvious when described, but some scammers are expert con artists. With the help of AI, they can scale their operations to reach even larger audiences—trusting that no matter how crude the scam may seem, someone will fall for it.

Solution: Vigilance and Smart Practices

Consumers should always exercise extra caution when handling invoices and money transfers and make a habit of double-checking all details to ensure accuracy. Protecting their devices, especially PCs, from remote access fraud is essential. We strongly recommend that consumers keep their security software up to date.

Additionally, banks should actively educate their customers about the latest scams online. Better informed consumers are less likely to fall for banking scams.

Remote access tools blocked by F-Secure during banking sessions

5

Social Media Scams

Social media is the third most common channel for receiving scam messages, following email and SMS. What sets scams on these platforms apart is the personal approach—scammers often reach out via direct messages, promoting investment opportunities, romance, or other too-good-to-be-true offers.

Problem: Scammers Exploit Trust

These scams are popular among cyber criminals because they can be sent in bulk while still feeling more personal than a generic email. Romance baiting scams, in particular, often begin on social media platforms and are built around convincing (and often very attractive) fake profiles. Another unique aspect of social media scams is that criminals frequently use hijacked accounts to send messages. Suddenly, a shady link seems less suspicious when it comes from a trusted friend.

It's not just personal accounts that scammers are after—Facebook Pages are valuable targets too. By taking over a Facebook Page with a large audience, scammers can alter its content and use its reach to amplify scams. Worse still, if it has a credit card attached, scammers can run fraudulent ads on the Facebook network.

As early as November 2022, F-Secure warned about a phishing campaign targeting Facebook Pages under the guise of 'Facebook Support'. Variants of this same scam were still active as of late 2024, and with the help of LLM translations, it now targets Facebook Pages in multiple languages.

Solution: Be Skeptical on Social Media

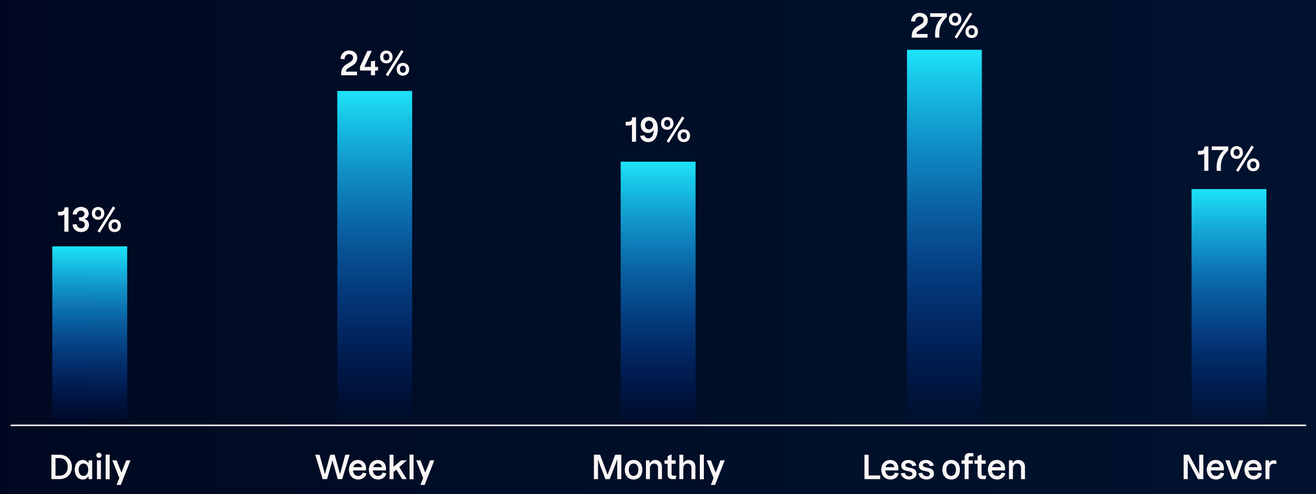
Whether it's fake ads, hijacked accounts, or unsolicited DMs, scammers are pulling out all the stops on social media. The challenges are even greater on newer platforms with less developed safety and security measures. Despite this, the old advice still applies: trust, but verify. Most 'too-good-to-be-true' offers turn out to be exactly that—not real.

Similarly, any unexpected requests involving money or payment services like PayPal or Venmo should raise immediate red flags. Good judgement serves as the first line of defense for consumers, with advanced security—either through a standalone app or embedded by their service provider—acting as the second layer of protection.

Source: F-Secure Digital Moments Survey 2025

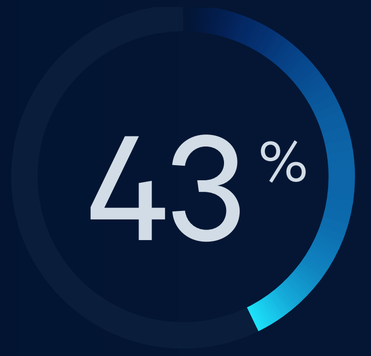
A LOOK AT CONSUMER ATTITUDES TO SCAMS IN 2025

In the last 12 months, how frequently have you encountered scams?



56% of people encounter scam attempts at least monthly

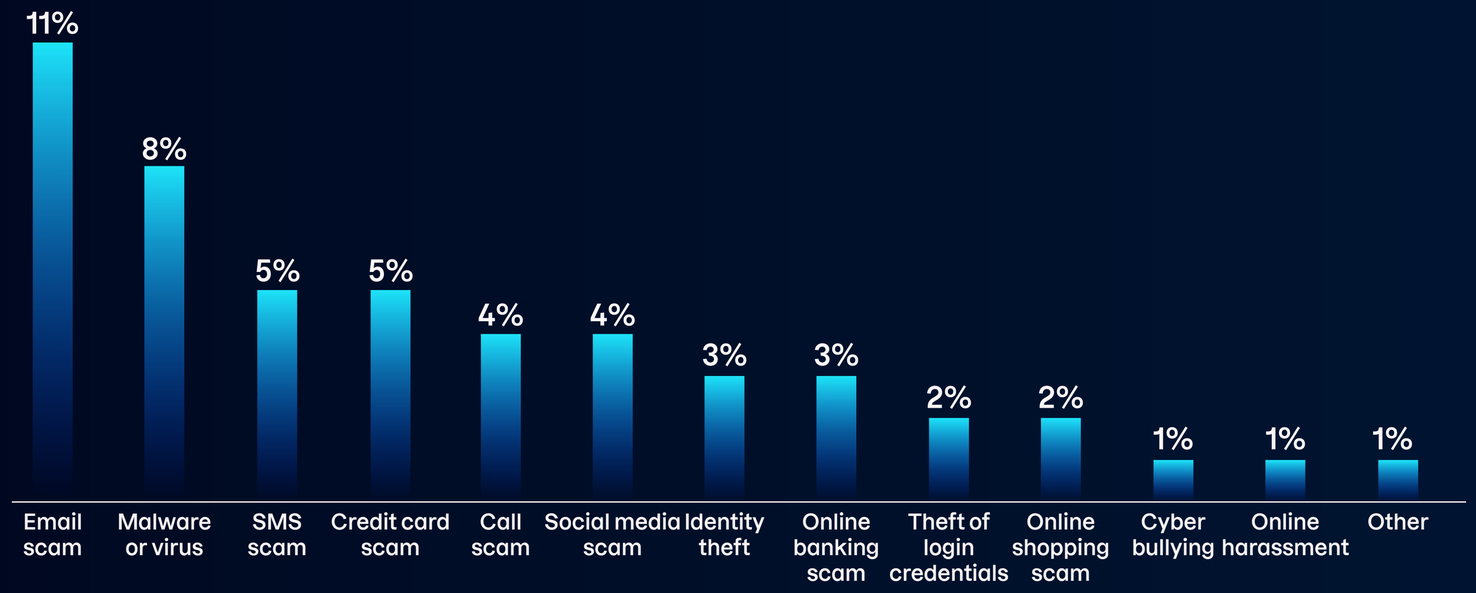
of people believe they know how to recognize an online scam

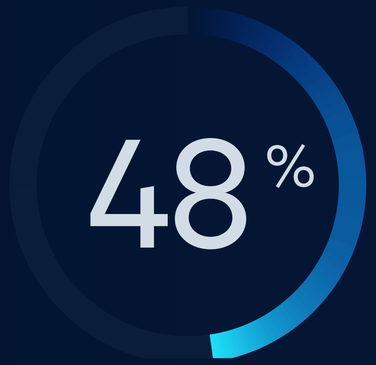


of those individuals also reported falling victim to a scam in the last year

Source: F-Secure Digital Moments Survey 2025

Have you fallen victim to some form of cyber crime in the past 12 months?





of people have fallen victim to cyber crime in the past 12 months

of people believe they are likely to fall victim to cyber crime in the future

Source: F-Secure Digital Moments Survey 2025

Key Takeaways from the Consumer Scam Landscape in 2025

56%

of consumers encounter scams at least monthly

48%

of consumers have fallen victim to cyber crime in the past 12 months

50%

of consumers believe they are likely to fall victim to cyber crime in the future

69%

of consumers believe they know how to recognize an online scam

43%

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

50%

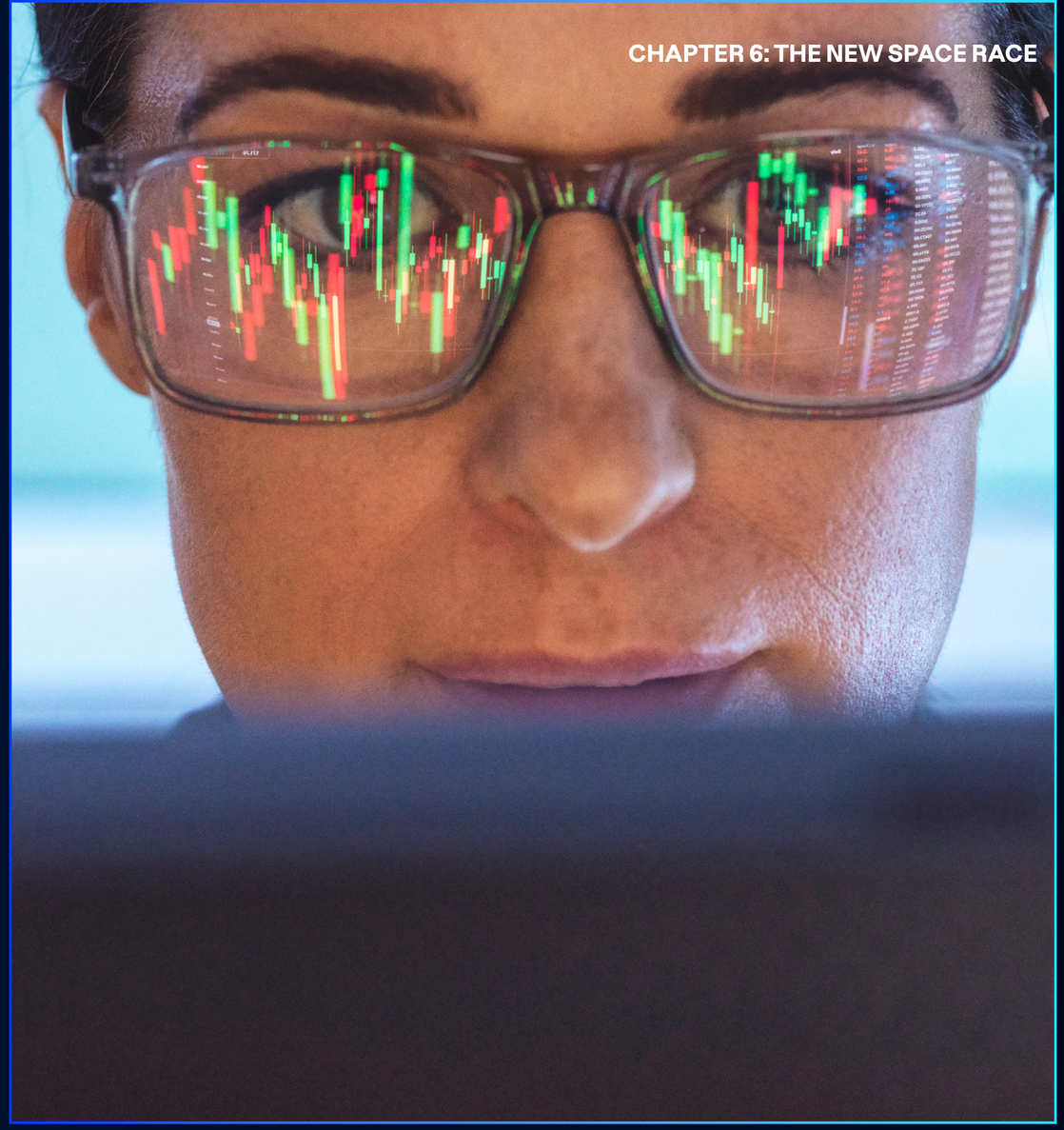
of all respondents are willing to pay for scam protection

Source: F-Secure Digital Moments Survey 2025. Countries: Finland, France, Germany, Japan, The Netherlands, Sweden, UK, USA, and Vietnam. Respondents: 9000 (1000/country), 18-75y, follows national representation of gender, region, and age category.

THE NEW SPACE RACE:

How to Adapt to Quantum Computing

An examination of quantum computing's transformative potential, focusing on its impact on security challenges and offering practical steps for service providers to prepare for the quantum era.



Quantum computing is set to transform the global cyber security landscape. Unlike traditional computers, which process data as binary bits (0s or 1s), quantum computers use quantum bits, or qubits. These qubits can represent 0, 1, or both at the same time, allowing quantum computers to perform multiple calculations simultaneously. This unique capability makes quantum computers extraordinarily powerful for solving complex problems. However, it also introduces significant risks, particularly for cyber security.

The Race for Quantum: US vs. China

While quantum computers can already be used, their capabilities currently remain limited. Nevertheless, their transformative potential has ignited a race among global superpowers.

"Much like the space race of the 20th century, this competition is about more than just technological achievement—it's about establishing dominance in a field that reshapes global power structures. The US and China are leading the charge, pouring billions into research and development to achieve quantum supremacy. However, when the first viable quantum computer comes online, it won't be televised or heralded with fanfare like the moon landing," explains Laura Kankaala, Head of Threat Intelligence at F-Secure.

This is because the stakes are so high: whoever achieves operational quantum computing first will gain unprecedented strategic and economic advantages. Global superpowers tend to treat such innovations as matters of national security, meaning much of the impact will unfold behind the scenes. Digital systems will shift in ways most users won't see directly—but the eventual effects on their lives will be profound, from cyber security disruptions to breakthroughs in technological advancement.

Ultimately, the race for quantum is a race for control over the future of information and trust. For organizations and governments, failing to prepare means falling behind in a world increasingly shaped by quantum-enabled computers. While the timeline remains uncertain—some experts predict within the next decade—there's little doubt that quantum computing will become a reality.

Quantum's Disruptive Potential: 3 Major Risks

Quantum computing has the potential to solve problems far beyond the capabilities of current computers, bringing both risks and opportunities.

1. Encryption under threat

Modern IT systems rely heavily on cryptographic protocols to secure communications, authenticate users, protect

data, and more. However, fully realized quantum computers could break these encryption methods, allowing attackers to intercept sensitive communications, forge digital signatures, and compromise online transactions. The most immediate risk lies in matters of national security—impacting infrastructure, defense, and communications worldwide.

The algorithms that protect everything from online banking to encrypted messaging would become vulnerable, meaning data could no longer be trusted to remain private, and its integrity would be in question. The solution, however, lies in post-quantum encryption—cryptographic methods designed to withstand quantum attacks. While these systems are already available, they have yet to be widely implemented. Transitioning requires careful evaluation, planning, and execution—making it a complex yet critical process.

2. Geopolitical risks

Geopolitical competition plays a major role in quantum computing's development. Nation-states investing in quantum technology may gain a strategic advantage, while others risk falling behind, creating an uneven security landscape. These dynamics could drive state-sponsored attacks, fuel cyber crime, and complicate international regulatory compliance.

3. Broader systemic risks

Digital ecosystems are expanding with the growth of connected devices, more powerful networks, and advanced servers. While nation-states are expected to leverage quantum computing first, any future commercial access to quantum technology could ultimately enable attackers to identify and exploit vulnerabilities at an unprecedented scale.

Inside F-Secure's Post-Quantum Shift

F-Secure has already implemented post-quantum encryption. We've learned the hard way that transitioning to quantum-resistant systems isn't straightforward and may bring unexpected challenges—such as browsing issues with quantum-proof cryptography in the F-Secure VPN.

The new encryption keys are larger, so they are split into two segments. The issue we encountered arose when the second segment arrived too late at the Apache Traffic Server. By delaying the first packet, it received both parts simultaneously, ensuring a smooth VPN experience.

This example highlights the importance of evaluating infrastructure readiness for post-quantum cryptography and reserving time to implement. Not all systems natively support these new standards, and the transition may require multiple steps and tailored solutions.

How to Prepare for the Quantum Era

For industries like telecommunications, banking, and insurance, the stakes are particularly high. Their reliance on secure communications and data protection makes them prime targets for quantum-powered threats. Preparing for these challenges involves several key steps:

1. **Evaluate current systems:**

Identify which systems rely on vulnerable cryptographic methods and prioritize them for updates.

2. **Adopt post-quantum encryption:**

Begin transitioning to quantum-resistant algorithms. The process is time-intensive and requires phased implementation to avoid service disruptions.

3. **Monitor legislative changes:**

Governments are increasingly recognizing the need for post-quantum standards. For example, efforts are underway globally to mandate the use of quantum-resistant encryption in critical sectors. Staying ahead of regulatory requirements is critical for maintaining compliance and avoiding penalties.

4. **Collaborate across industries:**

Addressing quantum threats will require collective action. Industries must share best practices and collaborate on the development of resilient systems.

Why Urgent Action is Critical

While quantum computing is not yet a reality, the window for preparation is narrowing. Transitioning to quantum-resistant infrastructure is a long-term effort and waiting until quantum computers are operational will leave organizations vulnerable. Encrypted data collected today could eventually be decrypted by quantum computers. Starting now not only mitigates future risks but also positions organizations to meet emerging regulatory demands.

This is the critical call to action: industries must act now to safeguard their infrastructure, protect their customers, and ensure the integrity of the systems they rely on. By embracing post-quantum encryption and preparing for the challenges ahead, service providers can turn quantum computing from a threat into an opportunity for innovation and growth.

THE COST OF DATA BREACHES:

Who Pays the Price?

An investigation into the hidden toll of data breaches—from the steps scammers take to compromise businesses to the consumers who ultimately bear the cost.

There is an abundance of online marketplaces that act as hubs for buying and selling stolen personal data, credentials, access to services, and even backdoor entry to end-user devices and browser sessions. In this underworld, where stolen data reigns supreme, the scale of data breaches is staggering, with thousands occurring annually.

How Personal Data Is Stolen and Sold

Data can be compromised by anyone. Criminals may target consumers with phishing attacks or malware to steal personal information, package it, sell it, and reap the profits. Alternatively, personal data can be obtained through a hacked business.

For criminal hackers, businesses are a goldmine. Accessing a single company's accounts can expose hundreds of thousands, or even millions, of consumer records—a far more efficient approach than targeting individuals one by one. As a result, businesses are increasingly subjected to social engineering attacks.

While companies unquestionably face the financial and legal consequences of these breaches, the true cost falls on consumers: their stolen data is sold, their identities exploited, and their money drained.

Exploiting an Organization's Weak Point

Criminals employ a variety of methods to hack businesses without direct human interaction. For example, they may identify and exploit vulnerabilities in a company's hardware or software—weak points unknown to the company and without available fixes. Attackers might also target data-driven applications such as databases, exploiting security vulnerabilities.

However, the majority of successful data breaches involve human victims through sophisticated, targeted social engineering attacks. Humans are often the weakest link in a system, and criminals exploit this by using psychological manipulation to orchestrate breaches. As detailed in the F-Secure Scam Kill Chain, social engineering attacks follow several stages, each designed to build on the previous one to ensure their success.

The Cost of Our Digital Identities

Much like eBay, 'dark web' marketplaces allow criminals to list illegal goods and services, including stolen data, with transactions typically conducted using cryptocurrencies to maintain anonymity. Stolen data is sold on publicly available forums, as well as through invitation-only forums and encrypted messaging apps like Telegram.

Data is sold on illicit marketplaces for various purposes. Some is used for further malicious activities, like spamming, while accounts directly linked to money—such as PayPal or crypto apps—can be exploited for financial gain or money laundering.

Average Prices of Stolen Data Being Sold Online

$0.50-$1	$0.90-$2	$1-$2	$1.50-$10	$80-$1,200	$400-$600	$1,000+
Meta accounts (Facebook, Instagram)	Credentials for a streaming service (Netflix, Disney+, Hulu, ESPN, Crunchyroll)	PayPal without balance	OnlyFans account with funds or linked credit card	PayPal with balance or other personal information added	Verified cryptocurrency app accounts (Kraken, Coinbase, Binance)	Verified social media accounts (Meta, TikTok)

To better understand the scale of the illicit data market, we investigated the cost of purchasing a victim's stolen personal data on these platforms. Data has a price—and the cost of disrupting consumers' lives is lower than you may think.

The affordability of stolen personal data on illegal marketplaces highlights both the scale of the problem and the urgent need for service providers to take decisive action. For just a few dollars, criminals can access sensitive consumer accounts, enabling fraud and identity theft. This affordability reflects the vast abundance of stolen data in circulation, much of which stems from poor decisions and preventable breaches.

Consequences of Personal Data Loss

Personal data isn't a physical, tangible asset, which is why many consumers don't fully understand the consequences of its theft. It's similar to managing physical cash versus online payments: cash feels more 'real', making it easier to control and manage, while contactless payments lack that tangible connection.

However, the consequences of losing personal data are very real—from financial losses and damaged credit scores to ransom demands and identity theft. The emotional toll—stress, anxiety, and a sense of violation—is significant, and consumers also face long-term vulnerability and an increased risk of future attacks.

How to Safeguard Consumer Data

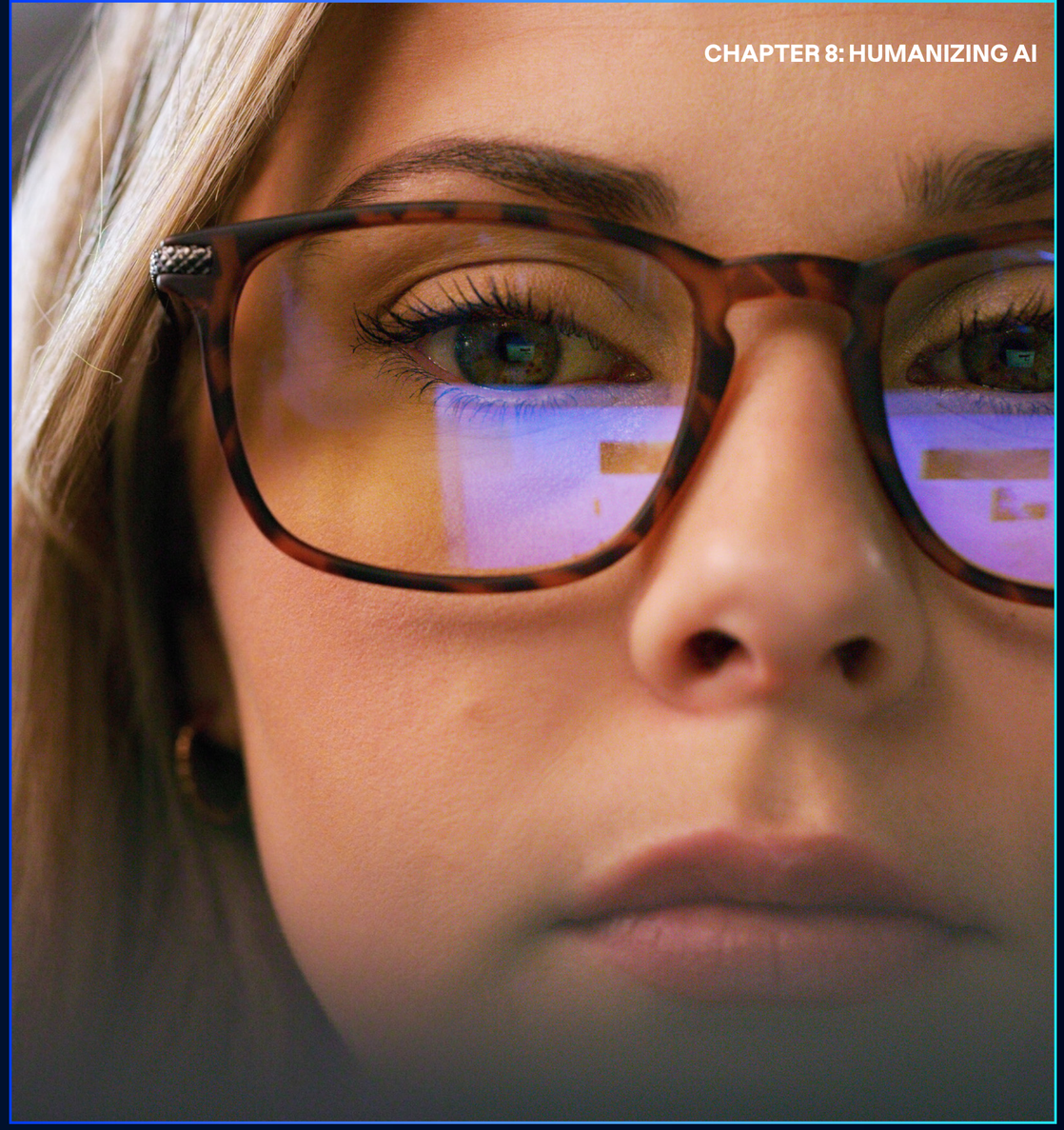
Protecting consumer data is achieved through a proactive strategy focused on prevention, detection, and response. Businesses must invest in strong security infrastructure, enforce robust authentication measures, conduct regular audits, and monitor for compromised credentials and third-party risks. Equally important is raising awareness of social engineering tactics among employees, empowering consumers to adopt better security habits, and having a solid incident response plan.

Ultimately, securing customer data is not just about compliance and responsibility—it's about building trust. Businesses that prioritize data protection are better positioned to succeed in a security-conscious consumer market.

THE NEXT FRONTIER OF DEFENSE:

The Role of Humanizing AI in the Future of Scam Protection

AI is a powerful force that can be used for good or bad. As cyber threats evolve at lightning speed, this chapter explores how humanizing AI could be the key to stronger, more intuitive scam protection.



Before November 30th 2022, artificial intelligence (AI) was still a largely futuristic and almost fanciful concept to the average person, highly glamorized by sci-fi movies and discussed at length by futurists and forward thinkers. But that all changed with the launch of Open AI's ChatGPT—a catalyst for the subsequent 'generative AI boom'.

From Notion to Novelty Almost Overnight

Now, AI has become the new normal. Chatbots and virtual assistants, or 'AI agents', support us with simple tasks. We ask large language models (LLMs) to give us comprehensive summaries of our questions instead of scrolling through search engines. Code is created—and data augmented—faster than ever before.

Like the internet, AI is fulfilling its promise to revolutionize how we interact with and perceive the modern world. However, as this technology enriches, expands, and streamlines our daily lives, there's also a darker side to its advancement. The rise of generative AI has made scams more effective in nearly every way: they're easier to create, faster to deploy, and harder to detect.

Technical Skill Is No Longer a Barrier

"In 2025, scammers no longer need to be tech-savvy to succeed. Instead, the internet now provides them with the tools, knowledge, and training to steal our data, money, and more," explains Laura Kankaala, Head of Threat Intelligence at F-Secure.

"Thanks to AI, creating convincing content for scams has never been easier. Today's scammers don't need to ask themselves, 'Can I do it?'—they simply ask, 'Do I want to?'"

Laura Kankaala
Head of Threat Intelligence
F-Secure

Living in the Age of AI

March 2024:
NVIDIA releases its Blackwell chip, raising the bar with advanced GPU microarchitecture to underpin AI training and research.

March 2024:
The European Union passes the AI Act, the first legal framework aimed at ensuring AI respects human rights.

September 2024:
OpenAI introduces their ‘o1 model’, codenamed ‘Strawberry’. Unlike GPT-4, which prioritizes speed, this model allocates more power to complex tasks, significantly improving reasoning and decision-making capabilities.

October 2024:
Apple launches ‘Apple Intelligence’ for iPhone 15, enabling Pro and Pro Max users to summarize documents, create custom emojis, personalize messages, and more.

January 2025:
DeepSeek, an AI chatbot developed by Chinese company DeepSeek, is officially launched. By January 27th, DeepSeek surpassed ChatGPT to become the most downloaded free app on the US iOS App Store.

February 2025:
Sam Altman, CEO and Founder of OpenAI, rejects an offer from Elon Musk to buy OpenAI for $97.4 billion.

Dr Laura James
Vice President of Research
F-Secure

AI's Advancement Comes at a Price

AI is a powerful technological breakthrough, but when misused, its impact can be significant and damaging. Dr Laura James, Vice President of Research at F-Secure, explores the key forces driving AI's rapid evolution and examines its broader implications.

"Alan Turing predicted the era of 'machines that think' in his 1950 paper, Computing Machinery and Intelligence. Today, we may be starting to see this materialize—and not just through ChatGPT or other LLMs and AIs," James explains.

"It's being made possible by our entire computing infrastructure—devices, networks, systems, computers, phones, apps, the web, and even hidden data systems we rarely consider. Combined, these enable new capabilities that may rival or exceed human skills in some tasks. LLMs exist because they have been trained on vast amounts of information—much of it created by people over many years, both online and offline (and then digitized). It's this interconnected web of data that fuels today's wave of generative AI".

But AI's advancement is not without cost. "Even though many end user tools seem free to users, the energy demands to create and operate these models are enormous—and growing rapidly," she continues. "This doesn't just mean high electricity bills. Data centers may strain power grids, exceed the capacity of renewables and storage, increase the carbon intensity of electricity generation, and impact local water sources for cooling".

Then there are the broader concerns surrounding generative AI. "Issues range from biased models and outputs reflecting inappropriate or outdated cultural views, to models built on incomplete or incorrect information. There's also excessive surveillance, the risk of unwanted deployment, and the extractive nature of AI technologies—exploiting creative and informational labor by paid people and unpaid individuals over many years".

"While AI's advancement is a significant shift in how we perceive and shape the world, it's important to recognize both its driving infrastructure and wider impact," James concludes.

Source: MIT News 'Explained: Generative AI's environmental impact' 2025

AI'S ORIGINAL VISION:

Has It Lost Its Way?

Over the past two and a half years, AI has increasingly been shaped by the priorities of large enterprises—focused on cutting costs, driving efficiency, and integrating new capabilities into products, software, and tools. Yet, looking back, we see that the original vision for this technology was deeply rooted in human-centric aspirations.

"Early visions of AI agents served individual users, empowering regular people with computer support that would act in their interests, under their control, and perhaps even with their own design," explains Laura James. "What we've ended up with, though, are huge AI platforms owned and operated by the most powerful companies on the planet".

"Yes, ChatGPT or Claude respond to my prompts," she continues. "But they are trained on a mass of internet content and optimized for the needs of the companies who operate them. They aren't trained on information I have confidence in, or towards my goals. They don't help me autonomously—I must guide them with prompt engineering to help me. So, it feels like we are not yet realizing those early visions".

1950

Alan Turing's Foundational Question:
In 1950, British mathematician Alan Turing asked, "Can machines think?" in his seminal paper, Computing Machinery and Intelligence. He introduced the Turing Test to determine whether a machine could exhibit intelligent behavior indistinguishable from that of a human.

1956

John McCarthy's Contribution:
In 1956, computer scientist John McCarthy coined the term 'artificial intelligence' and envisioned machines that could mimic human reasoning and solve complex problems independently.

1987

Apple's Knowledge Navigator:
In 1987, Byte magazine described Apple's 'Knowledge Navigator', which conceptualized earlier visions of AI agents serving individual users. Byte wrote: "The Navigator, which is not a reality yet, will be a portable computer that will combine multimedia databases with artificially intelligent agents. An agent could search through incoming and stored information and suggest nuggets of interest to the individual user, using previous inquiries and work as a guide".

2015

Open AI's Mission Statement:
In 2015, OpenAI, the generative AI trailblazer founded by Sam Altman, emphasized its commitment to human advancement in its mission statement: "Our mission is to ensure that artificial general intelligence benefits all of humanity".

Harnessing AI as a Trusted Companion

TL Viswanathan, Chief Product Officer at F-Secure, explains how we can harness AI as a trusted companion to protect consumers in their everyday lives from the dangers of scams.

AI's integration into modern society brings both immense rewards and vast complexities. While we don't condemn its use in improving corporate processes, there is value in reimagining the human-centric vision championed by its forebears—especially when it comes to protecting consumers' digital moments amidst the rise of scams.

"Scams aren't just evolving, they're exploding. They're smarter, faster, and nearly impossible to detect. The wide availability of generative AI has certainly contributed to this, but we can turn this on its head, using this technology to make everyday interactions and digital moments safer for consumers worldwide," Viswanathan explains.

"At F-Secure, our approach—and vision—for how we use AI for scam protection is that we want to be a trusted companion to the user. This isn't just about protection capabilities; it's about the user experience and how we can bring a sense of security into people's lives," he continues.

This begins with holistic protection across the scam kill chain. "We want to prevent, protect, and, in rare cases, help consumers recover from the impact of scams," says Viswanathan. "Prevention is key: by enabling users' privacy to remain invisible online and providing contextual, personalized, and well-timed information, we can prevent users from ever making it onto the target list. For example, informing users that a shopping site is a scam can prevent them from falling victim".

While it's true that harnessing the power of AI is not a new concept for cyber security companies, F-Secure's scam protection technology uses AI to take an in-the-moment approach to protection. "We are reimagining the security experience for consumers, acting as their trusted companion by providing real-time, contextual, and seamless scam protection—rather than relying on them to protect themselves," Viswanathan concludes.

Putting the People Back in AI-Powered Protection

Scams are rife, and consumers are already looking to the service providers they know and trust to protect them. In fact, 81% of consumers trust mobile or broadband operators to provide their internet security, while 71% trust their insurance companies. By harnessing AI as a trusted companion for effective consumer scam protection, we are bringing the vision of using technology for good to life—helping everyday people, everywhere.

"We want to prevent, protect, and, in rare cases, help consumers recover from the impact of scams."

TL Viswanathan
Chief Product Officer
F-Secure

Source: F-Secure Consumer Market Research 2023

Understanding the Risks of an Expanding Connected Home

Bill Lott, Head of Marketing, Embedded Solutions at F-Secure, discusses the increasing security risks consumers face as the number of Internet of Things (IoT) devices in our homes grows.

Q With the average US household now having 17 IoT devices, what are the biggest implications of this expanding network?

A As the number of IoT devices connected to home networks grows, so do the security, privacy, and usability risks for consumers.

Each new device expands the attack surface, offering cyber criminals more entry points.

Without proper security, every added device increases the risk of exploitation. Furthermore, the cloud systems managing these devices—each requiring its own login and user profile—provide more opportunities for hackers to gain access.

Privacy is another major concern. In today's digital world, data is a valuable currency. Every connected device generates data, yet

Source: Parks Associates 2024

most consumers are unaware of the privacy policies that govern them—and lack the agency to do much about it. As the number of devices grows, so does the amount of data collected on household habits. To help protect privacy, router-based security with ad-tracking blockers is highly recommended.

The growing smart home ecosystem also creates complexity due to different platforms. While companies like Apple have developed systems to manage connected devices, most manufacturers rely on their own cloud-based solutions. This leads to multiple logins, passwords, and platforms that often don't integrate seamlessly, making it harder to create a truly 'smart' home. Additionally, more connected devices require more frequent software updates to address security vulnerabilities and emerging threats.

Q What potential dangers arise as the number of connected devices grows?

A There are three key risks associated with each IoT device added to a home network.

First, every additional device creates another entry point for cyber attackers. Hackers often target devices with unpatched vulnerabilities, gaining access to one device and potentially compromising others on the network. Second, once hackers infiltrate a device, they can use it to steal data, insert malicious code, or even co-opt the device for large-scale botnet attacks—often without the owner's knowledge.

Finally, many users reuse the same email, username, and password across multiple cloud applications on their devices. This increases the risk of a data breach. Leaked credentials can be exploited to access other cloud services, giving hackers valuable information for highly targeted scams.

Q How does a vulnerable IoT device in a consumer's network make them a target for cyber attacks?

A Cloud login credentials and account profiles are often at risk of data breaches or theft. Once stolen, these credentials can be sold on the black market, providing hackers with valuable information for future targeted scams.

For instance, knowing a consumer owns a specific device, attackers can send an urgent email pretending to be from the device manufacturer, asking for sensitive information. Alternatively, a tech support scam could be launched, leveraging the knowledge and control over the consumer's device.

If the device itself is compromised, skilled hackers could gather even more personal data, which could then be used to craft more convincing and personalized scams.

Q Which IoT devices are commonly considered the 'weak link' in a connected home?

A Many smart devices—such as audio equipment, printers, routers, smart lighting, game consoles, storage devices, locks, sensors, and large appliances like refrigerators—are often manufactured without prioritizing security features. This makes them vulnerable for several reasons: their widespread presence in home networks, the likelihood that they remain unpatched, and the fact that security is often not a primary focus for manufacturers leaves these devices open to potential threats.

Q What are the implications for consumers when IoT devices reach their end-of-life?

A The main challenge for consumers is staying informed about which devices have reached their end-of-life. When devices stop receiving updates to patch vulnerabilities, consumers are left exposed to security risks. While the shutdown of cloud infrastructure isn't typically a major concern, as it can reduce attack vectors, there is still the possibility that a skilled hacker could find a way to 'take over' the infrastructure and exploit it for malicious purposes.

Recommendations for long-term IoT device security

In an increasingly connected world, IoT device manufacturers must adopt long-term strategies to ensure strong security, user privacy, and device longevity.

The first step is prioritizing security by design. By integrating security features into product development and considering hardware and software lifecycles together, manufacturers ensure that security is a foundational element, not an afterthought.

Equally important is designing products with robust authentication, such as multi-factor authentication, and enforcing strict access controls to prevent unauthorized access. Automatic firmware and software updates should be implemented as the industry standard—rather than opt-in—to address emerging vulnerabilities. Additionally, there should be transparency about the device's lifespan from the moment of purchase.

Communication service providers can also easily protect every IoT and smart device in their customers' connected homes by offering F-Secure Sense router-based security to defend against cyber threats.

2024 VS. 2025

Cyber Threat Predictions

A review of last year's cyber threat predictions from F-Secure threat intelligence experts, along with their insights on what's ahead for 2025.

Laura Kankaala
Head of Threat Intelligence
F-Secure

2024 PREDICTION

Scams Will Be a Unique Problem for Consumers

Last year, Kankaala predicted that scams would become the leading method for consumer-focused cyber attacks. She warned that they would pose an even greater threat to consumers' online lives by combining manipulation tactics with advanced technologies like AI to target specific groups, such as busy professionals and those without adequate cyber protection. She also anticipated the rise of real-time AI-driven scams using fake voices and images, warning that these would significantly enhance scam effectiveness.

What happened?

Scams became the primary method of consumer-focused cyber attacks, with criminals increasingly leveraging AI to enhance their tactics. While awareness of AI-driven scams is growing, GASA data shows that one-third of people are still unsure whether AI played a role in their scam encounters.

Highly targeted phishing attacks and scams have become more prevalent, with threat actors using voice cloning to impersonate victims' family members or colleagues. Deepfake videos of celebrities and well-known figures have also emerged as a common theme in romance scams worldwide.

Businesses have also fallen victim to real-time deepfake scams. In May, it was reported that the CEO of the world's largest advertising group was impersonated in a Microsoft Teams meeting using advanced deepfake and voice cloning technology. This is just one of many instances where attackers have exploited virtual meetings.

2025 PREDICTION

Scams Will More Closely Mirror Traditional Crime

Organized crime has become more prominent on the internet in recent years. Call and scam centers have long plagued people worldwide, but the worrying trend is that online scams are starting to resemble traditional crimes, including money laundering, human trafficking, and the recruitment of 'gang' members. Online crime groups can reach their full potential by establishing operations in countries with high corruption rates and using cryptocurrencies to transfer money globally. This trend will continue into 2025, as scams increasingly resemble classic forms of crime.

Tom Gaffney
Director of Business Development
F-Secure

2024 PREDICTION

AI Will Fuel an Evolution in Smart Home Attacks

Last year, Gaffney predicted that attackers would build on their previous targeting of smart home devices, noting that the rise of AI-enabled products like Amazon's Alexa and Echo—designed to streamline our daily lives—would increase the level of intimacy we share with these devices, making them more attractive targets for motivated attackers.

What happened?

Cyber attacks on smart home devices surged, exposing critical vulnerabilities in connected ecosystems. Meanwhile, consumer Wi-Fi devices remained prime targets, putting home networks at greater risk.

One major incident saw over 576,000 Roku accounts compromised through credential stuffing, exploiting users who reused passwords across multiple services. The rising number of IoT devices, such as smart TVs, has expanded the attack surface for criminals—especially as many lack robust security features.

By August, CISA warned that cyber criminals were exploiting misconfigured Cisco devices, including the legacy Smart Install feature, to hijack switches. Critical flaws in Cisco IP Phones were also found but won't be patched due to end-of-life status.

In October, hackers exploited a flaw in Ecovacs Deebot X2 Omni robotic vacuums, letting them bypass PIN entry to control the devices, chase pets, and yell slurs.

2025 PREDICTION

Regulator-Retailer Privacy Battles Will Intensify

In 2025, Gaffney expects social media and shopping giants to adopt new tactics to sidestep growing regulatory pressures, particularly on children's data collection. Recent EU fines against Meta, TikTok, and X have put companies like Amazon and Temu, whose business models rely on user profiling, under increased scrutiny.

As regulators push for stronger protections—especially for children—some governments, like Australia, plan to restrict teens' access to social media. However, a balance must be struck between protecting children's privacy and allowing them to explore the digital world. Collaboration between governments and tech companies is essential to provide security tools and educate both parents and children about cyber risks.

Joel Latto
Threat Advisor
F-Secure

2024 PREDICTION

AI-Enabled Threats Like Deepfakes Will Become Serious

Last year, Latto predicted that 2024 would mark a turning point in AI-enabled threats, as generative AI tools like ChatGPT and DALL·E became increasingly integrated into daily life for both consumers and scammers. He anticipated that scams and phishing attempts would become nearly impossible to detect due to flawless AI-generated visuals, copy, and messaging. He also warned of the growing complexity of the global threat landscape, with deepfake and vishing technologies posing risks on a much larger scale.

What happened?

Criminals used generative AI to create convincing visuals and messages, driving a surge in AI-powered attacks against consumers and organizations.

In March, a mother almost lost SEK 15,000 after receiving a call with her daughter's voice urging her to send money—however the voice was replicated by scammers.

Scammers also used deepfake audio and video to impersonate financiers, while AI-generated phishing emails targeted individuals and AI-generated websites mimicked multinational companies, tricking victims into transferring funds.

In late 2024, threat actors targeted employees of organizations using Microsoft 365, spamming them with phishing emails before following up with vishing calls on Teams, posing as tech support to gain remote access and deploy malware.

Wall Street has also warned that scammers are using AI to create fake IDs for opening fraudulent brokerage accounts or hijacking existing ones.

2025 PREDICTION

Scammers Will Use AI to Simulate Phone Calls at Scale

In 2025, Latto predicts that scammers will leverage sophisticated AI chatbots and deepfake audio to create scalable, human-like interactions in multiple languages, making call-based scams far more dangerous than traditional robocalls. AI removes the scalability limitations of social engineering schemes, enabling criminals to simulate genuine phone calls at an unprecedented rate.

To counter these evolving threats, defenses must adapt. Blocking call-forwarding malware, detecting suspicious numbers, and using advanced audio analysis to spot deepfakes are critical. Collaboration among security experts, telecoms, and regulators, alongside user education on scam warning signs, will be essential to stay ahead of attackers.

Sarogini Muniyandi
Senior Manager,
Scam Protection Engineering
F-Secure

2025 PREDICTION

Scammers Will Exploit Rising DeFi Investments

In 2025, Sarogini expects Decentralized Finance (DeFi) to attract more users as an alternative to traditional banking. However, she warns that its unregulated, anonymous nature makes it a prime target for scammers preying on those new to blockchain and digital assets like Bitcoin.

DeFi platforms promise high-yield investments and loans, but as their popularity grows, the increasing total value locked in these projects makes them vulnerable to large-scale fraud. The absence of regulatory oversight further amplifies these risks. While DeFi offers financial freedom and profit potential, its vulnerabilities make it a hotspot for scams—something Bitcoin investors must remain cautious of in 2025.

Calvin Gan
Senior Manager,
Scam Protection Strategy
F-Secure

2025 PREDICTION

Companies Will Be Penalized for Failing to Prevent Scams

In 2025, Gan expects global lawmakers to increase pressure on telecom operators, banks, and social media companies to take responsibility for protecting customers from fraud. New bills in Australia and the UK already hold companies accountable, with penalties for failing to prevent scams and mandatory reimbursement for victims in some cases.

While these legislative efforts will strengthen scam protections, businesses must collaborate with governments and consumers to combat fraud effectively. No legislation can prevent scams entirely, so consumers must remain vigilant, especially on high-risk platforms like social media and messaging apps.

Sources and Methodologies

Chapter 2 – How the Online Scam Landscape is Evolving in 2025

- GASA Global State of Scams 2024, https://www.gasa.org/research
- The World Economic Forum, 'Partnerships are our best weapon in the fight against cybercrime' 2020, https://www.weforum.org/stories/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/
- F-Secure Digital Moments Survey 2025. Countries: Finland, France, Germany, Japan, The Netherlands, Sweden, UK, USA, and Vietnam. Respondents: 9000 (1000/country), 18-75y, follows national representation of gender, region, and age category
- F-Secure blocked shopping websites data 2024-2025
- BBC, 'AI Brad Pitt dupes French woman out of €830,000' 2025, https://www.bbc.co.uk/news/articles/ckgnz8rw1xgo
- F-Secure scam protection data 2024-2025

Chapter 3 – From Hook to Heist: Inside the Scam Kill Chain

- F-Secure Scam Kill Chain 2025, https://www.f-secure.com/en/partners/scam-protection/scam-kill-chain. This work is inspired by the MITRE ATT&CK® Matrix for Enterprise; however, instead of mapping cyber security threats to organizations, it focuses on threats to consumers' online accounts, devices, and data

Chapter 4 – The Impact of Shifting Geopolitics on Global Cyber Crime

- The Wall Street Journal, 'Funding Cuts at CFPB Seen Leading to 'Regulatory Vacuum' for Big Banks' 2025, https://www.wsj.com/articles/funding-cuts-at-cfpb-seen-leading-to-regulatory-vacuum-for-big-banks-481a3ce3
- European Commission, 'The EU Digital Identity Framework Regulation Enters into Force' 2024, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+Digital+Identity+Regulation+Enters+into+Force
- GASA Global State of Scams 2024, https://www.gasa.org/research
- VOA News, 'US withdrawal from UN human rights body draws mixed reactions' 2025, https://www.voanews.com/a/us-withdrawal-from-un-human-rights-body-draws-mixed-reactions/7971418.html
- Vision of Humanity, 'Highest number of countries engaged in conflict since World War II', https://www.visionofhumanity.org/highest-number-of-countries-engaged-in-conflict-since-world-war-ii/
- Project HOPE, 'Hurricanes Helene & Milton: A Visual Timeline' 2024, https://www.projecthope.org/news-stories/story/hurricane-visual-timeline/
- BBC, 'Canada wildfire season is now the worst on record' 2024, https://www.bbc.co.uk/news/world-us-canada-65816466

- World Meteorological Organization, ‘Devastating rainfall hits Spain in yet another flood-related disaster’ 2024, https://wmo.int/media/news/devastating-rainfall-hits-spain-yet-another-flood-related-disaster

Chapter 5 – Scam CSI: 5 Biggest Consumer Threats in 2025

- CNN, ‘Finance worker pays out $25 million after video call with deepfake chief financial officer’ 2024, https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/
- Sender SMS Marketing Open Rate Statistics 2024, https://www.sender.net/blog/sms-open-rates/
- F-Secure Total blocked malicious messages on Android and iOS data 2024-2025
- F-Secure remote access tools blocked during banking sessions data 2024-2025
- F-Secure Digital Moments Survey 2025. Countries: Finland, France, Germany, Japan, The Netherlands, Sweden, UK, USA, and Vietnam. Respondents: 9000 (1000/country), 18-75y, follows national representation of gender, region, and age category
- F-Secure F-Alert November 2022, https://www.f-secure.com/en/partners/insights/2022-11-sharkbot-android-malware-returns

Chapter 7 – The Cost of Data Breaches: Who Pays the Price?

- F-Secure Threat Intelligence data, average prices of stolen data being sold online in 2025

Chapter 8 – The Role of Humanizing AI in the Future of Scam Protection

- NVIDIA News, ‘NVIDIA Blackwell Platform Arrives to Power a New Era of Computing’ 2024, https://nvidianews.nvidia.com/news/nvidia-blackwell-platform-arrives-to-power-a-new-era-of-computing
- European Parliament News, ‘Artificial Intelligence Act: MEPs adopt landmark law’ 2024, https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law
- OpenAI, ‘Introducing OpenAI o1’ 2024, https://openai.com/o1/
- Apple Newsroom, ‘Apple Intelligence is available today on iPhone, iPad, and Mac’ 2024, https://www.apple.com/uk/newsroom/2024/10/apple-intelligence-is-available-today-on-iphone-ipad-and-mac/
- BBC, ‘DeepSeek: The Chinese AI app that has the world talking’ 2024, https://www.bbc.co.uk/news/articles/c5yv5976z9po
- WIRED, ‘Sam Altman Dismisses Elon Musk’s Bid to Buy OpenAI in Letter to Staff’ 2025, https://www.wired.com/story/sam-altman-openai-reject-elon-musk-bid/
- MIT News, ‘Explained: Generative AI’s environmental impact’ 2025, https://news.mit.edu/2025/explained-generative-ai-environmental-impact-0117
- A.M. Turing, ‘Computing Machinery and Intelligence’ 1950
- J. McCarthy, ‘Dartmouth Summer Research Project on Artificial Intelligence’ 1956
- Byte Magazine, ‘The Navigator: A glimpse of the future of computing’ 1987
- OpenAI, ‘Introducing OpenAI’ 2015, https://openai.com/index/introducing-openai/

Chapter 9 – Understanding the Risks of an Expanding Connected Home

- Parks Associates, ‘Average U.S. Internet Home Had 17 Connected Devices in 2023’ 2024, https://www.parksassociates.com/blogs/in-the-news/parks-average-us-internet-home-had-17-connected-devices-in-2023

Chapter 10 – 2024 vs. 2025 Cyber Threat Predictions

- Entrepreneur, ‘Hackers Try Steal Money, Personal Information from Executives at the World’s Largest Advertising Company Using a Deepfake of the CEO’ 2024, https://www.entrepreneur.com/business-news/wpp-ceo-impersonated-in-deepfake-scheme-to-steal-execs-money/474065
- Security Affairs, ‘Roku disclosed a new security breach impacting 576,000 accounts’ 2024, https://securityaffairs.com/161765/data-breach/roku-second-data-breach.html
- The Record, ‘Cisco warns of critical vulnerabilities in routers’ 2024, https://therecord.media/cisco-warns-of-critical-vulnerabilities-in-routers
- The Verge, ‘Hackers took over robovacs to chase pets and yell slurs’ 2024, https://www.theverge.com/2024/10/12/24268508/hacked-ecovacs-deebot-x2-racial-slurs-chase-pets
- F-Secure F-Alert March 2024, https://www.f-secure.com/en/partners/insights/2024-03-criminals-phishing-in-plain-sight
- Tech Target, ‘Threat actors abusing Microsoft Teams in ransomware attacks’ 2025, https://www.techtarget.com/searchsecurity/news/366618294/Threat-actors-abusing-Microsoft-Teams-in-ransomware-attacks
- The Wall Street Journal, ‘GenAI Increasingly Powering Scams, Wall Street Watchdog Warns’ 2025, https://www.wsj.com/articles/genai-increasingly-powering-scams-wall-street-watchdog-warns-a6592d54

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