US Scam Intelligence & Impacts Report

Critical insights into emerging consumer scam trends for US service providers.

Contents

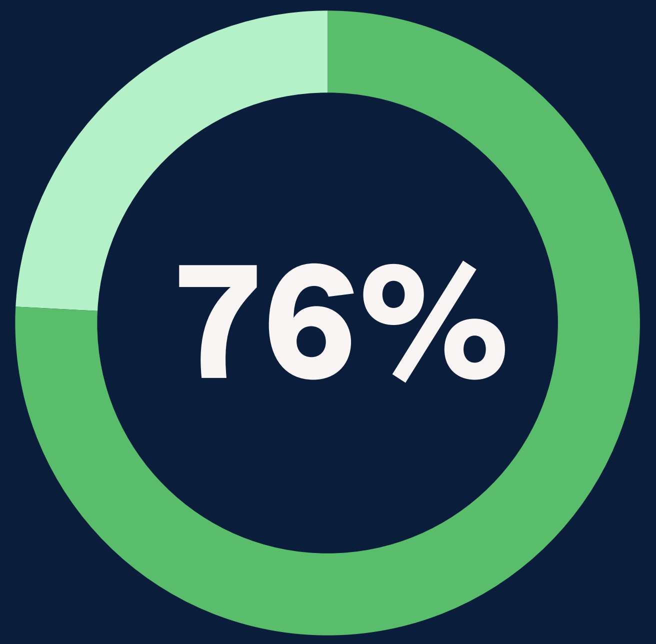
Key report highlights

$159 billion

was lost to scams in the US last year

*Source: GASA The Global State of Scams 2023

7 in 10 don't know who to trust online



of Americans worry about their online safety

of Americans received a digital scam attempt in 2023

AI has enhanced the effectiveness and scale of scams

Gen-Z

is 3 times more likely to fall victim to online scams worldwide (37%) than those aged 55 and above (12%)

Top 3 vulnerable online moments for consumers:

1. Paying bills
2. Online medical consultation
3. Online shopping

Top 3 scam attempts in 2023:

1. Online shopping scams
2. Investment scams
3. Fake invoice/debt scams

Who consumers consider trusted providers of internet security globally:

81% Carriers

71% Insurance companies

*Source(s): F-Secure Living Secure Survey 2024, F-Secure Consumer Market Research 2023

How do we tackle the scam pandemic?

"Legislation and government action are important, but they can only fix so much. The law is only followed by the law-abiding, and scammers will always throw out the rulebook when it comes to using modern technology to their advantage. Ultimately, it's up to us to take back our power and protect ourselves by combining education, best practices, vigilance, expertise, and technology. While we're in some way married to the devices that enable our digital moments, we must make sure we're doing what's needed to protect them too."

Laura Kankaala
Head of Threat Intelligence
F-Secure

The US scam landscape

Scammed. Swindled. Tricked. Cheated. Conned. These words all capture the same harsh reality: the pain of betrayal and theft online. Scamming, though not new, has become more effective with modern technology. And as data reveals, it's unfortunately here to stay.

In 2023, scams cost the US $159 billion, with 23% of US consumers falling victim to scams in just one year. The average loss per consumer was $2,663. As our lives become increasingly digitalized – with 70% of Americans shopping online, 66% using online banking, and 17% engaging with dating apps in 2023 – scammers are exploiting our growing reliance on many digital platforms.

Today, 3 in 4 Americans encounter scams monthly. It's clear that scamming is a nationwide issue – one that demands urgent and unified action.

F-Secure and Global Anti-Scam Alliance (GASA)

As scam rates escalate, F-Secure's partnership with GASA is committed to addressing this rising threat by uniting governments, law enforcement, and consumer protection organizations. By sharing expertise and coordinating efforts, we aim to enhance scam protection and forge a safer digital future, safeguarding consumers from both financial and emotional harm.

*Source(s): GASA The Global State of Scams 2023, Statista 2024

How safe do US consumers feel online?

Amidst the AI revolution, the global impact of scams has surged – affecting victims not only through financial losses, but also through the theft of personal details and data, the loss of valuable time, and heightened stress and concern. Our Living Secure survey highlights the prevalence of cyber crime today and underscores a critical issue: increasing concerns about trust and safety online are significantly impacting consumers' digital experiences.

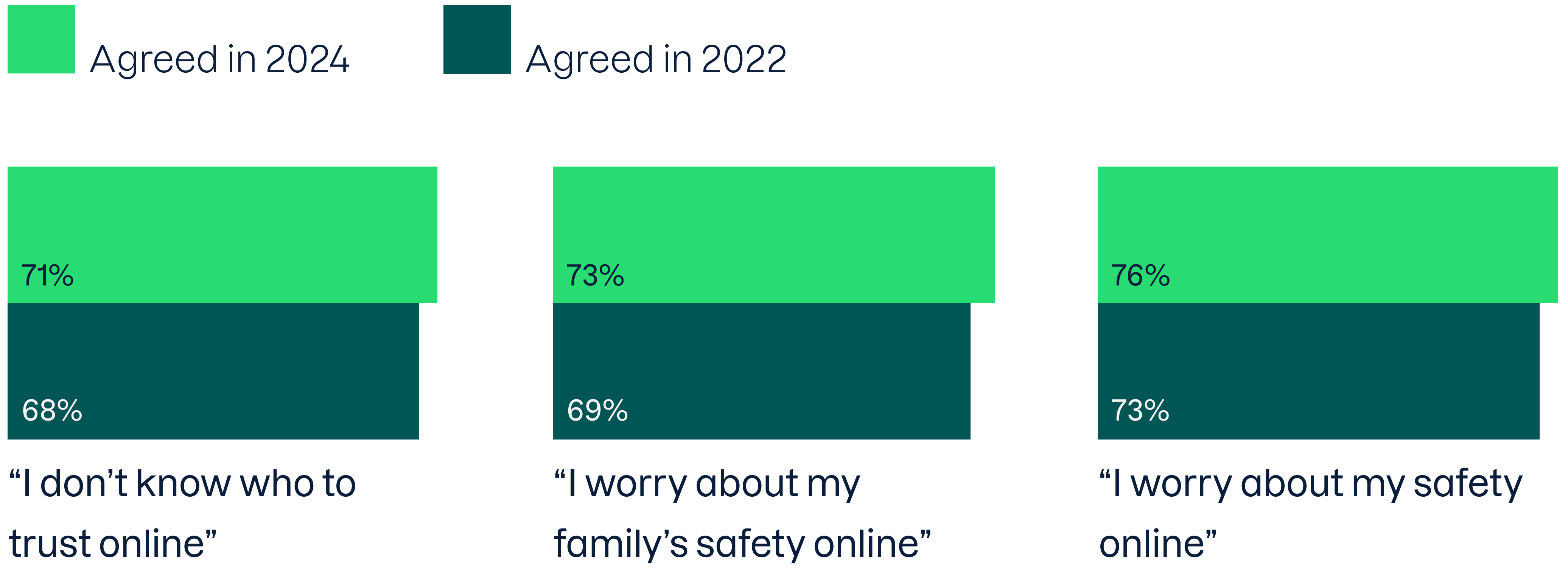
Consumer trust in 2024

When compared to our 2022 results, it's clear that trust continues to be a huge problem for consumers, with 76% of Americans surveyed in 2024 saying that they worry about their online safety – a 3% increase in the last two years.

Our findings reveal that diminished trust and insufficient transparency from service and hardware providers have left consumers feeling more vulnerable and uncertain when it comes to protecting their digital activities. Despite widespread marketing efforts, such as Capital One's popular ads with a standout celebrity cast, concerns about online security have escalated over the past 24 months. The proportion of individuals uncertain about who they can trust online has risen from 2022 to 2024.

How people feel about security (2024 vs 2022)

We asked people to provide us with responses to the following statements.



*Source: F-Secure Living Secure Survey 2024

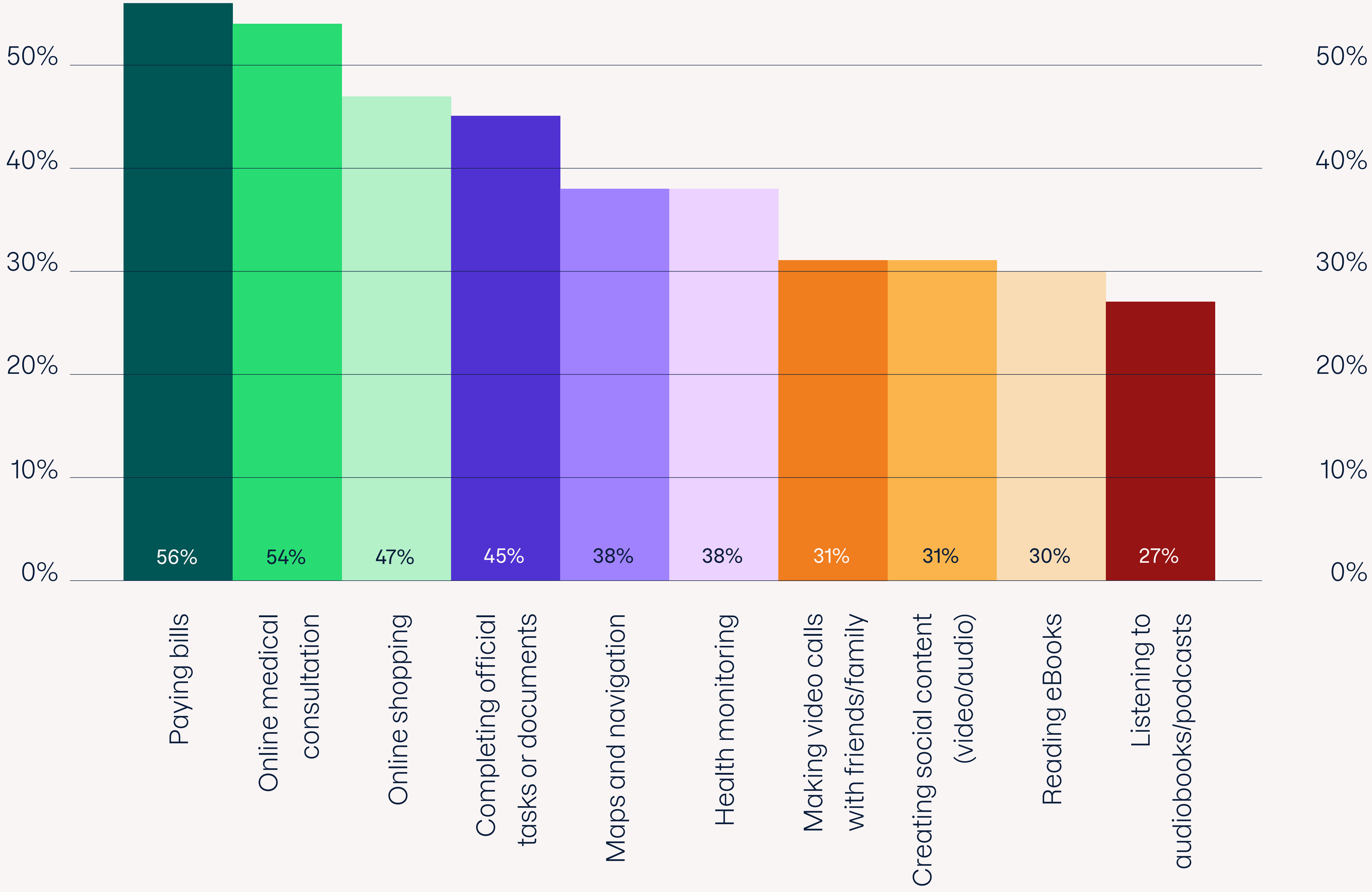
KEY TAKEAWAYS

76% of Americans worry about their online safety

54% of Americans have no idea if their devices are secure

7 in 10 Americans don't know who to trust online

Top 10 moments of consumer vulnerability in 2024



*Source(s): F-Secure Living Secure Survey 2024, F-Secure Consumer Market Research 2023

Opportunities for service providers

When lack of trust leads to feelings of vulnerability, confusion naturally follows. With 68% of Americans expecting an increase in cyber threats next year, consumers are turning to reliable service providers – such as their carrier, insurer, or bank – for reassurance. Significantly, 81% of people worldwide view carriers as credible sources of internet security, while 71% regard insurance companies as trustworthy providers.

How scams shape US consumer experiences

The 2024 Living Secure survey revealed that cyber crime has never been more prevalent: 90% of US respondents reported receiving a digital scam attempt in the past year, with more than 4 in 10 people encountering them at least weekly. Among the Americans surveyed, 40% said they face more scam attempts now than they did just 12 months ago – highlighting an escalating threat.

Real-world impacts of scams

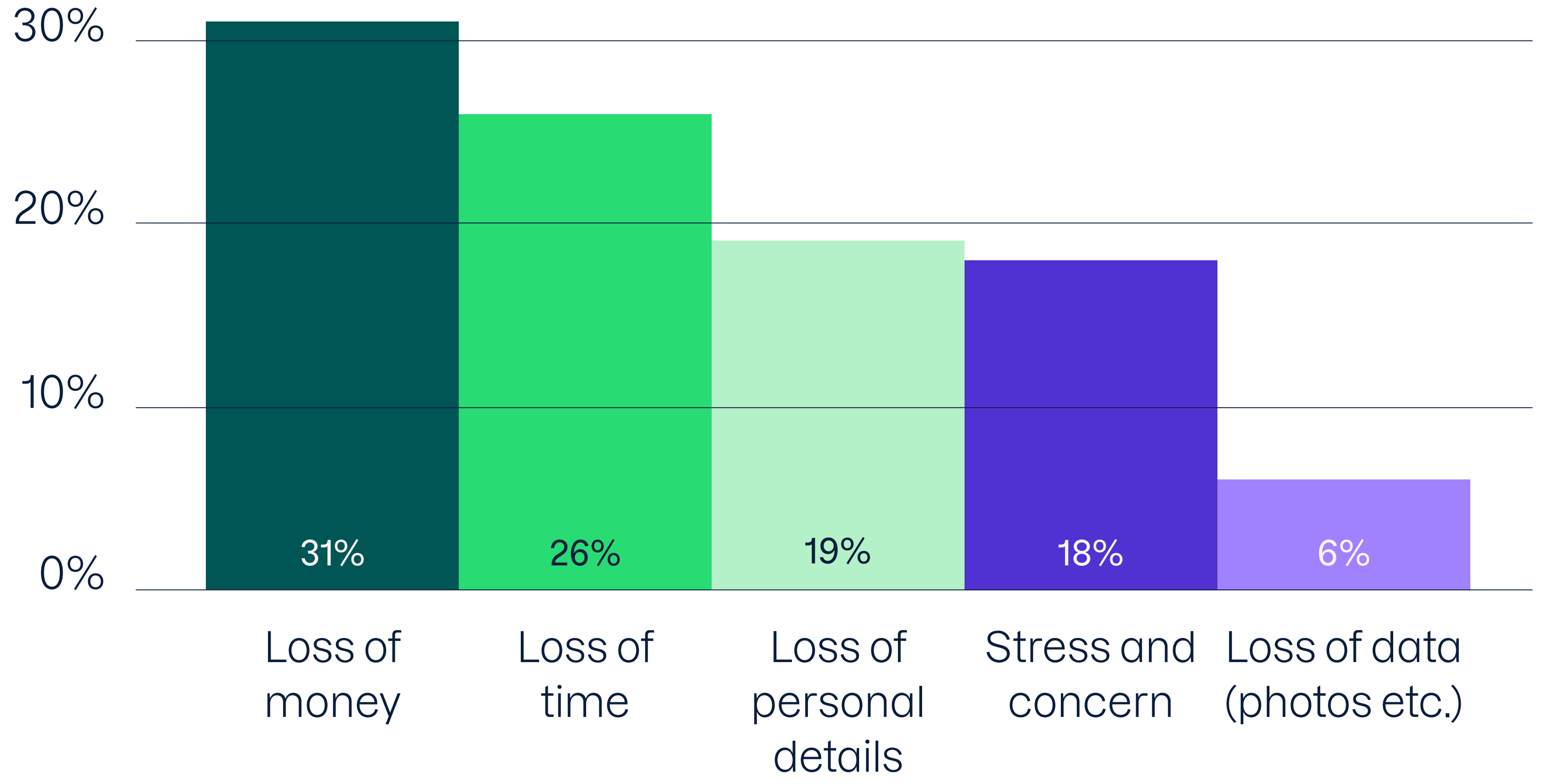
90% of Americans received a digital scam attempt in 2023, while 26% think they fell for a scam. Among those affected, 31% suffered some form of financial loss, while 26% reported a significant loss of time.

Weaponizing a wealth of platforms

Despite the rising prevalence of scams and the increasing sophistication of generative AI in crafting convincing content across images, video, text, and audio, 86% of Americans believe they can recognize an online threat. However, over a third (38%) of those who fell victim admitted that they couldn't identify or recognize the scam that deceived them.

Effects of a cyber scam

Discover how Americans were affected by cyber scams in 2024



*Source: F-Secure Living Secure Survey 2024

KEY TAKEAWAYS

26%	of Americans experienced a cyber scam in 2023
90%	of Americans reported receiving a digital scam attempt
57%	of Americans think they will be scammed in the future

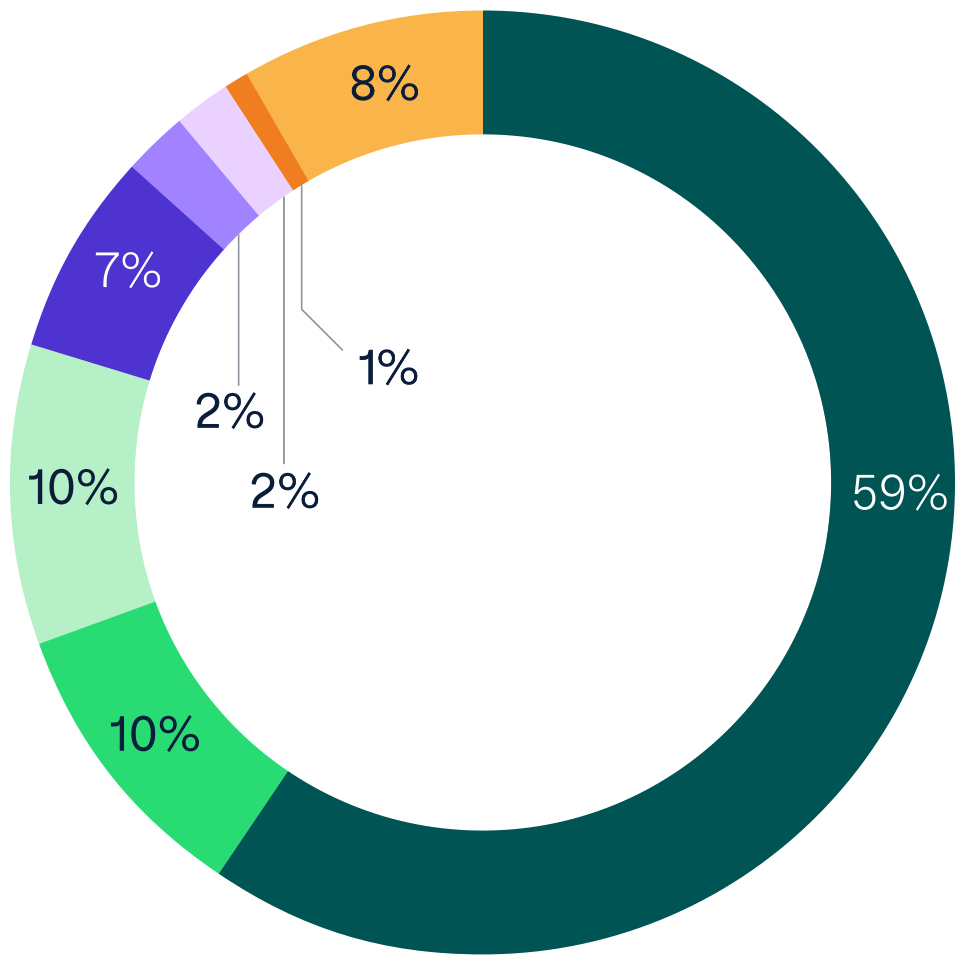
2024 scam breakdown

This overview provides a revealing snapshot of the types of scam attempts encountered by US respondents over the past year. Shopping scams top the list, highlighting consumers' increasing reliance on e-commerce and the risks that come with it as scammers exploit the convenience and anonymity of online transactions. Investment scams closely follow, emphasizing the persistent lure of financial gain for consumers, especially in the context of volatile markets and the rising popularity of online trading platforms.

Interestingly, 28% of respondents selected 'None of the above,' which could indicate a lack of awareness of the listed scam types or point to the emergence of newer, less understood scam techniques that may be underreported. This highlights the critical need for ongoing education and awareness for both consumers and service providers as scammers continually evolve and diversify their scam tactics.

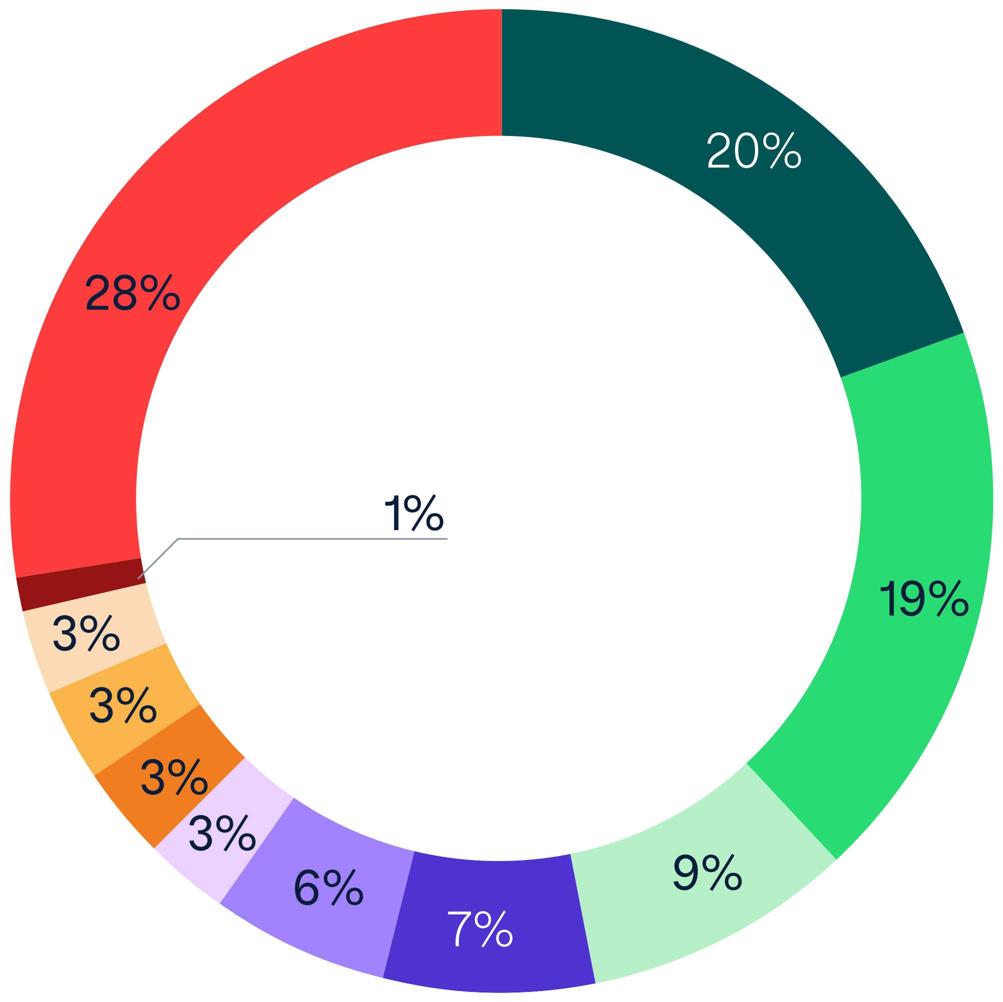
Scam attempts by channel

Discover the main channels being used by cyber scammers in 2024



Types of scams

An overview of the scam attempts received by our US respondents in the last year.



*Source: F-Secure Living Secure Survey 2024

Restoring consumer trust in the scam pandemic

F-Secure President and CEO, Timo Laaksonen, explores why consumer trust is in freefall – and what businesses can do to rebuild it.

The Covid-19 pandemic caused consumer trust to plummet – reaching a low of 45% in 2020. Although it has since risen to 50%, it has not yet returned to pre-pandemic levels, and among the most affected by cyber crime are Gen-Z. More than anyone, they need support in staying safe from scams and reassurance about the future stability of the world.

Impacts on service providers

A lack of trust prevents consumers from trying new services and products that they might need in our digitally connected world. Our recent survey reveals that 71% of

*Source: Qualtrics XM Institute Examining 12 Years of Consumer Trust Ratings 2024

Timo Laaksonen

President and CEO, F-Secure

Americans are unsure who to trust online, and with 66% encountering scams at least once a month, it's no wonder why. Gone are the days of antivirus being enough – there are so many more threats now.

Navigating the scam pandemic

F-Secure has decided that scams are a problem we need to solve. We've refocused our research to better understand how people are targeted and scammed, and to develop strategies – and technology – to protect them.

Building positive experiences

Consumers seek more than protection – they want a reassuring and positive experience. That's why we've integrated a sense of security directly into their digital interactions. For instance, with shopping protection, our user experience immediately informs consumers if an online store is trustworthy – there's no need to go to a separate app to find out.

And how do you provide a sense of security? You show them value. Total tells consumers exactly how the service is protecting them. Protection alone isn't sufficient if the value isn't clear, so we're enhancing our service with more guidance.

Driving retention for partners

Regarding our partner experience, we're doing everything we can to make the consumer experience unique to yours and so it mirrors your own service. The era of identical apps with the same functionalities is over. Now, we focus on tailoring the look and feel to align with each partner's brand.

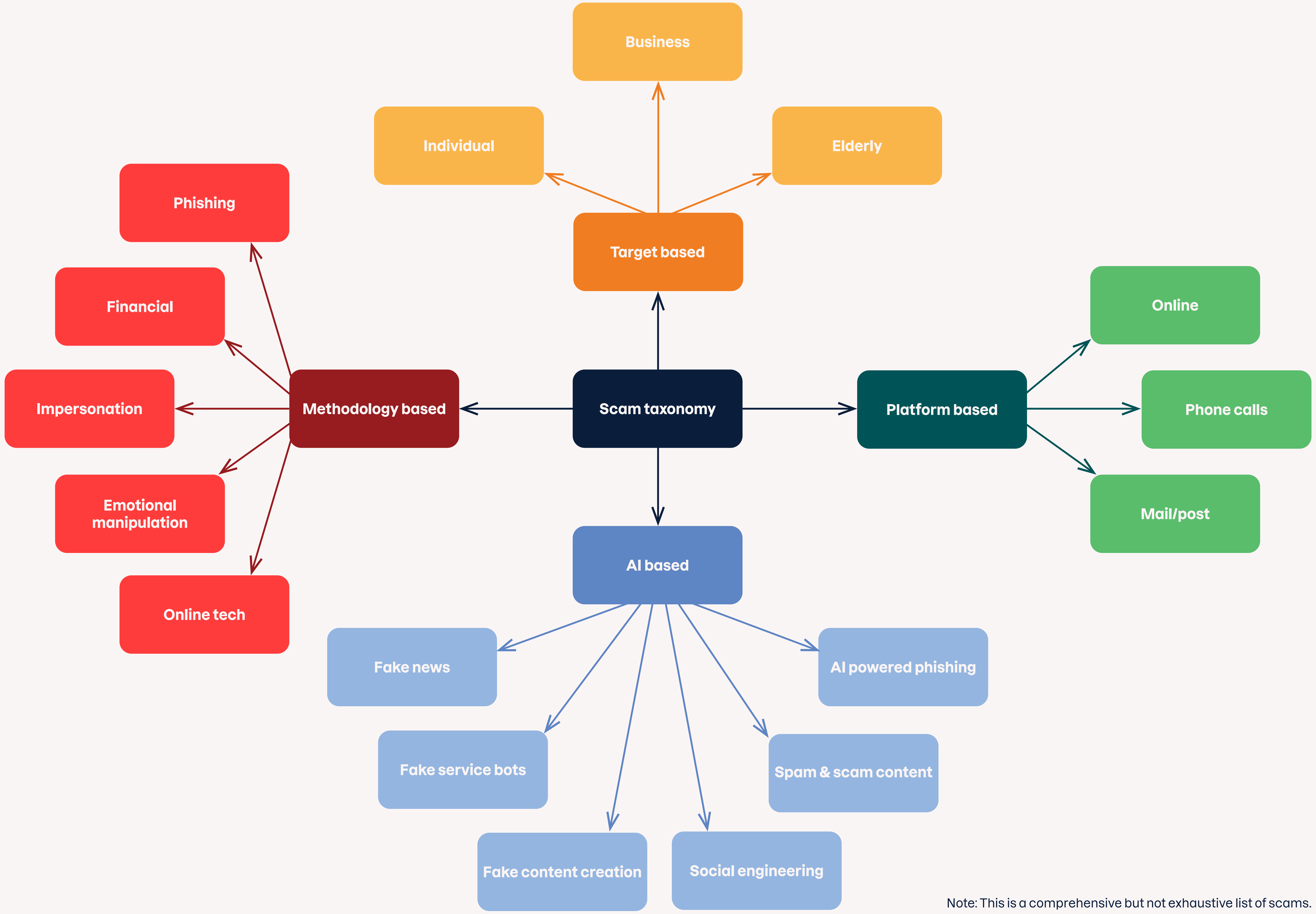
Restoring consumer trust

In the current scam pandemic, a sense of security has never been so important. That's where we step in, developing the best technology to protect people from scams while delivering an excellent experience that drives value, adoption, and retention. With 81% of consumers expecting their service providers to keep them safe, it's time for us to collaborate and seize this opportunity to restore lost consumer trust.

*Source: F-Secure Living Secure Survey 2024

F-Secure Scam Taxonomy: an A-Z of online scams

As technology evolves, online scams are growing more sophisticated. While new scams targeting bank accounts and personal data are frequently reported, many are simply old schemes repurposed with modern trends and techniques. That's why we created the **F-Secure Scam Taxonomy** – a classification system that organizes scams by characteristics, methods, attack vectors, and underlying strategies. It categorizes scams into four main groups: methodology-based, target-based, AI-based, and platform-based scams.



Note: This is a comprehensive but not exhaustive list of scams.

Methodology-based scams

Scammers design scams using specific techniques or methods. This may involve a series of steps or specific processes designed to deceive victims into divulging their money or personal information. Methodology-based scams include:

- **Phishing scams** via email, SMS, phone, or QR code
- **Financial fraud** like shopping and investment scams
- **Impersonation scams** often leading to identity theft
- **Emotional manipulation** like in romance scams
- **Online technology** such as posing as tech support

Target-based scams

Scammers devise and execute scams with a specific target in mind. Target-based scams typically fall into one of three categories:

- **Targeting specific individuals** for financial gain or personal information, such as gamers, job seekers, or taxpayers
- **Targeting businesses or organizations** for financial fraud, data theft, or ransom demands via ransomware, whaling, or spear phishing
- **Targeting the elderly** by taking advantage of their trust or unfamiliarity with technology. Common frauds include impersonations of grandchildren and government officials, as well as scams involving funerals, romance, and pensions

Platform-based scams

Scammers utilize specific platforms to execute their scams, exploiting platform features and user bases. These scams typically occur on one of three types of platforms:

- **Using online platforms** for social media deception, fake travel packages, utility company impersonations, fake pet adoption listings, and more
- **Using phone calls** to impersonate companies or people of authority
- **Using postal or mail services** to carry out fraudulent schemes

AI-based scams

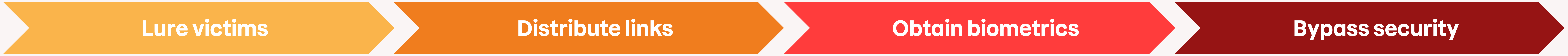
Scammers leverage artificial intelligence to deceive and exploit people with increased sophistication, scale, and effectiveness. AI-based scams include:

- **AI-powered phishing** emails, messages or phone scripts
- **AI-generated spam and scam content** such as fake reviews and comments
- **Social engineering attacks** such as targeted social media manipulation assisted by AI analyzing vast amounts of publicly available data
- **Fake content generation** such as deepfakes, fabricated images, or videos
- **Fake chatbots** using AI that impersonate customer service representatives
- **Fake news** articles designed to influence public opinion or cause panic

Learn more about the **F-Secure Scam Taxonomy** here.

Anatomy of a scam: Goldpickaxe trojan steals faces

A notable recent example of a methodology-based scam is the multi-phase Goldpickaxe scheme, engineered to trick victims into disclosing their biometric data. It was developed by Chinese threat actor GoldFactory and primarily focuses on mobile banking malware in Vietnam and Thailand. Their sophisticated trojan allows attackers to bypass victims' banking security and steal funds using stolen biometrics in a four-stage process.


Lure victims

Distribute links

Obtain biometrics

Bypass security

Stage 1: Lure victims

The attacker sends phishing messages directing victims to a communications app and may even call them posing as government entities to gain their trust. The goal is to get them to download a fake app disguised as a real service, like the Thai 'Digital Pension' app.

Stage 2: Distribute links

For Android users, the malware infects devices through a counterfeit website that closely resembles the official Play Store. For iOS, the threat actor convinces the victim to install special configurations, known as Mobile Device Management (MDM) profiles, allowing remote control of the device or the installation of apps from outside the App Store.

Stage 3: Obtain biometrics

After installing the malware, it prompts victims to provide their ID documents and record a video as a 'confirmation method', which is then used to create deepfakes. When capturing the video, instructions such as 'blink', 'smile', and 'tilt your face' are given to the victim on screen to create a comprehensive facial biometric profile.

Stage 4: Bypass security

The malware can also intercept text messages to steal verification codes used in two-factor authentication. Additionally, it allows the attacker to use the victim's phone to disguise their internet activity, enabling them to access banking apps while evading security measures on a victim's carrier, geographical location, or device ID.

Impacts of biometric data theft

Targeting biometric data is a big escalation in today's scam landscape. Unlike passwords or PINs, biometric data such as facial recognition, fingerprints, or voice prints is unique and cannot be easily changed if compromised. Once stolen, this information can be used to create highly convincing deepfakes or for other forms of identity theft, and victims may face long-term consequences including deep psychological impacts and financial loss.

Identity theft and fraud: making unauthorized withdrawals and purchases or bypassing an app's biometric security measures to take over accounts.

Deepfakes: used to create false narratives, leading to reputational harm for individuals or businesses, and may even result in blackmail or extortion.

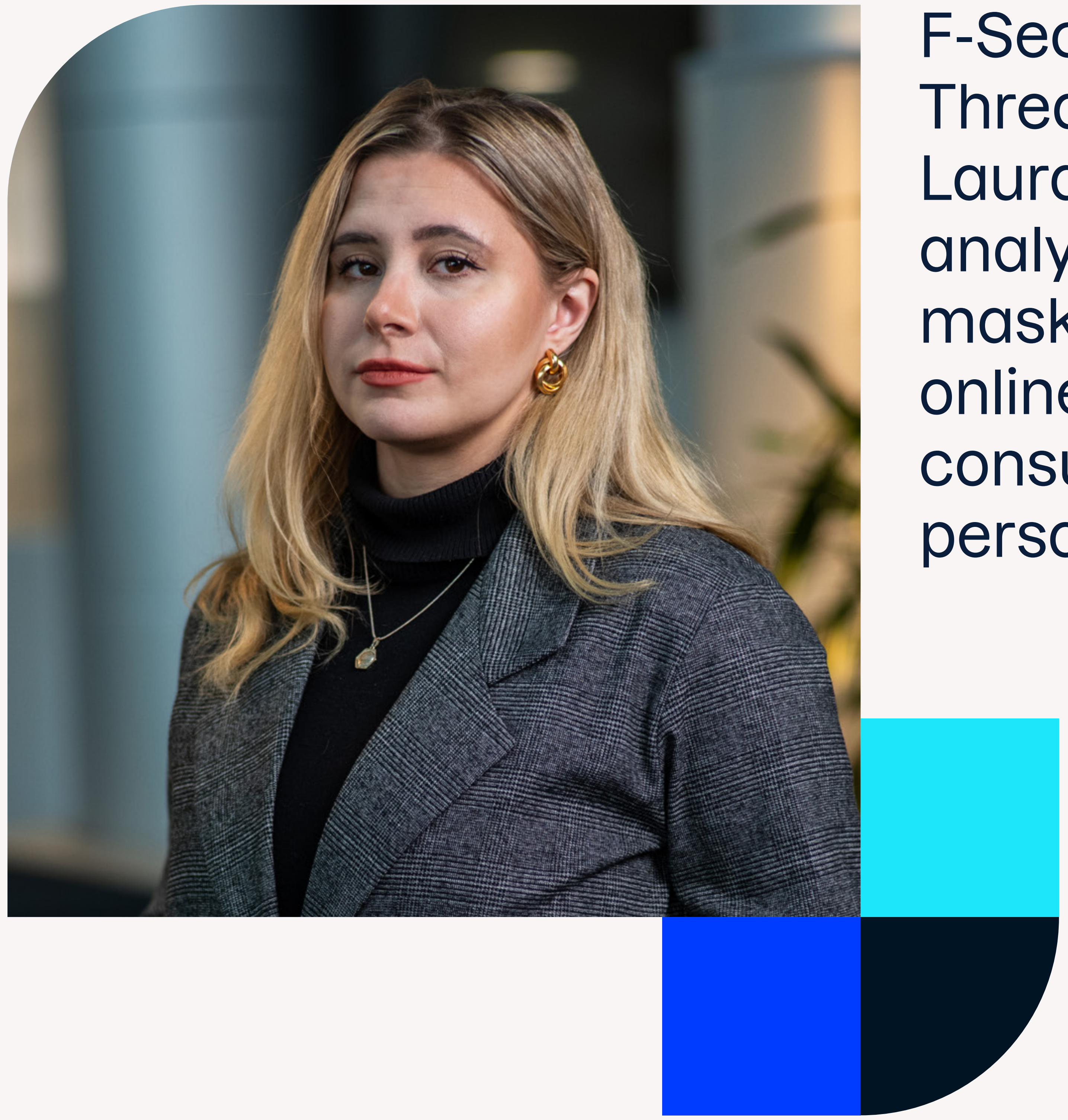
Psychological and emotional impact: a breach of biometric data can lead to a profound loss of trust, chronic anxiety and stress, and social stigma or judgment.

EXPERT INSIGHT:

"It's important to clarify that this malware does not bypass iOS or Android's biometric security features, but rather relies on social engineering. Providing consumers with a robust online security solution is the best way to keep them safe in an evolving threat landscape targeting biometrics. F-Secure technology blocks all currently identified indicators of compromise and variants for this threat on Android devices, as well as on iOS devices when F-Secure VPN is active."

Ash Shatrieh
Threat Expert

Internet anonymity: a scammer's greatest weapon



F-Secure's Head of Threat Intelligence, Laura Kankaala, analyzes the many masks that people wear online and explains why consumers fall for fake personas.

Consider this: the things in which we base our trust on the internet are anything but trustworthy. The foundations of trust are very artificial and easily forged. Reviews, likes, followers – crooks are selling and buying them. Everything online can be copied, even retail sites and social media. It's really incredibly easy to wear masks – or camouflage – on the internet.

Good masks versus bad masks

Not all masks are bad. In fact, we often wear 'good' masks online: curating our social media presence, participating in role-playing games, or sharing creative works online under a username. We all wear masks, and in today's digital world, we form relationships with strangers online – whether through romantic connections, purchasing items, or staying in someone's spare room.

Sometimes, it's easy to spot fake masks on social media profiles – sparse personal details, a lack of genuine connections, or using reverse image search to catch stolen images. But other times, scammers go to great lengths to craft convincing masks.

Meet Heidi Virtanen: our LinkedIn mask

- Heidi Virtanen is a fake persona that we created for the TV show 'Team Whack' in Finland to hide our identity when demonstrating how easily someone can infiltrate people's lives online. Her profile picture was generated by AI.
- We included a fake job history on her LinkedIn profile and added people to her contacts. At first, it was difficult – people were reluctant to accept her invitation. But after a while, when we got more connections, it became easier to get even more.
- Why? People base trustworthiness on the quality of their contacts. If a fake person connects with someone you know, they've then infiltrated your social network.
- We used this online mask very successfully, sending messages asking for peoples' phone numbers or for them to click on phishing links, and people did that. These LinkedIn users trusted Heidi Virtanen based on her fake online reputation.

Scammers are closer than you think

We often use the term 'dark web,' also known as the Tor network, to describe the internet's darkest corners – the place where everything bad online happens. The key reason for this is simple: dark websites don't have visible IP addresses, making it impossible to trace their physical location. This anonymity provides safety for scammers.

However, criminal activity isn't confined to the dark web. There are ways to hide IP addresses on the 'clear web' too, using services like Cloudflare, Telegram, Discord, bulletproof hosting servers, and remain anonymous using encrypted connections like HTTPS. The truth is, online criminals are often closer than we realize, hiding behind the same platforms we use daily to build relationships with us.

Building a safer digital future

We often assume that the younger generation is more tech-savvy, yet they are three times more likely to fall victim to online scams (37%) compared to those aged 55 and above (12%). This highlights a critical gap: while our most digitally native generation navigates new technologies with ease, they often lack a solid understanding of online scams. This is why educating them on how to identify and protect against scams is crucial.

Trust in internet services is essential for individuals and society to function. As scammers exploit trust through their many deceptive masks, their goal is to extract something valuable from consumers – whether it's money or data. However, these are the very things we can protect. By collaborating with service providers, we're building those safeguards around trust to ensure that consumers of all ages can feel safe in the digital world.

Why tech revolutions like AI are great – and awful

F-Secure's Principal Research Advisor, Mikko Hyppönen, examines the pros and cons of technological advancements in society – and scamming.

Technology revolutions change the world, both positively and negatively. But when we invent something that proves problematic, we can't make it go away. This is a consistent pattern throughout the history of technological innovation.

The internet is great – and awful

The internet has introduced us to global businesses, new ways of working in multinational teams, and international entertainment. It's great, but it has also brought global problems. Crime, once confined to local areas, has now become a worldwide issue. Today, the most probable place to encounter crime is online. Online scams are among the most common threats we face, and as potential victims, we are just as vulnerable as anyone else on the planet.

Social media is great – and awful

Social media has given everyone a platform to share their voice and publish information, which initially seemed like a great idea. However, it has proven to be problematic, contributing to the deep divides in today's world. It has introduced new types of conflict, with elections swayed by social media influencer campaigns and conspiracy theories flourishing more than ever before.

AI is great – and awful

Why are we seeing an explosion in AI right now? The foundational information has been available for decades, but we lacked the means to teach it to machines effectively. Teaching generative AI systems requires data, and in recent years, the nature of knowledge has transformed – where it once only existed on paper, it's now digitized and accessible as data. With all human knowledge converted into digital formats, we've now been able to teach AI systems. Recent advancements in algorithms and computing power have also enabled machine learning to drive the generative AI innovations we've seen over the past two years.

Does the good outweigh the bad?

There are endless tech innovations that are both great and awful. Strong encryption enhances our security and privacy, but it also provides the same protections to criminals. Technologies like Bitcoin, the Tor network, and quantum computers exemplify this dual nature. While they can greatly benefit society, they also pose serious threats. New technology can be used for both good and bad, reshaping the world in positive and negative ways. Historically, the benefits of technological revolutions have outweighed the drawbacks, but the risks are very real. Therefore, it's crucial that we continue to leverage the advantages of evolving technology to ensure robust protections for consumers against those disadvantages.

AI scams targeting consumers

- Mr. Beast has one of the most followed YouTube channels and is regularly used in deepfake scams targeting consumers who think he wants to financially help them.
- Stealing the voice and face of a celebrity isn't very hard with today's technology – but we're also seeing more targeted attacks.
- The CEO of a Nordic company had his voice cloned and used to send a WhatsApp voice message asking a financial clerk to disclose details of a deal.
- The problem isn't huge yet – we aren't seeing individual deepfake scams targeting everyday people on a large scale. But in the future, this will be a real problem.

AI: the future of scams – and the tools to stop them

F-Secure threat intelligence and cyber security experts share their forecasts on the future of online scams and discuss how AI will play a role in defending against them.

Joel Latto
Threat Advisor

"Before the general availability of generative AI, phishing emails, scam SMS messages, and fraudulent websites were much easier to spot because of grammatical errors, spelling mistakes, and generally poor visuals and copy. But now, these threats and scams will become nearly impossible to spot. And AI doesn't only pose a threat to consumers – the use of deepfake and vishing technology makes the threat landscape globally much more complex. I'd expect to see a rise in consumer desire to stay ahead of and protect against AI-enabled threats, both by becoming more vigilant and using the right technology."

Paula Al-Soufi
Director, Portfolio Strategy

"Consumers are increasingly unsure about who to trust, whether their devices are secure, and how they can protect themselves online. This is expected to intensify with the prevalence of deepfakes and AI-generated content. When it becomes harder to trust anything they see online, consumers turn to their established partners, such as telcos, insurance companies, and banks, seeking a comprehensive security solution for peace of mind online. Telcos, insurance companies, and banks are anticipated to leverage AI for the greater good by combining consumer security solutions with their own AI advancements."

Keep consumers safe from scams with F-Secure Scam Protection

- Banking protection secures over 1 million banking sessions each day.
- SMS scam protection blocks scam text messages, powered by AI.
- Shopping protection shields consumers from online shopping scams.
- Phishing and browsing protections safeguard consumers from malicious links and websites.

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/partners or follow us on our social channels.

F-Secure.