Digital Perception-Reality Gap Report

Exposing the gap between consumer confidence and real online risk—and the urgent role of trusted telcos and financial service providers in closing it.

F-Secure®

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

Laura James
Vice President, Research
F-Secure

Consumers Are Experiencing Cognitive Dissonance Online

As reliance on digital spaces grows, so too does consumer uncertainty. Escalating cyber crime continues to erode trust in online environments—yet consumer concerns don't always reflect real risk. We've found that people tend to worry more about unfamiliar or emotionally charged activities than about routine behaviors where threats are most likely to occur, leading to misplaced caution and missed protection in the moments that matter.

This report draws on findings from the F-Secure Consumer Market Survey 2025, exploring how perceptions of trust, risk, and routine shape digital behavior—and often diverge from real-world threats. To quantify this gap, we introduce two scoring models: the Worry Score, based on consumer sentiment, and the Threat Score, based on expert analysis. We also identify three mindset zones—Functional, Emotional, and Grey—that capture the disconnect between what consumers value, fear, and overlook in their digital lives.

For telcos, banks, and other digital service providers, this gap presents a strategic opportunity. By embedding protection into daily routines, trusted brands can meet both practical and emotional needs—redefining customer value through digital security.

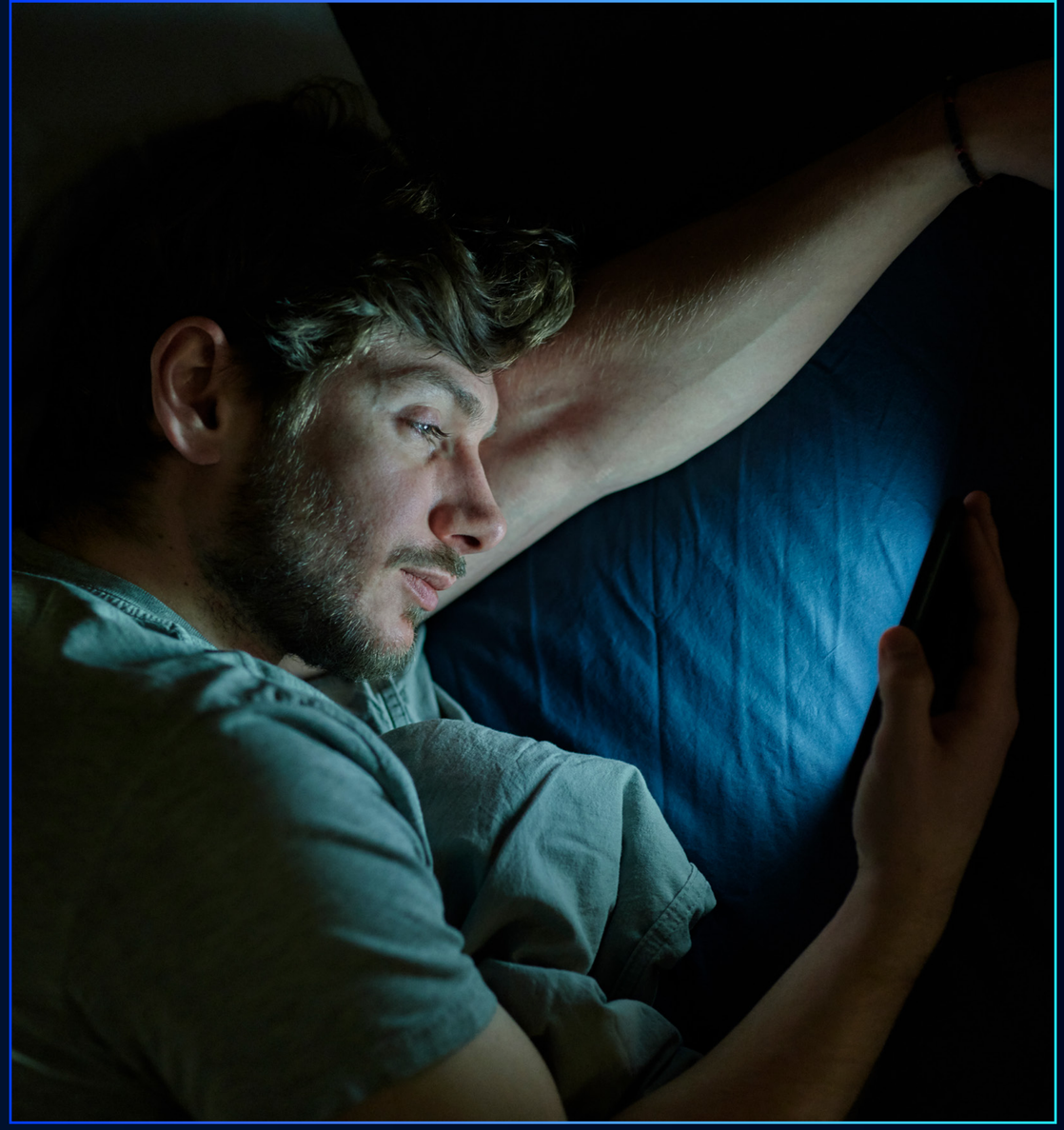
KEY REPORT FINDINGS

- While 69% of people feel confident in spotting scams, 43% still fell victim last year.
- Young adults (digital natives) are more than twice as likely to experience cyber crime (64%) than the oldest group of internet users (28%), driven by high online exposure and misplaced confidence.
- Consumers worry more about unfamiliar or emotionally charged online activities than about routine behaviors—where threats are more likely to occur.
- The misalignment between real and perceived online threats skews consumer behavior—leading to misplaced caution and overlooking areas where they're most exposed.
- Recognizing this gap is essential for addressing real-world vulnerabilities and closing the divide between perception and reality in digital risk. Effective protection strategies must bridge not only technical gaps, but psychological ones as well.
- Consumers want cyber security from familiar, everyday providers like banks (80%) and telcos (71%). This puts service providers in a unique position to deliver in-the-moment protection that meets demand and strengthens trust.

THE CONSUMER TRUST DISCONNECT:

When Awareness Isn't Enough

Digital spaces are more integral to daily life than ever, but consumer trust isn't keeping pace. It's easy to see why: in 2024, nearly half of survey participants (48%) were impacted by cyber crime, up sharply from 34% the year before. Even as awareness grows, so does anxiety. A growing majority of consumers—7 in 10—no longer know who to trust online. The result? An online environment shaped by caution, confusion, and fragile confidence.



Key Consumer Insights on Digital Distrust

Worry about their safety online

Believe their cyber security risks will increase next year

Don’t know who to trust online

Find cyber security too complex

Don’t know if their devices are secure

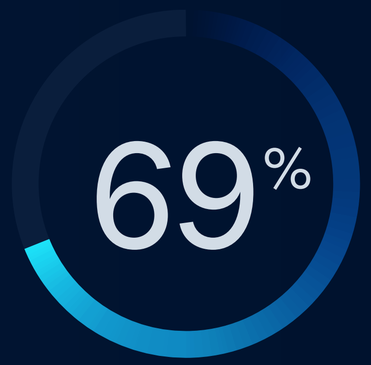
Don’t know how to identify a legitimate online shop

The Gap Between Concern and Capability

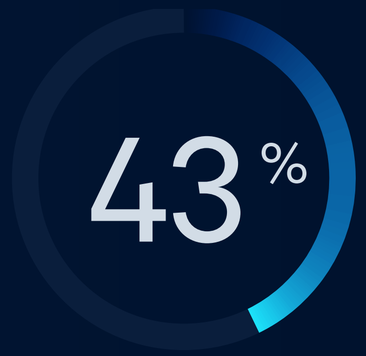
While concern is high (77%), most consumers lack the clarity, confidence, or tools to take control. Worry isn't translating into preparedness. And consumers aren't just concerned—they're overwhelmed. The complexity of staying safe online contributes to feelings of digital fatigue, driving disengagement and passive risk-taking. This presents an opportunity for service providers to fill the digital trust gap with accessible cyber security guidance.

The Trust Paradox: Digital Confidence Doesn't Equal Safety

Notably, while consumers feel insecure about trusting others online, most still trust their own ability to recognize digital threats. They place more trust in themselves than in the systems around them—but that confidence is often misplaced. Many people have learned to recognize poorly written scam attempts, but generative AI has changed the game, generating localized, highly optimized content that boosts criminals' chances of success.



of people believe they know how to recognize an online scam

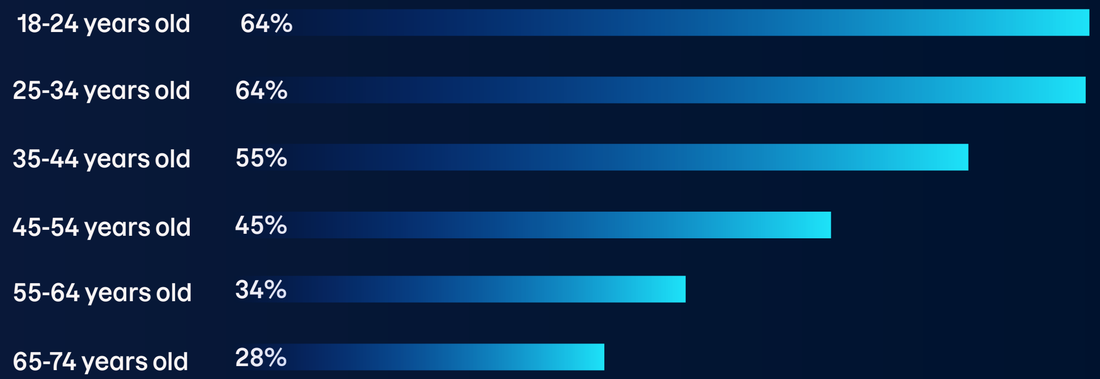


of those individuals also reported falling victim to a scam in the last year

A Discrepancy Between Confidence and Outcomes in Scam Detection

This disconnect between perceived ability and real-world outcomes—a 43% gap between confidence and victimhood—reveals a critical vulnerability. Overconfidence can be especially dangerous among the most cyber-aware individuals, who may overestimate their skills and underestimate evolving threats. Human intuition alone isn't enough. To stay safe, consumers must apply rational scrutiny to every potential threat they encounter.

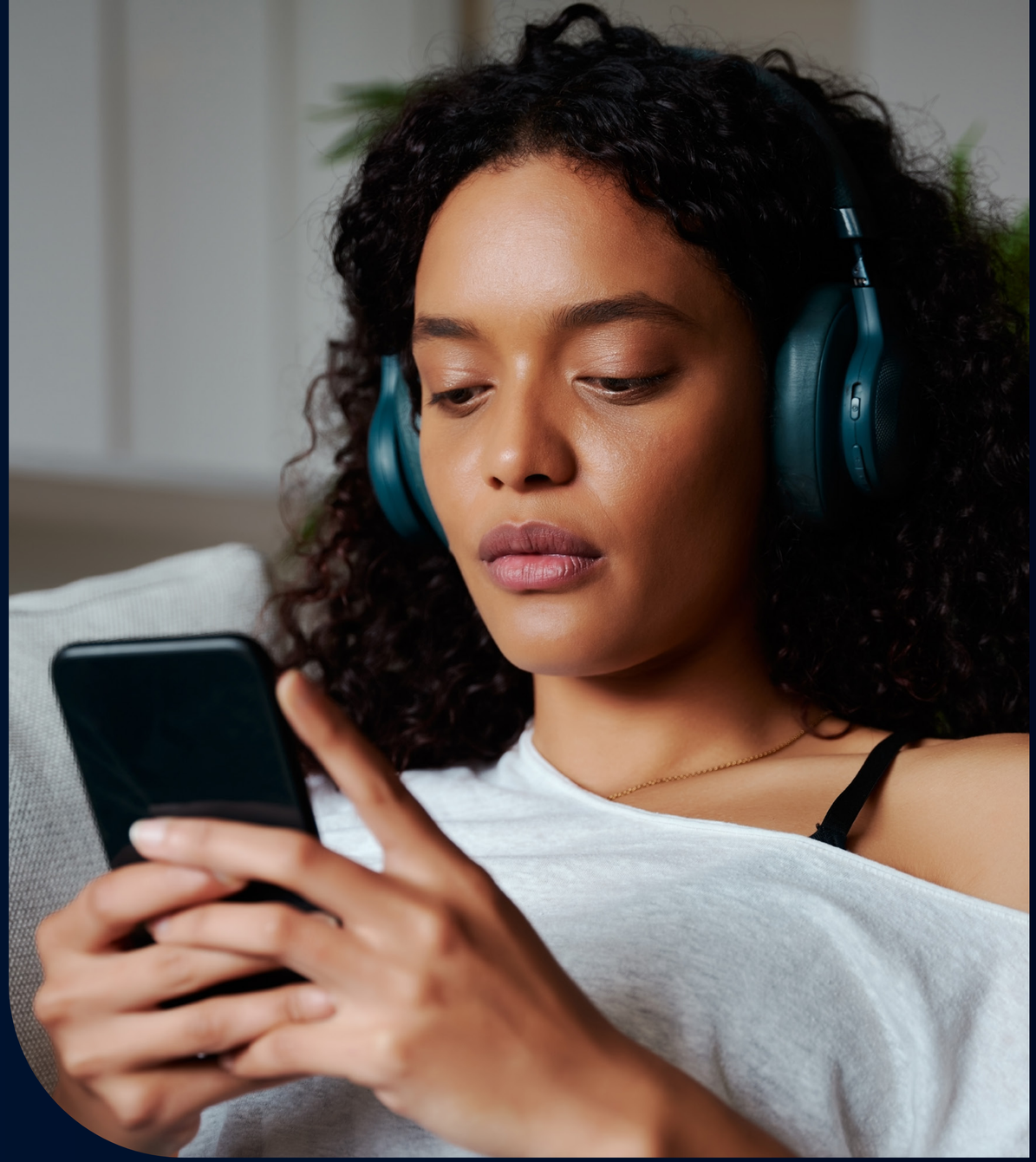
Rates of Cyber Crime Encounters by Age Group



The Greatest Risk Lies with Digital Natives

Even the most digitally savvy are not immune—sometimes, they're the most at risk. Young adults are more than twice as likely to experience cyber crime (64%) compared to the oldest group of internet users (28%), illustrating how a larger digital footprint can significantly increase exposure.

Overconfidence among those who grew up with the internet may further compound this risk, as many assume that familiarity with technology equates to strong cyber security awareness. Young adults are also typically early adopters of new tools—but this trust in technology can create blind spots. Combined, high exposure and misplaced confidence make digital natives one of the most vulnerable groups in today's threat landscape.



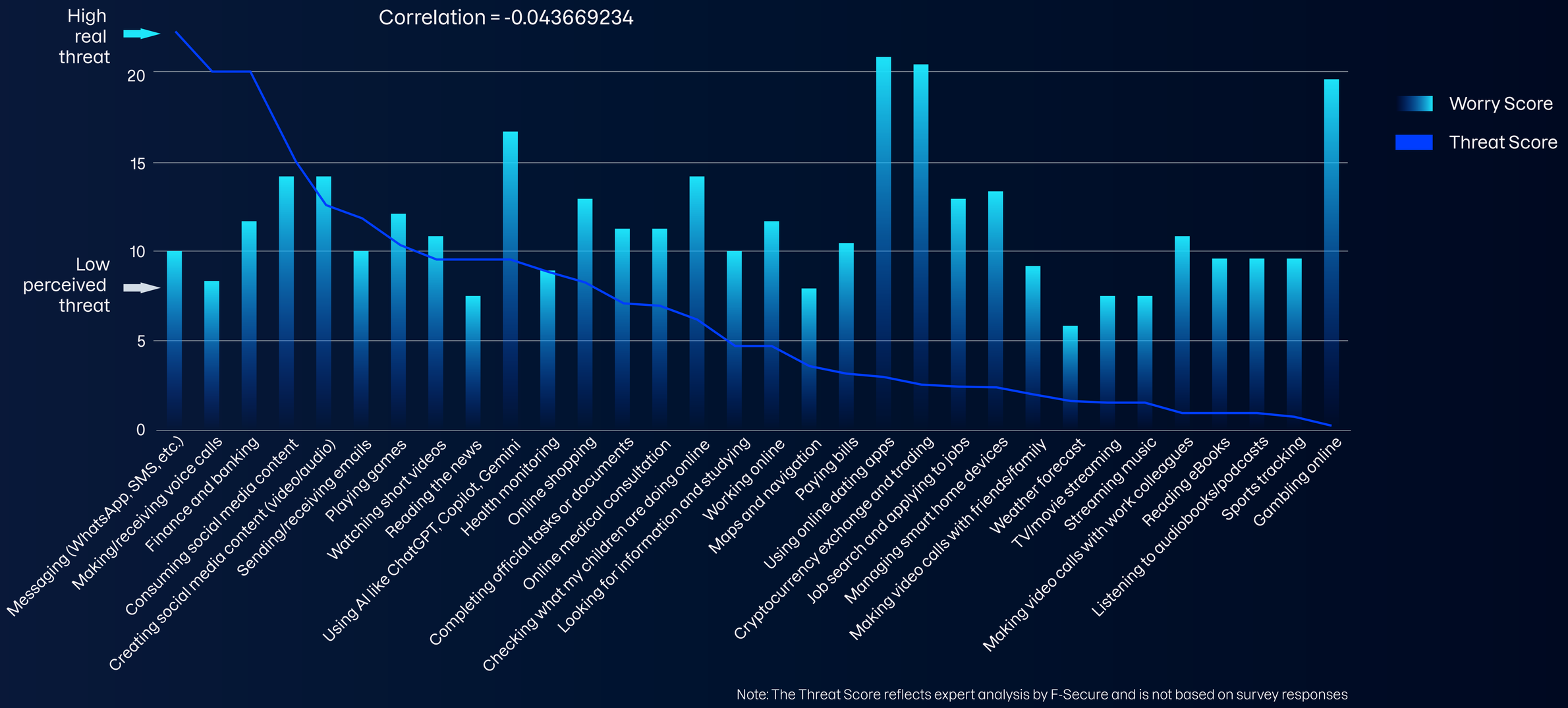
The Emotional Map of Consumers' Digital Lives

For the most part, consumers don't assess digital risks rationally—they react emotionally. What people feel is dangerous online often doesn't align with what's actually risky.

Our latest data reveals a stark disconnect between perceived threats and real cyber risks. Familiar, routine, or seemingly low-risk activities—such as messaging via SMS or WhatsApp, making voice calls, and banking online—often fly under the radar of concern, despite being prime entry points for cyber crime.

In contrast, tasks that feel more personal, unfamiliar, or have been amplified by media attention—like online gambling, cryptocurrency trading, and dating apps—tend to trigger disproportionate fear. This misalignment skews behavior, causing consumers to misplace caution and overlook the very areas where they're most exposed.

No Correlation Between Perceived Worry and Real Threat



Note: The Threat Score reflects expert analysis by F-Secure and is not based on survey responses

Methodology: Perceived vs Real Threat

To explore the disconnect between perceived risk and actual threat, two distinct scoring models were developed using F-Secure consumer market research and expert analysis.

Worry Score

This reflects consumer perception of risk, based on data from the F-Secure Consumer Market Survey 2025: the percentage of people who report feeling vulnerable during online activities.

The score captures the emotional weight—how concerned consumers feel while engaging in digital activities.

Threat Score

This estimates real-world cyber risk, based on expert analysis from F-Secure's threat intelligence team and insights from collaborative workshops. It combines three weighted parameters:

- **Impact:** How severe the consequences of the threat could be
- **Likelihood:** How likely an individual is to encounter the threat
- **Reach:** The proportion of the global population potentially affected

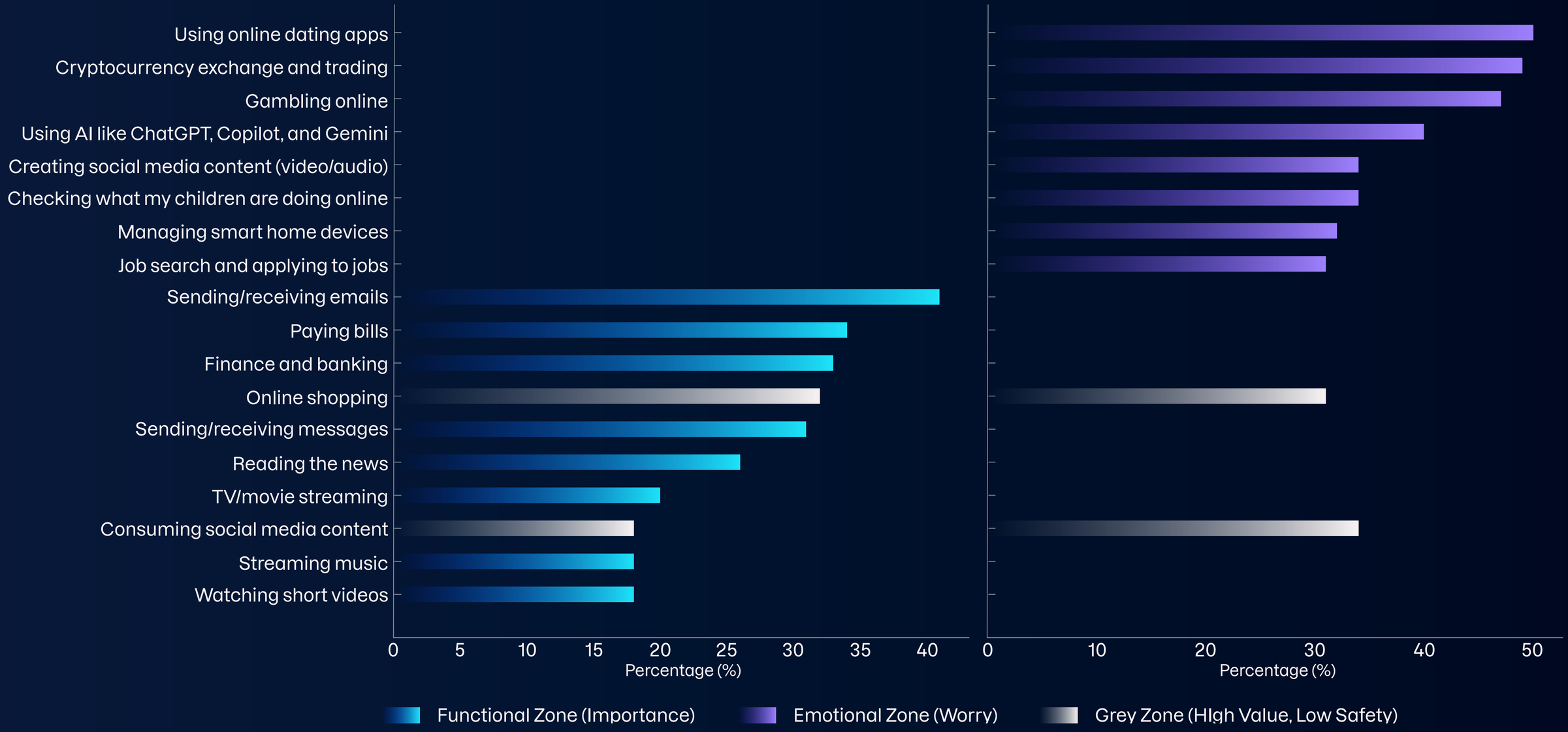
Together, these scores allow us to map the perception-reality gap, highlighting where consumers may overestimate—or underestimate—their digital risks.

The Consumer Mindset: Digital Risk Perception

To address the disconnect between real and perceived cyber risks, we've identified three distinct zones that shape consumer behavior: the Functional Zone, the Emotional Zone, and the Grey Zone. Each represents a unique intersection of digital habits, perceived value, and psychological responses to threat.

Top 10 Most Important Activities

Top 10 Most Worrying Activities



Functional Zone (Importance)

Themes of communication, financial management, and content consumption fall into this zone—areas that consumers rely on daily and expect to operate seamlessly. Disruptions here, such as scams or data breaches, feel like urgent threats to routine and productivity. Yet despite their high exposure, these routine activities are often perceived as low risk.

Emotional Zone (Worry)

This zone includes high-stakes or emotionally charged activities—such as online dating, gambling, and cryptocurrency trading—as well as emerging technologies like AI tools and smart home devices, which amplify uncertainty. Concerns around privacy, identity exposure, and family safety also sit here. Consumers feel less in control in these scenarios, and emotional weight heightens perceived risk.

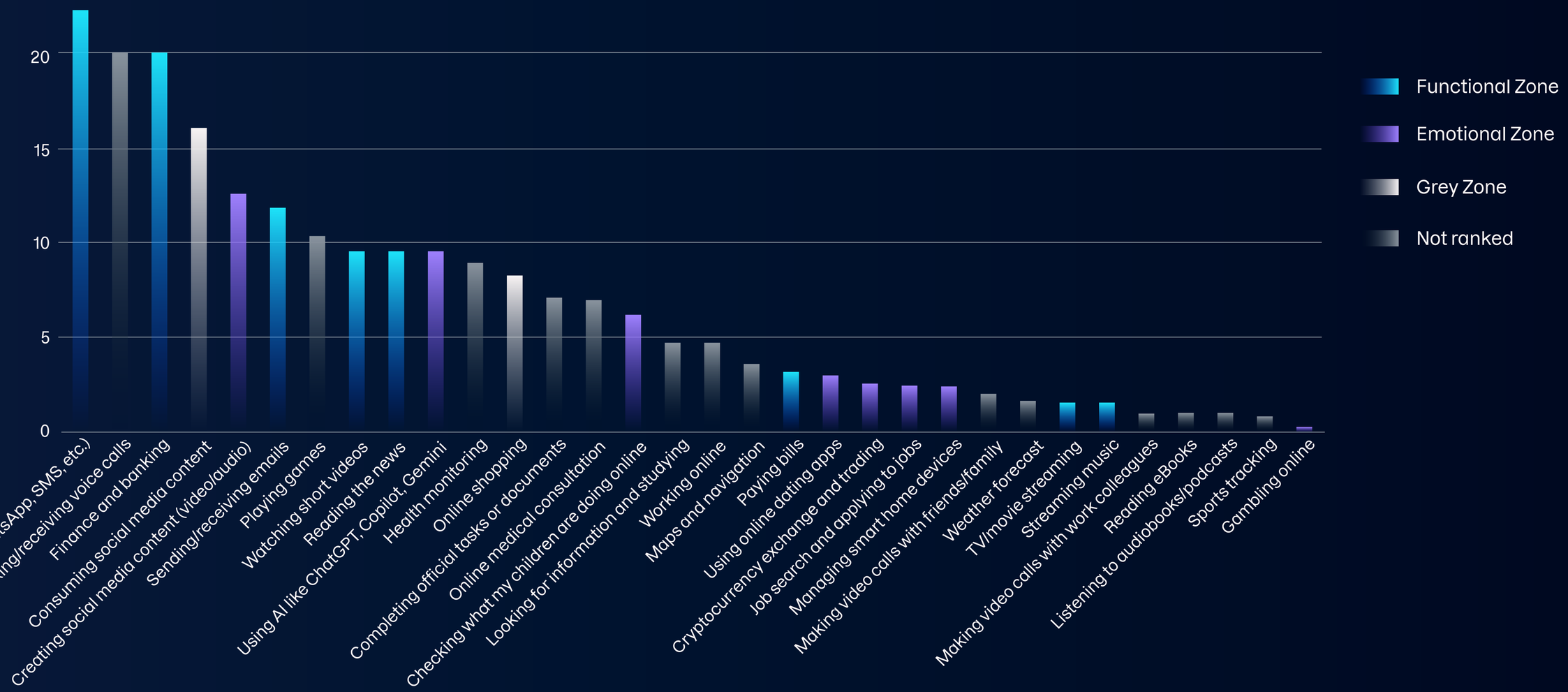
Grey Zone (High Value, Low Safety)

Online shopping and consuming social media content fall into a crossover zone—they're highly valued activities, yet consumers don't feel entirely safe engaging in them. These are areas of frequent use paired with persistent insecurity.

Comparing these zones, a clear pattern emerges: routine, high-exposure activities like sending emails and paying bills often trigger little concern, while newer, unfamiliar, or emotionally charged actions like online dating or gambling attract disproportionate anxiety. There's little overlap between what consumers do most and what they fear most.

However, when we examine where real threats lie, a different picture emerges—one that reveals the stark disconnect between worry, importance, and actual cyber risk. Many of the most significant cyber threats are tied to activities consumers consider highly important but don't actively fear.

Mapping Activity Threat Scores to User Behavior Zones



Note: The Threat Score reflects expert analysis by F-Secure and is not based on survey responses

Several activities that don't rank among the top 10 for either importance or concern—such as making or receiving voice calls and playing online games—actually carry some of the highest real-world risk. This further underscores the need to close the perception-reality gap and direct both protection and awareness efforts toward areas where consumers are most exposed yet least alert.

Digital Moments: Perception vs Reality

Consumers often fear what feels dangerous—such as AI or cryptocurrency—more than what actually is, like malicious messages, suspicious phone calls, and banking scams. Routine but high-risk activities are frequently overlooked, while unfamiliar, emotionally charged, or media-sensationalized tasks attract disproportionate concern. This misalignment leads to misplaced caution—and leaves consumers least protected where it matters most.

The Opportunity for Telcos and Financial Service Providers

Consumers are increasingly aware of digital threats, but many feel overwhelmed, uncertain, and ill-equipped to respond. According to our findings, 71% find cyber security too complex, which may help explain why 60% are unsure whether their devices are secure. For digital service providers, the disconnect between consumer trust and actual risk reveals a critical challenge: protection strategies must bridge not only technical gaps, but psychological ones too—even among the most tech-savvy users like digital natives.

Furthermore, consumers actively want accessible, trustworthy cyber security from familiar, everyday providers—including banks (80%) and telcos (71%). Banks and payment platforms are already seen as guardians of money and data—protection is expected here, making them natural providers of extended digital security. Telecommunication providers, meanwhile, are trusted for their control over connectivity and frequent customer interactions, giving them a strong position to deliver seamless, embedded protection.

Key Consumer Insights on Cyber Security

85%

Would use an app more frequently if it included scam protection and cyber security

80%

Prefer having scam protection and cyber security through an app they already use

80%

Prefer or would consider cyber security bundled with a banking or payment app

77%

Would switch providers for better scam protection and cyber security

76%

Would pay to upgrade to a premium version of an app that includes more cyber security features

71%

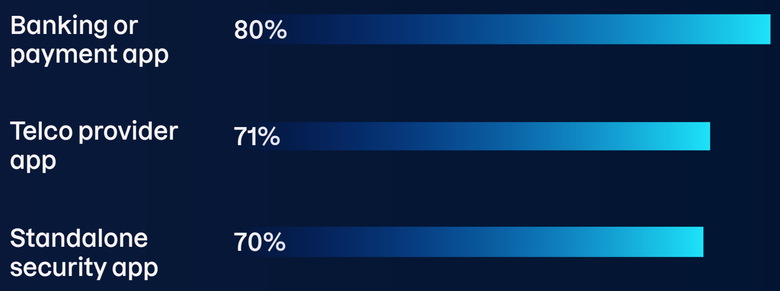
Prefer or would consider cyber security bundled with a telco provider app

Bridging the Trust Gap: From Provider to Protector

Telcos and financial services are among the most essential digital service providers for consumers. Yet trust is declining at the very moment consumers need it most—when they're facing fast-moving digital threats fueled by AI and other emerging technologies.

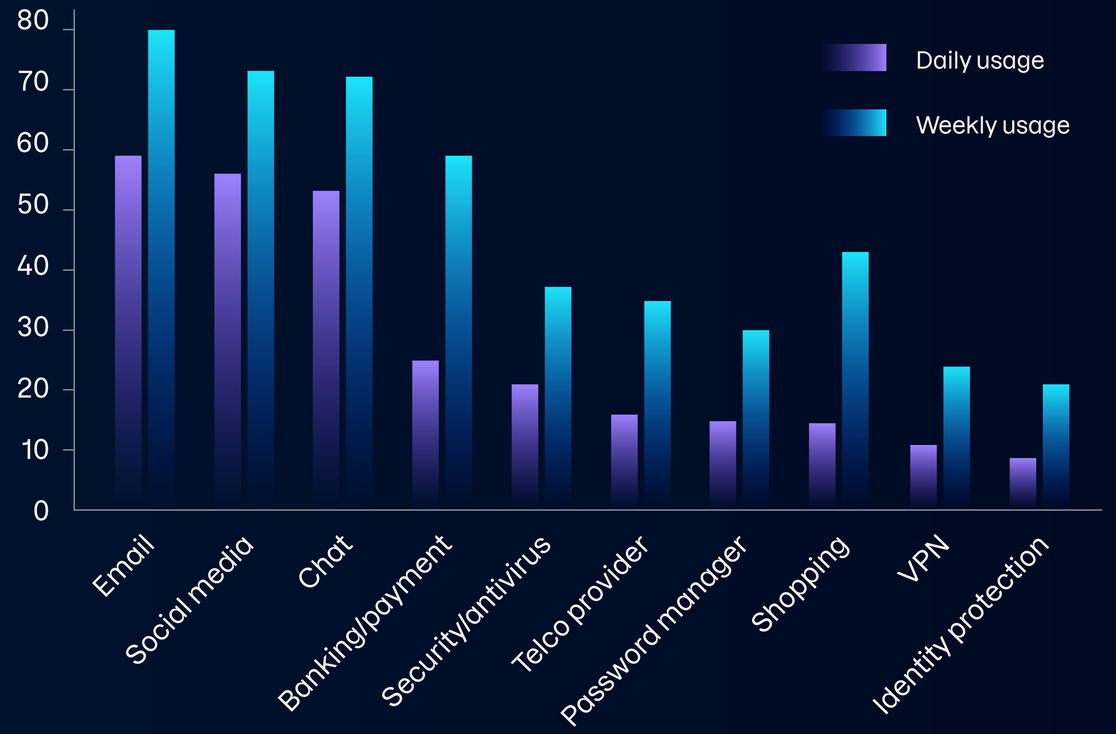
What does this mean for the customer–service provider relationship? Consumers still expect banks and telcos to protect not only their money and connectivity, but also their online security. To retain trust and loyalty, these providers must evolve into proactive enablers of digital safety.

Which Apps Are Consumers Open to for Providing Security?



This report reveals a significant perception–reality gap in how consumers understand digital risk—but also a clear opportunity to close it. 80% of consumers say they want protection embedded into tools they already use, and telcos and banks are uniquely positioned to provide in-the-moment security that aligns with daily behavior and builds long-term trust.

Consumer Behaviors in the Digital Space



Our latest data reveals a clear pattern in how frequently consumers engage with different types of apps. High-frequency apps—such as email (80%), social media (73%), and chat (72%)—are deeply embedded in weekly routines and viewed as essential for connection. In contrast, mid-frequency apps like banking (59%) and telco services (35%) support critical functions but are not accessed reflexively, despite handling sensitive tasks.

Enhancing app utility with security features—such as real-time scam alerts, fraud monitoring, or privacy controls—not only drives more consistent engagement, but also elevates the provider's role from service vendor to trusted digital ally.

Redefining Customer Value with Online Security

Online threats that were once out of sight, out of mind have become more personal—and more everyday users are recognizing the value of proactive protection. In fact, 76% say they'd pay to upgrade to a premium version of an app with enhanced cyber security, underscoring rising demand for built-in, visible protection.

By addressing both functional and emotional needs—where this demand already exists—service providers have a clear opportunity to evolve their role and help restore trust in digital services. Embedding cyber protection into telco or banking apps not only increases visibility but also drives engagement: 85% of consumers say they'd use an app more frequently if it included scam protection and security features.

More than just driving engagement, the true value lies in lasting impact. With 77% of consumers willing to switch providers for better scam protection, it's clear: digital safety is no longer just a feature—it's a competitive differentiator. For service providers, delivering embedded, seamless protection is now a decisive factor in earning trust and long-term customer loyalty.

"Our research makes one thing clear: consumers expect protection where they already engage. Security and digital safety are no longer nice-to-haves—they're part of consumers' daily lives. They're loyalty drivers and key points of differentiation for service providers, who have a unique opportunity to lead the next era of digital trust."

Fredrik Torstensson
Chief Partner Business Officer
F-Secure

Methodology

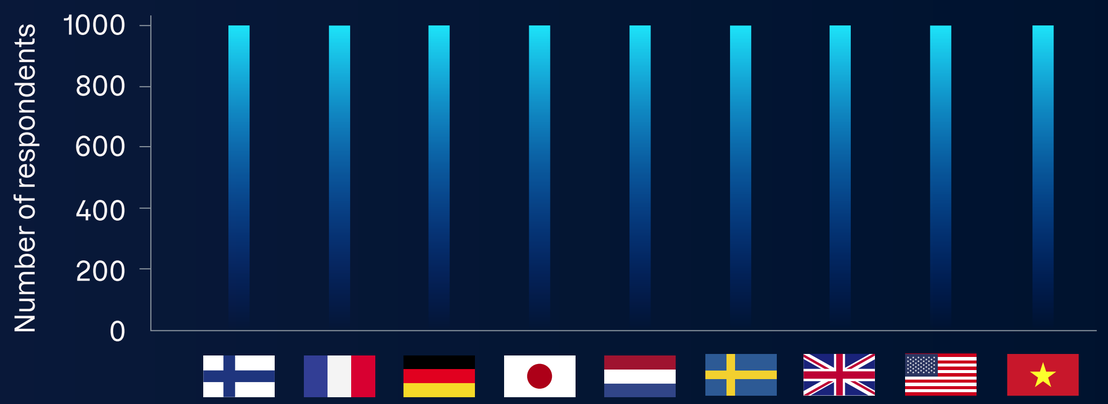
This section outlines how data was collected and analyzed for the F-Secure Digital Perception-Reality Gap Report, ensuring transparency and credibility behind the insights.

Market Research

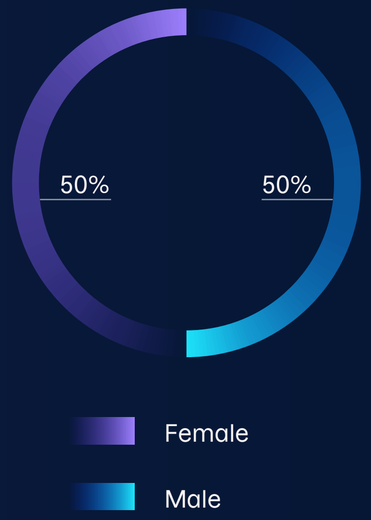
Consumer data was gathered via an online F-Secure Consumer Market Survey conducted in January 2025. While self-reported data reflects individual perception, results were validated through sample balancing to ensure demographic consistency across countries.

The survey captured responses from 9,000 consumers across nine countries, with 1,000 participants per country to ensure balanced geographic representation. Respondents ranged in age from 18 to 74, allowing for generational comparison in digital habits, and included a 50/50 gender split to reflect real-world diversity.

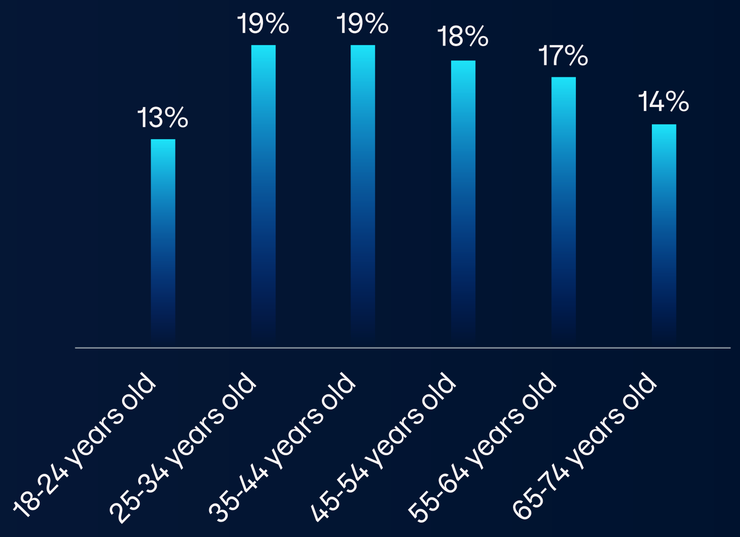
Countries surveyed



Gender



Age Group



Risk Score Framework

Two composite scores were used to assess the disconnect between perceived risk and actual threat:

- Worry Score – The number of respondents who feel worried about an online activity.
- Threat Score – Derived from expert workshops with F-Secure threat intelligence specialists, based on three weighted factors: the likelihood of threat occurrence, its potential impact, and its reach globally.

Expert Contributor

Laura Kankaala

Head of Threat Intelligence, F-Secure

- 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.

illuminate
By F-Secure

Shaping the Future of Digital Confidence

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

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

About F-Secure

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

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

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

F-Secure