F-Secure Digital Trust Report

AI Adoption in an Era of Conditional Trust

F-Secure®

Foreword: The State of Digital Trust

“Trust is one of the most fundamental forces shaping human relationships and everyday decisions. In the digital world, it strongly shapes whether users adopt and continue using services, especially when those services handle sensitive personal data or operate invisibly in the background. Yet trust in technology isn’t automatic. It’s shaped through design, transparency, perceived competence, and repeated experiences over time.

Trust is inherently linked to risk and uncertainty; it becomes necessary when outcomes aren’t guaranteed and vulnerability is involved. Because it operates under such conditions, trust can be misplaced. Over-trusting a technology may lead to misuse and harm. Conversely, when people don’t trust a technology, they may use it less or abandon it altogether, potentially missing out on its benefits.

To avoid these losses, trust must be calibrated—aligned with a system’s true capabilities. Trust calibration describes how accurately a person’s trust reflects that performance. When trust exceeds it, users may rely on a system inappropriately; when it falls short, they may ignore reliable guidance.”

Dr Amel Bourdoucen
User & Impact Researcher
F-Secure

The Role of Trust in Technology Adoption

In digital environments, where uncertainty and vulnerability are a part of everyday interactions, trust becomes central to technology adoption. And as systems grow more complex—particularly in mobile contexts—it takes more than usability alone to determine it. Research shows that trust is critical to initial acceptance. When people lack all the information, adopting a new system requires a 'leap of faith.' Here, we find that trust often outweighs other factors in shaping continued use.

However, adoption doesn't always imply genuine trust. Particularly in AI-driven contexts, people may use systems because the perceived benefits outweigh the risks, reflecting a pragmatic risk–benefit trade-off. Importantly, people may also lack trust in a technology provider yet continue using the technology out of convenience or because of a lack of options.

Security Apps as an Intermediate Trust Layer

In this image, we see how the mobile security app occupies a distinct position in the user's digital experience, sitting between goals and engagement in sensitive digital activities. Actions such as booking travel or managing finances require accepting vulnerability through data sharing and unseen risks, raising questions of trust. The security app serves as an intermediate trust layer—reducing uncertainty and enabling safer participation in the broader app ecosystem.

Security apps shape our digital experience by influencing our perceptions of safety, risk, and control. Yet because their value is preventive and less visible than that of task-oriented apps, they aren't always perceived as essential. Over time, however, convenience, seamless integration, and functional benefits may create a sense of necessity. Whether adoption is driven by trust, perceived risk, convenience, or situational dependency remains an open question.

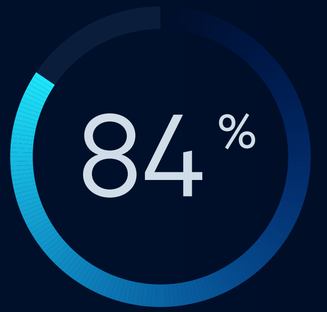
AI Is Everywhere—
But Trust is Conditional

Over the past few years, generative AI has rapidly embedded itself into everyday digital life. While some appreciate the convenience and efficiency these tools offer, there is widespread unease about what AI means for trust online.

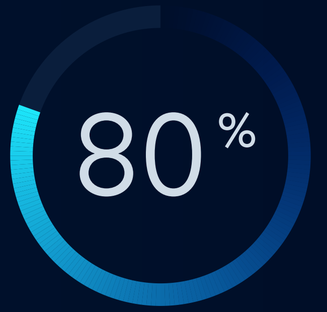
Our latest consumer research reflects the broader dynamics of conditional trust described earlier. AI adoption is accelerating, yet consumer concern remains high—focused not only on the technology itself, but also on the broader systems in which it operates.

As deepfakes, synthetic content, and automated misinformation grow more sophisticated, distinguishing between legitimate and fraudulent communications is becoming harder than ever. The challenge extends beyond detection: users must also navigate increasingly personalized and strategically targeted messages designed to shape beliefs and influence behavior at scale. This raises not only technical challenges, but governance ones as well.

These challenges extend beyond system performance to questions of power and accountability. Media narratives, regulatory uncertainty, platform dominance, and geopolitical tensions all shape how trust in AI is formed. As a result, control, accountability, and oversight are as critical as technical performance.



are worried AI will make it impossible to tell what's real online



are worried about using AI tools like ChatGPT, Copilot or Gemini

say using AI is an important online activity

Source: F-Secure Global Consumer Market Survey 2026. n = 10,000

AI's Trust Problem Is About Credibility, Not Capability

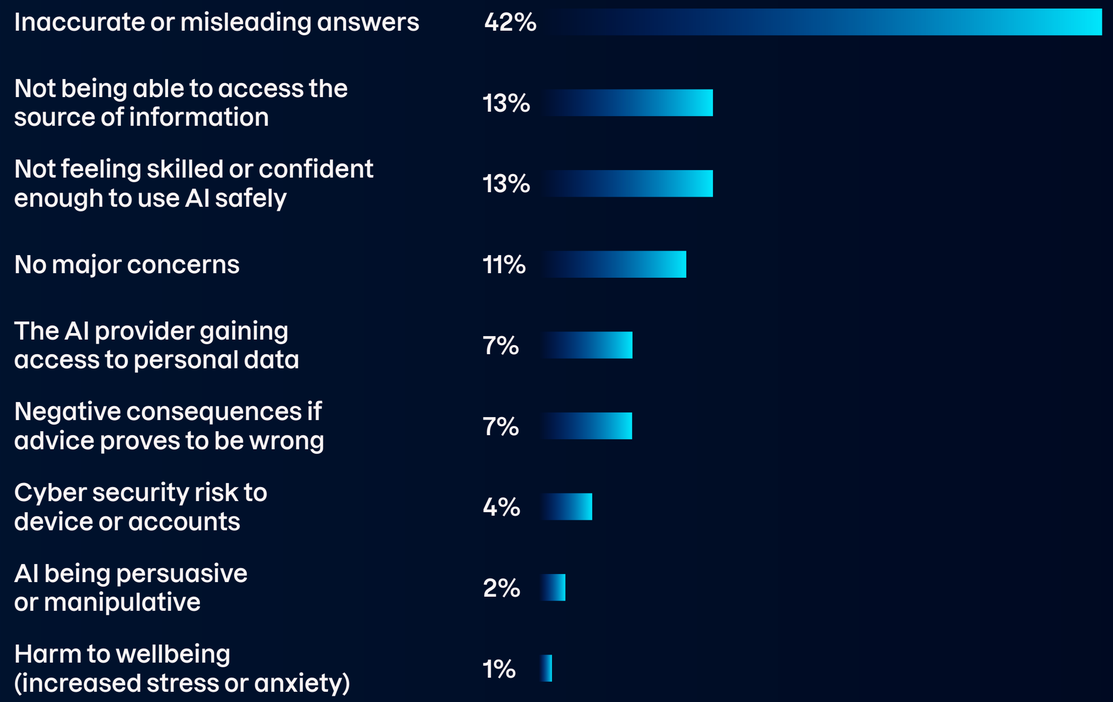
Consumers' primary concern with AI assistants isn't traditional cyber security risk—it's credibility. Inaccurate or misleading answers rank far above fears of device compromise or data theft. Hesitation reflects uncertainty about whether AI advice is reliable, verifiable, and trustworthy.

Nine out of ten respondents approach AI assistants with caution. The issue isn't access, but confidence in accuracy.

What this means for digital service providers:

Trust must be earned visibly over time—positioning transparency and verification as stronger differentiators than capability alone.

Biggest concerns about the security or safety of using AI assistants



Source: F-Secure Global Consumer Market Survey 2026. n = 10,000

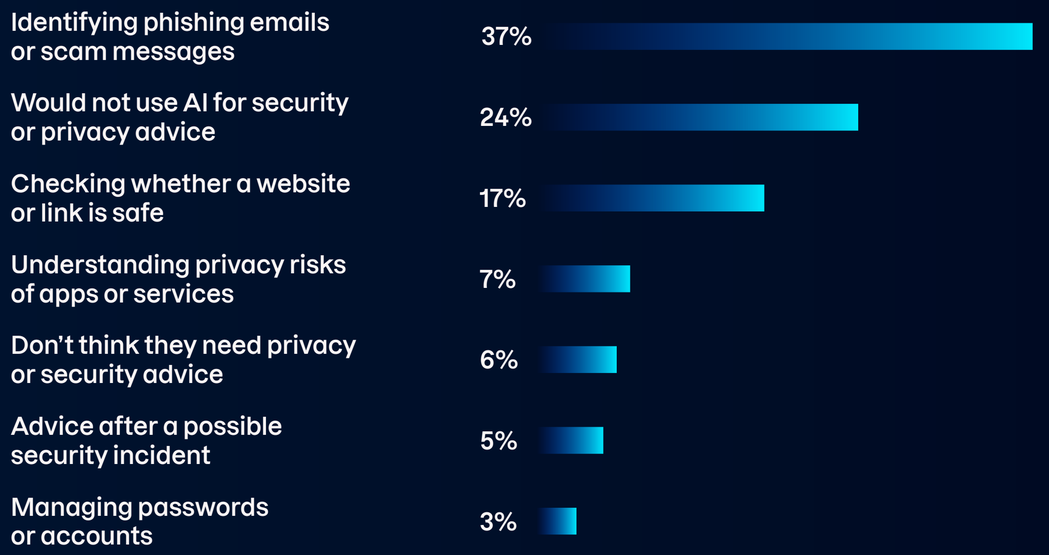
Security Is Where AI Creates Real Value

Despite broad hesitation, consumers show clear openness to AI in one area: cyber security support.

Likelihood of using an AI assistant for cyber security help

Many are willing to turn to AI when facing uncertain or high-risk situations, particularly phishing and scam detection. This signals an important pattern: AI can be valuable not as a general-purpose assistant, but as support in stressful moments when human judgment may not be sufficient.

Situations consumers would consider using an AI assistant for security advice



Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Trust, however, remains selective. Nearly one in four consumers wouldn't use AI for security or privacy advice. When responses sound confident but prove inaccurate, trust deteriorates quickly—especially in high-stakes security contexts.

What this means for digital service providers:

Consumers may be wary of AI companies, but they place clear expectations on their mobile and broadband providers: 80% expect protection from cyber threats, and 93% believe offering cyber security is important. By embedding security-focused AI within established customer relationships, providers can engage users at critical decision points, turning hesitation into reassurance.

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Trust Is Conditional—Reliability Must Be Demonstrated

Barriers to adopting AI for security advice mirror broader concerns around credibility and verification. The leading deterrents are doubts about accuracy and the inability to verify sources.

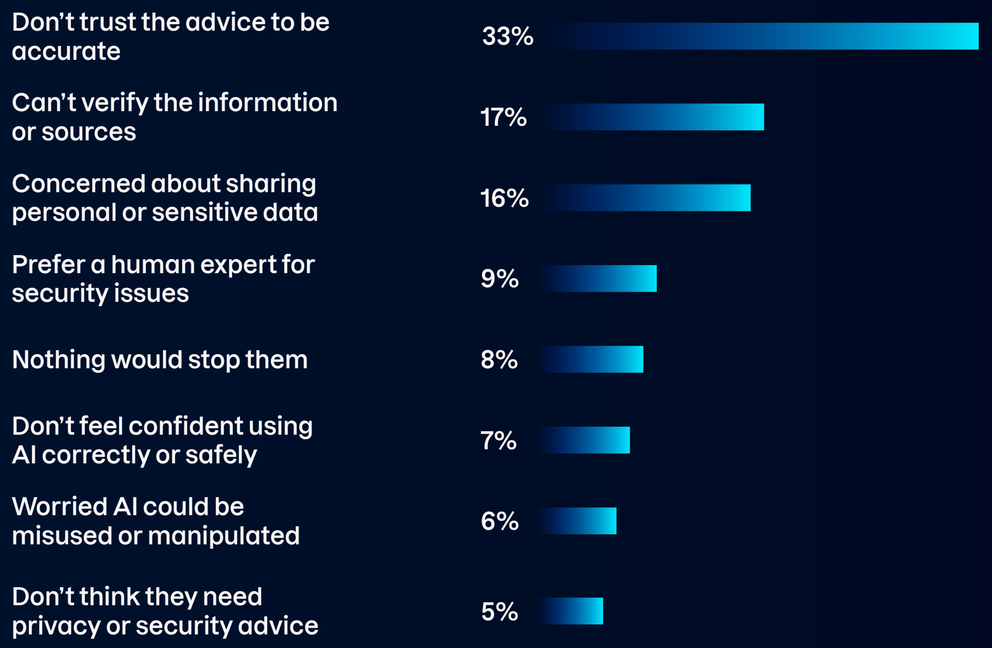
Consumers aren't rejecting AI outright. Instead, trust appears conditional. Confidence is lower when reliability and verification are unclear, particularly in situations where guidance could have real-world consequences.

Even so, many continue to use AI. The benefits are immediate and often hard to avoid—whether staying connected in online communities or using AI tools at work—while the risks can feel unclear. When alternatives are limited or less effective, convenience tends to outweigh concern.

What this means for digital service providers:

In high-stakes contexts, AI must meet a higher standard. Transparent safeguards and access to human expertise strengthen confidence and drive adoption.

What might stop consumers from using an AI assistant for security advice



Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Trust in AI Is Built on Agency and Control

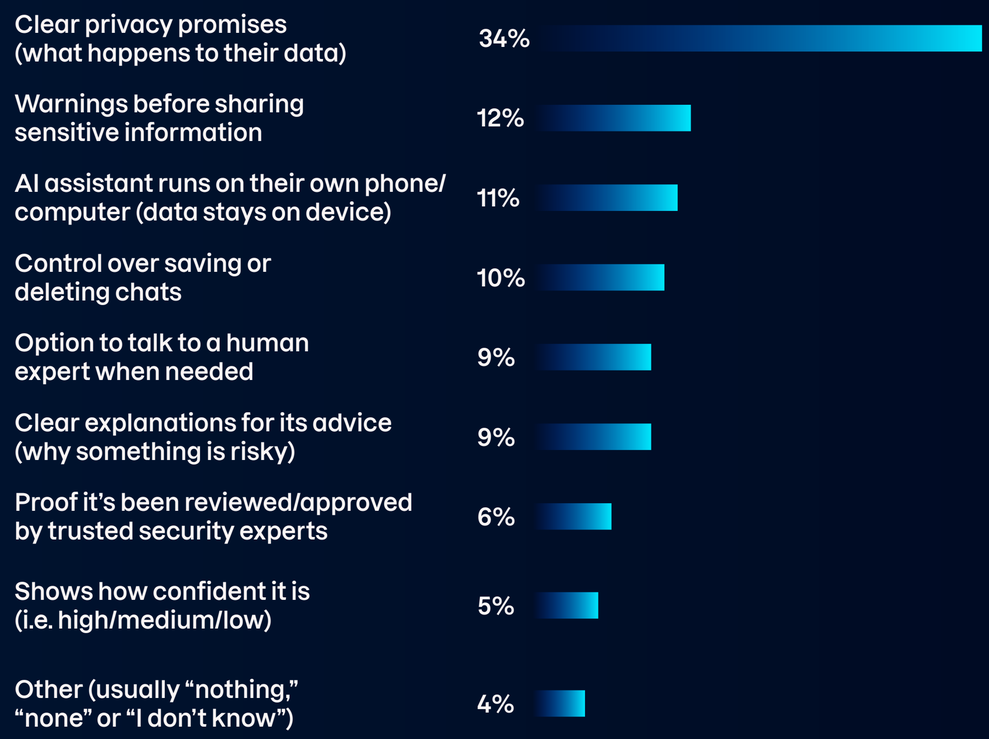
The strongest drivers of trust cluster around user control and transparency.

This shows that trust in AI is built on control and transparency rather than advanced features alone. It stems from agency: consumers want to understand how the system works, decide what data is shared, and retain oversight of its decisions.

What this means for digital service providers:

Designing AI around visibility, choice, and accountability—and positioning security as a core pillar of the customer relationship—strengthens not only protection, but trust, differentiation, and long-term growth.

Features that would increase trust in AI used for security guidance



Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

Setting a Higher Standard for AI Security Guidance

“Consumer acceptance of AI remains selective and conditional, and some consumers are strongly opposed to it. Many hesitate to use LLM-based AI platforms for security guidance because they understand that these systems can generate inaccurate or unverifiable responses. At the same time, finding reliable information online is becoming more difficult, making independent verification of such advice much harder.

Half of respondents said their primary concern about using an AI assistant for security advice was either potential inaccuracy or their inability to verify the information provided. That creates a clear opportunity for F-Secure and our partners to raise the standard and define a more trustworthy model for AI-driven security guidance.”

Dr Laura James
Vice President of Research
F-Secure

Repositioning Digital Security: 5 Recommendations for Service Provider Partners

The findings across this report point to five strategic shifts digital service providers should prioritize when repositioning their AI-powered digital security offering to customers.

1 Lead with trust, not features

Customers aren't motivated by security capabilities—they're motivated by confidence in you. Position security as an extension of the trusted relationship they already have with you as their telco or financial provider, not as a standalone product.

2 Anchor AI-powered security in your brand

80% of consumers are uneasy about AI tools, yet 43% would use AI for cyber security help. At the same time, 93% say it's important their telco offers cyber security, and 80% expect their provider to keep them safe. You are uniquely positioned to make AI feel trustworthy by delivering security and guidance through a brand customers already trust.

Source: F-Secure Global Consumer Market Survey 2026, n = 10,000

3 Shift messaging from protection to peace of mind

Scam detection and phishing identification are the top use cases consumers want help with. Lead with real pain points ("Is this message a scam?") rather than abstract threat statistics.

4 Make AI transparency visible

Clear data privacy promises, proactive warnings before sharing sensitive information, and plain-language explanations are the strongest trust-builders. Embed these into your user experience and customer communications.

5 Sell calibrated trust, not just security

Consumers are withholding trust until reliability is proven. Create visible moments of protection—alerts, confirmations, clear explanations—that build confidence over time, rather than asking customers to trust systems blindly upfront.

“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.”

Dr Laura James
Vice President, Research
F-Secure

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