STUDY

The global cybersecurity awareness report

A digital confidence paradox

2026

How consumers worldwide navigate digital adoption, cybersecurity and emerging technologies.

IDEMIA SECURE TRANSACTIONS

IPSOS BVA survey conducted for IDEMIA Secure Transactions
11 countries surveyed: France, Brazil, Japan, Malaysia, Mexico, Poland, South Africa, Sweden, United Arab Emirates, United Kingdom, United States of America.
3,303 respondents all aged 15+
February–March 2026

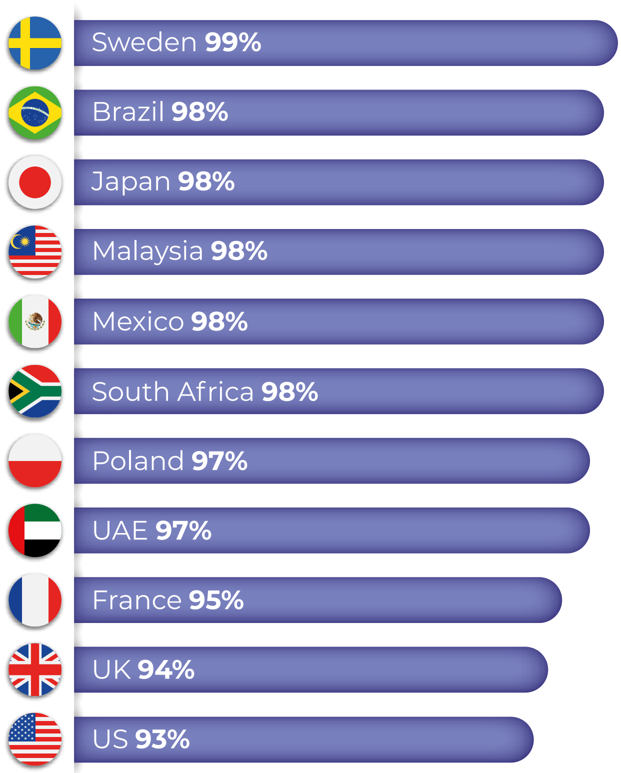
1 Digital adoption is accelerating worldwide but trust is at a crossroad

Digital services are now deeply embedded in everyday life across all regions of the world. From payments and connectivity to digital identity and online services, consumers increasingly expect seamless and instant digital experiences.

At the same time, concerns around cybersecurity, fraud and data protection continue to intensify. The study reveals a growing paradox: **while digital adoption keeps accelerating, users' understanding of increasingly sophisticated cyber threats is struggling to keep pace**.

In this context, users are expecting their digital services to be secured by design by their providers.

96%
of respondents globally describe themselves as frequent users of digital tools



74%

are concerned about fraud and personal data theft when using digital services

Cybersecurity concerns, such as fraud and data theft, are now a mainstream issue across all markets surveyed and half of respondents declare they are more worried than 5 years ago when using digital services.

67%

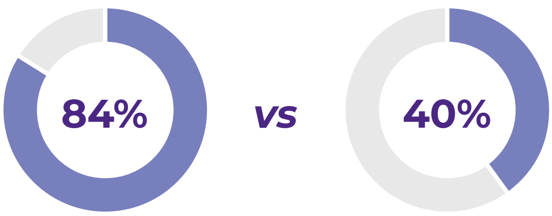
believe AI-driven cyberattacks are increasing cybersecurity risks

Consumers increasingly associate artificial intelligence with more sophisticated cyber threats, reinforcing concerns around the growing complexity of digital security.

44%

admit they do not really understand cybersecurity risks

The study reveals a major gap between awareness and understanding. While most consumers know cyber threats exist, many struggle to fully understand how these risks work or how they may be exposed.



81%

have never heard about quantum computers or don't know what they involve

While quantum computers could put at risk our modern cryptography as soon as 2030, a vast majority of respondents isn't aware of what it could mean for their cybersecurity.

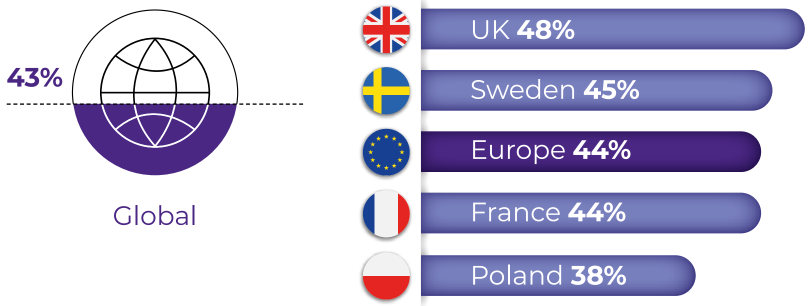
2 The rise of digital trust challenges across regions

While digital adoption is now global, attitudes toward trust, cybersecurity and emerging technologies differ significantly from one region to another. Some countries embrace innovation rapidly, while others adopt a more cautious and security-driven approach.

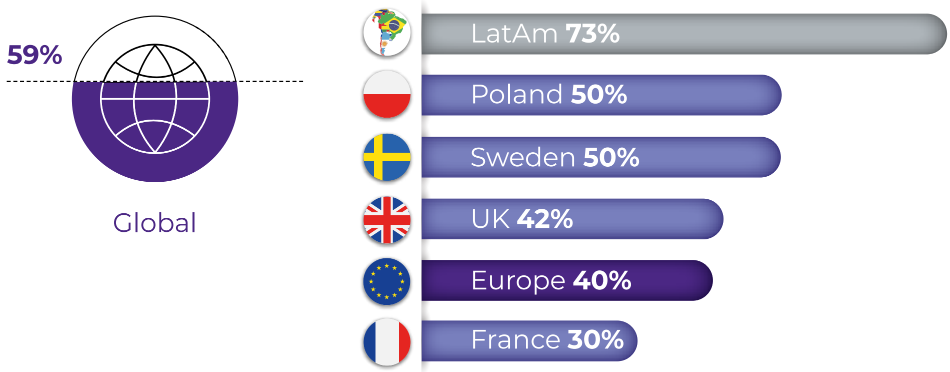
EUROPE | Mature but cautious

European consumers are highly digitalized but tend to adopt a more cautious approach toward digital trust and cybersecurity. They show strong concerns around fraud and personal data protection, while remaining more selective in adopting emerging technologies such as eSIM or cryptocurrencies.

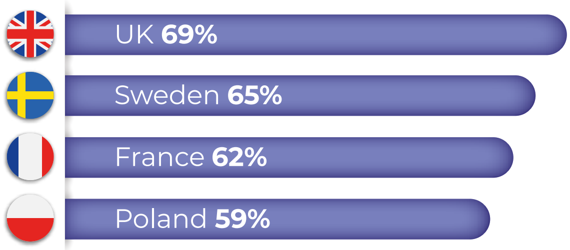
Consider security the #1 criterion when choosing a digital service:



Smartphone eSIM equipment:



Quantum computing as a cybersecurity threat*:

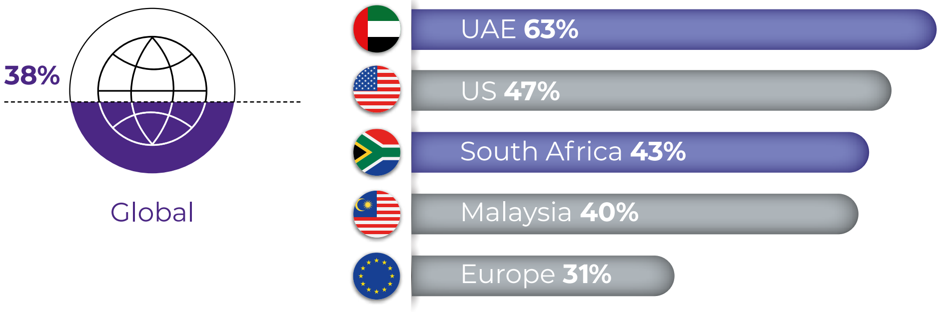


* Among people having heard about quantum computers

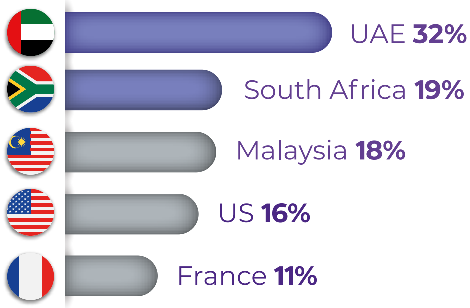
MIDDLE EAST & AFRICA | Strong digital enthusiasm, strong cyber concerns

Countries such as the UAE and South Africa combine extremely high digital engagement with some of the highest levels of cybersecurity concerns globally. Respondents in these markets also report the highest amounts of hacking and data theft.

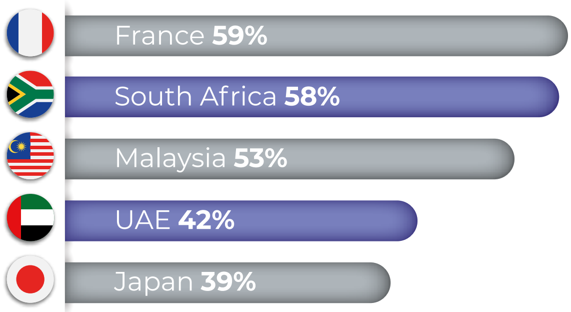
Declare to have already experienced hacking or data theft...:



...and declared it had financial consequences:



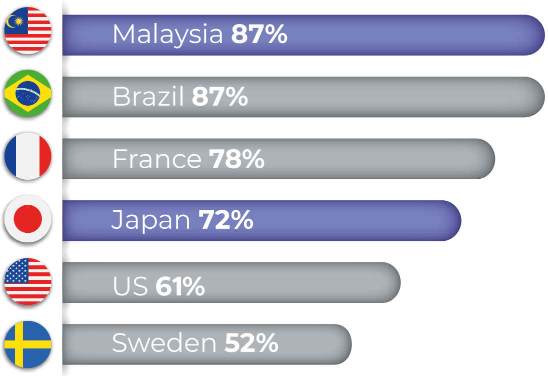
Report feeling more vulnerable online than 5 years ago:



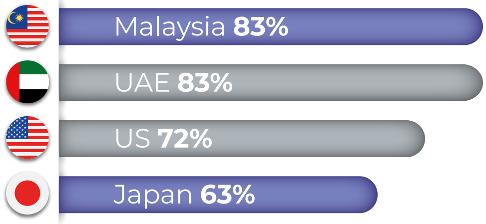
ASIA | High digital adoption with important trust challenges

Asian markets surveyed demonstrate strong digital usage but also reveal important gaps in cybersecurity understanding and trust. Malaysia stands out as one of the most digitally engaged countries surveyed, while Japan shows a more cautious relationship with digital services.

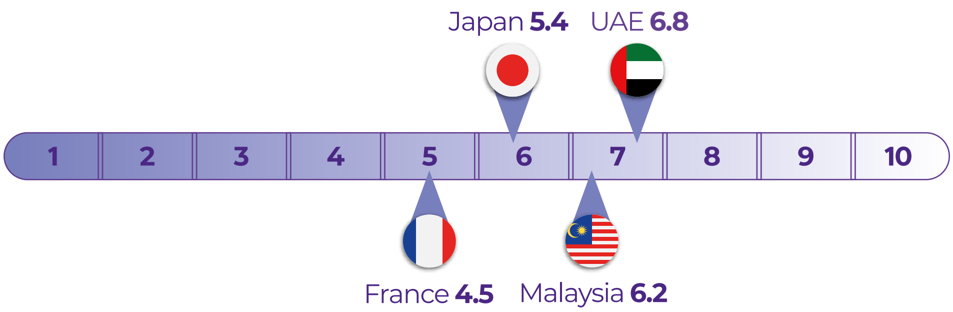
Concerns about digital fraud:



Quantum computing as a cybersecurity threat:



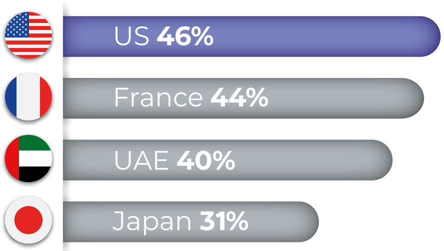
Cyber-trust in GAFAM:



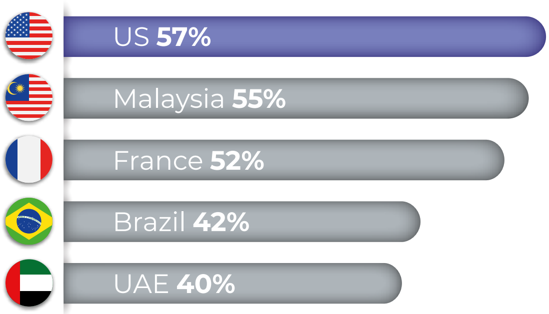
UNITED STATES OF AMERICA | Tech-savvy with cautiousness

American consumers combine strong adoption of digital services with a pragmatic relationship to cybersecurity. While digital payment usage and connected services are now mainstream, concerns around fraud, hacking and personal data theft are widespread, becoming an expectation for digital services to deliver strong built-in protection.

Level of security as a key criterion for choosing a digital service:



Private data considered as the most important security aspect:



3 Cybersecurity is becoming a core expectation across digital services

Across sectors, cybersecurity is no longer seen as an optional feature, but as a core component of user experience and trust.

eSIM | Convenience and security go hand in hand

Consumers primarily associate eSIM technology with convenience and flexibility. At the same time, security-related benefits — such as easier device protection in case of theft or loss — are being recognized.

47%
cite convenience as the main advantage

44%
cite security in case of theft/loss

Smartphone eSIM equipment:

PAYMENTS | Security is now part of the expected experience

Consumers expect payment experiences to combine simplicity with stronger control over security and privacy. Interest is particularly high for services allowing users to manage payment security directly from banking applications.

63%
see ease of payment as the main advantage of digital payments

61%
associate digital payments with cybersecurity benefits

Interested in managing payment settings from websites and apps via their banking apps:

AUTOMOTIVE | Trust is essential

As vehicles become increasingly connected, consumers expect mobility services to integrate stronger security mechanisms. Digital car keys are perceived not only as more convenient, but also as potentially more secure than traditional keys or remote control systems.

47%
associate digital car keys with stronger security

34%
value not carrying physical keys

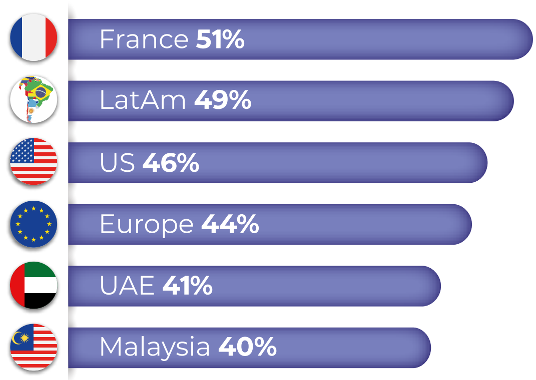
27%
cite biometric authentication benefits

CRYPTOCURRENCIES | Awareness is high, trust remains fragmented

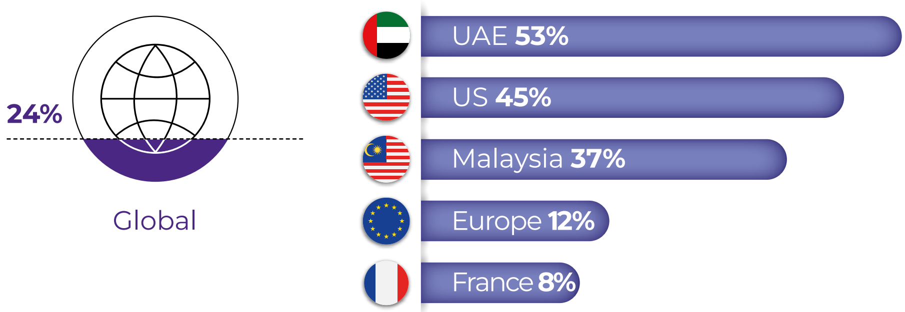
While cryptocurrency awareness is now nearly universal, trust and understanding remain uneven across markets and providers. Users continue to seek reassurance around wallet security, key management and trusted intermediaries.

94%
have heard about cryptocurrencies

Say they understand how they work:



Say they use them:



4 Preparing for the future of digital trust

The study highlights a broader transformation of the digital economy: consumers increasingly expect digital experiences to remain seamless, while demanding to their service providers stronger built-in protection against rapidly evolving threats.

Marc BERTIN,
CTO at IDEMIA Secure Transactions

“In today's digital economy, trust is as important as innovation itself. Consumers expect digital experiences to remain instant, seamless and intuitive, while also demanding stronger protection against increasingly sophisticated threats. Our findings demonstrate that while digital adoption continues to accelerate worldwide, understanding and confidence are not always evolving at the same pace.

At IDEMIA Secure Transactions, **our mission is to ensure that every payment, connection, movement and exchange of data is secure by design, with the strong conviction that security fosters trust.** As technologies such as AI, connected ecosystems and quantum computing reshape the cybersecurity landscape, the challenge for our industry is no longer only to secure transactions but also **build digital trust that is resilient, transparent and future-ready.”**

Related news from IDEMIA Secure Transactions

- IDEMIA Secure Transactions Unveils IDEMIA Sphere Cryptographic Library: A Certified Set of Algorithms for Quantum-Safe Security
- IDEMIA Secure Transactions Announces its First Hardware Accelerator Designed for Post-Quantum Cryptography
- IDEMIA Secure Transactions unveils a groundbreaking crypto agility solution for Post-Quantum
- The stakes of post-quantum cryptography

We make it possible

IDEMIA GROUP

www.idemia.com