After the scam: The emotional and financial impact of global fraud

A 2026 global survey

LSEG RISK INTELLIGENCE

Foreword

David Wilson,
Group Head of Risk Intelligence, LSEG

Financial scams have become one of the defining risks of the digital age and are now a global, mainstream threat that undermines trust in financial institutions and leaves a lasting emotional impact on its victims.

Our latest research explores how 21,000 adults across APAC, EMEA and North America perceive fraud risk, experience its impact, and struggle to navigate its aftermath. The findings reveal scams rising sharply worldwide and growing in sophistication – but the deeper story is the human crisis unfolding behind the statistics.

The **damage from fraud goes well beyond losing money because at its core every transaction or payment tells a story.** This is even more critical when it comes to scams with victims hesitating to transact online, retreating from the digital channels financial institutions depend on – losing trust not only in brands but in their own judgment, or hiding their experience – too embarrassed to even tell family.

The weight of these scams hits generations in different and nuanced ways. While younger generations are losing money more often, older generations feel more affected emotionally. And all victims are left to navigate shame, fear and uncertainty with little guidance or restitution in most cases.

Banks, payment processors, fintechs and technology providers have made substantial progress in strengthening fraud detection, prevention and customer protection. There is an ongoing opportunity and responsibility to continue advancing these efforts by further strengthening risk management and education, so that the digital economy feels not only more secure in theory, but genuinely safer and easier to navigate in everyday life.

Key findings

1 Scams and fraud are perceived as rising sharply worldwide

71% of adults globally believe financial scams are increasing, including 44% who say they are rising "significantly," with concern highest in markets like Australia, France and the UK.

2 Personal exposure and loss are widespread across markets and age groups

26% of adults have been personally targeted by a financial scam in the past two years, and 35% know someone who has. Of those targeted, 42% lost money – about one in nine adults around the world has already lost money to a scam.

3 AI-enabled and professional looking scams are amplifying impact and delaying detection, more strongly affecting younger, digital-first consumers

Phishing, impersonation and payment scams remain the most common, but more than one in five adults – and two in five for Gen Z-ers – has encountered AI-generated images, voice clones or deepfakes, contributing to the 15% of victims who took over a year to realise they'd been scammed.

4 The emotional and behavioural damage is long lasting

Over half of victims (52%) report anger or frustration and a third feel embarrassment or shame, while 97% say their behaviour has changed after being scammed - typically becoming more cautious with online payments, sharing fewer financial details and avoiding certain channels.

5 People are trying to protect themselves, but gaps remain

Many use strong passwords and multifactor authentication, yet only 13% say they fully understand what protections or reimbursements they are entitled to if scammed, and 28% are unaware of any protections at all, exposing a critical communication and education gap.

Research methodology

This report is based on an online survey conducted between November and December 2025, involving over 21,000 adults across 14 markets in APAC, EMEA and North America. The sample was designed to reflect a broad range of ages, digital behaviours and regional contexts, enabling analysis of fraud exposure, impact and risk perception across generations and geographies. The survey also explored emerging threats, including AI-enabled scams. For full details on sample composition, geographic coverage, scam definitions and generational cohorts, please refer to the full methodology in the Appendix.

Scammers target everyone, with Gen Z the most vulnerable

Scams today are highly produced, data driven and psychologically tuned attacks that blend seamlessly into the digital experiences people rely on every day, which is why even informed, tech savvy consumers are getting caught. Scammers are layering different tactics to create urgency, using FOMO (the fear of missing out on an opportunity) or exploiting existing trust.

Seven in ten adults worldwide say scams are increasing, and nearly half believe they are rising "significantly," with concern peaking in countries like Australia (81%), France (81%) and the UK (80%). Even in markets where anxiety is lower, such as Singapore or Germany, a clear majority (58%) still sees scams as a growing problem, and every generation – from Gen Z to Baby Boomers – recognises that the threat is building.

It's not just perception. More than a quarter of participants in our survey report have been directly targeted by a financial scam in just the last two years, and a third say someone they know has been targeted. In some countries, such as the UAE, Canada, Australia and the United States, around a third or more say they have personally been targeted.

Actual victims report real financial losses. Among those who have been targeted, over two in five (42%) have lost money – equivalent to about one in nine adults worldwide suffering a direct loss in just two years. Some countries like the UAE, Switzerland and Spain, appear more susceptible to losing money, while even in countries with lower loss rates, around a third of targets still lose money.

One in nine adults worldwide is suffering a direct loss in just two years.

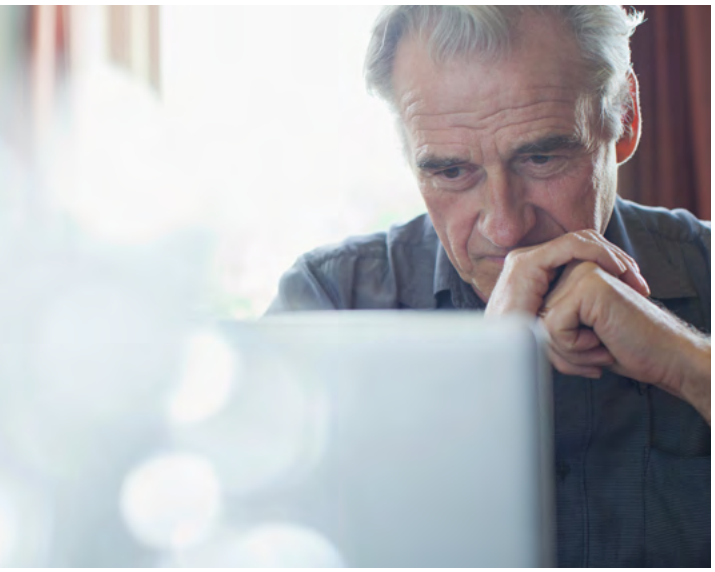
A deepfake-driven investment scam built for the scroll

A Gen Z professional is scrolling social media when an ad for a "crypto side hustle" pops up with a convincing, AI generated video of a well known influencer explaining the opportunity. It links to a sleek landing page mimicking a familiar trading app, complete with glowing reviews and phoney returns.

An "advisor" over chat ramps up the pressure – warning that the opportunity window is closing – while sending a QR code for "quick account verification" and an initial transfer. Distracted and worried about missing the chance, the victim scans the code and sends funds from a mobile banking app – and just like that, money is gone.

Baby Boomers: highly targeted but less likely to lose money

Everyone everywhere is a target, but there are important nuances to the vulnerabilities of each generation. For example, Baby Boomers are the most heavily targeted by phishing (57%) and payment scams (46%) among those who encounter scams, but overall, they lose less money compared to younger generations. Only 32% of targeted Boomers report losing money, compared with 49% of Gen Z and 47% of Millennials, and their losses on payment scams are lower as well – around 6% versus 10% for Gen Z.



The older generations face somewhat lower exposure to investment, deepfake and quishing scams, reflecting more cautious digital usage and less engagement with newer channels. Where Boomers are particularly at risk is with professional looking, impersonation style scams that appear reliable - attacks that play into their higher trust in polished communications and established institutions.

A Call from ‘the Bank’ that cost a lifetime of savings

A Baby Boomer gets an unexpected call and branded email from his bank’s fraud department recapping “suspicious activity” on his account.

The voice on the phone explains that to “protect” his savings, he needs to move funds into a new “safe account” while the investigation is under way. The script is professional, emailed security warnings convincing, so the Boomer authorises a series of transfers and confirms them via text codes.

Only later does he discover that the “fraud team” never existed, security cues were fabricated, and now a large share of his retirement savings is gone.

Gen Z: always online, overexposed to digital scams

Interestingly, younger generations seem particularly vulnerable: nearly half of Gen Z and Millennial victims report losing money, compared with about a third of Baby Boomers. This may seem counterintuitive, as one might expect younger generations' greater familiarity and engagement with technology to arm them with more savvy in spotting scams. But that same high level of engagement — with technology woven into nearly every aspect of Gen Z's lives — also exposes them to significantly more opportunities for scammers to reach them.

Gen Z faces a broad mix of scams, with 42% of those targeted reporting phishing attempts and 41% seeing payment scams, and they are especially vulnerable to the latter. When hit by payment scams, Gen Z records a 10% loss rate versus 6% for Baby Boomers, and around 34% report exposure to investment scams, which carry high loss rates across the board.

They are also the most exposed to emerging formats: 25% report deepfake scams and 23% quishing scams, with loss rates of about 4% for each. This pattern shows that younger adults are heavily targeted across channels and more likely to lose money when confronted with slick digital, AI driven and "fast money" offers.

Nearly half of Gen Z and Millennial victims report losing money, compared with about a third of Baby Boomers.

Millennials: digitally fluent, financially exposed

Millennials see high exposure to traditional scams – 53% report phishing, 44% payment scams and 34% impersonation scams among those targeted – and they frequently lose money when investment or payment scams hit. **About 35% have been targeted by investment scams, and Millennials, along with Gen X, show the highest loss rates on these offers at 10%.**

They also sit at the leading edge of newer threats, with 29% encountering AI generated images and elevated exposure to deepfake and quishing scams compared with older generations. As a result, Millennials straddle both worlds: they see the full range of legacy and AI enabled scams and are disproportionately likely to suffer financial harm from higher risk, "opportunity driven" frauds.

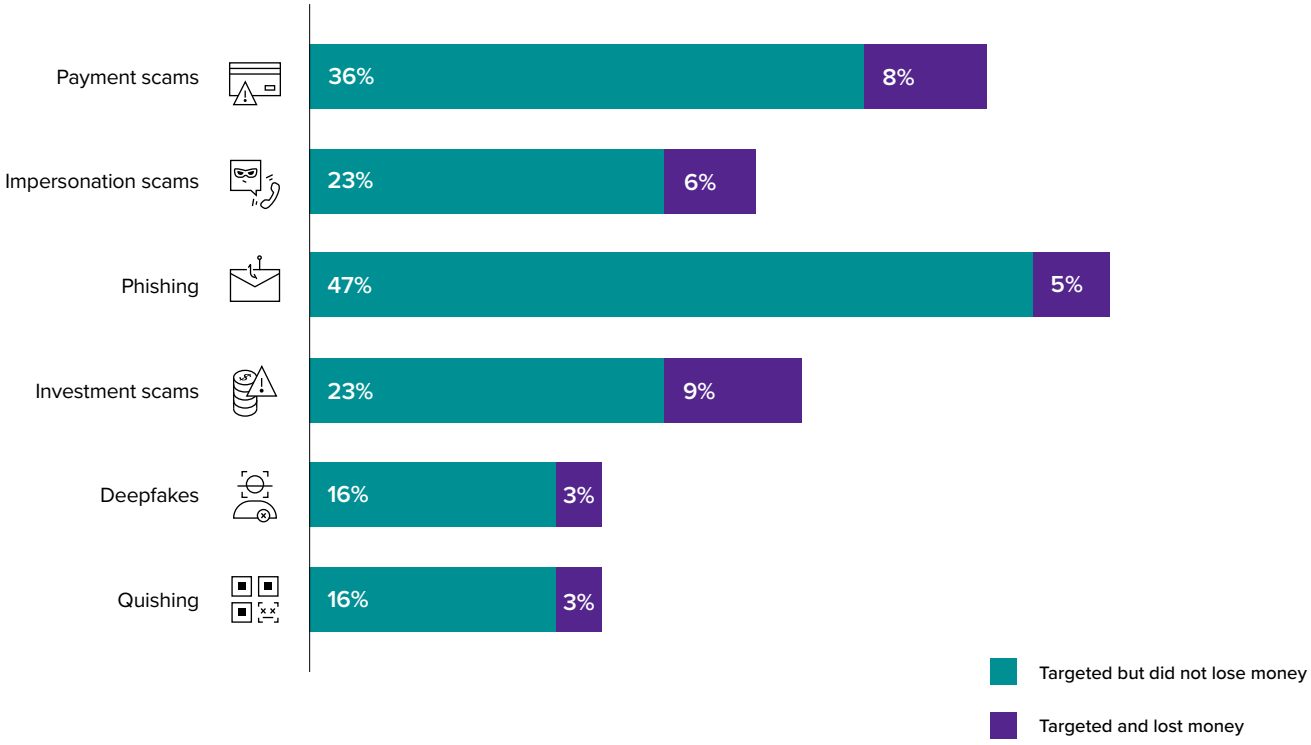
Gen X: busy, sceptical and still in the crosshairs

Gen X experiences consistently high exposure to the core scam types: 55% report phishing, 45% payment scams, 32% investment scams and 28% impersonation scams among those targeted. Like Millennials, Gen Xers record a 10% loss rate on investment scams, making them one of the groups most likely to lose money when pitched high return financial opportunities.

Their loss rates on other scams – such as phishing and payment fraud – are midrange: higher than Boomers' but generally lower than Gen Z's. This suggests Gen X combines substantial digital exposure with enough assets and risk appetite to make them attractive targets for more sophisticated financial pitches.

How people are targeted by different scams and where they lose money

Among people who have been targeted by financial scams:



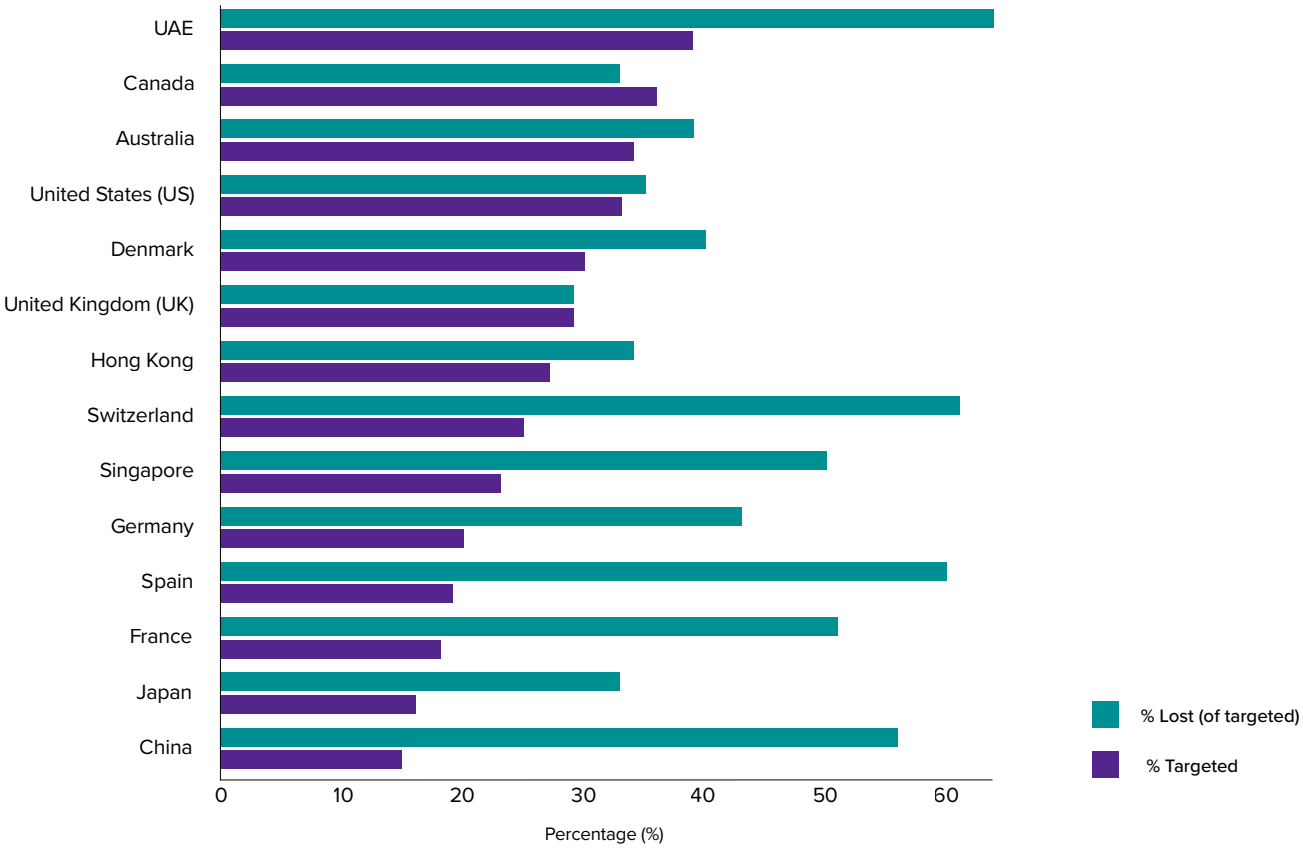
Location matters: where you live shapes perceptions and exposure to scams

Fraud is recognised as a growing issue worldwide, but intensity of concern varies widely. While over a quarter (26%) of people around the world stated they have been targeted by a financial scam, those in the UAE (39%), Canada (36%), Australia (34%) and the USA (33%) are most likely to say they personally have been targeted by a financial scam in the past two years. In contrast, those in France (18%), Japan (16%) and China (15%) are least likely to report having personally been targeted by a scam.

Further, certain countries appear more susceptible to losing money with the highest proportions seen in the UAE (64%), Switzerland (61%) and Spain (60%) whereas participants in Canada (33%), Japan (33%) and the UK (29%) are far less likely to have lost money to a financial scam after being targeted.

This may suggest that local factors – such as consumer education programmes or the maturity of fraud controls – may shape how often an attempted scam turns into an actual financial loss.

How financial scams targeting translates into financial loss - All countries:



The emotional cost of fraud and its impact on trust

Understandably, being scammed can evoke a wide range of emotions, with negative feelings far outweighing positive ones. Anger and frustration are the most reported emotions (52%), with this figure substantially higher among Baby Boomers (66%).

Anxiety or fear around money and finances is also commonly felt (34%) and is even more prominent in Hong Kong (51%) and Australia (42%).

Alarmingly, women are much more likely to experience this than men (40% vs 29%).

A third (32%) experienced embarrassment or shame, an emotion reported by nearly half of those in the UK (47%), the USA (41%) and Canada (41%).

Baby Boomers are the most likely to experience shame across all generations (39%).

Other emotional impacts of being scammed include guilt (28%), feelings of helplessness or loss of control (28%), and stress or sleep difficulties (25%) or feelings of disempowerment (19%).

While just one in seven (14%) report feeling paranoia, this is higher among younger generations, with 19% of Gen Z and 18% of Millennials.

From a more positive perspective, 7% say they felt empowered after being scammed and losing money.

Scams are changing behaviour, whom consumers trust

It is evident that experiencing a scam affects people's behaviour, with nearly all adults (97%) admitting their behaviour changed after being scammed. Nearly half (46%) say they are now more cautious when making online payments, highlighting how scams can influence decision making in the long term. This rises sharply to 64% among those in the UAE.

- Globally, those who have been scammed are taking greater care and carrying out more due diligence in their financial transactions, with two in five being more careful about where and how they share their financial details (41%). This is especially the case in China and the UAE (50% and 66% respectively).
- Furthermore, nearly two in five (37%) double check the legitimacy of the companies before making financial decisions, rising to 49% for Canadians
- And the same proportion (37%) avoid certain types of transactions or channels, rising to 47% in Singapore and 55% in UAE

The impact of losing money to scams on behaviour disproportionately affects older victims. Across the most common ways in which victims have changed their behaviour, Baby Boomers are significantly more likely to report doing them:

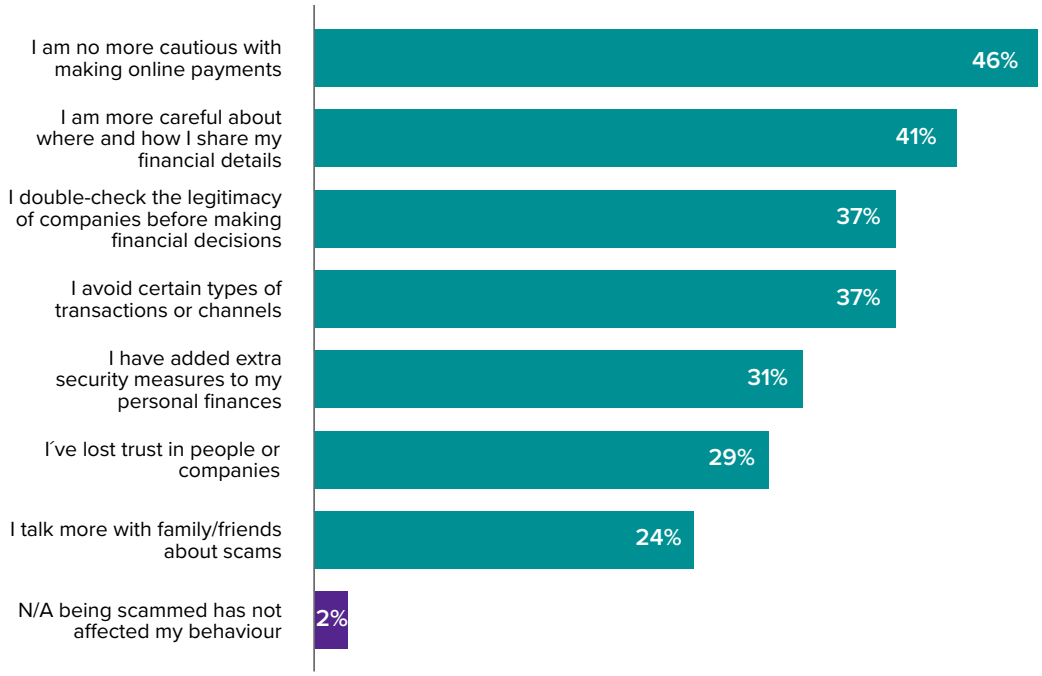
- Being more cautious with online payments (58%)
- Taking more care when sharing financial details (52%)
- Avoiding certain transactions or channels (both 44%).

Evidence shows scams have a lasting impact on consumer confidence, eroding trust in financial transactions, companies and even people more broadly. Across all victims, other behaviours changes include:

- Avoiding certain types of transactions or channels (37%)
- Adding extra security measures to their personal finances (31%)
- Losing trust in people or companies (29%)
- Talking more with family/friends about scams (24%)

Nearly all adults (97%) admit their behaviour changed after being scammed.

Behavioural impact of being scammed



While some of these changes are positive, because people are taking additional steps to protect themselves, others are more concerning. They suggest that scams have a lasting impact on consumer confidence, eroding trust in financial transactions, companies and even people more broadly.

The impact of AI-generated content illustrates the magnitude of this trust erosion, which could complicate financial companies' ability to engage with customer and prospects.

Since being exposed to AI-generated content, over two in five (44%) people say they are less trusting of phone calls from numbers they do not recognise. Beyond phone calls, 39% are less trusting of celebrity or CEO adverts with poor quality, 37% are less trusting of low-quality video calls, and 36% are less trusting of voice notes sent via messaging apps.

Evidence shows scams have a lasting impact on consumer confidence, eroding trust in financial transactions, companies and even people more broadly.

Gaps highlight need for focus on education

Education appears to be a crucial fault line. People who feel poorly educated about scams are far more likely to lose money when they are targeted, suggesting that awareness and practical know-how can make the difference. In our data, 58% of participants who lost money say they were poorly educated.

Somewhat paradoxically, participants globally generally believe they are educated about how to protect themselves from financial scams. Nearly a quarter (24%) say they are very well educated, while over half (54%) report being somewhat educated. While this is positive, there is still room for further education and improved understanding. A further 14% say they are poorly educated, while 4% feel they have not been educated at all.

But geographic differences emerge. Most Americans and Australians feel they have been educated in how to protect themselves including almost a third in both populations who state they have been very well educated. Japanese participants reported the lowest levels of education with only half (51%) stating they feel educated compared to 37% who believe they are uneducated about scams.

Low awareness of protections and reimbursements

There is a clear gap in knowledge when it comes to understanding what protections and reimbursements are available when someone is scammed. Just one in eight (13%) say they are aware of these protections. Even among those who were scammed in the past two years, only 17% say they are fully aware of what they are entitled to, indicating that scam protections are not being communicated effectively to those who experience them or that victims are not seeking help for other reasons.

Overall, the data points to a significant information gap. Low awareness, even among those directly affected, suggests governments and financial organisations may need to do more to clearly communicate available protections and help people recover more effectively from scams.

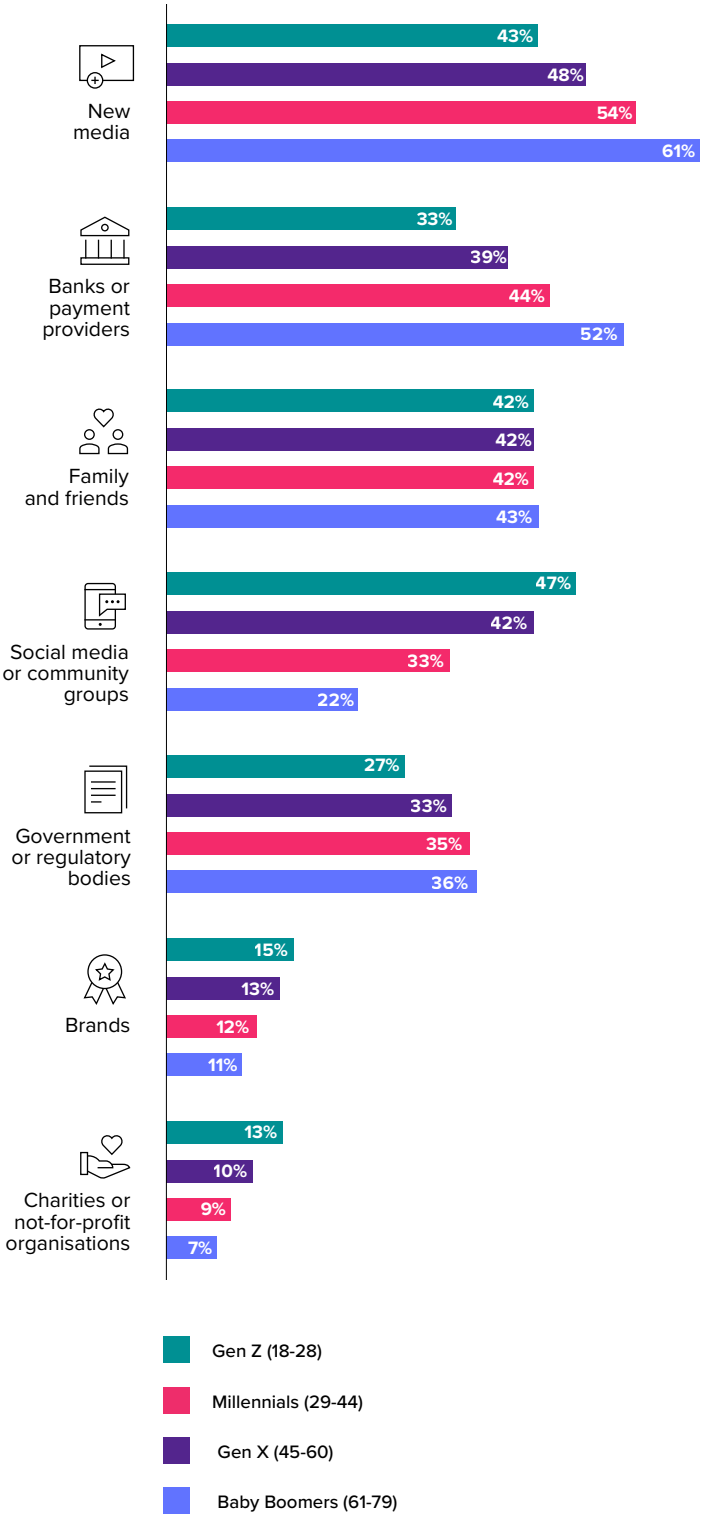
Education sources point to opportunity for financial institutions

People use a wide range of sources to get information about scams. Younger generations are more likely to use social media or community groups, with nearly half of Gen Z (47%) and two in five Millennials (42%) turning to social media. This makes social media the most commonly used source among Gen Z and Millennials.

However, consumers are also turning to their financial institutions for education. Banks or payment providers are cited by all participants including nearly half (44%) of Gen Z participants and 52% of Boomers.

Overall, this indicates that generations are receiving information about scams through different channels. This may influence how they perceive scams, how they respond to them, and the level of trust they place in different sources of information.

Where consumers primarily get their information about scams and how to protect themselves



Consumers are taking steps to protect themselves against fraud, but gaps remain

In response to the rise in scams worldwide, consumers are adopting a range of measures to protect their personal information, but some clear generational differences emerge. Older generations are more likely to already be taking safety precautions than younger generations. For example, use of strong passwords across all accounts is highest among Baby Boomers (59%), followed by Gen X (56%), Millennials (53%) and Gen Z (47%).

This pattern is consistent across most behaviours: for seven of the eight security measures asked about, Baby Boomers are the most likely to already be taking these precautions, while Gen Z are the least likely.

Differences also exist between countries. Those in Denmark (56%), Germany (52%) and Switzerland (51%) are most likely to already be taking security precautions, while people in Singapore (37%), Hong Kong (34%), China (32%) and Japan are least likely to do so. This suggests that those in APAC may feel less inclined, or may be less aware of the steps needed, to protect themselves against scams.

Older generations are more likely to already be taking safety precautions than younger generations.

Conclusion

Financial scams have moved from a peripheral risk to a dominant feature of the digital economy, touching every generation and market globally. The data shows a world where consumers are both more aware of fraud and more exposed to it.

Feedback from victims finds that the profound impact of fraud is not just about losing money. Nearly all victims suffer an emotional impact. Victims most often report intense negative emotions after a scam, especially anger and frustration, alongside anxiety about their finances and a loss of trust in people and companies. Many also experience embarrassment or shame, guilt, helplessness, and even sleep and stress problems, with these effects often hitting older victims hardest. The result is victims lose trust, change how they bank – hesitating to make payments and questioning every message – and ultimately retreat from digital channels that institutions depend on.

At the same time, the research surfaces a critical education gap particularly challenging as scammers' tactics grow more sophisticated. Complex, AI enabled scams are exploiting pressure, distraction and social proof faster than most consumers or financial institutions can respond, while only a small minority of victims feel they fully understand the protections or reimbursements from their financial institutions available to them.

As our survey shows, fraud is no longer a marginal threat – it is affecting people emotionally, financially and psychologically across every region. Awareness is rising, but confidence is falling and many people still do not understand the protections available to them from their financial institutions.

Addressing the human impact requires more than individual vigilance – it requires a coordinated effort across the entire financial ecosystem, including:

1. **Focus industry efforts on greatest weaknesses:** Scams increasingly exploit identity gaps, payment redirection, and psychological pressure. Educating customers about these moments of failure – particularly those amplified by AI driven impersonation – must become a shared focus across banks, payment providers, platforms and regulators.
2. **Customise educational efforts by generation:** Different generations rely on different channels for information and experience different forms of exposure. Education and support cannot be one size fits all, they must reflect how people live, transact and communicate.
3. **Make protections visible and understandable:** Only a small minority are fully aware of their rights or reimbursement options through their financial institutions, highlighting the need for clearer, more consistent communication.
4. **Cross-industry coordination:** Fraud does not sit within a single system. Banks, payment processors, fintechs, regulators and digital platforms all shape how individuals experience fraud risk. Coordinated approaches – including how scams are reported and communicated – will be essential.

To slow the growth of fraud, the industry must work together.

By aligning efforts across the ecosystem, organisations can better educate and communicate with customers about different fraud risks in the hope that fewer people experience the anxiety, shame or longtail behavioural change reflected in this research.

LSEG RISK INTELLIGENCE

Research methodology

This research is based on an online survey of **21,000 adults across 14 markets,** conducted between **early November and early December 2025.** The online research covers a wide range of ages and digital behaviours, enabling analysis of exposure, impact and risk perception across both regions and generations, including emerging AI-enabled threats. The sample was designed to provide broad geographic coverage across **North America, EMEA and APAC,** reflecting a range of market maturities, regulatory environments and digital adoption levels.

Sample distribution by region and market:

North America
4,000 total

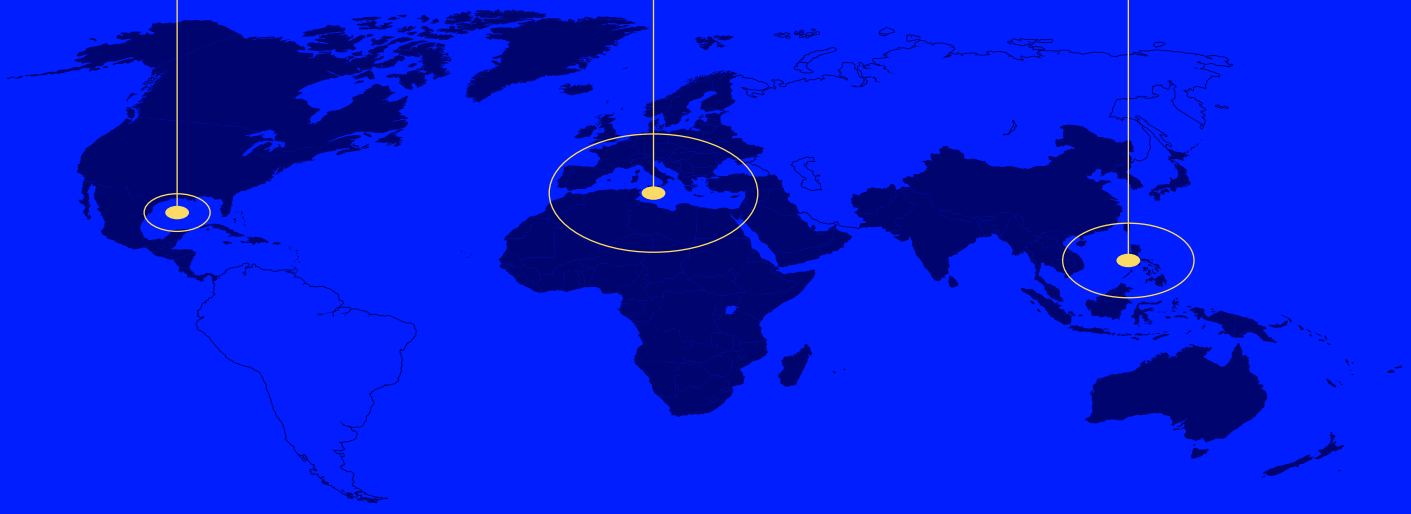
United States: 2,000
Canada: 2,000

EMEA
10,000 total

United Kingdom: 2,000
Germany: 2,000
France: 2,000
Spain: 2,000
Denmark: 1,000
Switzerland: 500
United Arab Emirates: 500

APAC
7,000 total

Australia: 2,000
China: 2,000
Singapore: 1,000
Japan: 1,000
Hong Kong: 1,000



LSEG RISK INTELLIGENCE

This report covers a wide range of scams

Deepfakes

AI generated videos, images or audio designed to convincingly mimic real people or events.

Impersonation scams

A fraudster pretends to be a trusted person (e.g., friend, family member, colleague) to deceive or pressure you.

Investment scams

Fake financial opportunities promising high or guaranteed returns.

Payment scams

Fraudsters send realistic looking fake invoices or payment requests to trick individuals or businesses into sending money.

Phishing

Fraudulent emails, texts or messages crafted to steal personal or financial information.

Quishing

Scanning a malicious QR code that redirects to a fake website designed to steal information or install malware.

Demographic groups in scope

Gen Z

Aged between 18-28 years old

Millennials

Aged between 29-44 years old

Gen X

Aged between 45-60 years old

Baby Boomers

Aged between 61-79 years old

LSEG RISK INTELLIGENCE

LSEG Risk Intelligence
Your partner in the fight against fraud

LSEG Risk Intelligence provides a suite of solutions to help organisations efficiently navigate risks, limit reputational damage, reduce fraud and comply with legal and regulatory obligations around the globe. From screening solutions through World-Check, to detailed background checks on any entity or individual through enhanced due diligence reports, and innovative identity verification and account verification solutions – organisations can trust LSEG Risk Intelligence to help them manage their risk, so they can operate more efficiently, more effectively and more confidently.

To learn more, visit **www.lseg.com/risk-intelligence.**

LSEG RISK INTELLIGENCE