UTILFORGE
CYBERSECURITY AND DIGITAL INCLUSION



Every dot in this report is a person's complaint. 1,008,597 dots, one for each complaint made to the Federal Bureau of Investigation in 2025, run from this cover across the top of every page to the back. The yellow dots are the 201,266 complaints from people aged 60 and over. Most fraud is never reported.

A DIGITAL INCLUSION REPORT · FIRST EDITION · OCTOBER 2026

THE DIGITAL TRUST DEFICIT

Who carries the cost of online scams?

Most of the money lost to online scams is counted by the people who lose it and by their banks, police and health services. The technology companies whose apps scammers use publish what they remove, not what people lose. This report shows what is measured, what is missing, what has already cut losses, and what you can do.

CYBERSECURITY AWARENESS MONTH · 2026 CHAMPION

UtilForge.org · Published for Cybersecurity Awareness Month 2026

At a glance: who carries the harm

Online scams reach everyone, and the harm is not shared equally. In all four countries that measure it, people with disabilities experience more fraud. People with the least to fall back on are the least likely to get their money back, and twice as many lower-income households hit by a scam reported financial hardship. Older people lose the most per report, and women are less likely to be online, and those who are online name safety and security as the main limit on how much they use it. Most countries do not yet publish these figures, so the people most affected are also the least counted.

18.1% vs 12.9%

of people with disabilities in Australia experienced personal fraud in a year, against people without disability (2023–24). In New Zealand the rate for adults with disabilities was 18%, twice the 9% for all adults (2025).

39% vs 20%

of bank-fraud victims in the United States who could not cover a US$400 emergency did not get all their money back, against victims who could also cover three months of expenses (2023).

58% vs 29%

of scammed households in the United States earning under US$80,000 reported moderate or severe hardship, against households earning more (June 2026).

200 million

more women than men do not use mobile internet in low- and middle-income countries, and women who are online name safety and security as the main limit on how much they use it, while women not yet online name affordability and digital skills as the top barriers (2026). In England and Wales women were more likely than men to be fraud victims once other factors were taken into account.

1 in 5

complaints to the Federal Bureau of Investigation in 2025 came from people aged 60 and over, and those complaints carried 37% of the money reported lost.

Most fraud

is never counted. In England and Wales about one fraud in seven reaches the police or Report Fraud. In the United States, 13 scams in 100 reached federal agencies in 2025.

At a glance: the money and what works

The money lost to online scams is mostly counted by the people who lose it, and by their banks, the police and health services. The technology companies whose apps and websites scammers use to reach people publish how many scam adverts and accounts they remove, but not how much money people lose.

85%

of bank-transfer fraud losses in the European Economic Area in 2024 were carried by the person. For card fraud the share was 38%.

0 of 7

large technology companies reviewed publish the money people lost to scams on their services, the refunds they paid, or the revenue from adverts later removed as scams.

54% → 65%

of scam losses by value were refunded in the United Kingdom after banks were made to pay, and 97% of the claims the rule covers.

−48.6%

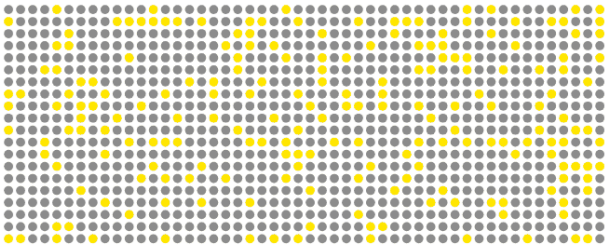
fall in persuasion scams at Mercado Pago in Argentina in 2025, after warnings were built into the moment of payment. Company figures (section 6).

Tools

from UtilForge.org, from knowing to sharing, each beside the problem it helps with. Every check runs on your own phone (section 13).

If it has just happened

Stop all contact. Call your bank on the number printed on your card. Report the scam and say where it began. The first steps are in section 1.



1,000 dots = 1,000 complaints

One dot for each complaint made to the Federal Bureau of Investigation in 2025.

About 1 in 5 dots is yellow: complaints from people aged 60 and over.

The report carries all 1,008,597.
Most fraud is never reported.

Figure 1. How the dots in this report work. The cover, the top of every page and the back cover carry 1,008,597 dots, one for each complaint made to the Federal Bureau of Investigation in 2025.

1 If it has just happened, and what you can do this week

If you think you have just been scammed

1. **Stop all contact** with the person, the website or the app. Do not send more money, even if you are promised your money back.
2. **Call your bank** on the number printed on your card or on its official website. In the United Kingdom, call 159 to reach your own bank.
3. **Report it, and say where it began**: the platform, the app or the phone number. Even a report with no money lost helps the count.
4. **Keep everything**: messages, screenshots, receipts and the account details you paid.
5. **Tell someone you trust.** Being scammed is a crime against you.
6. **Watch for a second contact.** Anyone who offers to get your money back for a fee is running a recovery scam.

Where to report

- **United States:** reportfraud.ftc.gov (the Federal Trade Commission) and ic3.gov (the Federal Bureau of Investigation).
- **United Kingdom:** reportfraud.police.uk or 0300 123 2040 in England, Wales and Northern Ireland; Police Scotland on 101. Forward scam texts to 7726.
- **Australia:** scamwatch.gov.au.
- **Canada:** the Canadian Anti-Fraud Centre, 1-888-495-8501.
- **India:** call 1930 or use cybercrime.gov.in.
- **Singapore:** the ScamShield helpline, 1799.
- **South Africa:** your nearest police station, or Crime Stop on 08600 10111.
- **Kenya:** the National Kenya Computer Incident Response Team, ke-cirt.go.ke.
- **Nigeria:** the Nigeria Police Force National Cybercrime Centre, nccc.npf.gov.ng.
- **Elsewhere:** UtilForge.org's Official Help page lists official reporting services in 33 countries and territories, and its Report and Recover Atlas sets out reporting routes and money-back rules for 38 countries and the European Union (utilforge.org/creators/report-and-recover).

What every reader can do this week

- **Families.** Agree one rule: no money moves under pressure, and anyone can pause it. Agree a family safe word, face to face, and name the people each of you would call to lock your accounts if a phone were lost or stolen.
- **Older people and the people who help them.** Hang up on an unexpected call and call back on a number you find yourself.
- **Students and job seekers.** Treat any request to pay before work begins as a reason to stop. Real employers pay you; they do not charge you to start.
- **Anyone offered an investment.** The Federal Bureau of Investigation's Operation Level Up, which contacts people caught in cryptocurrency investment fraud, found that 78% of the 3,780 people it contacted in 2025 did not know they were being scammed.
- **Small businesses.** Ask a second person to approve any change to a supplier's bank details, and turn on two-step sign-in (a code as well as a password).
- **People who build apps and websites.** Put the warning where the decision is made: on the screen where money is about to leave or a new payee is added, in plain words, and only when something looks out of pattern for that person. Section 6 shows what this did at one payment app in Argentina.
- **Charities and community groups.** Turn on two-step sign-in for every account, check what your suppliers hold, and apply for free protection such as Cloudflare's Project Galileo or Microsoft AccountGuard.
- **Journalists.** Say whether a figure is a reported loss, a survey estimate or a model, and whether it counts cases or money.
- **Shareholders and pension funds.** Ask the companies you hold whether they will publish the model disclosure in section 7.
- **Regulators and lawmakers.** Add a "where did it start" field to fraud reports, and publish response data platform by platform.

UtilForge.org's free checks run on your own phone or computer and help with several of these steps: Is This a Scam Text, Before You Pay, Before You Send, Before You Reply to a Recruiter, Family Safe Word, the Trusted People Card and the Official Help directory. Section 13 sets out every tool beside the problem in this report that it helps with.

2 Why this report

About 6 billion people are online and 2.2 billion are not, and 96% of the people offline live in low- and middle-income countries, according to the International Telecommunication Union (17 November 2025). A person who comes online can gain a bank, a classroom, a job search and a call to family on one screen, and meets scams that have been running for years.

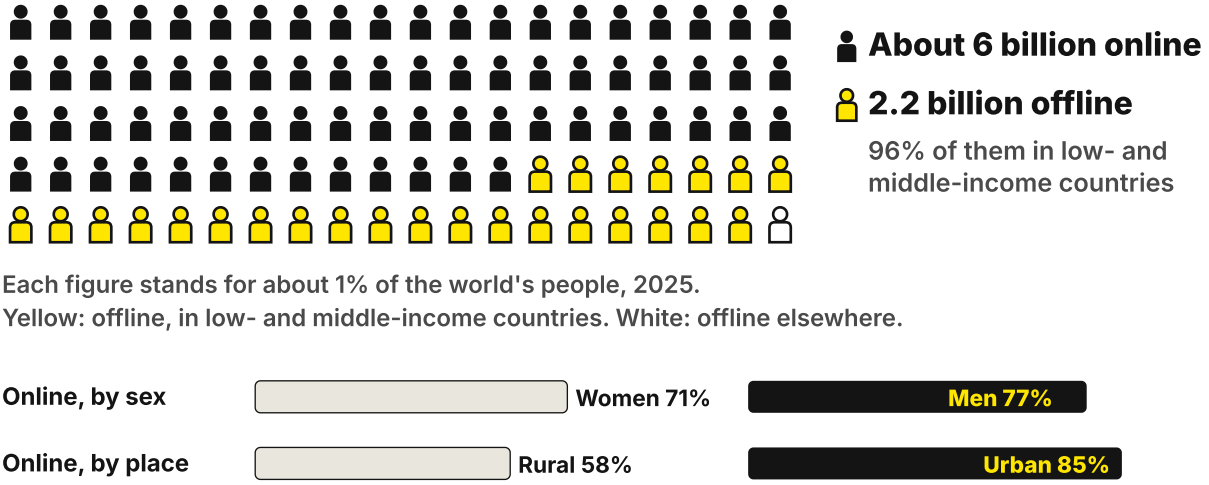


Figure 2. The world online and offline, 2025. International Telecommunication Union, Facts and Figures 2025.

What happens when many people come online in a short time can already be seen. In Latin America and the Caribbean the share of people using the internet rose from 68% to 81% between 2019 and 2023, according to the International Telecommunication Union, and the World Bank describes the region as the fastest-growing in the world for disclosed cyber incidents, up by an average of 25% a year over a decade, and as the least protected, with an average cybersecurity score of 10.2 out of 20 (World Bank, 28 November 2024). In a 2026 report on cybersecurity for people in the financial systems of the Americas, published by the Organization of American States, Mercado Libre, the company behind the payment app Mercado Pago, sets out the mechanism: each new user, each new payment and each new app gives a person services they did not have before, and also widens the ground on which fraud can be tried, so that “inclusion and exposure grow together”. In the same report the Development Bank of Latin America and the Caribbean adds the second step: a person who loses money to fraud can also lose the confidence to use the service again, which undoes the inclusion the service was built for. The 2.2 billion people still offline will arrive on the same terms unless protection arrives with them.

The gap between the safety people need online and the safety that reaches them is the digital divide this report examines. The gap between what people are asked to trust online and what anyone can show them is the trust deficit in the title.

Every day online asks a person to trust what they cannot check: a voice on the phone, a name on a message, a logo on an advert, a page that looks like a bank’s. For most of history a familiar voice or a known name was proof enough, and that proof is fading. In a study published in Scientific Reports in 2025, listeners judged a cloned voice to be the same person as the real speaker about 80% of the time, and correctly identified a voice as made by artificial intelligence only about 60% of the time (304 listeners; Barrington, Cooper and Farid, University of California, Berkeley). A scam draws on that trust and spends it three times: the person loses money and confidence, the bank or platform whose name was borrowed loses standing, and the next genuine call or message is met with doubt.

Take a typical scam. A criminal places a fake advert on a social media app, calls or texts the person who responds, and persuades them to send money from their bank account. The person knows what they lost. The bank records any refund it pays. The police record the crime if it is reported. A doctor

may treat the stress without knowing the cause. The app where the advert appeared usually records only that it removed the advert or the account.

Which trust does a scam damage?

Trust is measured in three ways, and a country can rank high on one and low on another. A scam reaches all three at once: it uses a stranger's voice, borrows an institution's name, and tests what a person does next. Researchers find that trust moves with income and growth, and no one has put a reliable price on losing it, so this report does not. What it can show is where trust is spent and not repaid: fraud that is never counted, platforms that do not publish what people lost, and refunds that depend on which country a person banks in.



Figure 3. Three kinds of trust. World Values Survey; Organisation for Economic Co-operation and Development, Trust Survey 2026; Edelman Trust Barometer 2026 (an online survey of 28 markets); Cohn and others, Science, 2019 (more than 17,000 wallets).

3 What is known

Online fraud is large and growing in most places that measure it, and its heaviest costs fall on older people, on people with fewer digital skills and on the public services that respond.

Six measures of one problem

Six figures describe scam losses in the United States in 2025. They differ because they measure different things: what people reported, what a survey estimates, and what a model adds for fraud nobody reported. Reported losses are always the minimum.

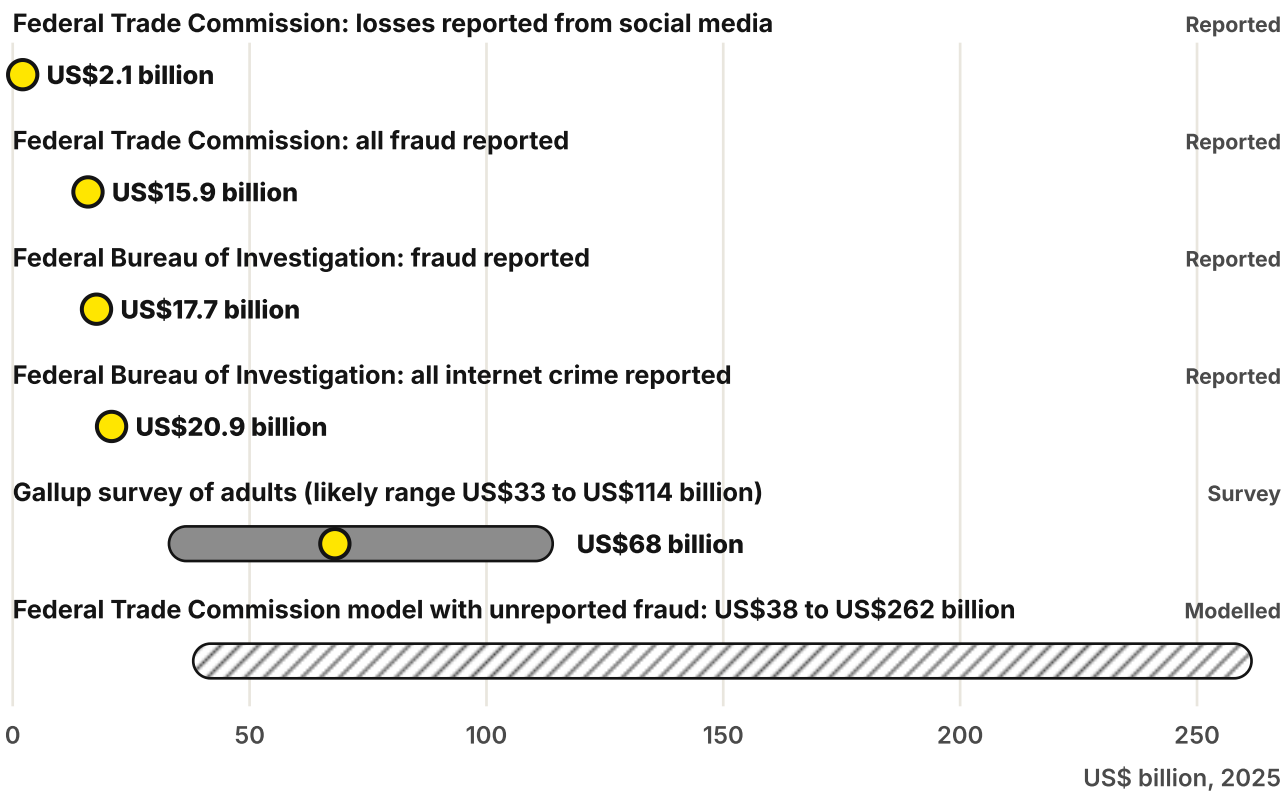
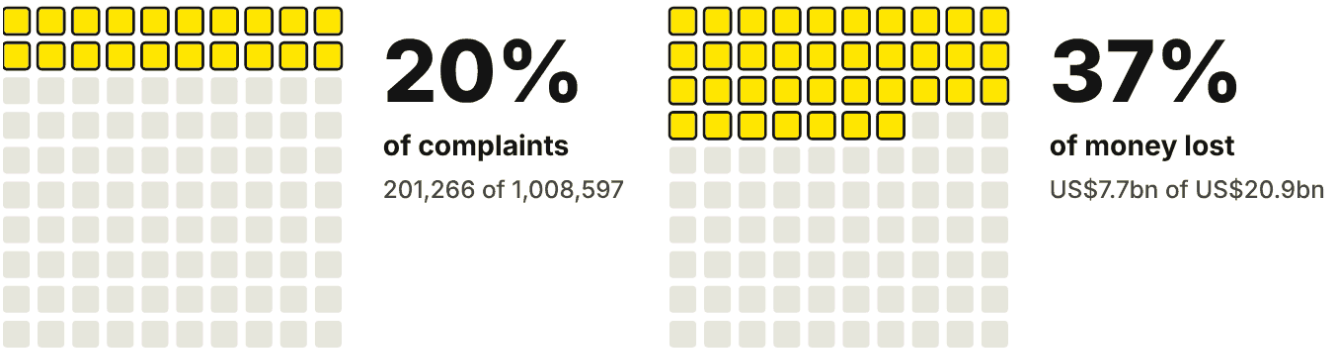


Figure 4. Six measures of scam losses, United States, 2025. Federal Bureau of Investigation, Internet Crime Report 2025 (April 2026); Federal Trade Commission (25 March 2026, 27 April 2026 and 19 October 2026); Gallup survey for the Stop Scams Alliance (June 2026). The model's range is for all consumers.

- **Federal Bureau of Investigation.** People reported losing US$20.9 billion to internet crime in 2025 across 1,008,597 complaints, up 26% on 2024. That total includes business email compromise, where criminals pose as a firm or supplier to redirect payments, and ransomware, which locks a victim's files until a ransom is paid. Fraud alone came to US$17.7 billion.
- **Gallup survey.** About 15 million adults (6%) were scammed in 2025 and lost about US$68 billion. The survey's likely range is US$33 billion to US$114 billion. In 66% of these scams nothing was recovered.
- **Federal Trade Commission.** People reported US$15.9 billion in fraud losses in 2025, and US$2.1 billion of reported losses began on social media. The commission's model, which adds an estimate for unreported fraud, puts the full cost to consumers between US$38.1 billion, which it calls very conservative, and US$261.5 billion.

Who is hit hardest



People aged 60 and over, complaints to the Federal Bureau of Investigation, United States, 2025. Each grid has 100 squares. Yellow squares are the share from people aged 60 and over.

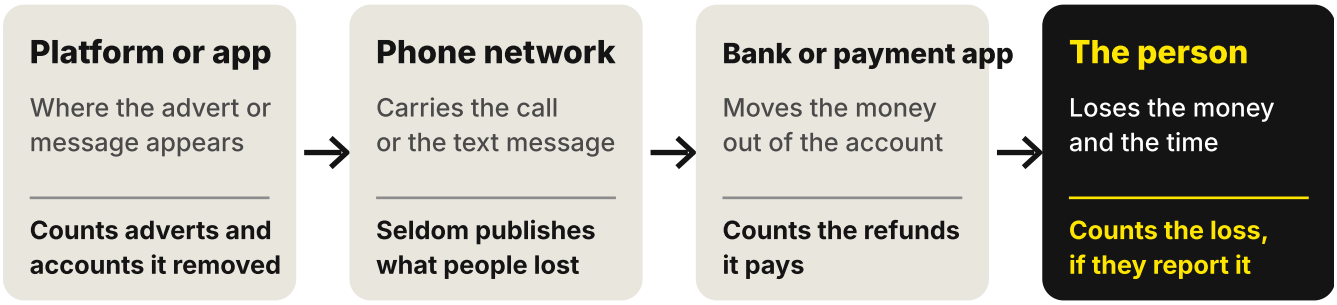
Figure 5. People aged 60 and over: share of complaints and of money lost. Federal Bureau of Investigation, Internet Crime Report 2025.

- **People aged 60 and over, United States.** They made 201,266 complaints in 2025 and reported US$7.7 billion in losses. Their losses rose 59% on 2024 and their complaints rose 37%.
- **Older Australians.** People in Australia's older age group are 17.1% of the population but reported 26.5% of the losses reported to Scamwatch. Losses reported across five Australian sources came to A$2.18 billion (about US$1.41 billion) in 2025, up 7.8% (National Anti-Scam Centre, March 2026).
- **People with fewer digital skills, United Kingdom.** People with the lowest digital skills were more likely to be scammed multiple times: 8.5%, against 4.6% of the most skilled (Lloyds Bank, Consumer Digital Index 2024).
- **People offline.** The 2.2 billion people offline are likely to meet scams as soon as they join, on the evidence in this section.
- **People with disabilities.** In Australia, England and Wales, New Zealand and Canada, the four countries that publish the figure, people with disabilities experience more fraud (section 4).
- **People with the least to fall back on.** In the United States, victims who could not cover a US$400 emergency were about twice as likely as victims who could also cover three months of expenses to be left without all their money back (section 4).

The cost beyond the money

- **England and Wales.** The Home Office estimates that fraud against individuals costs £9.2 billion a year (about US$12.1 billion), within £14.4 billion including businesses. The individual cost includes £3.2 billion in money lost, £1.9 billion in emotional harm, £1.1 billion in lost output, £887 million in health services, £0.9 billion spent trying to avoid fraud, and £1.1 billion in the cost of responding, from police, courts and the finance industry (figures rounded).

- **How common it is.** The Crime Survey for England and Wales estimated 4.5 million fraud incidents in the year to June 2026, up 11% from 4.1 million. That is about 46% of the 9.7 million incidents of headline crime the survey measures, a calculation for this report (Office for National Statistics, 22 October 2026).
- **Mental health.** In the Gallup survey, 73% of adults in households hit by a scam reported harm to their mental health or wellbeing, and so did 77% of the people scammed themselves.
- **Wellbeing.** Which? valued the yearly drop in wellbeing at about £3,684 for each victim of online fraud, against an average loss to fraud of about £600 (2019–20 data; Which?, 18 October 2021).
- **United Kingdom payment fraud.** £1.28 billion (about US$1.69 billion) was lost in 2025: £703.4 million in unauthorised fraud, where money is taken without permission, and £576.4 million in push-payment fraud, where a person is tricked into sending the money themselves, up 19% (UK Finance, the trade body for United Kingdom banks, June 2026).



Costs that land further on, England and Wales, each year

£1.9 billion	£1.1 billion	£887 million	£0.4 billion
Emotional harm	Lost output	Health services	Police and courts

Figure 6. A scam's journey, and who counts what. Costs in England and Wales from the Home Office, Economic and social cost of fraud 2023 to 2024 (second edition, 14 July 2026).

4 Who is reached, who is protected, who recovers

A scam reaches everyone who is online. What happens next depends on who the person is and where they live. This section gathers evidence from 31 countries on ten kinds of difference between people and asks three questions of each: how often are people reached, what protection is within their reach, and how well can they recover afterwards?

Seven findings

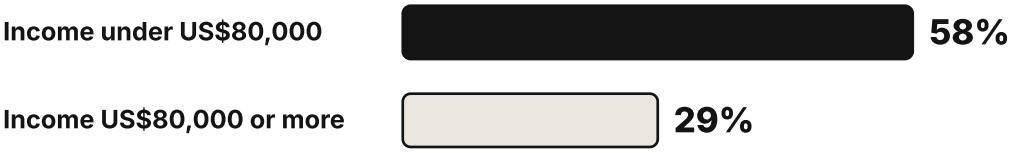
1. **Most losses are never reported, so countries that count more can look worse.** About one fraud in seven in England and Wales reaches the police or Report Fraud (a share of frauds). Canada's

Competition Bureau estimates that 5% to 10% of frauds are reported (a share of frauds). Mexico's statistics institute found that 93.4% of crimes of all kinds went unreported or uninvestigated in 2025, and 96.5% of frauds (shares of crimes). Interpol found that 89% of responding African countries describe under-reporting as widespread (a share of countries).

2. **How the money moved decides who carries the loss.** In the European Economic Area people carried about 85% of bank-transfer fraud losses and 38% of card fraud losses in 2024 (section 6). In the United States, bank transfers and then cryptocurrency carried the highest losses, while credit cards were the payment method reported most often (Federal Trade Commission, October 2026).
3. **Age changes the kind of harm as well as its size.** In the United States, people in their twenties were more likely to report losing money to the Federal Trade Commission in 2024 (44%, against 24% of people in their seventies), with a smaller median loss, the middle value (US$417, against US$1,000). People aged 80 and over had a median loss of US$2,000, and 17.0% of their reports were made by someone else on their behalf. In Japan in 2025, impersonation fraud rose 329% among people in their thirties and 362% among people in their twenties, while people aged 65 and over still accounted for 59.2% of losses to special fraud. Gallup's 2026 survey found no difference in the rate of being scammed by age. In the five-country Oh, Behave! survey of 2026, 64% of adults in Generation Z said they had lost money or data to scams, against 33% of baby boomers (see the update, 28 October 2026, before the sources).
4. **People with the least to fall back on are hurt most and recover least.** In the Gallup survey, 58% of scammed households earning under US$80,000 reported moderate or severe financial hardship, against 29% of households earning US$80,000 or more (June 2026). In the United States, 39.2% of bank-fraud victims who could not cover a US$400 emergency did not get all their money back, against 20.0% of victims with three months of savings (Federal Reserve Bank of Kansas City, 8 October 2025). Lower income does not always mean more fraud: in England and Wales, households earning under £10,400 were less likely to be fraud victims than households earning £52,000 or more (Office for National Statistics, March 2026). The difference lies in how hard the loss lands and how much comes back.
5. **People with disabilities experience more fraud in all four countries that publish the figure:** Australia, England and Wales, New Zealand and Canada. In Australia, people with disabilities were less likely to get a full refund for card fraud (66.6% against 74.5%), and in New Zealand the rate for adults with disabilities doubled between 2023 and 2025.
6. **Women face wider gaps in access, and more abuse through phones and money from partners.** About 200 million more women than men do not use mobile internet in low- and middle-income countries, and women who are online name safety and security as the main limit on how much they use it, and women not yet online name affordability and digital skills as the top barriers (GSM Association, 10 June 2026). In the European Union, 20.3% of women have experienced economic violence from a partner and 10.2% have had their location tracked by one (Eurostat, the European Union Agency for Fundamental Rights and the European Institute for Gender Equality, 3 March 2026). Fraud itself falls more evenly: women were more likely than men to be victims in England and Wales and slightly more likely to be scammed in Australia (3.5% against 2.7%), while most sexual extortion reports to Australia's eSafety Commissioner came from young men.

7. **The people most affected are the least counted.** Most fraud agencies do not publish losses by disability, sex, income or language, including the Federal Trade Commission and the Federal Bureau of Investigation in the United States.

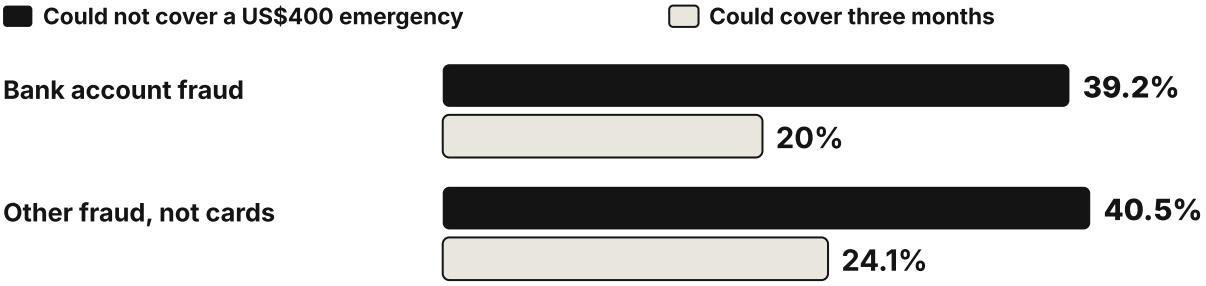
Scammed households reporting moderate or severe financial hardship, United States



Gallup survey for the Stop Scams Alliance, June 2026.

Figure 7. The same scam costs lower-income households more. Gallup survey for the Stop Scams Alliance, June 2026: one large survey.

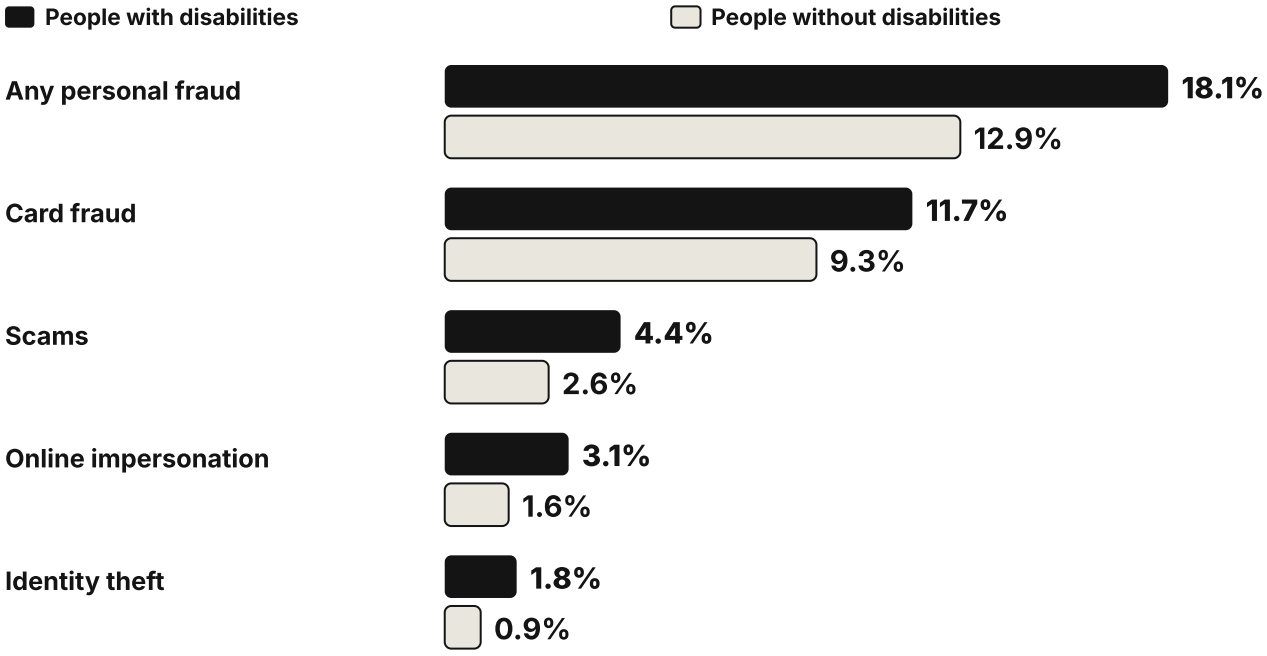
Victims who did not get all their money back, United States, 2023



Federal Reserve Bank of Kansas City, 8 October 2025; Federal Reserve household survey, fraud in 2023.

Figure 8. People who could not cover a US$400 emergency are about twice as likely to be left without all their money back. Federal Reserve Bank of Kansas City, from the Federal Reserve's household survey.

People who experienced fraud in the past year, Australia, 2023-24



Australian Bureau of Statistics, Disability and Crime, 20 November 2025. People aged 15 and over.

Figure 9. People with disabilities experience more of every kind of personal fraud measured. Australian Bureau of Statistics.

Women and men in two measures

Not using mobile internet, low- and middle-income countries, 2025



Experienced a scam in the past year, Australia, 2023-24



GSM Association, Mobile Gender Gap Report 2026 (10 June 2026); Australian Bureau of Statistics, Personal Fraud 2023-24.

Figure 10. Women are less likely to be online, and slightly more likely to be scammed where it is measured. GSM Association; Australian Bureau of Statistics.

By kind of difference

Work and job seekers

Fake jobs that ask for a fee, a deposit or a "top-up" to unlock earnings are reported across the world. In the United States, employment fraud cost US$362.9 million across 24,688 complaints to the Federal Bureau of Investigation in 2025. Australia's job scam reports more than doubled in 2025 (up 102.4%), and losses rose 81.5% to A$24.8 million (about US$16.0 million). Singapore recorded 5,575 job scam cases and about S$123.5 million (about US$94.5 million) lost. Canada recorded C$50.6 million (about US$36.2 million) lost to job fraud.

Gender

Women are 12% less likely than men to use mobile internet in low- and middle-income countries, which leaves 810 million women and 595 million men offline on mobile, and safety and security are women's top reported barrier (GSM Association, *Mobile Gender Gap Report 2026*). Worldwide, 71% of women and 77% of men use the internet (International Telecommunication Union, 2025). In England and Wales women were more likely than men to be fraud victims after adjusting for other factors (Office for National Statistics, March 2026), and in Australia 3.5% of women and 2.7% of men experienced a scam (2023–24). In the European Union, 20.3% of women have experienced economic violence from a partner and 8.5% have been cyberstalked (3 March 2026). In Mexico, 22.2% of women and 19.6% of men online experienced cyber-harassment, and threats to publish material for money were the most common kind women reported, at 43.2% (Instituto Nacional de Estadística y Geografía, 17 July 2025). Sexual extortion falls mostly on young men: 76% of such reports to Australia's eSafety Commissioner in 2021–22 came from men. Of 641 women in public life surveyed in 119 countries, 12% had intimate images shared without consent (UN Women, April 2026; a chosen sample).

Education and digital skills

In the United States, 7% of adults without a university degree were scammed in 2025, against 4% with one (Gallup). In the United Kingdom, people with the lowest digital skills were more likely to be scammed multiple times (8.5% against 4.6%).

Ethnicity and race

In a 2024 survey of 2,042 United States adults, 33% of Black and 30% of Hispanic respondents who met a cyberattack or scam lost money, against 13% of white respondents; the authors say the cause is unclear (Consumer Reports, October 2024). Gallup found 8% of Black, 9% of Hispanic and 5% of white adults were scammed in 2025.

Where people live

Brazil's states record electronic fraud at rates from 903.8 per 100,000 people in Santa Catarina to 48.8 in Pará, and three states do not report the category separately. Worldwide, 85% of people in towns and cities use the internet, against 58% in rural areas. The World Bank found that 14% of adults in low- and middle-income economies received scam messages, about 30% in Latin America and the Caribbean and in Sub-Saharan Africa.

Migration and language

Official warnings in migrants' languages, and losses by migration status, are largely not published. Sending money home to family costs 6.36% on average (World Bank, August 2025).

Businesses

In the United Kingdom, 43% of businesses (about 612,000) had a breach or attack in 2025/26, from 42% of micro businesses to 69% of large ones, and 43% of micro businesses use two-step sign-in (Department for Science, Innovation and Technology, 30 April 2026).

Disability

People with disabilities use the internet less where it is measured: in the European Union, 82.3% of people with a severe disability against 95.2% of people with none, and 51.0% against 69.3% for online banking (Eurostat, 27 August 2025). Across 46 countries, 28% of people with disabilities used the internet against 39% of others (United Nations Department of Economic and Social Affairs, *Disability and Development Report 2024*). In India, 49% of mobile internet users with disabilities named scams and fraud as a barrier, against 35% of others (GSM Association, July 2025; a small sample). Scamwatch in Australia, and Take Five to Stop Fraud with Mencap in the United Kingdom, publish easy-read scam guides.

Income and savings

In the United States, adults earning under US$50,000 lost a median of US$400 to fraud in 2025, the same sum the Federal Reserve uses to test emergency savings, and 37% of all adults could not cover a US$400 expense with cash or its equivalent (Federal Reserve Board, 13 May 2026). In the United Kingdom, victims got all their money back in 84% of card frauds but 56% of bank-transfer frauds (Financial Conduct Authority, May 2025), so the way a person can pay shapes what they recover. In Kenya, 9.8% of mobile money users reported losing money in 2024 (Central Bank of Kenya, *FinAccess Household Survey*). In Senegal, 43% of mobile money users received a scam attempt and low-income users sought redress less often (Consultative Group to Assist the Poor and Innovations for Poverty Action, June 2023).

Household

In the Gallup survey, 65% of adults whose household member was scammed reported harm to their own mental health or wellbeing. No national survey found for this report, as of 27 October 2026, measures people who live alone separately.

Where the money goes and how much comes back

- **Cryptocurrency kiosks,** the machines that turn cash into cryptocurrency. The Federal Bureau of Investigation received 13,460 complaints about them in 2025, with US$389 million in losses, up 58%; people aged 60 and over made 6,188 of the complaints and reported US$257.5 million, about two-thirds of the losses. Indiana became the first state to ban the machines, in a law signed on 9 March 2026.
- **Freezing money quickly.** The Federal Bureau of Investigation's Recovery Asset Team, which asks banks to hold stolen money before it moves on, froze US$679 million of US$1.164 billion across about 3,900 incidents in 2025, a 58% success rate.
- **Recovery scams,** where someone offers to get lost money back. The bureau received 10,516 complaints in 2025 with US$1.4 billion in losses, and notes that these losses may include the earlier scam that prompted the contact.

5 Most fraud is never counted

The online-safety record counts what is removed more readily than what is lost. Most people who lose money to a scam appear in no official count at all.

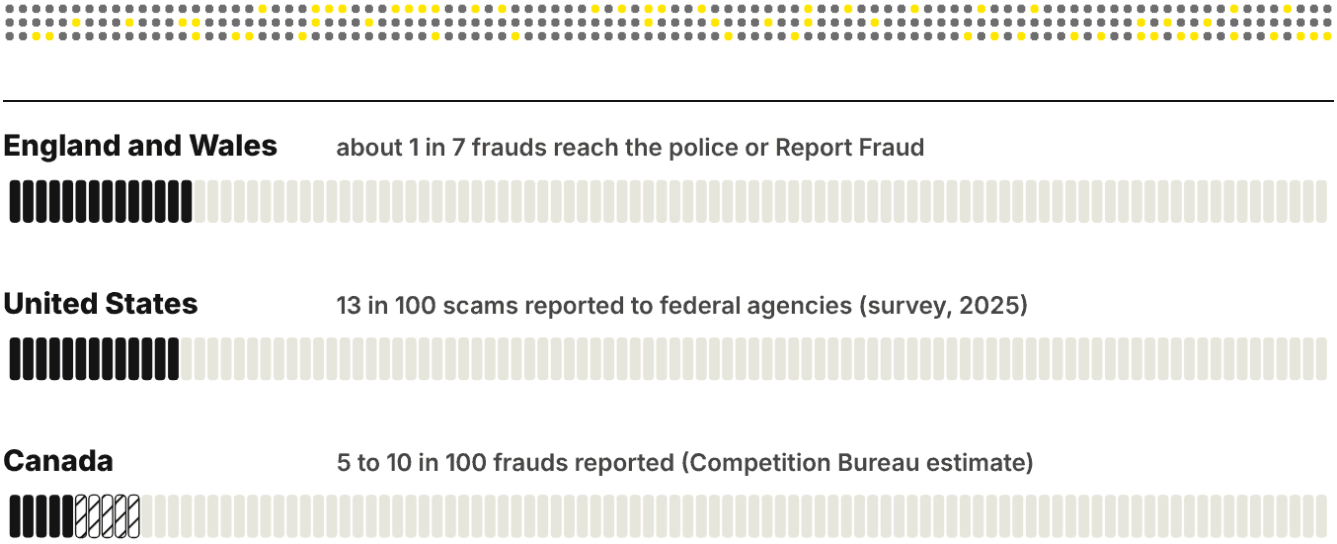


Figure 11. How many frauds reach an official count. Office for National Statistics, Crime Survey for England and Wales; Gallup survey for the Stop Scams Alliance (June 2026); Competition Bureau Canada.

What no one measures yet

- **Reporting.** The Crime Survey for England and Wales estimates that about one fraud in seven reaches the police or Report Fraud (Office for National Statistics, reviewed by the Office for Statistics Regulation, 3 April 2025). In the United States the Government Accountability Office cites an estimate that about 15% of fraud victims report to law enforcement (report 26-109023, 25 March 2026).
- **A definition.** The United States has no common definition of a scam, no government-wide estimate of losses and no national strategy; all 16 of the auditor's recommendations remain open, and no agency measures whether anti-scam education works (Government Accountability Office, report 25-107088, 8 April 2025).
- **Where scams start.** This is known mainly from what people remember when they report (Payment Systems Regulator, December 2024).
- **Charges.** Fewer than 1% of around 900,000 frauds reported each year in England and Wales led to a charge or prosecution (House of Commons Committee of Public Accounts, 31 March 2023).
- **Breaches.** Seventy per cent of United States data-breach notices in 2025 did not say how the breach happened, up from 65% in 2024 (Identity Theft Resource Center, January 2026).
- **Artificial intelligence.** Scams using artificial intelligence are counted only when a complaint mentions it: 22,364 complaints and US$893.3 million in 2025, a minimum (Federal Bureau of Investigation).
- **Platforms.** Money lost by the people using each platform, and revenue from adverts later removed as scams, are not published by the companies reviewed (section 7).
- **Who is harmed, in regional reports.** The Organization of American States' 2026 report on cybersecurity for people in the financial systems of the Americas asks who is affected when financial systems fail and whose risks are accepted. Its figures come from banks, payment companies, insurers and international bodies, and are given by institution, kind of fraud and country. None is broken down by age, sex, disability, income or language.

The people least counted

- **People with disabilities.** Four countries publish fraud rates for people with disabilities, and all four find them higher. Australia: 18.1% experienced personal fraud of any kind, against 12.9% of people without a disability (2023–24), and 4.0% experienced a scam, against 2.3% (2024–25) (Australian Bureau of Statistics, 20 November 2025 and 12 March 2026). England and Wales: higher odds of fraud for people with disabilities once age and other factors are taken into account (Office for National Statistics, 26 March 2026). New Zealand: 18% of adults with disabilities experienced fraud in 2025, up from 9% in 2023, against 9% of all adults (Ministry of Justice, 7 May 2026). Canada: 19% of people with a disability had experienced fraud in five years, against 16% (Statistics Canada, 2019 data, published 24 July 2023). The United States' Federal Trade Commission and Federal Bureau of Investigation do not publish losses by disability.
- **People who speak another language.** Few countries publish losses by language, and most reporting routes work in one language. AARP, the organisation for older Americans, describes research on people with limited English as scarcer still (17 September 2024).
- **Small businesses.** The Home Office puts the cost of fraud to businesses in England and Wales at £5.2 billion a year, and small firms rarely appear as a group in public fraud reporting.
- **People held in scam operations.** The Office of the United Nations High Commissioner for Human Rights cites estimates that at least 300,000 people from 66 countries work in scam operations across South-East Asia, many of them trafficked and coerced. They are victims of the same industry that targets the people in the rest of this report.

6 Who carries the cost, and what changes it

How the money moved decides who carries the loss. Where a rule made the firm best placed to stop a scam pay for it, measured outcomes changed.

Share of fraud losses carried by the person, European Economic Area, 2024

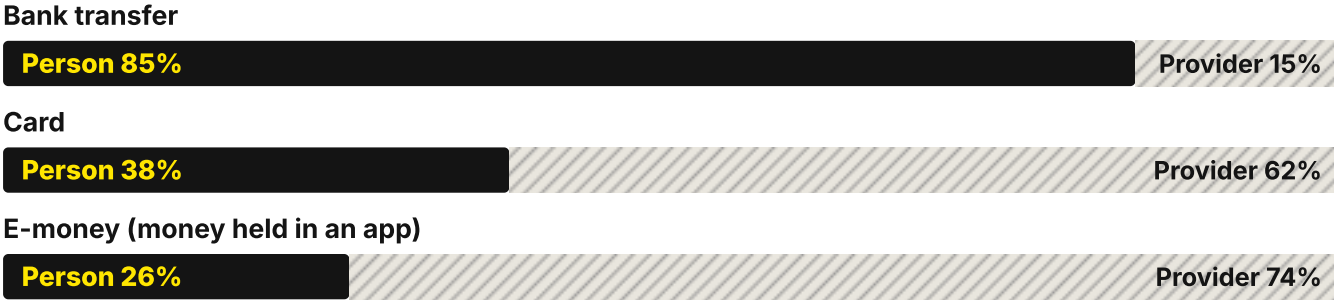


Figure 12. Who carries the loss depends on how the money moved. European Banking Authority and European Central Bank, report on payment fraud, December 2025. The European Economic Area is the 27 European Union countries plus Iceland, Liechtenstein and Norway.

Payment fraud in the European Economic Area came to €4.2 billion (about US$4.74 billion) in 2024. Card payments carry more protection: in the United States, Regulation Z limits what a person pays for misuse of a credit card to US$50, and in the United Kingdom section 75 of the Consumer Credit Act makes card companies share responsibility for purchases from £100 to £30,000. Neither covers a bank transfer a person was tricked into making.

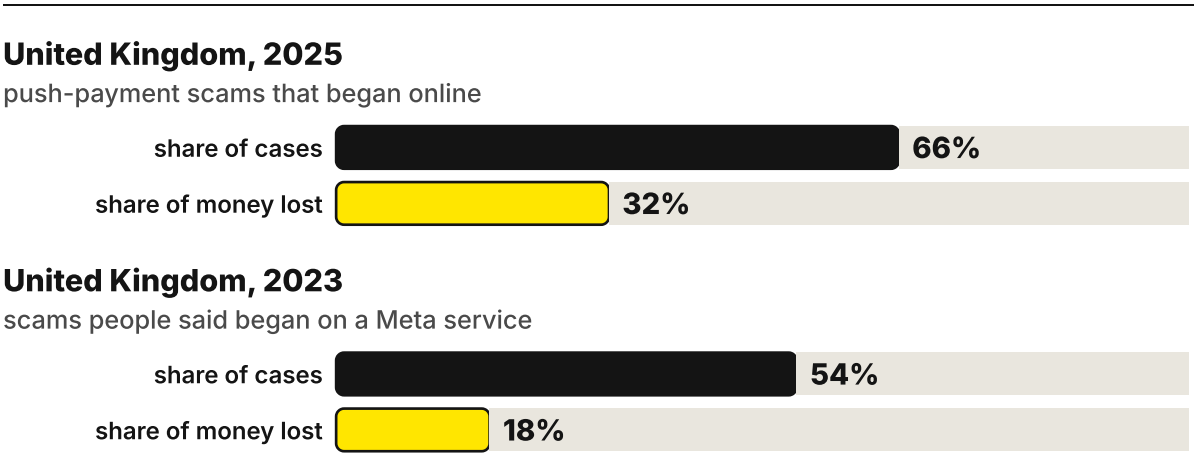


Figure 13. Where most scams start is not always where most money is lost. UK Finance, Annual Fraud Report 2026; Payment Systems Regulator, December 2024 (based on what people told their bank).

Refunds for bank-transfer scams: United Kingdom

The rule. Since 7 October 2024, when someone is tricked into sending money by bank transfer, their bank must usually refund them, and the bank that sent the money and the bank that received it share the cost.

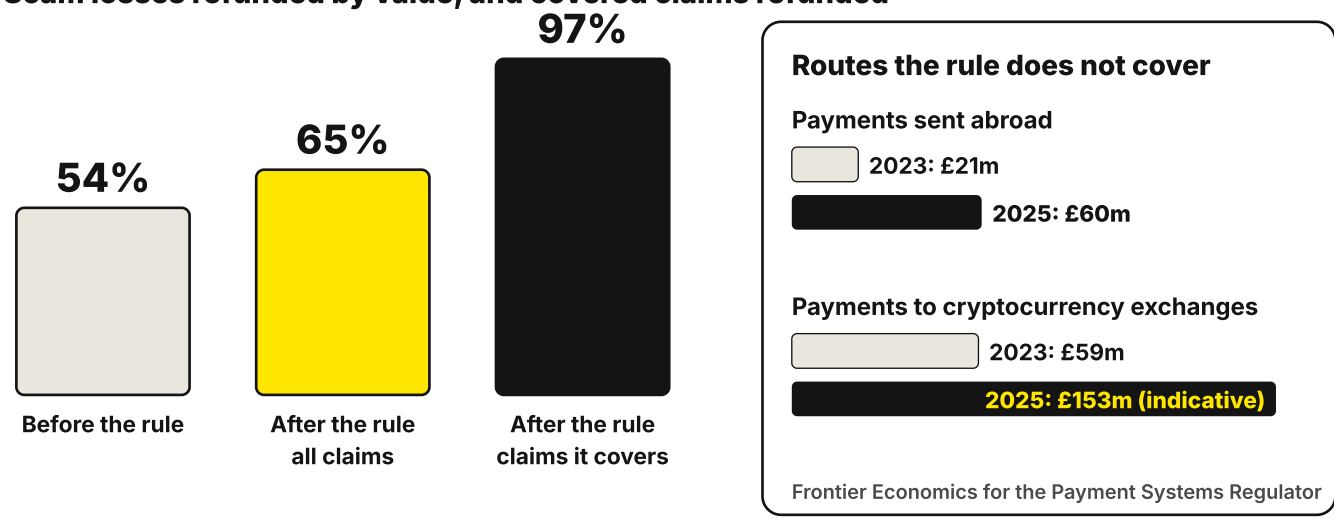


Figure 14. The United Kingdom refund rule, before and after. Payment Systems Regulator, 1 July 2026; Frontier Economics, Independent Evaluation of APP Scam Policies, 1 July 2026.

- Banks and payment firms now refund 65% of scam losses by value across all claims, up from 54% before the rule, and 97% of the claims the rule covers.

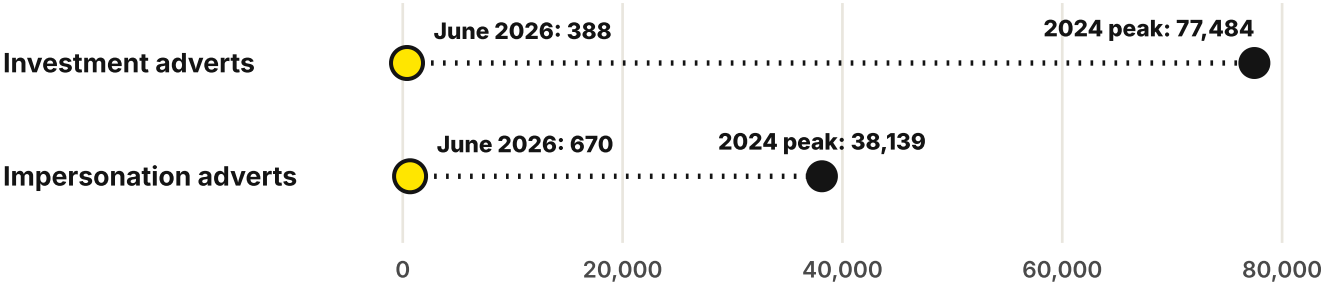
- Frontier Economics, the economics firm that evaluated the rule for the regulator, estimates that people lose about £73 million less each year and that there are about 35,000 fewer scams.
- Refund rates differ between firms, from 21% to 94%.
- Payments sent abroad and payments to cryptocurrency exchanges sit outside the rule. Over the same period, scams through international payments rose from £21 million in 2023 to £60 million in 2025, and scams through cryptocurrency exchanges from around £59 million to £153 million, a figure the evaluation calls indicative.
- An earlier figure counted money claimed back rather than all losses: in the first nine months, to 30 June 2025, firms returned £112 million, 88% of the money people claimed (Payment Systems Regulator, 8 October 2025). It is measured differently and cannot be compared with the evaluation's figures.

The Payment Systems Regulator is being merged into the Financial Conduct Authority under legislation before Parliament.

Advertiser checks: Taiwan

Since 31 July 2024, Taiwan's Fraud Crime Hazard Prevention Act has required large platforms to check who places adverts, publish yearly transparency reports and remove scam adverts within 24 hours. The Ministry of Digital Affairs reports falls in the scam adverts it detects each week.

Scam adverts detected each week, Taiwan



Ministry of Digital Affairs, Taiwan, 17 July 2026. Adverts detected, not money lost.

Figure 15. Scam adverts detected each week in Taiwan. Ministry of Digital Affairs, Administration for Digital Industries, 17 July 2026.

Warnings built into the app: Argentina

The change. Mercado Pago, a payment app used across Latin America, moved much of its protection to the moment when a person decides to send money, instead of relying only on checks behind the scenes. Its parent company, Mercado Libre, published the results for Argentina in the Organization of American States' 2026 report *From Bank to Blockchain*. They are company figures.

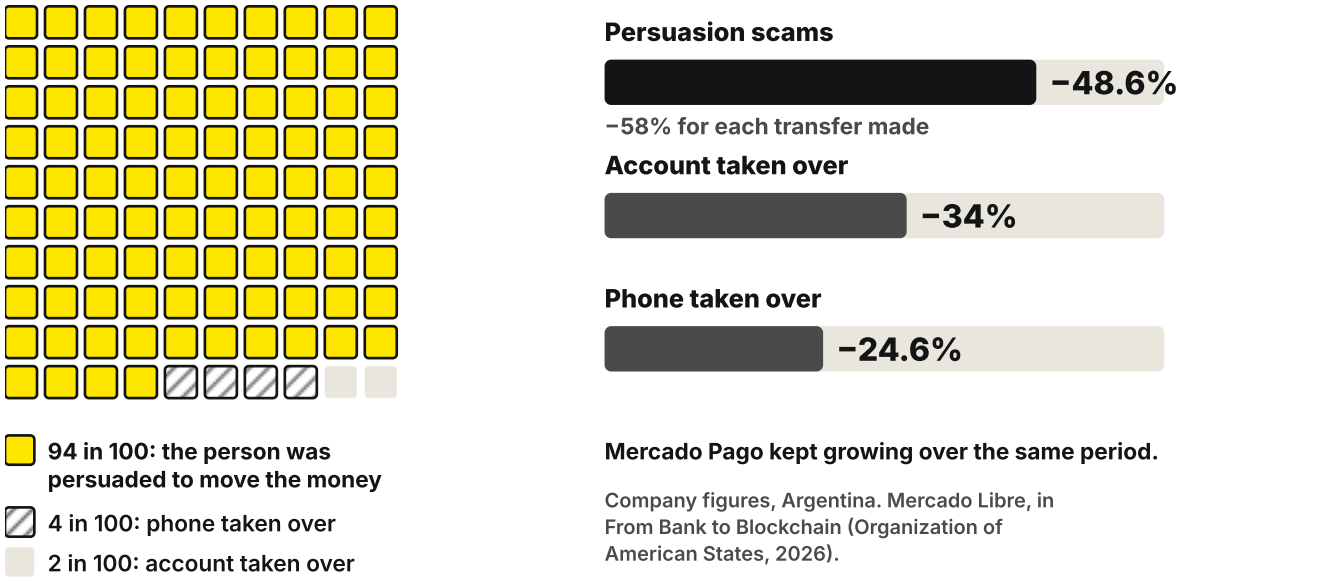


Figure 16. Warnings at the moment of payment, Mercado Pago, Argentina. Mercado Libre, in *From Bank to Blockchain: Cybersecurity for People in the Financial Ecosystem of the Americas*, Organization of American States, 2026. Company figures.

- **What it found.** From January to September 2025, 94.4% of confirmed fraud cases were scams in which no system was broken into: the person was persuaded to move the money themselves. For every account or phone taken over, there were on average seventeen people talked into a payment.
- **What it built.** A warning screen appears only when a payment is out of pattern for that person: a first payment to someone new, a recipient already reported for fraud, an unusually large amount, a sudden change in how the app is being used, a recipient name that imitates a known appeal, or a payment begun during a phone call, one of the strongest signs that a criminal is guiding the person in real time. When the app is opened during a call, a banner repeats one fact: Mercado Pago will never ask, on a call, for a code or for money to be moved. People can also name up to five trusted contacts who can lock the account from their own phones if a phone is lost or stolen, and can choose safe places, such as home, outside which balances are hidden and large transfers are limited. The safe-places setting began in Brazil in February 2026 and reached Mexico in May 2026.
- **What changed.** Against a year earlier, confirmed persuasion scams fell 48.6%, or 58% for each transfer made. Account takeovers fell 34% and phone takeovers 24.6%, while the platform kept growing. The company presents this as one illustration and not as proof that any one kind of financial firm is safer than another.
- **The limit.** Forsvar, a member of Cámara Uruguay Fintech, Uruguay's fintech association, writes in the same report that when organisations tighten controls without understanding the context, they add friction and shut out legitimate users, so that security itself becomes a barrier to inclusion. A warning protects people when it is rare, timely and specific.

For people who build apps and websites

1. **Put the warning where the decision is made:** on the screen where money is about to leave, a payee is added or a password is changed, and not only in a newsletter or a help page.
2. **Warn when something is out of pattern for that person,** not at one fixed amount for everyone, so that a warning stays rare enough to be read.
3. **Say one true thing in plain words:** what your service will never ask for, and how to reach you on a number the person finds for themselves.
4. **Treat a payment made during a phone call, to a new payee or after a sudden change in behaviour as a reason to pause,** and offer a pause before a refusal.
5. **Let people name trusted contacts** who can lock an account when the owner cannot.
6. **Let people set their own limits and safe places,** and keep every safety setting easy to find in a hurry.
7. **Test with the people least served,** including older people, disabled people, people new to the internet and people reading in a second language, so that protection never becomes a locked door.
8. **Publish what changed:** confirmed cases, money lost and how quickly people were helped, so that others can check and repeat what works.

Other measures and their results so far

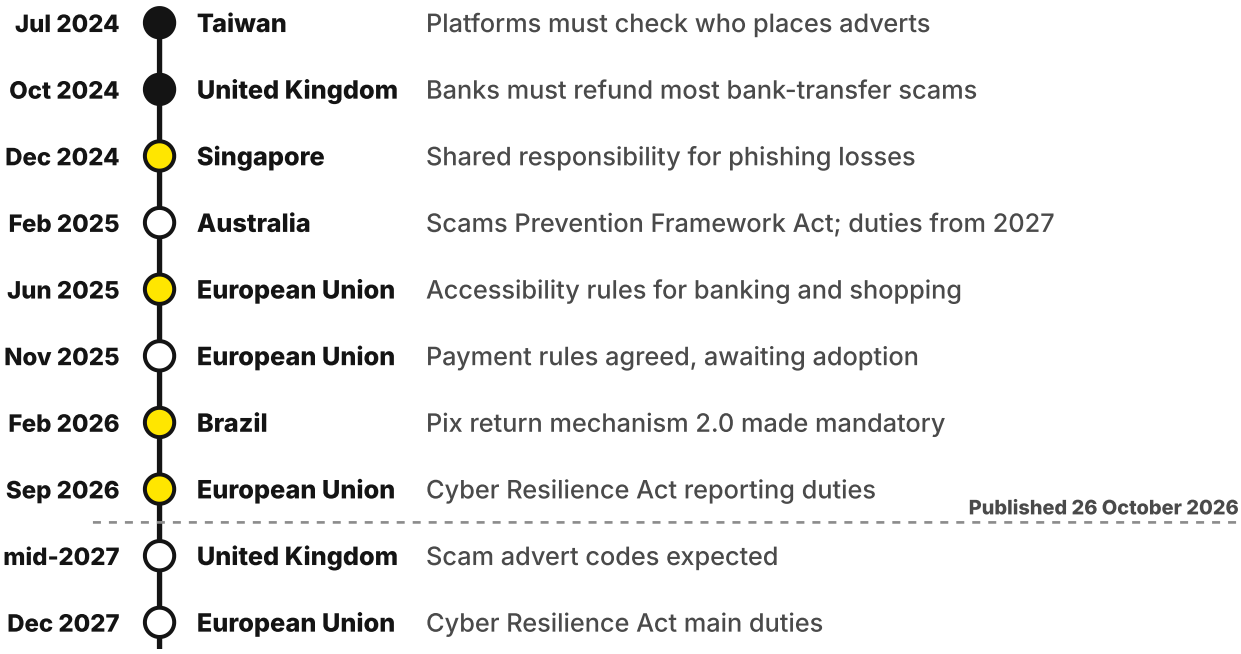


Figure 17. Rules that change who pays, 2024 to 2027, and whether a measured result has been published.

Police calls before money leaves: Hong Kong

Police contact people who appear to be in the middle of a scam. In 2025 they stepped in on 4,060 cases and stopped HK$480 million (about US$61.6 million) in payments (Anti-Deception Coordination Centre).

Helpline 1930: India

The Ministry of Home Affairs reports that more than ₹11,158 crore (about US$1.28 billion) had been saved through helpline 1930 and its reporting system by 30 June 2026 (Press Information Bureau, 28 July 2026).

Pix return mechanism: Brazil

Banco Central do Brasil, the central bank, reports that the earlier version of its return mechanism for Pix, the instant payment system, returned about 9% (9.2% from January to August 2025). Version 2.0 became mandatory on 2 February 2026.

Impersonation Rule: United States

Finalised in 2024. The Federal Trade Commission has obtained more than US$70 million in redress, money ordered back to the people harmed.

159: United Kingdom

A phone number that connects people safely to their own bank. It passed one million calls by 30 April 2025 (Stop Scams UK).

Shared responsibility: Singapore

In force since 16 December 2024, it sets out in order whether the bank or the telecoms firm pays for phishing losses. No outcome data has been published yet.

Name check before a transfer: European Union

Since 9 October 2025, payment providers in the euro area must check that the name of the person or business being paid matches the account before a euro transfer is sent, and tell the payer if it does not (Regulation (EU) 2024/886). This closes a common step in persuasion scams, where the criminal supplies an account in another name. No outcome data has been published yet.

Also on the way: Australia's Scams Prevention Framework, with duties on banks, telecoms firms and digital platforms phasing in from 2027; the United Kingdom's duties on the largest platforms to tackle scam adverts, with final codes from the Office of Communications expected by mid-2027; new European Union payment rules provisionally agreed between the Council of the European Union and the European Parliament on 27 November 2025, under which a platform that was told about fraudulent content and did not remove it would be liable to a bank that refunded the customer; the European Union's Cyber Resilience Act, which requires digital products to be safe as sold, with its main duties from 11 December 2027; and, in Spain, a register of the names companies use to send text messages, which telephone operators are introducing in 2026 so that messages from unregistered sender names are blocked before delivery (Ministerial Order TDF/149/2025, as described by Banco Santander in the Organization of American States' report).

7 What platforms publish, and what others found

Platforms publish the scale of what they remove, and those figures are large and real. Regulators, consumer groups and journalists publish what gets through. Seven large technology companies were reviewed against six things they could publish about scams, using their own transparency centres, annual reports and European Union Digital Services Act reports, as at 24 October 2026. The Digital Services Act is the European Union law that sets duties for large online platforms.

	Meta	Alphabet	Microsoft	Apple	Amazon	TikTok	X
Scam adverts or accounts removed	●	●	◑	●	◑	◑	◑
Time taken to act on reports	◑	●	●	●	●	●	●
Moderation staff	●	●	●	●	●	●	●
Money people lost on the service	○	○	○	○	○	○	○
Refunds paid to people scammed	○	○	○	○	○	○	○
Revenue from adverts later removed as scams	○	○	○	○	n/a	○	○

● Published ◑ Partly ○ Not found in the sources reviewed

As at 24 October 2026. Much of what is published covers the European Union only.

Figure 18. What seven companies publish about scams. This report's review of company publications, as at 24 October 2026.

Most of these companies publish removals, and every one publishes some moderator numbers or response times, at least for the European Union. None of them, in the sources reviewed, publishes what people lost to scams on its service, refunds paid to people scammed, or revenue from adverts later removed as scams.

Meta (the company that owns Facebook, Instagram and WhatsApp)

What Meta says. Meta removed more than 134 million scam adverts in 2025, up to 3 December, and reports of scam adverts from people using its services fell by more than half over 15 months (Meta, "Scams are bad for business", 3 December 2025). For the whole of 2025 it said it removed 159 million scam adverts and 10.9 million accounts linked to scam centres (as reported by The Record, 11 March 2026).

What a regulator found. In 2023, 14 United Kingdom banking groups recorded 222,534 bank-transfer scams. In 119,338 of them (54%) the person said the scam started on a Meta service, and those cases made up £62.7 million of about £341 million lost (18%) (Payment Systems Regulator, December 2024).

What journalists reported from Meta's internal documents (Reuters, 6 November 2025): an internal projection that about 10% of Meta's 2024 revenue, about US$16 billion, could come from adverts for scams and banned goods; an internal estimate that people were shown about 15 billion "higher risk" scam adverts a day, the documents' own label; that advertisers were banned only when Meta's systems were 95% sure of fraud, and suspected scammers below that level were charged more for adverts; and a 2023 internal finding that 96% of about 100,000 valid weekly reports of fraudsters sending messages were ignored or wrongly rejected. Reuters later reported that Meta's own tests found advertiser checks cut scam adverts "in some markets by as much as 29%" (31 December 2025).

What Meta said in reply. A Meta spokesperson said the documents "present a selective view that distorts Meta's approach to fraud and scams", called the estimate "rough and overly-inclusive", and said reports of scam adverts had fallen 58% over 18 months (Reuters, 6 November 2025). In March 2026 Meta's director of global threat disruption said "the 10% figure was misleading" (The Record, 11 March 2026).

Alphabet (the company that owns Google and YouTube)

What Google says. It blocked or removed 8.3 billion adverts and suspended 24.9 million advertiser accounts in 2025, including 602 million adverts and 4 million accounts "associated with scams", and its systems caught over 99% of policy-violating adverts before they were served (Google, 2025 Ads Safety Report, 16 April 2026).

What others found. In the European Consumer Organisation's testing, Google was sent 30 of the reported scam adverts. Google's report gives no figures for losses, refunds or revenue from removed adverts.

TikTok

What journalists reported. Forbes reported internal documents showing that the list of violations leading to an immediate advertiser ban was cut from 37 to 13 in November 2025, and that Better Business Bureau complaints mentioning TikTok rose 142% in the following six months, from more than 5,500 complaints that the bureau had not verified (Forbes, 7 October 2026).

What TikTok said in reply. A spokesperson said: "These false allegations misrepresent TikTok's commitment to advertiser safety, platform integrity, and enforcement."

X

What regulators found. On 5 December 2025 the European Commission fined X €120 million in its first non-compliance decision under the Digital Services Act. It found that the paid blue checkmark "deceives users" and that this "exposes users to scams, including impersonation frauds". Australia's eSafety Commissioner reported that X's engineers focused on trust and safety fell from 279 to 55 between 27 October 2022 and 31 May 2023 (published January 2024).

What X said in reply. X appealed the fine to the General Court of the European Union on 20 February 2026, saying it resulted from "an incomplete and superficial investigation" and that X "remains committed to user safety and transparency".

Microsoft (including Bing and LinkedIn)

What Microsoft says. It "thwarted $4 billion in fraud attempts" between April 2024 and April 2025 and introduced a "Fraud-resistant by Design" policy requiring product teams to assess fraud risks (Microsoft, Cyber Signals issue 9, 16 April 2025). The US$4 billion is attempts stopped, as reported by Microsoft. LinkedIn publishes a median of about 21 minutes to act on notices in the European Union.

Consumer groups tested nearly 900 adverts

Consumer groups in 13 countries reported scam adverts to Meta, TikTok and Google. Twenty-seven per cent were taken down after notice and 52% were rejected or ignored. Twenty-nine member groups in 27 countries then filed complaints (European Consumer Organisation, 21 May 2026).

What people scammed say

In a Payment Systems Regulator survey of 688 people scammed (December 2024), 22% were satisfied with how technology firms responded, against 74% for banks.

Who acts when rules exist

Singapore issued Meta the first implementation directive, a legal order to act, under its Online Criminal Harms Act on 24 September 2025. Brazil's Supreme Federal Court decided on 26 June 2025 that platforms are treated as responsible for illegal content in paid adverts and boosted posts unless they can show they took proper care.

Blame

A survey by AARP and the Financial Industry Regulatory Authority's Investor Education Foundation (June 2022) found that 53% of adults see fraud victims as at least partly "culpable and blameworthy".

Why the gap exists

- **Stock-market rules cover attacks on the company, not fraud against the people who use it.** The United States Securities and Exchange Commission's 2023 cybersecurity disclosure rule requires companies to report incidents serious enough to matter to investors in the company itself.
- **Sustainability standards have no measure for fraud against users.** The Sustainability Accounting Standards Board's standards for internet companies cover privacy, data security and government requests.
- **Shareholders have not yet asked.** None of the ten shareholder proposals at Meta's annual meeting on 27 May 2026 addressed scams.
- **Banks show it can be done.** The Payment Systems Regulator has published refund rates firm by firm.

A model disclosure

One page per company, each year, independently audited:

1. Reports of scams received from people, by country, and the median time to act on them.
2. Scam adverts and accounts removed, and the share removed before anyone reported them.
3. The share of advertisers whose identity has been checked.
4. Losses reported by people using the service and confirmed by their banks, where that information is available.
5. Revenue from adverts later removed as scams.

6. Refunds or compensation paid to people.

7. Trust and safety staff, by language.

Items 1, 2 and 7 are already published in part by several companies. Items 4, 5 and 6 were not found for any company in the sources reviewed. The share of checked advertisers, item 3, was not part of this review.

8 Around the world: institutions in their own words

Institutions across Africa, Asia, the Americas and Europe publish their own figures and run their own measures. What each country counts depends on what it measures, so these figures cannot be compared or ranked. United States dollar values are converted for this report at 2025 average exchange rates (section 14).

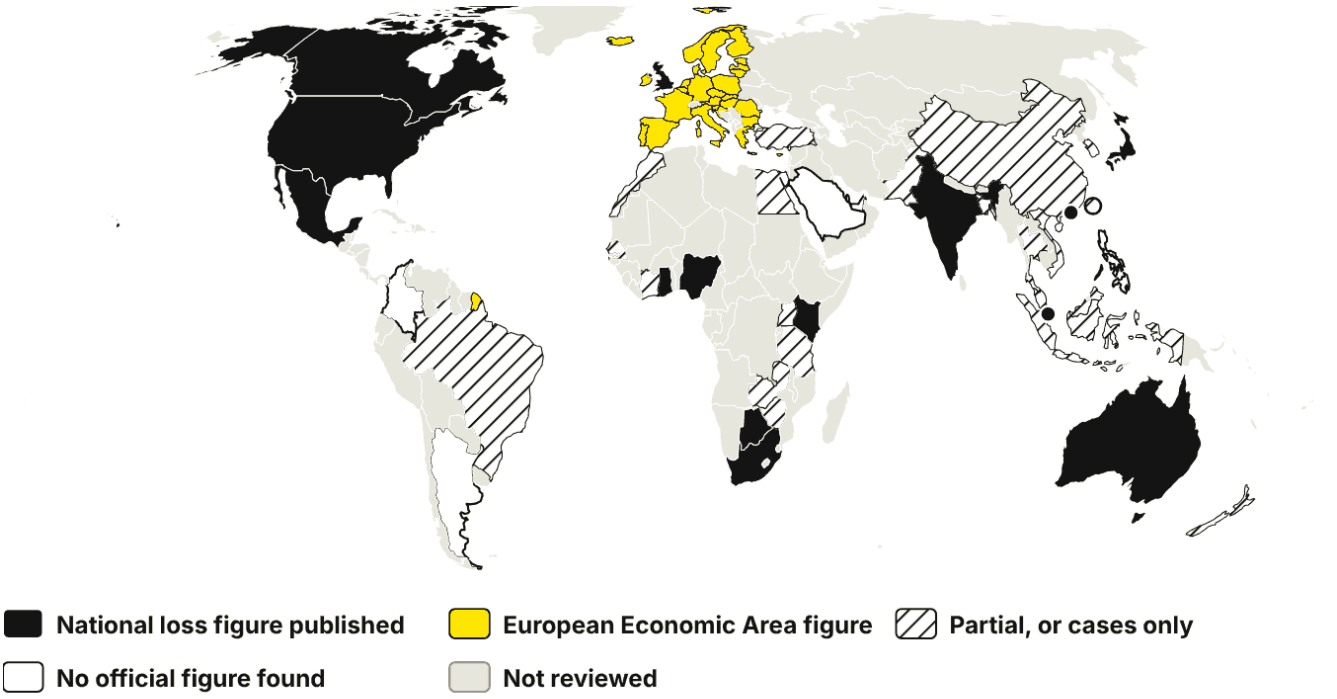


Figure 19. Who publishes an official scam-loss figure, as found on 27 October 2026. A country without a figure has fraud like everywhere else; what is missing is a published count.

South Africa

R2.407 billion (about US$135 million) in digital banking crime in 2025, from nine banks, up 29.2% from R1.86 billion in 2024. *Reported losses.* The 2024 statement counted all financial crime: R3.3 billion in 2023 falling to R2.7 billion in 2024, "almost 18 percent", with digital banking "65.3 percent of reported incidents". South African Banking Risk Information Centre. Card fraud on South African credit and debit cards rose 18% to R1.7 billion (about US$95 million) in 2025, and banking apps carried more than 70% of digital banking losses (same centre, 4 August 2026). In Statistics South Africa's survey of people aged 16 and over, 695,000 people (1.5%) had experienced consumer fraud in the five years before the 2025/26 survey, down from 1.0 million (2.3%) in the 2024/25 survey, a statistically significant fall of 31.8%. *Survey, fraud experienced over the past five years.* Governance, Public Safety and Justice Survey, 1 September 2026.

Nigeria

₦25.85 billion (about US$16.9 million) in fraud losses in 2025, down 51% from ₦52.26 billion, with cases down from 70,111 to 67,518. *Reported losses.* Its managing director said the 2024 figure was largely driven by a single fraud incident of ₦31.1 billion at one entity. Nigeria Inter-Bank Settlement System, January 2026; Techeconomy, 2 June 2026.

Kenya

KSh 1.594 billion (about US$12.3 million) lost to banking cyber fraud in 2024 across 353 cases, almost four times the KSh 412.5 million of 2023; mobile banking accounted for KSh 810.7 million. *Reported losses.* Central Bank of Kenya, Financial Sector Stability Report 2024, September 2025.

Ghana

24,778 fraud cases in 2025, up from 16,733 in 2024, with about GH¢101 million (about US$7.9 million) at risk, against GH¢99 million. Payment service providers, including mobile money, accounted for 24,124 of the cases. Banks and specialised deposit-taking institutions recovered GH¢3.7 million of the GH¢68.2 million at risk with them. *Money at risk.* Bank of Ghana, Banks, SDIs and PSPs 2025 Fraud Report, July 2026.

Africa-wide

Interpol, the international police organisation, reports that losses among the African countries responding to its survey rose from US$192 million to US$484 million between 2024 and 2025, with mobile money fraud the most common scam in 97% of them (36 countries, 2026). Its Operation Serengeti 2.0 made 1,209 arrests and recovered US$97.4 million across 18 African countries and the United Kingdom (August 2025).

More African institutions

Botswana: 175 fraudulent transactions and P8.16 million (about US$600,000) lost in 2024, and P2.26 million more across 32 cases by mid-2025 (Bank of Botswana, 28 August 2025). **Zimbabwe:** 3,241 fraud offences in January to March 2026 (Zimbabwe National Statistics Agency, cases only). **Uganda:** obtaining money by false pretences fell from 10,449 cases in 2024 to 8,455 in 2025 (Uganda Police Force, cases only). **Tanzania:** fraudulent attempts on phone networks fell 25.29% to 7,334 in April to June 2026 (Tanzania Communications Regulatory Authority, attempts, not losses). *Read on each institution's own publication.*

Reported through news: **Egypt:** EGP 116.8 million (about US$2.4 million) returned to fraud victims in 2025, against EGP 6.5 million in 2024, and EGP 4 billion of fraudulent transactions prevented (Central Bank of Egypt, 29 January 2026; Business Today Egypt). **Morocco:** 13,643 cybercrime cases in 2025, with 14.9 million dirhams (about US$1.6 million) lost to phishing by email and phone (General Directorate for National Security, 18 December 2025; TelQuel). **Côte d'Ivoire:** 12,100 complaints and 6.96 billion CFA francs (about US$11.9 million) lost in 2024 (National Agency for Information Systems Security; CIO Mag). **Senegal:** 3,794 cybercrime offences in 2025 (National Police; Dakaractu). **Zambia:** more than K111 million (about US$4.3 million) lost to cyber-related crime in January to June 2025 (ministerial statement to Parliament; Zambian Observer).

South Asia and Türkiye

Reported through news: **Pakistan:** Rs 8.32 billion (about US$29.5 million) lost over three years, with 76,646 complaints in 2025 (National Cyber Crime Investigation Agency documents; The Express Tribune, 11 September 2026). **Bangladesh:** Tk 926.01 million (about US$7.6 million) lost across 81,423 fraud cases in mobile money, cheques and cards in 2025 (Bangladesh Bank data; The Financial Express, 16 June 2026). **Türkiye:** in the first national crime victimisation survey, 3.5% of people aged 15 and over had been victims of cybercrime and 2.8% of consumer fraud in the past year (Turkish Statistical Institute, 20 May 2026; Medyascope). *Survey for Türkiye; reported figures elsewhere.*

India

24,02,579 complaints of financial fraud and **₹22,495 crore** (about US$2.58 billion; a crore is ten million rupees) reported to the national portal in 2025, against 19,18,835 complaints and ₹22,848 crore in 2024. *Reported losses.* Ministry of Home Affairs, Press Information Bureau, 11 February 2026. The Department of Telecommunications reports that its Financial Fraud Risk Indicator, which flags risky phone numbers to banks, has prevented ₹475 crore (about US$54.5 million) of losses (2 December 2025).

Singapore

37,308 scam cases in 2025, down 27.6% from 51,501, with losses falling from about S$1.1 billion to S$913.1 million (about US$699 million). Counting cybercrime as well, cases were 41,974, down 24.8%. In January to June 2026: 16,821 scam cases and about S$410.6 million lost. *Reported losses.* Singapore Police Force, 25 February and 26 August 2026. The Scams (Countermeasures) and Other Matters Act 2026, passed on 9 September 2026 and not yet in force, adds orders to disable accounts and limit services, and raises the maximum penalty under the Online Criminal Harms Act from S$1 million to S$10 million (Ministry of Home Affairs).

Hong Kong

43,212 deception cases in 2025, down 2.9%, with losses of about HK$8.1 billion (about US$1.04 billion), down 11.3%. In 80.4% of investment fraud cases the person was first contacted through social media or messaging apps. Its Scameter+ app, which checks suspicious contacts, had 1.15 million downloads. *Reported losses.* Anti-Deception Coordination Centre. From January to June 2026 the Hong Kong Police Force recorded 20,613 deception cases and HK$3.51 billion (about US$450 million) lost, both almost unchanged, while phone deception rose 45% to 4,830 cases. *Reported through news:* Sing Tao Headline and South China Morning Post, September 2026.

Japan

¥142.31 billion (about US$951 million) lost to special fraud, the police term for phone and impersonation fraud, and ¥183.43 billion (about US$1.23 billion) to investment and romance fraud on social media, in 2025. From 2026 the agency counts investment and romance fraud on social media inside its special fraud total: from January to August 2026 that total reached 29,687 cases and ¥236.07 billion (about US$1.58 billion), up ¥58.84 billion on the same months of 2025 counted the same way. *Reported losses, provisional.* National Police Agency, 2 October 2026.

South Korea

1.2578 trillion won (about US$885 million) lost to scam phone calls across 23,360 cases in 2025, up 47.2%. *Reported through news:* Herald Economy, 24 January 2026, citing the Korea National Police Agency, whose own page could not be reached. The agency's open data confirm the 23,360 cases (10,037 loan fraud and 13,323 impersonation, April 2026).

Taiwan

Detected scam adverts fell by about 99% and 98% between the 2024 peak and June 2026 (section 6). *Adverts detected, not money lost.* Ministry of Digital Affairs. Across all scams, about 162,000 cases and NT$89.326 billion (about US$2.87 billion) were lost in 2025, according to the National Police Agency's anti-fraud dashboard. *Reported through news:* Business Today, 6 January 2026.

South-East Asia and China

Reported through news: **Malaysia:** almost RM3 billion (about US$700 million) lost across more than 66,000 online crime cases in 2025 (Royal Malaysia Police; Malay Mail, 24 February 2026), and RM830 million to online scams in January to May 2026 (Ministry of Home Affairs, parliamentary reply). **Indonesia:** 411,055 reports and about Rp 9 trillion (about US$550 million) lost from November 2024 to December 2025; by September 2026, 702,342 reports and Rp 811.1 billion of victims' money blocked (Financial Services Authority, Indonesia Anti-Scam Centre; Kontan). **Thailand:** 31,198 cases and 1.792 billion baht (about US$54.5 million) lost in December 2025 alone (police figures presented by the Ministry of Digital Economy and Society; Pattaya Mail). **Vietnam:** losses estimated at more than 6,000 billion dong (about US$230 million) in the first 11 months of 2025 (Ministry of Public Security; Saigon Giai Phong). **China:** 258,000 telecom fraud cases solved in 2025, with no loss total published (Ministry of Public Security; Xinhua).

Australia

A$2.18 billion (about US$1.41 billion) in combined reported losses in 2025, up 7.8%; 2.7% of people aged 15 and over experienced a scam in 2024–25. *Reported losses and a survey rate.* National Anti-Scam Centre, March 2026; Australian Bureau of Statistics.

New Zealand

NZ$265 million (about US$154 million) in reported fraud losses across 12 banks, from an industry body, and a NZ$3 billion survey estimate. *Partial figures.* Payments NZ, Reported Fraud Monitor, November 2025; Netsafe.

Canada

More than C$704 million (about US$504 million) lost across more than 112,000 reports in 2025. *Reported losses.* Canadian Anti-Fraud Centre.

United States

US$20.9 billion reported lost across 1,008,597 complaints in 2025. *Reported losses.* Federal Bureau of Investigation.

Mexico

Fraud was the most frequent crime in 2025, at 8,290 per 100,000 inhabitants. 96.5% of frauds were not reported or did not lead to an investigation file, against 93.4% of all crimes. *Survey.* National Institute of Statistics and Geography, National Survey of Victimisation and Perception of Public Safety, 10 September 2026.

Argentina

94.4% of confirmed fraud cases at Mercado Pago, a payment app, from January to September 2025 were scams in which the person was persuaded to move the money. They fell 48.6% on a year earlier after warnings were built into the app (section 6). *Company figures.* Mercado Libre, in *From Bank to Blockchain*, Organization of American States, 2026. No official national loss figure was found.

Colombia

6 of 17 fintech companies with a financial education programme covered fraud prevention explicitly, in a survey by Colombia Fintech, the industry association; 15 of the 35 companies answering did not know what share of their users had been victims of fraud. *Survey of companies.* The number answering, about 35 of 285 members, is calculated for this report from the published percentages. Colombia Fintech, in *From Bank to Blockchain*, 2026. No official national loss figure was found.

Latin America and the Caribbean

Internet use rose from **68% to 81%** of people between 2019 and 2023 (International Telecommunication Union), and disclosed cyber incidents grew by an average of 25% a year over a decade, the fastest of any region. *Regional estimates.* World Bank, 28 November 2024.

Brazil

281,206 recorded cases of electronic fraud in 2024, and no national loss total. *Cases only.* Brazilian Forum on Public Security.

European Economic Area and Germany

€4.2 billion (about US$4.74 billion) in payment fraud across the European Economic Area in 2024 (European Banking Authority and European Central Bank). Germany's Federal Criminal Police Office counted about 335,000 cybercrime cases in 2025, with no figure for individuals' losses.

United Kingdom

£1.28 billion (about US$1.69 billion) in payment fraud in 2025 (UK Finance), and 4.5 million fraud incidents in England and Wales in the year to June 2026 (Office for National Statistics, survey). In Scotland, crimes of dishonesty recorded by Police Scotland, which include fraud, rose 6% in 2025-26, from 110,913 to 118,040 (Scottish Government, 23 June 2026).

Ireland

11,013 fraud, deception and related offences recorded in the year to the third quarter of 2025, down 6% from 11,765. Only incidents reported to An Garda Síochána, the national police service, are counted. *Reported offences.* Central Statistics Office, 22 December 2025.

No official national figure was found for Argentina, Colombia, Saudi Arabia, the United Arab Emirates, Qatar, Bahrain or the Philippines, or for the Middle East as a region; the figure in circulation for the Philippines comes from a private study. Figures in circulation for several of them come from industry or vendor surveys. These are gaps in what is published. For Argentina and Colombia, the company and industry figures above are labelled as such and do not fill the gap.

9 Charities, libraries and journalists

Charities, community groups and newsrooms hold sensitive information about the people they serve. Criminals target them, and in some cases so do governments, and many protect themselves with volunteers and free programmes.

- **United Kingdom charities.** An estimated 28% of charities (about 57,000) had a cyber breach or attack in the past year, and an estimated 525,000 cyber crimes were committed against them (Cyber Security Breaches Survey 2025/2026, 30 April 2026; survey estimates).
- **Attacks linked to governments.** Think tanks and non-governmental organisations were joint fourth among the sectors targeted by hackers linked to governments, at 7%, in what Microsoft observed among its own customers (Microsoft Digital Defense Report 2025).
- **Public-interest websites.** Cloudflare, a company that sells security services, reported blocking 38.5 billion attempted attacks against more than 3,400 public-interest websites in 120 countries protected by its free Project Galileo, between 1 February 2025 and 31 January 2026.

- **Spyware,** hidden software that watches a phone. Citizen Lab, a research laboratory at the University of Toronto, reported on 12 June 2025 that two European journalists had been targeted with spyware and confirmed one infection. Amnesty International reported on 16 December 2024 that spyware and phone-copying tools had been used against journalists and activists in Serbia.
- **Suppliers.** In August 2026 Beacon, a supporter-database supplier used by many charities, told its customers to assume that all their data had been downloaded.
- **Libraries.** The British Library's review of the ransomware attack of October 2023 found that the first detected access was at a server without two-step sign-in, and sets out 16 lessons (8 March 2024).

What charities are told, and what they have

Only 13% of charities report having all five basic controls of Cyber Essentials, the United Kingdom's baseline, and the funded programme for small organisations is closed to new applicants. Nine per cent review the security of their immediate suppliers. Thirty-six per cent of those that had a breach reported their most disruptive one outside the organisation. The share whose senior managers treat security as a high priority fell from 68% to 60%.

Who helps now

CyberPeace Builders, from the CyberPeace Institute, supported 645 non-profits with more than 1,600 volunteers (17 December 2025). The Ford Foundation raised the share of a grant that pays for running an organisation to at least 25% on project grants (2 November 2022). The Cybersecurity and Infrastructure Security Agency publishes guidance for civil society, *Mitigating cyber threats with limited resources* (14 May 2024).

10 From a scam to lost trust

The harm of a scam is larger than the sum stolen, and the difference is trust. Which? valued the yearly drop in wellbeing at about £3,684 for each victim of online fraud in the United Kingdom, against an average loss of about £600 (2019–20 data). In the Gallup survey, 77% of people scammed in the United States reported harm to their mental health or wellbeing. In a 2019 analysis of bank suspicious activity reports by the Consumer Financial Protection Bureau, the suspect was known to the older adult in 36% of reports, and the average loss was US$42,700 when the suspect was a family member against US$17,000 when it was a stranger.

The same chain runs through a whole financial system. The International Monetary Fund's Global Financial Stability Report of April 2024 found that cyberattacks had more than doubled since the pandemic, with financial firms the target of nearly one-fifth. Writing in the Organization of American States' 2026 report, an International Monetary Fund author sets out how the damage spreads: customers who lose trust in a bank after a breach or an outage can move their money out quickly, which some now call a "cyber run", and services that have no easy substitute can stop. Trust lost by one person, repeated across many, becomes a cost to everyone who relies on the same system.

Trust that rested on recognising a voice, a name or a logo can no longer carry the weight alone, because each can be copied. Trust that rests on checking can. For a person, that is a second route to the truth: hang up and call back on the number printed on the card, ask for the family safe word, or

run a free check before paying. For an institution, it is the same move at scale: publish the losses people report, the refunds paid and the revenue from adverts later removed as scams, so that anyone can check the claim that a service is safe. Each of the thirteen changes that follow replaces something people are asked to take on trust with something they can see.

11 Thirteen changes that would help

1. **Audited yearly disclosure by each large platform** of reports, removals, response times, checked advertisers, losses people report, scam-advert revenue, refunds and trust and safety staff, following the model in section 7. *Who acts: legislators and regulators; companies can begin voluntarily.*
2. **Platforms share the cost of refunds** where a scam began on their service and the platform was told and did not act. *Who acts: legislators, building on the European Union's payment rules.*
3. **Advertiser checks and fast removal of scam adverts,** as Taiwan requires. *Who acts: online safety regulators, including the Office of Communications in the United Kingdom.*
4. **One definition of a scam and one official loss estimate, with a range, in each country.** *Who acts: governments and statistics offices.*
5. **A standard "where did it start" field** in police, bank and regulator fraud reports, naming the platform or channel. *Who acts: police, banks and regulators.*
6. **A respectful reporting standard,** with satisfaction measured and published, so that no one is made to feel to blame. *Who acts: police, banks and platforms.*
7. **Plain-language, multilingual and accessible reporting routes,** with data published by age, disability and language. *Who acts: governments and platforms.*
8. **Safety settings on from the start, required in law.** *Who acts: legislators, following the Cyber Resilience Act.*
9. **Plain-language breach notices** that say what was taken and how. *Who acts: privacy regulators and legislators.*
10. **Funded community and library online-safety sessions, with results measured,** so that what works can be repeated. In the Oh, Behave! survey of 2026, 88% of people who had training found it useful and 50% of adults had none, and 32% of workers who use artificial intelligence had shared sensitive company information without their employer knowing. Employers can add to this by giving workers concrete examples of what may and may not be put into an artificial intelligence tool. *Who acts: governments, funders and employers.*
11. **A category for scams using artificial intelligence in crime reporting,** with a clear method note and research funding to match. *Who acts: statistics offices and police.*
12. **Cross-border tracing of stolen payments and shared-responsibility rules** for who pays, learning from Hong Kong, India, Singapore and Brazil. *Who acts: governments, central banks and banks.*
13. **Warnings built into the moment of payment,** shown when a payment is out of pattern for that person or begun during a phone call, with trusted contacts who can lock an account and safety

settings that are easy to find, tested with older people, disabled people and people new to the internet, and with results published (section 6). *Who acts: banks, payment apps, phone makers and the people who build apps and websites; regulators can ask for measured results, such as fewer confirmed scams, alongside lists of required controls.*

12 Find your place

Five questions locate a person, a household or an organisation. Each answer moves them along one of three lines: how exposed they are, how protected they are, and how well they could recover.

1. How do you connect?

Offline, by mobile phone only, or on several devices.

2. Do warnings reach you in your language and in plain words?

3. How do you pay?

Cash, mobile money, debit card, credit card or cryptocurrency. Cards usually carry the most protection.

4. What right to a refund do you have where you live?

5. Who can you ask before you act?

A family member, a friend who could lock your accounts if your phone were stolen, a librarian, a bank's official number, or a free check you trust.

- **A family member:** agree a call-back habit and a family safe word, and check which payment methods carry a refund right.
- **A person who works with older people, a library or a community group:** include the call-back habit and the reporting route in routine sessions, and share guides in the languages your community uses.
- **A policy maker:** define a scam in law, measure losses nationally, and publish the share of losses refunded, by payment method.
- **A bank, phone network or platform:** publish the losses people report, refunds paid and revenue from adverts later removed as scams.

Trust is rebuilt the same way at every scale, by giving people something they can check. A safe word for a family, a published number for a bank, an audited figure for a platform, and an official loss estimate for a country are the same act at different sizes.

13 The toolkit: from knowing to championing

The findings in sections 3 to 12 keep returning to the same moments: a message that asks for money, a call that sounds like family, a page that looks official, a document about to be pasted into an artificial intelligence. The next two pages set out UtilForge.org's free tools along a path, from knowing what you face to sharing what you know, each beside the problem in this report it helps with and beside the part that banks, platforms, phone networks and governments must play as well. The free large-print book *How to Become Safer Online* gathers the same checks in print, for people who share a phone, have a weak connection or are not online.

Why the tools are not scored

The two tools marked New, Before You Send and the Trusted People Card, answer the evidence in section 6.

SECTION 13 · THE TOOLKIT

FROM KNOWING TO CHAMPIONING

Each problem in this report has a tool that helps with it. The tools work in layers: **each tool covers one step, and using several adds layers.** Follow the path from what you know, to what you check, to what you set up, to what you share. Every tool runs on your own phone or computer at **utilforge.org/tools**, and what you type stays there.

KEY (L) Learn (C) Check (S) Set up (R) Recover

· **Their part**: what banks, platforms, phone networks and governments must do as well

1 KNOW

Know what you are facing

Insight first, so every choice after it is your own.

Their part: Platforms publish losses and refunds, and each country publishes one official loss figure (changes 1 and 4).

- (L) **This report** — who carries the harm, and what has cut it
- (L) **What Could a Criminal Find?** — what strangers can learn about you
- (L) **Password Habits Check** — six questions; you type no password
- (C) **Is This Warning Real?** — a forwarded warning, before you share it
- (R) **Official Help** — where to report, country by country
- (R) **First Hour Guide** — already paid? the steps, in order

2 CHECK

Check before you click, pay or reply

A pause at the one moment that matters.

Their part: Banks check the payee's name and warn at the moment of payment; platforms check who places adverts (changes 3 and 13).

- (C) **Is This a Scam Text?** — texts, emails and WhatsApp messages
- (C) **Delivery Text Check** — parcel and toll texts
- (C) **Email Sender Check** — look-alike senders
- (C) **Advert Check** — scam adverts on social media
- (C) **Shop Check** — a shop, before you pay it
- (C) **Official Site Check** — look-alike government sites
- (C) **Before You Pay** — payment pages, fees and links
- (C) **Before You Send** NEW — a transfer under pressure or on a call
- (C) **Before You Invest** — investment and crypto offers
- (C) **Before You Buy a Course** — courses and trading academies
- (C) **Before You Reply to a Recruiter** — fake jobs and fees to start
- (C) **Gift Card Request Check** — requests to pay in gift cards

3 PROTECT

Add layers to your phone and computer

Settings that keep working when you are busy or tired.

Their part: Phone makers and networks switch safety settings on from the start and block spoofed numbers (change 8).

- (S) **Phone Safety Checklist** — set up a relative's phone, together
- (C) **Before You Paste a Command** — fake “verify you are human” pages
- (C) **AI App Check** — AI apps and browser extensions
- (C) **VPN Check** — what a VPN does, and does not do
- (S) **Remove Photo Location** — hidden location inside photos
- (S) **Delete My Details** — your details on people-search sites

THE PATH CONTINUES →

4 MINDFUL

Think before you share with artificial intelligence

Human judgement stays in front of the machine.

Their part: Employers give staff concrete examples of what may and may not go into AI (change 10).

5 TOGETHER

Build the habit at home and at work

Rules agreed calmly, before anyone is under pressure.

Their part: Funders pay for community and library sessions and publish what they change (change 10).

6 SHARE

Share it, and bring others in

Online safety travels from one person to the next.

Their part: Governments make reporting routes plain, multilingual and accessible (change 7).

- **C** **Before You Paste Into AI** — what never to paste, and a check
- **C** **Prompt Injection Check** — hidden instructions in a page or email
- **C** **Release Check** — what hides in a document you send
- **S** **Family Safe Word** — a word only your family knows
- **L** **Check First poster and card** — five moments to pause, for the wall
- **S** **Kitchen and waiting staff cards** — habits for busy teams
- **S** **Hide Names From AI** — swap real names for labels first
- **C** **Invisible Character Remover** — hidden characters and tracking codes
- **S** **Redaction Studio** — black out details so they stay hidden
- **S** **Trusted People Card** NEW — who can lock your accounts, and a lock-screen reminder
- **S** **Staff AI Card** — four rules for staff using AI
- **L** **Digital Safety Clinics** — a 45-minute session plan



How to Become Safer Online, the free book

In 16-point type, for families, libraries and educators: the five steps most scams follow, the common frauds of 2026 each with a free check, a 45-minute session plan, and where to report, country by country.

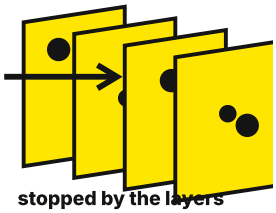
A printed copy reaches people who share one phone, have a weak connection or are not online. Anyone may print, photocopy and share it without asking. **utilforge.org/book**

This report is free to share and build on, with credit, and the Report and Recover Atlas sets out reporting routes and refund rules for 38 countries and the European Union.

One scam, several layers

Scams stack tricks: a cloned voice, a fake advert, a real-looking page, a request to pay. Each line covers the steps of one scam, so a gap in one tool is closed by the next.

A cloned voice of a relative asks for money	Family Safe Word → Trusted People Card → Before You Send → First Hour Guide
A deepfake advert promises investment returns	Advert Check → Official Site Check → Before You Invest → Official Help
A delivery text asks for a small fee	Delivery Text Check → Before You Pay → Is This a Scam Text? → First Hour Guide
At work, a customer's details are about to go into an AI assistant (not a scam: a data-sharing risk)	Before You Paste Into AI → Hide Names From AI → Staff AI Card



stopped by the layers

Every layer has holes. Harm gets through only where the holes line up, so each added layer leaves fewer ways through (layered defence, James Reason, 1990).

7 THE MOST IMPORTANT LAYER IS YOU

Every tool here waits for a person to use it and pass it on. **One warning shared with a parent, a friend or a colleague adds a layer for someone who may be most at risk.** Be the champion for the people you love and for those who need it most, and the safer online world this report describes is built one conversation at a time.

14 How to read the figures, and how this report was made

Four kinds of figure

- **Reported losses** are what people told an agency they lost. They are always lower than the real total, because most fraud is never reported.
- **Survey estimates** come from asking a sample of people and scaling up. They carry a likely range, given where the source gives it.
- **Modelled estimates** add an estimate for unreported fraud, using stated assumptions, and are given as ranges.
- **Company figures** are published by the company itself.

Where one source counts **cases** and another counts **money**, the report says which. The two tell different stories: in the United Kingdom in 2025, 66% of push-payment fraud cases began online, but they made up 32% of the money lost.

Words used in this report

Bank transfer (credit transfer): money sent from one account to another. **Push-payment fraud:** a scam in which a person is tricked into sending money from their own account. **Unauthorised fraud:** money taken without the person's permission, such as through a stolen card. **E-money:** money held in an app or digital wallet. **Mobile money:** money sent and stored by phone, such as M-Pesa. **Cryptocurrency:** digital money held outside the banking system. **Phishing:** fake messages that try to get passwords or money. **Recovery scam:** a second scam in which someone offers to get lost money back for a fee. **Two-step sign-in:** a code as well as a password when signing in. **Ransomware:** software that locks files until a ransom is paid. **Business email compromise:** criminals posing as a firm or supplier to redirect payments. **Median:** the middle value; half are higher and half lower. **Likely range:** the range in which a survey's true figure very probably lies. **Per 100,000 people:** out of every 100,000 people. **Crore:** ten million rupees. **Low- and middle-income countries:** the World Bank's grouping of countries by average income. **European Economic Area:** the 27 European Union countries plus Iceland, Liechtenstein and Norway. **Digital Services Act:** the European Union law that sets duties for large online platforms. **Transparency report:** a company's published report on what it removed. **Moderators, or trust and safety staff:** staff who review reports and remove harmful content. **Redress:** money ordered back to the people harmed. **Claims the rule covers:** scam claims that fall inside the United Kingdom refund rule.

Currencies

United States dollar values are converted for this report at the United States Internal Revenue Service's 2025 yearly average exchange rates (updated 17 September 2026). The Nigerian naira, Kenyan shilling and Ghanaian cedi are not in that table, so they are converted from HM Revenue and Customs 2025 annual average rates against the pound (published 31 March 2026). Figures from other years are converted at the same 2025 rates, so conversions are a guide to scale.

Method

Each figure was read on the publisher's own page or document where it could be reached, and each source is dated. Where a figure could only be read in news coverage, the text says so. Company figures are labelled as company figures. Internal documents are attributed to the news organisation that saw them, and the company's response sits beside them. Figures calculated for this report are marked as such. The draft was reviewed independently several times between 24 and 25 October 2026, and each figure a review questioned was checked again at its source.

Updated on 28 October 2026 to add the Oh, Behave! 2026 survey (see the update, 28 October 2026, before the sources), published on 22 October 2026. Updated on 29 October 2026 to add findings from the Organization of American States' report *From Bank to Blockchain* (2026) and figures from the World Bank and the International Monetary Fund (sections 2, 5, 6, 8 and 10), a thirteenth change (section 11) and the toolkit (section 13). Figures in that report that its authors credit to private security vendors were not used, because their original sources could not be read.

Limits

The report draws heavily on English-language sources and on countries that publish detailed fraud statistics. Survey and reported figures cannot be compared across countries or years. Where scams start is often known only from what people remember. Several primary documents could not be opened in full, and those items say so where they appear. Company figures, such as those from Mercado Pago, describe one company's own customers and cannot stand for a country.

Corrections and licence

Readers can send corrections to Lindsay McDonald at lindsay@utilforge.org, and every correction will be listed with its date at utilforge.org/reports/digital-trust-deficit. UtilForge.org plans to update the report as new data and new laws arrive.

UtilForge.org offers cybersecurity tools and guides for a safer online world for all, and is a 2026 Champion of Cybersecurity Awareness Month. This report is published under the Creative Commons Attribution 4.0 International licence: share it, quote it and build on it, with credit to UtilForge.org.

Spokesperson and media contact: Lindsay McDonald, lindsay@utilforge.org

UtilForge.org, 144 E 44th Street, Suite 106 #1033, New York, NY 10017, United States.
support@utilforge.org

> **Most fraud is never reported. Every scam a person reports, with where it began, makes the count more complete, and every figure that is published and checked returns a little of the trust a scam took.**

At a glance: what people say about their own protection

The Oh, Behave! survey of 2026 asked 5,000 adults in five countries what they feel, what they do and what happens to them. Younger adults say they lose money or data more often, people feel more confident than they act, and training closes the gap.

64% vs 33%

of adults in Generation Z, against baby boomers, said they had lost money or data to scams. Older people lose more each time; younger adults say it happens to them more often.

71% vs 41%

feel confident spotting a scam text, but only 41% always or very often report phishing, and 47% use two-step sign-in (multi-factor authentication) regularly.

88%

of people who had cybersecurity training found it useful, and 49% then started using two-step sign-in. Half of adults have no access to training.

39%

see data theft as an unavoidable cost of being online, and 33% say the same of losing money, while 66% fear becoming a victim and 37% expect to be one.

18%

have told an artificial intelligence a secret they had never told another person, and 40% have shared health information with one. 56% of artificial intelligence users have had no security or privacy training for it.

63%

believe criminals are more advanced than the people protecting them, and 57% doubt the capacity of law enforcement. This is the trust deficit in people's own numbers.

Oh, Behave! 2026, National Cybersecurity Alliance and CybSafe, published 22 October 2026: 5,000 adults in the United States, United Kingdom, India, Brazil and Singapore, surveyed 28 April to 19 May 2026. Self-reported figures from five countries.

Update, 28 October 2026: what people say about their own protection

The Oh, Behave! report 2026, from the National Cybersecurity Alliance and CybSafe, a company that studies how people behave online, asked 5,000 adults in the United States, United Kingdom, India, Brazil and Singapore between 28 April and 19 May 2026 and was published on 22 October 2026. It adds the view from the person's own side: what people feel, what they do and what they report. The answers are self-reported and come from five countries, so they sit beside the loss figures in sections 3 to 5 and are not added to them. This update was added on 28 October 2026, after the first edition of 26 October.

Adults who said they had lost money or data to scams, by generation, 2026



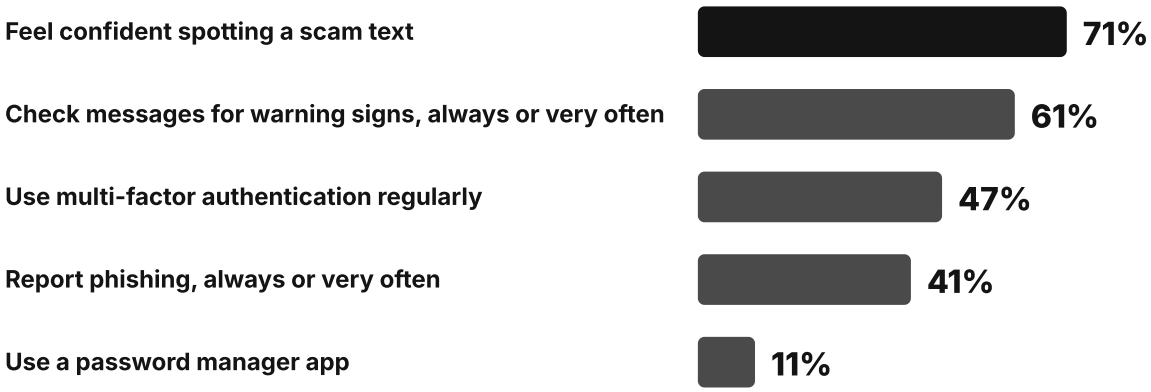
Oh, Behave! 2026, National Cybersecurity Alliance and CybSafe: 5,000 adults in five countries; figures via SecureWorld.

Figure 20. Adults who said they had lost money or data to scams, by generation. Oh, Behave! 2026 (National Cybersecurity Alliance and CybSafe, 22 October 2026), 5,000 adults in five countries. Generation figures as summarised by SecureWorld, 22 October 2026. The oldest group (aged 81 and over) is too small to compare and is not shown.

- **Younger adults say it happens to them more often, and older people lose more each time.** 64% of adults in Generation Z, 57% of millennials and 33% of baby boomers said they had lost money or data to scams. The survey's oldest group, people aged 81 and over, is too small to compare reliably and is left out. The Federal Trade Commission's reports show the same pattern for money in the United States: people in their twenties were more likely to report a loss (44%, against 24% of people in their seventies), and the middle loss was larger for older people (US$1,000 against US$417; section 4, finding 3).
- **Half of the adults surveyed have been a victim of cybercrime.** 50% said they had been a personal victim, up 6 points on 2025, across 5,662 incidents: phishing 16%, and job scams, identity theft and online marketplace scams 12% each. 66% fear becoming a victim and 37% expect to be one. 39% see data theft as an unavoidable cost of being online, and 33% say the same of losing money.
- **Confidence is higher than action.** 71% feel confident spotting a scam text and 64% a phishing email. 61% always or very often check messages for warning signs, and 41% always or very often report phishing. 47% use two-step sign-in regularly, up 6 points; 53% do not, and 21% know how to use it but do not (14%) or have stopped (7%). 60% reuse or slightly change a familiar password

when in a hurry, 11% use a password manager app, 70% understand passkeys at least a little and 39% use them.

What people feel and what they do, 2026

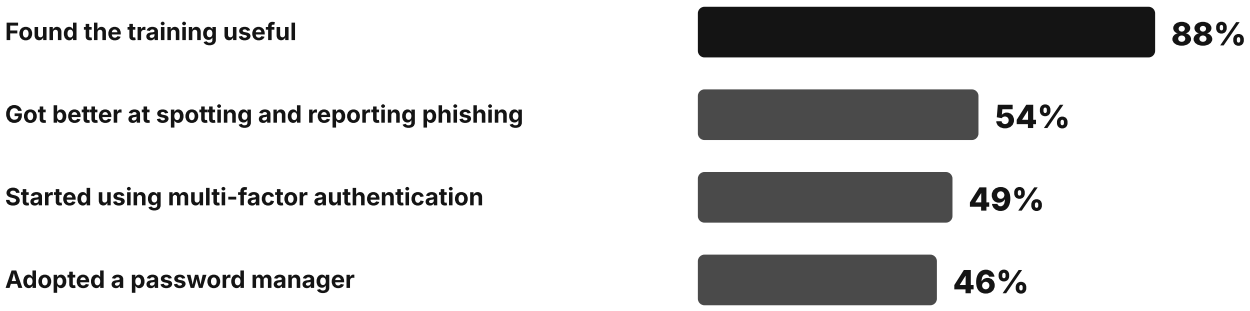


Oh, Behave! 2026, National Cybersecurity Alliance and CybSafe: 5,000 adults in five countries.

Figure 21. What people feel and what they do. Oh, Behave! 2026, 5,000 adults in five countries.

- **Training changes what people do.** 88% of the people who had cybersecurity training found it useful. Afterwards 54% got better at spotting and reporting phishing, 49% started using two-step sign-in and 46% adopted a password manager. Yet 50% of adults have no access to training, 47% of people in work face any mandatory training (in the United States, 55% of employed adults face none), and 50% say video is the format they prefer. Access to and use of training rose for every generation except Generation Z, where it fell by 8 points.

People who had cybersecurity training: what they said and did afterwards, 2026



Oh, Behave! 2026, National Cybersecurity Alliance and CybSafe: 5,000 adults in five countries.

Figure 22. What people who had cybersecurity training did afterwards. Oh, Behave! 2026, 5,000 adults in five countries.

- **Deepfakes.** 36% had received a deepfake call or video, up 2 points, and 40% of them lost money or data. In the United States 39% had been targeted and 28% of those lost money or data.
- **Artificial intelligence.** 80% use artificial intelligence, up from 65% a year earlier, and 56% of users have had no security or privacy training for it. 40% have shared health information with an artificial intelligence, 32% have shared feelings they would normally keep for someone close, and 18% have told one a secret they had never told another person.

- **Artificial intelligence at work.** Half of all adults use artificial intelligence at work: 41% began on their own initiative and 44% because their employer required or encouraged it. 52% of working people using it have had no security or privacy training for it, and 43% say their employer does not clearly explain what is acceptable to put into it. 32% of workers who use it have shared sensitive company information without their employer's knowledge (Generation Z 40%, millennials 35%, Generation X 22%, baby boomers 17%; 2,481 workers). Internal documents or customer data (50%) and financial data (47%) are most often shared. The survey's own advice to employers is to go beyond a signed policy and give people concrete examples of what is and is not acceptable.
- **Where people can learn.** Half of adults have no access to any cybersecurity training. Access is highest in information technology (76%) and finance (75%) and lowest in hospitality, where 58% have none, and it is higher for millennials (64%) and Generation Z (56%) than for baby boomers (26%). The formats people prefer are video (50%), online courses (38%), short lessons delivered when relevant (34%) and written guides (34%). The reasons given for skipping training are lack of time (21%), feeling already knowledgeable (19%), doubting it lowers risk (17%) and not seeing security as a priority (17%).
- **Countries.** India had the highest share of adults who said they had been a victim (63%), the most deepfake targeting (49%, and 55% of those lost money or data), the strongest sense that losing money (50%) or data (54%) cannot be avoided, the lowest share of adults who had received security training for artificial intelligence (27%), and the highest confidence in spotting artificial intelligence content. 69% of adults in India say artificial intelligence is good for society, against 37% in the United Kingdom. Singapore leads on training: 66% have access and 51% of those with access use it. Brazil has the most workplace oversharing with artificial intelligence (46% of workers who use it), and the United Kingdom the lowest victim share (40%). The survey does not report the Philippines.
- **Reporting.** 89% of incidents were reported somewhere, most often to a bank or card issuer, and the share reported to the police ranged from 27% to 41% by type of crime. These shares are higher than those in section 5 because this survey counts a report to any organisation, including a bank, while section 5 counts police and federal agencies. People who did not report named a loss too small to bother with, not knowing whom to contact and embarrassment.
- **Trust in the defenders.** 63% believe criminals are more advanced than the people protecting them, down 6 points, and 57% doubt the capacity of law enforcement, down 7. This is the trust deficit in people's own numbers.

Where people have training they act on it, and where they have none the gap between knowing and doing stays open. That is why change 10 in section 11 asks for funded community and library sessions with measured results, and for employers to give workers concrete examples of what may and may not be put into an artificial intelligence tool.

Sources

Sources were checked between 22 and 29 October 2026.

1. Federal Bureau of Investigation, Internet Crime Complaint Center, *Internet Crime Report 2025*, April 2026, including employment fraud and Operation Level Up. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
2. Federal Trade Commission, testimony to the Joint Economic Committee, 25 March 2026. https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud
3. Federal Trade Commission, *Protecting Older Consumers 2025–2026*, 19 October 2026. https://www.ftc.gov/system/files/ftc_gov/pdf/2026-older-adults-report-10192026.pdf
4. Federal Trade Commission, data on social media scam losses, 27 April 2026. https://www.ftc.gov/news-events/news/press-releases/2026/04/new-ftc-data-show-people-have-lost-billions-social-media-scams
5. Gallup for the Stop Scams Alliance, *United States of Scams*, June 2026. https://news.gallup.com/poll/710984/scam-victims-report-billions-lost-harm-mental-health.aspx
6. Government Accountability Office, report 26-109023, 25 March 2026. https://www.gao.gov/assets/gao-26-109023.pdf
7. Government Accountability Office, report 25-107088, 8 April 2025. https://www.gao.gov/products/gao-25-107088
8. Identity Theft Resource Center, *2025 Annual Data Breach Report*, January 2026.
9. AARP policy blog, 17 September 2024. https://blog.aarp.org/thinking-policy/more-data-needed-address-financial-exploitation-older-adults
10. AARP and the Financial Industry Regulatory Authority's Investor Education Foundation, *Blame and Shame in the Context of Financial Fraud*, June 2022.
11. Securities and Exchange Commission, Release 33-11216, 26 July 2023. https://www.sec.gov/files/rules/final/2023/33-11216.pdf
12. Meta Platforms, filing on the annual meeting of 27 May 2026. https://www.sec.gov/Archives/edgar/data/1326801/000162828026039193/meta-20260527.htm
13. Cybersecurity and Infrastructure Security Agency, *Mitigating cyber threats with limited resources: guidance for civil society*, 14 May 2024.
14. Consumer Reports, survey of 2,042 United States adults, October 2024.
15. Home Office, *Economic and social cost of fraud 2023 to 2024*, second edition, 14 July 2026. https://www.gov.uk/government/publications/economic-and-social-cost-of-fraud-2023-to-2024
16. Office for National Statistics, *Crime in England and Wales: year ending June 2026*, 22 October 2026. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2026
17. Office for Statistics Regulation, *Review of fraud and computer misuse statistics*, 3 April 2025.
18. House of Commons Committee of Public Accounts, *Progress combatting fraud*, 31 March 2023.
19. UK Finance, *Annual Fraud Report 2026*, June 2026.
20. Payment Systems Regulator, *Unmasking how fraudsters target UK consumers in the digital age*, December 2024. https://psr.org.uk/media/u0vnq1ra/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age-dec-2024.pdf
21. Payment Systems Regulator, reimbursement results, 1 July 2026. https://www.psr.org.uk/news-and-updates/latest-news/news/payment-fraud-falls-by-73m-following-psr-reimbursement-scheme/
22. Frontier Economics, *Independent Evaluation of APP Scam Policies: Summary Report*, 1 July 2026. https://www.frontier-economics.com/media/2ctd3jq2/app-fraud-evaluation-final-summary-report-26-06-26.pdf
23. Payment Systems Regulator, one year on, 8 October 2025. https://www.psr.org.uk/news-and-updates/latest-news/news/one-year-on-impact-of-app-reimbursement-on-victims/
24. Lloyds Bank, *Consumer Digital Index 2024*. https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/lb-consumer-digital-index-2024-report.pdf
25. Which?, 18 October 2021. https://www.which.co.uk/news/article/scams-impact-on-victims-costs-9-3-billion-a-year-a5mNq6i9316q
26. Department for Science, Innovation and Technology and Home Office, *Cyber Security Breaches Survey 2025/2026*, 30 April 2026.
27. British Library, *Learning lessons from the cyber-attack*, 8 March 2024.
28. Stop Scams UK, 159 one million calls, 2025.
29. Good Things Foundation, *Digital Nation 2026*, 14 July 2026.
30. Office of Communications, consultation on the fraudulent advertising code of practice, 2026.
31. National Anti-Scam Centre, *Targeting Scams Report 2025*, 30 March 2026. https://www.nasc.gov.au/system/files/targeting-scams-report-2025.pdf
32. Australian Bureau of Statistics, *Disability and crime*, 20 November 2025, and *Personal Fraud*, 12 March 2026.
33. eSafety Commissioner, transparency findings on X, January 2024.
34. Canadian Anti-Fraud Centre, top frauds of 2025, 25 February 2026. https://antifraudcentre-centreantifraude.ca/features-vedette/2026/02/top-fraud-2025-fraudes-plus-courantes-eng.htm
35. Meta, *Scams are bad for business*, 3 December 2025.
36. The Record, 11 March 2026. https://therecord.media/meta-scam-advertising-crackdown
37. Reuters investigations, 6 November and 31 December 2025, read through syndicated copies.
38. Google, *2025 Ads Safety Report*, 16 April 2026. https://blog.google/products/ads-commerce/2025-ads-safety-report/
39. Forbes, 7 October 2026.
40. Microsoft, *Cyber Signals issue 9*, 16 April 2025, and *Digital Defense Report 2025*.
41. Apple, App Store Transparency Report 2025; Amazon, *Trustworthy Shopping Experience Report 2025*, 22 April 2026; each company's Digital Services Act transparency reports.
42. European Commission, decision on X under the Digital Services Act, 5 December 2025. https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act
43. X, statement on its appeal, 20 February 2026.
44. European Consumer Organisation, 21 May 2026. https://www.beuc.eu/press-releases/consumer-groups-file-complaints-against-meta-tiktok-and-google-failing-protect
45. European Banking Authority and European Central Bank, report on payment fraud, 15 December 2025. https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf
46. European Parliament and Council of the European Union, payment services agreement, 27 November 2025.
47. International Telecommunication Union, *Facts and Figures 2025*, 17 November 2025. https://www.itu.int/en/mediacentre/Pages/PR-2025-11-17-Facts-and-Figures.aspx
48. Organisation for Economic Co-operation and Development, *Trust Survey 2026*; Edelman, *Trust Barometer 2026*; World Values Survey.

49. Cohn, Maréchal, Tannenbaum and Zünd, "Civic honesty around the globe", *Science*, 20 June 2019.

50. Office of the United Nations High Commissioner for Human Rights, report on scam operations in South-East Asia, February 2026.

51. Interpol, *Africa Cyberthreat Assessment*, 2025 and 2026, and Operation Serengeti 2.0, 22 August 2025.

52. Citizen Lab, 12 June 2025; Amnesty International, 16 December 2024.

53. Beacon incident statement, August 2026.

54. CyberPeace Institute, CyberPeace Builders annual report, 17 December 2025; Ford Foundation, 2 November 2022.

55. GSM Association, *The Mobile Gender Gap Report 2025*, and *Mobile Gender Gap Report 2026*, 10 June 2026 (source 85).

56. UN Women, survey of women in public life, April 2026.

57. World Bank, *Global Findex 2025*, and *Remittance Prices Worldwide*, August 2025.

58. South African Banking Risk Information Centre, annual crime statistics 2024 (28 August 2025) and 2025 (August 2026).

59. Nigeria Inter-Bank Settlement System, January 2026; Techeconomy, 2 June 2026.

60. Central Bank of Kenya, *Financial Sector Stability Report 2024*, September 2025.

61. Bank of Ghana, 2024 fraud report.

62. Ministry of Home Affairs, India, through the Press Information Bureau, 11 February 2026 and 28 July 2026. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2226441

63. Department of Telecommunications, India, 2 December 2025.

64. Singapore Police Force, annual brief 2025 (25 February 2026) and mid-year brief (26 August 2026). https://www.police.gov.sg/-/media/SPF/Advisories/Scams/Annual-Scam-and-Cybercrime-Brief-2025.pdf

65. Monetary Authority of Singapore and Infocomm Media Development Authority, Shared Responsibility Framework, 16 December 2024.

66. Ministry of Home Affairs, Singapore, implementation directive to Meta, 24 September 2025.

67. Anti-Deception Coordination Centre, Hong Kong, statistics. https://www.adcc.gov.hk/en-hk/statistic.html

68. National Police Agency, Japan, 2025 fraud statistics.

69. Herald Economy, 24 January 2026, citing the Korea National Police Agency.

70. Ministry of Digital Affairs, Taiwan, 17 July 2026. https://moda.gov.tw/en/ADI/news/latest-news/20198

71. Banco Central do Brasil, Fórum Pix, 4 December 2025; Supreme Federal Court of Brazil, decision of 26 June 2025; Brazilian Forum on Public Security, 2025.

72. National Institute of Statistics and Geography, Mexico, *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública 2026* (reference year 2025), 10 September 2026. https://inegi.org.mx/contenidos/saladeprensa/boletines/2026/envipe/ENVIPE2026_RR.pdf

73. Federal Criminal Police Office, Germany, 2025.

74. Payments NZ, Reported Fraud Monitor, November 2025; Netsafe, 2025 losses.

75. AARP, cryptocurrency kiosk protections. https://www.aarp.org/advocacy/crypto-atm-fraud-protections/

76. United States Internal Revenue Service, yearly average currency exchange rates, updated 17 September 2026. https://www.irs.gov/individuals/international-taxpayers/yearly-average-currency-exchange-rates

77. HM Revenue and Customs, 2025 average exchange rates, published 31 March 2026. https://trade-tariff.service.gov.uk/exchange_rates/view/2025-12?type=average

78. Australian Bureau of Statistics, *Disability and Crime*, 20 November 2025. https://www.abs.gov.au/articles/disability-and-crime

79. Ministry of Justice (New Zealand), New Zealand Crime and Victims Survey, Key Stories, 7 May 2026. https://www.justice.govt.nz/about/news-and-media/media-releases/key-stories-report-analyses-crime-stats/

80. Statistics Canada, *Self-reported fraud in Canada, 2019*, Table 3, 24 July 2023. https://www150.statcan.gc.ca/n1/pub/89-652-x/2023001/tbl/tbl03-eng.htm

81. Office for National Statistics, *Nature of fraud and computer misuse in England and Wales: year ending March 2025*, 26 March 2026. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2025

82. Federal Reserve Bank of Kansas City, *How Do Consumers' Fraud Experiences Vary with Their Financial Vulnerability?*, 8 October 2025. https://www.kansascityfed.org/research/payments-system-research-briefings/how-do-consumers-fraud-experiences-vary-with-their-financial-vulnerability/

83. Federal Reserve Board, *Economic Well-Being of U.S. Households in 2025*, 13 May 2026. https://www.federalreserve.gov/publications/2026-economic-well-being-of-us-households-in-2025-executive-summary.htm

84. Financial Conduct Authority, *Financial Lives 2024: Fraud and scams*, May 2025. https://www.fca.org.uk/publication/financial-lives/fls-2024-fraud-scams-financial-promotions.pdf

85. GSM Association, *Mobile Gender Gap Report 2026*, 10 June 2026. https://www.gsma.com/newsroom/?p=25938

86. International Telecommunication Union, *Facts and Figures 2025: the gender digital divide*, 15 October 2025. https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-the-gender-digital-divide/

87. Eurostat, the European Union Agency for Fundamental Rights and the European Institute for Gender Equality, EU gender-based violence survey, 3 March 2026. https://fra.europa.eu/en/news/2026/eu-wide-survey-highlights-scale-psychological-economic-and-cyber-violence-against-women

88. Instituto Nacional de Estadística y Geografía, *MOCIBA 2024*, 17 July 2025. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2025/mociba/MOCIBA2024_RR.pdf

89. eSafety Commissioner (Australia), sexual extortion reports. https://esafety.gov.au/newsroom/media-releases/young-men-bear-brunt-sexual-extortion-reports-rise

90. Eurostat, internet use by disability, 27 August 2025. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250827-1

91. United Nations Department of Economic and Social Affairs, *Disability and Development Report 2024*, Target 9.c. https://social.desa.un.org/sites/default/files/2025-09/DDR2024-Target9C.pdf

92. GSM Association, *The Mobile Disability Gap Report 2025*, July 2025. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2025/07/GSMA-The_Mobile-Disability_Gap_Report-2025.pdf

93. Central Bank of Kenya, *2024 FinAccess Household Survey*, December 2024. https://www.centralbank.go.ke/wp-content/uploads/2024/12/2024-FINACCESS-HOUSEHOLD-SURVEY-MAIN-REPORT.pdf

94. Consultative Group to Assist the Poor and Innovations for Poverty Action, *Digital Finance Consumer Risks: Senegal National Study*, June 2023. https://findevgateway.org/sites/default/files/publications/2023/Senegal_DFS%20Risks%20Survey%20Report.pdf

95. Sarah Barrington, Emily Cooper and Hany Farid, *People are poorly equipped to detect AI-powered voice clones*, Scientific Reports, 2025. https://pmc.ncbi.nlm.nih.gov/articles/PMC11958761/

96. Consumer Financial Protection Bureau, *Suspicious Activity Reports on Elder Financial Exploitation*, February 2019. https://www.consumerfinance.gov/data-research/research-reports/suspicious-activity-reports-elder-financial-exploitation-issues-and-trends/

97. Scottish Government, *Recorded Crime in Scotland, 2025-26*, 23 June 2026. https://www.gov.scot/publications/recorded-crime-scotland-2025-26/

98. Central Statistics Office, Ireland, *Recorded Crime Q3 2025*, 22 December 2025. https://www.cso.ie/en/releasesandpublications/ep/p-rc/recordedcrimeq32025/mainresults

99. South African Banking Risk Information Centre, annual crime statistics 2025, 4 August 2026. https://www.sabric.co.za/?p=4450

100. Statistics South Africa, Governance, Public Safety and Justice Survey 2025/26, 1 September 2026. https://www.statssa.gov.za/publications/P0341/P03412026.pdf

101. Bank of Ghana, Banks, SDIs and PSPs 2025 Fraud Report, July 2026. https://www.bog.gov.gh/wp-content/uploads/2026/07/FRAUD-REPORT-2025.pdf

102. National Police Agency, Japan, special fraud January to August 2026 (provisional), 2 October 2026. https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/261002/01.html

103. Ministry of Home Affairs, Singapore, second reading of the Scams (Countermeasures) and Other Matters Bill, 8 September 2026. https://www.mha.gov.sg/media-room/newsroom/second-reading-of-the-scams-countermeasures-and-other-matters-bill/

104. Korean National Police Agency, open data, 2 April 2026. https://www.data.go.kr/dcat/metadata/15063815

105. Bank of Botswana, press release, 28 August 2025; Zimbabwe National Statistics Agency, Crime in Zimbabwe, first quarter 2026; Uganda Police Force, Annual Crime Report 2025, 2 April 2026; Tanzania Communications Regulatory Authority, Communications Sector Performance Report, quarter ending June 2026.

106. News reports cited in section 8: Sing Tao Headline and South China Morning Post (Hong Kong, September 2026); Business Today (Taiwan, 6 January 2026); Business Today Egypt (29 January 2026); TelQuel (18 December 2025); CIO Mag (May 2025); Dakaractu (12 March 2026); Zambian Observer (July 2025); The Express Tribune (11 September 2026); The Financial Express (16 June 2026); Medyascope (20 May 2026); Malay Mail (24 February 2026); Business Today Malaysia (24 June 2026); Kontan (9 January and 6 October 2026); Pattaya Mail (February 2026); Saigon Giai Phong (7 January 2026); Xinhua (9 January 2026).

107. National Cybersecurity Alliance and CybSafe, *Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2026*, 22 October 2026. https://www.staysafeonline.org/articles/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2026

108. National Cybersecurity Alliance and CybSafe, press release, *Oh, Behave! Report Finds Cybersecurity Awareness Is High, and People Are Ready to Act*, 22 October 2026 (5,000 adults; fieldwork 28 April to 19 May 2026). https://www.globenewswire.com/news-release/2026/10/22/3386257/0/en/the-national-cybersecurity-alliance-and-cybsafe-s-oh-behave-report-finds-cybersecurity-awareness-is-high-and-people-are-ready-to-act.html

109. CybSafe, *Oh, Behave! 2026-2027*, report page, 22 October 2026. https://www.cybsafe.com/whitepapers/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2026-2027

110. SecureWorld, *Oh, Behave! 2026 Report: AI Moved in, Guardrails Didn't*, 22 October 2026, the source here for the generation figures, the artificial intelligence sharing figures, the deepfake figures and the reporting figures, which could not be read in the full report. https://www.secureworld.io/industry-news/oh-behave-2026-security-awareness

111. Organization of American States, Inter-American Committee against Terrorism, Cybersecurity Section, *From Bank to Blockchain: Cybersecurity for People in the Financial Ecosystem of the Americas*, 2026 (ISBN 978-0-8270-8258-8), including chapters by Banco Santander (2.1, 2.2), Mercado Libre (3.1 to 3.3), Colombia Fintech (3.4), Forsvar and Cámara Uruguay Fintech (3.5) and an International Monetary Fund author (8.1); the views are the contributors' own. https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=1567&lang=1

112. World Bank, Estefania Vergara Cobos and Hualong Diao, *From fiction to reality: How Latin America became the world's most critical cyber battleground*, 28 November 2024. https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

113. International Monetary Fund, *Global Financial Stability Report*, April 2024, chapter 3, *Cyber Risk: A Growing Concern for Macrofinancial Stability*, and the Fund's blog *Rising Cyber Threats Pose Serious Concerns for Financial Stability*, 9 April 2024. https://www.imf.org/en/blogs/articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

114. Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 on instant credit transfers in euro, including the check of the payee's name. https://eur-lex.europa.eu/eli/reg/2024/886/oj

115. National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, 26 February 2024. https://doi.org/10.6028/NIST.CSWP.29

116. James Reason, *Human Error*, Cambridge University Press, 1990, the source of the layered-defence model.

117. AV-TEST Institute, test procedures for security software (protection, performance and usability tested against live threats). https://www.av-test.org/en/about-the-institute/test-procedures/

118. UtilForge.org, *How to Become Safer Online*, a free large-print book, October 2026. https://utilforge.org/book



This report contains 1,008,597 dots, one for each complaint made to the Federal Bureau of Investigation's Internet Crime Complaint Center in 2025: 990,231 on this page, 3,966 on the front cover and 300 at the top of every page between. 201,266 are yellow, one for each complaint from people aged 60 and over, and 197,052 of them form the padlock on this page. Most fraud is never reported.

UtilForge.org · Cybersecurity first. A safer online world for all. Practical tools and guides for a digital future. · Digital inclusion reports and free cybersecurity tools · every check runs on your own phone or computer · utilforge.org · Free large-print book: utilforge.org/book · Videos: youtube.com/@utilforge · This report: utilforge.org/reports/digital-trust-deficit · Published under the Creative Commons Attribution 4.0 International licence. · UtilForge.org, 144 E 44th Street, Suite 106 #1033, New York, NY 10017, United States · Spokesperson: Lindsay McDonald, lindsay@utilforge.org · support@utilforge.org