GASA
Global Anti-Scam Alliance

SCAMADVISER

whoscall

State of Scams in Taiwan

2025 REPORT

INSIGHTS

LEARN MORE



Scams in Taiwan: Daily Attacks, Delayed Detection



Jorij Abraham
MANAGING
DIRECTOR

GASA
Global Anti-Scam Alliance

About GASA

The Global Anti-Scam Alliance (GASA) is a non-profit organization whose mission it is to protect consumers worldwide from scams. We realize our mission by bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, telecom operators, internet platforms and service providers, cybersecurity and commercial organizations to share insights and knowledge surrounding scams. We build networks in order to find and implement meaningful solutions.

Our study of 1,000 Taiwanese adults reveals something troubling: while 73% feel confident they can spot scams, 65% of these same people still fell victim to fraud in the past year. This gap between confidence and outcomes shows just how sophisticated modern scam operations have become.

Daily Digital Danger: 149 Scam Encounters Per Person Annually

Taiwanese adults face an average of 149 scam encounters per year—effectively one every two to three days. The research, conducted by the Global Anti-Scam Alliance and Gogolook, shows Taiwan is among the most heavily targeted populations globally, with fraud attempts hitting people across multiple channels relentlessly. What's particularly concerning: 32% of scam victims take longer than a day to recognize fraudulent activity. Generation Z and suburban residents seem especially vulnerable to these extended exposures, giving scammers crucial time to extract funds and personal information before people catch on.

Platform and Traditional Vulnerabilities

The numbers tell a clear story: 75% of scam attempts happen on platforms with direct messaging capabilities. Phone calls lead the way (50%), followed by email (37%) and social media (34%). Facebook and Instagram have become scammers' preferred hunting grounds, accounting for 52% and 42% of platform-based scams respectively.

Recovery Success Despite Reporting Challenges

Despite widespread victimization, there's some encouraging news: 85% of financial victims reported scams to payment services, and 38% successfully recovered at least partial losses. Scammers still prefer familiar methods—wire transfers (32%), cash payments (17%), and gift cards (17%)—to extract funds.

There's a notable disconnect in Taiwan's anti-scam landscape. While 26% of adults expect the government to lead prevention efforts, people actually rate banks and payment providers as most effective in practice. This mismatch suggests we need clearer roles and better coordination between sectors.

Human Impacts

The impact goes deeper than financial losses. About 52% of victims experienced significant stress, while 28% report becoming more vigilant—a lasting change in how they approach digital interactions. These psychological effects show how scams reshape behavior patterns across Taiwanese society.

Public Demands Severe Consequences

Reflecting frustration with the scam epidemic, 37% of Taiwanese adults favor severe punishments for major scam crimes, including life imprisonment for perpetrators who steal an entire annual salary. This strong sentiment indicates how deeply concerned people are about the current fraud environment.

Taiwan's digital future depends on addressing these vulnerabilities before they undermine trust in online commerce and communication. The data points to clear opportunities: better coordination between institutions, faster detection systems, and stronger protections on messaging platforms. Most importantly, it shows that despite growing sophistication in scam techniques, people are fighting back—reporting incidents, recovering losses, and adapting their behaviors.

Inside Taiwan's US$2 Billion Scam Crisis: Why Collaboration Is Key to Prevention



Boice Lin
CHIEF BUSINESS OFFICER
SCAMADVISER

About ScamAdviser

ScamAdviser is a global leader in AI-powered scam prevention, protecting businesses and individuals in real time. Our Anti-Scam Intelligence platform can protect users from untrustful websites, messages, and calls. Stopping scammers before they strike. Trusted by 400+ partners and used by over 1 billion people worldwide, ScamAdviser turns data into decisive action—so you can stay safe, stay ahead, and stay in control.

Confronting a US$2 Billion Scam Crisis

According to the 2025 Global State of Scams report, 72% of Taiwanese adults encountered scams last year, facing an average of one attempt every two days. With 61% falling victim and total losses reaching US$2 billion in the last year. 13% of Taiwanese adults claim to have lost money to scams in the last 12 months with $23276.3 lost to scams, per person, on average. These figures paint a picture that scams have become a daily threat, putting the personal and financial security of individuals, families, and businesses at risk.

A Threat Across Generations and Channels

Scams in Taiwan are evolving rapidly. Investment scams remain the most common, but impersonation, online shopping, and employment scams are rising fast. These scammers' attacks thrive on direct communication channels, especially social platforms such as Facebook and Instagram, where scam rates are highest.

Gen Z and suburban communities are among the most impacted. Many victims report taking more than a day to realize they had been scammed, giving fraudsters a dangerous head start. Alarmingly, 43% of Taiwanese parents with children aged 7 to 17 report that at least one of their children has been targeted by a scam. Even more troubling, 45% of victims say no action was taken after they reported the scam, deepening public confusion and frustration.

Scams is seen as National Challenge

While 39% of Taiwanese adults expect government agencies to take the lead, most also turned to banks, telecoms, and platforms as the most effective in actual scam prevention. At the same time, 40% of adults admit to committing acts deemed as fraudulent, showing just how difficult scam is to identify, revealing the deeper cultural and systemic challenges of scam prevention.

Our Approach: Data, Technology, and Partnerships in Sync

ScamAdviser sees scam prevention as a shared responsibility, one that demands awareness from individuals, coordinated action from institutions through the right tools and technology, and strong leadership from governments as trusted authority holders. Our mission is bold but clear: make scams unscalable by making defenses smarter, faster, and interconnected.

We work with the Taiwan government and financial institutions to track and remove fake ads and impersonation content. We also empower telecoms and software platforms to detect and harmful links, suspicious numbers, and impersonation attempts. Our Anti-Scam Intelligence (ASI) and Impersonation solution are purpose-built to work together with partners, to protect brands and users at scale.

Facing the Scam Pandemic: Taiwan's Collective Fight Against Digital Scam



Michelle Shen
DIRECTOR OF
PRODUCT OPERATION

whoscall

About whoscall

Whoscall, powered by Gogolook, is a cutting-edge digital anti-scam tool designed to protect users from scams across various channels, including phone calls, text messages, social media, and links. With over 100 million downloads globally, it features the most comprehensive database in East and Southeast Asia, covering more than 2.6 billion phone numbers.

In Taiwan, the scale and sophistication of scams have escalated at an alarming rate. Every month, tens of thousands of citizens fall victim to various forms of fraud, from phone impersonation and phishing texts to investment scams disguised under the guise of government agencies or well-known brands. In 2024 alone, scam losses in Taiwan exceeded US $ 1.7 billion, a sharp reminder of how pervasive and damaging this problem has become.

Scam Landscape in Taiwan: SMS Fraud Still Dominates

According to Whoscall 2024 Annual Report, SMS scams remain the most prevalent in Taiwan, accounting for nearly 90% of all scam attempts, with loan-related scam making up 80% of those messages. The most common types of scams include loan scams, romance or relationship scams and impersonation scams. These scams continue to exploit the convenience and speed of digital communication to deceive individuals at scale.

One Unified Scam-Checking System: Whoscall "Check"

To help users fight scams more proactively, Whoscall launched a unified scam-checking system called "Check" in 2024, a key step toward simplifying user protection. With just one interface, users can now screenshot a suspicious message, check unknown phone numbers, or verify the safety of suspicious URLs, all within the Whoscall app. This allows for real-time scam detection, regardless of the scam's form or entry point. This feature empowers users to act quickly and confidently when facing potential threats, eliminating the need to rely on fragmented information or separate tools.

A Whole-of-Society Defense Against Scams

While these initiatives represent significant progress, we believe there is more to be done. Scam prevention must evolve from reactive responses to proactive infrastructure. We call on industry leaders, platforms, and policymakers to embrace trust-by-design, improve cross-border data sharing, and mandate clearer identity verification in digital interactions.

At Whoscall, we believe fighting scams requires a coordinated, whole-of-society approach. That's why we've continued to work closely with Taiwan's Criminal Investigation Bureau (CIB), the Ministry of Digital Affairs, financial, telecom companies, and other key public and private stakeholders to deliver technology-based protection at scale.

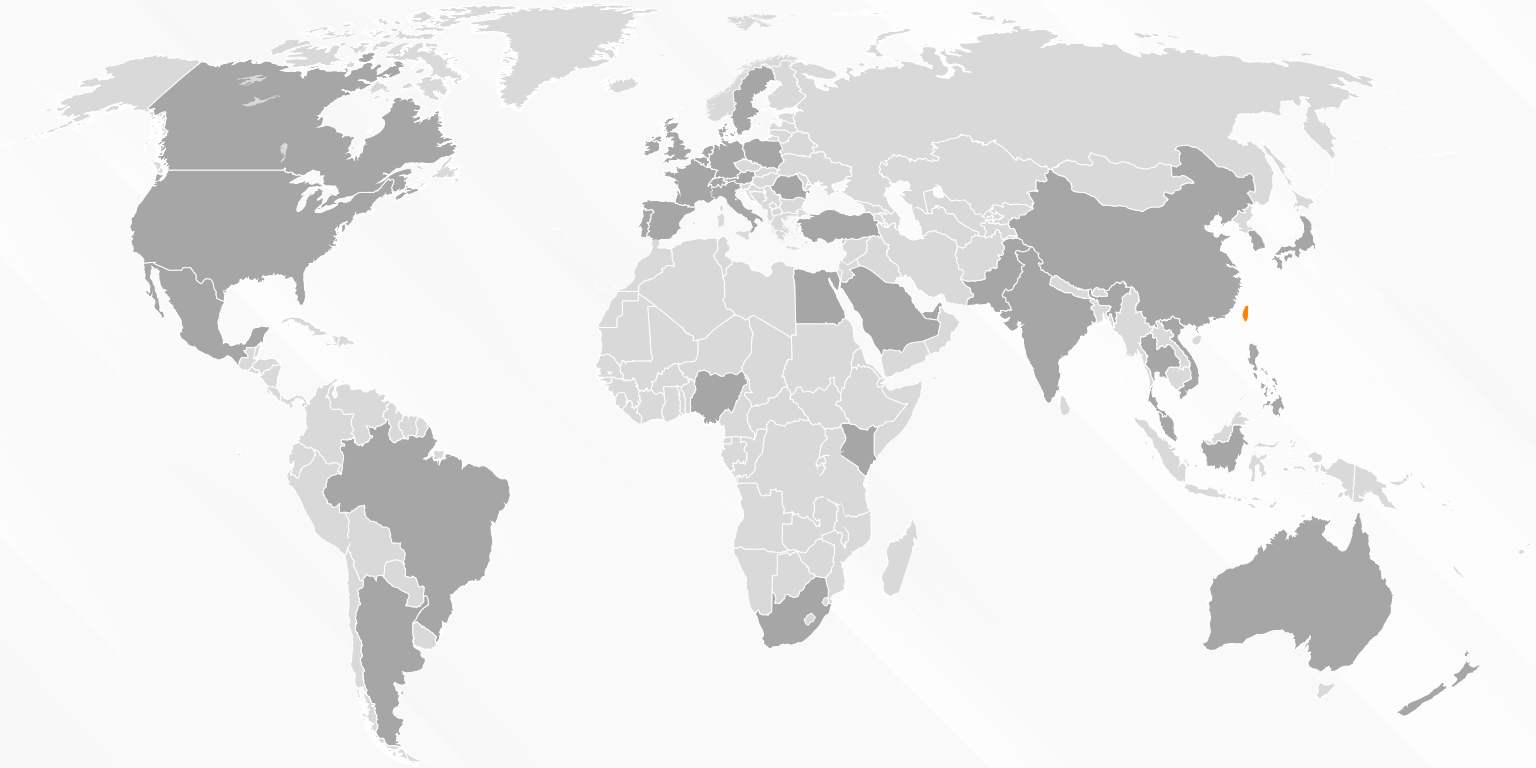
Ultimately, protecting consumers in the age of AI-driven scam requires not only awareness and enforcement, but also easy-to-access, intuitive tools that empower every individual. At Whoscall, we remain committed to staying one step ahead of scammers and building a safer digital environment for everyone in Taiwan.

The Global research surveyed over 46,000 respondents across 42 markets

MARKETS

Argentina
Australia
Austria
Belgium
Brazil
Canada
China
Denmark
Egypt
France
Germany
Hong Kong
India
Indonesia
Ireland
Italy
Japan
Kenya
Malaysia
Mexico
Netherlands
New Zealand
Nigeria
Pakistan
Philippines
Poland
Portugal
Romania
Saudi Arabia
Singapore
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Türkiye
UAE
United States
Vietnam

The data in this report will focus on findings within **Taiwan**



Who we spoke to in Taiwan

Sample size | 1,000 people

Audience | Adults aged 18+ living in Taiwan

Weighting | Nationally representative of Taiwanese adult population

Methodology | 15-minute online survey

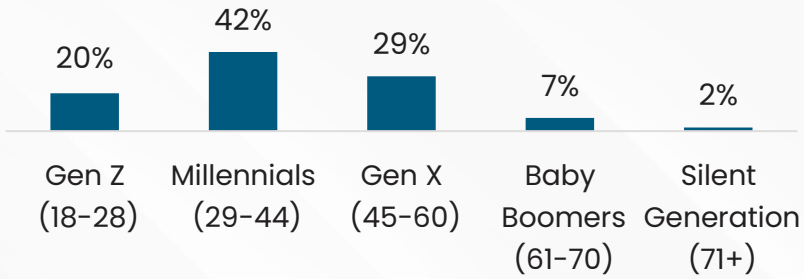
Sample source | Online research panel

Fieldwork | 26th February – 14th March 2025

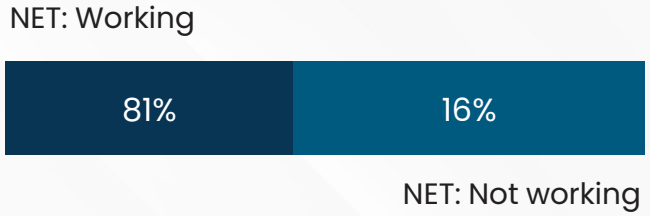
GENDER



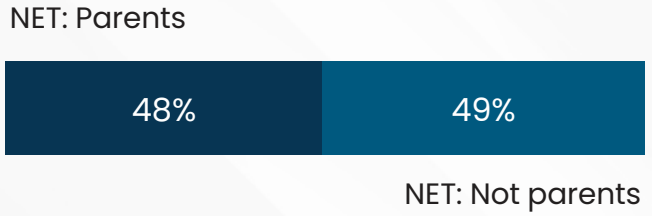
GENERATION / AGE



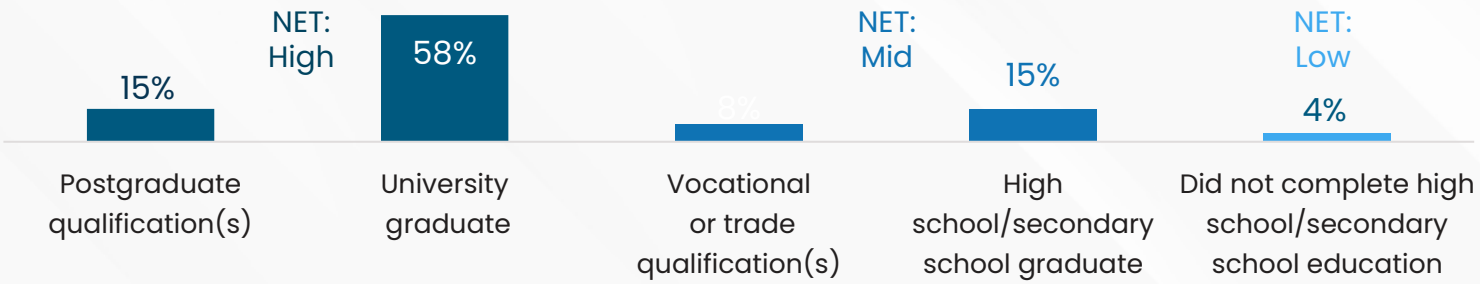
WORKING STATUS



PARENTAL STATUS



EDUCATIONAL STATUS



Base: All respondents Taiwan (1000)

Key Taiwan findings

PREVALENCE OF ENCOUNTERING A SCAM

72%

Of **Taiwanese** adults claim to have **encountered** a scam

Scams are most commonly encountered on a **weekly** basis, which equates to **149 scam encounters** on average per person, per year, in Taiwan

PREVALENCE OF EXPERIENCING* A SCAM IN LAST 12 MONTHS

61%

Of **Taiwanese** adults claim to have **been scammed** in the last 12 months

Amongst this group, an **Investment scam** (65%) is the most common type of scam experienced

*An experience, whether successful or not for the scammer

PREVALENCE OF LOSING MONEY TO A SCAM IN LAST 12 MONTHS

13%

of **Taiwanese** adults claim to have **lost money to scams** in the last 12 months with **$23276.3** lost to scams, per person, on average

Funds are most commonly sent via **wire bank transfer** (**32%**), cash, and gift cards (both **17%**)

PERCEIVED RESPONSIBILITY TO PROTECT PEOPLE FROM SCAMS

39%

Of **Taiwanese** adults feel it is the responsibility of **Public service organisations** to keep people safe from scammers, primarily the government (**26%**)

IMPACT OF SCAMS ON VICITM

52%

Of **Taiwanese** adults who were scammed felt very or somewhat stressed by the experience

28% say they will be more vigilant of scams as a result

PREVALENCE AND OUTCOME OF REPORTING TO PAYMENT PROVIDER

85%

Of **Taiwanese** adults who were scammed did report the scam to the payment service

38% were able to at least partly recover the money

The research covered four key topics

You can navigate through pages and sections of this report using the clickable icons in the navigation bar at the base of each slide.

Use the button to return to this page.

Click to navigate through sections

SCAM ENCOUNTERS

Uncovering the frequency of encountering scams, the platforms and channels used by scammers and the prevalence, barriers and outcomes of reporting scam encounters

EXPERIENCING SCAMS

Understanding the most common scams, value lost, and the prevalence, barriers, and outcomes of reporting them

IMPACT OF SCAMS

Exploring the reasons why scams are experienced as well as the impact on wellbeing and future actions of the victim

SCAM PREVENTION

Examining consumers' self-prevention tactics and perceptions of public and commercial organisations' roles in preventing and resolving scams

To find out more about the report and its authors:

ABOUT THE REPORT

ABOUT THE AUTHORS



SCAM ENCOUNTERS

Uncovering the frequency of encountering scams, the platforms and channels used by scammers and the prevalence, barriers and outcomes of reporting scam encounters

Almost three quarters of Taiwanese adults are confident they can recognise scams, with 15% claiming that they can "always recognise a scam"

Confidence in recognising scams

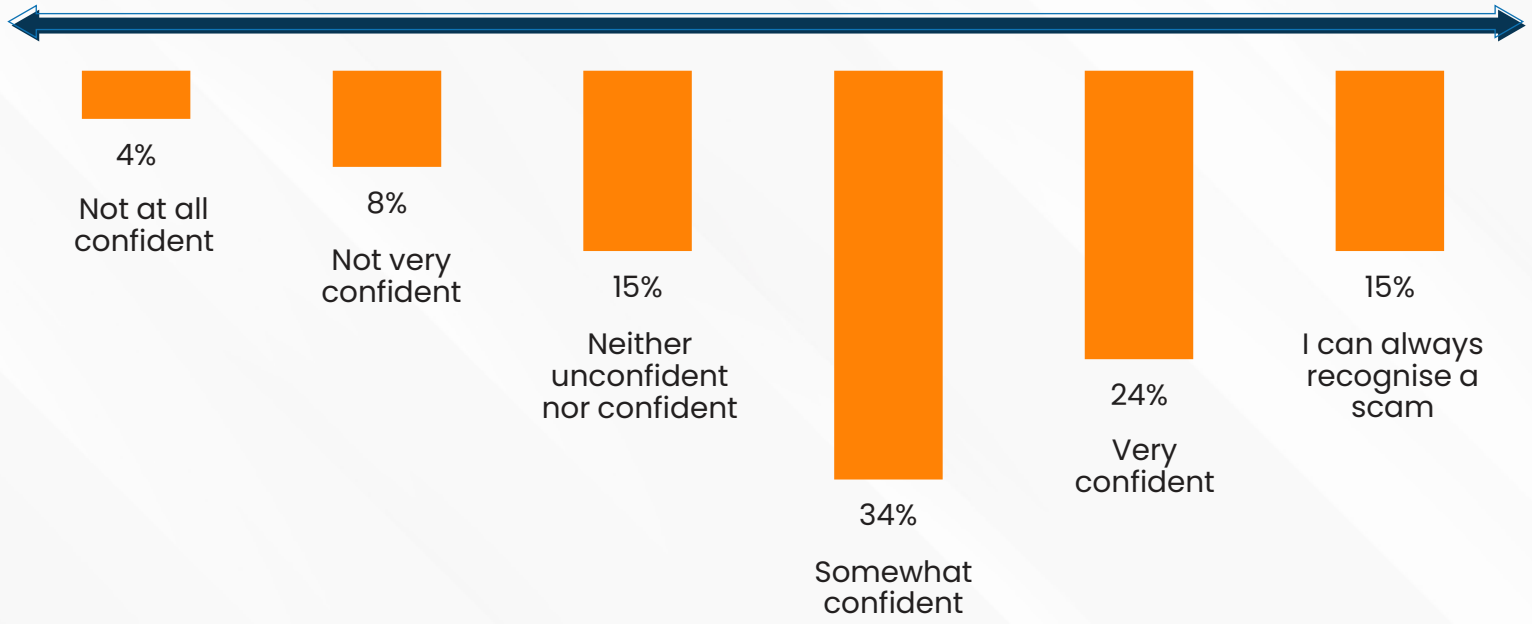
In Taiwan, Millennials (**77%**), Men (**79%**), those living in urban areas (**78%**), those with high education (**79%**), and parents (**76%**) are more likely to say they feel confident in their ability to recognise scams. Meanwhile those living in suburban areas (**22%**), those with mid education (**17%**), and non-parents (**16%**) are more likely to feel unconfident

13%

Do **not feel confident** in their ability to recognise scams

73%

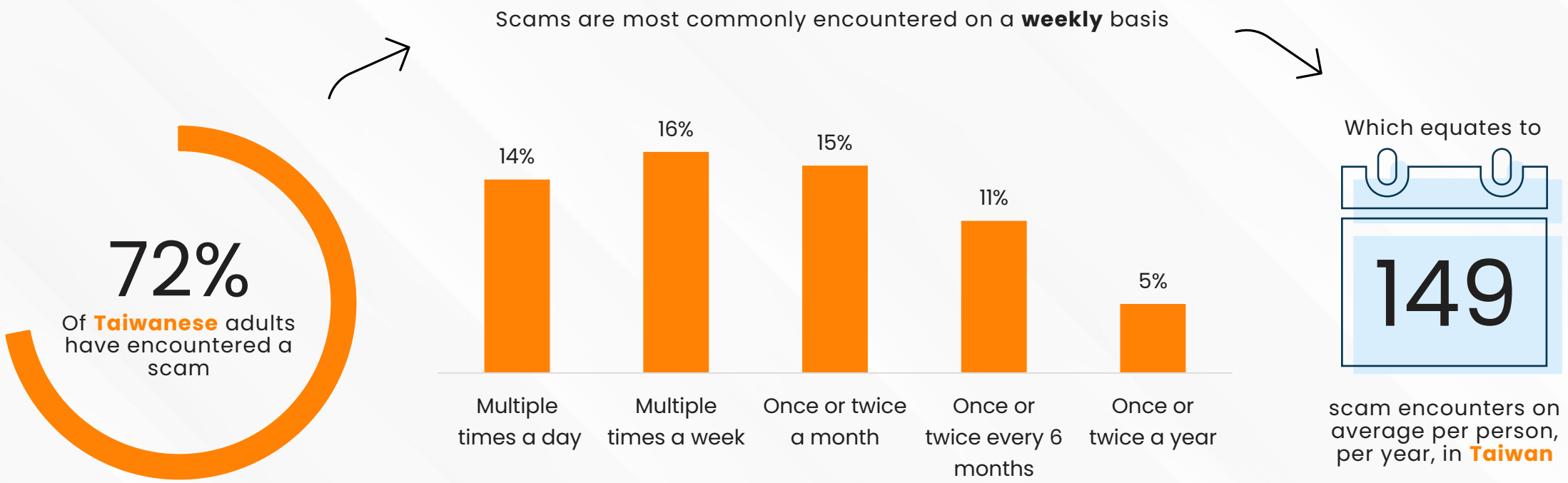
Do **feel confident** in their ability to recognise scams



Q1. How confident are you that you can recognise scams? Base: All respondents Taiwan (1000)

Almost three quarters of Taiwanese adults say they have encountered a scam, with an average of one scam encounter happening every two days

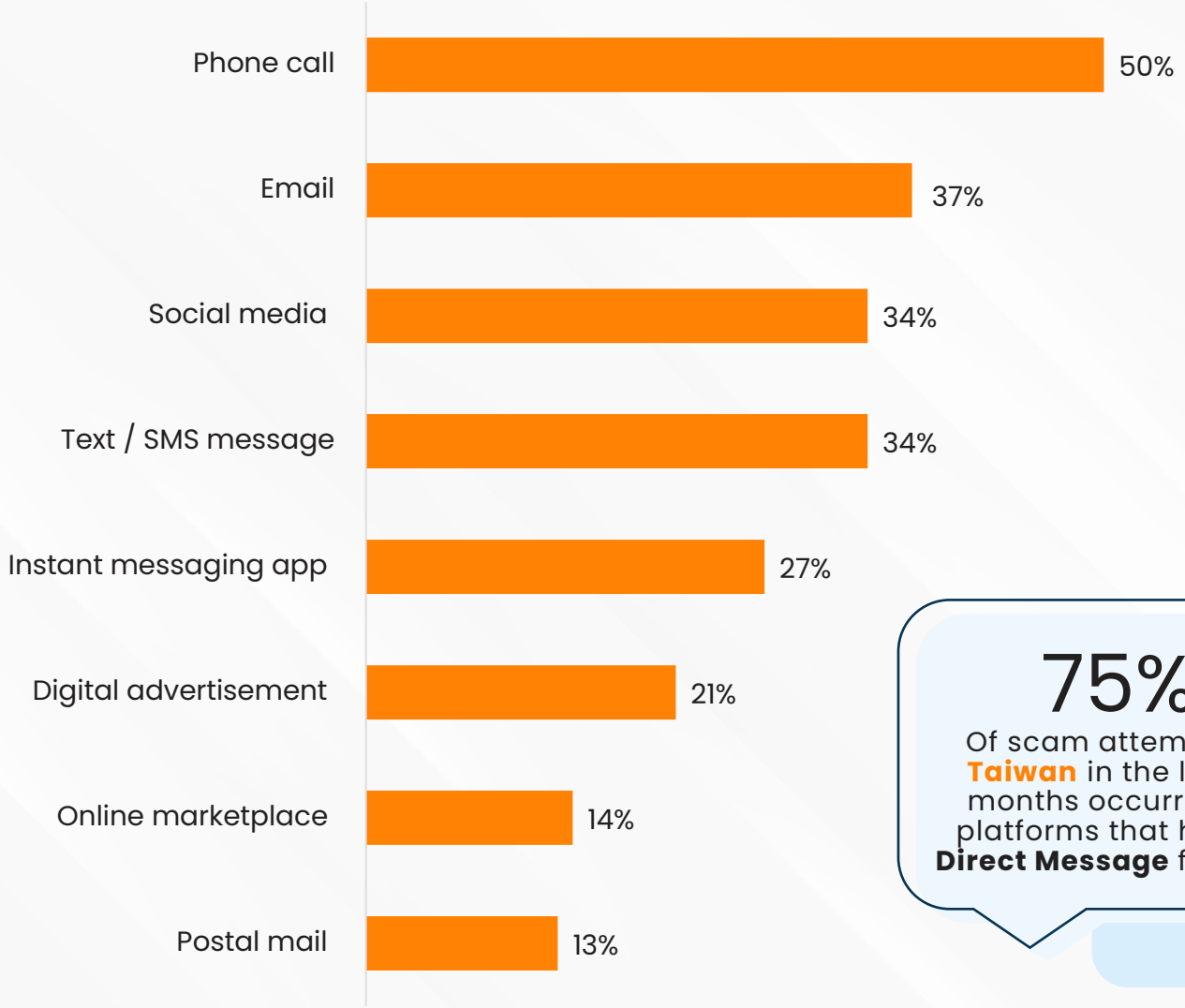
Prevalence & frequency of encountering a scam



Q2. How often, if ever, are you exposed to attempts to scam you? Base: All respondents Taiwan (1000)

Most of the scam encounters in Taiwan happen on platforms that have a Direct Message functionality, primarily Email, Social media, and Text message

Channels used by scammers – top 8



75%

Of scam attempts in **Taiwan** in the last 12 months occurred on platforms that have a **Direct Message** function

Q3. Through which communication channel(s) did scammers approach you in the last 12 months? Base: All respondents Taiwan who have been exposed to a scam attempt (618)

Facebook and Instagram are the top platforms where scam encounters occur

Top 10 online platforms used by scammers in last 12 months in Taiwan



52%



42%



38%



17%



16%



15%



13%



11%



10%



4%

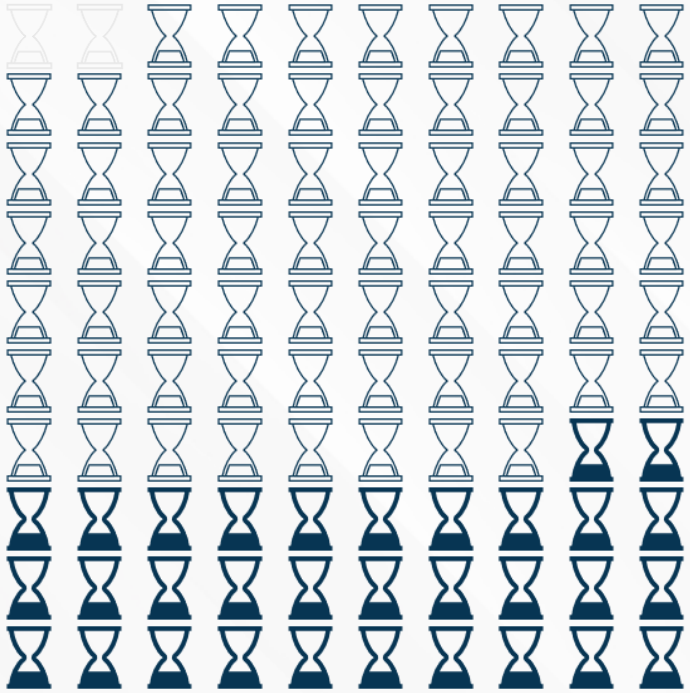
Q4A. Through which, if any, of the following global service or platform(s) did scammers contact you in the last 12 months? Base: All respondents in Taiwan who have been exposed to a scam attempt (618)

Two in five Gen Zs who experienced a scam encounter took longer than a day to recognise it was deceitful

Time taken to realise a scam encounter

66%

Said it took less than a day to realise someone was trying to scam them



However, for 32% it took a day or longer to realise...

Those in **Taiwan** who take longer to recognise a scam are more likely to be...

Gen Z (40%)

Those living in suburban areas (42%)

Those with mid education (42%)

Those approached by a scammer on:

TikTok (49%)
X (Twitter) (43%)

Q11. When a scammer approached you on , how long did it take you to realise they were trying to scam you? Base: All Taiwan respondents who have been contacted by a scammer on a platform (591)

TikTok, WeChat, and X (Twitter) are platforms where it takes the longest to recognise a scam

Time taken to recognise a scam encounter, by top 10 platforms

Key = | Under index vs average | Over index vs average

		Average across all platforms	WhatsApp	Instagram	WeChat	TikTok	Telegram	X (Twitter)	Facebook	Gmail	Outlook Email
Less than a day	Seconds	19%	22%	15%	10%	5%	14%	14%	17%	18%	24%
	Minutes	33%	36%	34%	34%	25%	29%	28%	38%	35%	43%
	Hours	14%	12%	16%	16%	20%	21%	14%	14%	15%	14%
A day or longer	Days	14%	9%	17%	21%	17%	19%	24%	14%	16%	8%
	Weeks	10%	10%	11%	15%	11%	6%	14%	9%	11%	7%
	Months	5%	5%	3%	2%	17%	7%	3%	3%	3%	2%
	About a year	1%	2%	1%	0%	2%	2%	3%	1%	0%	0%
	More than a year	1%	0%	0%	3%	1%	0%	0%	0%	0%	0%

Q11. When a scammer approached you on [platform allocated] , how long did it take you to realise they were trying to scam you? Base: All Taiwan respondents who have been contacted by a scammer on WhatsApp (100), Instagram (261), WeChat (68), TikTok (99), Telegram (83), X (Twitter) (99)), Facebook* (332), Gmail (250), Outlook Email (77). * Includes both Facebook and Facebook messenger

More than seven in ten of those encountering a scam have reported it at least once

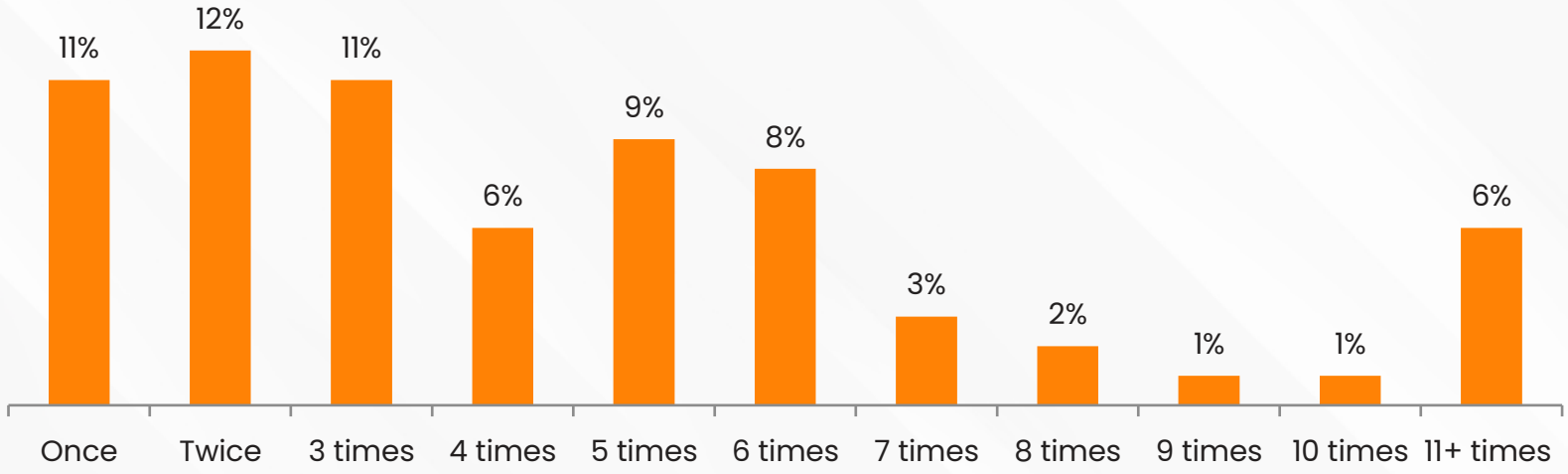
72%

Of those who have been exposed to scams in **Taiwan** **have reported a scam encounter in the last 12 months**

Higher amongst Gen Z (**86%**) and those who are parents (**75%**)

Frequency of reporting a scam encounter in the last 12 months

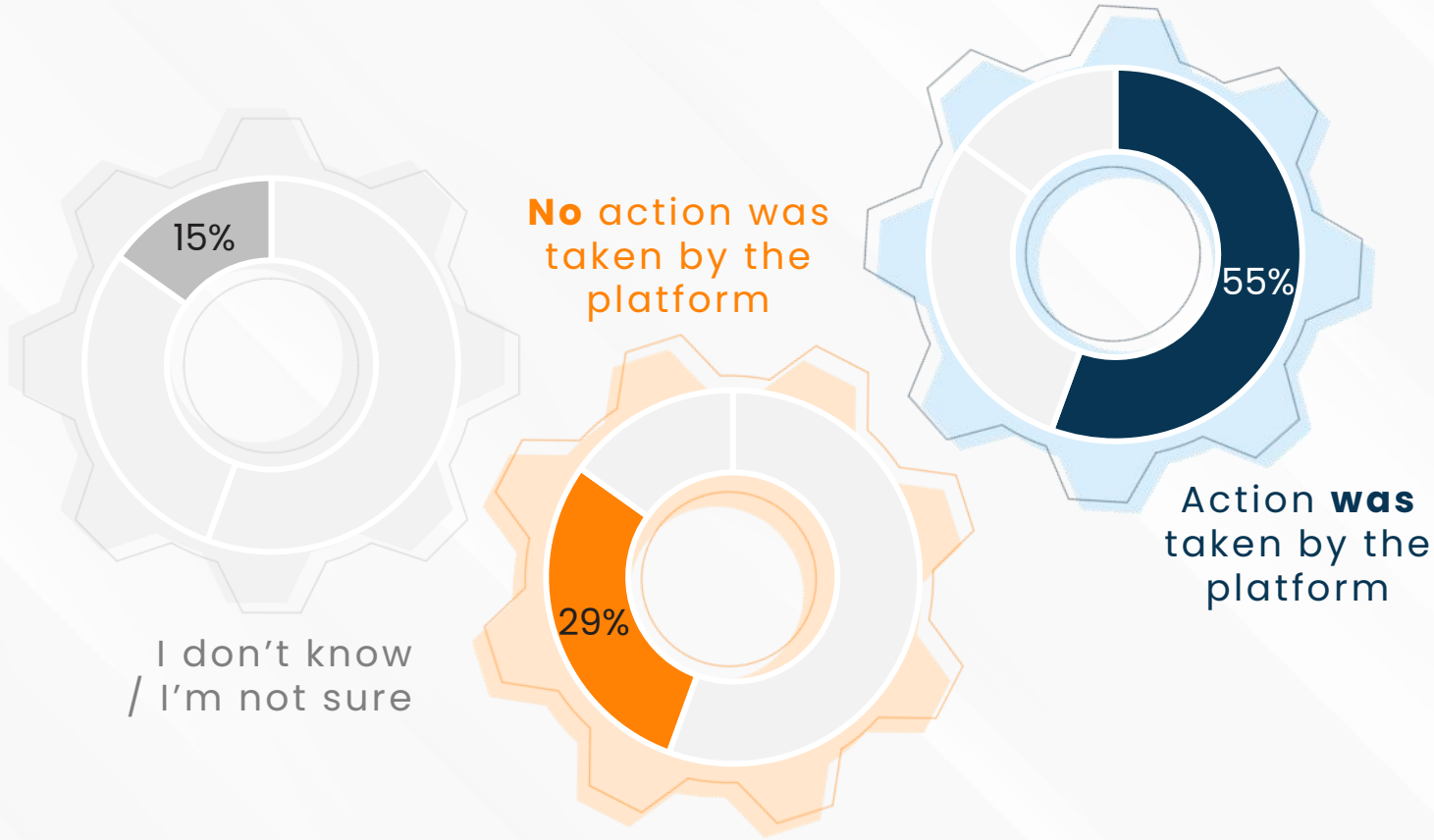
Each person has **reported** 3.2 scam encounters on average, **in the last year, in Taiwan**



Q5. How many times, if any, have you reported a scam attempt to the service or platform provider where you experienced the scam attempt in the last 12 months?
Base: All respondents in Taiwan who have been exposed to a scam attempt (608)

Three in ten say no action was taken by the platform when they reported the scam encounter

Outcome of reporting scam encounter to platform / service provider



45%

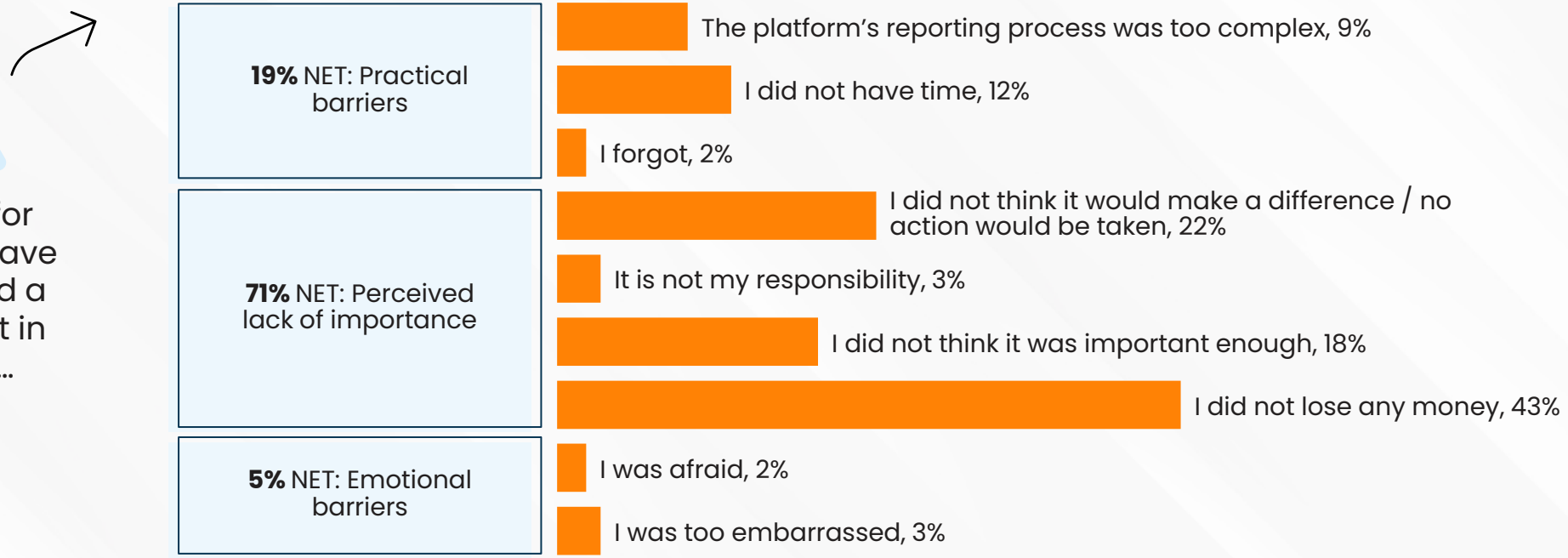
Of those reporting a scam in the last 12 months in **Taiwan** say that either **no action was taken (29%) or they aren't sure what the outcome was (15%)**

Q6. What happened when you reported the scam attempt to the platform or service provider? Base: All respondents in Taiwan who have reported a scam attempt in the last 12 months (439)

Not losing any money is the main reason scam encounters don't get reported

Barriers to reporting scam encounters

The barriers for the **26%** who have never reported a scam attempt in **Taiwan** are...



Q7. Why haven't you reported any scam attempts to service or platform providers in the last 12 months? Base: All respondents in Taiwan who have not reported scam attempts (151)



EXPERIENCING SCAMS

Understanding the most common scams, value lost, and the prevalence, barriers, and outcomes of reporting them

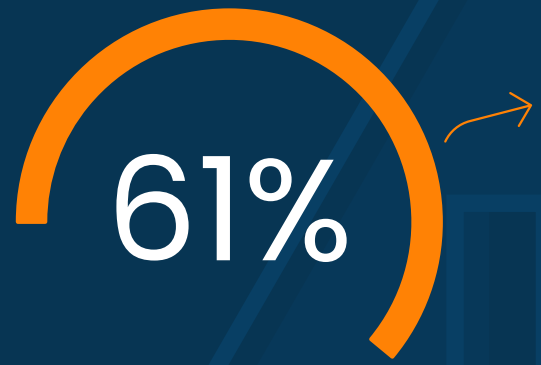
GASA Global Anti-Scam Alliance

SCAMADVISER

whoscall

Three fifths of Taiwanese adults have been scammed in the last 12 months

Prevalence of experiencing a scam in last 12 months



of **Taiwanese** adults claim to have been scammed in the last 12 months

With each **Taiwanese** scam victim being scammed on average

2.4

times

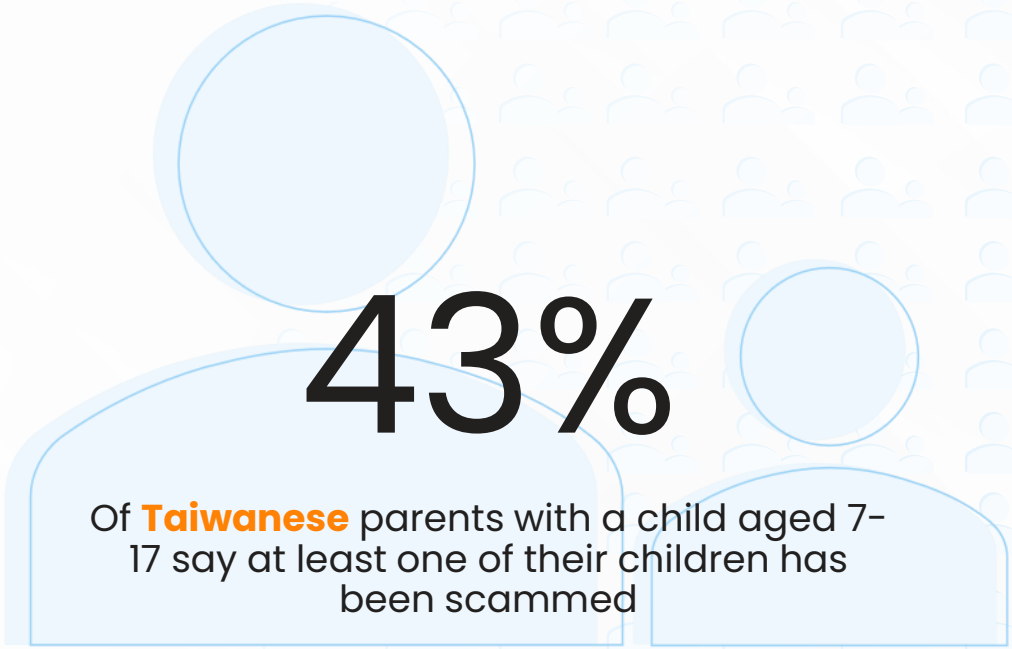
Those most likely to have experienced a scam are...

Men	**69%**	Those living in an urban area	**63%**
High level of education	**64%**	Parents	**72%**
Those who are confident in their ability to recognise a scam	**65%**		

Q8. Have any of the following scams happened to you in the last 12 months? Base: Rebased to all Taiwan respondents (1000)

And just over two fifths of parents say their children have experienced at least one scam too

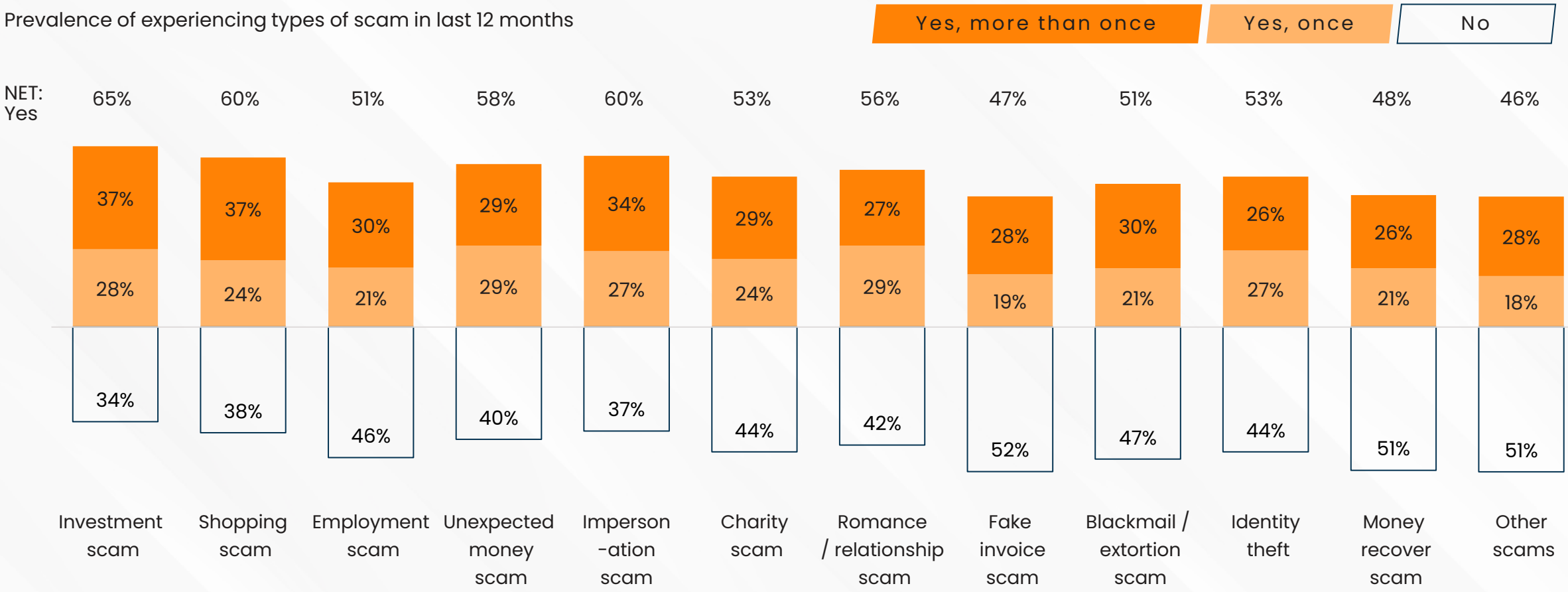
Proportion of parents reporting scam experiences amongst their children



Q23. Have any of your children between the age of 7-17 been scammed? Base: All Taiwan respondents who have children aged 7-17 (196)

Investment scams are the most experienced type of scam in Taiwan, affecting almost two thirds of those targeted

Prevalence of experiencing types of scam in last 12 months



Q8. Have any of the following scams happened to you in the last 12 months? Base: All Taiwan respondents who have been contacted by scammers (618)

Click here to review full scam descriptions seen by respondents within the survey

With some having money stolen via investment and romance scams

Scam victim description of experience

The foreign girl who was dated on Tinder with fake photos requested payment of relevant fees on the grounds that her family wanted to immigrate to my country.
Romance scam

I received a message to participate in a lottery, so I provided my personal information to participate. Then I received a winning message, and then I got a call saying that I had to pay a handling fee of 2,000 yuan before I could receive a TV worth 50,000 yuan. At this time, I realized it was a scam.
Unexpected money scam

They tricked me into passing customs duties under the guise of asking me to order and receive goods that have been cleared by customs.
Impersonation scam

I was defrauded of 1 million in investments.
Investment scam

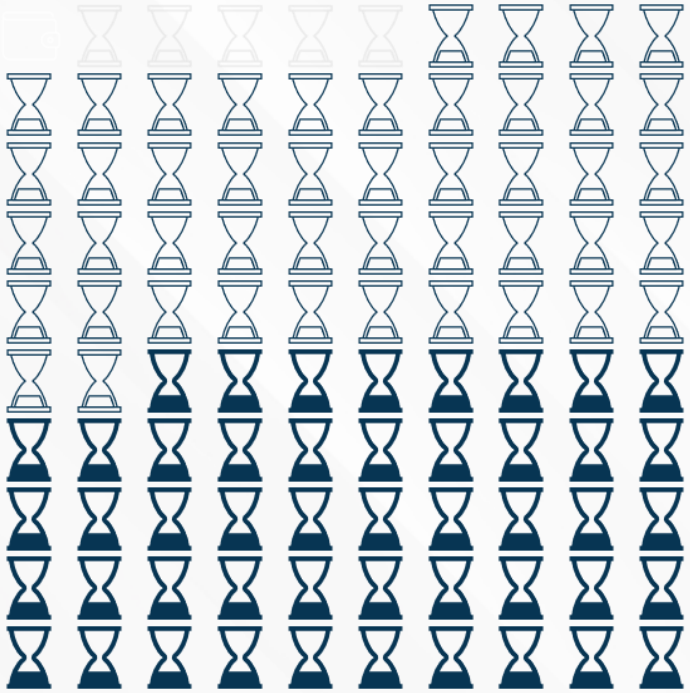
Q9. Please describe the scam you experienced in the last twelve months. Base: All Taiwan respondents who have been scammed (614)

For almost half of Taiwanese adults scammed, it lasted longer than a day

Length of scam

46%

Said it the scam lasted for less than one day



However, for 48% the scam lasted for longer than a day

Those in **Taiwan** whose scams lasted longer than a day are more likely to be…

Gen Z (56%)

Those living in suburban areas (56%)

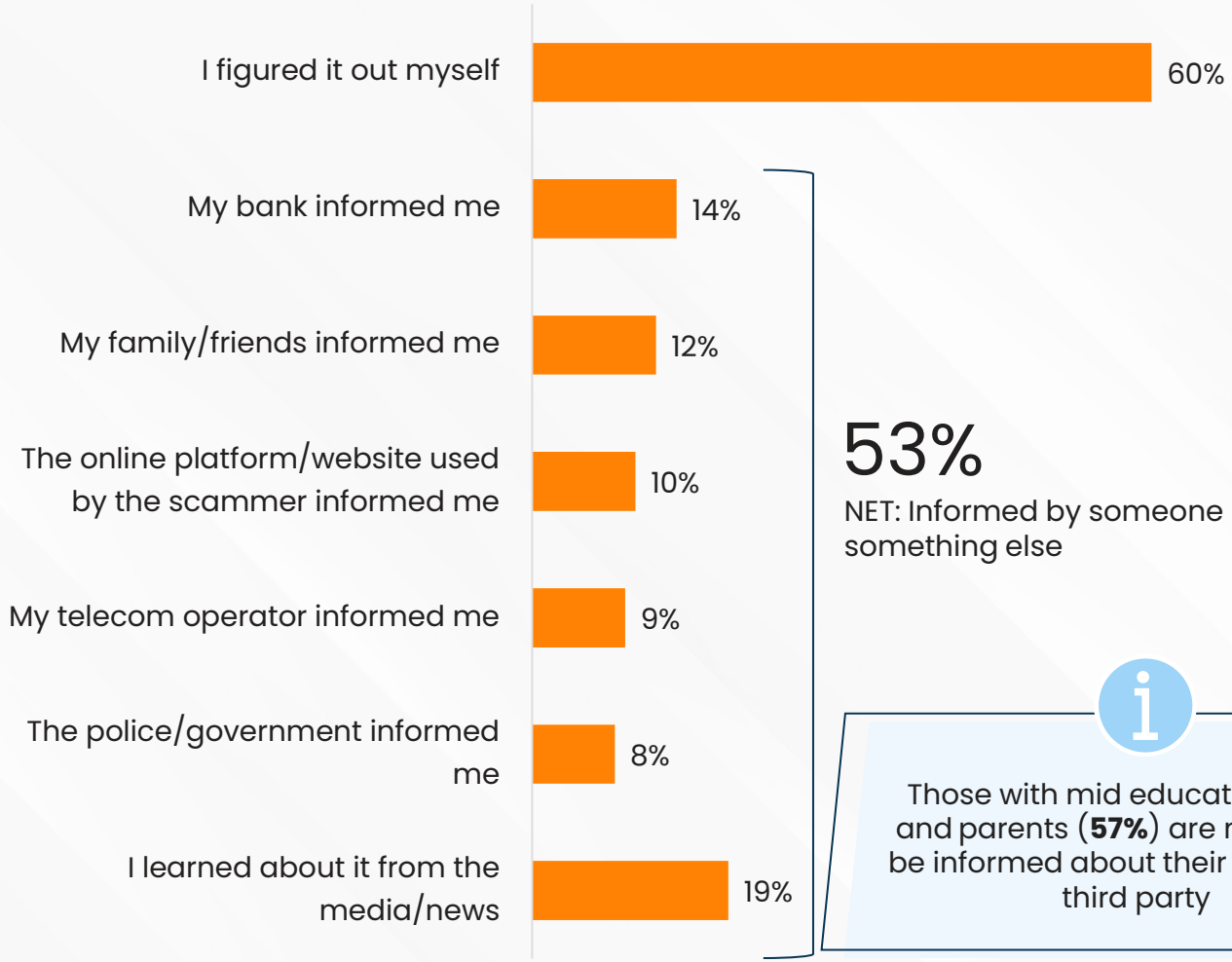
Those with mid education (58%)

Click here to see length breakdown by scam type

Q10. Thinking about the most recent time you were scammed, how long did it last? Base: All Taiwan respondents who have scammed (614)

Three fifths of scam victims realised they had been scammed by figuring it out for themselves

How victim discovered they were scammed



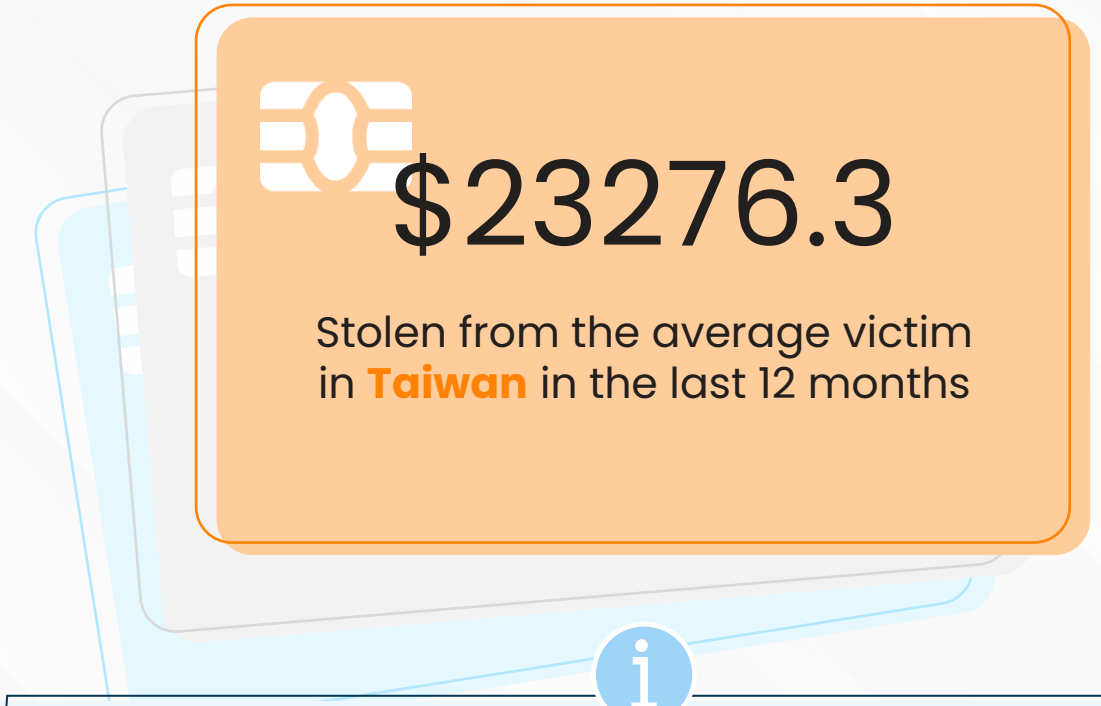
Those with mid education (**63**%) and parents (**57%**) are more likely be informed about their scam by a third party

Q12. How did you discover you were scammed? Base: All Taiwan respondents who have scammed (614)

$62.9 billion (US$2 billion) has been stolen by scammers in Taiwan in the last year

Value lost to scams

13% of **Taiwanese** adults claim to have lost money to scams in the last 12 months



$23276.3

Stolen from the average victim in **Taiwan** in the last 12 months

US$750.84

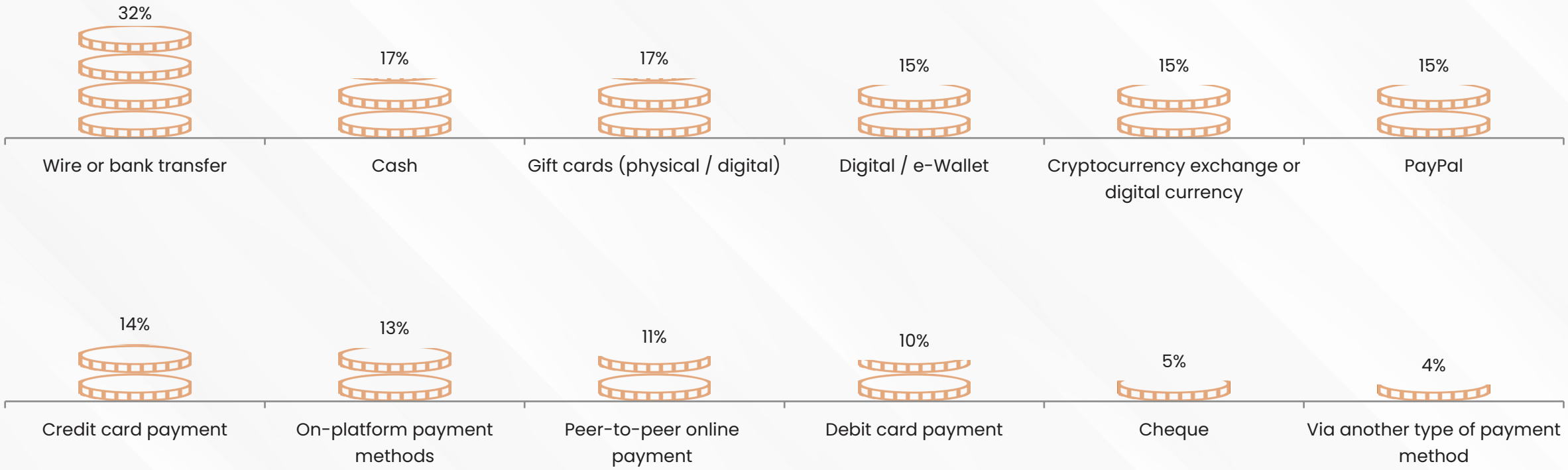
Click here to see conversion rate & calculation used

Gen X tend to have more stolen on average (**$41959.5**) vs Gen Z (**$1438.4**). Those who 'can always recognise a scam' have had **$5059.4** stolen on average in the last year in Taiwan

Q13. In the last 12 months, in total, how much money did you lose to scams? Please include the total amount of money lost, regardless whether you managed to partially or fully recover it. Base: All respondents Taiwan (1000)

With wire or bank transfer, cash, and gift cards being the most common methods of transferring the money

Payment channels scammers received the payment



Q14. How did the scammer receive your money? Base: All Taiwan respondents who have been scammed and lost money (142)

More than four in five reported their scam to the payment service, and almost two fifths said their money was at least partially recovered

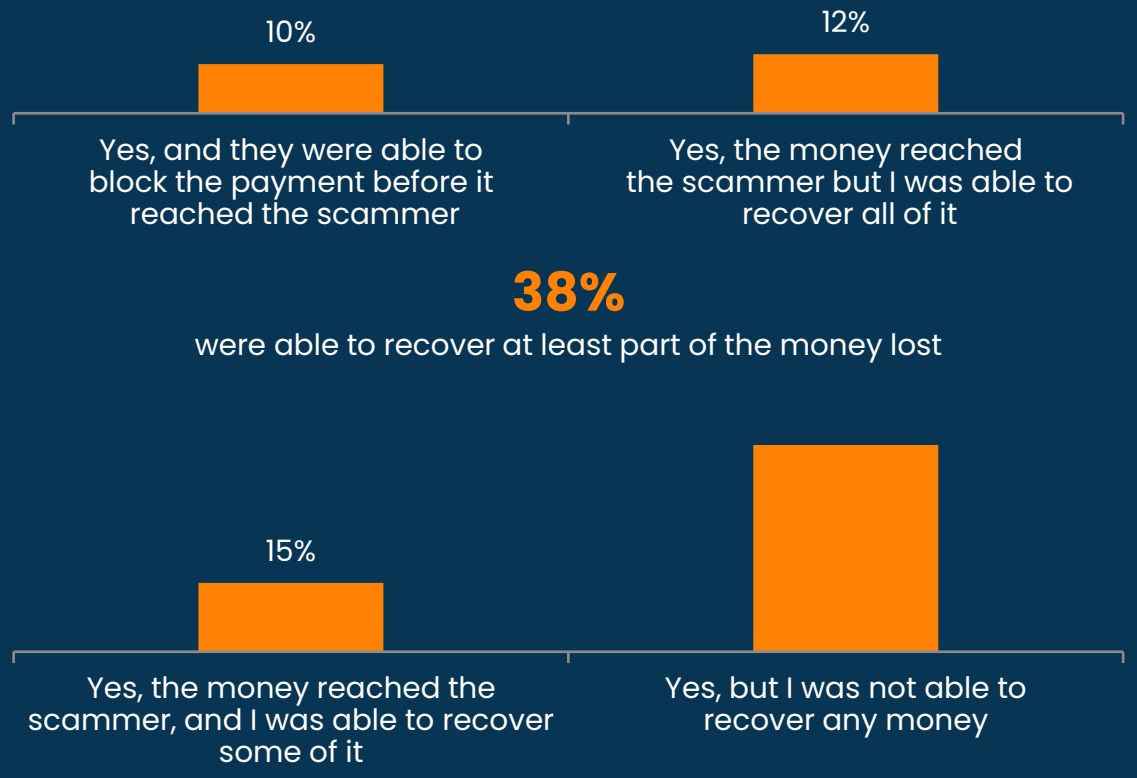
Did you report the scam to the payment service?



15%
Did not report the scam to the payment service

85%
Did report the scam to the payment service

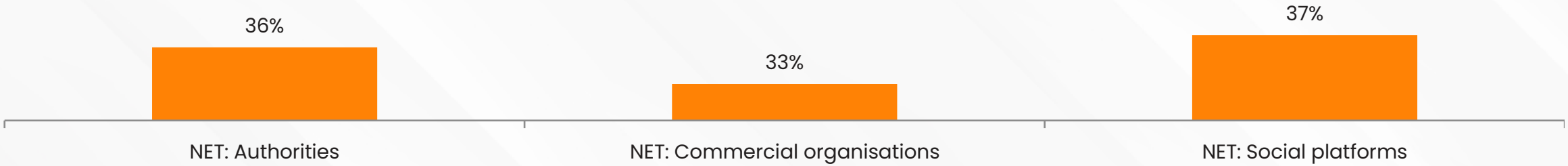
Recovery outcome



Q15. Did you report the scam to the payment service that was used to send your money to the scammer? Base: All Taiwan respondents who have been scammed and lost money (142)

Scams were more likely to be reported to social platforms than they were authorities

Channels / organisations scams reported to – top 10



National reporting website	11%	E-commerce / marketplace	6%	Family and Friends	19%
Local or national Police	20%	Internet service provider or hosting company	11%	Online review site	11%
Consumer protection authority or organization	9%	Financial institutions	13%	Social platform	15%
Financial protection authority	7%	Cryptocurrency exchange	5%		
		Telecom / mobile operator	8%		

Q21. Who did you report the scam to? Base: All Taiwan respondents who have been scammed (614)

Thinking their reports would not make a difference was the main reason for not reporting encounters

Barriers to reporting scams

19%

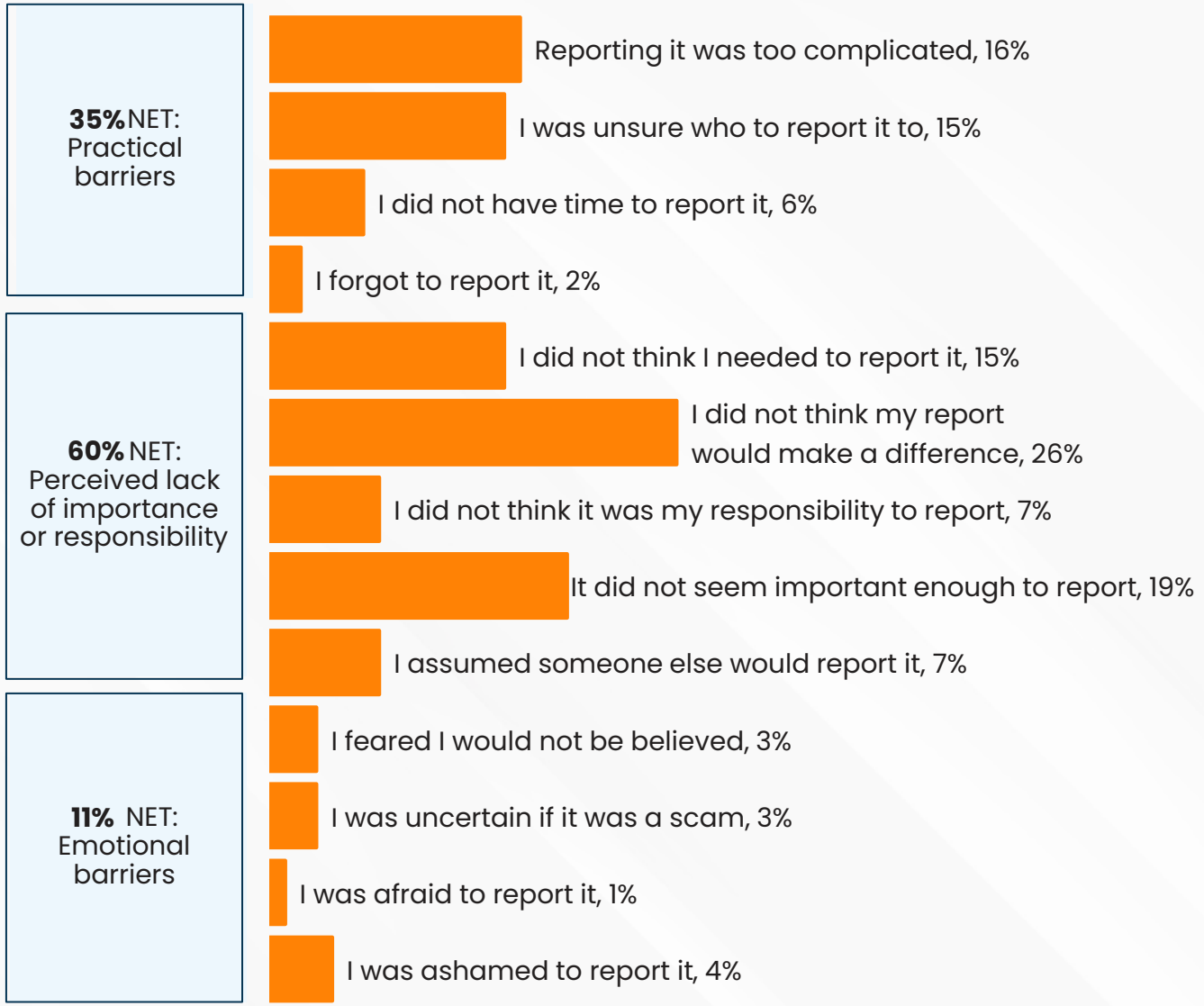
Of those experiencing a scam in the last 12 months in **Taiwan** did not report it

11%

Say there was no reason for them not to report the scam

26%

Did not think their report would make a difference



Q21. Who did you report the scam to? Base: All Taiwan respondents who have been scammed (614) Q22. Why didn't you report the scam? Base: All Taiwan respondents who did not report the scam they experienced (117)

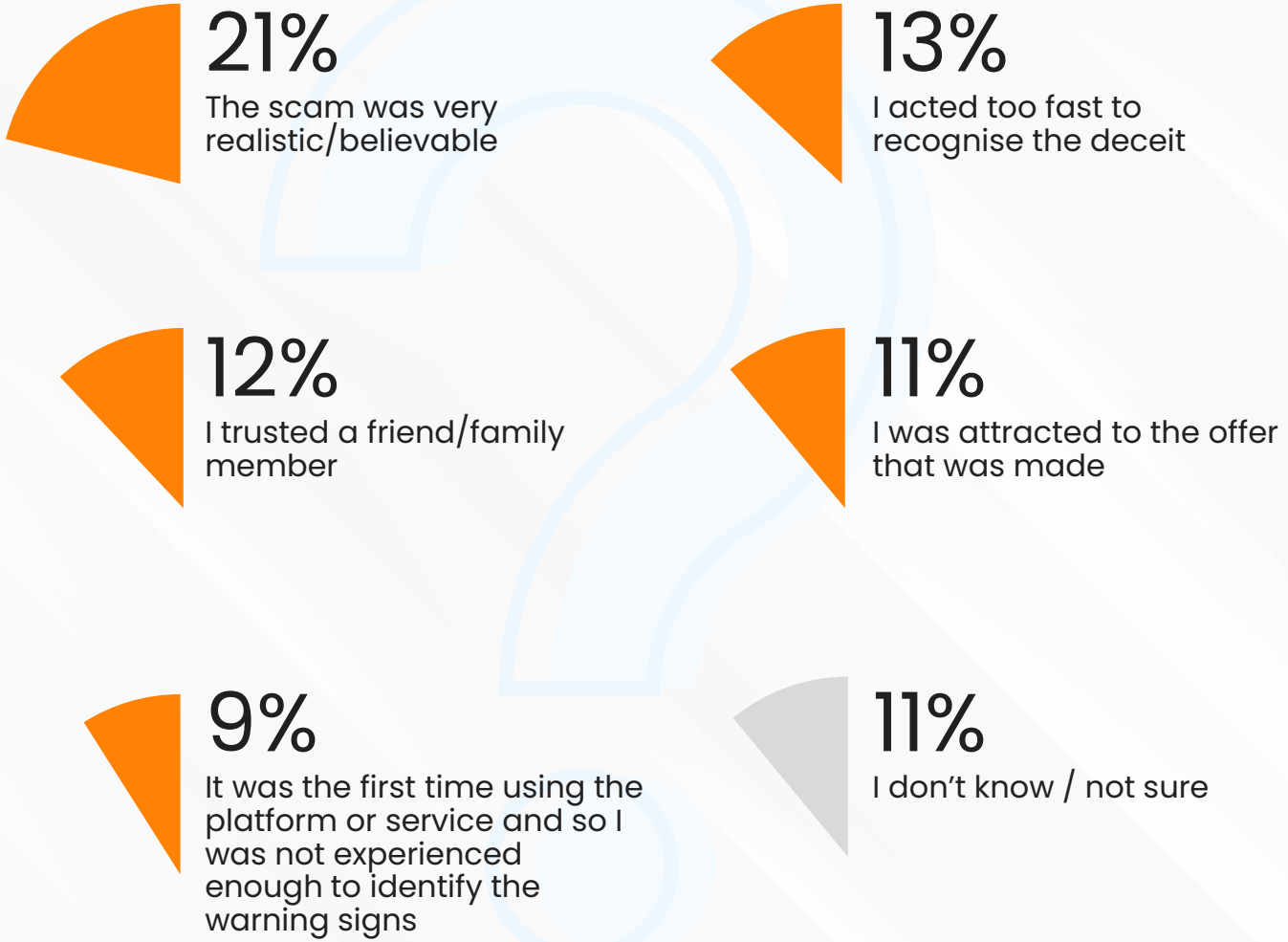


IMPACT OF SCAMS

Exploring the reasons why scams are experienced as well as the impact on wellbeing and future actions of the victim

The believability of the scam is the main reason why Taiwanese victims think they were scammed

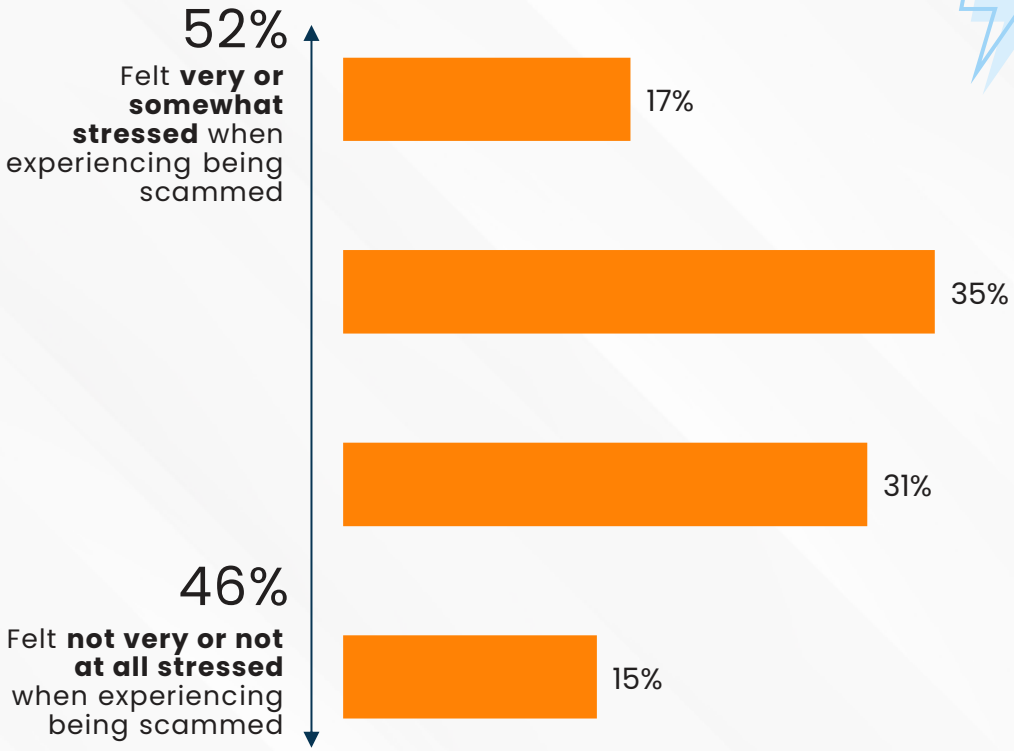
Reasons why scams experienced – top 5



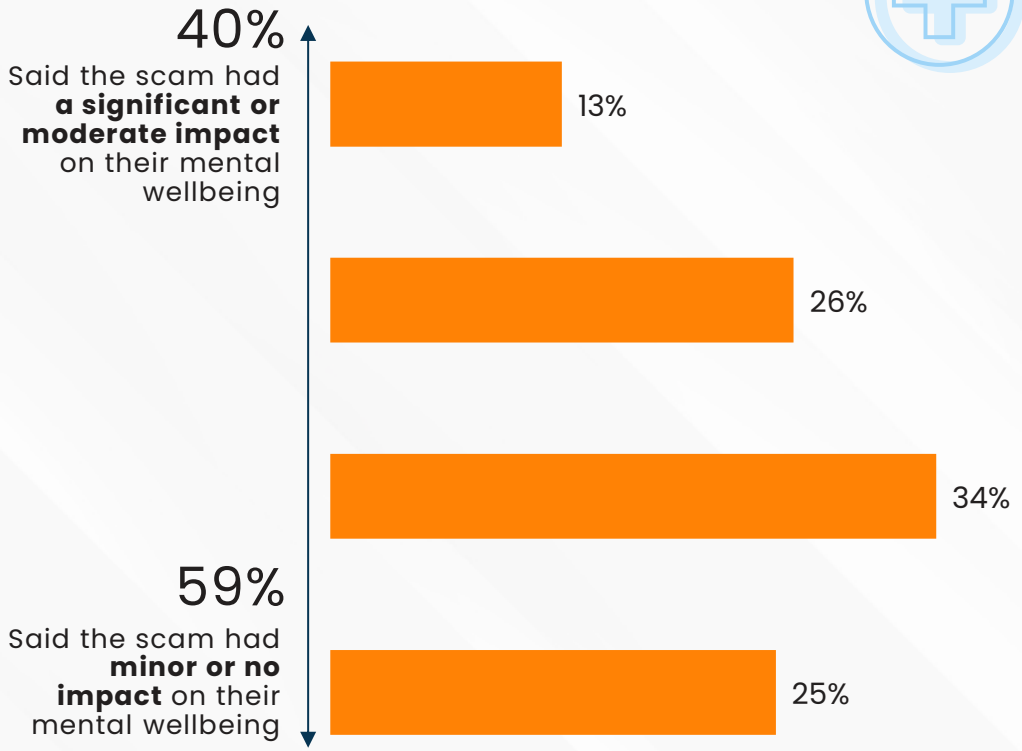
Q19. Why do you think you were scammed? All Taiwan respondents who have been scammed (614)

Two fifths of those scammed said it impacted their wellbeing, and just over half said it made them feel stressed

Impact of being scammed on stress



Impact of being scammed on mental wellbeing



Q16. To what extent was experiencing the scam stressful? Q17. To what extent did the scam impact your mental wellbeing? Base: All Taiwan respondents who have been scammed (614)

Whilst being scammed increases vigilance to future encounters, one in ten say they had to make additional costs such as legal support as a result

Impact of scams on those experiencing family – top 6



28%
More vigilant of scams



15%
More distrustful of digital tools and platforms



15%
Reduce normal spending behaviour



15%
Drop in confidence and second guessing myself



12%
Heightened tension and stress in family unit



9%
Making additional costs (e.g., legal support, counselling)

Q18. How has the scam(s) impacted you and your family? Base: All Taiwan respondents who have been scammed (614)

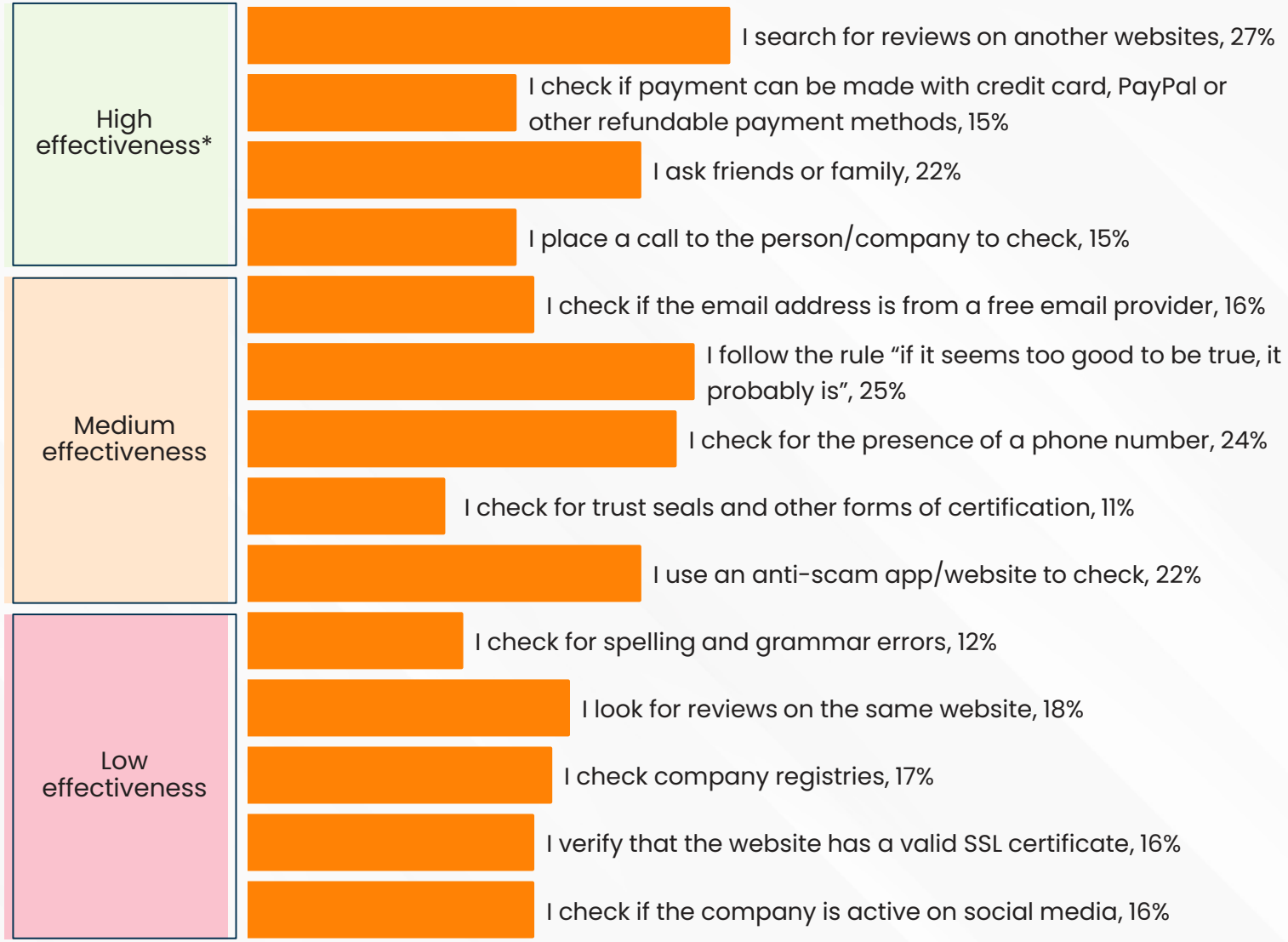


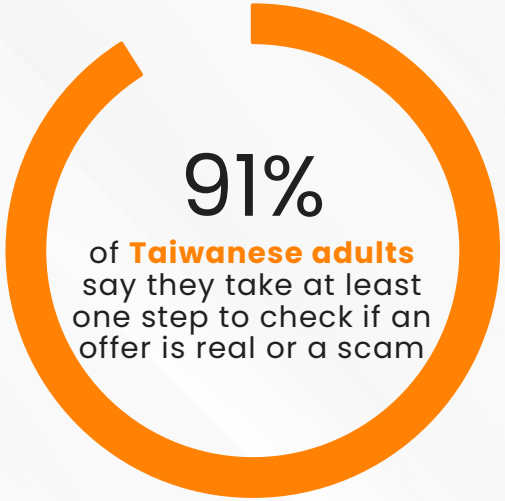
SCAM PREVENTION

Examining consumers' self-prevention tactics and perceptions of public and commercial organisations' roles in preventing and resolving scams

Over one in ten Taiwanese adults check spelling and grammar errors to legitimise an offer, but this has low effectiveness

Steps taken to check legitimacy of offer





Q20. What steps do you take to check if an offer is real or a scam? Base: All Taiwan respondents (1000) *Effectiveness groupings provided by GASA

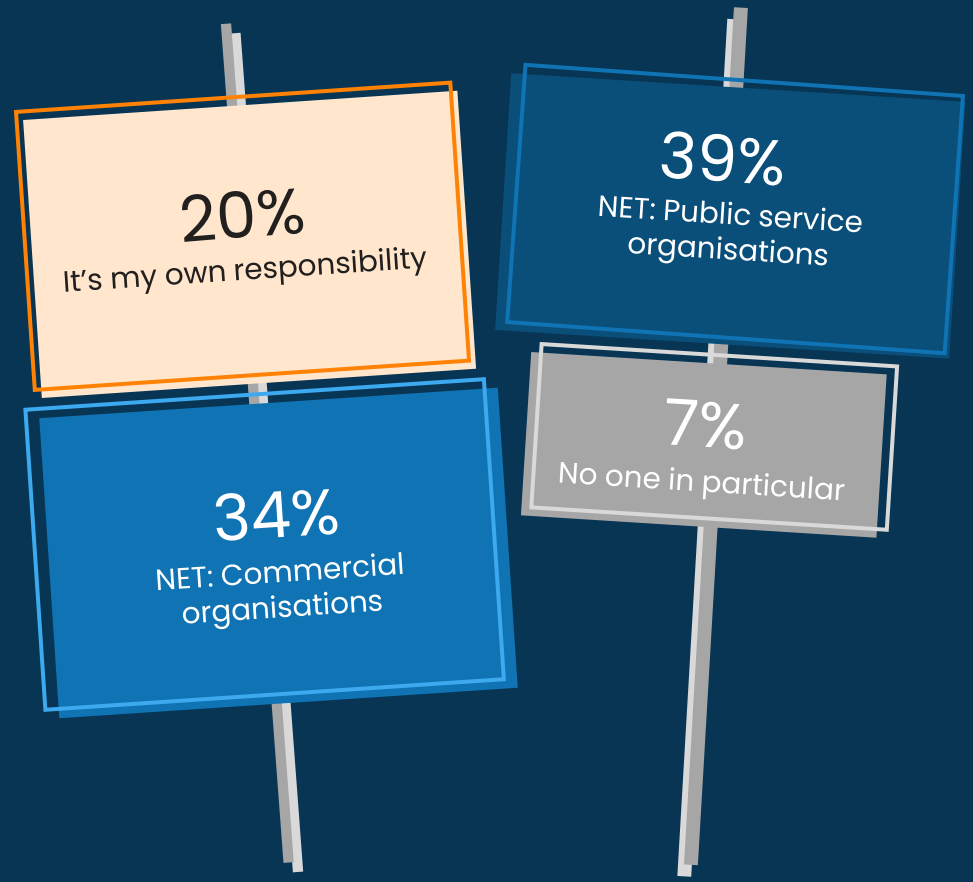
Taiwanese adults place the responsibility of keeping people safe from scams on public service organisations, primarily the government

Responsibility for keeping people safe from scammers ranking:

- 26% The government
- 11% The online platform used by the scammer
- 10% The website provider / hosting company used by the scammer
- 6% The police
- 6% My telecom or mobile operator
- 5% My bank, payment method or crypto exchange
- 4% Financial protection authorities
- 3% Consumer protection authorities
- 3% Insurance companies

Most responsible

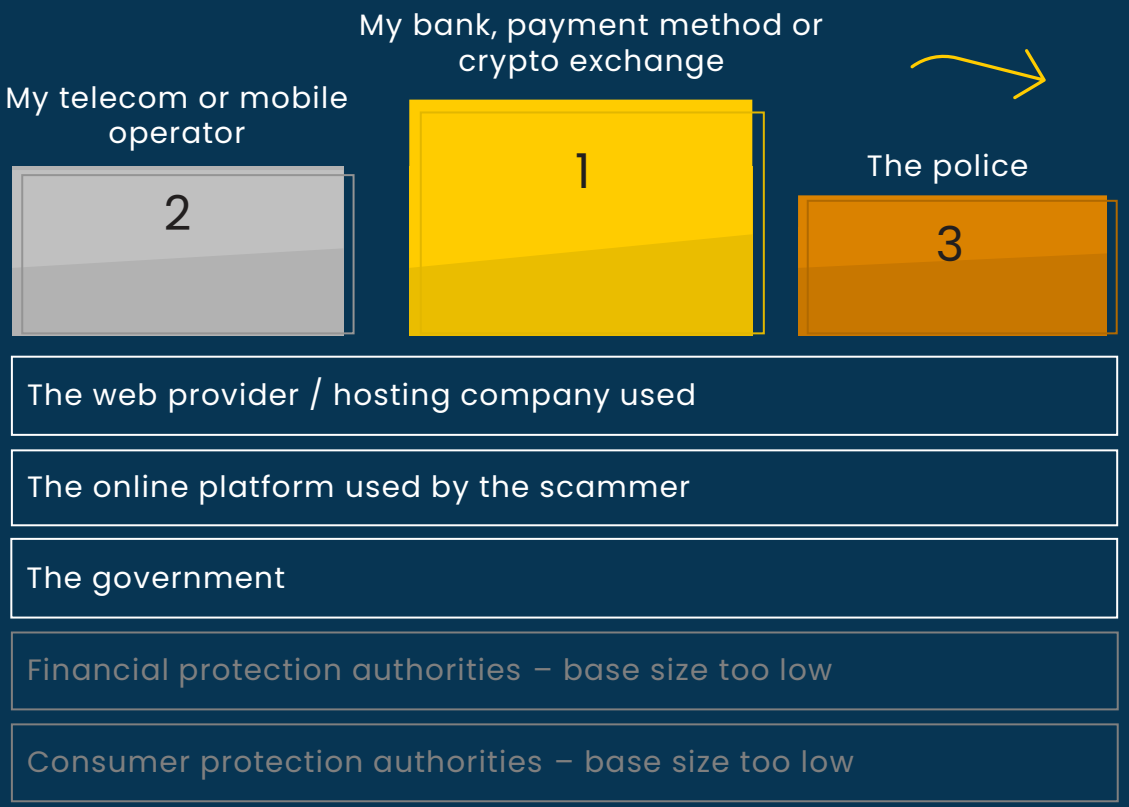
Least responsible



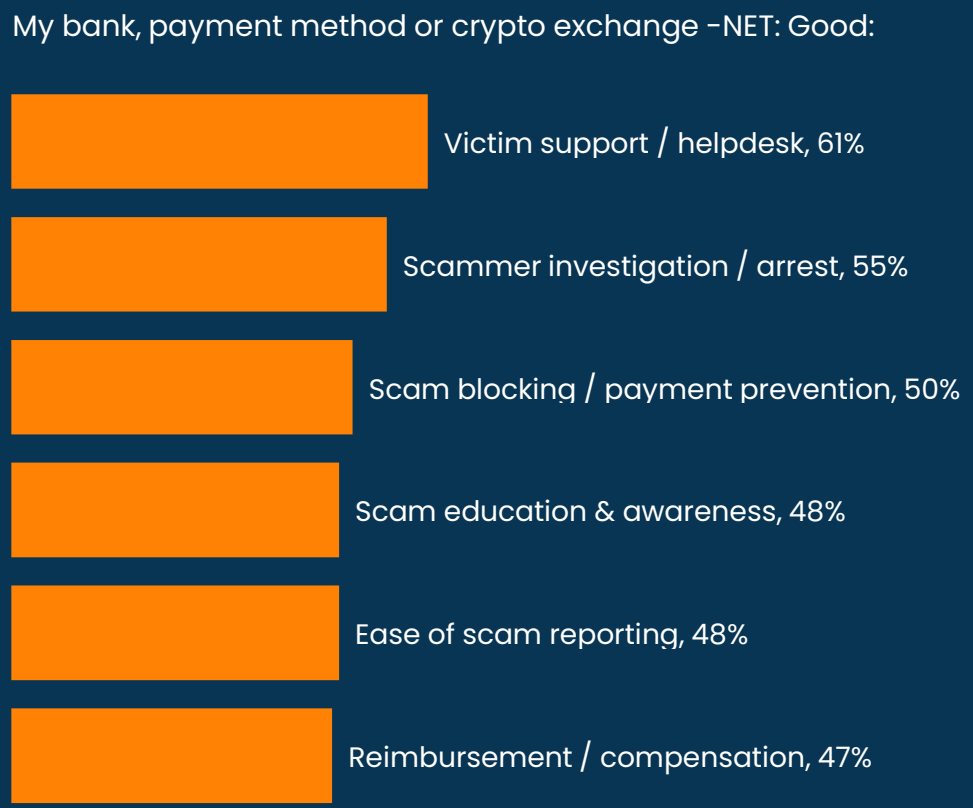
Q24. Who do you think should be most responsible for keeping people safe from scammers? Base: All Taiwan respondents (1000)

Meanwhile, Banks, payment methods, or crypto exchanges are rated highest amongst Taiwanese adults for preventing or resolving scams

Performance ranking on preventing / resolving scams



Click here to see full ratings



Q25. You said should be most responsible for keeping people safe from scammers. How do you rate on the following aspects: Base: All Taiwan respondents who think someone else should be responsible for keeping people safe from scammers (736), those who think Banks, payment methods or crypto exchanges should be most responsible (56)

Taiwanese adults expect the government to protect users from scams but see them as less effective than other organisations

Responsibility for keeping people safe from scammers ranking:

- The government
- The online platform used by the scammer
- The website provider / hosting company used by the scammer
- The police
- My telecom or mobile operator
- My bank, payment method or crypto
- Financial protection authorities – base size too low
- Consumer protection authorities – base size too low
- Insurance companies – base size too low

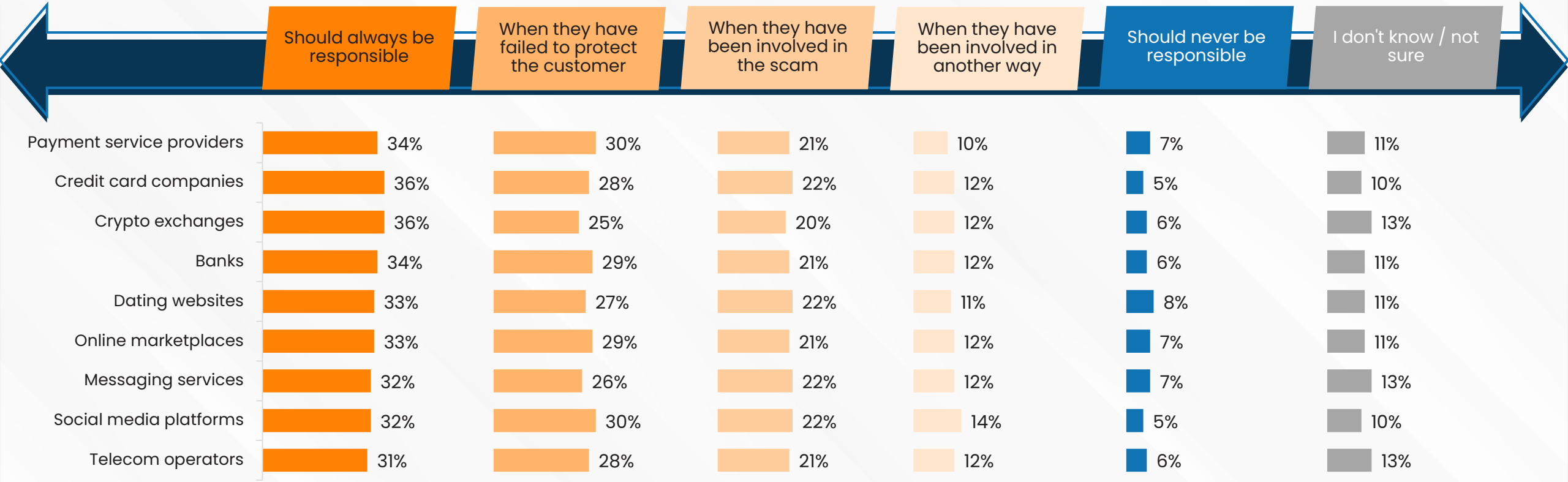
Performance ranking on preventing / resolving scams:

- My bank, payment method or crypto
- My telecom or mobile operator
- The police
- The web provider / hosting company used by the scammer
- The online platform used by the scammer
- The government
- Financial protection authorities – base size too low
- Consumer protection authorities – base size too low
- Insurance companies – base size too low

Q24. Who do you think should be most responsible for keeping people safe from scammers? Base: All Taiwan respondents (1000) Q25. You said should be most responsible for keeping people safe from scammers. How do you rate on the following aspects: Base: All Taiwan respondents who think someone else should be responsible for keeping people safe from scammers (736)

Over a third of Taiwanese adults believe Credit card companies and Crypto exchanges should always be responsible for reimbursing those experiencing a scam

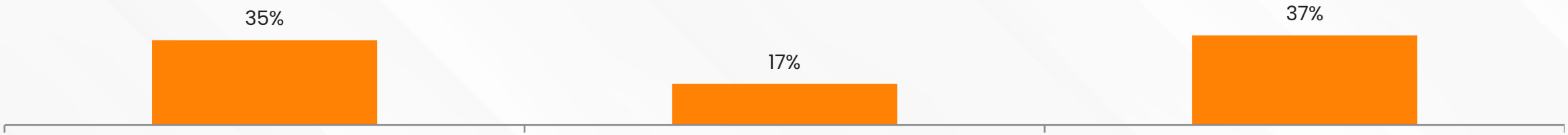
Level of expected responsibility for reimbursing scams – top 3 platforms



Q26. If someone is scammed on any of the following platforms, in what circumstances do you think the platform provider should be responsible for reimbursing them? Base: All Taiwan respondents (1000)

While Taiwanese adults believe full reimbursement should be the top penalty for scams, they also favour severe punishments

Maximum punishment for scamming someone of their entire annual wage



Full repayment to the victim	22%	Fines in addition to or instead of jail time	12%	Jail time (1 to 5 years)	8%
Mandatory public apology	4%	Suspended sentence / conditional release	3%	Jail time (6 to 10+ years)	13%
Community service	5%	Jail time (< 1 year)	3%	Life imprisonment	10%
Internet usage ban	5%			Capital punishment	5%

1%
of **Taiwanese adults** say there should **not** be a punishment for such a scam

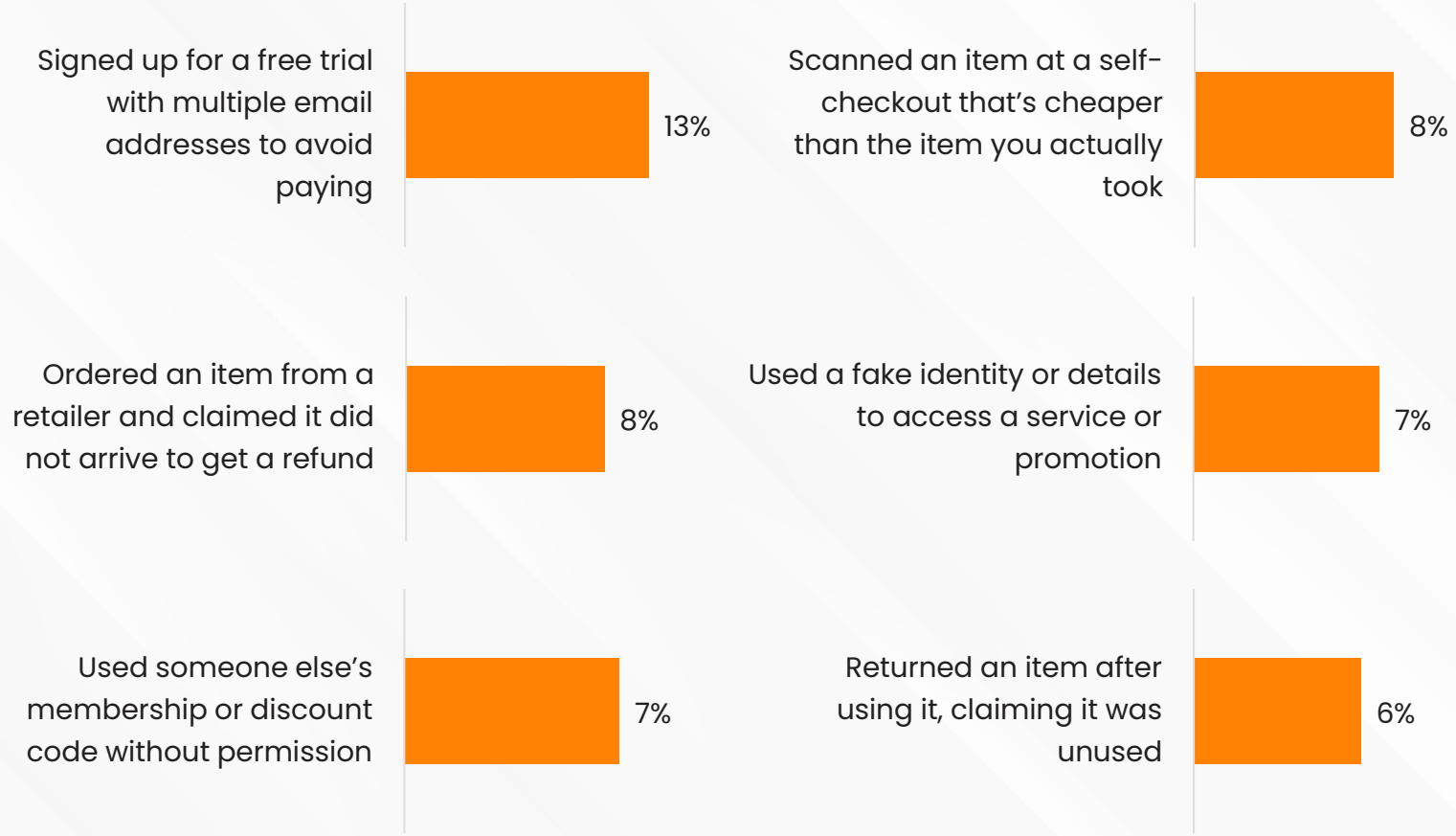
Q27. Please imagine a scenario where the following punishments were passed for crimes in your country. What do you think the maximum punishment should be for scamming someone of their entire annual wage? Base: All Taiwan respondents (1000)

Two fifths of Taiwanese adults admit to committing deceitful acts themselves

40%

Of **Taiwanese** adults admit to committing acts deemed as fraudulent

Top 6 fraud types committed by Taiwanese consumers



Q28. Which, if any, of the following have you done? Base: All Taiwan respondents (1000)

GASA Global Anti-Scam Alliance

SCAMADVISER

whoscall



GASA RECOMMENDATIONS

GASA Global Anti-Scam Alliance

SCAMADVISER

whoscall

GASA's ten recommendations to turn the tide on scams



Jorij Abraham
MANAGING DIRECTOR
GASA
Global Anti-Scam Alliance

Online scams are not just a consumer issue — they are now a major threat to digital trust, economic stability, and personal safety. As fraud networks become faster and more sophisticated, Europe needs to act decisively.

Governments often prioritize protecting critical infrastructure from cyberattacks. Yet scams targeting consumers undermine confidence in the digital economy — and criminals are evolving faster than our defences.

Through collaborative work at our global events, experts identified ten key actions to better protect consumers.

Empowering Consumers

1. Launch unified, permanent national campaigns to raise scam awareness.
2. Establish national helplines for scam victims, accessible online and by phone.
3. Create integrated victim support systems offering financial, legal, and psychological help.

Creating a Safer Internet

4. Build infrastructural protections with telecoms and tech providers to block scams before they reach consumers.
5. Improve fraud traceability across borders by requiring transparency from sellers, platforms, and payment providers.

Strengthening Cooperation

6. Set up an international network of national anti-scam centres, combining law enforcement, cybersecurity, and private sector expertise.
7. Develop a global scam data-sharing hub to detect cross-border fraud in real time.
8. Make service providers responsible and liable for fraud committed through their platforms.
9. Allow preventive action: enable providers to warn, block, and take down fraudulent activities without excessive liability risk.
10. Create a global scam investigation and prosecution network to target organized fraud groups across jurisdictions.

Protecting consumers is essential to securing the digital future. The Global Anti-Scam Alliance, its membership, and the international public & private sectors must lead the way.

GASA Global Anti-Scam Alliance SCAMADVISER whoscall



ABOUT THIS REPORT

Who are we?

The Global Anti-Scam Alliance (GASA) is a non-profit organization whose mission it is to protect consumers worldwide from scams. We realize our mission by bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, telecom operators, internet platforms and service providers, cybersecurity and commercial organizations to share insights and knowledge surrounding scams. We build networks in order to find and implement meaningful solutions.

GASA releases the annual Global State of Scams report, alongside many secondary reports which focus on the state of scams in various countries.

ScamAdviser is a global leader in AI-powered scam prevention, protecting businesses and individuals in real time. Our Anti-Scam Intelligence platform can protect users from untrustful websites, messages, and calls. Stopping scammers before they strike. Trusted by 400+ partners and used by over 1 billion people worldwide, ScamAdviser turns data into decisive action—so you can stay safe, stay ahead, and stay in control.

Whoscall, powered by Gogolook, is a cutting-edge digital anti-scam tool designed to protect users from scams across various channels, including phone calls, text messages, social media, and links. With over 100 million downloads globally, it features the most comprehensive database in East and Southeast Asia, covering more than 2.6 billion phone numbers.

Opinium is an award-winning strategic insight agency that utilises robust methodologies to deliver insights with impact for organisations across the private, public and third sectors.

GASA have partnered with Opinium to lead the 2025 Global State of Scams research programme.

Contact europe@opinium.com for enquiries.

Methodology notes

SAMPLE AND METHODOLOGY

- Sample size | 1,000 people
- Audience | Adults aged 18+ living in Taiwan
- Quotas | Quotas were used throughout fieldwork to ensure the sample was nationally representative of the Taiwanese adult population on age, gender and region
- Weighting | Weighting was applied on the final dataset to be nationally representative of the Taiwanese adult population on age, gender and region
- Methodology | 15-minute online survey
- Translations | Whilst this report is in English, the survey was translated into the local language for each market prior to completion by respondents
- Sample source | Online research panel
- Fieldwork | 26th February – 14th March 2025

CONVERSION RATES

The following conversion rate was used in this report:
1 USD equals 31 Taiwanese dollar

This rate was taken on 29th March 2025

VALUE LOST TO SCAMS CALCULATION

In this Nationally Representative survey of 1000 Taiwanese adults, 134 lost money to scams. 134 / 1000 * 20171331 (Taiwan adult population. Source: National Statistics Taiwan) = 2702958 (shorthand 2.7 million). $23276.3 * 2702958.354 = 62914869535.2102 (shorthand $62.9 billion).

FULL Q8 SCAM WORDING USED IN SURVEY

- **Investment scam**: Invested money with a person or company that deceived you about what you would receive, such as promising a guaranteed return on your investment or no risk of financial loss
- **Shopping scam:** Paid for any products or (subscription) services that you never received or that turned out to be a scam
- **Employment scam:** Paid money or given personal/financial information to get a job, employment, work-at-home position or business opportunity but were deceived about how the money would be used or what you would receive in return
- **Unexpected money scam:** Paid money or given personal/financial information to receive a prize, grant, inheritance, lottery winning, or sum of money that you were told was yours, but never received
- **Impersonation scam:** Paid money or given personal/financial information to a person who claimed to be a government official or working for a bank/lender or other company of authority
- **Charity scam:** Donated money to a charity or a charitable cause that later turned out to be fake or that you later suspected was fake
- **Romance/relationship scam:** Given money or personal/financial information to someone who pretended to be or pretended to be calling on behalf of a family member, friend, caregiver, or someone interested in you romantically, but that person was not who they claimed to be
- **Fake invoice scam:** Paid an invoice or a debt, but you found out you were being deceived, and the invoice/debt was not real or not yours
- **Blackmail or extortion scam:** Paid money or given personal/financial information because someone threatened or extorted you
- **Identity theft:** Personal information, e.g. your credit card, used without your consent OR did someone get access to a personal account(s), e.g., your bank, email, social media account, for financial gain, for example, to transfer money, take out a loan, request official documents, or buying products and/or services
- **Money recover scam:** Paid money or given personal/financial information to a company or person who promised to help me recover from a scam, but in the end deceived me.
- **Other scams:** Where you have paid money or given personal/financial information to someone who used deception in another situation not previously listed



ABOUT THE AUTHORS

GASA Global Anti-Scam Alliance

SCAMADVISER

whoscall

About the authors



Jorij Abraham

MANAGING DIRECTOR

Jorij Abraham has been active in the Ecommerce Industry since 1997. From 2011 to 2017, he was the Research Director of Thuiswinkel.org, Ecommerce Europe (the Dutch & European Ecommerce Association) and Managing Director of the Ecommerce Foundation.

From 2015 to 2024, Jorij was also a Professor of Ecommerce at TIO University. In 2018, Jorij took over ScamAdviser.com to help consumer due diligence efforts against online scams. He sold ScamAdviser to Gogolook in 2024 to focus on his current role as Managing Director at the Global Anti-Scam Alliance (GASA).



Molly Maclean

ASSOCIATE DIRECTOR

Molly Maclean is an Associate Director specialising in research for Thought Leadership.

Molly works with brands and organisations to help them use insights to raise awareness of key issues, influence decision-makers, and drive positive change.

She has over six years of experience conducting research for technology brands and organisations, particularly in the cybersecurity space.



Metje van der Meer

MARKETING DIRECTOR

Metje van der Meer leads global communications, brand strategy, and stakeholder engagement at the Global Anti-Scam Alliance (GASA). With over a decade of experience in B2B marketing and international outreach, she develops multi-channel campaigns and partnerships that advance GASA's mission to combat online fraud through cross-sector collaboration.

Metje plays a key role in promoting GASA's global and regional initiatives, including the Global Anti-Scam Summit (GASS) and the alliance's work across Southeast Asia. Her efforts focus on aligning public and private sector stakeholders to raise awareness and drive coordinated action against scams worldwide.

Join GASA, the Network to Defeat a Network

Exclusive Intelligence Sharing
Stay ahead of emerging scam trends through members-only webinars, expert-led discussion groups, and our monthly newsletter which is trusted by over 20,000 anti-scam professionals worldwide.

Authoritative Research Access
Get insider access to our Global State of Scam reports, 30+ in-depth regional studies, and best practice database that help shape anti-scam strategies.

High-Impact Networking
Connect with global changemakers at international summits, collaborate through local GASA chapters, and find partners through our members-only directory.

Global Solutions
Co-create or join concrete solutions to fight scams like the Global Signal Exchange where data is shared real-time scam intelligence and Scam.Org, the anti-scam hub being developed for consumers worldwide.

Become part of a global force against scams and help protect consumers everywhere.

See all benefits: **gasa.org/membership**

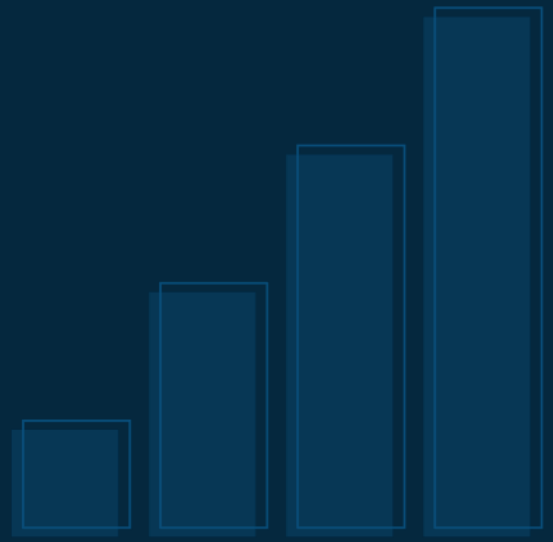
Our Foundation Members

amazon, Bitdefender, Capital One, Citizens, CSC, F-Secure, feedzai, Gen, Gogolook, Google, GSMA, ibfed International Banking Federation, JPMorganChase, LexisNexis Risk Solutions, Lloyds Banking Group, Mastercard, Match Group, McAfee, Meta, Microsoft, netcraft, Scamadviser, Scotiabank, The Media Trust, Trend Micro, VISA

Our Corporate Members

AnyDesk, Arab Bank, Arkose Labs, Banca Transilvania, cellcard, Chainalysis, Crystal, Cyberdefense, DANA, EBRAND, FICO, Remitly, Santander, sea, TeamViewer, tietoevry, VoiSek, VONAGE Part of Ericsson

GASA Global Anti-Scam Alliance · SCAMADVISER · whoscall



APPENDIX

GASA Global Anti-Scam Alliance

SCAMADVISER

whoscall

Money recover scams are the scam type mostly likely to last for longer than a day amongst Taiwanese adults

Length of scam – by scam type

Key = | Under index vs average | Over index vs average

	Average (across scam types)	Investment	Shopping	Employment	Unexpected money	Impersonation	Charity	Romance / relationship	Fake invoice	Blackmail or extortion	Identity theft	Money recover
Minutes	33%	29%	24%	24%	23%	26%	25%	26%	19%	25%	26%	20%
Hours	13%	14%	14%	15%	14%	14%	14%	14%	14%	12%	14%	14%
Days	19%	20%	24%	25%	25%	23%	24%	23%	29%	23%	25%	25%
Weeks	17%	19%	23%	20%	22%	22%	24%	23%	22%	25%	20%	27%
Months	7%	7%	8%	8%	6%	7%	6%	6%	7%	7%	7%	7%
About a year	3%	3%	3%	3%	3%	2%	2%	3%	3%	2%	2%	3%
More than a year	2%	2%	2%	2%	2%	1%	2%	2%	2%	2%	2%	1%

Q10. Thinking about the most recent time you were scammed, how long did it last? Base: All Taiwan respondents who have been scammed (614), across each scam type (280-415)

Telecom or mobile operator is at the top when it comes to scam blocking / payment protection and scammer investigation / arrest

Organisational ratings for aspects of preventing & resolving scams – NET: Good

	The government	The police	The online platform used by the scammer	The web provider/ hosting company used	My bank, payment method or crypto exchange	My telecom or mobile operator
Responsibility ranking	1st	4th	2nd	3rd	6th	5th
Scam education & awareness	25%	42%	30%	40%	48%	43%
Scam blocking / payment prevention	21%	39%	37%	40%	50%	51%
Ease of scam reporting	20%	44%	37%	44%	48%	51%
Victim support / helpdesk	19%	47%	32%	41%	61%	47%
Scammer investigation / arrest	19%	44%	33%	36%	55%	59%
Reimbursement / compensation	14%	35%	29%	41%	47%	43%

Q25. You said should be most responsible for keeping people safe from scammers. How do you rate on the following aspects: Base: All Taiwan respondents who think someone else should be responsible for keeping people safe from scammers (736). Across each organisation (54-261)

GASA
Global Anti-Scam Alliance

SCAMADVISER

whoscall

07 Op Opinium

DISCLAIMER

This report is a publication by the Global Anti-Scam Alliance (GASA) supported by ScamAdviser and Whoscall. GASA owns the copyrights for the report. Although the utmost care has been taken in the construction of this report, there is always the possibility that some information is inaccurate. No liability is accepted by GASA for direct or indirect damage arising from the use of information contained in the report.

COPYRIGHT

It is strictly prohibited to use information published in this report without the authors' prior consent. Any violation of such rule will result in a fine of €25,000, as well as in a further penalty of €2,500 for each day that such non-compliance continues. However, authors allows the use of small sections of information published in the report provided that proper citations are used (e.g., source: www.gasa.org)

Global Anti-Scam Alliance (GASA)

Oder 20 - UNIT A6311
2491 DC The Hague
The Netherlands

General & Press Inquiries: partner@gasa.org

X (Twitter): @ScamAlliance

LinkedIn: linkedin.com/company/global-anti-scam-alliance