



The State of Scams in Thailand 2024



Scammers hit 28% of Thai population as \$17.2 billion gone in 12 months





The 2024 State of Scams in Thailand report, conducted by the Global Anti-Scam Alliance (GASA), in association with Whoscall and ScamAdviser, provides an in-depth analysis of the evolving threat landscape of scams and frauds affecting Thai citizens. With input from 9,630 Thai respondents, this report reveals significant concerns regarding the increasing frequency and impact of scams across the nation.

Survey data indicates that 55% of Thai respondents are confident in their ability to recognize scams, reflecting a 5% increase in confidence since 2023. However, despite this growing awareness, 89% of Thai encounter scams at least once per month, with 58% experiencing more scam encounters over the last year. This represents an 8% increase in monthly scam encounters compared to 2023, highlighting a worrying trend of rising fraudulent activities.

Awareness of Al's potential use in scams is high among Thai respondents, particularly regarding Al-generated chat and voice, although fewer are aware of more complex Al-generated images and videos. Most scams are delivered via phone calls or text/SMS messages, with a notable 10% increase in text and SMS scams since 2023. Instant messaging apps, social media, and digital advertising are also common channels used by scammers, with platforms like Facebook, LINE, and Messenger being the most exploited.

One of the most alarming findings is that 67% of Thai did not report scams to law enforcement, a 5% increase from the previous year. This underreporting is driven by a lack of trust in the effectiveness of the authorities, with only 27% reporting scams to law enforcement or government bodies. The report highlights that 20% of

Thai were uncertain whether AI was involved in the scams they encountered, while 13% did not believe they were targeted by AI-driven scams.

Identity theft has overtaken shopping scams as the most prevalent type of fraud in Thailand, although both have seen an increase in incidence. The data shows that 28% of survey participants lost money in a scam, a figure that represents a 2% decrease in scam losses since 2023. On average, Thai victims lost \$1,106 each, contributing to a total loss of \$17.2 billion USD (591.75 billion Thai Baht), which equates to a staggering 3.4% of Thailand's GDP.

The speed and efficiency with which scammers operate is concerning, with 53% of scams completed within 24 hours of first contact. Additionally, 80% of victims realized they had been scammed on their own, or quite often through media and news, while one in five were informed by family and friends.

Only 2% of Thai victims fully recovered their losses, marking a decline in recovery rates, falling from 4% in 2023. 73% of scam victims reported experiencing a strong emotional impact, a 7% increase from the previous year. Trust in the Internet has also been severely compromised, with 70% of Thai reporting decreased trust due to scams.

Many Thai citizens are relatively "switched on" when it comes to scams. The extra vigilance is prominent with habits including checking for phone numbers and using anti-fraud apps and websites to verify the legitimacy of offers. However, nearly half of the survey participants reported that the process of reporting scams is too complex and unlikely to resolve the issue, with 7% assuming no one would refund their losses.

Citizens expressed dissatisfaction with the government's efforts to combat scams, with 49% rating the government's actions as poor, and only 14% considering themselves satisfied. Disturbingly, 4% of Thai respondents admitted they would consider being a money mule, though 92% firmly stated they would refuse such involvement. This tends to fall in line with many countries that we have researched this year, but we must also consider whether the answer to this question was

In conclusion, the State of Scams in Thailand report highlights the urgent need for improved preventive measures, stronger law enforcement action, and greater public awareness. The significant economic impact of scams, coupled with the emotional toll on victims, underscores the necessity for coordinated efforts to protect Thai citizens and restore confidence in both the government and digital platforms.





Jorij Abraham Managing Director



Sam Rogers
Director of Marketing

Thailand needs to integrate Al-driven scam detection across sectors





ScamAdviser is a global leader in scam prevention, committed to empowering businesses with its Al-powered Anti-Scam Intelligence (ASI). ScamAdviser provides real-time detection of suspicious activity and scam prevention for websites, calls. messages, and online platforms. With the world's largest scam database, ScamAdviser partners with over 400 organizations to protect more than 1 billion consumers worldwide, helping people confidently navigate the digital world. In this interview, Aaron Chiou, Product Director of ScamAdviser, will describe the current state of scams in Thailand and the advanced strategies needed for enterprises to protect consumers.

How significant has the issue of scams become in Thailand?

In Thailand, identity theft has emerged as the most common type of scam, overtaking traditional online shopping scams. There has also been a significant surge in Al-driven scams, particularly through deepfakes and voice impersonation technologies. Scams are frequently delivered through phone calls, SMS, and instant messaging apps such as LINE, Facebook, and Messenger. Additionally, phishing and investment scams, particularly those related to cryptocurrencies, have become increasingly common.

What actions have been taken by the government and organizations to protect consumers from scams? What best practices can we learn from?

The Thai government has introduced several anti-scam initiatives, including the Anti-Online Scam Operation Centre (AOC) and a 24-hour hotline (1441) to assist victims and prevent scams. In collaboration with banks and law enforcement, these efforts have successfully led to the freezing of fake accounts.

To address this, government agencies, along with telecommunications, e-payment services, and trusted technology providers, have launched anti-scam campaigns to educate users and the market. The National Cyber Security Agency is also working with technology partners to enhance anti-scam technologies and ensure timely updates on prevention methods. Moving forward, Thailand should focus on integrating Aldriven scam detection across sectors, improving coordination with social media platforms to remove scam content, and strengthening legal frameworks for quicker asset recovery.

What further actions could give consumers the upper hand in fighting scams?

To enhance consumers' ability to combat scams, sectors such as banks, telecom companies, and other industries should work together with the national authorities, collaborating to strengthen user protection and scamprevention efforts. Streamlining the reporting process and strengthening reimbursement policies would empower victims and minimize financial losses. Although many consumers already use anti-scam apps to verify suspicious activities, ongoing public education and awareness campaigns led by the government are essential to further prevent scams, particularly those that occur unintentionally. Through promoting vigilance and understanding, these measures can enable consumers to better protect themselves from fraudulent schemes.



Aaron Chiou Product Director



Rising scams require a comprehensive nationwide approach to ensure a safer digital environment for Thais





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, and links. In the Thailand 2024 State of Scams report, GASA interviewed Manwoo Joo, CEO of Gogolook Thailand, to share insights on the in-depth analysis of the evolving scam landscape in Thailand, to equip consumers with the knowledge and tools they need to stay one step ahead of scammers.

With more than 62.6 million mobile phone users and nearly 90% internet penetration rate, Thailand remains one of the most active fertile ground for scammers and attempted scamming activities in this region.

According to Whoscall's 2023 Annual Report, Thai people continue to experience a proliferation of phishing texts and phone scams- receiving an estimated 20.8 million scam calls and over 58.3 million scam text messages.

Alarmingly, this trend shows no sign of abating anytime soon. In the first six months of this year alone, Whoscall has identified nearly 19 million scam calls in Thailand. Our data aligned with The Royal Thai Police's official record which reported nearly 200,000 complaints of online scam cases from January to July 2024, averaging over 10,000 cases reported in each region.

Our latest insight further uncovered a troubling reality that scams affect all demographic groups, though in different ways. Middle-age to elderly individuals, particularly women aged 30-60 are the primary target by scammers due to lack of comfort with technology and the amount of financial resources in possession. Meanwhile, teenagers and young adults are increasingly

becoming more vulnerable due to constant online access to phones, tablets, computers, and gaming platforms because the more time spent online, the greater the exposure to potential risks.

Unsurprisingly, the top three most prevalent scam types identified by authorities are fake product selling; wire transfer scams linked to fake job offers and extortion schemes- many of which took place on popular digital and social media platforms such as Facebook, TikTok Lazada and LINE. In addition, loan scammers are leveraging advanced techniques such as deepfake and Al technology to impersonate government or banking officials to trick their victims. Thailand Consumers Council (TCC) estimated over the past three years, Thais have lost approximately 65 billion baht annually, or 180 million baht daily, to online scammers.

To combat the rising scams effectively, several jointcampaigns between public and private sectors have been initiated across various industries to create public awareness, disseminate information about online threats, prevention and response methods. The government also intensified its efforts by introducing several anti-scam policies, launching dedicated websites and hotline numbers as well as establishing designated authorities tasked with combating scams and fraudulent activities. Additionally, they are collaborating closely with private companies including Gogolook Thailand to raise public awareness and reduce risks of people falling victim to online threats. However, as cybersecurity threats loom and continue to evolve, so too the rules of the game and government policies that are constantly changing. As a result, Thais, especially vulnerable groups, find themselves lost, ashamed and distrustful when seeking

help from authorities - with many choosing to navigate the treacherous waters of the cyber realm with caution and vigilance by themselves through digital protection services or personalized anti-scam tools in the market. Therefore, more must be done and can be done to close this gap and ensure the safety and protections of Thai people.

Preventing scam victimization requires a comprehensive nationwide approach from top-down initiative at a policy-maker level from a centralized knowledge hub to a personal conversations among loved ones on what to do if they fall in victim and how to report.

By fostering collaboration across sectors, we can empower all Thais to take an active stand in combating scams and ultimately pave the way for a safer digital environment and scam-free society.

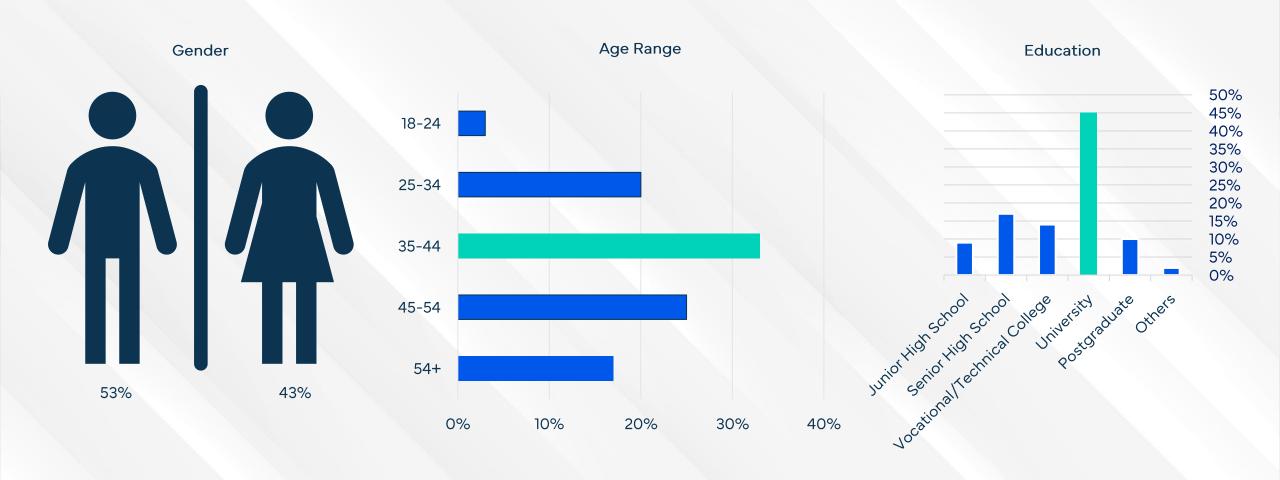


Manwoo Joo CEO Gogolook Thailand

Gogolook







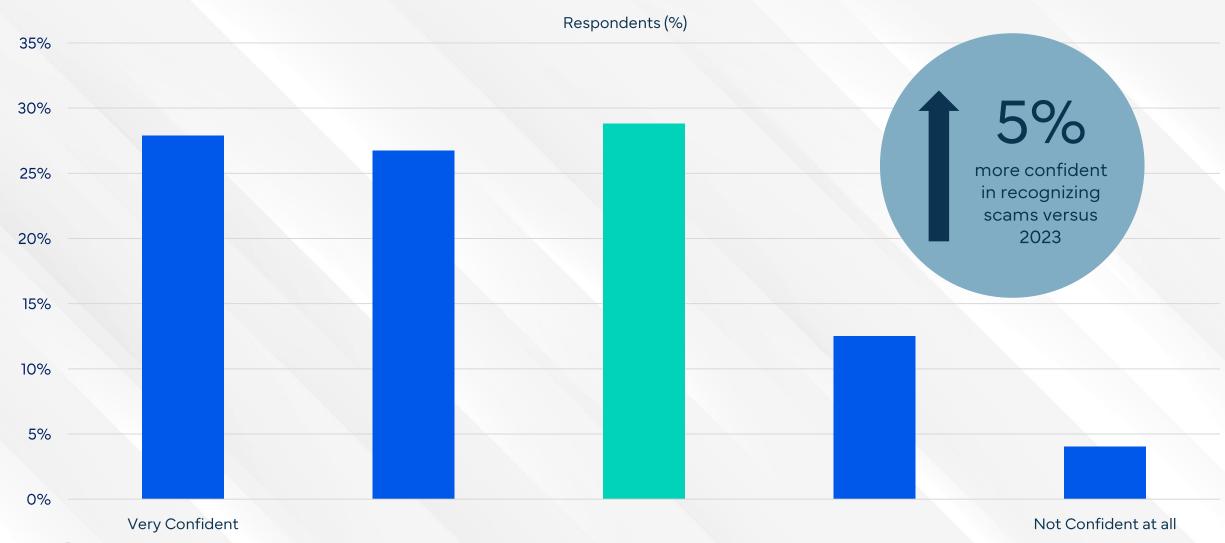


The demography of respondents to the State of Scams in the Thailand 2024 survey consists of more men than women. A large proportion were between 35-44 of age with a university education.

55% of Thai are confident in their ability to recognize scams







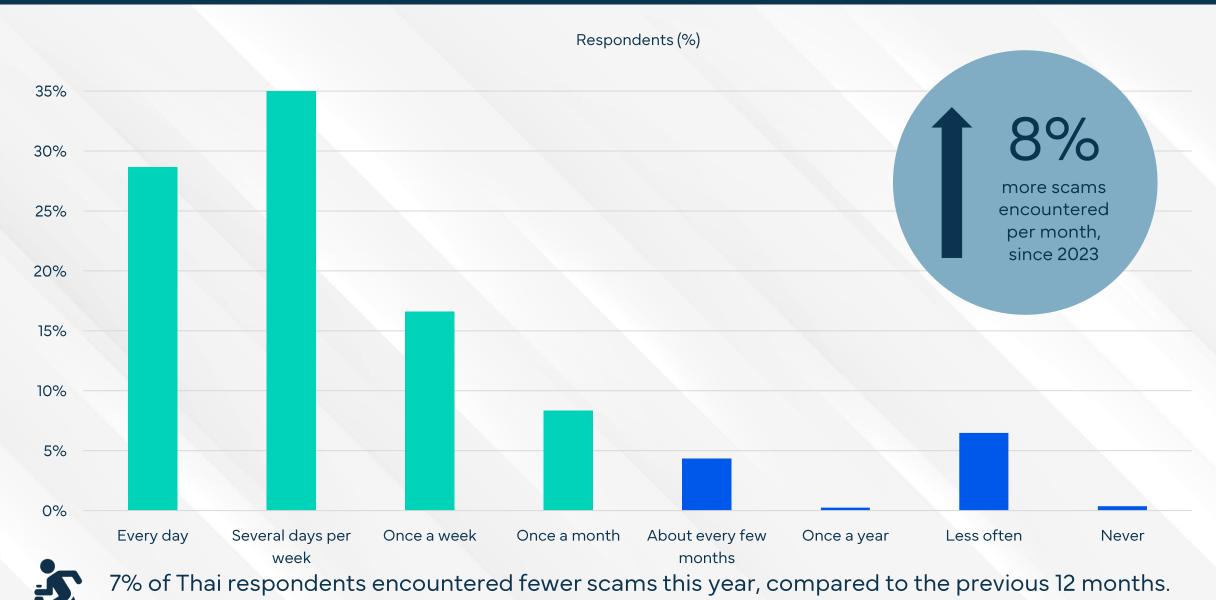


Only 17% of respondents are not (very) confident in recognizing scams, at all.

89% of Thai encounter scams at least once per month





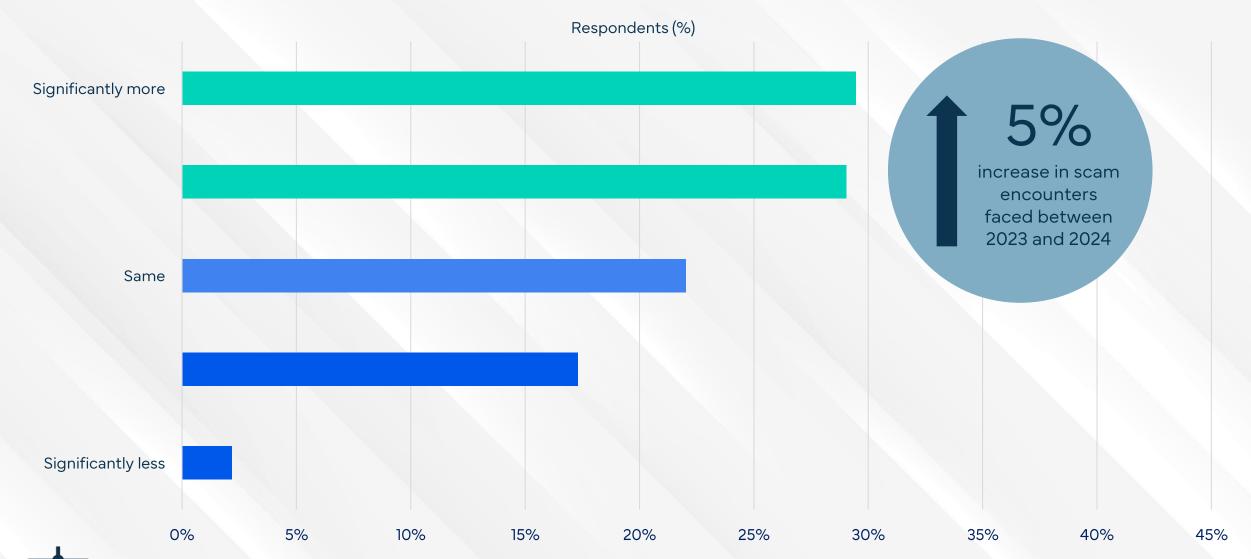


Q3 - In the last 12 months, how often have you been exposed to scam attempts? This includes receiving suspicious content, as well as seeing deceitful advertising.

58% of Thai faced more scam encounters in the last 12 months





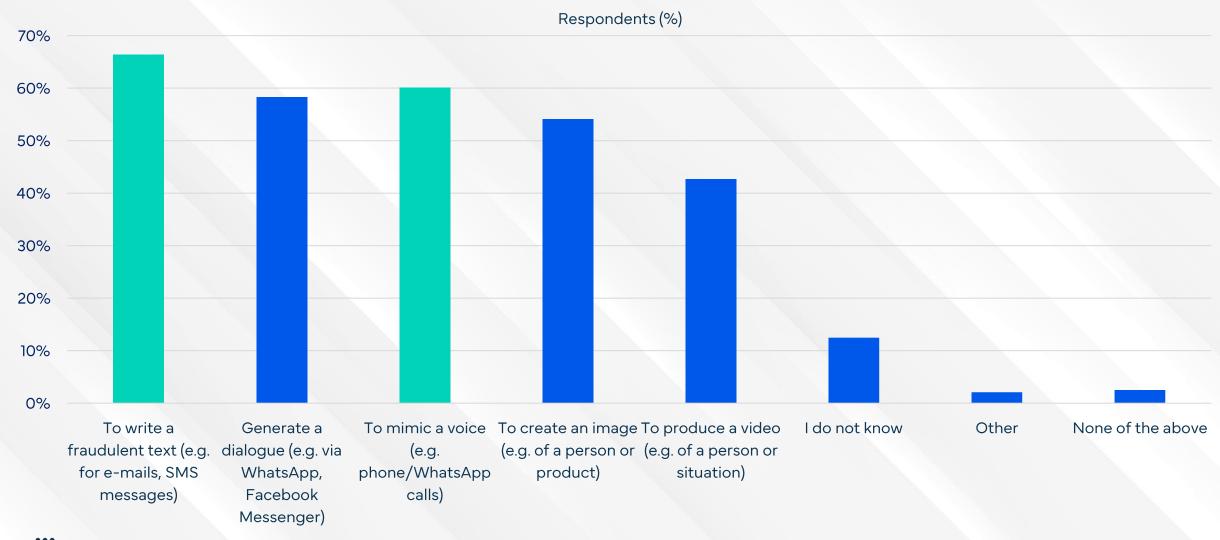


Only 19% of Thai respondents experienced a reduction in scam encounters in the past 12 months.

Most Thai are aware scammers can use Al against them







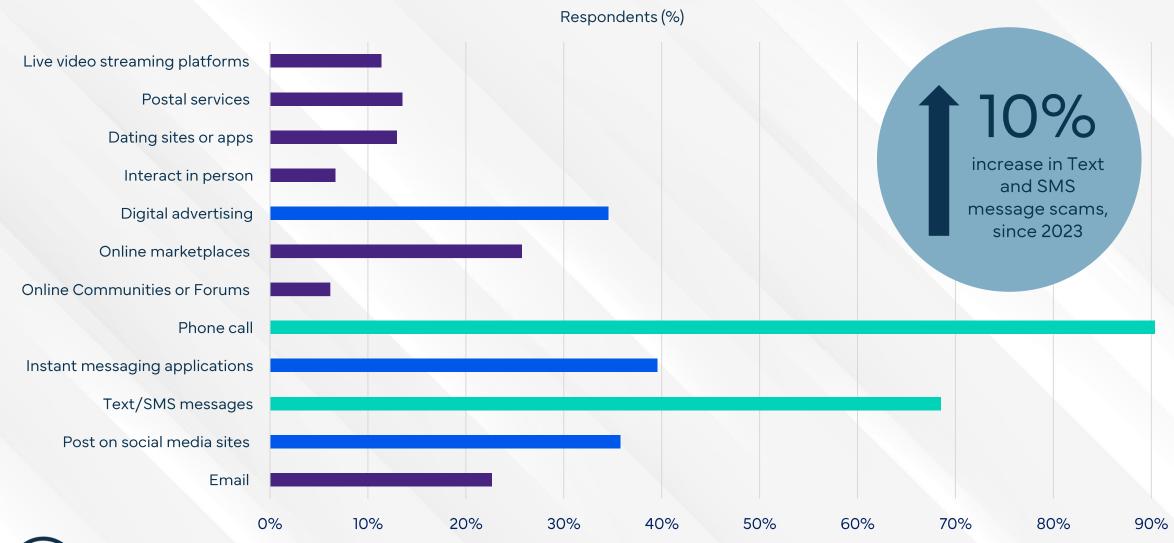


Awareness of Al generated chat & voice is high, while complex images & videos are less widely known.

Majority of scams are delivered via phone calls or text/SMS messages









Instant messaging apps, social media, and digital advertising are also common scam media.

Facebook, LINE, & Messenger are the most exploited platforms





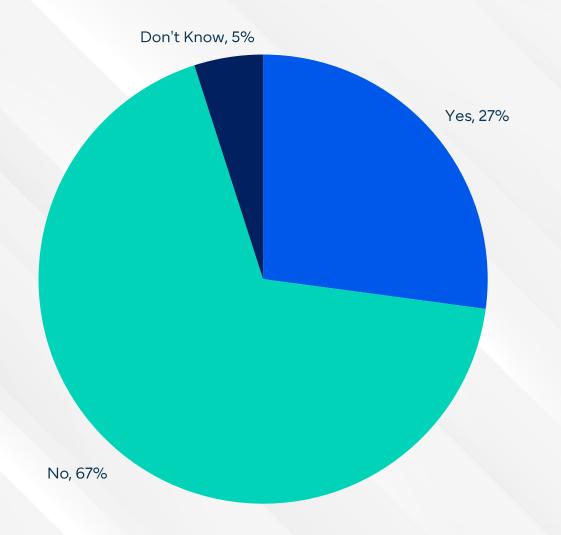


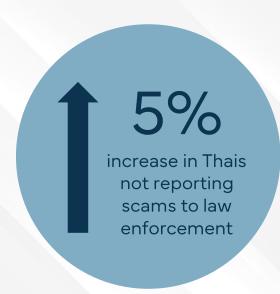


TikTok and Gmail round out the top five platforms where people encounter scams.









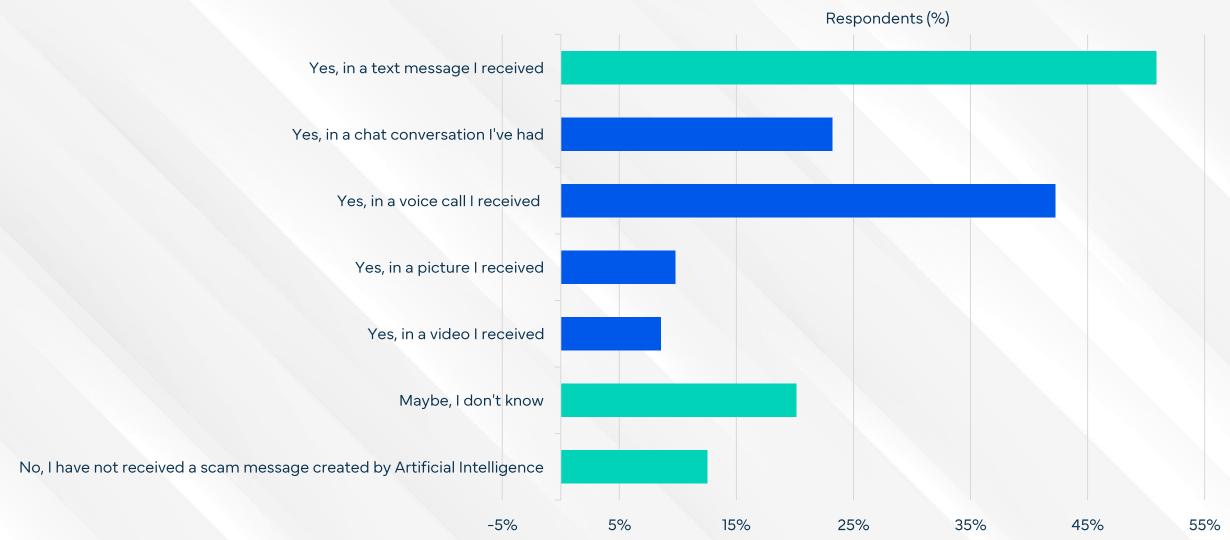


27% stated having reported the scam to law enforcement or another government authority.

20% of Thai were uncertain whether AI was used to scam them







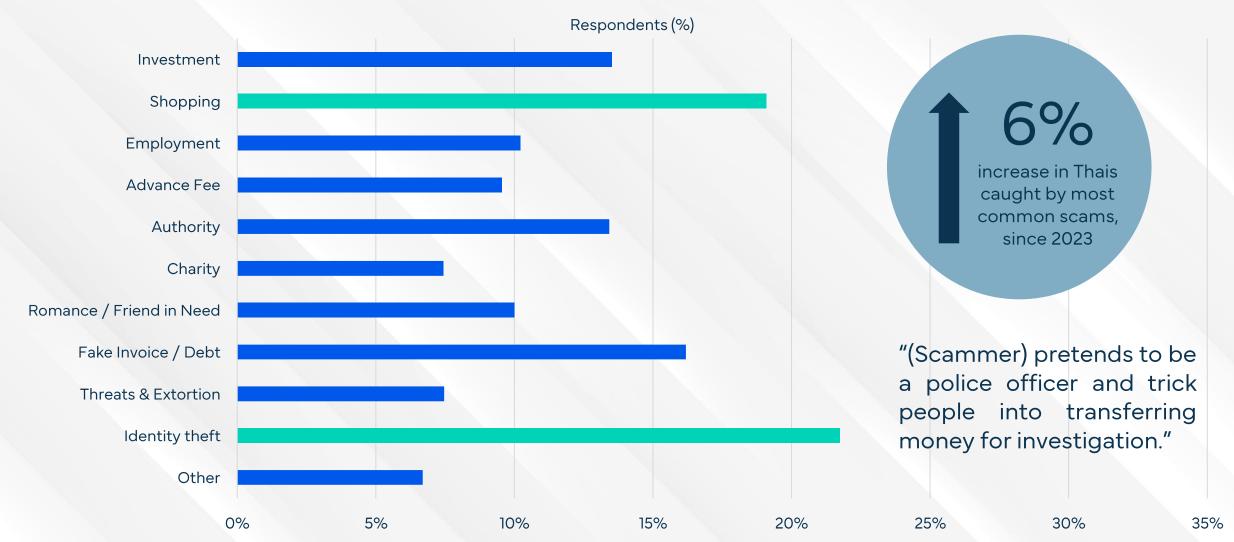


13% of Thai stated they did not believe they were subjected to scams utilizing artificial intelligence.

Identity theft overtakes Shopping scams as most prevalent









45% did not fall victim to the most common scams in the last year. 1.35 scams were reported per victim.

Thai scam victims share their stories



"Scams offering house cleaning services via Telegram. I was asked to make a deposit payment via QR touch & go of RM100. After the payment was made, I was immediately blocked from contacting the account."

"The scammer has threatened to spread false sexual information to family members if payment is not made. Payment of RM600 has been made 5 times."

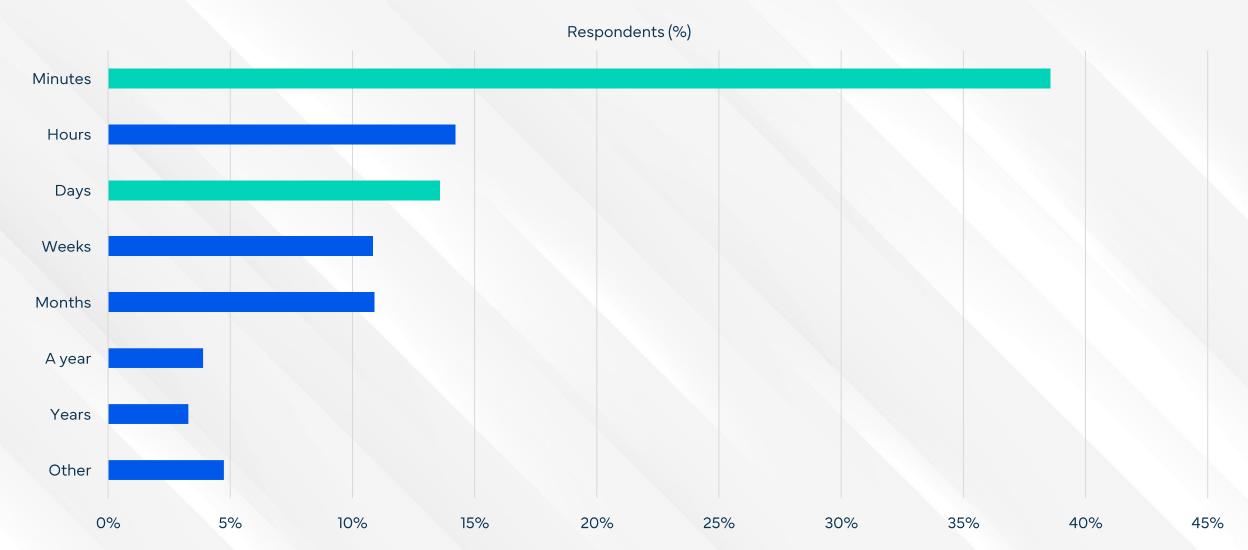
"I bought shares that promised immediate profit returns, but after (investing), there are several fees that need to be paid even though I was initially promised only a one-time fee."

"My credit card is used for online purchases abroad. I only realized it even received a bank statement. I made a report to the bank and got my money back."

53% of scams are completed within 24 hours of first contact







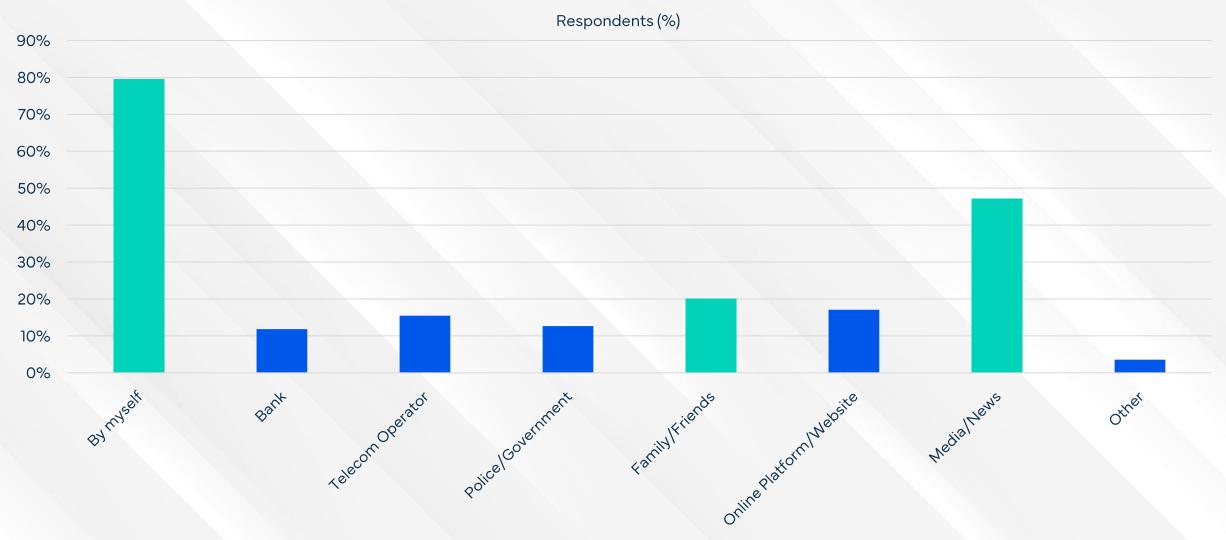


39% reported scams that were over in minutes, while 7% were scammed over a year or more.

80% concluded that they had been scammed without external advice









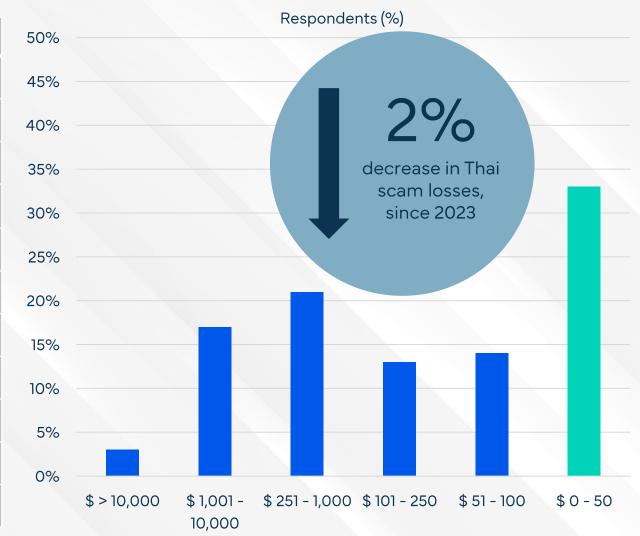
Half of victims are informed by media & news, while 1-in-5 are informed by family & friends.

In total, 28% of Thai survey participants lost money in a scam





Survey Key Statistics	
Persons approached	9,630
Participants losing money	2,654
% losing money / survey participants	28%
Average amount lost in US Dollars	1,106
Total country population	69,920,988
Population over 18 years	56,442,681
# of people scammed > 18 years	15,555,439
Total scam losses (USD)	17,204,315,282
Total scam losses (Thai Baht)	591,747,592,612
Gross Domestic Product (USD, millions)	512,193
% of GDP lost in scams	3.4%



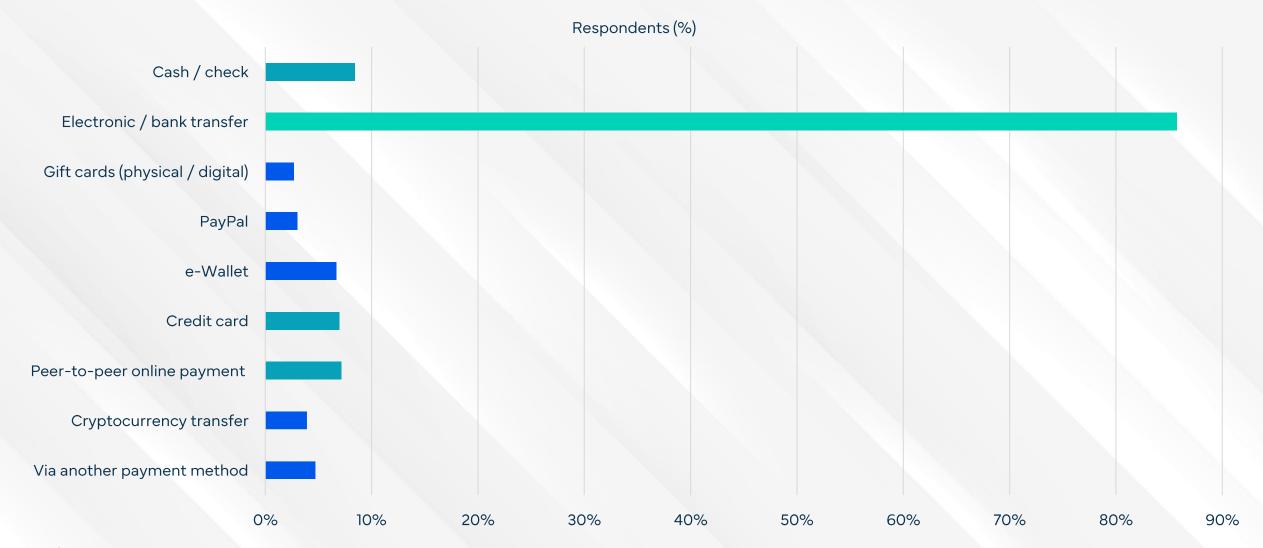


In total, the Thailand lost \$17 billion to scams, which is equal to 3.4% of Thailand's GDP.

Electronic/Bank Transfers account for 86% of scam payments in Thailand







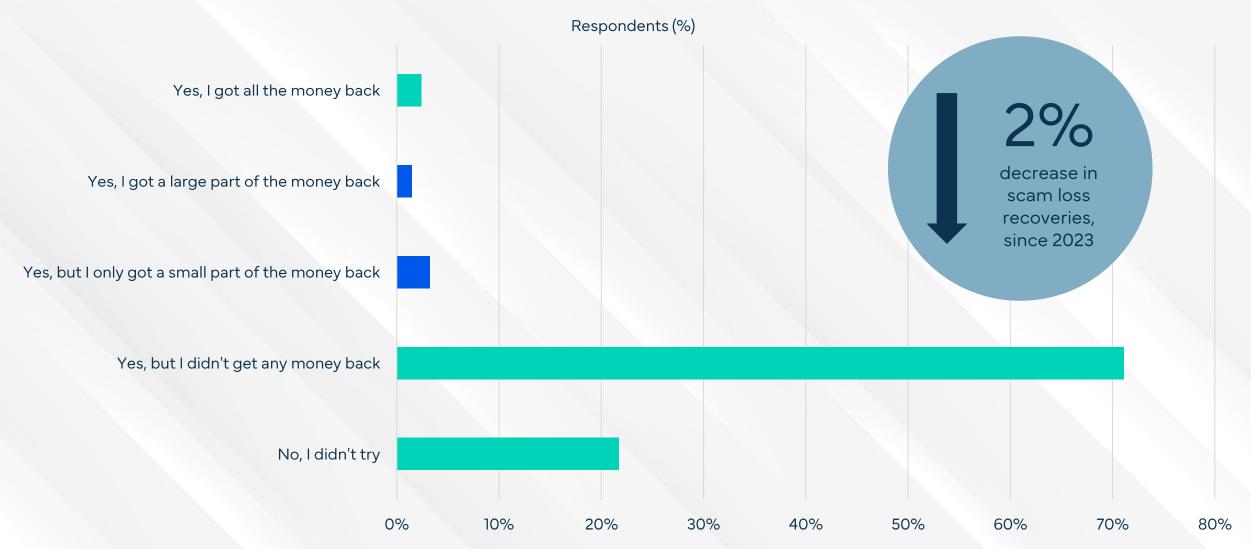


The remaining 14% of scam payments are spread relatively evenly across other payment methods.

Only 2% of Thai victims fully recovered their losses







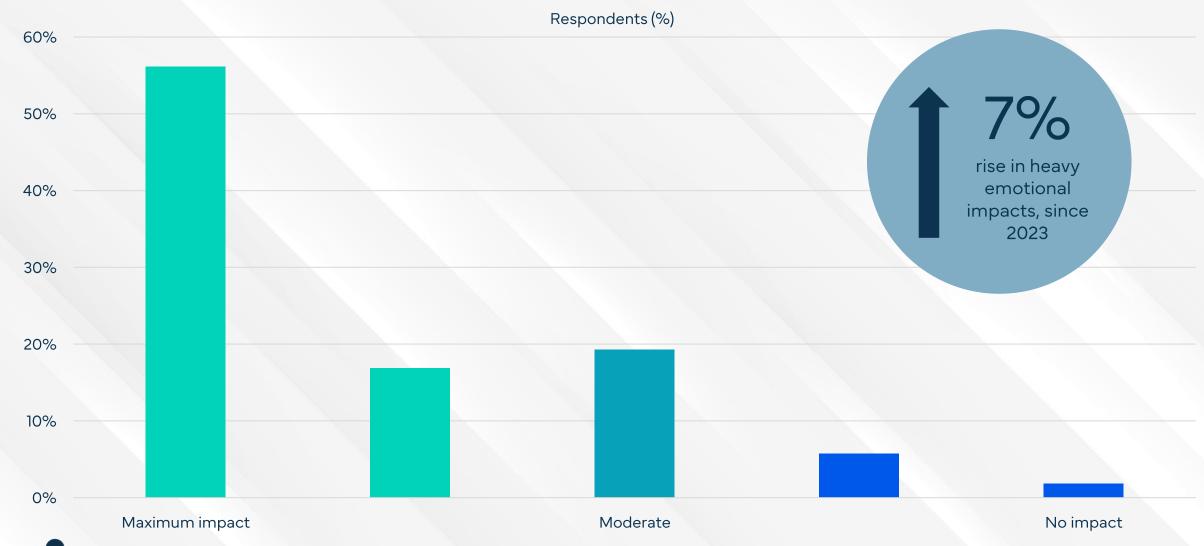


22% did not try to recover their funds. 71% tried but were not able to recover any money.

73% of the scam victims perceived a strong emotional impact







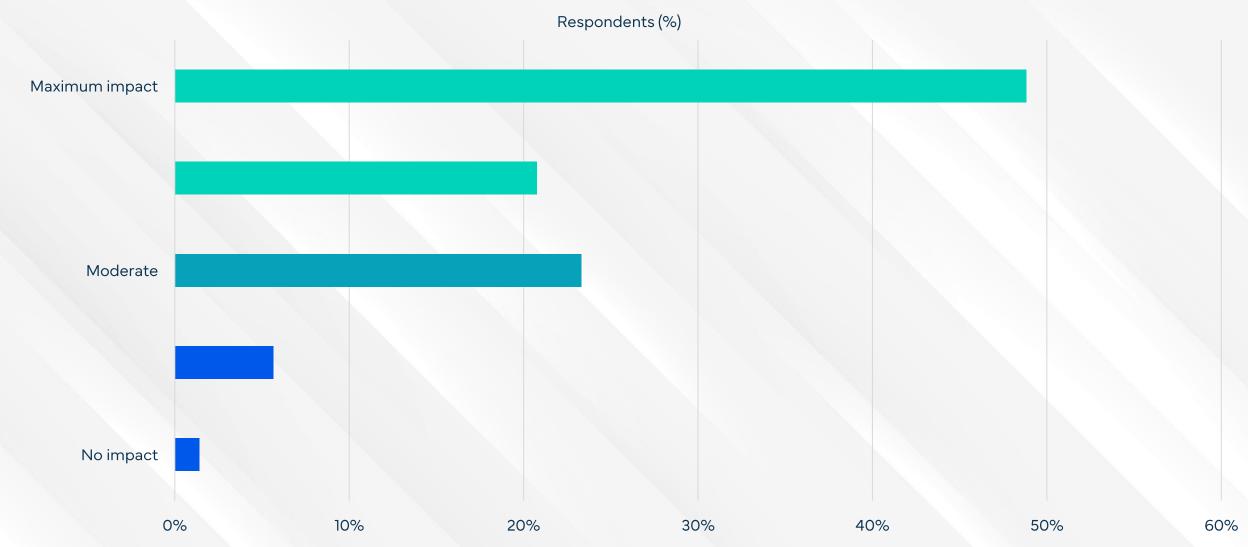


8% of the survey respondents reported little to no emotional impact due to scams.

70% of Thai have less trust in the Internet because of scams







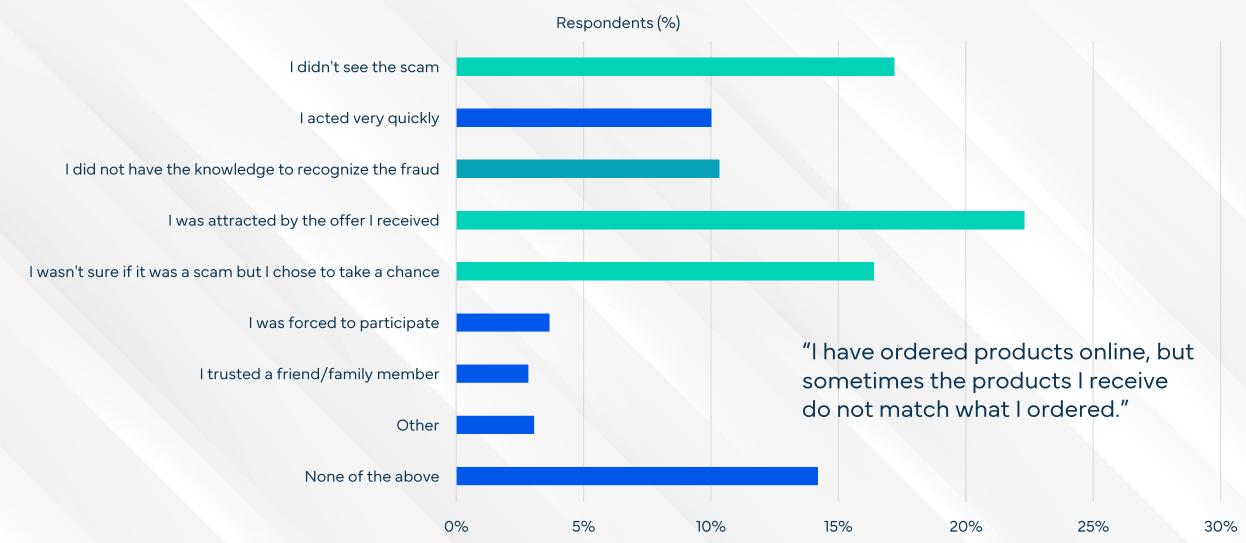


Only 7% of Thai reported little to no loss of trust in the Internet due to scams.

Thai are often scammed because of the attractiveness of the offer







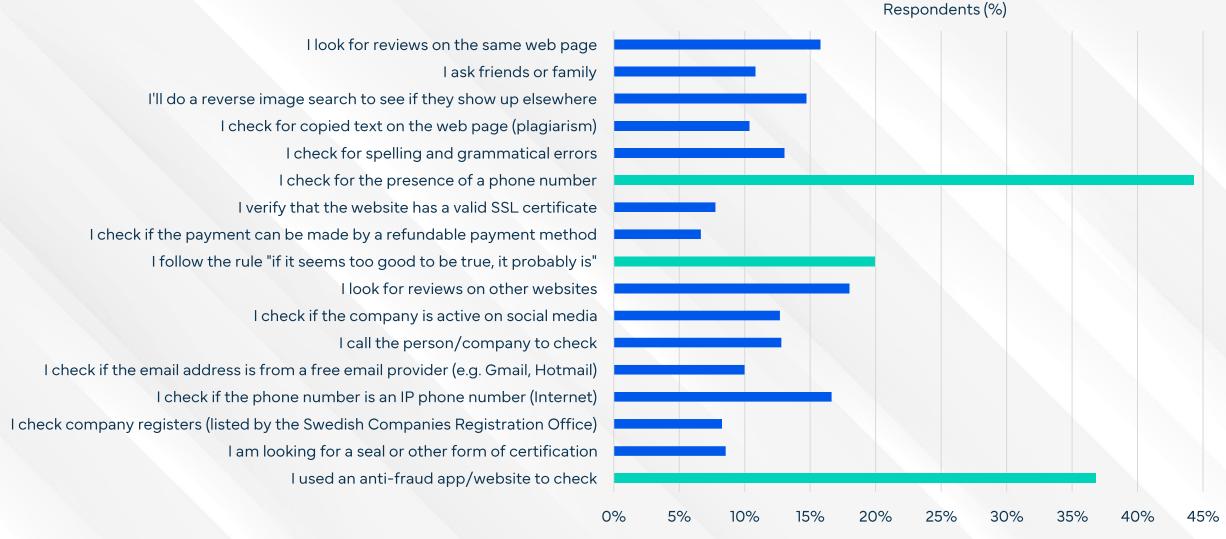


Several victims also reported inability to spot the scam while others were uncertain but chose to risk it.

Nearly half of participants check for the presence of a phone number







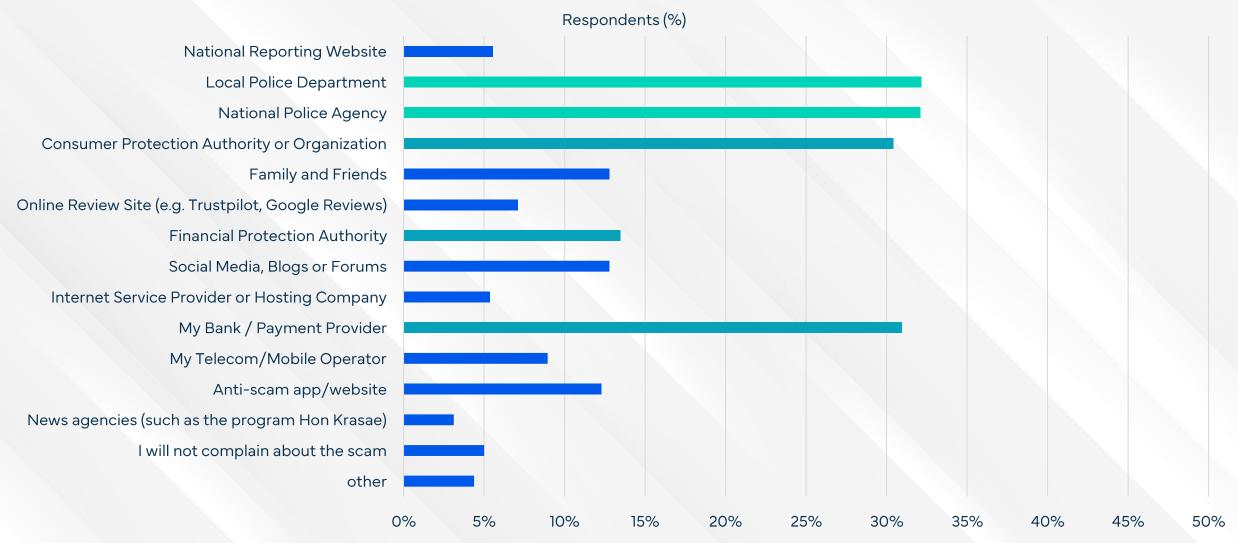


Many reported using anti-fraud app/website and following "if it seems too good to be true" rule.

Scams are mostly reported to Police, Banks, or Consumer Protection









Banks, consumer protection authority & financial protection agency are popular places to report scams.

Reporting processes are seen as too complex and unlikely to fix anything







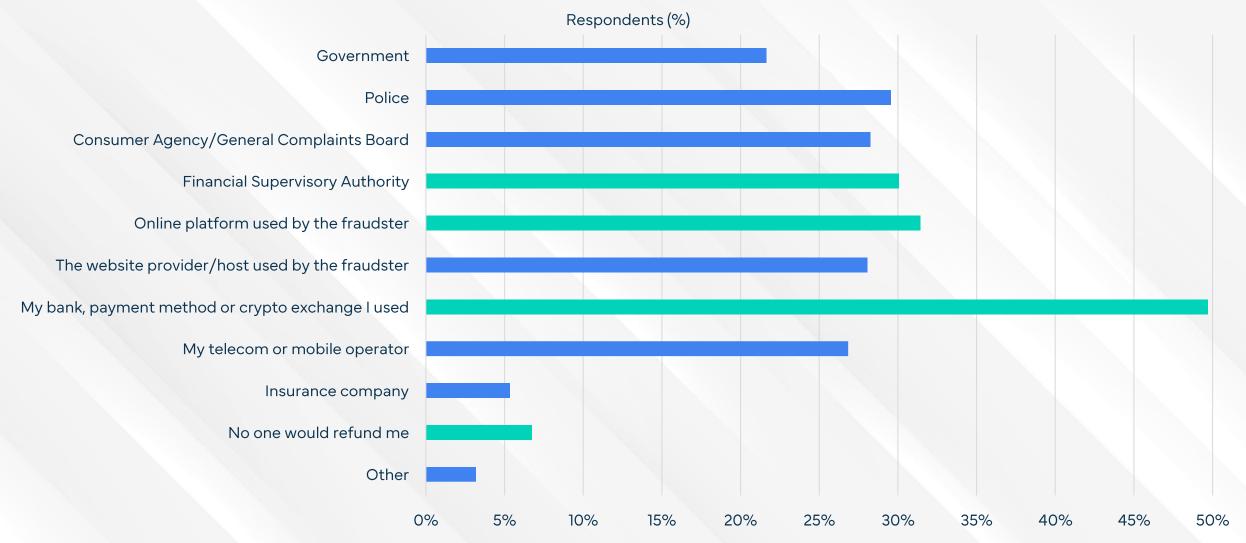


Another prominent reason for choosing not to report is an uncertainty of whom to report scams.

7% of Thai respondents assume no one will refund their scam losses







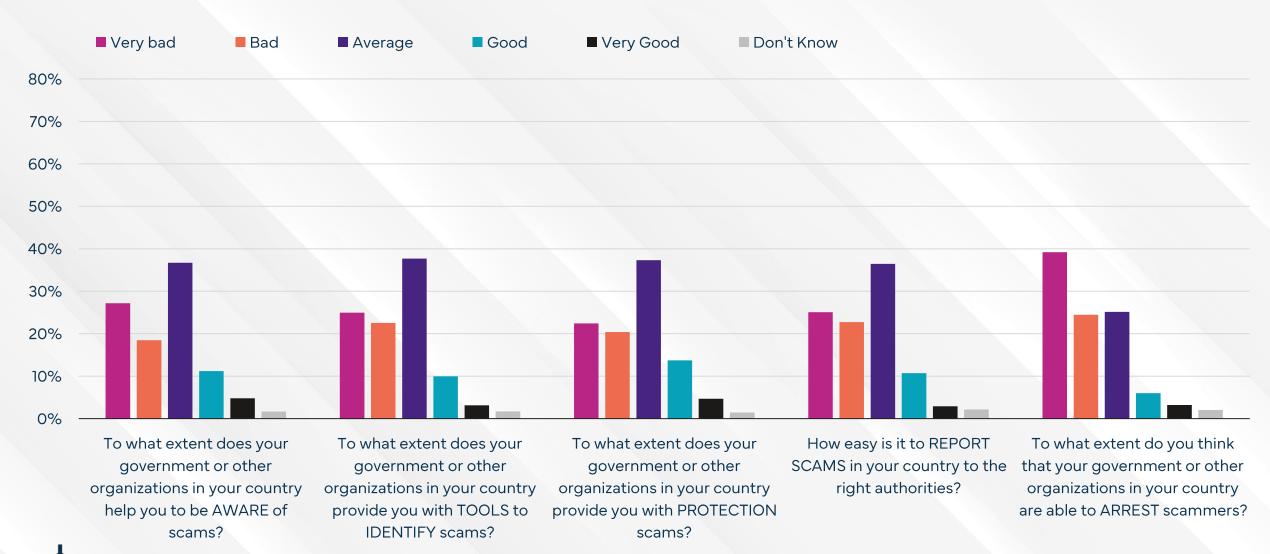


Others deem their banks, online platform used, and financial supervisory authority responsible.

Citizens are unhappy with the Thailand's attempts to arrest scammers







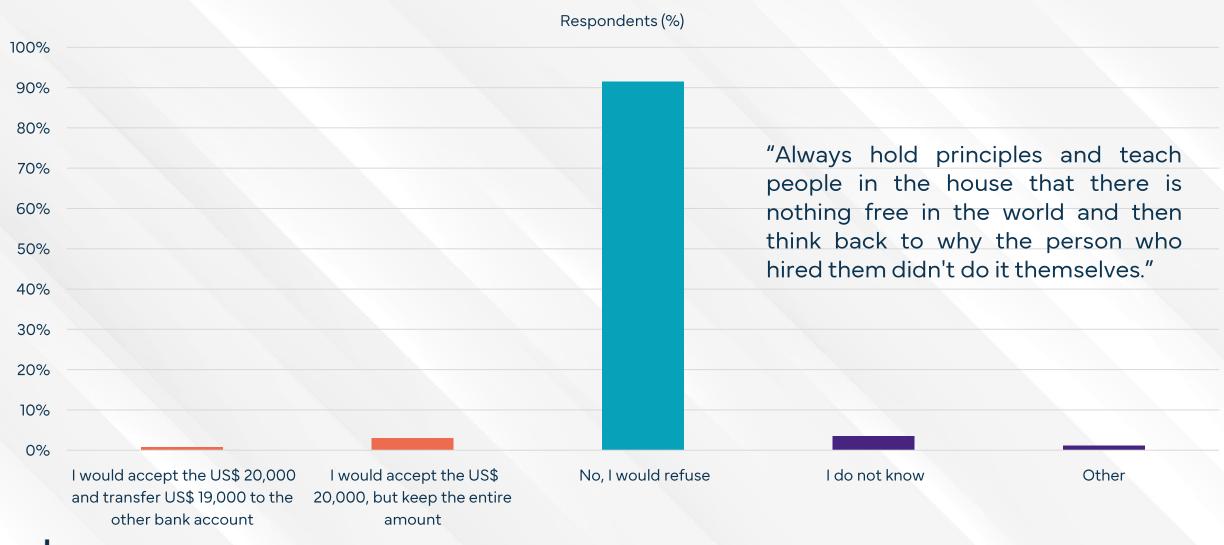
Overall, 49% of the participants rate the actions of the government as (very) bad, 14% as (very) good.

Q24 - Think about how well the government and other groups in your country are doing in the fight against online scams. How do you rate their efforts in the following categories?

4% of Thai admit that they would consider being a money mule









However, 92% of those surveyed would refuse to be involved in a "money mule" scam.



About This Report











The Global Anti-Scam Alliance (GASA) is a non-profit, bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, cybersecurity, and commercial organizations to share insights and knowledge surrounding scams. GASA releases the annual Global State of Scams report, alongside many secondary reports which focus on the state of scams in various countries.



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, 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.



ScamAdviser is a global leader in scam prevention, committed to empowering businesses with its Al-powered Anti-Scam Intelligence (ASI). Our platform delivers real-time detection of suspicious activities, protecting websites, phone calls, messages, and online platforms from potential scams. With the world's largest scam database, we share insights with 400+ partners, collectively protecting more than I billion consumers worldwide.

About the authors





Jorij Abraham has been active in the Ecommerce industry since 1997. From 2013 to 2017, he has been Research Director at Thuiswinkel.org, Ecommerce Europe (the Dutch & European Ecommerce Association) and the Ecommerce Foundation.

Nowadays, Jorij is a Professor at TIO University and Managing Director of the Global Anti-Scam Alliance (GASA) & ScamAdviser.



Clement Njoki is Editor and Researcher at GASA. His role involves creating engaging content about scams and fraud, simplifying complex financial information for various platforms. He also works on building GASA's online presence through blogs and news updates.

Clement possesses comprehensive expertise in identifying and combating deceptive practices and fraud, along with a strong background in cybersecurity.



Sam Rogers is GASA's Director of Marketing. Previously, he worked in Risk Advisory, before transitioning into a career as a researcher, copywriter, and content manager specialized in cutting-edge electrical engineering topics, such as photonics and the industrial applications of electromagnetic radiation.

Sam left the world of corporate industry seeking a role which would allow him to concentrate on networking and events management, while allowing him to contributing something worthwhile to society.



James Greening, operating under a pseudonym, brings a wealth of experience to his role as a scam investigator, content writer, and social media manager. Formerly the sole driving force behind Fake Website Buster, James leverages his expertise to raise awareness about online scams. He currently serves as a Content Writer and Social Media Manager for the Global Anti-Scam Alliance (GASA) and regularly contributes to ScamAdviser.com.

Join the Network to Beat a Network



INTELLIGENCE SHARING

Regular Virtual Meet-ups 8 Topic-based Email Groups 10,000 Professionals Newsletter

RESEARCH

Global State of Scams 30+ Regional Reports Policy Papers

NETWORKING

3 International Summits Online Member Directory National GASA Chapters

CYBERCRIME EXCHANGE

80+ Pooled Data Sources
Realtime Data Sharing
Access to Global Leaderboards

OUR FOUNDATION PARTNERS

amazon

Bitdefender.



















Disclaimer

This report is a publication by the <u>Global Anti-Scam Alliance</u> (GASA) supported by <u>ScamAdviser</u> and <u>Whoscall</u>. GASA holds the copyright 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. The authors permit 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

Email: partner@gasa.org X (Twitter): @ScamAlliance

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



