A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries

Mo Houtti, Abhishek Roy, Venkata Narsi Reddy Gangula, and Ashley Marie Walker

Abstract. Scams are a widespread issue with severe consequences for both victims and perpetrators, but existing data collection is fragmented, precluding global and comparative local understanding. The present study addresses this gap through a nationally representative survey (n = 8,369) on scam exposure, victimization, types, vectors, and reporting in 12 countries: Belgium, Egypt, France, Hungary, Indonesia, Mexico, Romania, Slovakia, South Africa, South Korea, Sweden, and the United Kingdom. We analyze six survey questions to build a detailed quantitative picture of the scams landscape in each country, and compare across countries to identify global patterns. We find, first, that residents of less affluent countries suffer financial loss from scams more often. Second, we find that the internet plays a key role in scams across the globe, and that GNI per capita is strongly associated with specific scam types and contact vectors. Third, we find widespread underreporting, with residents of less affluent countries being less likely to know how to report a scam. Our findings contribute valuable insights for researchers, practitioners, and policymakers in the online fraud and scam prevention space.

1 Introduction

Scams affect many people. A 2017 Federal Trade Commission (FTC) survey found that almost 16% of US consumers had been victims of fraud in the past year (Anderson 2019). This problem extends worldwide; a 2023 global survey by the Global Anti-Scam Alliance (GASA), a cross-stakeholder body, found that 78% of respondents had experienced a scam in the past year (Abraham et al. 2023). The material consequences of scams and fraud can be severe, extending far beyond moderate financial losses for consumers. There are many documented cases of individuals losing their life savings to scams, leading to severe material and emotional harm (Coakley 2024; Khandro 2024; Farivar 2022;

doi:10.54501/jots.v2i4.204

Kilmer 2023). In some cases, businesses have been destroyed by losing immense sums of money in a scam (Albright 2023). But even these facts focus on only one set of victims. The United Nations estimates that hundreds of thousands of human trafficking victims are forced by criminal organizations to carry out scams, often after being lured to a foreign country with false promises of a job opportunity (UN OHCHR 2024). In essence, the prevalence of scams has created lucrative opportunities for organized crime, with severe consequences for both victims *and* perpetrators.

The scope of this issue will likely become more important as internet access and the availability of digital payments continue to increase (FICO 2023). The growing prevalence and widespread access to generative AI tools, such as voice cloning and high-fidelity image manipulation technology, could also exacerbate the scam problem even further. For example, in a recent incident, perpetrators used AI-generated voice and images to impersonate a company's CFO, successfully tricking a Hong Kong finance worker into wiring $25.6 million to fraudulent bank accounts (Ianzito 2024). Proliferation of such tools could enable scams to be much more believable and harder for users to discern (Bethea 2024). Unless curbed, this could increase the likelihood of victimization, and potentially reduce trust in online interactions and transactions as a whole (FCC 2024).

To help better understand and combat this problem, governments around the world regularly collect data on scams in their local jurisdictions. The FTC, for example, conducts surveys and publishes detailed reports (Anderson 2019; Federal Trade Commission 2023) to map the landscape of scams in the United States. The European Commission assumes similar responsibilities in the EU (European Anti-Fraud Office 2024), and analogous data collection efforts happen in places like the United Kingdom (Jones 2022), Australia (Australian Bureau of Statistics 2024), and South Korea (Park 2023).

But despite these efforts, we do not have a good quantitative understanding of scams at a global level. Because data collection typically happens *within* jurisdictions, methodological differences make it impossible to compare findings across borders. While some global reports do exist, they either compile data from existing sources or use survey methodologies that do not achieve population-representative samples (e.g., Abraham et al. (2023) and Lewis, Malekos Smith, and Lostri (2020)). Some industry firms (e.g., NortonLifeLock (2022)) have conducted representative global surveys, but these have tended to be more high-level and are therefore insufficiently granular to let us draw precise and practical conclusions about the global scams landscape. This in turn hinders policymakers, practitioners, and researchers from identifying and targeting scams in contextually appropriate ways.

To address this gap, we conducted a nationally representative survey (n = 8,369) in 12 countries: Belgium, Egypt, France, Hungary, Indonesia, Mexico, Romania, Slovakia, South Africa, South Korea, Sweden, and the United Kingdom. The survey asked people about their experiences with scams, including the type of scam they had most recently experienced, the vector through which they experienced the scam, whether they had sent the scammer money, and whether/where they reported the scam. Importantly, we ask these questions through a global and nationally representative survey, making it possible to draw true comparisons and contrasts between countries. This provides a two key advantages. First, it lets us contextualize local findings. If we find that 25% of South Africans report having lost money from a scam in the past year, is that a lot? According to our survey, the answer in this case is yes—but this argument would be much more difficult to make in the absence of global data. Second, while not a perfect substitute for *comprehensive* global data, analyzing scam data across a broad spectrum of countries can help resource-constrained governments prioritize their efforts. If consistent scam types emerge across diverse economies, or if similar economies suffer from specific scam types, they can be valuable signals to guide local data collection and enforcement efforts. Concretely, the survey let us answer the following research questions in multiple countries:

- RQ1: How common are scam exposure and victimization?
- RQ2: How prevalent are specific scam types?
- RQ3: To what extent are scams technology-mediated?
- RQ4: How comprehensive are reporting-based data sources about scam victimization?

We present several useful findings, from which we contribute concrete takeaways for researchers, practitioners, and policymakers in the online safety and fraud prevention spaces. First, we find that residents of less affluent countries suffer financial loss from scams more often. Second, we find that the internet plays a key role in scams across all surveyed countries, but that gross national income (GNI) per capita is strongly correlated with specific scam types and contact methods from scammers. For example, money-making scams are more common in less affluent countries. Third, we find widespread underreporting of scams. On overage, half of those exposed to a scam in a given country do not report it at all—and residents of less affluent countries are more likely to not know how to report a scam.

2 Background

2.1 Scam Exposure and Victimization

Scams are a growing issue, with losses from reported scams increasing at a rapid rate. Industry surveys and reports compiled by law enforcement are the primary sources of scam prevalence data. The FBI's Internet Crime Report 2023 showed that losses grew at upwards of 20% year over year in the last three years (FBI 2023). GASA's State of Scams 2023 report estimated that losses from scams topped $1 trillion in 2023 and accounted for about 1% of global GDP (Abraham et al. 2023). While estimates for exposure to scams vary widely across surveys and countries, it is generally accepted that the exposure to scams is increasing year over year. GASA's 2023 report stated that 78% of participants experienced at least one scam in the past 12 months.

The GASA report estimated that developing countries like Kenya, Vietnam, Thailand, and Brazil lost more than 3% of their GDP to scams (Abraham et al. 2023). A 2020 survey commissioned by the European Commission (EC) found that the exposure to fraud is generally higher in "connected countries," identified as countries with a relatively high proportion of individuals making internet purchases (European Commission 2020). In the context of online scams, increased internet activity (e.g., online purchases) expands the pool of potential targets and the opportunities for motivated offenders (Kigerl 2011; Felson and Cohen 1980; Miró 2014). Prior research indicates that a variety of psychological (e.g., overconfidence, optimism bias), sociodemographic (e.g., age, education) and situational factors (e.g., emotional distress, financial strain) play a role in susceptibility to scams (Whitty 2019; Modic and Lea 2014; Button et al. 2014).

In this study, we looked at how the exposure and victimization to scams vary across geographies.

2.2 Scam Types and Technology's Role in Scams

Scams are heterogeneous and evolve based on a variety of factors, such as emerging technologies (e.g., cryptocurrency), changing communication channels (e.g., social media), and global events (e.g., the COVID-19 pandemic, the Russia-Ukraine war) (Xu et al. 2022). Scammers adapt their methods based on the individual circumstances of their targets, ranging from preying on financial vulnerabilities through lottery scams to exploiting loneliness through romance scams. While attempts have been made by multiple government agencies and researchers, there is still no universally accepted classification of scams. DeLiema, Li, and Mottola (2022) classify consumer fraud into four categories: opportunity-based scams, threat-based scams, consumer purchase scams, and phishing scams. In contrast, FINRA's Financial Fraud Research Center has developed a framework for a taxonomy of fraud modeled after international crime classification systems (Beals, DeLiema, and Deevy 2015). In this study, we used a scam classification based on the role scammers play and the service they purportedly offer to understand the prevalence of such scams.

As stated earlier, scammers take advantage of technological advances to effectively reach and scam their targets. Scammers use a variety of communication channels such as phone calls, text messages, emails, social media, and mobile apps to establish contact with their targets. Scammers also leverage advances in payment methods, with the emergence of irreversible payment methods such as real-time payments, cryptocurrency, digital wallets, etc. Notably, scams using cryptocurrency have skyrocketed; the FTC reports that cryptocurrency scams make up more than 85% of losses due to investment scams (Federal Trade Commission 2023). In this study, we looked at how scammers use technology to reach their targets and receive payments across countries of interest.

2.3 Limitations of Reporting-based Data Sources

Despite scams leading to devastating financial losses and causing enormous psychological distress to victims (Munton and McLeod 2023), they are highly underreported to authorities. The FTC estimates that only 10–12% of scams are actually reported to them (Federal Trade Commission 2023). Deliema, Shadel, and Pak (2019) show that scams are underacknowledged and underreported even in survey research, likely due to social desirability bias or refusal to acknowledge victimization. In the limited studies that surveyed known victim pools, only about half of known fraud victims admitted to being defrauded (Button, Lewis, and Tapley 2009b; FINRA Foundation 2007). This shows that survey-based estimates are better than reporting-based estimates to assess scam prevalence and victimization.

While reports like those from the FBI and industry players provide valuable information, they suffer from methodological disadvantages that hinder their representativeness. Reports based on complaint data do not provide a complete picture, as scams are severely underreported to government agencies. Some surveys by industry players are global but often focus on a narrow aspect of the problem, such as real-time payments-based scams or text message scams, or have representativeness issues. Through this survey, we looked at scam exposure, victimization, and reporting attitudes across regions using a representative sample of participants in order to identify regional disparities and inform targeted prevention and intervention strategies.

3 Methods

3.1 Survey Overview

The questions analyzed in this paper were part of a larger survey covering a variety of digital safety issues. The survey was deployed through Morning Consult (MC)—a leading survey research firm—using a mixed-panels approach, which leverages the strengths of different data collection methods to create a more comprehensive and representative picture of public opinion. MC uses roughly 55 survey panel providers to conduct interviews across numerous countries. This panel network provides access to tens of millions of survey respondents via recruitment from thousands of websites, mobile apps, social networks, email lists, and publishers. They use a wide mix of panel providers with different recruitment methods to diversify their respondent pools and ensure maximal access to different respondent groups. Recruited participants completed the survey online, using mobile or desktop devices.

Twelve countries were surveyed: Belgium, Egypt, France, Hungary, Indonesia, Mexico, Romania, Slovakia, South Africa, South Korea, Sweden, and the United Kingdom. Questions were translated by teams with native speakers in the target languages through a process consisting of translation, editing, proofreading, and quality assurance. Demographic factors used for stratified sampling and weighting varied by country to account for contextual factors such as the availability of reliable census data. Weights and sample targets were based on general population proportions for adults (18 years and older) in Belgium, Egypt, France, Hungary, Indonesia, Romania, Slovakia, South Korea, Sweden, and the UK. Mexico and South Africa have internet access penetration below 80%, and people without access to the internet are more likely to fall into lower education demographics. Therefore, to avoid overrepresenting adults with lower education, weights and sample targets for those two countries were based on internet population proportions for adults (18 years and older). Responses were weighted using standard raking procedures (Battaglia, Hoaglin, and Frankel 2009). Table 1 reports the demographic factors used to derive sample targets and weights in each country.

Table 1: Demographic factors used for stratified sampling and weighting in each country.

Country	Sample size	Sample targets based on	Weighting dimensions
Belgium	504	Age, gender	Age, gender, education, region
Egypt	740	Age, gender	Age, gender, education, region
France	738	Age, gender	Age, gender, education, region
Hungary	527	Age, gender	Age, gender
Indonesia	752	Age, gender	Age, gender, education, region
Mexico	778	Age, gender, education	Age, gender, education, region
Romania	761	Age, gender	Age, gender, education, region
Slovakia	724	Age, gender	Age, gender
South Africa	773	Age, gender, education	Age, gender
South Korea	782	Age, gender	Age, gender
Sweden	533	Age, gender	Age, gender, education, region
United Kingdom	757	Age, gender, education	Age, gender, education, region

3.2 Survey Questions

We used the FTC's online fraud reporting tool (FTC 2024) as a guide when formulating our survey questions. This let us ensure that the questions captured the kind of information about scams that is useful to government institutions and that the multiple-choice options adequately covered common scam experiences. To account for the likelihood of multiple scam experiences, respondents were instructed to answer questions based on their most recent scam experience (if any) in the past year. We reasoned that respondents might have trouble recalling details of earlier scam experiences, making their reports less reliable. Obtaining a cross-section of the most recent scam experiences would also closely approximate the breakdown of scam experiences overall while letting us simplify the survey for respondents.

While “scams” and “fraud” technically have different definitions, the two terms are often used interchangeably to refer to attempts to trick someone for monetary gain. Indeed, the aforementioned FTC reporting tool (FTC 2024) does not distinguish between the two. Rather than providing a narrow definition that might unintentionally exclude instances commonly considered to be scams, we decided to mirror the FTC and rely on respondents' colloquial understanding of the term.

Recall that we articulated four research questions. We state each research question before its corresponding survey questions.

RQ1: *How common are scam exposure and victimization?*

We analyzed responses to Q1 to understand the frequency with which internet users are exposed to and materially harmed by scams:

Q1: ***In the past year, have you been the target of a scam?***

- Yes, I have been the target of a scam, but I did not lose money.
- Yes, I have been the target of a scam and I did lose money.
- I have not been targeted by any scams.
- I do not know if I've been targeted by a scam.

RQ2: *How prevalent are specific scam types?*

We analyzed Q2 to understand the types of scams internet users experience:

Q2: ***What kind of scam were you targeted by? Choose the one that most accurately describes your experience.***

- An impersonator (e.g., fake government, business, love interest, grandchild)
- Job, investment, money-making opportunity, franchise
- Phone, internet, TV service
- Health (e.g., weight loss, eye care, treatment)
- Online shopping (e.g., fake stores/pages)
- Sweepstakes, prize, lottery
- Auto sale, repair
- Credit, debt, loan (e.g., debt collection, credit report, student loan debt relief)
- Something else

RQ3: *To what extent are scams technology-mediated?*

Responses to Q3 and Q4 let us understand to what extent users' scam experiences are technology-mediated. Q4 was only given to respondents who indicated they had directly sent the scammer money in a separate question.

Q3: ***How did it start (e.g., how did they first contact you, where did you see an ad)?***

- Phone call

- Social media (e.g., Facebook/Meta, Instagram)
- Online ad or Pop-up
- Website or App (e.g., Craigslist, OfferUp, Marketplace)
- Messaging app (e.g., Google Hangouts, WhatsApp)
- Email
- Text
- Mail
- In-person
- TV or Radio
- Print media (e.g., newspaper, magazine)
- Other (please specify)

Q4: ***How did you pay or send the money?***

- Scammer transferred from my account without my consent
- Paid through a payment or banking app on phone
- Paid via a payment or banking website on computer
- Mailed cash, cheque, or money order
- Bought gift cards & shared the details with the scammer
- Other (please specify)

RQ4: *How comprehensive are reporting-based data sources about scam victimization?*

Finally, Q5 and Q6 let us contextualize the current research information landscape on scams, which often relies heavily on reporting-based data.

Q5: ***Did you report the scam to anyone?***

- Yes
- No
- I wanted to, but didn’t know how

Those who did report the scam were asked:

Q6: ***Who did you report the scam to?***

- To a financial authority (e.g., bank)
- To the service provider (e.g., Cisco, IBM, McAfee)
- To the authorities (e.g., the police)
- To my email provider
- To the online security provider
- To my network provider
- To my family (who take action on my behalf)
- To my work/place of education

3.3 Analysis

For each survey question, we report the weighted percentage of respondents who selected each multiple-choice option in a heatmap. Countries are ordered along the x-axis by ascending GNI per capita in 2021 (the most recent year for which complete data was available). Where the heatmaps suggest possible GNI-based patterns among the most frequently selected or most pertinent options, we compute Spearman's rank-order correlations to verify and quantify the associations.

4 Results

RQ1: *How common are scam exposure and victimization?*

4.1 Users in Less Affluent Countries Are at Greater Risk

On average, 15% of a country's internet users lost money from scams in the past year (Figure 1). Our results also reveal a troubling pattern: internet users in less affluent countries are at greater risk of falling victim to scams. South Africa, for example, had a GNI per capita of $12,948 and the highest scam victimization rate at 25%. South Korea, with a GNI per capita of $44,501, had less than a third of South Africa's victimization rate (7%). We found a strong inverse correlation between GNI per capita and scam victimization rate (ρ = -0.73, p = 0.007). This is especially concerning because lower incomes in countries with lower GNI per capita make it more difficult for victims to recover from financial loss.

4.2 Scam Exposure Does Not Reduce Victimization Rate

Some countries with low rates of scam exposure nevertheless have a high rate at which those who do experience scams actually suffer losses (e.g., Egypt, Mexico, and Sweden). Users in these countries may simultaneously be well protected from *exposure* to scams, but not resilient against scams themselves. Indeed, one could reasonably hypothesize that less frequent scam exposure might make users less alert and therefore less resilient overall.

However, we found no correlation in either direction between the scam loss rate—the top row in Figure 1—and scam exposure rate—the sum of the following two rows (ρ = 0.04, p = 0.90). This suggests a more complicated relationship between scam exposure and avoidance of financial loss from scams, with additional factors possibly at play. For example, countries where users are frequently exposed to scams may become more resilient in *absolute* terms, but be targeted using more sophisticated techniques in response. This kind of tailoring would be consistent with the results we cover next, demonstrating some differences in scam types and communication vectors based on countries' affluence.

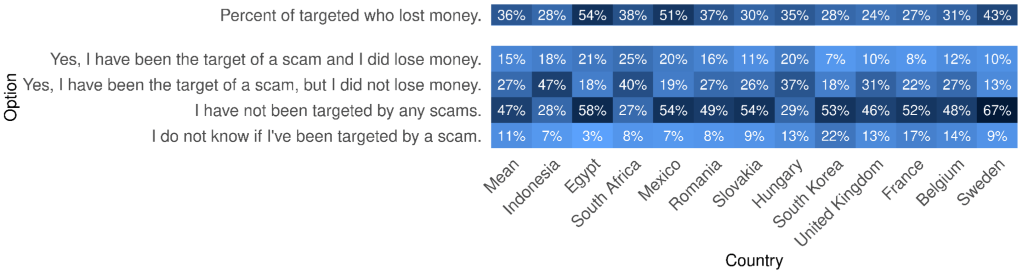


Figure 1: Weighted within-country proportions of responses to Q1: *In the past year, have you been the target of a scam?* Darker colors gradually indicate higher values. The top row describes the percent who lost money among those who experienced a scam; it is computed from the two rows immediately below it.

RQ2: *How prevalent are specific scam types?*

4.3 Top Scam Types Are Fairly Consistent Across Countries

The two most common scam types were online shopping and money-making scams (Figure 2). There were only two countries where neither of these was the most-selected option: Indonesia's was sweepstakes/lottery scams (30%), and South Korea's was impersonation scams (28%). In both cases, however, money-making and online shopping scams were still in second and third place, respectively.

Despite this consistency, we did see differences based on countries' economies. Money-making scams were more common in less affluent countries; GNI per capita and the prevalence of money-making scams had a very strong inverse correlation (ρ = -0.90, p < 0.001). The prevalence of online shopping scams was not significantly correlated with GNI per capita (ρ = 0.44, p = 0.15).

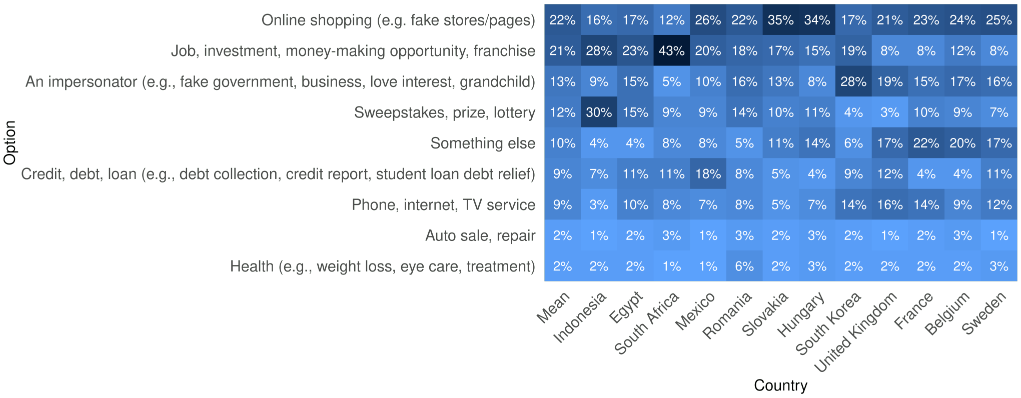
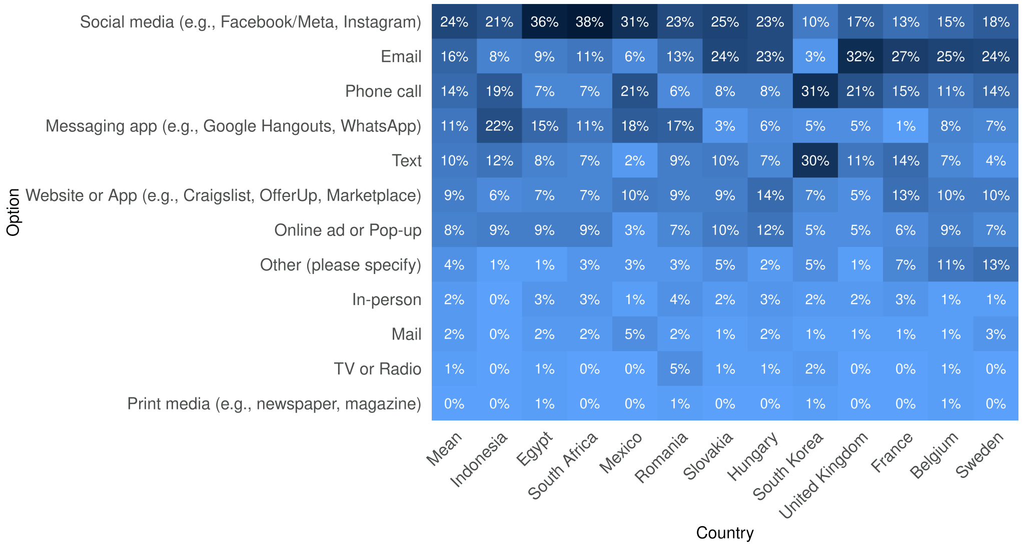


Figure 2: Weighted within-country proportions of responses to Q2: *What kind of scam were you targeted by? Choose the one that most accurately describes your experience.* Darker colors gradually indicate higher values.

RQ3: *To what extent are scams technology-mediated?*

4.4 From First Contact to Payment, the Internet Plays a Key Role

Consistent with FTC reports in the US (Federal Trade Commission 2023), the most common method of first contact across countries (Figure 3) was social media (24%), followed by email (16%) and phone (14%). On average, 68% of those exposed to a scam in a country had first contact with a scammer through an internet-based technology (social media, email, messaging app, website or app, or online ad or pop-up). Social media and messaging apps were more common as initial contact methods in less affluent countries, while email-based scams were more prominent in more affluent countries. GNI per capita had a strong inverse correlation with the prevalence of social media (ρ = -0.71, p = 0.009) and messaging apps (ρ = -0.65, p = 0.02) as first contact methods, and a strong positive correlation with email (ρ = 0.67, p = 0.02). Interestingly, South Korea was a major outlier in our data; phone calls and texts were the most common contact methods there, with internet-based methods making up only 30%.



Option	Mean	Indonesia	Egypt	South Africa	Mexico	Romania	Slovakia	Hungary	South Korea	United Kingdom	France	Belgium	Sweden
Social media (e.g., Facebook/Meta, Instagram)	24%	21%	36%	38%	31%	23%	25%	23%	10%	17%	13%	15%	18%
Email	16%	8%	9%	11%	6%	13%	24%	23%	3%	32%	27%	25%	24%
Phone call	14%	19%	7%	7%	21%	6%	8%	8%	31%	21%	15%	11%	14%
Messaging app (e.g., Google Hangouts, WhatsApp)	11%	22%	15%	11%	18%	17%	3%	6%	5%	5%	1%	8%	7%
Text	10%	12%	8%	7%	2%	9%	10%	7%	30%	11%	14%	7%	4%
Website or App (e.g., Craigslist, OfferUp, Marketplace)	9%	6%	7%	7%	10%	9%	9%	14%	7%	5%	13%	10%	10%
Online ad or Pop-up	8%	9%	9%	9%	3%	7%	10%	12%	5%	5%	6%	9%	7%
Other (please specify)	4%	1%	1%	3%	3%	3%	5%	2%	5%	1%	7%	11%	13%
In-person	2%	0%	3%	3%	1%	4%	2%	3%	2%	2%	3%	1%	1%
Mail	2%	0%	2%	2%	5%	2%	1%	2%	1%	1%	1%	1%	3%
TV or Radio	1%	0%	1%	0%	0%	5%	1%	1%	2%	0%	0%	1%	0%
Print media (e.g., newspaper, magazine)	0%	0%	1%	0%	0%	1%	0%	0%	1%	0%	0%	1%	0%

Figure 3: Weighted within-country proportions of responses to Q3: *How did it start (e.g., how did they first contact you, where did you see an ad)?* Darker colors gradually indicate higher values.

Mobile apps were a key vector for payments to scammers. Mobile-based payments were almost twice as common as computer-based ones (Figure 4). This pattern held across most countries—France and Belgium were the only exceptions. This may simply reflect online banking habits across countries, but it nonetheless provides good evidence that scam prevention should include a focus on mobile payments, and it further substantiates reports calling out the risks of the increasing global adoption of real-time payments (RTP) (FICO 2023). The prevalence of mobile-based payments to a scammer had a strong inverse correlation with GNI per capita (ρ = -0.79, p = 0.002), suggesting the adverse effects of RTP adoption may be more prominent in less affluent countries.

RQ4: *How comprehensive are reporting-based data sources about scam victimiza-*

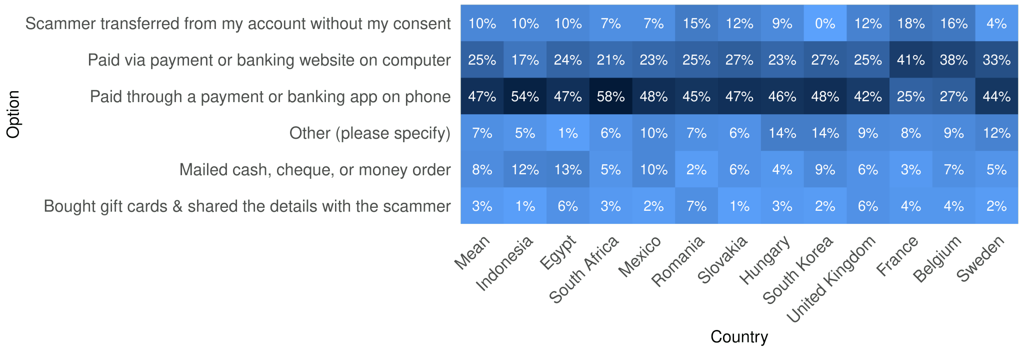


Figure 4: Weighted within-country proportions of responses to Q4: *How did you pay or send the money?* Darker colors gradually indicate higher values.

tion?

4.5 Many Scams Go Unreported

Our findings substantiate the widespread understanding that scams are underreported, and provide quantitative evidence of the extent to which this is true globally. On average, over a third (37%) of a country's scam victims did not report the scam to anyone (Figure 5). In Slovakia and South Korea, that number was closer to half (50% and 54%, respectively). Users in less affluent countries more often wanted to report scams but did not know how (ρ = -0.82, p = 0.001). This suggests that inferences based on victim reports are likely to suffer more underreporting bias in resource-constrained countries, where survey data is also less likely to exist.

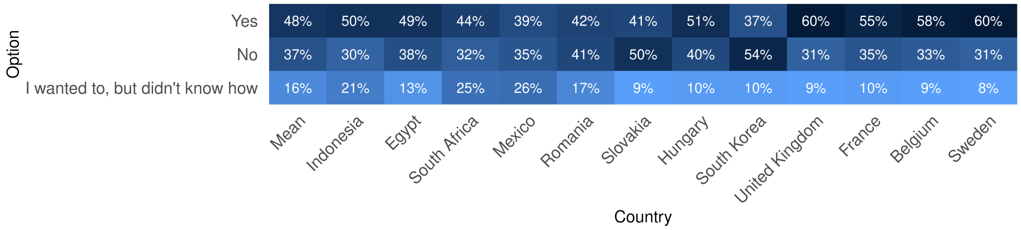


Figure 5: Weighted within-country proportions of responses to Q5: *Did you report the scam to anyone?* Darker colors gradually indicate higher values.

Reporting to government authorities constituted an even smaller fraction of these totals (Figure 6). Of those who reported scams, less than a third (27%) reported them to the authorities. This varied widely by country—e.g., 57% of South Koreans who reported scams reported them to authorities versus only 16% of South Africans. GNI per capita did not correlate significantly with reporting to either authorities (ρ = 0.47, p = 0.12) or financial institutions (ρ = 0.19, p = 0.56), though the proportions may reflect the degree to which victims in each country believe a particular institution may be able to take action for them (e.g., retrieve their lost money).

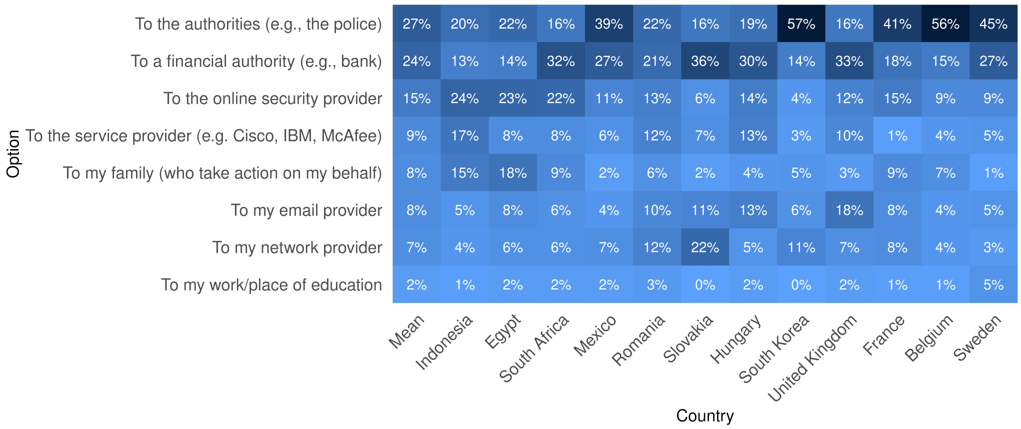


Figure 6: Weighted within-country proportions of responses to Q6: *Who did you report the scam to?* Darker colors gradually indicate higher values.

5 Discussion

Scams are a widespread and growing problem affecting people worldwide. The recent cost-of-living crisis (EIU 2023) has exacerbated the financial impact of scams, leaving victims even more vulnerable. Greater rates of financial loss from scam victimization coupled with more difficulty recovering from financial loss (due to low income) in less affluent economies make this issue worth even more attention. Consequently, governments, central banks, industry, and civil society around the world have responded with various tools in their arsenal, from public awareness campaigns to regulations (Stainsby and Eastwood 2023).

The lack of standardized data hinders our ability to understand and address scam victimization effectively. Without a global survey on scam prevalence and victimization, it is hard to accurately assess and describe the true size of the issue, develop effective solutions, or bring appropriate resources to bear. Our work tries to fill in some of the gaps in terms of understanding who is most at risk, and to what types of scams, so regulators and industry can better target their interventions. Furthermore, as our numbers on contact method and payment method show, the scams landscapes in countries with low GNI per capita often look different, so minority-world-focused solutions are likely not going to be as effective in the majority world. This survey aims to fill that gap in literature.

In this section, we highlight some of the key drivers of scam victimization across countries as demonstrated by our findings, and define a multilevel structural approach to fight back against this issue.

5.1 Drivers of Scam Victimization Across Countries

While the specific tactics and methods used by scammers vary across countries, there are several common tailwinds and themes contributing to the widespread vulnerability and victimization to scams.

5.1.1 Widespread and fast adoption of digital payment systems globally post-COVID-19 appears to be a key driver in increased scam prevalence.

As we show in Figure 4, digital payment solutions are involved in a large fraction of the scams incidents across all the countries we surveyed. This observation mirrors the growth of the total number of non-cash transactions happening globally, which is estimated to accelerate to $2.3 trillion by 2027, growing at a rate of 15% annually (Capgemini 2023).

Frauds and scams are not, however, unique to digital payment systems. While digital payment systems are fast and convenient, and thereby have a large volume, they often offer limited recourse for victims as compared to other modes of payment like credit cards. With the adoption of such payment systems there has been a massive growth in economic activity, but this has also increased the total number of scam activities over time. For example, the UK's Payment Systems Regulator (PSR) found 0.1% of fast payments in 2021 were fraudulent—well above the global average of 0.03% for card transactions (World Bank 2023). While this trend of growth in adoption of digital payments has implications for the total volume of scams occurring globally, it is particularly pertinent in the Asia-Pacific region, where non-cash transactions seem to be growing at an estimated rate of 19.8% annually (Capgemini 2023). The type of scams that are prevalent vary country to country, but it appears that focusing research and enforcement efforts on scams facilitated through digital payment services is a productive intervention space.

5.1.2 Scams follow where users go online, and locale-specific factors are highly salient in understanding specific scam victimization.

As we show in Figure 2, the types of scams that are popular differ by country, but there seems be a trend of scammers using hooks that are most likely to yield results in their target locales. For example, a high rate of gambling-related scams in Indonesia is correlated with a rapid rise in the illegal gambling industry in the country; one PPTAK (Indonesian Financial Transaction Reports and Analysis Center) spokesperson noted that the turnover in this industry grew from Rp57 trillion in 2021 to Rp81 trillion in 2022 (Bhwana 2023). Similarly, we note that the high rate of jobs scams in South Africa is correlated with South Africa having one of the highest unemployment rates in the world at 32.1%, signifying that scammers are preying on a large market of job-seekers in the market (Manamela and Phoshoko 2024).

5.1.3 Scams are severely underreported, creating ecosystem-wide blind spots.

Since globally only about half the scams are reported to authorities, the current national-level estimates of scam victimization and prevalence are most likely highly underestimated (see Figure 5). This trend of underreporting is especially pronounced in countries like Indonesia, South Africa, and Mexico, where more than 1 in 5 users reported being unable to report scams to authorities due to unclear reporting mechanisms. As we discuss further in the next section, generating public awareness of reporting tools and mechanisms available to the general public could be a productive intervention.

The low effective rates of enforcement against scams and low likelihood of loss recovery may also play a role in discouraging victims from reporting scams to authorities (Dolgin and Currier 2023). For example, the 2023 State of Scams in Asia report by GASA found that there was a positive correlation between the recovery of financial losses and people's willingness to report scams to authorities (Global Anti-Scam Alliance 2023). Another recent report by Third Way, a public policy think tank, estimated that in the US the enforcement rate for reported incidents to the Internet Crime Complaint Center (IC3) was 0.3% (Eoyang et al. 2018). Governments and central banks must allocate more resources to law enforcement agencies, streamline reporting mechanisms, and ensure that people have access to proper redressal mechanisms.

5.2 Addressing the Scam Problem: Potential Interventions

Scam victimization erodes consumer trust, jeopardizes businesses, and harms the broader economy. A multifaceted, targeted intervention approach is necessary to develop and assess the effectiveness of various intervention approaches. As we show in Section 4.4, internet-based communication methods play a critical mediating role in victimization. Prior work in this area has classified scams along the following broad categories (DeLiema, Li, and Mottola 2022):

1. Opportunity-based scams: typically involves some monetary, social, or emotional reward-based hook.

2. Threat-based scams: typically involves threats of negative consequences and blackmail.

3. Consumer purchase scam: typically happens during online shopping or marketplace interactions.

4. Phishing scams: often involves techniques like impersonation of a person/entity that victims trust. This is then parlayed to elicit either money or sensitive information from the victim.

As we show in Section 4.3, the top scam types remain fairly consistent across surveyed countries; the most popular scam channels were shopping (consumer purchase scam), job/investment (opportunity-based scam) and impersonation-based scams (phishing, romance or friends/family impersonation scams). This bodes well for an approach that targets and educates users about the underlying manipulation techniques used in these scams, strengthens the resilience of such channels themselves, and raises overall awareness. For countries with outlier patterns, like Indonesia (high victimization from lottery scams), South Africa (high victimization from job-based scams), and South Korea (impersonation and romance scams), it would make sense to take a more "white glove" approach, where the public and private sectors collaborate to target and curb these trends.

Recognizing that users are often the weakest link in the scam ecosystem (Baral and Arachchilage 2019), we must prioritize strategies to enhance their resilience. A multifaceted approach, akin to a "swarm the problem" strategy, is necessary to develop and assess the effectiveness of various intervention approaches. This area is ripe with opportunities to borrow from intervention tool kits developed and tested against other forms of online harms like misinformation (Kozyreva et al. 2024). We provide several examples next.

5.2.1 General awareness campaigns

Public awareness campaigns help raise awareness of common scam tactics and warning signs, and can theoretically help the broader public to recognize and avoid potential threats (Miller 1983). Having some preexisting familiarity with scam types has been shown to help individuals better manage risks, but while general awareness campaigns are one of the most prominent intervention strategy deployed by stakeholders, its efficacy in bolstering user resiliency is mixed and unproven (Downs, Holbrook, and Cranor 2006; Jensen, Gerlings, and Ferwerda 2024). There is some research showing efficacy of such campaigns in raising awareness about reporting channels, and in that capacity this could be a tool of interest for stakeholders to potentially alleviate the problem of underreporting that we noticed across most countries (Burke, Perez-Arce, et al. 2022).

5.2.2 Behavioral nudges and credibility cues

Embedding lightweight behavioral nudges might be a good low-friction way to guide users toward safer online practices (Pennycook et al. 2021). For instance, research has shown that using attention prompts to verify if someone is receiving or sending money on a fast payment app can significantly reduce the risk of falling victim to scams that rely on the user not paying attention and sending money instead of receiving it (Jha and Delima 2022). Furthermore, since impersonation-based scams are prevalent across all surveyed countries and users rely on visual trust indicators to assess credibility online (Jakobsson et al. 2007), another intervention worth exploring more broadly would be to provide users with additional credibility cues (e.g., verification check marks) for verified accounts across platforms. As we show in Figure 3, since most scams begin from platforms like social media, emails, phone calls, and text messages, adding positive credibility cues (like verification check marks) or negative credibility cues (like potential spam labels) could forewarn individuals and help guide them toward making safer interaction decisions online.

5.2.3 Inoculation-styled interventions

Scammers often rely on a handful of manipulation techniques to trick their victims into falling for scams. Like vaccines, inoculation-style interventions expose users to weaker forms of these techniques in a controlled environment to help them build immunity or “mental antibodies” to real-world threats (McGuire 1961). Prior research has attempted to map out victims’ user journeys and understand what manipulation techniques are at play, particularly for romance scams (Whitty 2013). Building on this, future research could replicate such mapping to the three most popular scam journeys across countries: consumer purchases online, opportunity-based scams (job/investment), and impersonation-based scams (phishing, romance and family/friend impersonation). Users can then be *inoculated* against these manipulation techniques and tactics. For example, Robb and Wendel (2022) showed that there is strong evidence that inoculation techniques increased users’ ability to detect SSN scam emails (government impersonation) as compared to general tips about scams.

5.2.4 Digital and financial literacy-based interventions

Since scammers prey on the lack of digital and financial literacy among new and habitual internet users, an effective preventative measure could be deploying low-cost, comprehensive intervention programs that equip individuals with the knowledge and skills to navigate the digital landscape safely, critically evaluate information, and make informed decisions (McGrew and Breakstone 2023). Research has shown that educational interventions can reduce susceptibility to financial fraud pitches (Burke, Kieffer, et al. 2022). While digital literacy is known to enhance resilience (Graham and Triplett 2017), the field lacks interventions comparable to those addressing misinformation (Kozyreva et al. 2024). Such tools could be powerful interventions against opportunity-based scams, particularly those that involve investment schemes preying on individuals with low financial literacy.

5.3 Scope for Future Research

To effectively combat scams, we need a more comprehensive understanding of the phenomenon. While quantitative data, such as that presented in this study, helps to gauge the scale of victimization, we also need equally powerful qualitative research to better understand the issues uncovered in this study, particularly in less affluent countries. In-depth qualitative research, particularly in the following areas, could help tailor effective interventions and policies.

5.3.1 Understanding lived experiences of scam victims

Scam victimization leaves behind profound and lasting scars. Beyond immediate impacts, like financial hardships, and emotional repercussions, like feelings of shame, anger, and betrayal, victimization can lead to long-term instabilities and social isolation if victims lose trust in those around them (Cross 2018; Button, Lewis, and Tapley 2014; Whitty and Buchanan 2015). But while qualitative research related to the lived experiences of victims in more affluent countries has been insightful, the experience of victims in non-affluent countries largely remains a blind spot. Findings from Section 4.1 in this study underscore an urgent need for such studies, as GNI per capita and scam victimization rates were strongly negatively correlated. Understanding victims' coping strategies, whether seeking support, changing their behavior, or even withdrawing, is critical for developing effective support from industry and policymakers.

5.3.2 Understanding vulnerability and resilience

As we discuss in Section 4.2, while top scam types remain fairly consistent across surveyed countries, scam exposure and victimization rates vary across countries. This suggests that there is a complex interplay of factors contributing to vulnerability and resilience among populations across these countries. Prior research has identified demographic factors (like income, age, and education), psychological traits, and risky online behavior as key contributors to victimization (Vitak et al. 2018; Modic, Anderson, and Palomäki 2018; Whitty 2020; Norris, Brookes, and Dowell 2019; Modic and Lea 2014). We find that while demographic factors like income and internet access are linked to scam victimization, financial losses stemming from victimization is more common in less affluent countries, even when controlling for internet access. This suggests that factors such as cultural attitudes toward risk, financial/digital literacy, and access to information and support could also play a role in resilience, warranting further research.

5.3.3 Identifying barriers to scam reporting in countries with low reporting

The underreporting of scams, particularly in less affluent countries where individuals lack awareness of or access to reporting mechanisms, hinders efforts to understand and address the issue, as highlighted by our results (see Figure 5). Prior research has shown that shame, stigma, and fear of retaliation or judgment often prevent victims from seeking help or reporting scams, particularly in romance scams (Havers et al. 2024). Distrust in authorities and victim-blaming further deter victims from reporting (Button, Lewis, and Tapley 2009a). The complexity of reporting processes can also be a barrier, especially considering victims' post-victimization state of mind (Button, Tapley, and Lewis 2012). It is likely that this problem can be addressed with increased focus on qualitative research in such areas to understand underlying factors leading to low reporting in these countries.

6 Conclusion

Through a nationally representative, multi-country, scams-focused survey, the present study addresses a substantial gap in our understanding of the global scams landscape. Our findings substantiate recent theories about the role of real-time payments in facilitating scams' proliferation, and highlight the value of consistent scams reporting across countries to help us understand regional issues in context. By analyzing data from a diverse range of economies and cultures, we contribute important insights for researchers, practitioners, and policymakers in online fraud and scams prevention.

References

Abraham, Jorij, Marianne Junger, Loka Koning, Clement Njoki, and Sam Rogers. 2023. *State of Scams Report 2023.* Technical report. Global Anti-Scam Alliance.

Albright, Amanda. 2023. "A $12 Million Request to Cover a Crypto Scam Sank a Bank CEO." *Bloomberg News* (September 27, 2023). https://www.bloomberg.com/news/articles/2023-09-27/crypto-scam-led-to-demise-of-heartland-tri-state-bank.

Anderson, Keith B. 2019. *Mass-Market Consumer Fraud in the United States: A 2017 Update.* Technical report. Federal Trade Commission, October. https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf.

Australian Bureau of Statistics. 2024. *Personal Fraud,* March 20, 2024. https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release.

Baral, Gitanjali, and Nalin Asanka Gamagedara Arachchilage. 2019. "Building Confidence Not to Be Phished Through a Gamified Approach: Conceptualising User's Self-Efficacy in Phishing Threat Avoidance Behaviour." In *2019 Cybersecurity and Cyberforensics Conference (CCC),* 102–10. IEEE, October 3, 2019. https://doi.org/10.1109/CCC.2019.000-1.

Battaglia, Michael P., David C. Hoaglin, and Martin R. Frankel. 2009. "Practical Considerations in Raking Survey Data." *Survey Practice* 2, no. 5 (May 31, 2009): 1–10. ISSN: 2168-0094. https://doi.org/10.29115/sp-2009-0019.

Beals, Michaela, Marguerite DeLiema, and Martha Deevy. 2015. "Framework for a Taxonomy of Fraud." *Financial Fraud Research Center,* https://www.finrafoundation.org/sites/finrafoundation/files/framework-taxonomy-fraud.pdf.

Bethea, Charles. 2024. "The Terrifying A.I. Scam That Uses Your Loved One's Voice." *The New Yorker* (March 7, 2024). https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice.

Bhwana, Petir Garda. 2023. "OJK Blocks 1,700 Bank Accounts Linked to Online Gambling." *Tempo* (October 10, 2023). https://news.worldcasinodirectory.com/indonesia-blocks-1700-bank-accounts-involved-in-online-gambling-market-with-12-billion-handle-110668.

Burke, Jeremy, Christine Kieffer, Gary Mottola, and Francisco Perez-Arce. 2022. "Can Educational Interventions Reduce Susceptibility to Financial Fraud?" *Journal of Economic Behavior & Organization* 198 (June): 250–66. ISSN: 0167-2681. https://doi.org/10.1016/j.jebo.2022.03.028.

Burke, Jeremy, Francisco Perez-Arce, Christine Kieffer, Robert Mascio, Gary Mottola, and Olivia Valdes. 2022. *Can Educational Interventions Reduce Susceptibility to Financial Fraud?* Technical report. FINRA Foundation, March 28, 2022. https://doi.org/10.1016/j.jebo.2022.03.028.

Button, Mark, Chris Lewis, and Jacki Tapley. 2009a. *A Better Deal for Fraud Victims: Research into Victims' Needs and Experiences.* National Fraud Authority. https://pure.port.ac.uk/ws/portalfiles/portal/1924328/NFA_Report_1_15.12.09.pdf.

———. 2009b. *Fraud Typologies and the Victims of Fraud: Literature Review.* National Fraud Authority. https://pure.port.ac.uk/ws/portalfiles/portal/1926122/NFA_report3_16.12.09.pdf.

———. 2014. "Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families." *Security Journal* 27, no. 1 (February 1, 2014): 36–54. https://doi.org/10.1057/sj.2012.11.

Button, Mark, Carol Mcnaughton Nicholls, Jane Kerr, and Rachael Owen. 2014. "Online Frauds: Learning from Victims Why They Fall for These Scams." *Australian and New Zealand Journal of Criminology* 47, no. 3 (March 28, 2014): 391–408. https://doi.org/10.1177/0004865814521224.

Button, Mark, Jacki Tapley, and Chris Lewis. 2012. "The 'Fraud Justice Network' and the Infra-structure of Support for Individual Fraud Victims in England and Wales." *Criminology & Criminal Justice* 13, no. 1 (July 6, 2012): 37–61. https://doi.org/10.1177/1748895812448085.

Capgemini. 2023. *World Payments Report 2023.* Technical report. September. https://www.capgemini.com/insights/research-library/world-payments-report/.

Coakley, Amber. 2024. "70-year-old Carlsbad Retiree Loses Life Savings in Scam Involving Bitcoin." Fox5 San Diego, April 19, 2024. https://fox5sandiego.com/news/local-news/70-year-old-carlsbad-retiree-loses-life-savings-in-scam-involving-bitcoin/.

Cross, Cassandra. 2018. "More Than Just Money: Getting Caught in a Romance Scam Could Cost You Your Life." *The Conversation* (May 30, 2018). https://theconversation.com/more-than-just-money-getting-caught-in-a-romance-scam-could-cost-you-your-life-97258.

DeLiema, Marguerite, Yiting Li, and Gary Mottola. 2022. "Correlates of Responding to and Becoming Victimized by Fraud: Examining Risk Factors by Scam Type." *International Journal of Consumer Studies* 47, no. 3 (November 11, 2022): 1042–59. https://doi.org/10.1111/ijcs.12886.

Deliema, Marguerite, Doug Shadel, and Karla Pak. 2019. "Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors." *Journal of Consumer Research* 46, no. 5 (May 28, 2019): 904–14. https://doi.org/10.1093/jcr/ucz020.

Dolgin, Sarah, and Samantha Mai Currier. 2023. "Scams Overwhelm Law Enforcement." The News House, May 1, 2023. https://www.thenewshouse.com/infodemic/scams/scams-overwhelm-law-enforcement-police/.

Downs, Julie S., Mandy B. Holbrook, and Lorrie Faith Cranor. 2006. "Decision Strategies and Susceptibility to Phishing." In *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06.* New York: ACM Press, July 12, 2006. https://doi.org/10.1145/1143120.1143131.

Economist Intelligence Unit. 2023. *Worldwide Cost of Living 2023.* Technical report. November. https://www.eiu.com/n/campaigns/worldwide-cost-of-living-2023/.

Eoyang, Mieke, Allison Peters, Ishan Mehta, and Brandon Gaskew. 2018. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, October 29, 2018. https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.

European Anti-Fraud Office. 2024. *OLAF Home.* https://anti-fraud.ec.europa.eu.

European Commission. 2020. *Survey on Scams and Fraud Experienced by Consumers.* https://commission.europa.eu/system/files/2020-01/factsheet_fraud_survey.final_.pdf.

Farivar, Cyrus. 2022. "How One Man Lost $1 Million to a Crypto 'Super Scam' Called Pig Butchering." *Forbes* (September 9, 2022). https://www.forbes.com/sites/cyrusfarivar/2022/09/09/pig-butchering-crypto-super-scam/?sh=d87d03aec8ed.

Federal Bureau of Investigation. 2023. *Internet Crime Report 2023.* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

Federal Communications Commission. 2024. *Deep Fake Audio and Video Links Make Robocalls and Scam Texts Harder to Spot.* Technical report. February. https://www.fcc.gov/consumers/guides/deep-fake-audio-and-video-links-make-robocalls-and-scam-texts-harder-spot.

Federal Trade Commission. 2023. *Social Media: A Golden Goose for Scammers,* October. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers.

———. 2024. *ReportFraud.ftc.gov.* https://reportfraud.ftc.gov/assistant.

Felson, Marcus, and Lawrence E. Cohen. 1980. "Human Ecology and Crime: A Routine Activity Approach." *Human Ecology* 8:389–406. https://ojp.gov/ncjrs/virtual-library/abstracts/human-ecology-and-crime-routine-activity-approach.

FICO. 2023. *FICO 2023 Scams Impact Survey.* Whitepaper. https://www.fico.com/en/latest-thinking/white-paper/fico-2023-scams-impact-survey#:~:text=In%20January%202023%2C%20FICO%20conducted,relationship%20between%20RTP%20and%20scams.

FINRA Foundation. 2007. *Senior Fraud Risk Survey.* https://www.finrafoundation.org/sites/finrafoundation/files/senior-fraud-risk-survey.pdf.

Global Anti-Scam Alliance. 2023. *State of Scams in Asia Report 2023.* Technical report. November. https://files.gogolook.com/2023-asia-scam-report.pdf.

Graham, Roderick, and Ruth Triplett. 2017. "Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization." *Deviant Behavior* 38, no. 12 (December): 1371–82. https://doi.org/10.1080/01639625.2016.1254980.

Havers, Benjamin, Kartikeya Tripathi, Alexandra Burton, Wendy Martin, and Claudia Cooper. 2024. "A Qualitative Study Exploring Factors Preventing Older Adults from Reporting Cybercrime and Seeking Help." *CrimRxiv* (May 30, 2024). https://doi.org/10.21428/cb6ab371.8c4e3181.

Ianzito, Christina. 2024. "AI Fuels New, Frighteningly Effective Scams." AARP, April 3, 2024. https://www.aarp.org/money/scams-fraud/info-2024/ai-scams.html.

Jakobsson, Markus, Alex Tsow, Ankur Shah, Eli Blevis, and Youn-Kyung Lim. 2007. "What Instills Trust? A Qualitative Study of Phishing." In *Financial Cryptography and Data Security,* 356–61. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-540-77366-5_32.

Jensen, Rasmus Ingemann Tuffveson, Julie Gerlings, and Joras Ferwerda. 2024. "Do Awareness Campaigns Reduce Financial Fraud?" *European Journal on Criminal Policy and Research* (March 11, 2024): 1–36. https://doi.org/10.1007/s10610-024-09573-1.

Jha, Himani, and David Delima. 2022. "Google Pay Will Now Warn Users About Fraudulent, Suspicious Transactions: Details." Gadgets 360, October 20, 2022. https://www.gadgets360.com/apps/news/google-pay-fraud-detection-technique-warning-suspicious-activities-3622161.

Jones, Pete. 2022. "Nature of Fraud and Computer Misuse in England and Wales." *Office for National Statistics* (September 22, 2022). https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022.

Khandro, Linda. 2024. "I'm a College Professor. I Fell for a Scam that Drained My Life Savings." *The Seattle Times* (February 2, 2024). https://www.seattletimes.com/opinion/im-a-college-professor-i-fell-for-a-scam-that-drained-my-life-savings/.

Kigerl, Alex. 2011. "Routine Activity Theory and the Determinants of High Cybercrime Countries." *Social Science Computer Review* 30, no. 4 (October 5, 2011): 470–86. https://doi.org/10.1177/0894439311422689.

Kilmer, Liz. 2023. "Man Loses Life Savings in Elaborate Scam, FBI Says Many in Western Pennsylvania Have Fallen Victim." WPXI, September 6, 2023. https://www.wpxi.com/news/local/man-loses-life-savings-elaborate-scam-fbi-says-many-western-pennsylvania-have-fallen-victim/ELJYLV2FBVADJA5OMVSN2UZTP4/.

Kozyreva, Anastasia, Philipp Lorenz-Spreen, Stefan M. Herzog, Ullrich K. H. Ecker, Stephan Lewandowsky, Ralph Hertwig, Ayesha Ali, et al. 2024. “Toolbox of Interventions Against Online Misinformation.” *Nature Human Behavior* 8 (May 13, 2024): 1044–52. https://doi.org/10.1038/s41562-024-01881-0.

Lewis, James Andrew, Zhanna L. Malekos Smith, and Eugenia Lostri. 2020. “The Hidden Costs of Cybercrime.” Center for Strategic & International Studies, December 9, 2020. https://www.csis.org/analysis/hidden-costs-cybercrime.

Manamela, Desiree, and Dihlolelo Phoshoko. 2024. “Stats SA Media Release February 2024.” Statistics South Africa, February 20, 2024. https://www.statssa.gov.za/publications/P0211/Media%20release%20QLFS%20Q4%202023.pdf.

McGrew, Sarah, and Joel Breakstone. 2023. “Civic Online Reasoning Across the Curriculum: Developing and Testing the Efficacy of Digital Literacy Lessons.” *AERA Open* 9 (June 7, 2023): 23328584231176451. https://doi.org/10.1177/23328584231176451.

McGuire, William J. 1961. “The Effectiveness of Supportive and Refutational Defenses in Immunizing and Restoring Beliefs Against Persuasion.” *Sociometry* 24 (2): 184–97. https://www.jstor.org/stable/2786067.

Miller, Jon D. 1983. “Scientific Literacy: A Conceptual and Empirical Review.” *Daedalus* 112 (2): 29–48. http://www.jstor.org/stable/20024852.

Miró, Fernando. 2014. “Routine Activity Theory.” *The Encyclopedia of Theoretical Criminology* (January 31, 2014): 1–7. https://doi.org/10.1002/9781118517390.wbetc198.

Modic, David, Ross Anderson, and Jussi Palomäki. 2018. “We Will Make You Like Our Research: The Development of a Susceptibility-to-Persuasion Scale.” *PLoS One* 13, no. 3 (March 15, 2018): e0194119. https://doi.org/10.1371/journal.pone.0194119.

Modic, David, and Stephen E. G. Lea. 2014. “Scam Compliance and the Psychology of Persuasion.” *SSRN Electron. J.* (January 4, 2014). https://doi.org/10.2139/ssrn.2364464.

Munton, James, and Jelita McLeod. 2023. *The Con: How Scams Work, Why You’re Vulnerable, and How to Protect Yourself.* Rowman & Littlefield.

Norris, Gareth, Alexandra Brookes, and David Dowell. 2019. “The Psychology of Internet Fraud Victimisation: A Systematic Review.” *Journal of Police and Criminal Psychology* 34, no. 3 (July 2, 2019): 231–45. https://doi.org/10.1007/s11896-019-09334-5.

NortonLifeLock. 2022. *2022 Norton Cyber Safety Insights Report: Special Release – Online Creeping.* https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-online-creeping/.

Park, Jun-hee. 2023. “Koreans Lost Nearly W1.7tr to Phishing Scams Over Past 5 Years: Data.” *Korea Herald* (February 21, 2023). https://www.koreaherald.com/view.php?ud=20230221000590.

Pennycook, Gordon, Ziv Epstein, Mohsen Mosleh, Antonio A. Arechar, Dean Eckles, and David G. Rand. 2021. “Shifting Attention to Accuracy Can Reduce Misinformation Online.” *Nature* 592, no. 7855 (March 17, 2021): 590–95. https://doi.org/10.1038/s41586-021-03344-2.

Robb, C.A., and S. Wendel. 2022. “Who Can You Trust? Assessing Vulnerability to Digital Imposter Scams.” *Journal of Consumer Policy* 46, no. 1 (December 23, 2022): 27–51. https://doi.org/10.1007/s10603-022-09531-6.

Stainsby, Jenny, and Andrew Eastwood. 2023. “Global Approaches to Regulating Rising Fraud.” *The Banker* (October 9, 2023). https://www.thebanker.com/Global-approaches-to-regulating-rising-fraud-1696836353.

United Nations Human Rights Office of the High Commissioner. 2024. *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia,* April 2, 2024. https://bangkok.ohchr.org/online-scam-and-trafficking-sea/.

Vitak, Jessica, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. “’I Knew It Was Too Good to Be True“: The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-efficacy Online.” *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (November 1, 2018): 1–25. https://doi.org/10.1145/3274445.

Whitty, Monica T. 2013. “The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam.” *British Journal of Criminology* 53, no. 4 (July): 665–84. ISSN: 0007-0955. https://doi.org/10.1093/bjc/azt009.

———. 2019. “Predicting Susceptibility to Cyber-Fraud Victimhood.” *Journal of Financial Crime* 26, no. 1 (January 7, 2019): 277–92. https://doi.org/10.1108/JFC-10-2017-0095.

———. 2020. “Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims.” *European Journal on Criminal Policy and Research* 26, no. 3 (September 2, 2020): 399–409. https://doi.org/10.1007/s10610-020-09458-z.

Whitty, Monica T., and Tom Buchanan. 2015. “The Online Dating Romance Scam: The Psychological Impact on Victims – Both Financial and Noninancial.” *Criminology & Criminal Justice* 16, no. 2 (September 3, 2015): 176–94. https://doi.org/10.1177/1748895815603773.

World Bank. 2023. *Fraud Risks in Fast Payment.* Technical report. October. https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf#page=10.45.

Xu, Ding, Laurie Murphy, Tingzhen Chen, and Philip L Pearce. 2022. “Differentiating Tourist Scam Cases: Towards a Taxonomy of Deceptive Schemes.” *Journal of Hospitality and Tourism Management* 50:159–67. https://doi.org/10.1016/j.jhtm.2022.01.011.

Authors

Mo Houtti (mhoutti@google.com) is a Student Researcher on the Trust & Safety Research Team at Google.

Abhishek Roy (abhishekroy@google.com) is a Staff UX Researcher on the Trust & Safety Research Team at Google.

Venkata Narsi Reddy Gangula (narsi@google.com) is a Senior UX Researcher on the Trust & Safety Research Team at Google.

Ashley Marie Walker (amwalker@google.com) is a Senior UX Researcher on the Trust & Safety Research Team at Google.

Disclosures

This research was funded in its entirety by Google. Google is a member of the Global Anti-Scam Alliance, a coalition body of over 100 organizations, including governments, law enforcement, consumer protection, financial authorities and services, social media, internet service providers and cybersecurity professionals.