© Shutterstock

Countering Digital Scams

STEMMING THE TIDE ON AN URGENT DEVELOPMENT CHALLENGE

UNDP Issue Brief

Executive Summary

A text message offering a flexible employment opportunity. A direct message sharing a new investment scheme. An email warning of unpaid fines. Digital scams have become a global development challenge, inflicting costs of up to one trillion dollars annually.

Beyond financial losses, scams inflict emotional harm and erode trust in digital systems, weakening confidence in governments, financial institutions, and online services. As countries accelerate digital transformation – expanding digital payments, digital public infrastructure, and online public services – scammers are exploiting new and existing vulnerabilities such as gaps in digital literacy, consumer protection, and scam detection capacities.

The threat is especially acute in developing countries, where lower institutional capacities and higher levels of economic precarity increase exposure and amplify losses. Four trends are accelerating this challenge: rapid digitalization, AI-enabled scams, expanded demographic targeting, and declining institutional trust.

Effectively countering digital scams is essential not only to mitigate harm, but also to strengthen digital trust, support safer participation in the digital economy, and advance the Sustainable Development Goals. This opportunity hinges on the power of collective action: coordinated efforts across governments, financial institutions, platforms, and civil society that span the full scams lifecycle are essential to increase safety and rebuild trust online.

This brief is intended for policymakers, practitioners, and international and private-sector partners engaged in building safer and more inclusive digital ecosystems.

UNDP will work to counter digital scams by aiming to help countries mobilize evidence, strengthen capacity, and create safer, more resilient digital environments. This approach is grounded in UNDP's whole-of-society digital transformation framework, an intentionally inclusive approach to build ownership, support human-centered design, and mitigate risks. It is informed by UNDP's work with more than 130 countries to support core digital transformation, including the strengthening of infrastructure and practices that improve integrity, authentication, and data provenance in developing countries.

PART 1

Why digital scams are a critical development challenge

Digital technologies hold enormous potential for accelerating global development and prosperity. Indeed, research shows that digital technologies support more than 70 percent of the Sustainable Development Goals' (SDGs) targets.[i] At the same time, the use of digital tools also introduces new vulnerabilities and reveals systemic gaps, increasing exposure to new and emerging forms of harm, including digital scams.

A One Trillion Dollar Challenge

According to research by the Global Anti-Scam Alliance, digital scams are estimated to cost the world between 442 billion and one trillion USD each year. Globally, more than half of people around the world have been exposed to a digital scam in the last 12 months.[ii] But even these figures likely significantly undercount the incidence of digital scams as many encounters go unreported. Although not a new form of digital threat, digital scams have grown precipitously over the past five years, into what is sometimes referred to as a global scamdemic or scampocalypse.[iii] This increase was initially driven by the lockdowns and economic shocks of the COVID-19 pandemic and is now accelerated by advances in artificial intelligence and other emerging technologies.[iv]

Digital Scams

Digital scams or tech-enabled scams are deceptive activities that use digital technologies to manipulate or trick individuals into transferring funds, disclosing sensitive information, or enabling unauthorized access to their accounts and identities. They can cause financial, social, emotional, and psychological harm.

Digital scams are deceptive activities that use digital technologies to manipulate or trick individuals into transferring funds, disclosing sensitive information, or enabling unauthorized access to their accounts and identities.* They can cause financial, social, emotional, and psychological harm. Today's digital scams are often carried out using social engineering tactics and conducted via trusted digital pathways. Scammers psychologically manipulate their victims into giving up sensitive and confidential information (i.e. phishing) or performing actions that compromise security by exploiting their trust. This may be done through impersonation of an institution, authority, family member, or celebrity. Scammers manipulate their victims by creating urgency around a time-sensitive situation or building what feels like deep emotional connections with their victims.

** For the purposes of this brief, "digital scams" are defined in here and refer to digital deception targeting individuals. This brief explicitly excludes broader forms of financial fraud and wider cybercrime landscape, which are legally and technically distinct. The brief therefore encourages further research and policy analysis on the evolving relationship, boundaries, and regulatory overlaps between digital scams and fraud.*

Types of Digital Scams*

Digital scams take many forms, but all are underpinned by manipulation and deception. Some common types of scams include:

Ecommerce/Shopping Scams: Fraudulent sellers exploit online marketplaces and social media platforms by offering products at attractive prices. Victims either never receive the goods or receive counterfeit or substandard items.

Investment Scams: Scammers lure victims with promises of high returns through fake or fraudulent investment opportunities, often using cryptocurrency.

Social Engineering and Impersonation Scams: Exploitation of human psychology to deceive individuals into divulging sensitive information or transferring funds. Scammers may impersonate authorities such as law enforcement officials, utility companies, debt collectors, friends, relatives, or tech support. Victims may be threatened with arrest or with public exposure of sensitive information. Scammers often collect funds in the form of cryptocurrency.

Fake Charity Scams: Fraudulent solicitations for donations, often during crises or disasters, where funds are misused or stolen.

Business Email Compromise Scams: Scammers impersonate executives or vendors in organizations to deceive employees into making unauthorized transactions.

Advance Fee Schemes: Scammers promise victims large rewards, payments, or donations in exchange for an upfront fee. These include prize and lottery scams.

Romance and Relationship Scams: Scammers use fake profiles on social media or dating apps to form emotional relationships with victims, ultimately exploiting them for financial gain. This includes sextortion scams that often target minors.

Employment Scams: Scammers offer fake employment opportunities to extort money from job seekers, harvest their personal information, or in the most extreme cases, traffic them to work in scam centers.

** For the purposes of this brief, the analysis is anchored in the digital scams typology developed in the UNDP's Anti-Scam Handbook series[v]. This brief recognizes that digital scams can be categorized in multiple ways; accordingly, this typology is not intended to be exhaustive or definitive, but to provide a structured and illustrative overview of the breadth of prevalent scam types for analytical and policy purposes.*

Beyond Financial Costs

The scale of financial costs is vast, but borne disproportionately. Although victims in developed countries experience higher average losses per scam, developing countries suffer significantly higher costs in terms of Gross Domestic Product. Scams have been estimated to cost richer countries approximately 0.2 percent of GDP, while developing countries experience losses of 3 to 4 percent, with some individual countries losing 10 to 11 percent of GDP to scams.[vi]

But the full toll of digital scams extends beyond significant financial loss. Scams can exact a significant emotional and psychological toll, with victims experiencing feelings of shame and embarrassment and harm to interpersonal relationships.

Scams also erode trust and confidence in digital transactions. Research shows that exposure to scams can diminish trust, even among people who are not directly victimized.[vii] In a survey of nine countries, 79 percent of respondents reported that receiving a scam message made them less likely to trust that communication channel.[viii] In a separate study, one quarter of scam victims reported becoming more distrustful of digital tools and platforms as a result.[ix]

The loss of digital trust is especially worrisome. Trust and confidence are foundational for inclusive digital transformation,[x] and the erosion of trust is nonlinear. Even a small number of highly visible or personally salient scams can undermine confidence in digital systems, especially in contexts where institutional trust is already fragile.

Digital scams increasingly rely on the manipulation of trusted digital pathways and when these pathways become highways for scams, not only is the integrity of specific channels compromised, but people are less likely to trust digital technologies overall. The use of digital payments, digital ID or online government services requires that people understand and trust the underlying system. Repeated experiences with scams can lead to people doubting the ability of governments, financial institutions, and digital platforms to protect them, a particular risk in countries where trust is already low. This can lead to digital backsliding, when people and businesses avoid digital platforms and services to protect themselves from potential digital harms.

Recognizing these risks, UNDP has increasingly focused on strengthening safeguards around foundational digital public infrastructure (DPI) – including digital ID systems, payment platforms, and data exchange layers – to ensure they are safe, rights-based, and resilient to misuse. Through the UN DPI Safeguards Initiative[xi] UNDP supports countries to embed protections for security, privacy, transparency, and accountability directly into the design and governance of these systems, helping to prevent scams from exploiting trusted digital pathways and undermining public confidence.

Finally, the industrialization of digital scams is also fueling a global crisis in human trafficking, according to INTERPOL. Its profits fuel transnational organized criminal groups who use the proceeds from scams to extend their networks and expand their illegal operations.[xii] The activities of these groups also often overlap with other illicit commodities, including drugs. Once confined to a small geographic area in Southeast Asia, scam centers are expanding worldwide.[xiii]

Digital Scams in Developing Countries

As the threat continues to grow and research shows the serious harms that scams inflict in developing countries, understanding the relationship between development and digital scams has become an urgent policy priority at the national, regional, and global levels.

Global Policy and Security Responses to Digital Scams

The security implications of digital scams and the transnational organized criminal groups they support have garnered important attention from policymakers. The UN Convention against Cybercrime, adopted in 2024, commits states parties to adopt measures to criminalize digital-enabled cyber threats. INTERPOL has coordinated multiple global and regional operations and supports capacity development and training for law enforcement agencies.[xiv] In 2025, the Association of Southeast Asian Nations (ASEAN) adopted the ASEAN Declaration on Combatting Cybercrime and Online Scams, which commits to deepening law enforcement coordination and strengthening the capacity of front-line officers to disrupt and prosecute scammers. In 2026, ASEAN launched the ASEAN Guide on Anti-Scam Policies and Best Practices to serve as a framework for regional cooperation to counter scams. Countries are also taking action, with support from global and regional partners, to arrest scammers and take down scam centers.[xv]

In addition to the costs outlined above, developing countries face several unique vulnerabilities that can expand their exposure to and the harms of digital scams. These include more limited institutional capacities to monitor, educate, and enforce against scams; weaker consumer protection and digital literacy and hygiene; rapid and uneven digitalization that has expanded market participation faster than safeguards can scale; informal digital economic activity; and pre-existing criminal networks.[xvi]

Together, these factors expand market vulnerabilities and create uneven protections for users across digital channels and populations. These features can also make developing country contexts early testing grounds for new scam tactics, as increasingly agile, high-velocity, and sophisticated scam techniques – often relying on social engineering and AI-enabled tools – outpace existing defensive systems, education approaches, and accountability mechanisms, especially given weaker safeguards and significant underreporting of scams.

Developing countries currently face a challenging economic landscape characterized by high interest rates, weak global economic growth, and greater uncertainty. Official Development Assistance declined by 6 percent between 2023 and 2024 with further cuts projected through at least 2027.[xvii] Putting even a fraction of the money lost to scams to productive use in developing economies would be especially meaningful at a moment of such economic strain.

Scam centers themselves bring additional threats to development outcomes. Their illicit gains fund both illicit and licit economic activity, distorting local economies and leaving these actors dependent on the scamming operations. [xviii] They can offer an attractive employment option to people who have digital skills, particularly youth, but lack other job prospects. The presence of many scam centers in close proximity further exacerbates these risks and countries that have scam center regions, often located in areas with weaker governance, can suffer damage to their international standing and lose broader development partnerships.

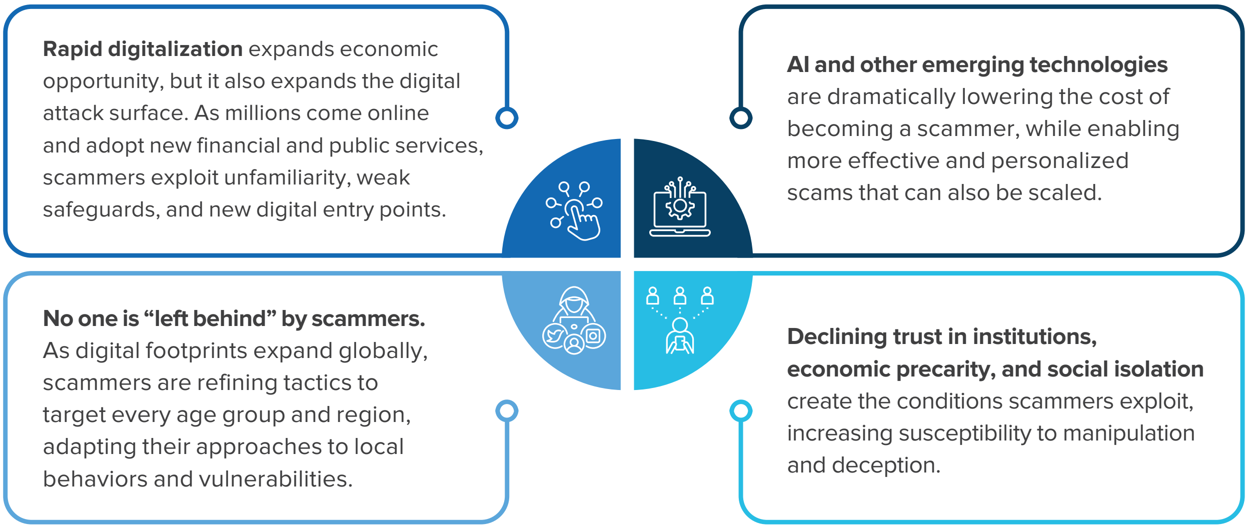
As these vulnerabilities intensify, understanding what accelerates scams is critical for shaping an effective response.

PART 2

Four trends accelerating digital scams

The widening impacts of scams, from financial losses to erosion of trust, make it essential to understand what is accelerating their spread. This section examines four interconnected trends that are transforming the global scam ecosystem. Together, they reveal a rapidly evolving threat landscape that requires equally adaptive, coordinated, and forward-looking responses.

Trends Accelerating Digital Scams



Rapid digitalization expands economic opportunity, but it also expands the digital attack surface. As millions come online and adopt new financial and public services, scammers exploit unfamiliarity, weak safeguards, and new digital entry points.

AI and other emerging technologies are dramatically lowering the cost of becoming a scammer, while enabling more effective and personalized scams that can also be scaled.

No one is "left behind" by scammers. As digital footprints expand globally, scammers are refining tactics to target every age group and region, adapting their approaches to local behaviors and vulnerabilities.

Declining trust in institutions, economic precarity, and social isolation create the conditions scammers exploit, increasing susceptibility to manipulation and deception.

Rapid digitalization is expanding both opportunities and risks.

Global access to digital technologies has continued to expand rapidly, transforming how people communicate, learn, work, and participate in civil and economic life. In 2025, an estimated six billion people – roughly three-quarters of the world's population – were using the internet, making continued progress toward broader connectivity, with over 240 million people coming online in the past year alone.[xix] Yet, despite this growth, significant gaps remain: 2.2 billion people remain offline, with stark inequalities in affordability and service quality across regions and populations. As of 2025, more than four in five people globally owned a mobile phone, and mobile broadband subscriptions nearly matched the world's population, though access and quality remain uneven across countries.

Mobile money and digitally enabled bank accounts are driving financial inclusion. Globally, 61 percent of adults made a digital payment in 2024, a 27 percent increase from 2014. This increase translates into millions of people previously underserved around the world now able to engage in economic activity, save, borrow, and receive digital government services among other benefits. The use of digital merchant payments has soared, allowing small businesses to grow, and governments are also increasing distributing funds digitally. In 2024, 75 percent of recipients of government wages, pensions or social transfer payments received these funds digitally.[xx] These trends underscore both the strides made in connecting people worldwide and the continuing challenges in achieving equitable, meaningful access to digital technologies.

Beyond payments, countries are increasingly digitizing public services, including through digital public infrastructure (DPI). When implemented safely and inclusively, DPI can be used to distribute public benefits, verify identities, enable voter registration, and provide secure banking, among other development benefits.[xxi, xxii] In many instances, these systems are designed to minimize friction for users by prioritizing speed and convenience and minimizing interruption for users. This enables governments to rapidly scale services, including for the most vulnerable, provide the foundations for private innovation, and achieve greater efficiencies. UNDP works with governments to strengthen design, governance, and safeguards of DPI, including through the 50-in-5 initiative and DPI Safeguards Initiative.[xxiii]

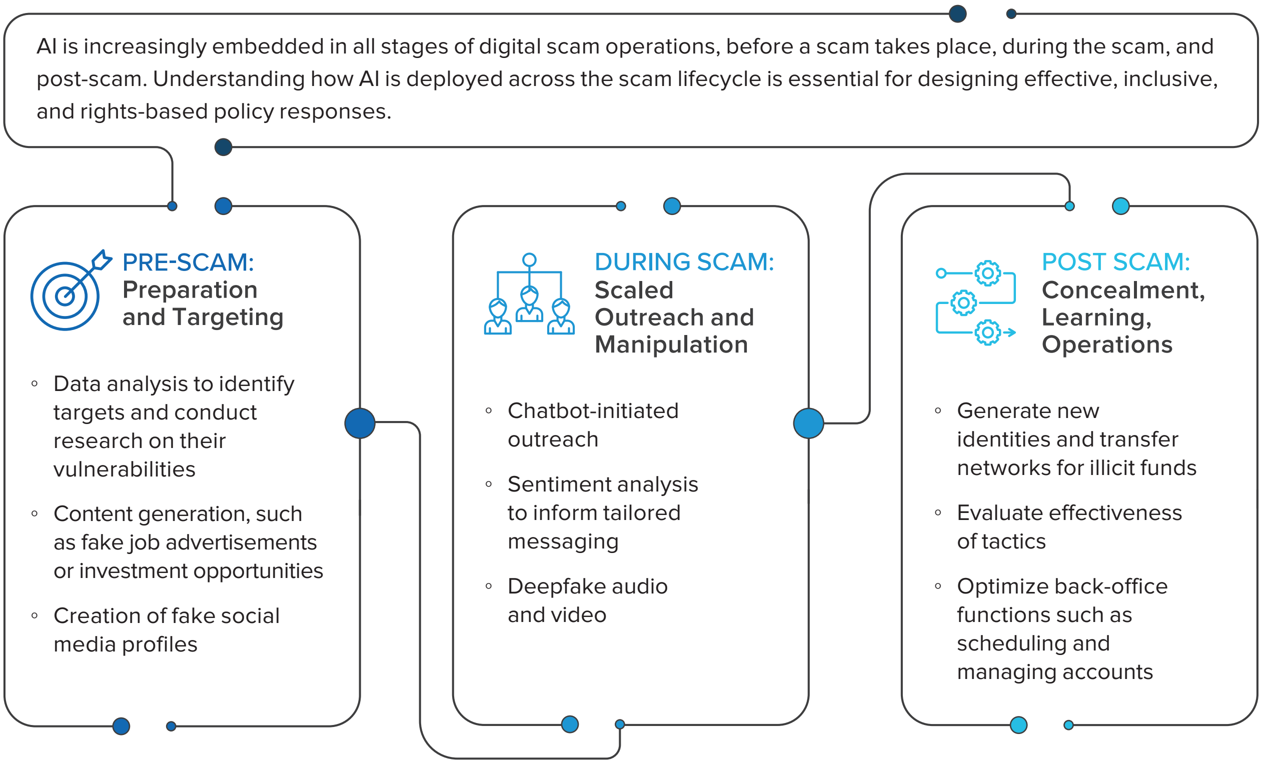
While offering these critical benefits, rapid digitization also significantly expands digital entry points into people's financial and civic lives - such as payment platforms, digital IDs, online service portals, and messaging channels. When rapid digitalization is not accompanied by appropriately scaled investments in digital safety and capacity, as the number of entry points grows, so does exposure: people are increasingly likely to encounter scam attempts or malicious actors, especially first-time or newly connected users. These expanded entry points also create new vulnerabilities that scammers seek to exploit, from banking credentials to social protection and government payment systems. In addition, rapid and widespread adoption in digital services and tools, such as new digital payment systems or the use of QR codes, means that individuals have less time to learn the accompanying safety practices.

AI and other technologies are turbocharging scams while also bolstering defense.

Advances in AI and other digital technologies serve as a force multiplier for the global scams industry,[xxiv] widening the gap between people's confidence and their ability to recognize scams.[xxv] Scam techniques are evolving in speed, sophistication, and adaptability, often outpacing existing defensive systems. Scammers are using AI for nearly every step in their attacks, from surveilling, researching, and identifying potential targets, to tailoring and personalizing outreach, setting dynamic pricing models, generating deepfakes, as well as managing operational functions within scam centers, such as setting schedules and managing other administrative tasks.[xxvi] AI is also making scam and fraud networks more resilient and anonymous by enabling constantly changing identifiers and links to evade URL takedowns. While people still play a central role in developing and perpetrating scams, these technologies are transforming scams from a labor-intensive activity into a high-volume, increasingly sophisticated automated enterprise.

Indeed, the MIT Risk Repository demonstrates a significant increase in the proportion of AI risks related to scams and fraud, from 9 percent of all risks in 2020 to nearly 50 percent in 2025.[xxvii]

How AI is Used Through the Scams Lifecycle



AI is increasingly embedded in all stages of digital scam operations, before a scam takes place, during the scam, and post-scam. Understanding how AI is deployed across the scam lifecycle is essential for designing effective, inclusive, and rights-based policy responses.

PRE-SCAM: **Preparation and Targeting**

- Data analysis to identify targets and conduct research on their vulnerabilities
- Content generation, such as fake job advertisements or investment opportunities
- Creation of fake social media profiles

DURING SCAM: **Scaled Outreach and Manipulation**

- Chatbot-initiated outreach
- Sentiment analysis to inform tailored messaging
- Deepfake audio and video

POST SCAM: **Concealment, Learning, Operations**

- Generate new identities and transfer networks for illicit funds
- Evaluate effectiveness of tactics
- Optimize back-office functions such as scheduling and managing accounts

In addition, scammers are using cryptocurrency in a range of different types of scams, including romance and crypto investment schemes.[xxviii] Scammers take advantage of the decentralized and distributed nature of crypto, the lack of financial intermediaries, and the fact that crypto transactions cannot be reversed to hide, launder, and protect stolen funds.

These advances have been accompanied by evolving business models in which malicious actors package and sell or rent scamming tools and datasets as cybercrime-as-a-service, dramatically lowering the barriers to entry for scamming. In addition to making it easier to become a scammer, these developments are helping to accelerate the pace of scam innovation to make them more effective and evasive.

As AI and other technologies are making scamming more effective, they are also being put to work to fortify detection and defense capabilities against scams. For example, Singapore's GovTech developed the recursive Machine-Learning Site Evaluator (rMSE) to rapidly analyze and classify large numbers of suspicious URLs. Working together with Singapore Police Force, rMSE enables police operators to analyze more than 400 thousand sites per day and share identified malicious URLs with Google's Safe Browsing (Web Risk) blocklist, which blocks the sites from more than five billion devices worldwide. Since its launch in 2023, this system has identified and blocked more than 240,000 scams.[xxix]

Digital platforms, payment companies and others are also using AI to identify and remove scam posts, transactions, and accounts, enabling scaled detection and removal. These approaches may become even more important as AI enables increasingly realistic and personalized scams. Despite these advances, the distribution of AI capabilities still currently favors scammers. Offensive AI is less expensive and easier to adopt while defensive AI is more compute- and data-intensive and requires additional investments in skills and coordination. This capability gap is particularly acute in developing countries.

Scammers "leave no one behind."

Scam tactics are also evolving in terms of the demographic and geographic groups that are targeted. Although there is significant attention to scams targeting older people in Western countries, emerging data shows that scammers are refining tactics to cover all areas and ages.

Research by the Global Anti-Scam Alliance shows that across 42 countries, 57 percent of respondents have encountered a scam in the past 12 months. But regional analysis reveals that this includes 72 percent of respondents in South America and 68 percent of respondents in Africa. Further, 23 percent of respondents in the same survey had money stolen through a scam in the past year. But the figures for South America and Africa are substantially higher, reaching 41 percent of all respondents.[xxx]

Available statistics likely underestimate the true scale of the problem, as scams remain significantly underreported due to stigma, lack of awareness, limited or unclear reporting mechanisms, and mistrust in authorities – particularly in low- and middle-income contexts. Underreporting is therefore a challenge in its own right, suggesting that the real number of victims and the overall impact of digital scams are substantially higher than captured by official figures.

The data on scams also challenges common assumptions about the vulnerability of scams presented by different age groups or education levels in ways that have important implications for developing effective policy responses. Although they are the most confident in their ability to recognize and avoid scams, Gen Z and Millennials are more likely to have lost money to scams than older generations. People with higher education are also slightly more likely to lose money to scams than the global average.

Different groups may be more susceptible to different types of scams. For instance, younger generations may be more likely to fall victim to shopping or employment scams while older generations may be more likely to be targeted through social engineering scams. Yet scams are a threat to all ages online.

As digitalization efforts accelerate, it is crucial that digital literacy keep pace to ensure that those newly using digital services are able to practice safe online behaviors, know how to identify potential scams, and are aware of actions they can take to protect themselves.

Lower trust in institutions and uncertain economic prospects can increase susceptibility to scams.

Globally, trust in institutions remains low and fragile. While recent data show modest increases in trust in government and government leaders, they continue to be the least trusted actors, reinforcing widespread perceptions that institutions serve narrow interests.[xxxi]

Automation, increased trade barriers, and uncertain economic prospects are increasing fears about job security, particularly for young people. The number of young people not in education, employment or training is rising in low-income countries. Young adults in low-income countries are three times more likely to rely on insecure forms of employment when compared to those in high-income countries.[xxxii]

Finally, one in six people around the world feels lonely.[xxxiii] Though digital technologies can offer the opportunity to make new connections, loneliness can also make a person more vulnerable to social engineering that appears to offer love or friendship.

Taken together, these factors can lead to riskier behaviors and more openness to "get rich quick" schemes, increasing exposure to and susceptibility to scams, particularly ones that promise quick financial rewards or offer virtual companionship.[xxxiv]

PART 3

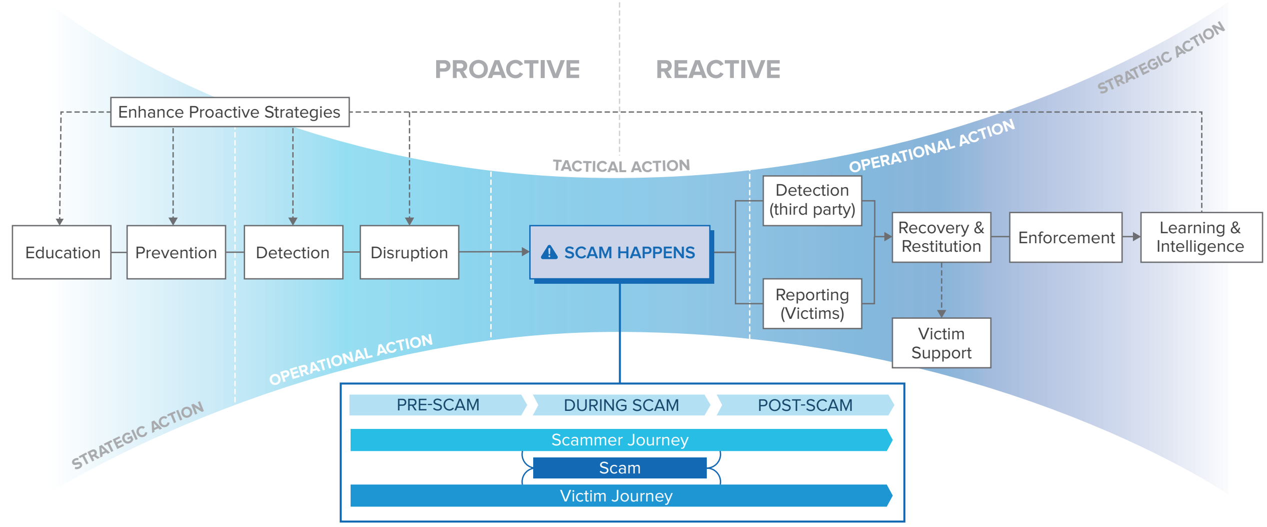
What is needed to effectively counter digital scams

What do these trends tell us?

Taken together, these trends offer three clear implications for policy and practice.

A holistic lifecycle approach is essential.

First, effectively countering scams requires a holistic approach that incorporates both proactive and reactive elements, extending from scam prevention to detection to response. UNDP's Anti-Scam Handbook developed the Scams Response Spectrum, a framework that identifies responses to scams with interventions that can be applied across all stages of the scam lifecycle, pre-, during, and post-scam.



Source: UNDP Anti-Scam Handbook 2.0

The Scams Response Spectrum underlines that effectively countering scams depends as much on pre-scam mitigation as it does on response, recovery, and enforcement post-scam. Proactive strategies that bolster education through public information and cyber hygiene programmes help build the digital literacy needed to identify scams. Systems to identify and disrupt scams, such as blocking URLs or phone numbers, can stop individual scam attempts while the introduction of pauses or verification steps in high-risk transactions and other prevention-by-design approaches can disrupt the urgency that scammers often rely on and reduce the likelihood of a scam attempt's success.

Reactions post-scam are also not confined to just reporting and recovery, although these are crucial steps. Additional critical actions include victim support, enforcement, and learning and intelligence to inform future proactive interventions. This includes constant synthesis of insights into how scams are evolving, new tactics and approaches, and factors that can increase susceptibility to being victimized by a scam.

Cooperation is key for tackling scams effectively.

Second, no single actor or sector can tackle scams on their own. Scammers work across multiple platforms and are able to take advantage of gaps in information sharing across actors. A whole-of-society approach is therefore needed to tackle this challenge, where governments, banks, digital platforms, and others have crucial roles to play. Acknowledging that this requires overcoming misalignments in incentives that can serve as roadblocks, each actor has different sets of data, insights, and levers that can be exercised to support cooperative action against scams. For instance, banks provide a range of anti-scam services to their customers, from detection to awareness raising, and possess data on where clients have been victimized. Governments provide public information on scams, collect data on trends in scam incidence and scam reporting, and have access to law enforcement information on scammer organizations. Digital platforms have data on scam attempts on their platforms and are well placed to view how scams are evolving and the adoption of new scamming tactics.

There are several important platforms that bring together actors across sectors. The Global Anti-Scam Alliance connects governments, the private sector, and consumer protection organizations to protect consumers from scams. Cross-sector partnerships, such as the example between Singapore and Google, discussed previously, can also deliver important tangible results.

Technology is both a challenge and part of the solution.

Third, digital tools are strengthening defenses to detect, disrupt, and respond to scams. Even as AI and other new technologies are making scams easier and more prevalent, actors across government, the private sector, and civil society are deploying technology in novel ways to counter scams. Payments companies, for instance, are using AI to validate identities, identify scammer accounts, and recognize suspicious transactions and patterns.

There are also promising opportunities for AI to support safe, trusted and universal DPI by detecting patterns of scams by identifying behavioral patterns and developing predictive modeling.[xxxv] There is growing attention to safeguards and guardrails, as digital technologies are not neutral. Ensuring trust and safety therefore requires balancing effectiveness in countering scams with the protection of fundamental rights.

UNDP's AI Trust and Safety Re-imagination Programme, has gathered 17 innovation teams, over one-third of which have developed tools and methods adapted to local environments in developing countries to detect, disrupt, and respond to scams.[xxxvi] This programme has brought to light how working with communities and adapting technology to context can scale in practical and impactful ways.

How can we leverage these insights, particularly in developing countries?

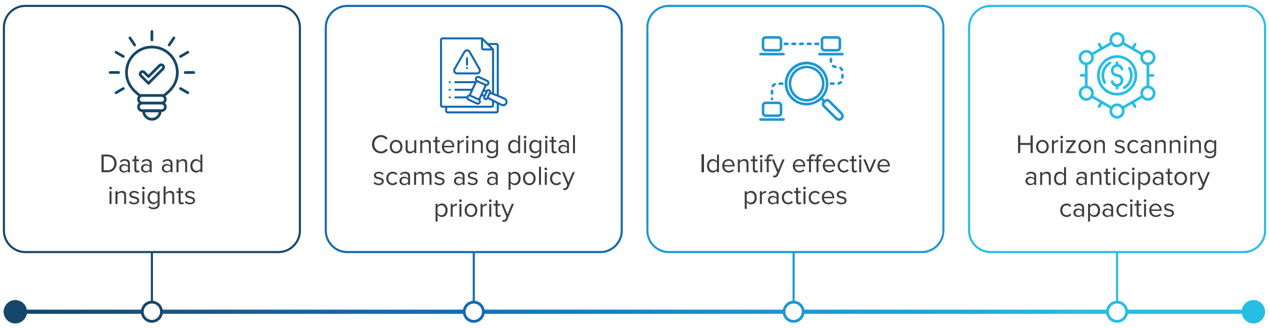
This analysis suggests four priorities for leveraging these insights, with a particular focus on developing countries.

First, more **data and insights** are needed on how the rapidly evolving digital scams threat is experienced in developing countries. Existing data shows that scams are a significant and growing challenge in developing countries, but these datasets tend to prioritize the largest developing countries. Expanding data on scams in developing countries will help to build effective strategies for education, collaboration, and response and to strengthen understanding of how scams impact digital adoption and financial inclusion. It will also provide crucial insights for understanding scams globally, including tactics that may first be tested in developing country contexts before being deployed globally by scammers.

Second, more data on scams in developing countries can also help to elevate **countering digital scams as a policy priority** at national, regional, and global levels. Because coordinating action across actors and sectors can be challenging, naming digital scams as an explicit priority for policymakers helps direct attention and resources to the problem. This includes the need for greater information sharing within government and across actors to build capacity across the Scams Response Spectrum – from digital hygiene and cyber-awareness skills to the capacities required to investigate and process scams – and conduct gap analyses to identify priority areas for intervention.

Third, because scams evolve quickly and require coordination across sectors, it is crucial to **identify effective practices** to stop them, from the use of new technologies to effective forms of partnership to supporting digital skilling and hygiene, particularly in developing country contexts. This allows countries, companies, and others to reuse and adapt existing tools and approaches, reducing duplication and improving speed of response. For this effort, it will be particularly important to tailor effective approaches to local needs and context. This can also help identify where further investments are needed and facilitate cross-sector and cross-country learning.

Finally, scams are evolving in real time. Investments **in horizon scanning and anticipatory capacities** can help anti-scam collaborators prepare for new developments and forms of scams. Taking advantage of the strengths of across public and private sectors, such investments can reinforce holistic approaches: the identification of new tactics, for instance, can inform digital awareness and skills building, and strengthen both scam detection and disruption. As scammers approaches adapt quickly, so too must defensive efforts.


Data and insights

Countering digital scams as a policy priority

Identify effective practices

Horizon scanning and anticipatory capacities

These four priorities are at the heart of how UNDP works with governments, international organizations, the private sector, civil society, and others to further build the evidence base on the impact of digital scams, particularly in developing countries; foster learning on effective approaches to countering digital scams and the adaptation and adoption of existing tools and strategies that work; build policy momentum to anchor multistakeholder collaboration; and invest in forward-looking capacities to anticipate where scammers are headed to inform agile holistic responses. The foundation of this work is UNDP's digital transformation framework, a coordinated cross-sector approach to build ownership, support human-centered design, mitigate risks, and establish accountability.

UNDP will work with countries and other partners to move from reactive enforcement to integrated action across the scam lifecycle. UNDP welcomes other actors working at the intersection of scams and sustainable development to join this effort.

Conclusion

Digital scams are reshaping the risk landscape of digital development, threatening financial stability, trust, and sustainable development progress. Left unaddressed, they risk undermining the very systems that countries rely on to deliver development gains at scale. Yet this challenge is solvable. With coordinated action across governments, financial institutions, platforms, and civil society, countries can strengthen prevention, improve detection, and support victims while safeguarding digital public infrastructure.

Acknowledgements

The authors of this Issue Brief are Megan Roberts, Engagement Specialist at the United Nations Development Programme (UNDP), and Vitalii Zakhozhyi, Digital Partnerships, Strategic Positioning and Engagement Specialist at UNDP. They would like to thank the following individuals for their valuable inputs and feedback: Benjamin Bertelsen, Yu Ping Chan, Gary Chew, Shermeen Eng, Alessandro Ercolani, Calum Handforth, Brian Hanley, Alexander Hradecky, Jennifer Louie, Alice Marwick, Nils Mueller, Ameera Naguib, Andre Ng, Keyzom Ngodup, Allison Pytlak, Aafreen Siddiqui, Andrei Skorobogatov, and Courtney Weatherby. The authors would also like to thank Justin Foster for his research support.

UNDP's global work on scams is generously supported by the Government of Singapore's Ministry of Foreign Affairs and Infocomm Media Development Authority. This ongoing support is very much appreciated and remains essential. The team also thanks Amy Bennett for copy-editing, Renata Figueiredo for the design and layout, and Andrea Petkovic for support with outreach and communications.

UNDP is the leading United Nations organization fighting to end the injustice of poverty, inequality, and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at undp.org or follow the conversation at @UNDP.

The views expressed in this publication are those of the authors and do not necessarily represent those of the United Nations, including UNDP or the UN Member States.

Endnotes

[i] SDG Digital Acceleration Agenda – UNDP and ITU: https://www.undp.org/publications/sdg-digital-acceleration-agenda.

[ii] Global Anti-Scam Alliance, Global State of Scams Reports, 2024 and 2025. The 2024 report provides a global estimate of one trillion dollars. The 2025 report provides an estimate of $442 billion for the 42 countries included in the survey.

[iii] Asia's scamdemic: How COVID-19 supercharged online crime, NikkeiAsia, November 2022, https://asia.nikkei.com/spotlight/the-big-story/asia-s-scamdemic-how-covid-19-supercharged-online-crime. Scam: Inside Southeast Asia's Cybercrime Compounds, Ivan Franceschini, Ling Li, and Mark Bo, Verso, 2025.

[iv] Ibid.

[v] https://www.undp.org/sites/g/files/zskgke326/files/2024-10/undp_anti-scam_handbook_v1.0.pdf
https://www.undp.org/sites/g/files/zskgke326/files/2025-05/undp_anti-scam_handbook_v2.0.pdf

[vi] Global State of Scams 2025 Report, Global Anti-Scams Alliance, https://www.gasa.org/research.

[vii] UNDP, Anti-Scam Handbook v2.0: Collective Response and Tools to Safeguard Development (Singapore: UNDP Policy Centre, 2025).

[viii] Global Scams Report: The damaging impact of consumer scams on reputation and revenue, Callsign, May 2023, https://programs.callsign.com/hubfs/content/reports/callsign-global-scams-report-reputation.pdf.

[ix] Ibid. Global Anti Scam Alliance, 2025.

[x] UNDP, Inclusive Whole-of-Society Digital Transformation Framework: https://www.undp.org/sites/g/files/zskgke326/files/2023-11/%5Bconcept%20note%5D%20digital%20transformation%20framework.pdf.

[xi] DPI Safeguards Initiative, https://www.dpi-safeguards.org.

[xii] Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia, UN Office of Drugs and Crime, September 2025. https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf.

[xiii] INTERPOL Issues Global Warning on Human Trafficking-Fueled Fraud, INTERPOL, June 2023, https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-issues-global-warning-on-human-trafficking-fueled-fraud.

[xiv] Cybercrime – Our Response, INTERPOL https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-our-response.

[xv] The Scam Epidemic Won't Wait. Neither Should We. Stimson Center, Mario Masaya, September 2025, https://www.stimson.org/2025/the-scam-epidemic-wont-wait-neither-should-we.

[xvi] Ibid. UNDP Anti-Scam Handbook v2.0.

[xvii] Final OECD statistics on official development assistance (ODA) and other resource flows to developing countries in 2024, OECD, December 2025, https://www.oecd.org/en/topics/policy-issues/official-development-assistance-oda.html.

[xviii] INTERPOL Issues Global Warning on Human Trafficking-Fueled Fraud, INTERPOL, June 2023, https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-issues-global-warning-on-human-trafficking-fueled-fraud.

[xix] Measuring digital development - Facts and Figures 2025. ITU, https://www.itu.int/itu-d/reports/statistics/facts-figures-2025/

[xx] The Global Findex Database 2025, World Bank, World Bank Findex 2025, https://www.worldbank.org/en/publication/globalfindex.

[xxi] UNDP Report "The Human and Economic Impact of Digital Public Infrastructure." https://www.undp.org/publications/human-and-economic-impact-digital-public-infrastructure.

[xxii] SDG Digital Acceleration Agenda, ITU and UNDP, 2023: https://www.sdg-digital.org/accelerationagenda

[xxiii] https://50in5.net/ and https://www.dpi-safeguards.org/.

[xxiv] Ibid. ScamGPT.

[xxv] Ibid GASA 2025 and "Australians struggle to spot AI scam images, study shows," Security Brief Australia, January 2026, https://securitybrief.com.au/story/australians-struggle-to-spot-ai-scam-images-study-shows.

[xxvi] Ibid. ScamGPT and UNODC. Disrupting Malicious Uses of AI: An Update, Open AI, October 2025, https://cdn.openai.com/threat-intelligence-reports/7d662b68-952f-4dfd-a2f2-fe55b041cc4a/disrupting-malicious-uses-of-ai-october-2025.pdf.

[xxvii] AI Incident Tracker, MIT AI Risk Initiative, 2025 https://airisk.mit.edu/ai-incident-tracker/timeline-sub-domains.

[xxviii] Compound Crime: Cyber Scam Operations in Southeast Asia, Global Initiative Against Transnational Organized Crime, May 2025, https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

[xxix] Ibid. UNDP Anti-scam Handbook v2.0 and Singapore GovTech.

[xxx] Ibid. Global Anti Scam Alliance.

[xxxi] 2026 Edelman Trust Barometer Global Report: Trust Amid Insularity, Edelman, January 2026, https://www.edelman.com/sites/g/files/aatuss191/files/2026-01/2026%20Edelman%20Trust%20Barometer%20Global%20Report_01.21.26_0.pdf.

[xxxii] Global Employment Trends for Youth 2024, International Labor Organization, August 2024, https://www.ilo.org/resource/article/global-employment-trends-youth-2024-figures#recovery.

[xxxiii] From Loneliness to Social Connection: Charting a Path to Healthier Societies, World Health Organization, Report of the WHO Commission on Social Connection, June 2025, https://cdn.who.int/media/docs/default-source/who-commission-on-social-connection/whocsc-plainlanguage-en_comp.pdf?sfvrsn=c5396dff_6&download=true.

[xxxiv] Ibid. ScamGPT.

[xxxv] Bridging AI and DPI for Long-term Development, Naveen Varshan Ilavarasan, UNDP, April 2025, https://www.undp.org/digital/blog/bridging-ai-and-dpi-long-term-development.

[xxxvi] UNDP AI Trust and Safety Re-imagination Programme, https://www.undp.org/digital/ai-trust-and-safety-re-imagination-programme-building-frameworks-future.