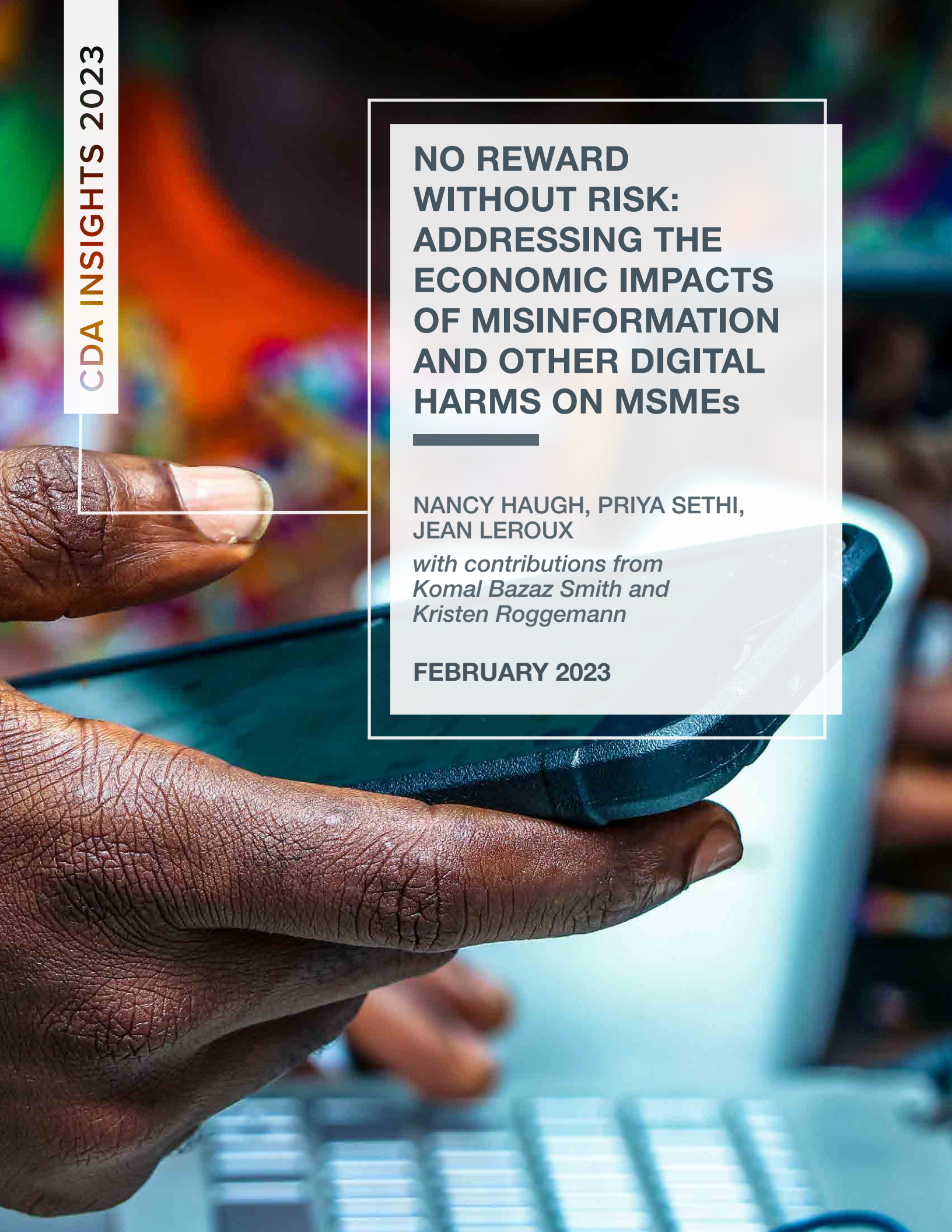


CDA INSIGHTS 2023

NO REWARD WITHOUT RISK: ADDRESSING THE ECONOMIC IMPACTS OF MISINFORMATION AND OTHER DIGITAL HARMS ON MSMEs

NANCY HAUGH, PRIYA SETHI, JEAN LEROUX

with contributions from Komal Bazaz Smith and Kristen Roggemann

FEBRUARY 2023

Contents

CENTER FOR DIGITAL ACCELERATION

DAI's Center for Digital Acceleration helps our clients integrate digital tools and approaches across their portfolio, especially in emerging markets. We do this by engaging end users, building digital products, and understanding the broader ecosystems that drive the success of technology-based initiatives. Our clients include bilateral and multilateral donors, private sector companies, foundations, and others seeking to drive positive social change across sectors including health, governance, agriculture, education, and economic growth.

Cover Photo: Olumide Bamgbelu on Unsplash

Design: Jennifer Geib, www.jennifergeib.com

Executive Summary

MSMEs are fundamental drivers of economic growth in emerging markets. When digital downsides keep them from safely doing business online, their ability to fully participate in the digital economy is inhibited.

Digitalization presents both opportunities and challenges for micro, small, and medium-sized enterprises (MSMEs) in emerging markets. While it creates opportunities for enterprise growth, digitalization also exposes MSMEs to misinformation, fraud, and cyber attacks. Such "digital downsides" can lead to financial losses, reputational damage, loss of customer trust, and other challenges that hinder MSMEs' ability—and desire—to participate in the digital economy. These dynamics have an outsized impact in emerging markets because MSME activity underpins the economic resilience of low- and middle-income countries (LMICs). MSMEs are key engines of economic growth, job creation, and innovation in emerging markets, accounting for 90 percent of businesses globally[1] and 30-40 percent of the GDP in growth markets such as India and Kenya.[2, 3]

In 2022, DAI interviewed 85 MSMEs across Kenya, India, and Cambodia to better understand their experiences of the drawbacks associated with using online tools and platforms. The entrepreneurs we spoke to cited financial harms such as non-payment for goods and services; misinformation, including fake news, malicious rumors, and online bullying and harassment; and technical harms such as hacking, phishing, and social engineering. In Kenya, many of the MSMEs experienced financial harm, whereas in India and Cambodia MSMEs were more likely to encounter general misinformation such as false, negative reviews or COVID-related misinformation (for example, rumors that a particular product causes coronavirus infection).

While few of these businesses stopped using digital tools altogether, the financial losses and reputational damage they incurred eroded their trust in digital tools and platforms. Our research also shows that their adverse experiences are compounded by the limited availability of reporting tools, uncoordinated and one-off mitigation methods, and inadequate training resources to help MSMEs minimize harm to their businesses. By the same token, this training vacuum offers opportunities for development practitioners to serve MSMEs with instruction in digital skills and countering misinformation—previously, such training has been targeted mainly at governance or media-focused entities.

MSMEs are fundamental drivers of economic growth in emerging markets. When digital downsides keep them from safely doing business online, their ability to fully participate in the digital economy is inhibited. In providing MSMEs with opportunities to embrace the digital economy, therefore, we should also equip them with strategies to mitigate risk and tools to enhance enterprise resilience, as detailed in this report. The following recommendations show how development practitioners can reinforce MSME resiliency to misinformation and other digital downsides while enabling MSMEs to leverage online resources for business growth.

Recommendations for development practitioners and agencies seeking to support MSMEs

Invest in comprehensive digital literacy solutions that incorporate cyber hygiene and other skills to combat misinformation.

Building MSMEs' capacity to discern the quality and authenticity of information sources—and stop the spread of misinformation—will be critical for MSMEs' ability to safely operate online and contribute to an ethical business and information environment. Cybersecurity curricula that incorporate misinformation training offer a greater return on investment for the donor community, which should also invest in impact evaluations to assess how digital literacy curricula help MSMEs discern, detect, and respond to digital harms.

Improve the accessibility and availability of digital safety resources.

Cyber awareness campaigns to share best practices, such as two-factor authentication, can help protect MSMEs' online transactions, reducing the risk of hacking or financial information theft. Online platforms and technology companies can include digital safety tools and resources in their existing small business guides and make reporting mechanisms more accessible, available in more local languages, and paired with personal, human support to assist MSMEs in navigating the platforms. Governments and other actors can further support research on the efficacy of applications that identify, flag, and report inaccurate content quickly and clearly.

Invest in community-based approaches and networks.

MSMEs in developing countries often rely on their local networks, small business associations, or ethnic or religious communities to grow their businesses. Investing in community-based trainings or resource hubs offers a scalable approach to reach smaller, newly online businesses that are facing digital harms.

Assist governments to sustain their critical role in the business innovation and protection ecosystem.

Governments can take proactive steps to help businesses protect themselves from online risks. For example, agencies that support small business development could offer protections and accountability mechanisms such as hotlines where consumers and business owners can lodge complaints, report scams, or flag fake accounts; these agencies could also hold perpetrators to meaningful account and advocate for better protections, such as insurance for victims of financial fraud. Donors could fund innovation opportunities to encourage the development of local solutions, tools, or applications that help MSMEs readily identify and report inaccurate content. Existing online communities of MSMEs would be natural partners in facilitating such engagement, which should in turn open up a broader network of MSMEs in need of training and resources.

Introduction

MSMEs in emerging markets are increasingly leveraging digital tools[i] to reduce costs, increase revenue, and reach more customers.[4] As more MSMEs move online, they face different operating environments, risks, and harms, compared to businesses with no online presence. These "digital downsides" include increased exposure and vulnerability to misinformation, fraud, and scams that can negatively affect a business' brand, customer base, and growth potential. These digital downsides disincentivize businesses from using digital tools, which affects their ability to reach new customers, protect themselves from economic shocks or losses, and engage in the global digital economy.

To examine the digital downsides confronting MSMEs, DAI conducted a research study of 85 businesses in Kenya, India, and Cambodia. The study revealed insights into MSME's experiences with digital harms and the mitigation strategies employed to manage the impact on their companies. The interviews also illuminated opportunities for further engagement and training with MSMEs to support their digital transformation journeys. **To support MSME resilience in the digital economy, governments, technology platforms, donors, and development practitioners should (1) recognize how misinformation and other digital harms impact MSMEs and (2) invest in comprehensive digital literacy training, cyber hygiene, and community-based approaches that equip and enable MSMEs to leverage digital tools with trust, safety, and success.**

The Importance of MSMEs and Digitalization in Emerging Markets

The critical role of MSMEs in emerging markets cannot be overstated. MSMEs account for more than 50 percent of employment around the world, including 70 percent of formal jobs in key growth markets such as Kenya, India, and Cambodia.[5] In Kenya, MSMEs generate 92 percent of all new jobs in the country, whereas in India, they employ more than 110 million people, and in Cambodia, they account for 58 percent of the country's gross domestic product. MSMEs play a vital role in determining the growth trajectories of emerging markets, often adopting digital tools and emerging technologies to meet increased demands.

Many digital services that MSMEs in emerging markets introduced during the height of the COVID-19 pandemic remain popular.[6] Consumers in Kenya, for example, are growing accustomed to paying extra for home delivery, and businesses are willing to adapt to meet this demand. Lockdown restrictions similarly pushed businesses toward adopting e-commerce in India and Cambodia. In a survey of 476 Indian MSMEs, 70 percent reported integrating e-commerce platforms into their business model during the pandemic.[7] In Cambodia, 45 percent of MSMEs reported similar integration of digital business tools, an increase of almost 10 percent from the previous year.[8] MSMEs played a fundamental role in helping people adjust to new ways of doing business by fast-tracking delivery of goods and introducing e-commerce platforms to customers that kept economies moving.

---

i Digital tool use and online activity are defined in this study as using social media, messaging services, digital payment services or e-commerce applications, and/or as digitizing back-office applications to buy or sell goods or services, engage with customers, and market the business.

Misinformation and other Digital Downsides facing MSMEs in Emerging Markets

Many MSMEs rely on social media platforms and chat applications to engage customers and share information about their products and services. However, digital risks such as misinformation, which often targets a company's reputation, blends into normal activity and newsfeeds, leading audiences to unwittingly consume false content and share it with their networks.[9] In the fast-moving online ecosystem, rumors about small businesses, previously shared by word-of-mouth or within local communities, find accelerated pathways to reach new audiences and affect customer sentiment. Algorithmic amplification of sensational content[10] creates an environment where misinformation can spread through social media platforms at a speed and scale not seen in traditional media.[ii] Further, as the ecosystem adapts, bad faith actors innovate and evolve to take advantage of online business interactions. The rapid development of artificial intelligence (AI) enhanced manipulation tools[11] is making it easier for malicious actors to develop bots, deepfakes, or other forms of manipulated content that can steer customers away from small businesses. Users with limited technical expertise now face lower barriers to entry for falsifying information or defrauding consumers and business owners.

Malicious actors seeking financial gain, a competitive advantage, or to promote specific content can target MSMEs with financial and technical risks and misinformation that damages customer trust. Such actors can use fake reviews, rumors, or false images to promote negative content or create backlash against a business' brand and reputation. In extreme cases, targeted attacks on individuals, businesses, or communities can lead to human rights violations and exacerbate existing tensions.

METHODOLOGY

This research was conducted through 85 semi-structured key informant interviews in Kenya, India, and Cambodia from June 20–August 30, 2022. Respondents were asked open-ended questions and questions on a Likert scale that assessed their understanding and awareness of misinformation and other digital downsides.[iii] Sampling criteria included MSMEs[iv] that use digital tools to operate their businesses in part or fully online. See Annex A for business demographic data and the full interview questionnaire.

ii "Traditional media" refers here to non-social media platforms (ie. newspapers, television broadcasts, radio, etc.). Respondents indicated that WhatsApp, Instagram, Facebook, Telegram, and Twitter are the primary social media platforms they use to conduct business.

iii Caveat: Not all of the participants in this study were asked the same questions (as shown by "N/A" in the table). The analysis below reflects the four prompts that received the most responses. Please see the full Likert response data in Annex B.

iv This report uses the term "micro, small, and medium enterprises" (MSMEs) to refer to the businesses interviewed for this research, in line with the terminology used by multilateral institutions such as the International Finance Corporation and the United Nations. Although many countries have different official definitions of MSMEs, DAI applied a standardized definition for consistency across all countries included in this research, based on the number of full-time, part-time, or seasonal employees or workers (including the respondent): micro (one employee), small (two to nine employees), and medium (10 to 249 employees).

FIGURE 1

Types of Misinformation and Other Digital Harms

Scholars of misinformation traditionally observe the topic through a governance or public health lens. While both topics are important and necessary for advancing our collective understanding of misinformation, this study reveals an additional lens: a business lens. As part of this study, our field teams asked business owners where they find misinformation and what form it takes (see Annex A.2). For the MSMEs interviewed, **misinformation is synonymous with scams, fraud, and hacking** because in the act of carrying out these activities, a malicious actor provides false or misleading information that harms the business owner.[12] While traditionally labeled as cybersecurity risks, for the MSMEs interviewed, scams, fraud, hacking, and other digital harms resonate as forms of misinformation. In understanding this finding, misinformation researchers and digital development practitioners can better respond to capacity building needs among MSMEs and anticipate future needs regarding MSMEs' digital transformation.

For the MSMEs we interviewed, digital harms took three primary forms: financial, such as stolen bank account information; misinformation, such as false rumors about a business or its products; and technical, such as hacking of a company's social media accounts. See Annex C for a complete list of examples.

FINANCIAL

Some MSMEs we interviewed faced fraud or scams that we categorized as Financial harms.

"Someone stole my bank information."

"My customer refused to pay for the goods they received!"

MISINFORMATION

Other MSMEs experienced digital harm via Misinformation, including online bullying, harassment, fake news, or general misleading information about their business.

"Someone I don't know posted hateful comments on a post I made on social media."

"Someone sent around a link to an article with claims that my product was harmful. It was, of course, false!"

TECHNICAL

Lastly, MSMEs that had their company's images stolen, their social media platforms hacked or cloned, or were a victim of phishing fall under the Technical harms category.

"Screenshots of my products were sent around that were edited to show false pricing and information."

"The password of my business account was stolen, and I lost access to the original account.

Summary of Key Findings

In all three countries, respondents recognized that **digitalization is a double-edged sword.** This study found that **even though digital tools greatly benefit MSMEs in emerging markets, without the resources to address misinformation, scams, and other digital risks, MSMEs in these markets are vulnerable to harms such as financial losses, damaged reputations, and/or loss of customer trust.** Despite these risks, very few businesses completely stopped using digital tools altogether. In fact, even those that had experienced direct harm to their businesses did not abandon digital tools entirely because the reach and growth potential of digital tools and online platforms was deemed worth the risk. Instead, businesses mitigated the digital downsides through a variety of means, including implementing greater due diligence and basic cyber hygiene practices, like two-factor authentication, as well as sharing their experiences within their networks.

The study also identified digital risk training gaps and opportunities to improve MSME resilience to the financial harms, misinformation, and technical harms. These opportunities include enhancing MSMEs' digital capabilities by providing comprehensive digital literacy and cybersecurity training, as well as resources to enhance their awareness of potential risks and to better protect themselves from harm or loss. In addition, this study showcases a wider need to elevate the collective voice of MSMEs seeking redress mechanisms and increased protections from government and the private sector. This report highlights overall trends with detailed findings and recommendations to help strengthen MSME capacity to manage financial harms, misinformation, and technical harms while sustaining digital tool usage in support of their companies.

Financial Loss: The Most Reported Digital Downside

Financial loss, in both actual and potential revenue, was cited by 30 percent of MSMEs in Kenya, 50 percent in India, and 30 percent in Cambodia as the most common harm resulting from operating online. Interviewed MSMEs' examples of digital harms included non-payment for services or goods, traditional advance-fee scams, and clickbait messaging suggesting that a business owner must reimburse goods that were never ordered. In some cases, scammers reached out via social media posing as a real account and sending messages that seemed credible only to devolve into demands or harassment upon further engagement. These scams often used intimidation and fear to induce business owners to pay or make decisions quickly before they were able to check and verify the claims.

While risks such as fraud or scams are not a new challenge for MSMEs, the potential damage financial harms, misinformation, and technical harms can cause has increased due to the unprecedented speed and reach of misinformation online. Since MSMEs rely on social media to interact with customers, the time it takes to mitigate misinformation and other digital harms, as well as restore trust among their consumer base, is a large opportunity cost. When subject to these harms, MSMEs' subsequent financial loss not only consists of the stolen money, but also affects their ad campaigns and outreach to new customers. MSMEs reported that losing access to their social media accounts is a primary fear, as many of them depend significantly on social media as their main channel for customer engagement and business growth.

MSMEs' Trust in Online Tools is Being Eroded

Financial harms, misinformation, and technical harms not only eroded the trust between the customer and the business owner, but they also affect MSMEs' trust in digital platforms. Damage resulting from misinformation is the second-most frequently reported harm in all three countries, as fake reviews, rumors, or fake images were commonly used by malicious actors to promote harmful content, increased scrutiny, or backlash against the business' brand. Following this experience, MSMEs struggled to regain customer trust and report needing to provide additional assurances on the trustworthiness or quality of their business. A country-specific breakdown of findings on financial harms, misinformation, and technical harms, as well as the impact of misinformation on a business' reputation, can be found in Annex D.

FIGURE 2

COVID 19 Misinformation Case Study

One family-run farming business suffered financial losses when rumors about watermelons causing COVID-19 decreased sales. The family was forced to let the watermelons rot in the fields, incurring a $3000-4000 USD loss. The misinformation caused panic, uncertainty, and fear among potential customers and business owners trying to conduct normal business activities.

One widely reported digital harm shared by interviewed MSMEs is COVID-19 misinformation. Nearly half of the interviewed businesses in India report examples of rumors and fake news about the spread of COVID-19 that directly impacted their produce and livestock (see Figure 2). Further, businesses report industry rumors where misinformation resulted in the devaluation of a product, sowing mistrust among customers, and negatively impacting the companies' revenue. Textile and retail business owners especially fear a loss of revenue as customers began buying lower-quality materials from scammers.

As trust decreased, MSMEs assumed the financial and time burden of providing additional, such as photographs of their products, before a customer was willing to commit to a purchase. Further, when the platform itself was slow to, or simply did not, offer clear redress mechanisms to MSMEs, business owners began to doubt the efficacy and utility of online platforms in general. The MSMEs that tried to reach out for support from the digital platforms[v] themselves reported that their requests were not addressed. The downturn effects of losing customer trust in their products and not having digital platforms support them in restoring their reputation required spending additional time and energy to reassure customers of the authenticity and quality in their products.

v About 10 percent of MSMEs sought support from digital platforms in response to digital harms. For more information on mitigation methods used by MSMEs, please see Annex D.

MSMEs Continue to Operate Online – Albeit Cautiously

Despite the recognized downsides, the vast majority of interviewed MSMEs continue to operate online and despite being widely observed, most respondents do not think that digital risks, namely misinformation and fraud, are the most pressing problems facing their online business.[vi] About 30 percent of respondents also indicated they took no mitigation measures often because, in their opinion, their business is too small to be targeted by scams, fraud, misinformation, and hacking in the first place, a sentiment echoed largely by Indian and Cambodian microenterprises.[vii] This finding suggests a major gap in awareness among microbusiness owners about the potential digital risks their business could face. While the benefits of operating online outweighed the risks, about 70 percent MSMEs further report a lack of confidence in their ability to protect their businesses.[viii] They attempt to mitigate risks through various means, such as enhanced due diligence, sharing experiences with others, and/or modifying their online behavior.

For example, despite nearly a third of the interviewed Cambodian businesses reporting no experience or impact of misinformation and other digital harms on their business, they attempted to preemptively prevent losing access to or abandoning their accounts by being more cautious when clicking on links and accessing their accounts from unsecured locations. Business owners expressed a need to constantly monitor social media for incidents where their product photos or content was being used for fraudulent purposes or where malicious individuals post inauthentic, negative reviews (see Figure 3). The burden of mitigating misinformation and other digital harms falls on the business owner, who may not be technically proficient with the cybersecurity safeguards required to safely run their business online.

FIGURE 3

The Opportunity Cost of Hyper Vigilance

Interviewed MSMEs in Kenya note that to prevent reputational misinformation spreading online about their business, they must dedicate resources toward monitoring social media. Melanie, the owner of a medium-sized social media management business, had her business tarnished on Twitter after users began scrutinizing and targeting her business' client management practices. The subsequent online bullying campaign garnered almost 5 million impressions. Melanie ultimately stopped using Twitter and experienced a significant financial loss in ad revenue. She and her staff now monitor social media for mentions of her business. This hyper vigilance is time consuming and labor intensive, and MSMEs like Melanie's do not always have the resources they need to hire additional staff dedicated to social media monitoring.

vi About 38 percent of participants in this study responded to the prompt "I think mis/disinformation is a big problem for my business today." The total average response of 3.6 indicates that of the respondents asked, many MSMEs only slightly agree that mis/disinformation (as defined in this study) is a problem for their businesses. Just more than one-third of the participants of this study respondent to this prompt, and only two Kenyan MSMEs responded to this prompt.

vii Of 28 interviewed microenterprises, 30 percent (0 Kenyan, 5 Indian, and 4 Cambodian) indicate that they did not take mitigation measures and/or that their business was too small to be a target.

viii About 72 percent of participants were asked to respond to the prompt, "I feel equipped to protect my business from mis/disinformation" on a scale of 1 to 5, where 1 is low confidence or strongly disagree, and 5 is high confidence, strongly agree. the average response was 2.8, indicating a slight disagreement in being equipped or a lack of confidence in their ability to protect their business.

"During the first COVID-19 lockdown, there was so much misinformation saying that the national road to my business was closed down. This scared away customers and forced us to delay staff trainings. "

– Stung Treng Cashew Nut Handicraft, Cambodia

PHOTO: DAI

Many MSMEs find refuge in their peers, looking to other business owners within their industry, associations, and business groups for support, a practice that exemplifies their reliance on local networks and supportive business communities (see Figure 4). More than a fifth of all businesses interviewed shared their experiences with others by posting their stories on digital platforms to both call out false accounts and warn others of potential digital risks.

Finally, 14 percent of businesses reported a change in online behavior, such as no longer using social media platforms or digital payment options, after experiencing a digital harm. Of those, most MSMEs changed their digital habits and business models to accept cash on delivery instead of online transactions to avoid further fraud or scams, and three businesses we interviewed were forced to shut down entirely.

FIGURE 4

Community Support to Combat Online Harassment

When faced with online harassment against Muslim businesses, a small business hotel owner in Kerala, India, turned to the Hotel Owners Association in his community. The Association's members voluntarily came out to support the owner on social media and helped him defend against misinformation and hateful rhetoric posted about the business.

MSMEs Need Support to Protect Themselves from Digital Risks

MSMEs expressed an eagerness for learning how to mitigate digital risks, correcting and repairing damage caused by digital harms, and productively utilizing social media reporting channels. Most businesses interviewed said there is little they can do to report fraud or counter misinformation online.[ix] Some respondents indicated that they have no idea what to do in response to financial harm, misinformation, and technical harm, with Cambodian respondents being the least sure how to solve these problems. Respondents further said that they considered reporting incidents to official channels such as law enforcement, though few ultimately submitted such reports. Those who reached out for support from social media platforms found them generally ineffective in responding to their concerns. While social media platforms are making proactive efforts to address misinformation and provide digital safety resources,[13] these resources are not easily accessible or particularly useful for MSMEs in LMICs.

Lastly, respondents identified training and capacity building as a major need and there is a clear gap in prior training on misinformation and technical risks such as account cloning. Training interests largely focus on the general aspects of running an online business, but respondents specifically pointed out the need for training on identifying and reacting to instances of misinformation, mitigating the impact of frauds and scams, and securing their business' information online, as well as more holistic training on cybersecurity and media literacy. This training gap offers an opportunity for development practitioners to consider digital skills training and countering misinformation as broader issues affecting MSMEs, and not limit countering misinformation efforts to governance or media-focused programming.

"It scares me the thought of trending online, whether good or bad, if we trend for the good then we have to expand quick if for the bad it means we are shutting down. If a brand is damaged, it's quit difficult to reconstruct, it requires a lot of resources"

– Royal Super Maize, Kenya

PHOTO: LAURA C/UNSPLASH

ix About 66 percent of participants in this study responded to the prompt "I know what to do if my business is targeted by mis/disinformation." The total average response to this prompt is 3, indicating that respondents have mixed knowledge of what to do when targeted by mis/disinformation.

Country Deep Dives

KENYA

Kenyan MSMEs we interviewed represent a variety of business sectors including agriculture and food service, textiles, retail and jewelry sales, hospitality, events planning, and digital marketing. The businesses use online platforms, such as Instagram, Facebook, Twitter, and WhatsApp, to advertise goods and services, connect with suppliers, interact with customers, and conduct payment transactions.

Experiences of Digital Harm

MSMEs are mindful of the risks associated with fraud and scams and are aware that clickbait headlines are often used to lure users into clicking on dubious links. They are equally aware of the opportunity to use social media to support their business. **This interplay between risk and opportunity is central to the respondents' cited challenges with digital business**. Phelisha, the owner of a small retail business, shared that while she has a modest social media following for her business, "You get to a certain number of followers [and] the business [becomes] at risk of a hack." Similarly, Njeri, the owner of Nails by Njeri, shared that in general, "There is a lack of awareness that most people lose their accounts from phishing attempts. Once you have built an account you can't be taking risks by clicking on links you don't know." These examples highlight the double-edged sword that running a business online creates: the business reaches more potential customers online and, in doing so, increases their exposure to digital risks.

Financial risks were the most frequently encountered digital risk among interviewed Kenyan MSMEs, with one in three reporting an experience of financial harm. Many respondents indicated that these risks were framed as an "opportunity." Scammers and fraudsters promised free social media followers, shopping, or mobile data offerings to MSMEs to entice them into providing their account details or cash. Some of these "offers" were framed as employment or business opportunities and later turn out to be scams. These incidents eroded MSMEs' trust in the platforms they used and created doubt around legitimate business or networking opportunities. In this way, misinformation and other digital harms not only target an individual business, but also potential customers.

Several respondents raised technical risks such as clone accounts appropriating their brand and content as an issue (see Figure 5). Further, respondents also raised hacking of their social media accounts as a challenge. Dimples Kitchen, a medium-sized food delivery business operating through Instagram, shared that the company was hacked twice and the owner only found out about the hacks because customers would reach out and ask the business if they were selling food items that they did not typically carry. The hackers changed the business page's name and content before demanding to meet the business owner in person to hand over a 2,000 Kenyan shilling ransom. The hacker refused money via M-Pesa and the female employees did not feel safe meeting the hacker in person, leading the business owner to hire men to deliver the money. Ultimately, the owner of Dimples Kitchen believes the business was targeted by someone who has made a career out of hacking and ransoming money from small businesses. As a whole, technical risks were reported among interviewed Kenyan MSMEs at a greater frequency compared to India and Cambodia. As evidenced by these examples, fraud, clone accounts, and hacking continue to pose a major risk to Kenyan MSMEs.

Impact

In the case of Melanie, the owner of a medium-sized social media management business, hackers used her Instagram business account and associated financial information to purchase a total of 40,000 Kenyan shillings in ads. This case shows how real financial losses associated with fraudulent on-platform ad-buys- occurred after a business owner's social media account was compromised. Business owners additionally incurred loss from creating a product for a customer that was then not used. For instance, Nancy, the owner of a small bakery, produced a reel for Instagram that was meant to be promoted by an influencer. However, the reel was pulled from the platform because someone falsely reported that it used pirated content and violated community terms of service.

Financial losses also coincided with a loss of trust among both prospective customers of a business and business owners in a digital platform. For example, Solomon, the owner of a microenterprise called Sosisi Creative Arts, had his online artworks stolen by a clone account seeking to get a commission without attributing Solomon as the creator of the art. According to Solomon, when a customer receives subpar work from a scammer pretending to be the genuine artist, it not only cuts into his revenue and makes him distrustful of social media platforms, but it also harms his brand.

FIGURE 5

Technical Digital Risks – The Challenge of Clone Accounts

Jacqueline, the owner of a small bakery called Mam Imran Creations, had images of her cakes stolen on Instagram and reposted as though they did not belong to her business. Clone accounts engaging in these activities represent two primary risks for MSMEs: 1) if the falsified content harms customers by, for example, financially conning them, the legitimate business owner's brand could be damaged; and 2) customers' trust in the real business could be diminished.

FIGURE 6

Buyer Beware

Kenyan MSMEs reported digital harms to online community platforms to seek support, warn others, and even occasionally counter misinformation. For instance, Vicky, the owner of a hospitality microenterprise, shared that a hotel owner claimed she was stealing from him. He then began posting misinformation and false reviews on Buyer Beware about her business, going as far as to falsify a police report. Rather than amplifying the message however, community members using Buyer Beware countered the misinformation and supported Vicky on the platform. As a result, Vicky's experience with misinformation turned into a positive marketing opportunity for her business.

Reputational damage resulting from hacked accounts or inauthentic negative reviews on business community forums such as Buyer Beware similarly impacted interviewed Kenyan MSMEs, though not always negatively, as Figure 6 illustrates. Some participants, such as Melanie, abandoned social media accounts entirely due to the wide reach that misinformation has on Twitter. In a separate incident, Melanie indicated that her business brand was tarnished by an inauthentic negative review posted on Twitter and her personal contact information was released. Similarly, Charity, the owner of a medium-sized retail business, had her Instagram business account hacked and subsequently lost 70 percent of her potential earnings for that day. The hack created uncertainty around the authenticity of her page, and she has been working to watermark her images and rebuild trust ever since. Even after an account is recovered, business owners need to regain the trust of their audience. Although businesses such as Charity's experienced financial loss and reputational damage, they continue to operate online and did not modify their online behavior or digital tool use.

Mitigation

The mitigation efforts reported by respondents focused on two themes: minimizing their companies' exposure to digital risks and minimizing the severity of its impact. More than half of the respondents took a preventative approach by practicing good cyber hygiene and personal due diligence to avoid falling victim to frauds or scams. These approaches included using two-factor authentication; asking the client more questions than usual; looking out for false reviews about their companies; and protecting financial and bank account details on their personal phones. Kenyan businesses also frequently reported sharing their experiences with their community through platforms such as Buyer Beware (Figure 6) to notify others of potential fraudsters and scams.

INDIA

Indian MSMEs we interviewed for this study represented a variety of business sectors, including agriculture and food service, textiles, retail and jewelry sales, and hospitality. The businesses use online platforms, such as Instagram, Twitter, and WhatsApp to advertise goods and services, interact with customers, and conduct payment transactions.

Experiences of Digital Harm

Nearly half of the interviewed MSMEs report experiences with misinformation, primarily rumors and fake news about how COVID-19 spreads, that affected the sale of their produce and livestock. Poultry businesses in Bihar and farming businesses in Jharkand suffered severe financial losses when they were forced to dispose of chickens, watermelons, and even cake from a bakery over fears of spreading the virus. As a result of COVID-19 misinformation, one-third of the poultry businesses interviewed chose to close their businesses while others diversified their offerings to avoid dependency on a single commodity.

In addition to COVID-19 misinformation, rumors and false advertising about the quality and production of specific textile products, such as *chanderi* silk *sarees*, affected the ability of businesses to standardize prices across the industry. Shakil, a textile trader selling batiks in Gujarat, shared how fake Instagram accounts misused the brand name of his products while sharing photos and prices of goods at lower prices than those set by the industry. With little accountability for online businesses or individuals pushing fake content, his business not only lost customers but also suffered reputational damage as customers lost trust in him when he advertised his products. MSMEs' dependency on online platforms to run their businesses requires trust in online transactions and engagements with others. Fear of being exploited erodes that trust, especially following experiences of financial loss or reputational damage. Several businesses that experienced misinformation or online harassment described an emotional toll and distress caused by the incidents, with one business owner changing how she conducts outreach and advertising for her business through social media to avoid further harms.

Indian businesses also experienced fraud and financial-based scams, particularly related to digital payments or one-time password demands on social media. In some cases, business owners received calls or messages from "customers" after products were purchased with claims that the money transferred exceeded the cost of the product and demands that the business owner refund the difference. In other cases, scammers posed as customers and demanded refunds for products they never purchased by showing falsified receipts.

Other examples of digital harm included misinformation attacking the reputation of the business or falsely advertising a product or service. Amrita, a small retail business owner, said "This has happened multiple times. I believe that even if they [came] across my [Instagram] reel, they won't buy because another person has misrepresented me." When she responded to the false claims, the perpetrator took screenshots and posted her response on social media to further tarnish her reputation.

Initial outreach by scammers posing as potential customers is a unique form of disinformation[x] that MSMEs experienced that exacerbated their distrust of online platforms. Of the five cases of disinformation among the interviewed businesses, half consisted of hate speech posted on the business' social media channels. Other examples included the online harassment of women. Further, racist comments or offensive religious attacks caused one microenterprise to lose sales and customers, as hateful comments about their religious identity spread over social media.

FIGURE 7

MSMEs call for more human interaction when seeking support from digital platforms

"The response is always the same. The Instagram algorithm reads it and doesn't find anything wrong. One of those screenshots was a proper chat screenshot of someone abusing me. But nothing happened. It is disheartening. I think there should be a person involved rather than the algorithm."

–Rouble, Madam Sweet Tooth, India

Impact

Among the businesses that reported challenges, the most prevalent impact among the interviewed Indian MSMEs was financial loss followed by reputational damage. Financial scams, fraud, and COVID-19 misinformation led businesses to lose customers or incur financial losses due to a lack of payment from fraudulent customers or from off-loading their produce and livestock.

Most of the interviewed businesses continue to operate online rather than leave digital spaces completely. Ultimately the benefits of remaining online outweighed the risks of financial threats, and some businesses reported that financial harms, misinformation, and technical harms have no impact on their business.[xi] Apart from three poultry farms that were forced to close due to COVID-19 misinformation, most businesses continue to operate online but said they are using more proactive, cautious behavior when encountering suspicious messages.

Mitigation

Indian MSMEs encountered challenges when seeking recourse in the face of digital harms (see Figure 7). Those businesses that turned to digital platforms seeking support experienced challenges with the automated help desk and algorithms. Female business owner Rouble, who operates Madam Sweet Tooth, relies on Instagram and Facebook to advertise her products and engage with customers. Rouble's business experienced COVID-19 misinformation and online harassment as her profile grew. She reported the harassers to the social media platform but said the algorithm did not determine the content to be harmful. This scenario echoes reporting issues mentioned by Cambodian MSMEs below, where business owners struggled to reach live customer support services, and instead had to communicate through automated platforms or algorithms that owners said missed key contextual details of specific complaints. Overall, business owners prefer that real people assist with customer service challenges and disputes instead of automated services.

Lastly, more than a fifth of interviewed businesses mitigated misinformation and other digital harms by sharing their experiences with others. When Chandana, the owner of a medium-sized fabric store, began posting her products online to advertise her business, she was contacted by scammers claiming they had mistakenly sent her the wrong amount of money and asked her to return the balance. After verifying that the transaction was false and confronting the fake customer, she also posted the incident on her Instagram stories. "People can learn from my experience. In many cases, they also relate and say they faced similar things. Additionally, when they learn about the fraud, they [take] extra precautions in their transactions." Similar to Kenyan MSMEs, Indian MSMEs such as Chandana's often rely upon their communities to defend their reputations.

x Disinformation is defined as the deliberate falsification and spread of information with the purpose to mislead and misinform.

xi For more detail on interview responses, see Annex B

CAMBODIA

Cambodian MSMEs we interviewed represented a variety of business sectors, including agriculture and food service, textiles, retail and jewelry sales, hospitality, the beauty industry, and computer services. The businesses use online platforms such as Instagram, Facebook, Telegram, and WhatsApp to advertise goods and services, connect with suppliers, interact with customers, and conduct payment transactions.

Experiences of Digital Harm

Almost one-quarter of Cambodian MSMEs we interviewed, all of which are micro-enterprises, did not experience misinformation. When asked why this might be the case, microentrepreneurs said that their companies are too small and do not have enough of a social media presence to be a target. They also shared that they are likely not targeted because they are hypervigilant to messages from strangers sharing links or promising "free money" (see Figure 8).

FIGURE 8

MSME Due Diligence through Hypervigilance

In discussing their experiences with digital harm, interviewed MSMEs often echoed digital literacy principals. In one example, Sopha Chum, the owner of Indoor Plants & Clay Pots, said she no longer uses Facebook Live on her business page, as users would post false phone numbers in the comments for Chum to contact, only to feign interest in her products. Chum reported not trusting these numbers to be genuine inquiries. This experience was echoed among interviewed MSMEs that did not trust messages that seemed "too good to be true."

The size of the business and the owner's cyber hygiene practices seemingly prevented some microenterprises from experiencing digital harms directly, with only one Cambodian microentrepreneur reporting an experience of direct misinformation. Chha Sreyneang, the owner of food service business Neang Chnai, said that early in the COVID-19 pandemic, rumors spread that eating uncooked or fermented foods such as pickles makes people weak and suppresses their immune systems, making them susceptible to the virus. The rumors spread through social media and were widely believed despite Sreyneang's efforts to counter them. As a result, she lost about 80 percent of her income and had to pick up a second job to survive. In 2022, Sreyneang reopened her business, however, the misinformation deeply impacted her business' profitability.

While financial and technical risks such as scams, fraud, and hacking were the most common experiences among the businesses we interviewed in Cambodia, one-third of these businesses also experienced misinformation. Small businesses were subject to misinformation about how to register their business online and secure business licenses (see Figure 9). For example, Soklin Lim, the owner of a small computer services business, and Hour Kim, the owner of an optical services business, separately heard rumors that the government would fine companies that were operating from a Facebook page without a license. This form of misinformation preys upon business owners' fear of formal repercussion from the Cambodian government. It further suggests that they could lose their platform, the primary source of revenue for many of these small businesses.

Impact

MSMEs cited emotional distress and distrust of online platforms, especially regarding the security of their financial information, as negative impacts of operating online. Vathika and Dara, owners of an online textiles and apparel microenterprise, said: "[We] feel insecure about online payments or keeping money in [the] account. Online business is very challenging. [We are] busy all the time, [it's] very complicated when dealing with each customer, and [we are] constantly worried about fraud and scams." This sentiment resembles the financial challenge of hypervigilance MSMEs take on and incorporates the emotional toll brought about by the digital harms facing MSMEs when operating online.

MSMEs additionally relied on social media platforms and algorithms to boost their ads and marketing, which required linking their business accounts to their personal credit cards to pay for boosting. This practice makes their business accounts particularly attractive to hackers. In April 2022, Chriv Sokun's Instagram account for her beauty business was hacked and she lost access altogether. This loss was devastating for her business, as 70 percent of her customers came through Instagram and, given the hack, she could no longer contact them or advertise her business. When subject to fraud or hacking, the subsequent financial loss not only consisted of stolen money, but also affected the business' ad campaigns and ability to reach new customers. Such technical risks are a primary fear for MSMEs operating online.

Finally, business owners did not just report distrust of the platforms, but also reported a fear that the general misinformation circulating about their industry, products, and procedures would undermine customers' trust in their businesses. Senghorng Lang, a *durian* farmer, noticed in April 2022 that a *durian* wholesaler on Facebook was advertising the sale of local *durian*, a premium fruit in Cambodia that is twice as profitable as *durian* imported from Thailand and Vietnam. However, the timelines did not match. Local *durian* was not available in April as the harvest season for *durian* takes place from late May through July. When Lang tried to verify the *durian* by asking to visit the farm, the wholesaler would not let him. Lang, who usually purchases 10 tons of *durian* during the harvest season thus decided not to purchase from this wholesaler. While Lang did not directly lose the trust of his customers, he feared that the wholesaler's advertising and sale of imported *durian* as a local could lead customers to doubt the quality and authenticity of his produce.

FIGURE 9

Misinformation creates an environment of fear and uncertainty around online business.

In the cases of Lim and Kim, uncertainty over platform policies and regulations around operating an online business, combined with scams and hacking attempts they had experienced, made them wary and distrustful of digital platforms. Both women were concerned over the platform's ability to safeguard their business' financial information and did not trust that there would be recourse if they reported their experiences. Ultimately, the licensing misinformation did not directly impact their businesses but instead added to a growing list of concerns that made both business owners wary of operating online. This growing distrust in platforms because of digital harm was shared by almost 10 percent of the Cambodian MSMEs that rely on the same platforms to operate their business.

For business owners like Kim, misinformation can lead customers to try to negotiate down the price of a product. Customers will claim that another seller has the product retailing for less and thus unintentionally "cheat" the business owner out of revenue over misinformation about product value. Instances like this reinforce the skepticism and mistrust of customers against business owners operating online.

Mitigation

The Cambodian MSMEs that experienced misinformation mitigated it either in the immediate aftermath or retrospectively (see Figure 10). For example, Sreyneang tried to counter the misinformation about fermented foods by sharing the facts with her community and reminding them to not believe everything they see on the internet. She was, however, forced to alter her business model because of the financial loss caused by misinformation. Other business owners practiced due diligence in response to misinformation. For example, Kim reported that she pauses and tries to "double check before believing" information shared by strangers or rumors about business licensing. Some MSMEs said that in the future they would go to the Government of Cambodia's website to check for information on business registration regulations.

FIGURE 10

MSMEs Incorporate Due Diligence into their Business Model

Mr. Lang shared his process for fact-checking the durian wholesaler as follows: "First I see the way they present the information, which [if it is] too tempting [means it] might be not true, [check] who [is] presenting it, [then] verify the source; individual, or institution, check if they are legit, and check if the information is referencing correctly." In the immediate aftermath of this incident, Mr. Lang had to change his business model and procure durian from a different wholesaler.

When it comes to reporting, Cambodian business owners recalled numerous government agencies with whom they filed complaints, such as the Ministry of Commerce when it involved business regulations or licenses, or the Anti-Cyber Crime Department for financial and technical harms. Others reported issues of fraud or misinformation to Facebook and had their accounts restored, however, 52 percent of the respondents were not aware of any reporting options or organizations they could trust if they were subject to digital harm. Ultimately, only Lim's business stopped using social media altogether due to the digital harm.

"I hear rumors about online business licenses. That if a business sells products online, it must get a license or it will get fined."

–Lala Garden, Cambodia

PHOTO: SATYADEV MALLADI /DAI

Training and Reporting Resources Deep Dive

MSMEs interviewed for this study identified training and capacity building as major needs for effective operation of their online business. Of the 85 businesses interviewed, 16 completed digital literacy or online safety training, with only five businesses in Kenya reporting that they attended a course dedicated to online business training and mitigating risks. Many of the small businesses that attended courses were self-taught in digital marketing, social media branding, and advertising, and/or separately took courses on cybersecurity. Businesses specifically identified the need for online safety and security guidance when using social media platforms and on digital payment tools for secure transactions.

Total Requests for Training (top three topics from 85 participants)	
Marketing and branding	37
Internet safety and privacy	35
Safety of online banking and digital payment tools	31

Interestingly, respondents varied significantly about where they sought training resources. Many respondents have found like-minded groups or sought out online communities for help in reaching new markets and customers or as sources where they can share information about the risks of digital business. When asked about specific institutions that should provide training and support, there was a general perception by many business owners that their respective governments could and should do more to support small businesses and provide better protection for all companies. For example, respondents indicated that an official national certification for online businesses could add a layer of trust.

Additionally, businesses across all three countries noted that clear and effective reporting mechanisms for incidents of digital harm are not accessible and, for the few mechanisms that do exist, they need more information about how to utilize these tools. Greater regulations to combat account cloning or legal resources to contact when dealing with harassment or fraudulent accounts are needed. Similarly, participants said that authorities should play a more active role in dispute resolution. Suggestions included working with law enforcement to report incidents and sharing more information about scammers to increase the business community's awareness of potential threats. Lastly, businesses recommended that online safety and misinformation awareness courses be made a requirement for online business registration. They suggested that this mandate would raise the level of awareness of digital harms and provide proactive solutions for businesses to preemptively mitigate risks.

Further, business owners specifically requested more training on how to use platform security tools and coupling marketing and branding training with online safety courses. Respondents suggested several ideas to increase accountability on the part of social media platforms. Whether by proactively removing content posted by known scam networks or fraudsters, or by responding to reports of such activities on their platforms more quickly, respondents said that the platforms they use should do more to make operating a business online safer. Further, MSMEs operating in rural areas where connectivity is low or local dialects are not reflected in automated services had more trouble accessing resources. They said they feel a lack of attention from the platforms and want more direct/human customer support and issue resolution.

Recommendations

Supporting MSME growth and small firms' ability to thrive in the digital economy must include tactics to mitigate the downsides of operating online businesses. The following recommendations are intended to advance this goal and address the gaps identified by the MSMEs we interviewed.

Invest in comprehensive digital literacy solutions for MSMEs that incorporate cyber hygiene and discernment skills to combat misinformation.

Building MSMEs' capacity to identify and evaluate the quality of information sources, recognize false narratives or content, and stop their spread will be critical for MSMEs ability to safely operate online. Training business leaders with a "Learn to Discern"[14] model can help them contribute to an ethical business and information environment while strengthening their resilience to reputational risks and misinformation.

Development practitioners and implementing partners should develop and incorporate information integrity and literacy tools into existing digital literacy training courses to help MSMEs engage effectively and safely online. This involves helping people build scrutiny and healthy skepticism about the information environment in which they work. Sharing trustworthy fact-checking resources and offering guidance on how to spot reputable sources and cross-reference information can increase MSMEs' capacity to identify and mitigate the spread of misinformation online.

Incorporating countering misinformation tactics into cybersecurity training can offer a more holistic cache of digital safety and security lessons, thereby reducing training redundancy and generating more return on investment for businesses. Development practitioners must integrate such digital safety training early into any digital literacy programs and incorporate awareness of risks and harms into the design of new initiatives and activities.

Improve accessibility and availability of digital safety and security resources.

Protecting MSMEs includes helping them reduce the impact of potential exposure to digital risks and build their resilience to future digital harm. Promoting cyber hygiene best practices, such as two-factor authentication on digital payment tools or changing passwords frequently, can help protect MSMEs' online transactions by reducing the risk of hacking or financial information theft that harms their businesses.

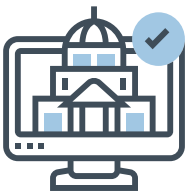
Online platforms and technology companies can include digital safety tools and resources within their existing small business guides. Many social media companies already offer MSMEs resources to launch and scale their businesses on their platforms through business skills and digital marketing training. In connecting with small business communities, platforms should also transparently share information on potential digital harms affecting MSMEs' value chains, their consumers, and the way they use social media to advertise their products and services, while simultaneously offering resources and clear reporting guidelines when MSMEs encounter digital harm. For example, simple user interfaces for reporting tools or nudges[15] to click on fact-checking resources will help MSMEs easily access resources for assistance and understand how to cross-reference or block suspicious content. It is important that these resources extend to emerging markets and become accessible in local languages, with personalized, human support to assist MSMEs in navigating the platforms.

MSMEs must also integrate safety measures to protect their brands and reputations, especially when online reviews and comments affect their activities. Monitoring comments and reviews is time intensive, but donors can support MSMEs, directly or through existing online MSME communities, in developing counter-messaging strategies or responses so that MSMEs can better respond to digital risks.

Invest in community-based approaches and networks.

MSMEs in developing countries often rely on their local networks, small business associations, or ethnic or religious communities to support their companies. Investing in community-based trainings or resource hubs offers a scalable approach to reach smaller, newly online businesses. These trusted allies offer influence and reach, both as an awareness-raising venue to verify or share information on nefarious actors, fraudulent accounts, or trends of false content, and as a response force to support those businesses that have been impacted. As seen in examples from Kenya and India, community members can also rally around business owners to bolster counter-messaging and share facts to counter misinformation. They can serve as a collective voice for MSMEs when advocating for better protections or regulations to support their growth.

Opportunities that spotlight MSME stories and experiences will educate policymakers, regulators, and tech firms of the potential risks MSMEs confront when operating online. Governments and social media platforms could point new MSMEs toward existing community-led reporting mechanisms and groups as part of the online business registration or account creation process. Donors and development practitioners can create dialogue, feedback loops, and channels to share MSMEs' concerns with local leaders, policymakers, and private sector stakeholders so that policies, standards, and regulations are inclusive of MSME interests.



Assist governments to sustain their critical role in the business innovation and protection ecosystem.

Creating an innovation-friendly business environment implies consumer protection, trust in online business activity, and mitigating risks of fraud and theft. To nurture MSME economic growth, governments must take proactive steps to help businesses protect themselves from the potential downsides and negative effects of digitalization. For example, government agencies that support MSMEs could couple requirements for online business registrations with required training or certification courses that raise awareness of digital risks. This includes offering verification methods for businesses operating online, such as Jumia's e-commerce platform[xii] in Kenya, to instill trust and offer assurance for consumers seeking to verify the MSME. Ministries and government agencies that support small business development could offer protections and accountability mechanisms, such as hotlines or bureaus where consumers can lodge complaints and report scams or fake accounts. Taking further action to protect consumers may include penalizing or fining perpetrators, similar to recourse following copyright or intellectual property violations. Such methods can strengthen deterrence and alleviate fears of MSMEs operating online. Ministries of MSMEs can also advocate for better protections when MSMEs are impacted, such as insurance for victims of financial fraud or providing secure digital tools through large banks.

Lastly, the donor community can create and incentivize comprehensive solutions to help MSMEs safely operate online. Donors can invest in **impact assessments and evaluations** to assess how digital literacy curricula help MSMEs discern, detect, and respond to digital harms, while providing evidence-based methods and best practices that apply to emerging economies. Expanding knowledge on how such training has been received should be shared with other funders to inform their programs. Finally, donors can also **fund innovation opportunities** to encourage the development of local solutions, tools, or applications to support MSMEs in identifying, flagging, or reporting inaccurate content quickly and easily. Existing MSME online support communities that offer this form of engagement can be leveraged to reach a broader network of MSMEs in need of training and resources.

xii Jumia is an e-commerce platform offering MSMEs in Kenya a platform to sell goods and services. https://group.jumia.com/about/business-services/sme-tool-kit.

PHOTO: DAVID DVORACEK/UNSPLASH

Conclusion

MSMEs' increased use of digital tools for online business is opening space for their inclusive growth in emerging markets while simultaneously presenting a new set of risks they must navigate. Misinformation and other digital harms can affect MSMEs that may not have the resources or staff to address these problems. The increased complexity and frequency of financial harms, misinformation, and technical harms require increased vigilance at a high resource cost for MSMEs. When MSMEs, especially those with owners from minority or marginalized backgrounds, must stop doing business online because of digital risks, their ability to grow and fully participate in the digital economy is inhibited. This leaves MSMEs poorly positioned to capture the benefits of the global shift to digital business and continue their vital role as engines of economic growth in LMICs. As such, providing MSMEs with opportunities to digitize their operations and grow their businesses online must also be coupled with risk awareness strategies, dual digital literacy and cybersecurity training that incorporates countering misinformation, and other resources to identify and minimize the impact of digital harm, build MSME resilience to misinformation and other digital harms, and support the overall digital economies of emerging markets.

ANNEX A:

Research Methodology

Business Demographics

No.	Country	Location	Gender (of business owner)	Business Sizes
30	Kenya	Nairobi	Female: 21 Male: 9	Micro: 6 Small: 14 Medium: 10
28	India	Chattisgarh, Orissa, Uttar Pradesh, Delhi, Jharkand, Gujurat, Bihar	Female: 10 Male: 17 N/A[xiii]: 1	Micro: 11 Small: 10 Medium: 7
27	Cambodia	Phnom Penh, Siem Reap, Kompot, Kompong Cham, Battambang, Kratie, Steun Treng, Kandal, Ratanak Kiri,	Female: 18 Male: 8 N/A: 1	Micro: 11 Small: 7 Medium: 9

Interview Questionnaire

1. INTRODUCTION AND WARM UP: 5 MINS	
Intent	**Suggested questions / topics**
Introductions	Hello, I'm _____ from XXXX, and I am here with my colleagues _____. [introduce the others in the room]
Purpose, logistics, setting the scene	We are undertaking this study on behalf of DAI to better understand how MSMEs that use digital tools for their business are affected by [insert response type] and its possible impact on the business. This is not an exam; everything you say is going to be helpful to us. The interview will take about 60 minutes. We are here to learn from you so please feel free to be honest with us so that we can fully understand how you are using the internet, so we can try to improve products and services for people like you. We will not be sharing your personal information or business details and will anonymize your response. If we would like to quote something you said, we will ask you first before including it in any report or shared material. Please understand that your participation is voluntary and subject to your approval. If you agree to participate, you have the choice to stop participating in the discussion at any time. Kindly let me know if you do not wish to continue. You may also refuse to answer any question. There will be no penalty for your refusal to answer any question. The information you share will be kept confidential. We will NOT publish your name, phone number, or personal information. The answers you give will be kept secure and combined with several other respondents in a summary report.
Putting respondents at ease/breaking the ice	Respondent introduction [to be adapted for local context] • Name (First name only) • Name of business • Size of business • Date Founded • TBD

xiii N/A is used here to denote firms that did not share the gender of their business owner with our field teams.

2. CURRENT USAGE OF THE INTERNET: 10 MINS	
Intent	**Suggested questions/topics**
Business details	**Tell me about your business. What does it do, make, or sell?** • Do you/your employees currently use the internet or social media platforms for work purposes? If so, which ones? • What device(s) do you primarily use to connect to the internet for work purposes?
How they use internet for business purposes	• What business activities do you use the internet/social media for? Examples: marketing, customer communications, supplier communications, customer research, hiring, etc. • What sort of content do you post or share? • Has using the internet/social media helped your business? How?
3. DIS/MISINFORMATION DEEP DIVE: 30 MINS	
A. Awareness	• When using the Internet or social media, do you encounter any of the following things happening to you? » Online bullying, such as someone sending you a hateful message or comment through social media » Fraud, such as someone stealing your bank information or your money » Fake news defined as false information presented as if it is real and true » Misleading information about an individual or business » Manipulated content such as fake images of a real individual or business » Insert other examples to assist respondent • If yes, where do you encounter [insert response here]? » News websites » Newspapers and magazines » Social media platforms (Facebook, Instagram, etc.) » Messenger platforms (WhatsApp, Telegram, Viber, etc.) » TV channels and radio » YouTube, Reddit, TikTok » Email » Advertisement banners and billboards » I never come across it • When using the internet or social media, tell me about a time when someone sent you something you were not sure about? Please describe. • I feel that I can accurately identify [insert response type] (5-point Likert scale agree-disagree) • (If response is 3-5) Please describe how.
B. Business impact	• I think [insert response type] is a big problem for my business today. (5-point Likert scale SA-SD) • (If response is 3-5) Tell me how. • Has your business been a target of [insert response type]? Please describe what happened. » How did you response to/resolve it? • (If they did not have an experience) If you were to have such an experience, what worries you the most about [insert response type]? Especially for your business? • How did the experience impact your business? Probe here—For example, customer retention, advertising and marketing, brand reputation, competitive landscape, revenue and profit, hiring, staff retention, etc. • Did the experience change how others use/engage with your business? • How has it changed the way you use the internet/social media?

C. Community impact	• Are you aware of other communities that have been the target of [insert response type]? • In your experience, do you see women-owned businesses being targeted by [insert response type] more often than male owned businesses?
D. Response	• I feel equipped to protect my business from [insert response type]. (SA-SD scale) • I know what to do if my business is targeted by [insert response type] (SA-SD scale) • (If business was a target of [insert response type]) Did you share your experience with others? What happened as a result of sharing the experience? • Do you have measures in place to protect against or respond to [insert response type] targeted at your business? Examples may include: re-sharing a post with a disclaimer that this is mis/disinformation to inform your network; encouraging your friends and family to check sources and cross-reference information; checking your own biases with information; etc. • What types of solutions would be helpful to make sure this doesn't happen again? • Are there any people or organizations that you trust that you would go to if you were a victim of [insert your response here]? Examples may include: tech platforms, civil society organizations, journalists, business associations, trusted advisors, etc. • Are there specific measures on the internet or social media applications that you use to protect your business?
4. WRAP UP: 10 MINS	
A. Training	This has been great, thank you. Let's move on to the last topic. • What do you think business owners like you need to feel safe online? Examples may include: training, better protections online, government policies, etc. » Who do you think should provide this? » How should they provide it? • Have you ever attended an addressing [insert response type] training? » Yes, for my business. » Yes, at school, college or education centers. » No, I have never taken a training • If yes, how did you change your behavior to fight against [insert response type]? • What training topics would most benefit your business? » Internet safety and privacy » Safety of online banking and digital payment tools » Fact-checking tools » Media literacy and discernment » How to identify types of [insert response type] » How to report instances of [insert response type] » How to respond to instances of [insert response type] Ethical online business practices » Marketing and branding » Regulations/policies on social media platforms » Other » Don't Know • Are there any resources that we did not mention today that would help your business? • Is there anything else you would like to share about this topic today?

ANNEX B:

Likert Questions and Response Data

Likert Scale Responses from Participants in Kenya, India, and Cambodia					
Question	**Number of Respondents**	**Total Average Response***	**Kenya Average**	**India Average**	**Cambodia Average**
I feel equipped to protect my business from mis/ disinformation	61	2.8	3.28	3.59	2.3
I know what to do if my business is targeted by mis/ disinformation	56	3	3.3	3.3	2.67
I think mis/disinformation is a big problem for my business today	32	3.6	4	3.94	3.33
I feel that I can accurately identify scams	25	3.5	3.91	N/A	3
I feel that I can accurately identify fake news	20	3.3	N/A	3.3	N/A
I feel that I can accurately identify disinformation	17	2.9	N/A	N/A	2.9
I feel that I can accurately identify misinformation	15	2.9	N/A	N/A	2.89
I know what to do if my business is targeted by mal-information	13	2.6	N/A	N/A	2.6
I feel that I can accurately identify mal-information	11	2.8	N/A	N/A	2.8
I feel equipped to protect my business from mal-information	11	2	N/A	N/A	2
I think mal-information is a big problem for my business today	9	3.5	N/A	N/A	3.5
I am able to discern whether content received through the Internet is legit or not	4	3.75	N/A	3.75	N/A
I feel that I can accurately identify a fake link or fraud	2	3.5	N/A	N/A	3.5

ANNEX C:

Types of Misinformation and other Digital Harms

Type	Experience	Examples
FINANCIAL	Financial fraud or scams	Someone stealing your bank information or your money. Non-payment for services or goods or advance-fee scams. Misrepresentation or inflation of the price of inputs or the value of a product.
MISINFORMATION	Online bullying or harassment	Someone sending you a hateful message or comment through social media. • A response from an unknown person on your company's social media accounts harassing other users. • An offensive response to a post you've made on social media from a person you do not know.
	Fake news defined as false information presented as if it is real and true	• A link to a website, a message, or other communication that made sensational claims which later turned out to be false. • A link to a website that contained an article with a misleading or irrelevant headline or information.
	Misleading information about an individual or business	• A product or service that was deceptively advertised. False information shared about the validity or quality of a product or industry. • A social media post making false claims about your or another organization. • A claim that a certain business or their owner was guilty of misconduct or criminal activities, which later turned out to be false. • A claim that a certain law or regulation will be passed, which later turned out to be false. • A claim that a business event was canceled, which turned out to be false.
TECHNICAL	Manipulated content such as fake images of a real individual or business	• A screenshot of an event captioned in a way that misconstrues the context. • Blurry, indiscernible, or decontextualized video footage of an alleged event, product, or service that later turned out to be falsely attributed. • Images or screenshots that have been edited using photo editing software to falsely advertise a product or service. • Videos in which the sound has been altered to add or remove information. • Comments or posts by users that use profile images of other persons or businesses.
	Hacking, social engineering, or phishing scams to steal business information	• Comments or posts by users that make use of AI-generated profile pictures. • Duplicating a business account via "cloning." • Stealing the password of a business account, causing the owner to lose access to the original account. • A message, email, or text inviting someone to click a link, only to then steal that person's information.

ANNEX D:

Country Deep Dives

Kenya

Experience of Misinformation and Digital Harm Breakdown

Type	Example	Instances	Impact
Financial	Scams	4	Distrust among business owners and customers in online interactions Business owners stop using digital tool Financial loss among business owners
	Fraud	13	
Misinformation	Online bullying	1	Distrust among business owners and customers in online interactions No impact
	Attack on brand reputation	3	
Technical	Hacking	5	Financial Loss Brand and reputation damage
	Manipulated Content	4	Financial loss among business owners Loss of trust among customers in the business
No examples	Aware, but no impact to business	7	Business owners did not express concern with misinformation or other digital harms

Impact Breakdown

Financial loss among business owners	9
Loss of trust among customers in the business	7
Distrust among business owners and customers in online interactions and platforms	1
Change in the business owner's online behavior/use of digital tools for conducting business	2
Reputational damage to the business	2
No impact reported	8

*1: Strongly Disagree; 2: Disagree; 3: Neither Agree nor Disagree; 4: Agree; 5: Strongly Agree

Mitigation Breakdown

Due diligence[xiv], cyber hygiene, fact-checking, social media monitoring	17
Change in business owner's online behavior (ie, change online payments, stopped online business, cash on delivery, stopping posting online)	3
Counter messaging from business and training provided to employees	2
Reporting to police/formal institutions or platform support	2
Change in business model	6
Sharing experience with community on social media	6

India

Experience of Misinformation and Digital Harm Breakdown

Type	Example	Instances	Impact
Financial	Scams	5	Distrust among business owners and customers in online interactions Financial loss among business owners
	Fraud	8	
Misinformation	Cyber-bullying, harassment	2	Distrust among business owners and customers in online interactions
	Communal rhetoric, hate speech	1	
	COVID rumors	11	Financial loss among business owners Reputational damage to the business Loss of trust among customers in the business
	Textile industry rumors	5	
	Discrediting business online	2	
Technical	Manipulated content	2	Financial loss among business owners Change in the business owner's online behavior/use of digital tools for conducting business
	Hacking, social engineering, or phishing scams	10	Financial loss among business owners Change in the business owner's online behavior/use of digital tools for conducting business Distrust among business owners in using digital tools to conduct business
No examples	Aware, but no impact to business	5	Business owners increased due diligence and cyber hygiene practices to avoid misinformation and other digital harms

xiv This can include not accepting friend requests from strangers, establishing two-factor authentication, cross checking unusual emails with IT professionals, and not clicking on links or downloading files from organizations outside of your network

Impact Breakdown

Financial loss among business owners	14
Loss of trust among customers in the business	4
Distrust among business owners and customers in online interactions and platforms	3
Change in the business owner's online behavior/use of digital tools for conducting business	3
Reputational damage to the business	6
No impact reported	7

Mitigation Breakdown

Due diligence, cyber hygiene, fact-checking, social media monitoring	6
Change in business owner's online behavior (ie, change online payments, stopped online business, cash on delivery, stopping posting online)	1
Counter messaging from business and training provided to employees	1
Reporting to police/formal institutions or platform support	0
Change in business model	2
Sharing experience with community on social media	6

Cambodia

Experience of Misinformation and Digital Harm Breakdown

Type	Example	Instances	Impact
Financial	Scams	9	Financial loss among business owners
	Fraud	4	Loss of trust among customers in the business Distrust among business owners and customers in digital platforms and online transactions
Misinformation	Rumors of online business registration	4	Financial loss among business owners
	Industry rumors	2	
	COVID rumors	4	Change in the overall business model

Technical	Hacking	7	Financial loss among business owners Distrust among customers in online interactions with the business Reputational damage to the business
No examples	None	7	Business owners did not express concern with misinformation or other digital harms

Impact Breakdown

Financial loss among business owners	8
Loss of trust among customers in the business	3
Distrust among business owners and customers in online interactions and platforms	3
Change in the business owner's online behavior/use of digital tools for conducting business	1
Reputational damage to the business	5
No impact reported	9

Mitigation Breakdown

Due diligence, cyber hygiene, fact-checking, social media monitoring	11
Change in business owner's online behavior (ie, change online payments, stopped online business, cash on delivery, stopping posting online)	1
Reporting to police/formal institutions or platform support	4
Change in business model	9
Sharing experience with community on social media	7

ANNEX E:

Stakeholder Activity Map

The following matrix provides an illustrative example of which recommended activities various stakeholders can engage in to respond to MSMEs' concerns regarding digital risks.

	Stakeholders			
Activities	**Governments**	**Social Media - Tech Platforms**	**Donors**	**Development Practitioners**
Increase awareness of risks	**X**	**x**	**x**	**x**
Lean into community support networks			**x**	**x**
Strengthen discernment skills and digital risk response tools		**x**	**x**	**x**
Improve business resiliency	**X**	**x**	**x**	**x**
Enable innovation and protection	**x**		**x**	
Impact assessments and evaluations			**x**	**x**
Fund innovation and research opportunities	**x**		**x**	**x**

Endnotes

1 The World Bank. 2023. "Small and Medium Enterprises (SMEs) Finance." https://www.worldbank.org/en/topic/smefinance.

2 Buteau, S. 2021. "Roadmap for Digital Technology to Foster India's MSME Ecosystem – Opportunities and Challenges," *CSI Transactions on ICT,* 9(4): 233-244.

3 UNDP. 2021. "Supporting MSME recovery and resilience during and post COVID-19," United Nations Development Program, https://www.undp.org/kenya/blog/supporting-msme-recovery-and-resilience-during-and-post-covid-19.

4 DAI. 2021. "Insights from Emerging Markets: MSMEs and Digital Tool Use amidst the COVID-19 Pandemic," *Center for Digital Acceleration*, https://www.dai.com/our-work/solutions/digital-acceleration-solutions/msme-study.

5 The World Bank. 2023. "Small and Medium Enterprises (SMEs) Finance." https://www.worldbank.org/en/topic/smefinance.

6 Digital Society. 2020. "How Technology is Changing the Landscape for Businesses in Kenya," *Vodafone,* https://www.vodafone.com/news/digital-society/how-technology-is-changing-the-landscape-for-businesses-in-kenya.

7 Goyal, T.M. 2022. "E-commerce, digital transformation keys for growth of MSMEs," *The Economic Times*, https://economictimes.indiatimes.com/small-biz/sme-sector/e-commerce-digital-transformation-keys-for-growth-of-msmes/articleshow/90741524.cms?from=mdr.

8 DAI. 2021. "Insights from Emerging Markets: MSMEs and Digital Tool Use amidst the COVID-19 Pandemic – Cambodia Country Brief," *Center for Digital Acceleration*, https://www.dai.com/uploads/cambodia-country-brief.pdf.

9 Kuru, O. et al. 2022. "Chapter 7 Encountering and Correcting Misinformation on WhatsApp: The Roles of User Motivations and Trust in Messaging Group Members," in *Disinformation in the Global South*. John Wiley & Sons Inc. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119714491.ch7.

10 Petropoulos, G. 2021. "The Great Infodemic; Time to Consider a Fake News Tax," *Bruegel.* https://www.voxpol.eu/algorithmic-transparency-and-content-amplification/.

11 Honigberg, B. 2022. "The Existential Threat of AI-Enhanced Disinformation Operations," Just Security. Accessed August 11, 2022. https://www.justsecurity.org/82246/the-existential-threat-of-ai-enhanced-disinformation-operations/.

12 UNHCR. 2022. "Factsheet 4: Types of Misinformation and Disinformation." https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf.

13 Google. 2023. "The Applied Digital Skills." https://grow.google/applied-digital-skills/; Facebook. 2023. "Digital Literacy Library." https://www.facebook.com/safety/educators; Twitter. 2023. "Report impersonation accounts." https://help.twitter.com/en/safety-and-security/report-twitter-impersonation.

14 IREX. 2023. "Learn to Discern (L2D) – Media Literacy Training." https://www.irex.org/project/learn-discern-l2d-media-literacy-training.

15 Moonshot. 2023. "The Redirect Method." https://moonshotteam.com/the-redirect-method/.

Acknowledgments

The authors wish to thank the following people and organizations for their contributions to and support of this research: Kathleen Duffy, Shikoh Gitau and Qhala, Osama Manzar and the Digital Empowerment Foundation, Sotheavy At, Anand Varghese, and Araba Sapara-Grant.

PHOTO: STEWARD MASWENENG/UNSPLASH

SHAPING A MORE LIVABLE WORLD.

www.dai.com

@daiglobal