MONTHLY BULLETIN

SEPTEMBER 2026|#06







In this Issue

This month's bulletin examines the growing challenges posed by online scams across Southeast Asia, highlighting intensified enforcement efforts, evolving criminal networks, and strengthened regional cooperation. It also explores the economic and financial impact on financial integrity, businesses, and public confidence. The featured research further examines country-level risks across Southeast Asia, with particular attention to Cambodia's exposure, socioeconomic impacts, and responses.

This edition also features key economic data tracking September's commodity prices, oil prices, and exchange rates, and concludes with recent researcher training activities and events organized by the APM Center.

About APM Center

The **Akkak Pundit Sapheachar AUN Pornmoniroth Center for Policy Studies and Training (APM Center)** was established to advance knowledge, foster innovation, and enhance capacity across a wide range of stakeholders to support economic development and the development of the banking sector in Cambodia through its research and human resource development initiatives. The center operates under the technical and financial guardianship of the Agricultural and Rural Development Bank (ARDB).

+855 93-294-793 / +855 78-824-411
www.apmcenter.ardb.com.kh
info_apmcenter@ardb.com.kh

NEWS SPOTLIGHT

Crackdowns Intensify as Southeast Asia's Scam Networks Adapt

By: Tith Ratana & Pengte Sao Socheata

Online scams have become an increasingly urgent transnational challenge across Southeast Asia, prompting governments, law enforcement agencies, and private-sector actors to intensify efforts against the networks supporting them. According to ASEAN (2026), estimated scam losses across ASEAN reached USD 23.6 billion in 2024, but the relative economic burden varied considerably across countries. As shown in Figure 1, estimated losses among six Southeast Asian countries ranged from around 0.2% to 2% of GDP, with Malaysia recording the highest estimated share at approximately 2%, followed by the Philippines at around 1%. Estimated losses were lower but still economically significant in Thailand, Viet Nam, Singapore, and Indonesia. These differences show that while the scale of exposure varies across national economies, scams are imposing measurable financial costs across the region. The United Nations Office on Drugs and Crime (UNODC, 2026) estimated that victims across East Asia, Southeast Asia, Australia, and New Zealand lost USD 88.3 - 114.1 billion in 2025, highlighting the wider international reach of scam networks.

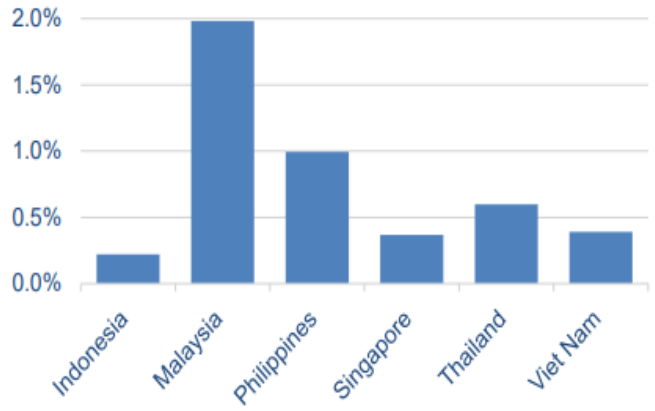


Figure 1: Scam losses as a proportion of GDP (%) (ASEAN, 2026)

From Domestic Measures to ASEAN-wide Cooperation

The cross-border nature of online scams has made action by individual Southeast Asian countries increasingly difficult on its own. Scam calls and messages can originate in one country while targeting victims in another, while criminal networks can exploit differences in SIM card registration, caller-ID authentication, and other national safeguards. As shown in Figure 2, the predominant source of scam communications varies across ASEAN member states. Domestic calls are more prominent in Cambodia, Indonesia, Lao PDR, Malaysia and the Philippines, whereas international calls are more prominent in Brunei Darussalam, Myanmar, Singapore, Thailand and Viet Nam. For scam-related SMS, domestic sources are more prominent in most countries shown, although international sources are more prominent in Singapore and Thailand (ASEAN, 2026). This has pushed ASEAN member states toward greater regional coordination alongside their domestic anti-scam measures. In response, ASEAN established an Anti-Scam Working Group in 2024 to strengthen information sharing, training, and capacity building, followed by the ASEAN

Declaration on Combating Cybercrime and Online Scams in 2025. Regional efforts have since expanded to include stronger SIM card and telecommunications controls, real-time scam detection, cross-border information sharing, and the development of mechanisms for tracing scam communications across jurisdictions (ASEAN, 2026; Alifha, 2026). These measures reflect growing recognition that disrupting transnational scam networks requires countries to close gaps between their national systems and coordinate across borders rather than responding to each case in isolation.

Crackdowns Move Beyond Physical

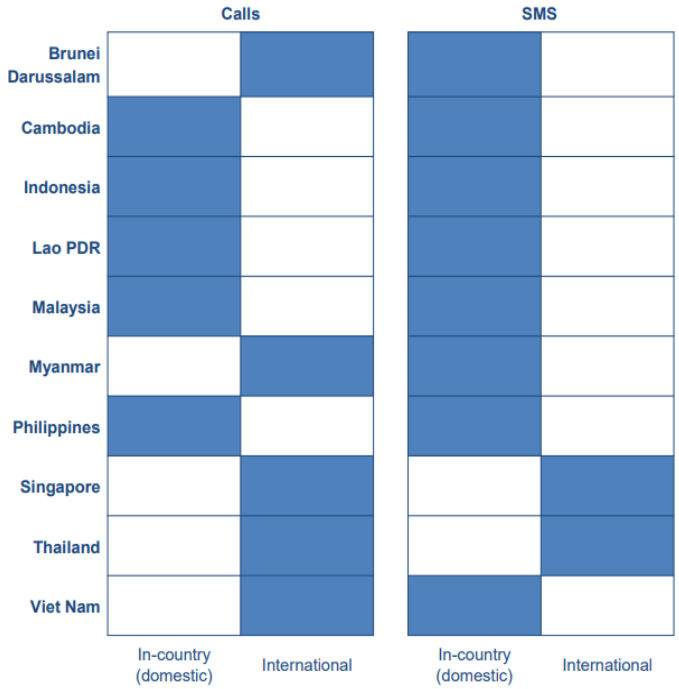


Figure 2: Most scam calls/SMS in AMS originate within the country, but international sources remain a growing threat (ASEAN, 2026)

Compounds

Enforcement is also increasingly targeting the financial and digital infrastructure that allows scam networks to operate. In April 2026, the U.S. Department of Justice's Scam Center Strike Force announced coordinated actions against Southeast Asian scam networks that included restraining more than USD 700 million in cryptocurrency, seizing 503 fraudulent investment websites, and taking control of a Telegram channel allegedly used to recruit workers to a Cambodia-based scam compound (U.S. Department of Justice, 2026a).

The response has since expanded through cooperation with technology and financial companies. During a U.S.-led "Disruption Week" in May 2026, participating companies disrupted criminal activity across more than 1.4 million social media and email accounts, interrupted malicious network connections, and decommissioned servers and hosting infrastructure linked to scam networks in Southeast Asia. Information sharing also enabled private-sector participants to freeze more than USD 3.8 million in cryptocurrency, while Thai authorities arrested seven suspected scammers and opened additional investigations (U.S. Department of Justice, 2026b).

Enforcement continued to target the service infrastructure surrounding the industry. In September 2026, U.S. authorities seized Telegram channels associated with an alleged illicit marketplace offering services to scam center operators, including customized fraudulent investment websites, money laundering, and recruitment. Approximately USD 52 million in cryptocurrency was restrained in the operations, bringing cryptocurrency

restrained by the Scam Center Strike Force to approximately USD 938 million (U.S. Attorney's Office for the District of Columbia, 2026).

Stronger Enforcement but an Adaptive Industry

Despite mounting pressure, recent evidence suggests that disruption does not necessarily eliminate scam operations. Criminal networks can replace seized digital infrastructure, relocate operations, or shift toward alternative services and jurisdictions. In April 2026, for example, U.S. authorities reported seizing a new fraudulent investment domain associated with scam centers in Myanmar after an earlier version of the platform had already been seized. UNODC has similarly described Southeast Asia's organized-crime landscape as increasingly interconnected and technology-enabled, allowing criminal actors to draw on shared financial, technological, and logistical services and expand across illicit markets (U.S. Department of Justice, 2026a; UNODC, 2026).

This adaptability is changing the nature of the response. Closing physical compounds remains important, but authorities are increasingly attempting to disrupt the broader ecosystem that sustains them, including financial proceeds, digital platforms, telecommunications infrastructure, recruitment channels, and criminal service providers. ASEAN's 2026 framework similarly emphasizes that effective anti-scam measures must be adaptive, technologically enabled, and supported by cross-border cooperation because scammers can exploit the weakest safeguards across jurisdictions (ASEAN, 2026).

The international response continued to broaden in September 2026, when governments, law-enforcement agencies, financial regulators, cybersecurity experts, technology companies, and international organizations met in Phnom Penh for the International Conference on Combating Online Scams (ICCOS-2026). Co-sponsored by Cambodia, UNODC, INTERPOL, and the Lancang-Mekong Integrated Law Enforcement and Security Cooperation Centre, the conference reflected growing recognition of online scams as a transnational challenge requiring cross-government and cross-sector cooperation (ASEAN, 2026).



FEATURED RESEARCH

Beyond Cybercrime: The Economic Cost of Online Scams in Southeast Asia

By: Leang Seakleng, Sara Sreyneath, and Tung Davy

Rise of Online Scams in Southeast Asia

Evolution of the Online Scam Economy

Online scams in Southeast Asia are not new, but their structure and scale have changed substantially. Earlier operations were largely scattered and relied primarily on telephone-based fraud involving relatively small groups. From the mid-2010s, however, operations became increasingly consolidated and professionalized, with modern scam centers recruiting specialized workers, including ICT and digital-sales personnel (UNODC, 2024; Gunn, 2025). This transformation was linked to the expansion of casinos and offshore online gambling from the mid-2000s (UNODC, 2024).

The COVID-19 pandemic marked a major turning point rather than the beginning of the industry. Travel restrictions reduced casino activity and cross-border mobility, while growing reliance on digital platforms, payments, and cryptocurrencies created new opportunities for criminal networks. With much of the necessary infrastructure already in place, some casino complexes were repurposed into large-scale scam compounds, accelerating the expansion of cyber-enabled fraud (UNODC, 2023). ASEAN-Australia Counter Trafficking similarly links the rise of industrial-scale scam compounds to the convergence of declining casino activity, technology, social media, crypto-currency, and other enabling conditions (ASEAN-Australia Counter Trafficking, 2026).

By the mid-2020s, the scam economy had developed into a more organized and trans-national criminal ecosystem, increasingly intersecting with human trafficking, money laundering, corruption, and organized crime, a convergence described as “poly-criminality” (ASEAN–Australia Counter Trafficking, 2025). Major operations have been documented in Lao PDR, Myanmar, Cambodia, and the Philippines, while UNODC (2024) estimates that organized criminal networks engaged in cyber-enabled fraud across Southeast Asia generate between USD27.4 billion and USD36.5 billion annually.

Technological advances have further increased the sophistication and reach of these operations. AI-generated content, deepfakes, translation software, and virtual assets enable networks to target victims across borders and move illicit proceeds through increasingly complex channels. Despite mounting enforcement pressure, scam operations continue to evolve by relocating, fragmenting, and adapting their operating models and geographic reach.

Geographical Concentration and Regional Spread

Southeast Asia's online scam economy is concentrated in several major locations but operates across national borders, with compounds established in urban developments, border areas and special economic zones. Loughlin (2026) traces this expansion partly to the offshore movement of Chinese-linked capital and criminal networks following tighter restrictions on gambling and financial activities in China. With support from local intermediaries providing access to property, labor, and financial services, operations expanded into different Southeast Asian jurisdictions.

Border areas are particularly important to this regional geography. Myanmar's Myawaddy region illustrates how scam compounds can operate in territories involving armed groups and local authorities, while northern Lao PDR hosts scam activity around the Golden Triangle SEZ near the Thai and Myanmar borders. Thailand plays a different role: its proximity to major scam locations makes it an important transit and enforcement jurisdiction connecting neighboring countries through cross-border movement and infrastructure. In the Philippines, by contrast, scam operations have been associated more closely with commercial developments and offshore-gambling facilities, demonstrating the different environments in which these networks operate (Loughlin, 2026).

These locations are connected through the cross-border movement of workers, capital, and illicit financial flows. Recruitment networks supply workers from different countries, while offshore banking, crypto-currency, and informal financial channels connect scam operations to financial centers beyond their host jurisdictions (Loughlin, 2026). The regional scam economy therefore extends beyond the physical locations of individual compounds, linking operating centers, transit jurisdictions, and international financial networks.

Operating Structure of the Modern Scam Economy

Modern scam operations in Southeast Asia increasingly resemble organized enterprises rather than loosely coordinated groups of individual scammers. Gunn (2025) describes scam centers as organized or semi-structured systems that can mimic legitimate businesses, with personnel assigned to functions such as technical support, marketing, victim engagement, and payment processing. Specialized tasks may also be outsourced through cybercrime-as-a-service providers, allowing different actors to contribute specific capabilities to the wider operation.

Recruitment forms an important part of this structure. Scam centers may employ willing participants but also rely on people trafficked for forced criminality, often recruited through deceptive job advertisements and subsequently compelled to conduct online fraud.

Social media, messaging applications, and online advertisements facilitate cross-border recruitment, while some operations specifically seek workers with technical or digital skills. As a result, some individuals conducting victim-facing scams may themselves be victims of trafficking and exploitation (Gunn, 2025).

Within the operation, technology enables networks to standardize and scale victim engagement. Bulk-messaging systems, auto-dialers, and VoIP software can reach large numbers of targets before responsive victims are transferred to human operators. Workers may then use prepared scripts and customer relationship management (CRM) systems to manage conversations and victim profiles, while fraudulent websites can display fabricated balances or restrict withdrawals to reinforce the appearance of legitimate investment platforms (UNODC, 2025a).

The final stage involves receiving and moving criminal proceeds. Scam operations rely on money-mule accounts, underground banking, automated transfers, and virtual assets, while cryptocurrency conversion and mixers or tumblers can further obscure transaction trails and complicate cross-border tracing and recovery (UNODC, 2025a; Gunn, 2025).

Technology and Financial Infrastructure

Technology has become a critical enabler of Southeast Asia's scam economy, increasing the scale, credibility, and sophistication of fraud. Criminal networks increasingly use AI-generated deepfakes, synthetic identities, voice cloning, and real-time facial manipulation to strengthen impersonation, romance, and investment scams. UNODC (2024) identified more than 10 deepfake software providers marketing services to criminal groups involved in cyber-enabled fraud in Southeast Asia, while its 2025 assessment found that some voice-cloning tools require as little as 20 seconds of audio (Gunn, 2025). INTERPOL (2026a) also reported that discussions of deepfakes on cybercriminal forums and Telegram channels used by Southeast Asian threat actors increased by approximately 600% between February and June 2024, indicating the growing integration of AI into the regional criminal ecosystem.

Telecommunications infrastructure enables these operations to reach victims across jurisdictions. Automated calling systems, VoIP services, SIM boxes, and other tools allow communications to be conducted or disguised remotely and at scale. Gunn (2025), for example, documented the use of IMSI-catchers and false base stations in Thailand to imitate mobile infrastructure and distribute fraudulent messages. Differences in caller-ID authentication, SIM-card controls, and other national safeguards can also be exploited by transnational syndicates, increasing the importance of cross-border coordination (ASEAN, 2026).

Financial infrastructure, meanwhile, enables scam proceeds to be transferred and concealed across accounts, assets, and

jurisdictions. Criminal networks use mule accounts, digital financial services, and cryptocurrencies, with funds sometimes converted across virtual assets or routed through mechanisms designed to obscure transaction trails. In 2026, Thai authorities uncovered scam proceeds moved through cryptocurrencies and cross-chain token swaps, with one associated wallet processing more than USD 122.5 million in ten months. In a separate case, authorities in Singapore and Oman blocked a USD 6.6 million cross-border transfer linked to a business email compromise scam (INTERPOL, 2026b).

Together, these systems reinforce one another: technology expands the reach and credibility of scams, while financial infrastructure enables the proceeds to move rapidly across borders, making detection, disruption, and asset recovery more difficult.

Adaptation and Displacement Following Crackdowns

Despite intensified crackdowns across Southeast Asia, scam operations have often adapted rather than disappeared. Enforcement pressure can lead operations to temporarily close, relocate or fragment into smaller and less conspicuous facilities, with workers and equipment transferred between sites or across borders (Amerhauser & Thill, 2025). This pattern has been observed across several regional scam hubs and may also be extending beyond established locations, with UNODC (2025b) identifying signs of a Southeast Asia-style operation emerging in Timor-Leste. These developments suggest that crackdowns can disrupt individual sites without necessarily dismantling the wider networks behind them.

Economic and Financial Impact

The most immediate economic consequence of online scams is the transfer of wealth from victims to criminal networks. The ASEAN Guide on Anti-Scam Policies and Best Practices cites an estimate by the Global Anti-Scam Alliance that scam losses across Southeast Asia reached approximately USD 23.6 billion in 2024 (ASEAN, 2026). At the household level, the ASEAN Consumer Scam Report 2026, covering Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam, found that 8% of surveyed consumers had been scammed during the previous 12 months. Among victims, 68% lost money; of those suffering financial losses, 82% recovered nothing, and only 10% recovered their losses in full (Falvey, 2026). As shown in Figure 3, exposure varied across the six markets, with reported scam incidence highest in Vietnam (13%) and the Philippines (10%), compared with 5–6% in the other surveyed countries (Falvey, 2026). Such losses reduce savings and disposable income available for consumption, investment, and other financial obligations.

Losses can also vary considerably by scam type. Singapore illustrates how investment and impersonation scams can generate disproportionately large financial damage.

Although total reported scam losses fell 17.9% to approximately SGD 913.1 million in 2025, investment scams accounted for SGD 336.2 million, government-official impersonation scams cost SGD 242.9 million, and job scams cost SGD 123.5 million. Cryptocurrency-related losses reached approximately SGD 182.2 million, or 20% of total losses, highlighting the role of digital assets in scam-related financial transfers (Singapore Business Review, 2026).

Businesses face both direct losses and additional defensive costs. Fraud may involve business email compromise, false invoices, executive or supplier impersonation, and manipulated payment instructions. At the same time, businesses must also spend money on cybersecurity, transaction verification, staff training, and internal controls. Bank Negara Malaysia warned that businesses, including financial institutions, were increasingly targeted by sophisticated scams involving AI-generated impersonation. Malaysian police recorded 12,110 online-fraud cases involving RM 573.7 million in losses in Q1 2025, illustrating the broader resources businesses and institutions must devote to securing legitimate digital transactions (Ministry of Digital, 2025).

Financial institutions also bear costs even when they are not the direct victims. Banks must strengthen fraud monitoring, investigate suspicious transactions, and continuously invest in operational and cyber resilience. Bank Negara Malaysia (2026) reported continued investment in operational-risk controls in the second half of 2025, while losses associated with operational-risk incidents remained relatively small at 0.11% of total banking-system capital. Substantial consumer scam losses therefore do not necessarily imply banking-system instability; for financial institutions, the more immediate effects concern operational risk, fraud prevention and compliance costs, payment integrity, customer protection and reputation.

Beyond direct financial losses, scams can also weaken confidence in the digital economy. *Figure 3* shows that 66% of ASEAN-6 consumers changed their behavior because of scams, far exceeding the 8% who personally reported being scammed in the previous 12 months. This gap was particularly pronounced in Vietnam and the Philippines, where 79% and 78% of consumers, respectively, changed their behavior despite reported scam exposure of only 13% and 10% (Falvey, 2026). The findings suggest that the effects of scams extend well beyond direct victims, as wider concerns about fraud can influence how consumers engage with digital services. Consequently, the economic impact is not limited to stolen funds but can also include more cautious digital behavior and weakened confidence in the broader digital economy.

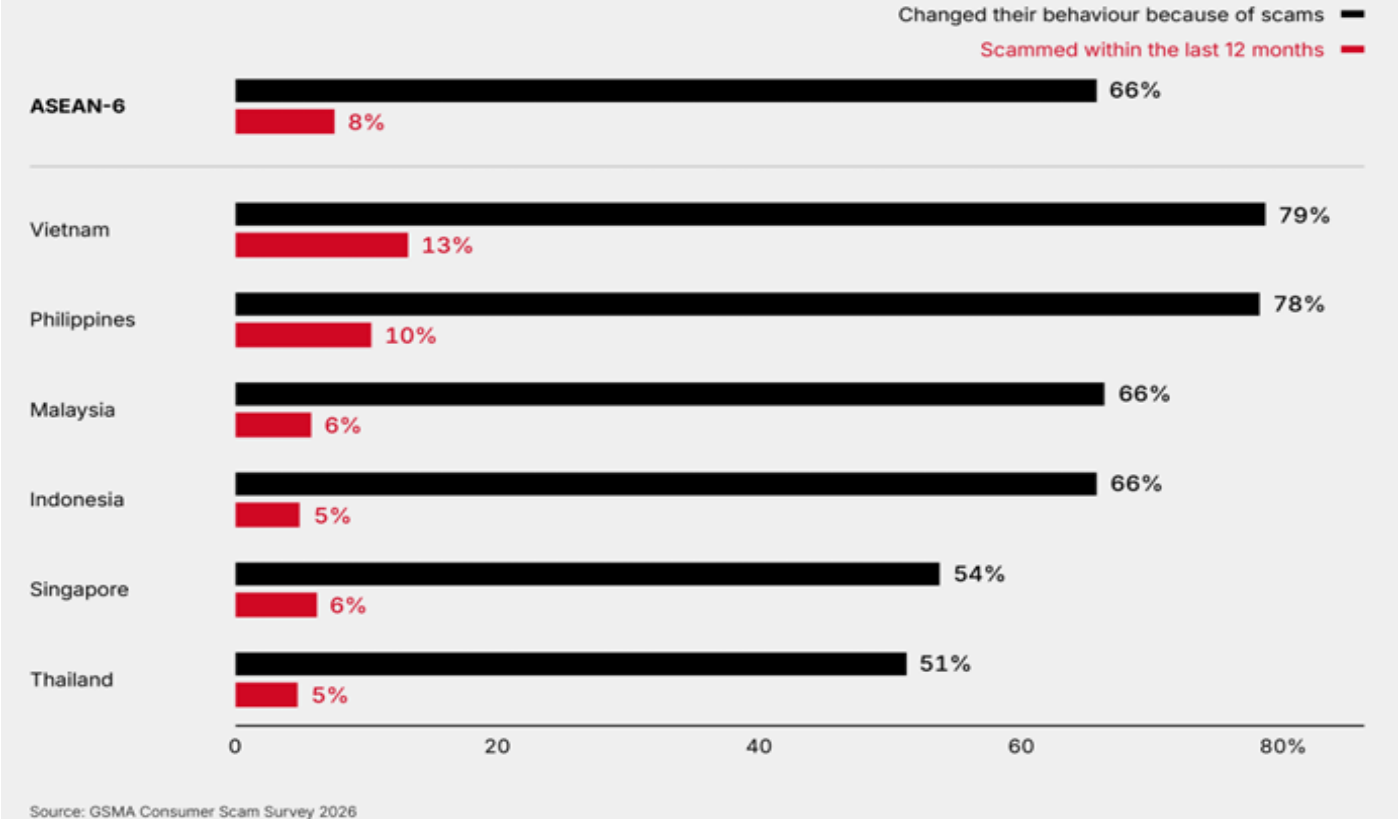


Figure 2: How Scams touch ASEAN consumer (Falvey, 2026)

Country-Level Risk Profiles Across Southeast Asia

❖ *Thailand:* Thailand faces a multi-dimensional scam risk involving both its digital financial system and proximity to major cross-border scam centers. As tighter controls restrict conventional mule accounts, fraudsters have increasingly shifted funds to cryptocurrency mule accounts, making transactions more difficult to trace. The share of reported loss value transferred to these accounts rose from approximately 75% in Q4 2024 to 90% in Q1 2025 (Sodsrichai, 2025). Authorities have since expanded controls to bank and e-money accounts, including measures addressing the growing misuse of accounts belonging to young people. These interventions have reduced some financial harm: losses from authorized push-payment fraud fell from THB 8.6 billion in Q2 2024 to THB 1.8 billion in Q2 2026, a decline of almost 80% (Sodsrichai, 2026). Thailand's exposure also has an important cross-border dimension. Scam operations have been documented immediately across the Thailand–Myanmar border, where Thai authorities have sought to disrupt their supporting infrastructure. In February 2025, Thailand cut electricity, internet signals, and fuel supplies to five border locations suspected of hosting scam operations and strengthened controls over internet connections, mobile signals, and mule accounts linked to these networks (Thepgumpanat & Naing, 2025). At the

same time, the Bank of Thailand has strengthened safeguards to prevent the use of deposit accounts and e-money to move illicit funds, including stronger KYC, customer due diligence, and end-to-end mule-account controls (Bank of Thailand, n.d.).

- *Myanmar:* Myanmar's principal risk stems from the concentration of large scam centers in conflict-affected border areas, particularly Myawaddy and surrounding areas of Kayin State. Fragmented territorial control among different armed actors complicates enforcement and has allowed operations to persist or relocate despite repeated crackdowns. UNODC (2024) documents major cyber-fraud compounds around Myawaddy and Shwe Kokko, with some activities shifting elsewhere along the Thai border following enforcement pressure. These operations also create substantial human-trafficking and forced-criminality risks. In June 2026, the Thailand-based Civil Society Network for Human Trafficking Victim Assistance estimated that more than 5,300 people remained trapped in scam centers near the Thailand–Myanmar border, including nationals from numerous countries, with many reportedly trafficked and forced to conduct online fraud (Reuters, 2026). The scale of foreign involvement remains significant: between January 2025 and July 2026, Myanmar authorities reported detaining 14,731 foreign nationals who had illegally entered Myawaddy Township, of whom 13,811 had been repatriated or transferred through Thailand (Myanmar News Agency, 2026). Myanmar's exposure therefore extends beyond fraud losses to the intersection of cybercrime, human trafficking, illicit finance, and armed conflict. Amerhauser & Thill (2025) find that scam centers form part of Myanmar's wider illicit economy, where political instability and conflict create conditions in which criminal markets can operate and provide resources to different armed actors.
- *Lao PDR:* Lao PDR's risk profile is closely linked to the exploitation of special economic zones (SEZs), border areas, and commercial properties for cyber-enabled fraud. UNODC identifies the Golden Triangle SEZ in Bokeo as a significant regional cybercrime hotspot and notes that SEZs with limited regulatory oversight can be particularly vulnerable to organized criminal networks (Gunn, 2025). However, scam activity has also appeared outside established hubs, including in rented guesthouses and private homes, indicating that operations can shift into less conspicuous premises. Recent enforcement illustrates the scale and transnational nature of the problem. From January to mid-June 2026, Lao authorities dismantled 20 electronic-fraud operations and detained 2,652 suspects from 14 nationalities, prompting expanded inspections of hotels, guesthouses, entertainment venues, and

rental properties, alongside tighter border and immigration controls (Lao News Agency, 2026a). SEZs nevertheless remain an important vulnerability: a 2026 operation in the Boten Special Economic Zone resulted in the arrest of 135 suspects from five countries and the seizure of 1,902 mobile phones and 182 computer monitors. Authorities alleged that the network used fake social media accounts and fraudulent investment, cryptocurrency, and gambling platforms to target victims domestically and abroad (Lao News Agency, 2026b). Lao PDR's exposure therefore extends beyond individual losses to the potential misuse of SEZs, border connectivity, and legitimate commercial properties by transnational scam networks. The involvement of multiple nationalities and the movement of operations into less visible premises also create challenges for immigration control, financial integrity, and cross-border enforcement.

- *The Philippines:* The Philippines faces both domestic consumer exposure and residual risks from the former offshore-gaming ecosystem. Following the shutdown of licensed Philippine Offshore Gaming Operators (POGOs), authorities reported that some scam operations shifted toward smaller and less conspicuous premises. In 2025, the Presidential Anti-Organized Crime Commission described this as a "guerrilla" model, involving small groups operating from rented properties (Gita-Carlos, 2025). This pattern persisted after the Anti-POGO Act of 2025: in April 2026, the National Bureau of Investigation dismantled an alleged scam hub operating from condominium units in Parañaque, arresting 48 individuals allegedly involved in romance, "pig-butchering," and crypto-currency investment scams. Another operation in May uncovered a smaller call center setup using messaging platforms, cryptocurrency wallets, and AI-based face-replacement technology (National Bureau of Investigation, 2026a, 2026b). Consumer-facing fraud and misuse of financial accounts remain additional vulnerabilities. The PNP Anti-Cybercrime Group reported 766 cybercrime-related arrests between January and July 2026, with online-selling scams being the most prevalent offense during the period (Caliwan, 2026a). Separately, 67 individuals were arrested in 60 operations during the first two months of 2026 involving the illegal sale or misuse of bank accounts, online-banking profiles, and e-wallets as money mules (Caliwan, 2026b). The Philippines therefore faces a dual risk: a former POGO-linked scam activity re-emerging in smaller and more dispersed forms, alongside continuing consumer fraud and exploitation of legitimate financial channels.
- *Singapore:* Singapore's risk profile is shaped by its highly digitalized economy and financial system, where scams

continue to generate substantial losses despite declining overall cases. In the first half of 2026, Singapore recorded 16,821 scam cases and SGD 410.6 million in losses, down 14.4% and 17.9%, respectively, from the same period in 2025. Nevertheless, scams still account for 91.5% of reported scam and cybercrime cases (Chan, 2026). Losses are particularly concentrated on high-value financial and business-related fraud. Investment scams generated the largest losses at SGD 169.8 million, while Business Email Compromise (BEC) losses surged 193.1% year on year to SGD 57.3 million. BEC poses a particular risk to businesses because compromised or spoofed corporate accounts can be used to redirect legitimate payments (Ellyana, 2026; Chan, 2026). Digital assets represent another vulnerability, with cryptocurrency involved in approximately SGD 65.5 million, or 16% of total scam losses, in the first half of 2026 (Chan, 2026). Singapore's exposure is therefore less about physical scam compounds and more about the exploitation of its highly connected financial, corporate, and digital-payment ecosystem. Investment fraud can generate large individual losses, BEC can compromise commercial payments, and cryptocurrency creates additional channels for transferring stolen assets. Protecting consumers, businesses, and payment channels therefore remains an important financial-integrity challenge despite the recent decline in overall scam losses.

- *Malaysia*: Malaysia's risk profile centers on substantial consumer losses and the misuse of legitimate financial channels to move scam proceeds. Bank Negara Malaysia (BNM) reported that the impact of fraud reached approximately RM 2.8 billion in 2025, highlighting both the financial harm to consumers and risks to confidence in digital payments (Bank Negara Malaysia, 2025a). Consumer exposure remains broad: part-time job scams alone recorded 10,304 cases and RM 251.2 million in losses between January 2025 and March 15, 2026 (Bernama, 2026). A particularly important financial-system vulnerability is the use of mule accounts, which enable illicit funds to pass through legitimate banking and payment channels. Stronger enforcement contributed to 969 convictions of mule-account holders in 2025, while BNM has expanded the National Fraud Portal and introduced protocols for identifying and managing mule accounts among e-money issuers as well as banks (Bank Negara Malaysia, 2025b). Malaysia therefore faces a dual challenge: reducing consumer losses while preventing its banking, e-money, and digital-payment infrastructure from being exploited to receive and transfer scam proceeds.

- *Indonesia:* Indonesia's risk profile is characterized by the large volume of scam reports and financial accounts linked to suspected fraudulent transactions, creating challenges for consumer protection and financial integrity. From the launch of the Indonesia Anti-Scam Centre (IASC) in November 2024 through August 2026, it received 668,441 reports involving 1,276,688 reported accounts. Of these, 659,419 accounts were blocked, while approximately IDR 771.2 billion in victims' funds was frozen (Otoritas Jasa Keuangan, 2026). The scale of these cases requires extensive coordination among banks, payment providers, and regulators to identify suspicious accounts and trace scam proceeds. The risk is further complicated by illegal digital-finance activities, including fraudulent investment and crypto schemes operating through websites and applications, some of which change their online presence to avoid detection. Indonesia's exposure therefore extends beyond individual losses to the challenge of identifying and disrupting large volumes of suspicious accounts, transactions, and illegal digital-finance activities across an interconnected financial ecosystem (Otoritas Jasa Keuangan, 2026).
- *Vietnam:* Vietnam's risk profile combines broad consumer exposure to sophisticated digital fraud with a significant cross-border dimension. In September 2026, the Ministry of Public Security identified 25 prominent scam scenarios involving AI, deepfakes, voice cloning, social media, digital banking, and electronic payments. These included impersonation of authorities and financial institutions, fraudulent investment schemes, and attempts to steal banking credentials or induce transfers (Thien Dung, 2026). Cross-border networks create an additional vulnerability. In May 2026, Quang Tri police dismantled an alleged fraud network, arresting 61 suspects accused of using stolen personal information and fraudulent cryptocurrency and foreign-exchange platforms to target victims; investigators estimated that the network was appropriating more than VND 3 trillion annually (Voice of Vietnam, 2026). Other 2026 cases involved Vietnamese nationals operating from Cambodia and moving across countries following enforcement actions (Báo Khoa học và Đời sống, 2026). At the same time, Viet Nam can itself serve as an operating base: in July, police dismantled an alleged network involving 11 Chinese nationals operating from Viet Nam and targeting victims in France (Ha & Trong, 2026). Vietnam, therefore, faces a two-way transnational risk, as its consumers are targeted by networks operating abroad, while infrastructure within the country can also be exploited to conduct fraud against overseas victims.
- *Brunei Darussalam:* Brunei Darussalam's risk profile is characterized primarily by consumer-facing online fraud through social media and digital communications, alongside exposure to transnational scam

networks. In August 2026, the Royal Brunei Police Force (RBPF) identified several Facebook accounts allegedly offering fictitious loans, with reported losses of approximately BND 4,270. E-commerce scams involving accounts on TikTok and Instagram caused a further BND 8,220 in reported losses (PPDB, 2026). Authorities have also warned about impersonation scams and the misuse of bank accounts and SIM cards, including the recruitment of young people as mule-account or SIM-card holders. Brunei's exposure also has a clear cross-border dimension. During Operation FRONTIER+ III from March to May 2026, Brunei police investigated 193 scam cases involving BND 1.85 million in losses and arrested 14 individuals, with cases including government-official impersonation, e-commerce, social-media impersonation, and loan scams (Borneo Bulletin, 2026). Across the ten participating jurisdictions, the operation was linked to more than 138,000 cases and USD 752 million in losses, demonstrating how Brunei's domestic scam exposure forms part of a wider transnational fraud ecosystem (Borneo Bulletin, 2026).

- *Timor-Leste:* Timor-Leste presents a different and potentially emerging risk profile. Rather than an established scam economy, UNODC (2025b) warns that transnational criminal networks may exploit investment structures and regulatory vulnerabilities to establish Southeast Asia-style operations. In the Special Administrative Region of Oecusse-Ambeno (RAEOA), UNODC identified developments indicative of possible scam-center activity and warned that the Oecusse Digital Centre free-trade zone could be vulnerable to organized crime operating under the guise of legitimate investment. In August 2025, Timorese authorities searched a hotel in Oecusse and seized SIM cards and Starlink devices, equipment associated with scam operations elsewhere in Southeast Asia. UNODC nevertheless cautioned that it remained unclear whether individuals at the site were knowingly involved or were themselves trafficking victims (UNODC, 2025b). Timor-Leste's principal risk is therefore preventive and institutional: legitimate investment, hospitality, and digital-development structures could potentially be exploited as infrastructure or cover for transnational criminal activity, threatening financial integrity and regulatory credibility before such operations become more deeply established (UNODC, 2025b).

The Case of Cambodia: Exposure, Impact, and Responses to Online Scams

Cambodia's Exposure to the Online Scam Economy

Cambodia's exposure to online scams reflects both its rapid digitalization and the presence of organized scam-center activity. Digital connectivity has expanded considerably: Cambodia's Digital Economy and Business Committee (n.d.) reports that 68.48% of

individuals use the internet, alongside 20.69 million mobile subscriptions and 19.62 million internet subscriptions. However, expanding access is not necessarily matched by digital and financial capabilities. Among adults with internet access, Cambodia recorded a digital financial literacy score of 43 out of 100, while available national digital-literacy data from 2020 show that 32% of the population had basic skills and only 5% each had intermediate and advanced skills (Figure 4). This combination of widespread connectivity and relatively limited digital capabilities can increase exposure to fraud conducted through social media, messaging applications, and digital financial services. Cambodian authorities have also warned of increasingly sophisticated online fraud, including impersonation, fake investment schemes, prize scams, and phishing through platforms such as Telegram (TRC, 2025).

Cambodia's exposure extends beyond consumer-facing fraud to organized scam-center operations. UNODC (2024) identified reported cyber-fraud compounds and related locations across several parts of Cambodia, including Sihanoukville, Poipet, Pursat, Koh Kong, Kandal and Bavet (Figure 5), while cautioning that the location and status of individual operations can change as enforcement evolves. These operations form part of wider transnational networks involving money laundering, underground banking, virtual assets and cross-border financial flows (UNODC, 2024; Gunn, 2025). The scale of subsequent enforcement also illustrates the extent of the challenge: Cambodian authorities reported cracking down on 665 online-scam sites between July 2025 and June 2026, alongside inspections of 28,512 locations (Ministry of Interior, 2026).

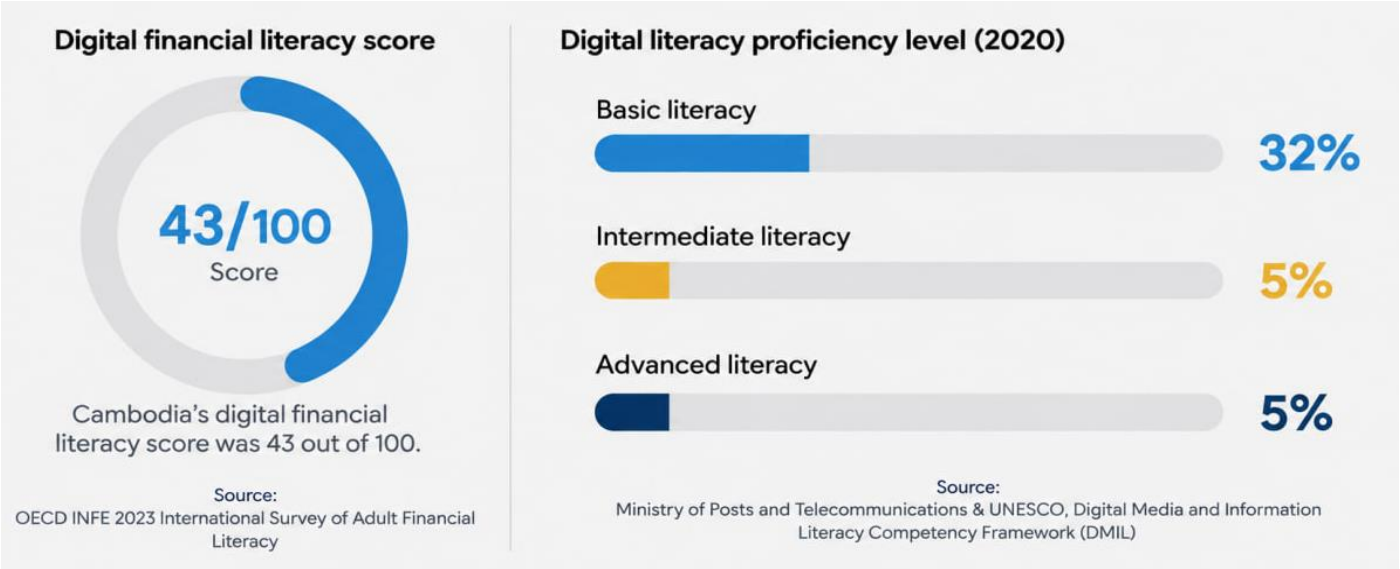


Figure 3: Digital Financial Literacy & Digital Literacy Proficiency Level (Digital Economics and Business Committee, n.d.)

Estimates of the industry's economic scale further highlight the potential implications for Cambodia, although such figures should be interpreted with caution. One research estimate suggests that scam-related activities may generate approximately USD 12.5–19 billion (Sims, 2025). However, given the informal and opaque nature of these activities, the figures remain difficult to verify independently. These developments point to broader economic, financial and social considerations for Cambodia, extending beyond cybersecurity and law enforcement to include consumer protection, financial governance, the prevention of illicit financial flows, and the protection of legitimate economic activities and financial integrity.

Impact of Online Scams in Cambodia

- *International Reputation:* The presence of online scam operations involving criminal networks in Cambodia has attracted increased international attention and created reputational challenges for the country. International organizations and foreign governments have raised concerns about cases involving cyber fraud, human trafficking, and the exploitation of individuals in connection with these activities. The U.S. Department of State's 2024 Trafficking in Persons Report documented cases in which Cambodian and foreign nationals were recruited through deceptive employment offers and subsequently subjected to forced detention and exploitation in online scam operations, including in Sihanoukville and other locations (U.S. Department of State, 2024). International enforcement measures have also contributed to greater scrutiny of activities linked to certain individuals and entities operating in Cambodia. In 2025 and 2026, the U.S. Department of the Treasury announced sanctions against individuals and entities over alleged involvement in cyber-enabled fraud, human trafficking, and related illicit financial activities (U.S. Department of the Treasury, 2025, 2026). These developments have implications beyond law enforcement, particularly in relation to Cambodia's international image and the confidence of international partners. The economic implications are also noteworthy. In July 2026, the International Monetary Fund (IMF) highlighted concerns that reputational effects associated with scam-related activities could weigh on economic activity, particularly tourism, while creating potential risks to financial stability. The IMF also underscored the importance of maintaining depositor and investor confidence and safeguarding the integrity and stability of the financial system (IMF, 2026). Accordingly, the issue extends beyond the criminal activities themselves, raising broader considerations for Cambodia's international reputation, tourism, investment climate, and financial sector. Continued efforts to address

criminal networks, strengthen institutional coordination, protect victims, and reinforce regulatory and enforcement frameworks are important to maintaining international confidence and supporting legitimate economic activity.

- *FDI and Business Environment:* Online scam activity creates risks for Cambodia's investment and business environment by affecting investor confidence and increasing concerns over financial and regulatory integrity. An IMF assessment of Cambodia's capital market in 2026 identified significant investor-confidence concerns amplified by scams and low financial literacy, alongside fundraising challenges and other structural weaknesses in the securities market (Khanolkar, 2026). These concerns are particularly relevant as Cambodia seeks to deepen its capital markets and attract higher-quality investment. These risks should not be interpreted as evidence that foreign investment in Cambodia generally is associated with criminal activity. Legitimate FDI remains an important source of economic activity and employment: Cambodia received approximately USD 5.1 billion in FDI in 2025, supporting an estimated 400,000 formal jobs (World Bank, 2026). Rather, concerns over illicit activity can increase scrutiny of legitimate businesses and financial transactions. The IMF (2025), for example, noted that sanctions targeting Cambodian scam centers could increase AML/CFT compliance costs for banks conducting cross-border transactions, creating an additional burden on legitimate international financial activity. Maintaining a credible investment environment therefore requires stronger governance, regulatory oversight and financial integrity. The IMF emphasized in 2026 that improving Cambodia's business climate, governance and rule of law, together with attracting higher-quality investment, remains important for strengthening the country's growth model (IMF, 2026). Cambodia's authorities have similarly linked the continued crackdown on online scams with efforts to maintain a safe and trustworthy investment environment (Chuon, 2026).
- *Tourism:* Online scam activity can affect Cambodia's tourism sector primarily through reputational and destination-image risks. Sihanoukville provides a prominent example, once known principally as a coastal tourism destination, its rapid casino and property development was followed by growing international association with organized crime and large-scale scam operations. Recent international reporting continues to identify the city as a major location within Cambodia's scam economy, potentially complicating efforts to promote it as a legitimate tourism and investment destination (Anantha Lakshmi, 2026; Board, 2026). The economic relevance of this reputational risk is increasingly recognized. In July 2026, the IMF explicitly

reported that reputational damage associated with scam activities was weighing on economic activity and weakening tourism (IMF, 2026). Such developments can influence perceptions of safety and potentially affect legitimate tourism businesses, including hotels, restaurants, retailers and tour operators, that have no connection to criminal activity. However, online scams should not be treated as the sole explanation for changes in Cambodia's tourism performance. Tourism is also affected by border tensions, global economic conditions, travel connectivity and other domestic and external factors. The more defensible conclusion is that scam-related crime represents an additional reputational and security risk that can weaken destination confidence and complicate Cambodia's efforts to strengthen its tourism recovery.

- *Human Trafficking and Loss of Human Capital:* One of the most serious social and economic consequences of Cambodia's online-scam economy is its connection with human trafficking and forced criminality. UNODC (2023) documents how victims are recruited through fraudulent job advertisements before being transported to scam compounds, where they may be confined and forced to conduct online fraud. Similarly, the U.S. Department of State reports that traffickers recruit Cambodian and foreign adults and children through false offers of high-paying technical jobs and subsequently compel some victims to participate in online gambling, cryptocurrency, romance and telephone scams. Victims have reportedly faced physical and sexual abuse, wage deductions, debt bondage, and other forms of coercion (U.S. Department of State, 2024). Beyond immediate exploitation, trafficking can cause physical and psychological harm, lost earnings and productive employment, family disruption, and difficulties reintegrating into legitimate work, representing a loss of human capital for both victims and their communities. It also generates additional costs related to victim identification, rescue, repatriation, and support services. Given that recruitment often extends across national borders, UNODC (2023) further highlights the involvement of international recruitment networks in Cambodia's scam-compound operations, underscoring the transnational nature of the challenge. Consequently, online scams in Cambodia should be viewed not only as financial crimes but also as a human-trafficking and human-capital concern, requiring effective victim identification and protection alongside criminal enforcement.
- *Pressure on the Financial System and Financial Loss:* Online scams create both direct financial losses for Cambodian consumers and broader financial-integrity risks. According to Cambodia's Ministry of

Interior, Cambodian citizens lost more than USD 45 million to domestic online scams in 2025, while less than USD 20 million was recovered. Reported methods included bank impersonation, prize-related fraud, emotional manipulation and blackmail (K. Rithy Reak, 2026a). Beyond reducing household savings and purchasing power, the difficulty of recovering stolen funds illustrates the lasting financial consequences scams can impose on victims. The financial-system impact extends beyond direct losses because scam proceeds can move through bank accounts, payment services, crypto-assets and other domestic and cross-border financial channels. International scrutiny adds another layer of pressure. Recent reporting has highlighted U.S. enforcement and sanctions involving individuals, companies, and financial channels allegedly connected with Cambodia-based scam operations, illustrating how concerns over illicit financial flows can extend into international financial relationships (The Korea Times, 2026). These actions should be understood as allegations and enforcement measures against specific parties rather than evidence of wrongdoing across Cambodia's broader financial sector. Nevertheless, together with the IMF's assessment, they demonstrate how scam activity can increase compliance, supervisory and reputational pressures on legitimate financial institutions and cross-border transactions. Cambodia's financial sector therefore faces a dual challenge: protecting consumers from direct losses while preventing legitimate financial infrastructure from being exploited to receive, transfer or conceal illicit proceeds. Strengthening customer due diligence, transaction monitoring, suspicious-transaction reporting, and cooperation among regulators and financial institutions is consequently important for protecting financial integrity without unnecessarily disrupting legitimate financial activity.

Cambodia's Response to Online Scams

Cambodia's response to online scams has expanded as the issue has evolved from primarily a cybercrime and human-trafficking concern into a broader law-enforcement, financial-integrity and transnational organized-crime challenge. The response intensified particularly from 2025 through the Commission for Combating Online Scams (CCOS), which coordinates relevant ministries, law-enforcement agencies and subnational authorities. By 31 August 2026, authorities reported inspecting 832 suspected locations and taking enforcement action at 663, including 86 major scam compounds. A total of 446 cases involving 3,927 suspects from 29 nationalities had been referred to court, while authorities also reported legal action against officials allegedly involved in scam activities (Agence Kampuchea Presse, 2026).

The response has increasingly extended beyond raids and arrests to the financial infrastructure supporting scam operations. Between July 2025 and August 2026, Cambodia reported freezing more than USD 300 million in bank accounts linked to online-scam crimes, while additional assets were undergoing freezing and valuation procedures (Agence Kampuchea Presse, 2026). These measures indicate a growing emphasis on cutting off criminal proceeds and pursuing assets alongside prosecuting offenders.

Preventive measures have also expanded across Cambodia's telecommunications and financial sectors. In June 2026, the Ministry of Posts and Telecommunications (MPTC) and the National Bank of Cambodia (NBC) launched a nationwide campaign to verify SIM-card identities against bank and payment-account identities. The initiative, involving tele-communications operators and financial institutions, aims to strengthen digital security and reduce technology-enabled fraud by limiting the misuse of mobile numbers and financial accounts (Sum, 2026).

Cambodia has also broadened enforcement against the physical and commercial infrastructure used by scam networks. By March 2026, authorities reported closing 236 scam-related sites, including 91 casino-based operations and 145 sites operating from borey, villas, condominiums and other residential properties (CCOS, 2026). Enforcement subsequently expanded to apartments, hotels, guesthouses and other premises as some operations became smaller and more dispersed. By August 2026, CCOS reported scam activities shifting into locations including rental rooms, houses, vehicles and coffee shops (K. Rithy Reak, 2026b). Casino regulation has also formed part of the response: between July 2025 and July 2026, authorities reported inspecting 195 licensed casinos, revoking 20 licenses and suspending 29 in connection with alleged cyberfraud activities (K. Rithy Reak, 2026c).

Cambodia has simultaneously strengthened its legal framework. The Law on Combating Technology-Enabled Scams, which took effect in April 2026, established specific offences covering technology-based fraud, organizing or leading scam centers, recruiting or training people to commit such fraud, malicious collection of personal identification information and a specific form of money laundering. Depending on the offence and severity, penalties can include imprisonment, fines of up to 1 billion riel and asset seizure (C. Nika, 2026). The law provides a more specific legal basis for targeting not only individual scammers but also organizers, recruitment networks and financial activities supporting scam operations.

International cooperation has become another major pillar because many scam operations involve foreign victims, workers, criminal networks and financial flows. Cambodia has

expanded cooperation with foreign law-enforcement authorities on investigations, intelligence exchange, victim repatriation, digital forensics and the tracing of illicit proceeds. In September 2026, Cambodia and the United Kingdom signed an MoU providing for stronger intelligence sharing, cyber investigations and digital-forensics cooperation, alongside measures to identify suspects, support victims and trace and disrupt illicit financial flows (Home Office, 2026).

This international dimension was further strengthened when Cambodia hosted the International Conference on Combating Online Scams (ICCOS-2026) in Phnom Penh on 23–24 September 2026. The conference concluded with the adoption of the Phnom Penh Declaration, supported by delegates from 28 countries and seven international organizations. Its 11 commitments cover international cooperation, disruption and recovery of criminal proceeds, technological innovation, stronger legal and regulatory frameworks, capacity building, public-private partnerships, prevention of fraud and human trafficking, protection of trafficked and vulnerable victims, and dismantling scam compounds and related infrastructure (Heng, 2026).

Taken together, Cambodia's response has evolved from primarily disrupting individual scam operations toward a more multi-dimensional approach combining enforcement and prosecution, financial disruption, digital prevention, legal measures, victim protection

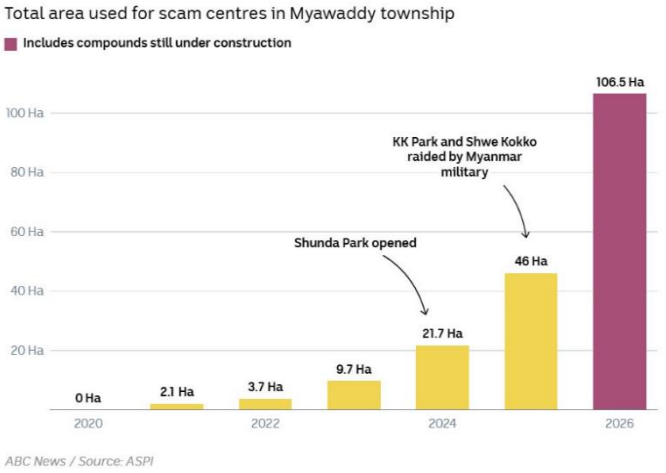


Figure 7: Exponential growth of scam centers on Myanmar-Thailand border (Hongan et al., 2026)

and international cooperation. The continued adaptation and dispersal of scam networks, however, means that sustained financial investigations, preventive controls, and cross-border cooperation remain important alongside physical crackdowns.

Remaining Challenges and Way Forward in Southeast Asia

Despite intensified enforcement, scam networks remain adaptable, posing a major challenge across Southeast Asia. Recent evidence from Myanmar indicates that operations are continuing to evolve rather than simply disappearing: satellite analysis found that at least 25 suspected scam sites had appeared or significantly expanded around Myawaddy since the beginning of 2026, while investigators reported newer operations moving farther inland and into less visible locations (BreachSpot, 2026). Moreover, as shown in Figure 7, the total area identified as being used for scam centers in Myawaddy reached 106.5 hectares in 2026, up from 46

hectares in 2025, despite enforcement against major sites such as KK Park and Shwe Kokko (Hogan et al., 2026). The Philippines has faced a similar challenge, with authorities continuing to address scam centers after the POGO ban, while UN reporting notes that such operations can move across borders and adapt quickly (Gaspar, 2026). These developments suggest that enforcement must increasingly address both established scam hubs and smaller, relocated or decentralized operations.

A second challenge is disrupting the financial and technological infrastructure that allows scam networks to operate across borders. Scam operations can separate their physical locations, financial flows, communications, and supporting services across different jurisdictions, making disruption more difficult. ASEANAPOL (2026) has consequently strengthened cooperation among national anti-scam centers through intelligence sharing, operational coordination, and victim-protection mechanisms. Continued financial investigations, asset tracing, and cooperation with financial, telecommunications, and technology providers will therefore remain important for disrupting the wider infrastructure supporting scam networks.

Finally, cross-border coordination remains essential as individual countries can address only part of networks operating across multiple jurisdictions. In September 2026, ASEANAPOL coordinated a regional study program on anti-scam center practices, with visits to Thailand, Malaysia, and Singapore aimed at exchanging practices and strengthening regional approaches (ASEANAPOL Secretariat, 2026a). Regional cooperation has also increasingly focused on strengthening intelligence sharing and using technology to identify interconnected criminal networks and support cross-border investigations (ASEANAPOL Secretariat, 2026b). These developments demonstrate growing cooperation, but sustained information sharing, financial tracing, and coordinated enforcement will remain necessary as scam networks continue to operate across national borders.

REFERENCES

Agence Kampuchea Presse. (2026, September 2). Cambodia freezes more than USD300 million in online scam crackdown, 446 cases sent to court. https://www.akp.gov.kh/post/detail/380136

Alifha, F. (2026, March 25). *How Scam Ready ASEAN is helping communities respond to online fraud*. *The ASEAN Magazine*. https://theaseanmagazine.asean.org/article/how-scam-ready-asean-is-helping-communities-respond-to-online-fraud/

Amerhauser, K., & Thill, A. (2025, May). *Compound crime: Cyber scam operations in Southeast Asia*. Global Initiative Against Transnational Organized Crime.

Anantha Lakshmi, A. (2026, January 13). *The country at the heart of the global scam industry*. *Financial Times*. https://www.ft.com/content/fe55d264-3fc4-4987-9cce-dee1c42c5a6e

ASEAN. (2026, September 23). Secretary-General of ASEAN delivers remarks at the High-Level Session of the International Conference on Combating Online Scams. https://asean.org/secretary-general-of-asean-

delivers-remarks-at-the-high-level-session-of-the-international-conference-on-combating-online-scams

ASEAN–Australia Counter Trafficking. (2025, May 29). *Compound crime: Cyber scam operations in Southeast Asia*. https://www.aseanact.org/resources/compound-crime-cyber-scam/

ASEAN–Australia Counter Trafficking. (2025, June 27). *Trapped behind the scam*. https://www.aseanact.org/story/trapped-behind-the-scam/

Association of Southeast Asian Nations. (2026). *ASEAN guide on anti-scam policies and best practices*.

ASEAN–Australia Counter Trafficking. (2025, May 29). *Compound crime: Cyber scam operations in Southeast Asia*. https://www.aseanact.org/resources/compound-crime-cyber-scam/

ASEANAPOL. (2026, June). ASCOT curriculum development workshop, Semarang, Indonesia, June 2026. https://aseanapol.org/en/news-media/news/ascot-curriculum-development-workshop-semarang-indonesia-june-2026

ASEANAPOL Secretariat. (2026a, September 2). ASEANAPOL Study Visit Programme Coordination Meeting. https://www.aseanapol.org/en/news-media/news/aseanapol-study-visit-programme-coordination-meeting-2026-09-02

ASEANAPOL Secretariat. (2026b, September 18). ASEANAPOL and ClearTrail Technology strengthen cooperation against transnational crime. https://www.aseanapol.org/en/news-media/news/aseanapol-cleartrail-technology-transnational-crime-2026-09-18

Bank of Thailand. (n.d.). *Financial safeguard commitments*. https://www.bot.or.th/en/finsafeguard/finsafeguard-commitments.html

Bank Negara Malaysia. (2025a). *Fraud resolution: Building trust through shared accountability*. In *Annual report 2025*. https://www.bnm.gov.my/publications/ar2025/box4

Bank Negara Malaysia. (2025b). *Maintaining financial integrity*. In *Annual report 2025*. https://www.bnm.gov.my/publications/ar2025/ch1g

Bank Negara Malaysia. (2026). *Operational risk*. In *Financial stability review: Second half 2025*. https://www.bnm.gov.my/publications/fsr2025h2/ch1c

Báo Khoa học và Đời sống. (2026, September 7). *Hai Phong authorities dismantled a transnational fraud ring operating in Laos*. Vietnam.vn. https://www.vietnam.vn/en/hai-phong-triet-pha-o-nhom-lua-dao-xuyen-quoc-gia-tai-lao

Bernama. (2026, April 8). *'Like' and 'share' approach used to lure job scam victims*. *New Straits Times*. https://www.nst.com.my/news/nation/2026/04/1412709/and-share-approach-used-lure-job-scam-victims

Borneo Bulletin. (2026, May 22). *RBPF joins cross-border anti-scam crackdown*. https://borneobulletin.com.bn/rbpf-joins-cross-border-anti-scam-crackdown/

Board, J. (2026, June 1). *Cambodia's crackdown on scam centres leaves trail of stranded victims as criminal groups switch tactics*. CNA. https://www.channelnewsasia.com/asia/cambodia-scamming-crackdown-victims-crime-6149341

BreachSpot. (2026, July 24). Satellite images uncover the sudden emergence of suspected scam compounds. https://breachspot.com/news/cyber-attacks/satellite-images-uncover-the-sudden-emergence-of-suspected-scam-compounds/

Caliwan, C. L. (2026a, September 1). *766 cybercrime suspects arrested January to July 2026*. Philippine News Agency. https://www.pna.gov.ph/articles/1283047

Caliwan, C. L. (2026b, March 25). *PNP busts 67 money mules, scammers in first 2 months of 2026*. Philippine News Agency. https://www.pna.gov.ph/index.php/articles/1271713

Chan, E. (2026, August 26). *Overall scam cases, losses in Singapore fall in first half of 2026*. CNA.

https://www.channelnewsasia.com/singapore/scam-cases-losses-down-first-half-2026-cybercrime-report-6337016

C. Nika. (2026, April 23). *Prime Minister orders continued crackdown on online scams without pause*. Agence Kampuchea Presse. https://akp.gov.kh/post/detail/368511

Chuon, B. (2026, September 1). *The Royal Government continues to crack down on online scams to ensure a safe and trustworthy investment environment*. Radio National of Kampuchea. https://rnk.gov.kh/article/73681

Digital Economy and Business Committee. (n.d.). *Digital landscape*. https://digitaleconomy.gov.kh/en/supporting-sector/digital-landscape

Ellyana, F. (2026, September 18). *Business email compromise & social media impersonation scams*. Intercorp Solutions. https://www.intercorpsolutions.com/business-email-compromise-social-media-impersonation-scams/

Falvey, L. (2026). *ASEAN consumer scam report 2026: Defences rising, cases unresolved*. GSMA.

Gaspar, M. (2026, April 24). *Scam no more: How the Philippines is cracking down on online fraud centres with UN support*. United Nations Philippines. https://philippines.un.org/en/314407-scam-no-more-how-philippines-cracking-down-online-fraud-centres-un-support

Gunn, G. (2025, October). *The nexus between cybercrime and corruption*. United Nations Office on Drugs and Crime.

Gita-Carlos, R. A. (2025, January 14). *80% of 400 POGO hubs shut down; small-scale ops monitored*. Philippine News Agency. https://www.pna.gov.ph/articles/1241787

Ha, T., & Trong, D. (2026, July 9). *11 Chinese nationals arrested in Vietnam for allegedly running online scam targeting French citizens*. Tuoi Tre News. https://news.tuoitre.vn/11-chinese-nationals-arrested-in-vietnam-for-allegedly-running-online-scam-targeting-french-citizens-103260709163240317.htm

Heng, P. (2026, September 24). *Phnom Penh Declaration on combating online scams adopted*. Agence Kampuchea Presse. https://akp.gov.kh/index.php/post/detail/382092

Home Office. (2026, September 24). *United Kingdom and Cambodia join forces to crackdown on online scam centres*. GOV.UK. https://www.gov.uk/government/news/united-kingdom-and-cambodia-join-forces-to-crackdown-on-online-scam-centres

Hogan, L., Fankhauser, J., & Fell, J. (2026, July 21). Scam centres growing 'exponentially' despite Myanmar crackdown. ABC News. https://www.abc.net.au/news/2026-07-21/myanmar-scam-compounds-exponential-growth/106603324

INTERPOL. (2026a, June 17). *New INTERPOL report highlights escalating cyber threats across Asia and South Pacific*. https://www.interpol.int/News-and-Events/News/2026/New-INTERPOL-report-highlights-escalating-cyber-threats-across-Asia-and-South-Pacific

INTERPOL. (2026b). *Over 5,800 arrests, USD 293 million intercepted in global fraud bust*. https://www.interpol.int/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust

IMF. (2026, July 7). *IMF staff completes 2026 Article IV mission to Cambodia*. https://www.imf.org/en/news/articles/2026/07/07/pr26241-cambodia-imf-staff-completes-2026-article-iv-mission

IMF. (2025). *Cambodia: 2025 Article IV consultation—Press release; staff report; and statement by the executive director for Cambodia* (IMF Country Report No. 25/002). https://www.imf.org/-/media/files/publications/cr/2025/english/1khmea2025002-source-pdf.pdf

Khanolkar, N. S. (2026, August). *Cambodia: Risk based supervision in capital markets* (IMF High-Level Summary Technical Assistance Report No. 2026/050). IMF. https://www.imf.org/-/media/files/publications/hls/2026/english/hlsea2026050.pdf

K. Rithy Reak. (2026a, February 17). *Cambodians lose USD45M in 2025 as interior minister warns of deadlier online scams*. Agence Kampuchea Presse. https://akp.gov.kh/post/detail/362458

K. Rithy Reak. (2026b, March 24). *Cambodia intensifies crackdown on online scams, 50 suspects arrested in Sihanoukville*. Agence Kampuchea Presse. https://www.akp.gov.kh/index.php/post/detail/365736

K. Rithy Reak. (2026c, August 17). *751 cyber scam sites uncovered, hundreds shut down in 12-month operation*. Agence Kampuchea Presse. https://www.akp.gov.kh/index.php/post/detail/378594

Lao News Agency. (2026a, June 18). Laos intensifies *crackdown on cyber scam networks, pledges to eliminate online fraud*. https://kpl.gov.la/En/detail.aspx?id=101697

Lao News Agency. (2026b, July 29). *Lao police arrest 135 suspected online scammers in Boten Special Economic Zone*. https://kpl.gov.la/En/detail.aspx/detail.aspx?id=102485

Loughlin, N. (2026). Digital crime, dirty money and the state: Southeast Asia's illicit political economy and the rise of cybercrime. *Development and Change, 57*(4), 812–839. https://doi.org/10.1111/dech.70071

Ministry of Interior. (2026, September 23). *His Excellency Abhisantibindit Sar Sokha highlights 4 main causes leading to the global rise in online scams and announces the plan to establish the National Center for Combating Online Scams*. https://www.interior.gov.kh/en/news/KOTitPr7esKR

Ministry of Digital. (2025, August 5). *AI guidelines, training programmes among proactive measures by the Ministry of Digital to combat online scams*. https://www.digital.gov.my/en-GB/siaran/Garis-Panduan-AI,-Program-Latihan-Antara-Langkah-Proaktif-Kementerian-Digital-Untuk-Memerangi-Online-Scam

Myanmar News Agency. (2026, August 5). *2 foreign nationals transferred over telecom fraud links*. *Global New Light of Myanmar*. https://www.gnlm.com.mm/2-foreign-nationals-transferred-over-telecom-fraud-links/

National Bureau of Investigation. (2026a, April 20). *NBI dismantles a sophisticated online scamming hub in Paranaque; arrests 48 individuals*. https://nbi.gov.ph/press_releases/2026/04202026/9819/

National Bureau of Investigation. (2026b, May 19). *NBI-SAU dismantles online love scamming and crypto fraud operations in Parañaque City; 17 arrested*. https://nbi.gov.ph/press_releases/2026/05192026/10018/

Otoritas Jasa Keuangan. (2026, September 10). *Press release August 2026 of the Board of Commissioners' Meeting: Financial services sector performance and intermediation remain solid, supporting accelerated economic growth*. https://iru.ojk.go.id/iru/WebSite/ArticleList/View/1060_Press_Release_August_2026_of_The_Board_of_Commissioners%E2%80%99_Meeting_Financial_Services_Sector_Performance_And_Intermediation_Remain_Solid%2C_Supporting_Accelerated_Economic_Growth

PPDB. (2026, August 7). *PPDB advises people to beware of loan and online buying scams*. Pasukan Polis Diraja Brunei. https://www.polis.gov.bn/ppdb-nasihatkan-orang-ramai-supaya-berwaspada-terhadap-penipuan-pinjaman-dan-jual-beli-dalam-talian/

Reuters. (2026, June 23). *Over 5,000 people trapped in Myanmar scam centres near Thai border, rights group says*. https://www.reuters.com/world/china/over-5000-people-trapped-myanmar-scam-centres-near-thai-border-rights-group-says-2026-06-23/

Sodsrichai, P. (2025, April 15). Let's build a "Horse Account" defense shield. Bank of Thailand. https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/article-20250415.html

Sodsrichai, P. (2026, September 15). *Combining the strengths of Thailand's financial sector to create opportunities and build resilience for a sustainable future*. Bank of Thailand. https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/article-20260915.html

Singapore Business Review. (2026, March 2). *Scam losses fall to $913.1m in 2025*. https://sbr.com.sg/information-technology/news/scam-losses-fall-9131m-in-2025

Sims, J. (2025). *Policies and patterns: State-abetted transnational crime in Cambodia as a global security threat*. Humanity Research Consultancy.

Sum, K. (2026, June 17). *MPTC and NBC launch nationwide SIM verification campaign*. Agence Kampuchea Presse. https://vps.akp.gov.kh/post/detail/373338

Telecommunication Regulator of Cambodia. (2025, September 15). *Announcement on rising incidents of fraudulent activities on Telegram*. https://www.trc.gov.kh/en/media/news-releases/7-news-release

Thepgumpanat, P., & Naing, S. (2025, February 5). *Thailand cuts power, fuel and internet supply to parts of Myanmar*. Reuters. https://www.reuters.com/world/asia-pacific/thailand-cuts-power-fuel-internet-supply-parts-myanmar-2025-02-05/

Thien Dung. (2026, September 18). *Cybercriminals launch 25 scam scenarios, AI becomes a new "weapon"*. Báo Nghệ An. https://baonghean.vn/en/toi-pham-mang-tung-25-kich-ban-lua-dao-ai-thanh-vu-khi-moi-10351600.html

United Nations Office on Drugs and Crime. (2026, July). *An interconnected criminal ecosystem: Transnational organized crime threat assessment for South-East Asia 2026*.

United Nations Office on Drugs and Crime. (2025b, September). *Strategic infiltration of vulnerable jurisdictions through criminal foreign direct investments: The case of Timor-Leste* (Southeast Asia and the Pacific Organized Crime Threat Alert).

United Nations Office on Drugs and Crime. (2025a, September). *Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia*.

United Nations Office on Drugs and Crime. (2024, October). *Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape*.

United Nations Office on Drugs and Crime. (2023, September). *Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia*.

U.S. Attorney's Office for the District of Columbia. (2026, September 9). *Scam Center Strike Force conducts seizures of Chinese-run illicit scammer marketplace, and restrains $52 million in laundered crypto scammer funds in one day*. U.S. Department of Justice. https://www.justice.gov/usao-dc/pr/scam-center-strike-force-conducts-seizures-chinese-run-illicit-scammer-marketplace-and

U.S. Department of Justice. (2026a, April 23). *Scam Center Strike Force takes major actions against Southeast Asian scam centers targeting Americans*. https://www.justice.gov/opa/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers-targeting

U.S. Department of Justice. (2026b, June 3). *Scam Center Strike Force announces results of U.S. & private industry "Disruption Week"*. https://www.justice.gov/opa/pr/scam-center-strike-force-announces-results-us-private-industry-disruption-week

U.S. Department of State. (2024). *2024 trafficking in persons report: Cambodia*. https://2021-2025.state.gov/reports/2024-trafficking-in-persons-report/cambodia/?safe=1

U.S. Department of the Treasury. (2025, September 8). *Treasury sanctions Southeast Asian networks targeting Americans with cyber scams*. https://home.treasury.gov/news/press-releases/sb0237

U.S. Department of the Treasury. (2026, April 23). *Treasury sanctions Cambodian senator Kok An and scam center network defrauding Americans*. https://home.treasury.gov/news/press-releases/sb0469

Voice of Vietnam. (2026, May 8). *Police bust transnational fraud ring, arrest 61 suspects*. https://english.vov.vn/en/society/police-bust-transnational-fraud-ring-arrest-61-suspects-post1289996.vov

World Bank. (2026, June 9). *Strong policy action key to protecting Cambodia's jobs and livelihoods amid shocks*. https://www.worldbank.org/en/news/press-release/2026/06/09/strong-policy-action-key-to-protecting-cambodia-s-jobs-and-livelihoods-amid-shocks

EVENTS AND ENGAGEMENTS

OUR TRAINING PROGRAM

Sharing Session on "Stocktaking on Low-Carbon Rice Farming in Cambodia"

October 21, 2026

On October 21, 2026, the APM Center held a sharing session on "Stocktaking on Low-Carbon Rice Farming in Cambodia," led by Dr. Mak Soeun, Advisor to ARDB and the Ministry of Agriculture, Forestry and Fisheries (MAFF). The session provided a comprehensive overview of the current state of low-carbon rice farming in Cambodia and its contribution to building a more resilient and sustainable agricultural and food system. It also explored the policy and strategic frameworks that support the transition toward low-carbon agriculture, with a particular focus on the rice sector. The session also reviewed the ongoing initiatives and pilot projects, highlighting the technologies, innovations, practices, and lessons learned from efforts to promote low-carbon rice farming in Cambodia.



DATA DASHBOARD

AGRICULTURAL COMMODITY PRICE MONITOR: SEPTEMBER 2026

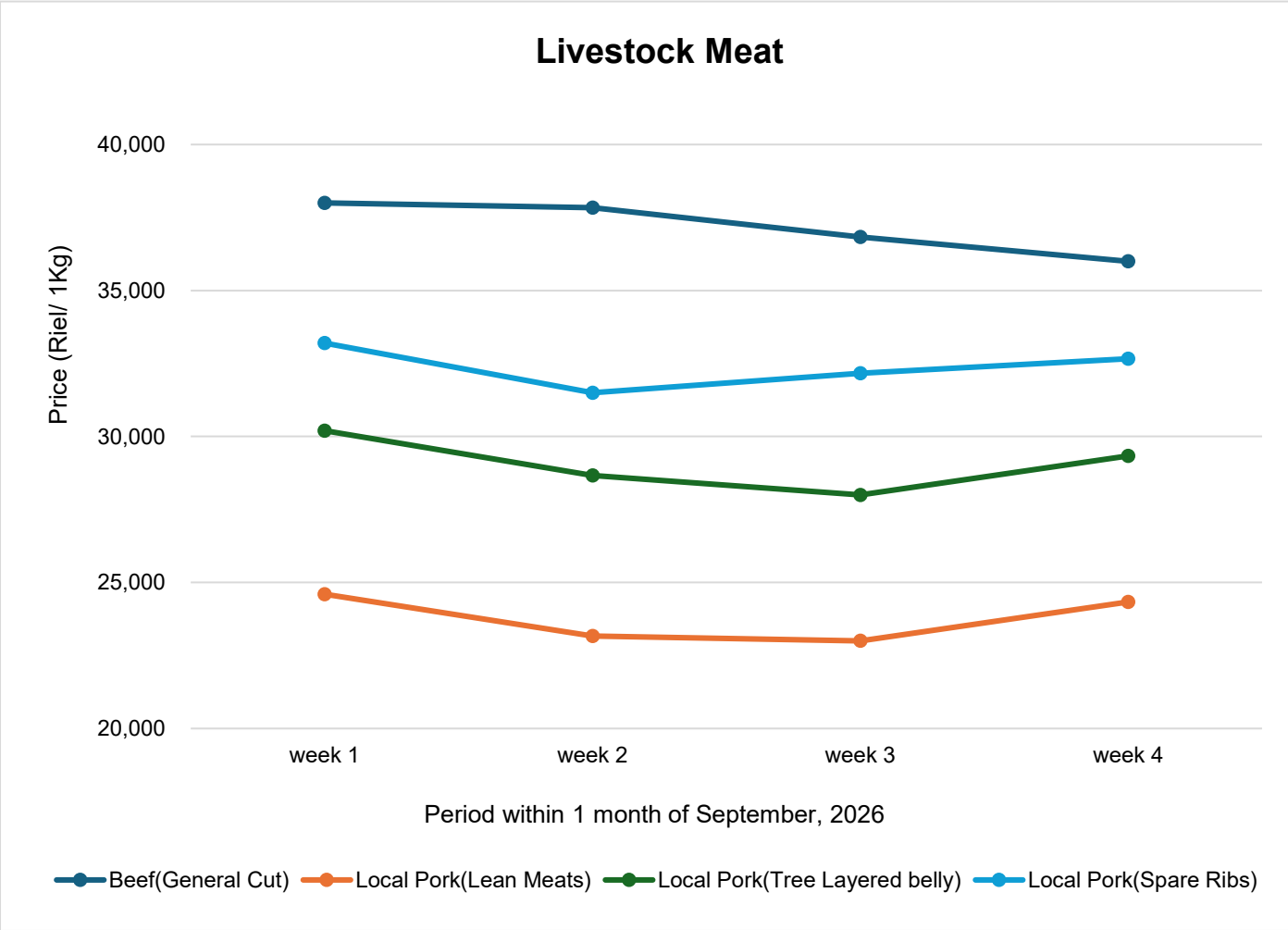
By: Sara Sreyneath and Ken Chenda

In September 2026, the Cambodia Agricultural Commodity Price Monitor indicates slight declines in the prices of livestock and meat, poultry, fruits, and vegetables, while prices of eggs, cereals, and grains remained relatively stable. In contrast, oil prices and the exchange rate showed an upward trend. Meanwhile, in Vietnam, livestock and meat prices declined, while spices and stimulants, as well as rice and grains, recorded slight increases during the month.

Cambodia

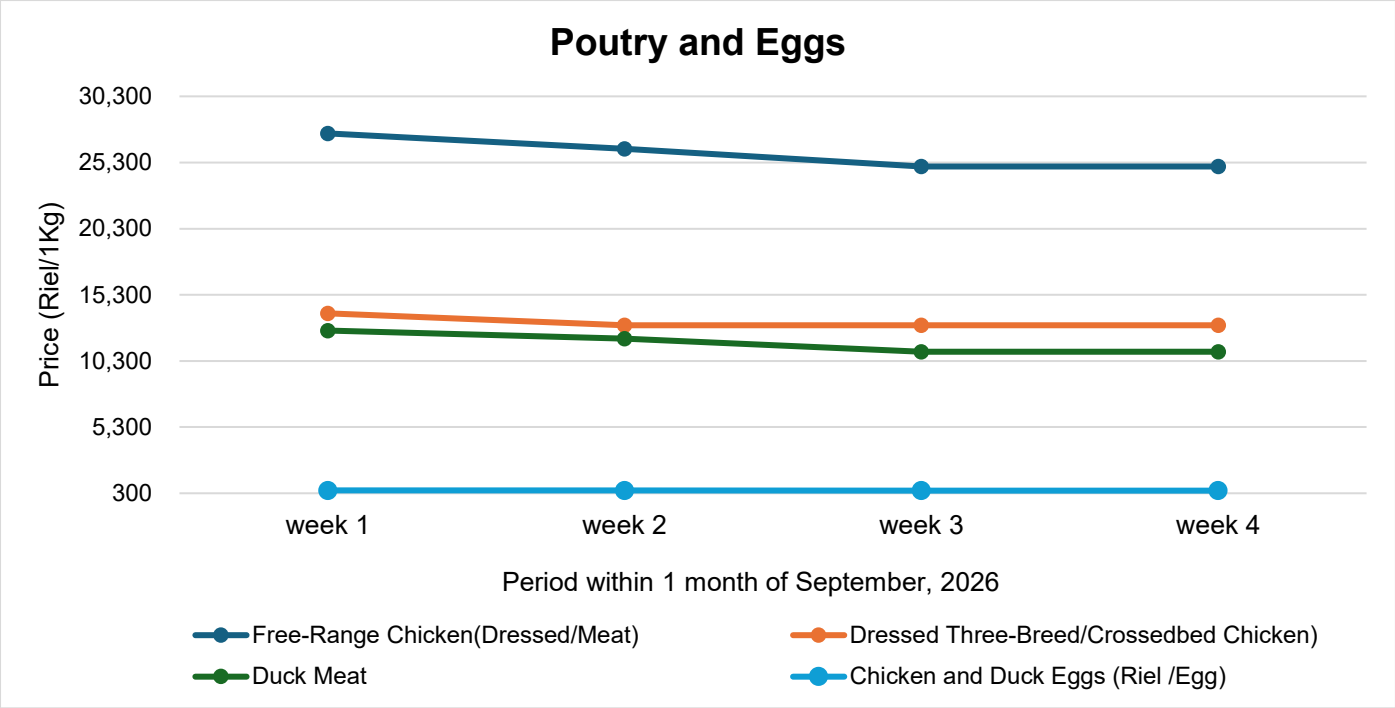
MEAT PRICE

1. *Livestock Meat*



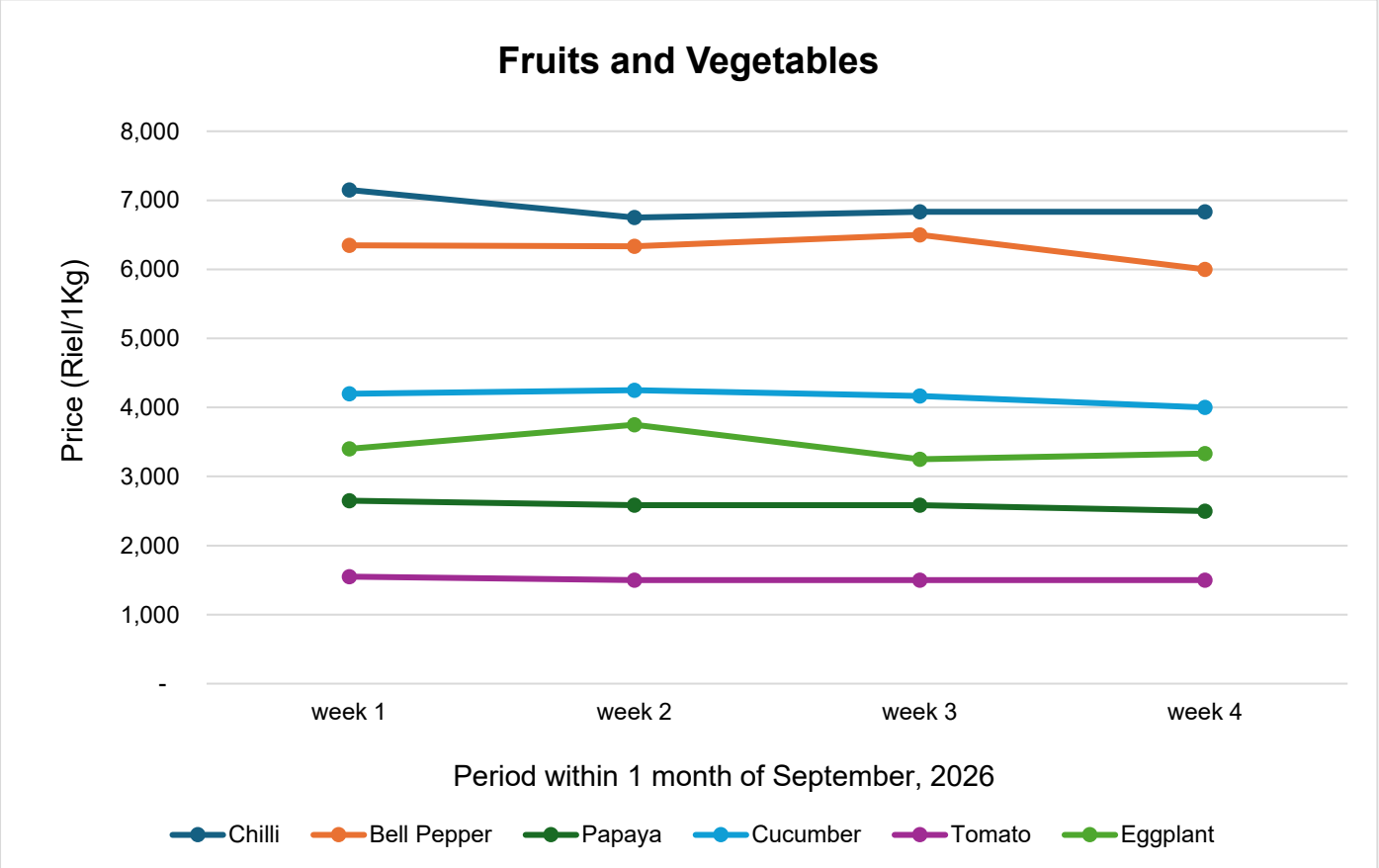
Source: Department of Government Policy Support of ARDB

2. Poultry and Eggs



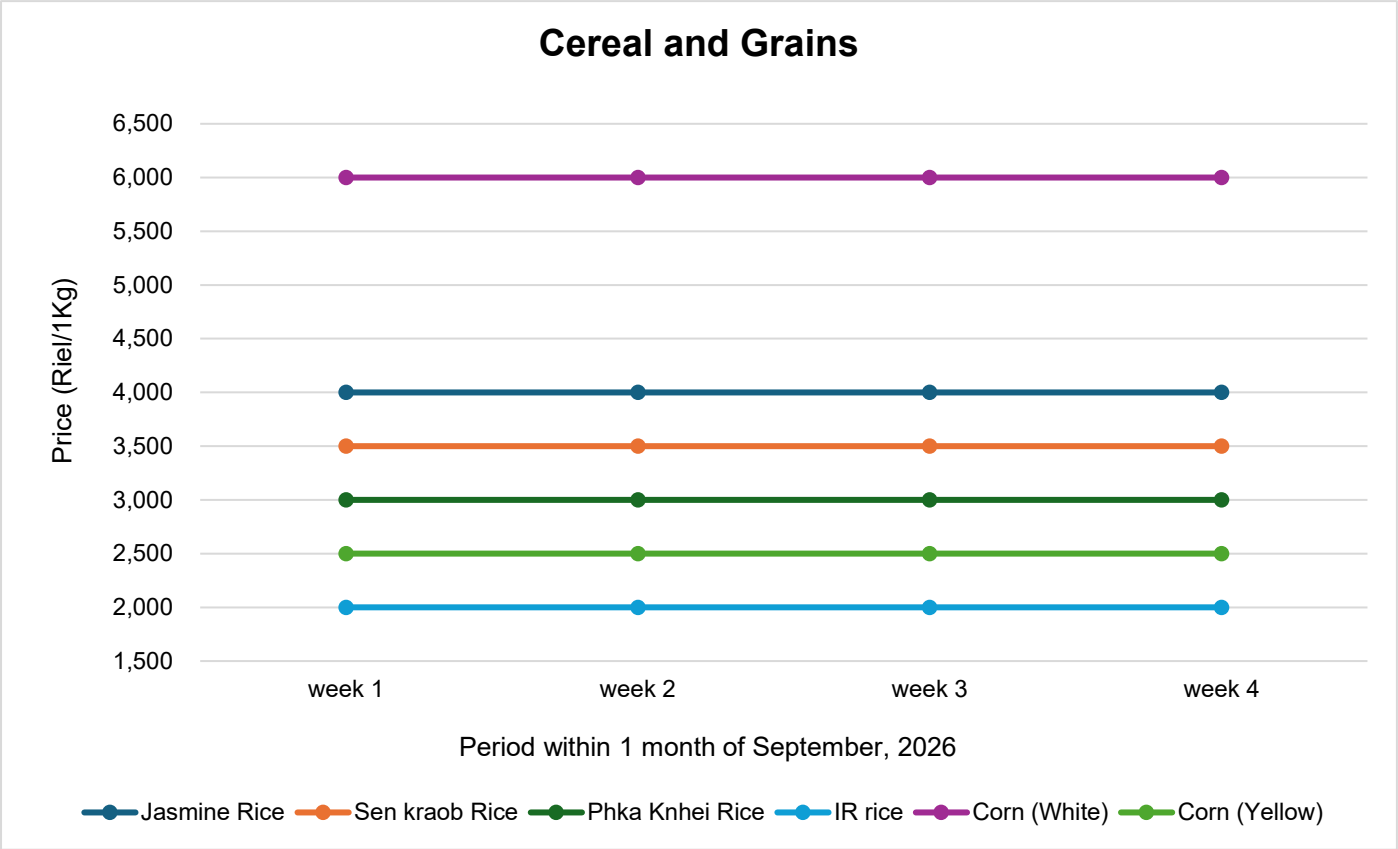
Source: Department of Government Policy Support of ARDB

3. Fruits and Vegetables



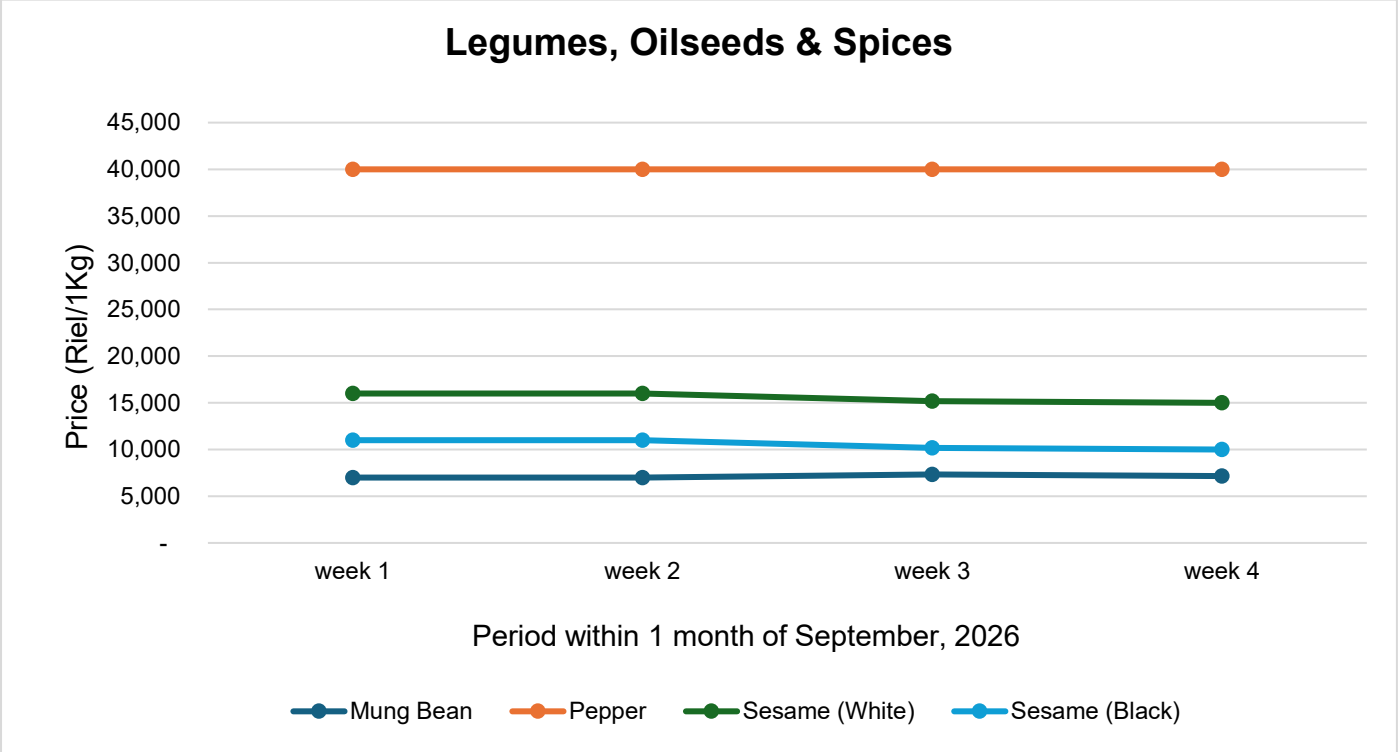
Source: Department of Government Policy Support of ARDB

4. Cereal and Grains



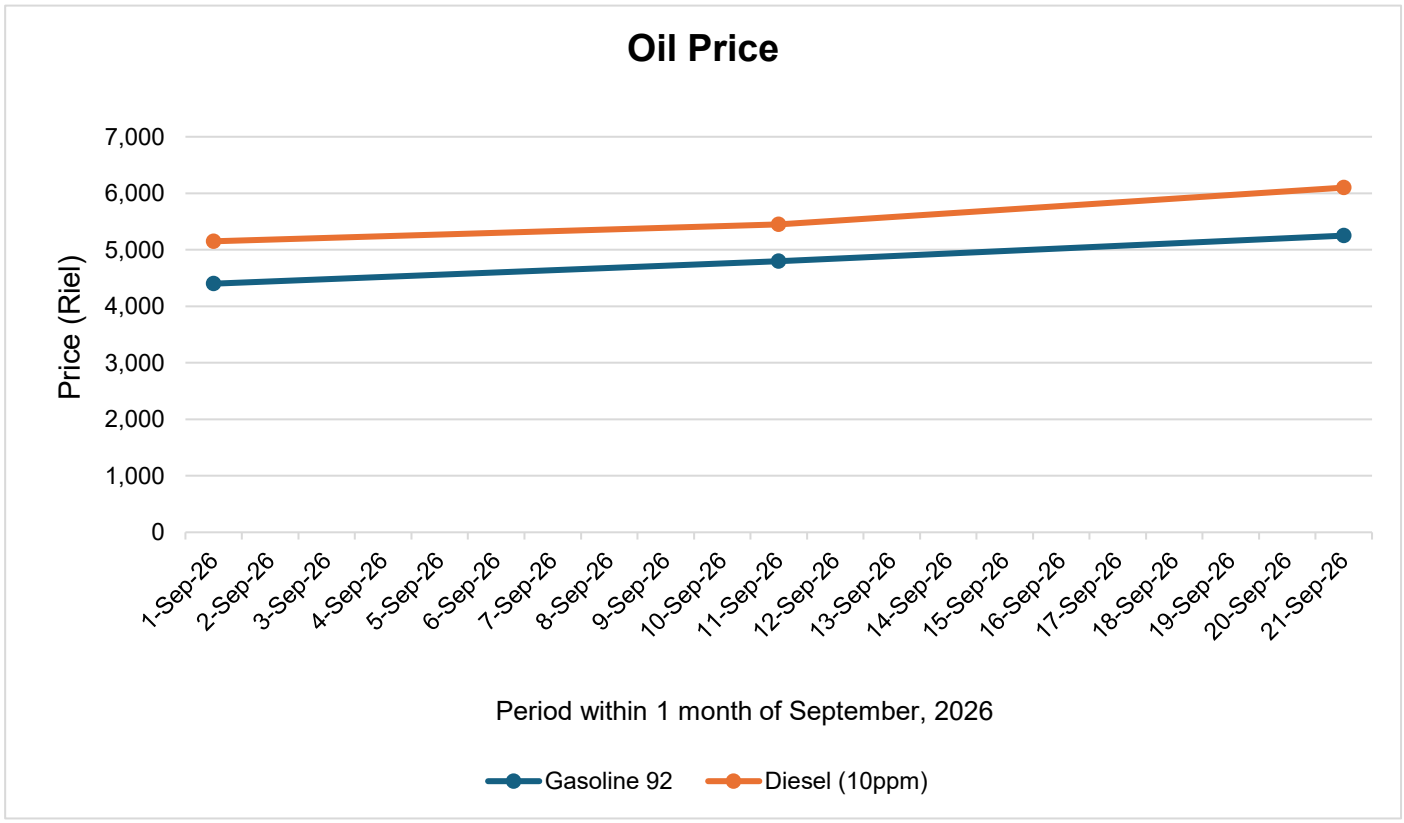
Source: Department of Government Policy Support of ARDB

5. Legumes, Oilseeds & Spices



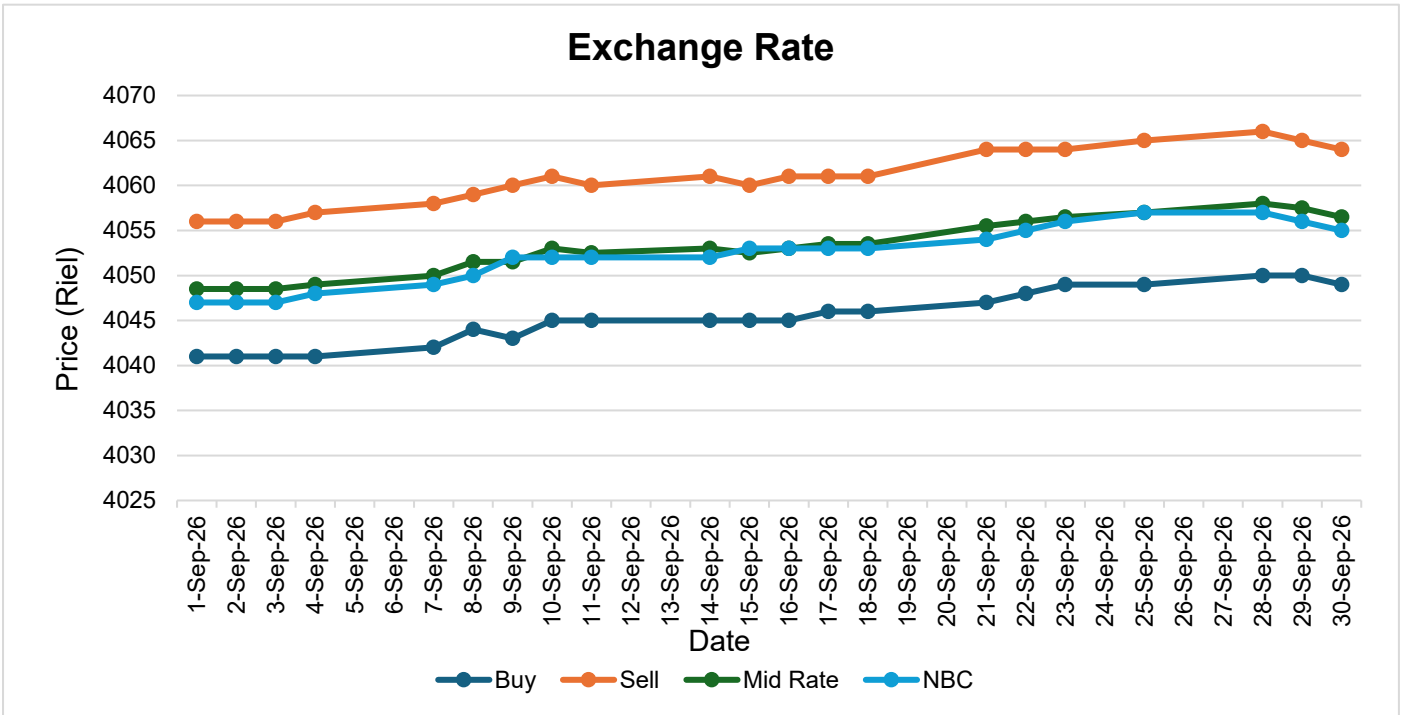
Source: Department of Government Policy Support of ARDB

OIL PRICE



Source: Ministry of Commerce, Cambodia

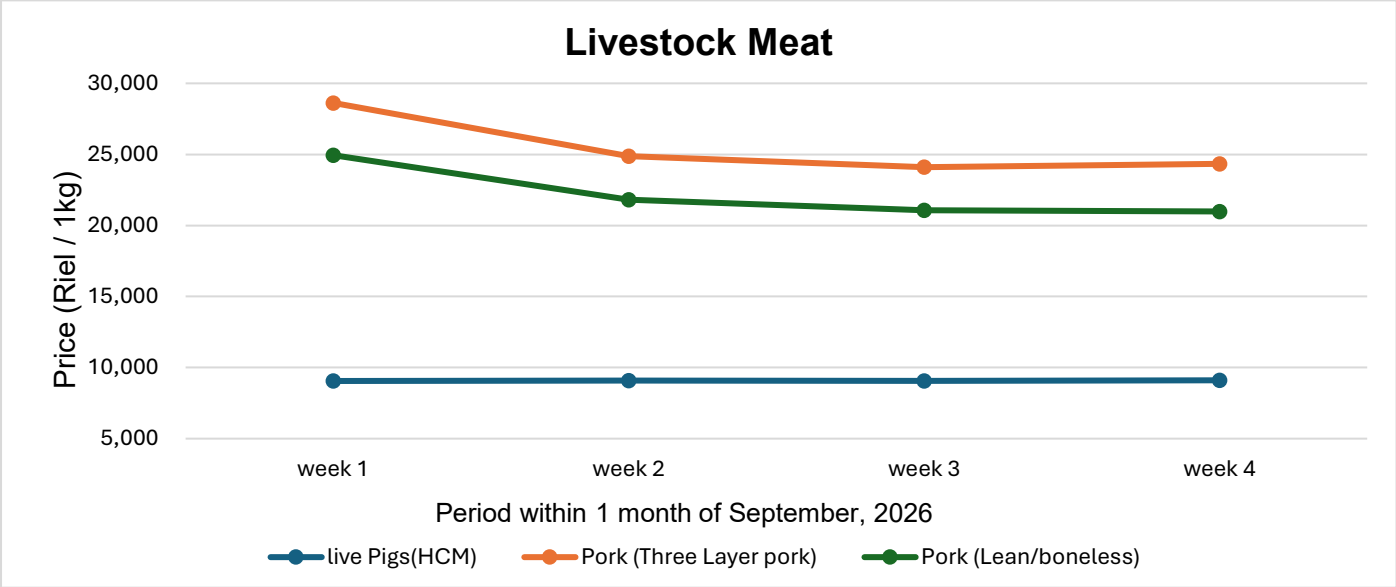
EXCHANGE RATE



The buy and sell prices are excerpted from the ARDB Bank's exchange rate

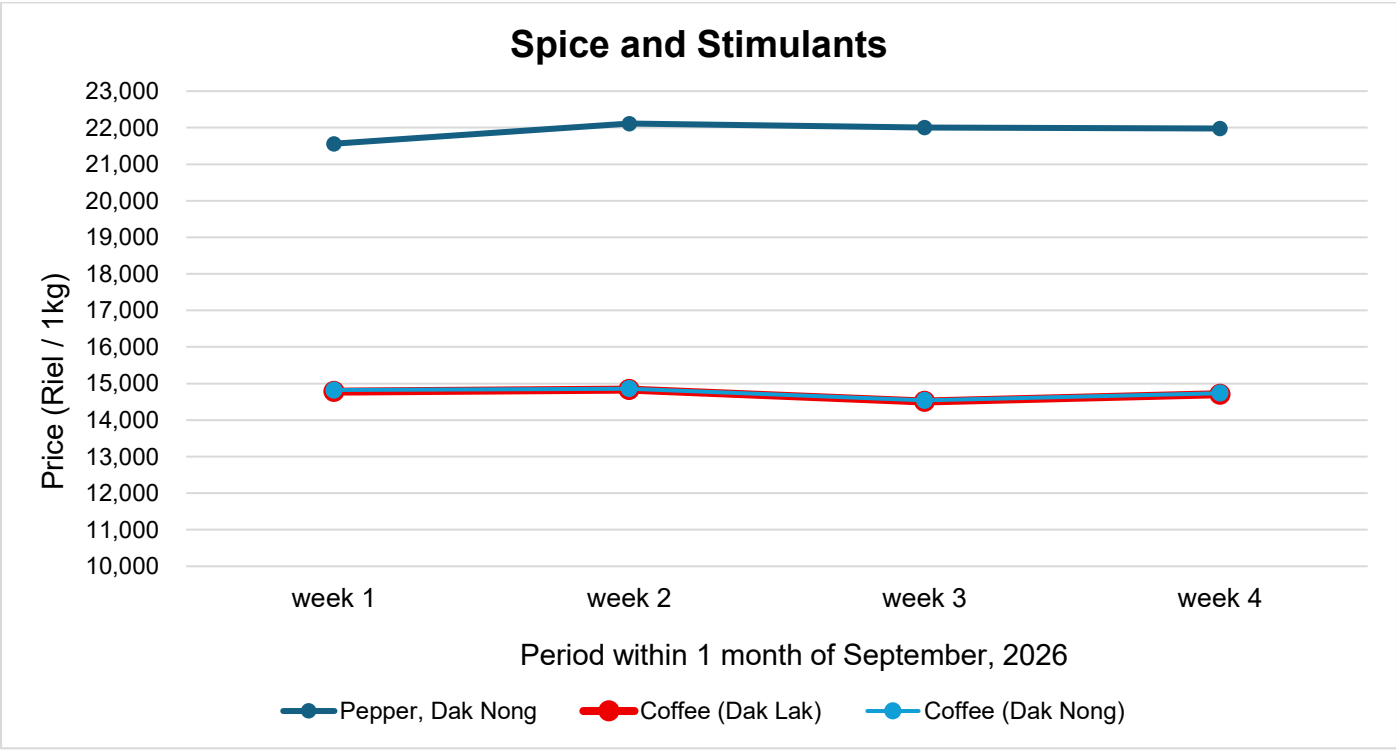
Vietnam

LIVESTOCK



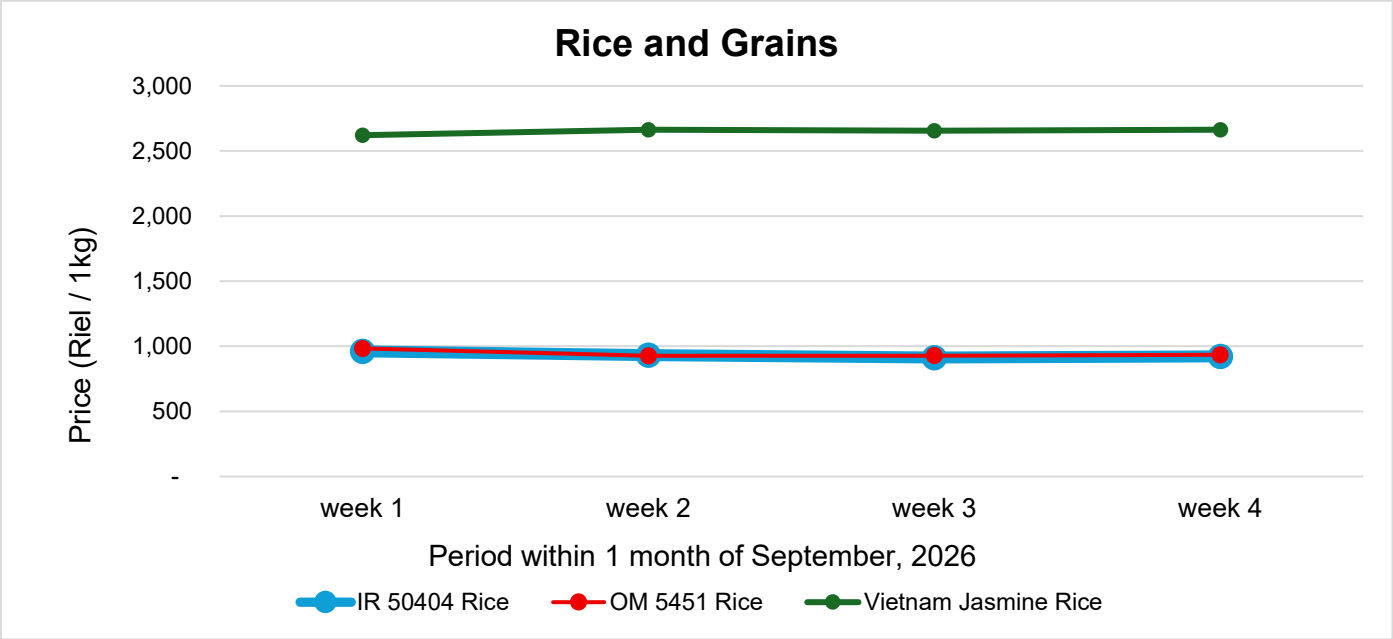
Source: https://vietnambiz.vn/ (2026)

SPICE & STIMULANTS



Source: https://vietnambiz.vn/ (2026)

RICE & GRAINS



Source: https://vietnambiz.vn/ (2026)

ជណ្ដុំបណ្ឌិតសភាចារ្យ អួន ពន្ធមុនីរ័ត្ន
Akkak Pundit Sapheachar Aun Pornmoniroth Center

Empowerment Excellence Collaboration Integrity Respect