SOCIAL MEDIA: A DOUBLE-EDGED SWORD IN THAILAND'S CYBER SCAM CRISIS

Since 2022, Thailand has witnessed a surge in cyber scam-related news and scandals, making online fraud the second most pressing concern among Thai citizens by the end of 2024. While fraud operations take many forms, investment schemes and cross-border scams have emerged as two of the most prevalent. Social media plays a vital role in these schemes, providing scammers with unrestricted access to victims and unsuspecting accomplices. At the same time, it has been instrumental in driving public outrage, raising awareness and bringing cases to national and international attention.

This article examines the role of social media in cyber scams in Thailand through two high-profile cases: the iCON Group case, a pyramid-based investment and sales scam, and the case of Chinese actor Wang Xing, who was trafficked to a scam compound in Myanmar, along the Thai border. These two cases show the complex relationship between fraud operations and digital platforms, where social media facilitates exploitation to lure victims while, at the same time, being used for scrutiny and public accountability.

Luring Victims: How Cyber Scams Exploit Social Media

In a context where the majority of Thai people have digital identities through platforms such as Facebook and TikTok – 90% and 83% of internet users in 2024, respectively – social media plays a crucial role in cyber scam operations. It enables scammers to identify potential targets and manipulate them in increasingly sophisticated ways, making them more likely to fall victim to fraud.

One of these tactics is the use of celebrity endorsements to legitimise scam operations, where celebrities are recruited to act as spokespeople and to promote scams on social media, lending their public credibility to the ventures. The case of The iCON Group, a documented example of a pyramid scheme, illustrates this

tactic. Established in 2018 and seeing a boom during the pandemic, the iCON Group initially sold health and beauty products, then gradually marketed itself as an online sales course provider. Once unsuspecting victims were enrolled, they were asked to make larger financial commitments to purchase the Group's products and were instructed to recruit other victims into the scheme. In one of the biggest financial scams perpetrated in the country, over 10,000 individuals have already filed complaints about losses totalling more than THB 3.2 billion.

To further promote the scam, the Group engaged high-profile Thai celebrities to oversee specific public-facing divisions by promoting products and courses through their social media pages. In return, figures such as actors and TV hosts like Kan Kantatavorn were compensated THB 80 million (USD 3.34 million) and Pechaya "Min" Wattanamontree received THB 11 million (USD 322,000) for her roles in promoting the Group. By the time law enforcement seized operations, at least 15 prominent celebrities had been linked with the Group.

Social media also facilitates cyber scam operations by disseminating false job advertisements, creating a breeding ground for human trafficking, particularly targeting individuals in financially vulnerable situations and affecting people from Thailand and neighbouring countries. Frequently posted in employment forums or job-search groups on social media platforms like Facebook, these ads lure victims into crossing borders into neighbouring countries like Myanmar or Cambodia. Once there, they are forced into running the scam operations and have their passports and other identification documents confiscated to prevent them from escaping the compound. Victims are not allowed to leave unless they fulfil an impossible quota to "pay off" their debts. Aggravating the concern is the fact that Thai authorities have denied the extent of the problem, broadly claiming that those trafficked to operate the scams do so voluntarily. However, following widespread public backlash on the statement, authorities later apologised and clarified that this information was inaccurate, revealing that most of the individuals involved were, in fact, victims.

The case of Chinese actor Wang Xing's disappearance in early January 2025 illustrates the extent of the problem. Scam operators posed as legitimate casting agents from the production company "GMM Grammy" and lured Wang with fake job offers. These scammers built trust with Wang on social media and were able to lure him to travel from China to Thailand for what he believed was a genuine acting opportunity. They then forcefully transported him to a fraud compound in Myanmar, where he was imprisoned and coerced into participating in fraud activities.

These two examples highlight the role of social media as an enabler of fraud. Platforms such as Facebook, Instagram and TikTok provide scammers with direct access to potential victims, allowing them to exploit trust through celebrity endorsements and fraudulent job postings. The iCON Group case exemplifies how cybercriminals leverage public figures to legitimise deceptive schemes, while the trafficking of individuals through false job ads underscores the darker consequences of digital manipulation. As scam operations grow in sophistication, the need for stronger digital literacy, regulatory measures, and cross-border cooperation becomes more urgent. Addressing these challenges requires not only law enforcement action but also a collective effort to enhance public awareness and platform accountability to mitigate the risks posed by cyber scams.

Raising Awareness on Social Media to Combat Cyber Scams

Social media can also serve as awareness-raising tools, exposing cyber scams to the public. Viral exposés and investigative reporting shared online have played a crucial role in bringing fraudulent operations to light. As a result, digital platforms are not just spaces for exploitation but also arenas for public scrutiny and accountability, demonstrating the need for stronger regulation and digital literacy to navigate the risks of online fraud.

Attention on Wang's case began in late December 2024 when his girlfriend's post on Chinese social media, Weibo, became internationally viral and subsequently shared amongst Thai social media users. As the story gained traction, public outrage erupted in both Thailand and China, leading to pressure for Thai law enforcement to conduct a rescue operation. Wang was eventually brought back to Thailand and returned home in early January 2025. His rescue operation brought public attention to the role of human trafficking in scam operations and prompted further investigations into the tactics used by traffickers.

In the case of The iCON Group, online interest soared after a prominent show "Hone-Krasae" – a TV talk show discussing emerging scandals – covered the issue. The segment ignited widespread discussion, encouraging many individuals to share their personal experiences with the company across social media platforms. This fostered greater public outrage and engagement on content related to the issue.

Research conducted by Wisesight, a social media analytics company, with the support of Thai Media Fund through its "Media Alert" project, found that these were some of the most discussed topics online. The iCON Group's fraudulent activities became the most engaged content in October 2024, and it continues to receive media attention months after the news first broke.

Research also found that Wang's case was similarly highly engaged and generated widespread discussion online, albeit limited to the relatively short period between when Thais got hold of the news and when Mr Wang was rescued (early January 2025). In both cases, in a matter of days, viral videos, memes, and critiques flooded the digital landscape, with users not just consuming the content but actively debating, expressing outrage, and dissecting the broader implications.

What fueled the public's interest in these particular scams was not only the financial losses involved but also how the cases intersected with broader trends within Thailand's digital space. The connection between well-known public figures and criminal activity tapped into a broader fascination with fame and scandal and sensationalised these cases – something that, in Thailand, attracts high levels of engagement online.

The sensationalisation of these cases illustrates how Thailand's "scandal culture" – where public outcry is not only amplified but sustained through the viral nature of social media – was vital in highlighting potential failures in addressing cyber scam cases sooner and more effectively. The interactive nature of social media resulted in large amounts of online content, "liked", shared, and commented on by thousands, highlighting failures on the part of authorities – whether due to delayed responses or concerns about institutional involvement in the operations themselves. This was of note in particular for the iCON Group cases where politicians and some bureaucratic officials were exposed to be supporting the operation of the Group to avoid scrutiny. Meanwhile, in the case of Wang Xing, the crime's severity – the use of human trafficking – was the key reason why public anger erupted. In addition, the scandal also touched on broader implications for the Thai tourism industry caused by the damage to Thailand's international reputation.

Policy Responses and the Path Forward

Instances of cyber scam operations, exemplified by the Wang Xing and The iCON Group scandals, present a significant challenge for policymakers. These high-profile scams, which gained widespread attention, have triggered intense public outcry, placing pressure on authorities to respond swiftly and effectively. In the wake of these scandals, and as investigations continue, policymakers are considering a range of reforms aimed at strengthening the regulatory framework.

At a national level, one such proposal is that financial institutions and mobile service providers should face penalties if they do not actively implement measures to prevent fraud. This could include steps like

improving security systems, monitoring transactions for suspicious activity, or offering customers fraud protection services. By holding these companies accountable, the aim is to incentivise them to be more vigilant and proactive in protecting their clients.

There is also increasing agreement on the importance of addressing gaps in existing regulations. These loopholes allow fraudulent activities to slip through the cracks, such as pyramid schemes, false direct sales practices and inadequate consumer protection.

The controversy surrounding the alleged protection of the iCON Group by a Member of Parliament (MP) has sparked calls for increased political transparency and accountability. The claims suggest that the MP may have shielded the group from scrutiny, which has raised concerns about the influence of private interests on public office. In response, the Speaker of the House took decisive action by ordering a thorough investigation into the conduct of MPs to ensure that such actions are addressed and to restore public trust in the integrity of elected officials. In a related development, politician Samart Janechaijittawanich was implicated in accepting bribes from the iCON Group after a recording of a phone conversation with the group's leader was leaked and shared online and in the media. The leak sparked widespread public pressure and outrage, leading to his expulsion from his political party.

Policymakers recently debated cutting electricity and internet supply lines between the Thai-Myanmar border, which scam operations have been exploiting for illegal activities. After months of intense discussion between the government and the opposition, on 5 February 2025, Thailand decided to cut supply lines to certain areas, citing national security concerns. Meanwhile, the government is currently working with Chinese authorities to crack down on scam centres along the border areas. The government's decision highlights the growing urgency to combat cross-border criminal activities.

On the regional front, ASEAN has taken notable steps towards combating online fraud. In January 2025, ASEAN's Digital Ministers convened in Bangkok. The ministers committed to enhancing cross-border cooperation in the fight against cybercrime by developing an early warning system and capacity-building for officials. This followed a step taken by consumer protection councils and mechanisms in ASEAN+3 countries to sign an MOU on cross-border support in cyber scam prevention.

Addressing cyber scams requires a multifaceted approach, combining national regulatory reforms with regional cooperation. While domestic measures such as holding financial institutions accountable, closing legal loopholes, and enhancing political transparency are crucial, they must be reinforced by broader cross-border efforts. ASEAN's commitment to strengthening regional collaboration through early warning systems and joint cybercrime prevention initiatives marks a significant step forward. However, sustained political will, effective enforcement, and continued public engagement will be essential in tackling the evolving tactics of cybercriminals.

The Path Ahead: Strengthening Protections Against Cyber Scams

As cyber scams continue to rise, policy solutions will be a crucial step in addressing this growing threat. Looking at the measures adopted by Thailand's ASEAN counterparts offers valuable insights. In Singapore, the Protection from Scams Act (2024) empowers law enforcement to intervene in fraudulent transactions at the bank level. However, critics within the country have raised concerns about personal privacy and the potential for government overreach. Malaysia's National Scam Response Center (NSRC), established in 2022, reflects the growing recognition of the need for dedicated institutional frameworks to combat digital fraud. However, the NSRC has been criticised as ineffective due to its lack of enforcement powers, particularly its inability to coordinate the work of multiple ministries and agencies. Thailand can learn from these challenges and ensure that its own measures include both strong enforcement mechanisms and credible checks and balances to prevent misuse of authority.

A long-term strategy should also focus on Media Information and Digital Literacy (MIDL) to increase public awareness and resilience. Individuals with low digital literacy – often those already socially and economically disadvantaged – are disproportionately targeted by scammers. While stricter regulations can help mitigate immediate risks, they must be complemented by broader public education efforts. Developing a national MIDL strategy would require collaboration between government bodies such as the Thai Media Fund, private sector actors, and technology companies, alongside active public engagement.

Finally, the public should also learn from past cyber scams and recognise the role of social media as a tool for meaningful change. Social media has the potential to drive awareness, resistance, and collective action on issues affecting society. Encouraging its responsible and impactful use will be key to fostering a more informed and vigilant digital community.

Overall, the rise of cyber scams in Thailand highlights the delicate balance between opportunity and risk in an increasingly digital world. While social media platforms can be exploited for fraudulent activities, they also serve as powerful tools for public accountability and advocacy. Moving forward, Thailand's enhancement of enforcement mechanisms, regularity frameworks and ethical guidelines for public officials will be key. Additionally, improving media literacy will be essential in equipping the public with the skills to navigate the digital landscape safely. Most importantly, the country's capacity to learn and adapt from cyber scam cases will help shape the future of consumer protection in the digital era, aligning with Thailand's vision for a secure and resilient digital sphere.

ASIACENTRE

Asia Centre is a civil society research institute in Special Consultative Status with the United Nations Economic and Social Council (UN ECOSOC).

The Centre's core activities involve research, capacity-building, advocacy and media initiatives, having its programmatic priority on four key constitutional liberties as enshrined in the Universal Declaration on Human Rights (UDHR): freedom of religion or belief (Article 18), freedom of expression (Article 19), freedom of association (Article 20) and the right to public and political participation (Article 21).

Asia Centre collaborates with civil society stakeholders, international non-governmental organisations (INGOs) and duty-bearers to support their respective initiatives.

It operates from its Research Hub and Meeting Hub in Bangkok (Thailand), Media Hub in Johor Bahru (Malaysia) and Training Hub in Phnom Penh (Cambodia).

Asia Centre
Asia Centre
Asia Centre
@asiacentre_org
asiacentre_org
asiacentre

website: asiacentre.org
email: contact@asiacentre.org