

บอร์ดกสทช.ไฟเขียวประกาศ'วิทยุ'

พล.อ.ท.ชนพันธุ์ ทรัพย์เจริญ กรรมการ กสทช. ด้าน วิทยุกระจายเสียง เปิดเผยว่า ที่ประชุมบอร์ด กสทช. เมื่อ วันที่ 10 เม.ย. ได้มีมติเห็นชอบ 3 ร่างประกาศด้านวิทยุ กระจายเสียงระบบเอฟเอ็ม (ระบบแอนะล็อก) ที่ผ่านการ ประชาพิจารณ์แล้ว เพื่อนำไปประกาศลงราชกิจจานุเบกษา ได้แก่ ร่างประกาศ กสทช. เรื่อง แผนความถี่วิทยุกิจการ กระจายเสียงระบบเอฟเอ็ม, ร่างประกาศ กสทช. เรื่อง มาตรฐานทางเทคนิคเครื่องส่งวิทยุกระจายเสียงระบบเอฟ เอ็ม และร่างประกาศ กสทช.เรื่อง หลักเกณฑ์ ป้องกัน การรบกวนการใช้คลื่นความถี่ของสถานีวิทยุกระจายเสียง ต่อกิจการวิทยุการบิน โดยร่างประกาศดังกล่าวเป็นแผนใน การเปลี่ยนผ่านวิทยุเอฟเอ็มทดลองออกอากาศ ที่จะสิ้นสุด สิ้นปี 67 ไปสู่ระบบใบอนุญาตในปี 68

นอกจากนี้ยังให้นำร่างประกาศ กสทช.ที่เกี่ยวข้อง กับวิทยุกระจายเสียงระบบดิจิทัล จำนวน 3 ฉบับ เพื่อนำ

ไปปรับปรุงความคิดเห็นได้แก่ ร่างประกาศ กสทช. เรื่อง แผน ความถี่วิทยุกระจายเสียงระบบดิจิทัล, ร่างประกาศ กสทช. เรื่อง มาตรฐานทางเทคนิคเครื่องส่งวิทยุกระจายเสียงระบบ ดิจิทัล และ ร่างประกาศ กสทช. เรื่อง มาตรฐานทางเทคนิค เครื่องรับวิทยุกระจายเสียงระบบดิจิทัล สำหรับร่างประกาศ นี้ เป็นทางเลือกเพื่อเปลี่ยนผ่านวิทยุกระจายเสียงระบบ แอนะล็อก ทั้งรายเก่าและรายใหม่มีทางออกในการออก อากาศในระบบดิจิทัล

ทั้งนี้กิจการวิทยุกระจายเสียง ถือเป็นอุตสาหกรรม สุดท้ายที่เปลี่ยนจากระบบสัมปทาน สู่ระบบใบอนุญาต และเปลี่ยนผ่านจากระบบแอนะล็อกสู่ดิจิทัล ซึ่งไม่เคยมี การพัฒนามามากกว่า 30 ปี โดยในส่วนของสถานีวิทยุ ชุมชนและสาธารณะไม่ต้องประมูลอยู่แล้วก็จะได้เข้าสู่ ระบบ โดยตามแผนจะออกประกาศเชิญชวนภายใน ไตรมาสที่ 2 นี้ เพื่อให้ได้ออกอากาศต่อในปี 68.

กสทช.ควงดีเอสไอทลายเสาเถื่อน ตัดวงจรแก๊งคอลเซ็นเตอร์และกลุ่มทุน



เกาะรอยคดีดัง

ภักดี วีระรัตน์



สืบเนื่องจากการขยายผลในการปฏิบัติงานร่วมกันของสำนักงานตำรวจแห่งชาติ กสทช. และ ดีเอสไอ ประกอบกับการวิเคราะห์สัญญาณและข้อมูลการใช้โทรศัพท์คนร้าย พบว่ามีข้อมูลการเคลื่อนไหวของแก๊งคอลเซ็นเตอร์จาก ฟังประเทศเพื่อนบ้าน (เกาะสน, เกาะสอง และ เกาะคู) นำมาสู่การบูรณาการกวาดล้างจับกุมเครือข่ายแก๊งคอลเซ็นเตอร์และกลุ่มทุนหนุนหลังที่คอยจัดเตรียมอุปกรณ์เทคโนโลยี เช่น กล่องบรรจุซิมอิเล็กทรอนิกส์ (Sim Box) และจัดหาซิมที รวมทั้งจัดตั้งสถานีวิทยุคมนาคมเถื่อนเพื่อกระจายสัญญาณอินเทอร์เน็ตและโทรศัพท์เคลื่อนที่ไปสนับสนุนกลุ่มแก๊งเหล่านี้

ล่าสุดเมื่อวันที่ 2 มี.ค. 67 ที่ผ่านมา ดีเอสไอ ในการลงพื้นที่ ตรวจสอบหาแหล่งที่ตั้งแก๊งคอลเซ็นเตอร์และเครือข่ายสนับสนุน หลังพบต้นตอมาฝั่งประเทศเพื่อนบ้าน (เกาะสน, เกาะสอง และ เกาะคู) ตรงข้าม จ.ระนอง ของไทย โดยมีกลุ่มทุนให้การสนับสนุน จึงประสานการปฏิบัติสนธิกำลัง สืบสวนรวบรวมพยานหลักฐาน จนนำมาสู่การจับกุมผู้กระทำความผิดตั้งเสาสัญญาณเถื่อนพร้อมของกลางหลังพบต้นตอมาฝั่งประเทศเพื่อนบ้าน (เกาะสน, เกาะสอง และ เกาะคู) ตรงข้าม จ.ระนอง ของไทย โดยมีกลุ่มทุนให้การสนับสนุน จึงประสานการปฏิบัติสนธิกำลัง สืบสวนรวบรวมพยานหลักฐาน จนนำมาสู่การจับกุมผู้กระทำความผิดตั้งเสาสัญญาณเถื่อนพร้อมของกลาง

1. เสาสัญญาณเถื่อน บริเวณท่าเรือแห่งหนึ่ง ต.ปากน้ำ อ.เมือง จ.ระนอง
2. เสาสัญญาณเถื่อน ช่างร้านอาหารแห่งหนึ่ง

ต.ปากน้ำ อ.เมือง จ.ระนอง 3. เสาสัญญาณเถื่อน บริเวณบ้านพักหลังหนึ่ง ต.ปากน้ำ อ.เมือง จ.ระนอง 4. แหล่งติดตั้งซิมบ็อกซ์ ต.บางริน อ.เมือง จ.ระนอง 5. แหล่งจำหน่ายซิมที ในพื้นที่ใกล้เคียงยึดซิมทีได้นับพันซิม ชุดจับกุมได้ทำการรื้อถอนอุปกรณ์และสืบสวนหาผู้ต้องหาผู้ต้องหามาดำเนินคดีต่อมาทาง กสทช. และผู้ประกอบการโทรศัพท์เคลื่อนที่ ตรวจสอบความเคลื่อนไหวแก๊งคอลเซ็นเตอร์และเครือข่าย หนาแน่นในพื้นที่ตะเข็บชายแดนด้าน จ.ระนอง และประเทศเพื่อนบ้าน จึงได้ขยายผล และระดมเครื่องมือพิเศษ (Spectrum Analyzer) ลงไปตรวจวิเคราะห์หาแหล่งกระจายสัญญาณแหล่งติดตั้งกล่องบรรจุซิมอิเล็กทรอนิกส์ (Sim Box) พบมีการลักลอบติดตั้งสถานีวิทยุคมนาคมเถื่อนจำนวนหลายแห่ง เพื่อกระจายสัญญาณข้ามไปยัง เกาะสอง เกาะสน และเกาะคู ประเทศเมียนมา

นอกจากนี้ยังพบแหล่งติดตั้งกล่องบรรจุซิมอิเล็กทรอนิกส์ (Sim Box) และแหล่งจำหน่ายซิมที จึงได้สนธิกำลังกับตำรวจไซเบอร์ บก.สอท.5 และ ดีเอสไอ

ทำการไล่ล่ากวาดล้างกลุ่มแก๊งเหล่านี้ ซึ่งสามารถจับกุมสถานีวิทยุคมนาคมเถื่อน พร้อมตรวจยึดอุปกรณ์ของกลางได้เป็นจำนวน 3 แห่ง เป็นความผิด ตาม พ.ร.บ.วิทยุคมนาคมฯ, พ.ร.บ.ว่าด้วยการประกอบกิจการโทรคมนาคมฯ และ จับกุมซิมทีได้นับพันซิมตาม พ.ร.ก.มาตรการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีฯ

ในการนี้เจ้าหน้าที่ได้ทำการรื้อถอนตรวจยึดอุปกรณ์ทั้งสถานีวิทยุเถื่อน กล่องบรรจุซิมอิเล็กทรอนิกส์ และซิมที พร้อมจับกุมตัวผู้ต้องหา ส่งพนักงานสอบสวนดำเนินคดีตามกฎหมาย เพื่อสกัดกั้นไม่ให้กลุ่มแก๊งเหล่านี้เข้าถึงสัญญาณอินเทอร์เน็ตและโทรศัพท์เคลื่อนที่ได้โดยง่าย ขณะเดียวกันเจ้าหน้าที่ตำรวจที่มีพื้นที่รับผิดชอบติดกับแนวชายแดนประเทศเพื่อนบ้านร่วมกับหน่วยงานที่เกี่ยวข้อง ลงพื้นที่สืบสวนหาข่าว ติดตามจับกุมการกระทำผิดกฎหมายในลักษณะดังกล่าวอย่างต่อเนื่องต่อไป

DIGITAL ASSETS

Online scam crackdown focuses on P2P crypto channel

KOMSAN TORTERMVASANA

State authorities working to suppress online scams have joined forces, pushing for the development of rules to supervise the purchase and sale of cryptocurrencies on a peer-to-peer (P2P) basis.

According to these agencies, scammers spend the money obtained from their nefarious activities to buy cryptocurrencies P2P, aiming to reduce the risk of being traced following the fraud.

The Securities and Exchange Commission (SEC) needs to adjust or develop existing regulations related to digital assets to regulate P2P activities and limit the channel for scammers, said Prasert Jantararuangthong, digital economy and society (DES) minister.

Of total online fraud damage estimated at 100 million baht per day, roughly 80% of fraudsters use the P2P channel for money transfers because it is not regulated, according to the ministry.

Mr Prasert said the SEC may have to study and consider launching additional conditions to supervise the P2P channel of crypto exchange activities.

Existing regulations focus on regulating crypto trading on unauthorised market exchanges.

He said the focus on the P2P channel is part of a series of measures to develop complete solutions to handle online fraud and call centre gangs.

Mr Prasert said there are 2 million crypto accounts held by individuals, according to the SEC.

"The move to regulate the P2P platform would not affect cryptocurrency traders on authorised exchanges," he said.

Mr Prasert held a meeting on April 9 with related authorities to address call centre gangs and suppress all forms of online crimes.

The meeting included representatives from the SEC, the National Broadcasting and Telecommunications Commission (NBTC), National Electronics and Computer Technology Center, Bank of Thailand, Thai Bankers' Association, Anti-Money Laundering Office (Amlo), Department of Special Investigation, Royal Thai Police, Interior Ministry, Defence Ministry and Foreign Affairs Ministry.

The meeting follows an April 1 order by Prime Minister Srettha Thavisin that state authorities show concrete results related to the crackdown on rampant online fraud within 30 days.

Mr Prasert said he will inform the premier about a new scheme to regulate P2P cryptocurrency purchases if the SEC shows no progress in developing existing regulations to deal with the issue.

Apart from the focus on the P2P channel, the meeting also outlined measures to comprehensively prevent online fraud and call centre scams.

First, the relevant parties are expected to jointly accelerate their data integration. The DES Ministry and the Anti-Online Scam Operation Centre (AOC) are co-hosting the

integration. All agencies must submit related information to them, such as mule accounts, mule SIM cards and suspected URL/Line information of gambling websites.

Second, the central bank and the Thai Bankers' Association are expected to immediately remove the mule accounts.

Last week Amlo closed 318,298 mule bank accounts, while the AOC closed 102,900 mule accounts.

The NBTC has been working to control the problem of mule SIM cards. The regulator asked people with more than 100 SIM cards to re-register their SIM cards and verify their identities by Feb 14.

Some 2.57 million SIM card owners verified their identities. The DES Ministry and Royal Thai Police deactivated more than 800,000 mule SIM cards.

The Defence Ministry, NBTC and Royal Thai Police are expected to step up efforts to remove illegal telecom signal towers along the borders.

The meeting also assigned the Royal Thai Police to prepare an action plan to suppress call centre gangs and online crime with a clear goal.

The DES Ministry and Royal Thai Police are expected to seek cooperation from neighbouring countries to solve online crime problems.



The SEC may have to study and consider launching additional conditions to supervise the P2P channel of crypto exchange activities.

PRASERT JANTARARUANGTHONG
DES minister

MONITORING REQUESTED
Authorities want to develop rules to regulate peer-to-peer cryptocurrency trading to foil online scammers. **B2**

EXPLAINER

KOMSAN TORTERMVASANA AND SUCHIT LEESA-NGUANSUK

Surveying efforts to halt cybercrime

Fraudsters use innovative tactics, but authorities are mustering a coordinated response to the threat

Despite attempts by state authorities to suppress cybercrime, the number of cases and damage have yet to decline as fraudsters continue to devise increasingly sophisticated ways to deceive people.

Q WHY HAS CYBERCRIME CONTINUED UNABATED?

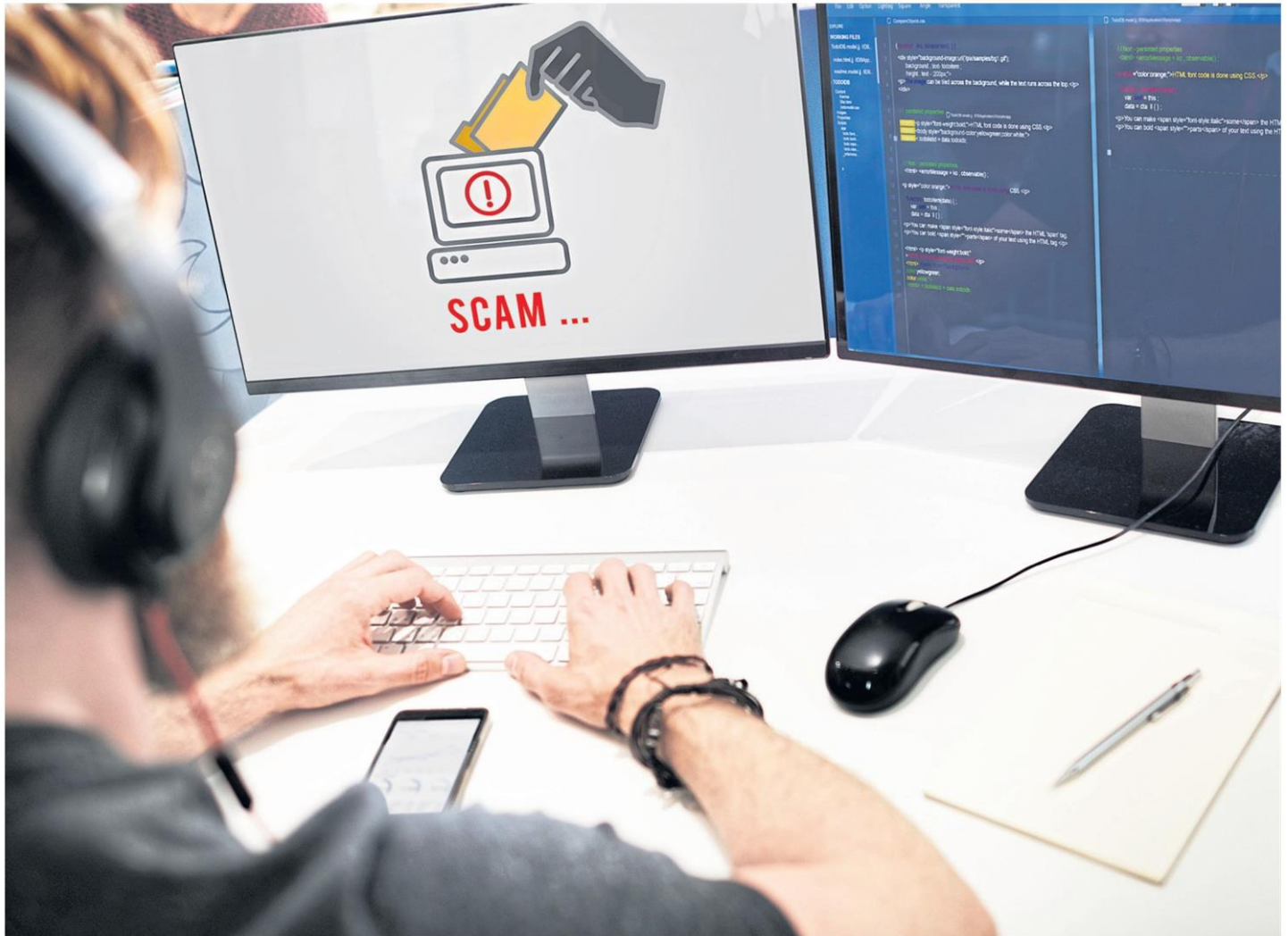
According to Prasert Jantararungthong, the digital economy and society (DES) minister, the number of cybercrime cases remains constant and damage averages 100

million baht daily, though the ministry's Anti-Online Scam Operation Centre (AOC) was established as a one-stop service point to tackle rampant online scams.

He attributed the ongoing online scams to more sophisticated strategies.

More importantly, there is not seamless integration among all relevant agencies working to reduce online crime, said Mr Prasert.

"Handling online scammers and preventing damage cannot be accomplished by some agencies. A concerted effort is needed



The DES minister attributes the inability to control online scams to more sophisticated strategies.

by all state agencies to create comprehensive protection," he said.

A source in the telecom industry who requested anonymity said one crucial issue is the "full-circuit connection," as Thai telecom operators install underground cables near border areas and expand into neighbouring countries through cooperative agreements with local companies in those nations.

This infrastructure is meant to lower telecom costs for clients under these agreements, but these connections are being used by scammers to make calls to phone numbers in Thailand, said the source.

WHAT MEASURES HAVE BEEN IMPLEMENTED?

In the past, state authorities introduced a series of efforts to deal with cybercrime, such as measures suppressing mule accounts and mule SIM cards.

These included the removal of illegal telecom towers, internet cable and telephone lines along border areas.

The National Broadcasting and Telecommunications Commission (NBTC) has been working on mule SIM cards. The commission requested people with more than 100 SIM cards to re-register them and verify their identities by Feb 14 this year.

Some 2.57 million card owners verified their identities. The DES Ministry and Royal Thai Police deactivated more than 800,000 mule SIM cards.

Recently Google Thailand partnered with the DES Ministry to launch initiatives to keep Thais safe online.

An enhanced Google Play Protect feature safeguards Android mobile phone users against scams and financial fraud. The feature blocks the installation of potentially risky "sideloaded" apps.

Sideloading is the installation of software or apps from other downloaded sources that are not authorised.

The feature was rolled out to users in Thailand, the second country after Singapore.

Google also has multiple layers of built-in protections on Android and Google Play, including spam protection in messages, safe browsing on Chrome, and Google Play Protect, which now includes real-time scanning.

WHAT NEW MEASURES CAN CONSUMERS EXPECT IN THE FUTURE?

Mr Prasert held a meeting on April 9 with related authorities to deal with call centre gangs, aiming to suppress all forms of online crime.

The meeting included representatives from the Securities and Exchange Commission (SEC), NBTC, Bank of Thailand,

Thai Bankers' Association, Anti-Money Laundering Office, Department of Special Investigation, Royal Thai Police, Interior Ministry, Defence Ministry, and Foreign Affairs Ministry.

The meeting follows an order by Prime Minister Srettha Thavisin on April 1 that related state authorities show concrete results of their crackdown on rampant online fraud within 30 days. This fraud includes call centre scams, illegal online gambling and fake news.

The meeting called for several measures to tackle cybercrime and call centre scams, but Mr Prasert acknowledged everything could not be accomplished within 30 days, as some measures require agencies to revise their rules.

The state agencies also asked the Office of the Consumer Protection Board to revise rules related to cash on delivery to prevent scams from the sale of online products. Progress on this revision is expected by May.

Relevant agencies were also instructed to accelerate their data integration. The DES Ministry and the AOC are expected to co-host the integration.

All agencies must submit related information to the AOC and the ministry, such as mule accounts, mule SIM cards, suspected URL/Line information of gambling websites, or other information the AOC requests.

The meeting on Tuesday also assigned the Royal Thai Police to prepare an action plan to suppress call centre gangs and online crime, devising a clear goal.

The DES Ministry and Royal Thai Police are expected to seek cooperation with neighbouring countries to solve online crime problems. They are also instructed to ask the Department of Provincial Administration to survey migrants living in Thailand and report the information to the AOC, which will examine whether the migrants are members of call centre gangs.

HOW MANY SCAMS ARE OCCURRING IN THAILAND?

According to the Royal Thai Police, there were 461,044 cybercrime cases from March 1, 2022 to March 15, 2024, resulting in damage of 63.6 billion baht.

The scam with the highest amount of damages was tricking people into making an online investment, with 37,829 cases and damage of 20.7 billion baht.

Call centre scams totalled 31,184 cases with damage of 7.84 billion baht.

There were 59,187 reported cases where victims transferred money to scammers in exchange for jobs, resulting in damage of 7.4 billion baht, and 3,558 cases related to digital assets with damage of 3.67 billion baht.

During the period, victims requested

294,097 suspicious bank accounts be frozen with a value of 20 billion baht, of which 4.87 billion was frozen.

In the 2023 Asia Fraud Annual Report by Whoscall, an app that identifies unknown callers and prevents smartphone scams, scam attempts in Thailand increased by 12.2 million from 2022.

The report found Thailand is the biggest target for SMS scams in Asia, receiving 58 million suspicious messages throughout the year.

Scammers used fake links, fake log-in requests, prompts to download malicious software and fake one-page shopping sites in their attempts to trick users.

Though scams decreased in Asia and globally, the study found Thais are at greater risk than ever of online fraud, with 79 million fraudulent calls and scam SMS messages attempted, an 18% increase from 66.7 million attempts in 2022.

Last year Thais received 20.8 million scam calls, up by 22% from 17 million in 2022.

Fraudulent SMS messages increased by 17% to 58 million in 2023.

Thais have the highest risk of SMS fraud in Asia. Whoscall reported Thais received an average of 20.3 fraudulent SMS messages last year, followed by the Philippines with 19.3 and Hong Kong 16.2.

Fraudulent SMS scams in Thailand focus on online gambling and loans, attracting victims with phrases such as "new username", "free giveaways" and "get 500 baht free when making your first deposit".

In addition, scammers also started impersonating government agencies, such as the electricity authority.

The annual report warned about such tactics, including impersonating delivery services in attempts to defraud the public.

The report tallied 347 million phone and SMS scams worldwide, a 14% decrease from 405 million recorded in 2022.

In Asia, the fraud trend decreased for a second consecutive year because of cooperation to raise awareness of online fraud threats between governments, business and the public, according to the company.

In June 2023, Whoscall introduced features to allow users to scan URLs and detect suspicious SMS messages.

As a result, it found 4.5% of messages contained suspicious links, with the three most common messages featuring fake log-in requests (27%), prompts to download malicious software (20%) and links to fake one-page shopping sites (8%).