

ข่าวหุ้น

Khao Hoon
Circulation: 80,000
Ad Rate: 1,100

Section: First Section/บริษัทจดทะเบียนด้านสาธารณูปโภค

วันที่: จันทร์ 6 กุมภาพันธ์ 2566

ปีที่: 29

ฉบับที่: 7116

หน้า: 1(บนขวา), 9

Col.Inch: 43.05

Ad Value: 47,355

PRValue (x3): 142,065

คลิป: สีสี่

หัวข้อข่าว: กสทช.ดีดลูกคิดรอTHCOM จ่ายค่าไลเซนส์วงโคจรดาวเทียมเร็วสุดเดือนนี้



กสทช.ดีดลูกคิดรอTHCOM

● จ่ายค่าไลเซนส์วงโคจรดาวเทียมเร็วสุดเดือนนี้

กสทช. มั่นใจ “ไทยคม” ยื่นขอใบอนุญาตกิจการโทรคมนาคมแบบที่ 3 ก่อนสิ้นตาย 17 ก.พ.นี้ ด้านกสิกรไทยประเมินผู้ชนะประมูลวงโคจรดาวเทียม 119.5 และ 78.5 องศาตะวันออกชำระเงินงวดแรก 10% และแบ่งกักรันตี เร็วสุดเดือนนี้ ก่อนรับใบอนุญาตให้ใช้สิทธิเข้าใช้วงโคจร

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ หรือ กสทช. เปิดเผยว่าตามประกาศของ กสทช.นั้น ผู้ที่ชนะการประมูลวงโคจรดาวเทียมสำหรับการอนุญาตให้ใช้สิทธิในการเข้าใช้วงโคจรดาวเทียมในลักษณะจัดชุด (Package) เมื่อวันที่ 15 ม.ค. 2566 ที่ผ่านมา และต้องทำใบอนุญาตประกอบกิจการโทรคมนาคมแบบที่ 3 ซึ่งเป็นใบอนุญาตการประกอบกิจการโทรคมนาคมเพิ่มเติม ที่มีโครงข่ายดาวเทียมสื่อสารเป็นของตนเอง เพื่อให้เข้าใช้ที่มีลักษณะการให้บริการ โดยจะต้องยื่นเอกสารดังกล่าวภายใน 30 วัน นับตั้งแต่ได้รับแจ้งผลรับรองว่าเป็นผู้ชนะการประมูล หรือ ประมาณวันที่ 17 ก.พ.นี้

ล่าสุดจากข้อมูลเบื้องต้น ขณะนี้ผู้ชนะการประมูล หรือ บริษัท ไทยคม จำกัด (มหาชน) หรือ THCOM อยู่ระหว่างการเตรียมการเอกสารเพื่อดำเนินการขอใบอนุญาตประกอบกิจการโทรคมนาคมเพิ่มเติม และจัดส่งรายละเอียดของแผน คาดว่าผู้ชนะการประมูลจะเข้ามายื่นเอกสารทันตาม

กรอบเวลาเงื่อนไขที่ กสทช.กำหนดแน่นอน ทั้งนี้หลังจากที่ยื่นเอกสารใบอนุญาตประกอบกิจการดังกล่าวแล้ว หลังจากนั้นจะมีการนำเสนอเข้าในที่ประชุมเพื่อพิจารณาขออนุญาตการให้ประกอบกิจการโทรคมนาคมต่อไป ขณะที่ในส่วนของการชำระเงินงวดแรกนั้น ก็เป็นไปตามเงื่อนไขที่ทางกสทช.กำหนดคือภายใน 90 วัน ประมาณ 10% ของมูลค่าราคาประมูล หลังจากที่มีการแจ้งผลรับรองผู้ชนะการประมูลเช่นกัน ตามประกาศเงื่อนไขการประมูลในครั้งนี้

สำหรับผลการประมูลการอนุญาตให้ใช้สิทธิในการเข้าใช้วงโคจรดาวเทียมในลักษณะจัดชุด (Package) ตามที่ทางคณะกรรมการ กสทช.ได้ให้การรับรองอนุมัติ 3 บริษัทได้แก่ 1.บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) หรือ NT ผู้ชนะการประมูลชุดที่ 4 วงโคจรที่ 126E 2.บริษัท สเปซ เทค อินโนเวชัน จำกัด ในเครือ THCOM ผู้ชนะการประมูลชุดที่ 3 วงโคจรที่ 119.5E และ 120E และชุดที่ 2 วงโคจรที่ 78.5E

ด้านนายพิสุทธิ งามวิจิตรวงศ์ ผู้อำนวยการ

อาวุโส ฝ่ายวิเคราะห์หลักทรัพย์ บริษัทหลักทรัพย์ กสิกรไทย จำกัด (มหาชน) คาดว่าไทยคมจะขอใบอนุญาตประกอบกิจการโทรคมนาคมแบบที่สาม ภายในวันที่ 17 ก.พ.นี้ ก่อนจะไปชำระเงินงวดแรก 10% ของวงเงินที่ประมูล พร้อมทั้งแบ่งกักรันตี เร็วสุดภายในเดือน ก.พ. หรือ มี.ค.นี้ แต่ไม่เกินวันที่ 17 พ.ค. 66 นี้

ทั้งนี้ภายหลังจากการชำระเงินงวดแรก กสทช.จะออกใบอนุญาตสิทธิการเข้าใช้วงโคจร 119.5 และ 78.5 องศาตะวันออกให้กับ THCOM อย่างไรก็ตามเชื่อว่าไทยคมจะชำระเงินทั้งสองวงโคจรดังกล่าวโดยวงโคจรที่ 119.5E จะเป็นวงโคจรที่ใช้ยิงดาวเทียมไทยคม 9 ขึ้นแทนไทยคม 4 ซึ่งจะสร้างมูลค่าคิดเป็นต่อหุ้นที่ 2 บาทต่อหุ้น

ส่วนวงโคจร 78.5E ใช้สำหรับยิงดาวเทียมไทยคม 10 ขึ้นไปทดแทนไทยคม 6 และ 8 ซึ่งจะสร้างมูลค่าคิดเป็นต่อหุ้นที่ 2 บาทต่อหุ้น ที่ 3.0 บาท อย่างไรก็ตามนักลงทุนยังรอดูแผนธุรกิจของไทยคมที่ชัดเจน โดยเฉพาะขนาดของดาวเทียมที่จะใช้ยิงขึ้นไปทดแทนของเดิม หากใหญ่กว่ามีประสิทธิภาพดีกว่า ก็จะมีการปรับเป้าหมายราคาหุ้น THCOM ต่อไป ■

ANALYSIS

Online scammers in the crosshairs

Authorities step up measures to combat cybercrime as schemers develop a host of ploys to fleece victims, write **Komsan Tortermvasana, Suchit Leesa-nguansuk and Narumon Kasemsuk**



Picking up a phone call from a stranger or downloading a malicious app can make life miserable for people who fall prey to call centre gangs or online scammers who have developed several tactics to fleece victims.

Scores of people have been tricked into wiring money to mule accounts or clicking malicious links provided by scammers claiming to be officials from state agencies, such as the Revenue Department.

Many also come across text messages disguised as being from banks, e-commerce operators and airlines that offer privileges, luring them into clicking links.

The Digital Economy and Society (DES) Ministry said more than 200 mobile apps were identified that are able to steal mobile users' information or control their mobile phones.

Malware embedded in these apps can take control of infected phones and secretly wire money out of users'

5 WAYS TO PREVENT CYBERTHREATS

- Do not enter important personal information online
- Do not download untrusted apps or programs
- Do not use public accounts for financial transactions
- Make your password strong and change it periodically
- Log out every time you stop using apps or programs

Source: Anti-Fake News Center
BANGKOK POST GRAPHICS

bank apps.

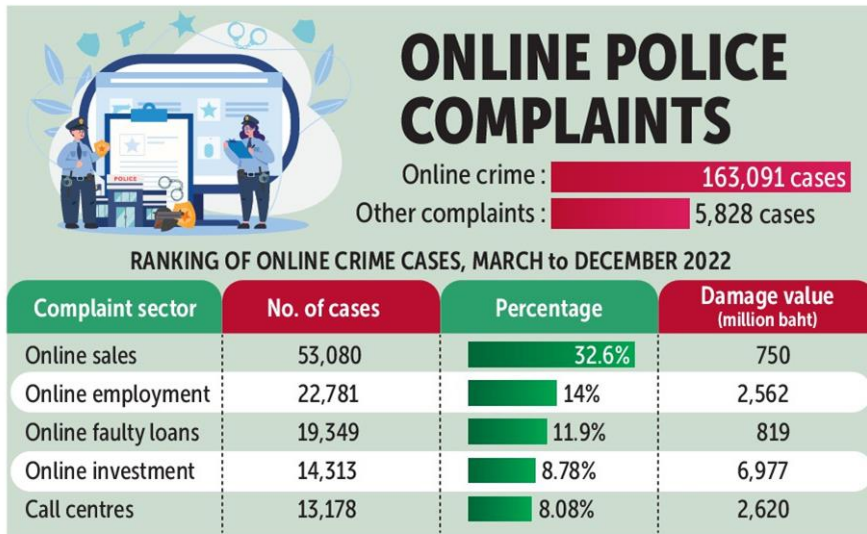
The Royal Thai Police reported 163,091 online crime-related complaints were lodged through www.thaipoliceonline.com from March 1 to Dec 31, 2022, causing an estimated 27.3 billion baht in damage.

Bogus online sales was the No.1 category of complaints, followed by being deceived into transferring money for work, fake loans, investment scams and call centre gangs.

According to the DES Ministry, 118,530 phone numbers were blocked last year because they were suspected of being used to lure victims via calls and text messages.

Some 166 suspected call centre gang members were arrested and 673 suspected investment fraudsters were apprehended in 2022. A total of 58,463 mule bank accounts were frozen.

As technology progresses, deceptive tactics will likely become more complex and fine-tuned to capture as many victims



Source: Thaipoliceonline.com

BANGKOK POST GRAPHICS

as possible.

FREE TICKETS RUSE

A recent case of swindling that used air travel as bait was identified last month when hundreds of users received a text message offering an air ticket as a reward from Lion Air.

The swindler extracted personal data from victims and withdrew around 10 million baht from a user’s bank accounts on Jan 23, while three other victims also lost money, including more than 100,000 baht in one instance.

Thai Lion Air said it reported this issue to the Cyber Crime Investigation Bureau (CCIB) last week and informed the authorities that more than 300 users said they were sent this phishing attempt.

The airline issued a statement to the media and

warned consumers about being lured into such fraudulent schemes, saying the airline didn’t have a policy to provide free tickets or other privileges via text messages.

Any transactions with the airline must be done at www.lionairthai.com.

Thai Lion Air said the CCIB agreed to help block access to criminal websites, but it would be difficult to stop scammers from sending messages to users.

HIGH GUARD NEEDED

Recently the Bank of Thailand and the Thai Bankers’ Association (TBA) released a joint statement to warn banks and consumers to keep up their guard against the elevated risk of financial cybercrime.

The statement came in response to a report that a mobile phone user possibly

lost his information and money in his bank account through a public charging cable.

Following a joint investigation by the central bank and the TBA, it was determined the fraud was not caused by a charging cable. Money was transferred from the phone’s owner because malware had infected the device, with the owner “tricked” into installing it.

The malware enabled a hacker to remotely monitor and control the phone to transfer money from the user’s bank account. The operation happened when the phone was not in use by the owner.

The central bank said fraudsters have developed many kinds of tricks, such as deceptive text messages, call centres, fake loan applications and, most recently, manoeuvres to lure consumers to install malware-embedded applications on their phones.

The regulator said it continues to introduce measures to prevent and deal with these types of fraud. The central bank has also collaborated with relevant state

Continued on Page B4

Dealing with cybercrime storm

authorities to implement measures to prevent fraud.

The Bank of Thailand urges financial institutions to consistently upgrade their tools to counteract cybercrime, as well as improve collaborative mechanisms with related parties to prevent such crimes.

MALICIOUS APPS

AVM Amorn Chomchoey, secretary-general of the National Cyber Security Agency (NCSA), said malware was found in various mobile apps that can steal the data of mobile users or take control of their phones.

In 2022, more than 200 dangerous apps were detected in iOS and Android operating systems.

Users must uninstall the apps immediately and update the latest version of their mobile operating system, he said.

“People need to be cautious about downloading or installing apps on their mobile phones as they risk data leaks or having their phones remote-controlled by others, who could wire money out of their bank accounts,” said AVM Amorn.

The DES Ministry is cooperating with Play Store and App Store to blacklist these malicious apps.

He also urged people to refrain from clicking on links in suspicious text messages. People should not add friends with Line IDs displayed on messages that offer privileges that appear too good to be true, such as approval of 50,000 baht worth of loans, or those that pose threats, such as “click link to avoid having bank account frozen”.

AVM Amorn said NCSA is gathering information on people sending fraudulent text messages in order to stop their transactions. The agency is also working with the National Broadcasting and Telecommunications Commission (NBTC) to notify mobile operators in order to block spam SMS senders, he said. Japan’s Line Corp was contacted to blacklist scammers and block those disguised as trusted firms.

AVM Amorn said banks have upgraded their apps to ward off screen captures, aiming to prevent hackers who have managed to gain unauthorized access to victims’ smartphones, obstructing them from obtaining important information.

Some websites of agencies under the Public Health Ministry contained gambling and casino ads, prompting NCSA to notify these organisations to tackle the issue, he said.

AVM Amorn expressed concern about ransomware and cloud security for Thailand this year. He urged corporations using cloud services to follow through on security checklists.

More state agencies will be offering online services to people in line with the Digitalisation of Public Administration and Services Delivery Act, which could increase the risk of cyber-attacks if they do not have proper security measures



Zero trust is the key that organisations need to embrace to ensure security.

AVM AMORN CHOMCHOEY
Secretary-general, National
Cyber Security Agency

in place.

“Zero trust is the key that organisations need to embrace to ensure security,” AVM Amorn said.

NCSA will compile a handbook on how to keep data secure, report incidents and recover data for state agencies.

The agency also plans to work with schools to provide cybersecurity education for students so they can share such knowledge with their parents.

ANTI-FRAUD MEASURES

DES Minister Chaiwut Thanakamanusorn said the government previously tried to amend the anti-money laundering law as part of measures to fight online scams.

However, the process took a long time so it decided to usher in a draft emergency decree designed to combat online fraud instead.

“The number of online fraud cases grows every day and enacting the decree should expedite efforts to combat the problem,” he said.

The cabinet on Jan 24 approved the

draft emergency decree on the prevention and suppression of technology crimes. The decree, which must be vetted by the Council of State, is expected to be enforced this month.

Then the legislation is brought to the House of Representatives for consideration. If the draft is overturned by MPs, the decree will be abolished.

Mr Chaiwut believes MPs will support the decree because it is a useful tool to deal with online fraud.

The legislation enables financial institutions and business operators to exchange information about their clients’ accounts and transactions through a data exchange system. The law also allows telecom operators to exchange information about their customers and enables the Royal Thai Police, the Anti-Money Laundering Office and authorised agencies to gain access to this data.

The NBTC office is authorised to develop a centralised database with users’ mobile service registrations and short messages for investigation and fraud prevention.

The decree allows financial institutions and businesses that are able to identify suspicious transactions or are notified by officials of such transactions to suspend them. They must also inform other financial institutions or businesses that received the transferred money to halt further transactions temporarily.

If the transaction is legitimate, it may proceed.

When they are notified by fraud victims, financial institutions and busi-

nesses are required to suspend transactions and immediately notify financial institutions or businesses that received transferred funds to suspend further transactions temporarily. This step is meant to give the victims time to lodge a police complaint within 48 hours, while police investigators are obliged to probe the suspicious accounts within seven days of being notified.

The notification of related information and evidence can be done via a phone call or electronic means.

In terms of penalties, the decree prohibits individuals from providing access to their bank accounts, electronic cards or e-wallet accounts to others that do not intend to use them. Individuals are also barred from allowing others to use their SIM cards if they know such a move could facilitate illegal activities.

Violators could face a jail term of up to three years and a maximum fine of 300,000 baht, or both.

Anyone working for others to procure or sell bank accounts, electronic cards, e-wallet accounts, SIM cards or advertises such offerings that could facilitate crimes could face a jail term of 2-5 years and a fine of 200,000-500,000 baht, or both.

Mr Chaiwut said the law can help unlock restrictions on the disclosure of personal data while clearing up some legal complications that hamper collaboration between relevant organisations in the effort to combat online crimes. He said these organisations can work together to come up with artificial intelligence-based systems or solutions

to help the authorities monitor suspicious activities or mule accounts on the National Interbank Transaction Management and Exchange platform.

RE-REGISTER SIM CARDS

Mobile SIM cards are important tools used by scammers to swindle victims out of money through phone calls. SIM cards are also tied to mule bank accounts to receive money from victims online.

In the past, many SIM dealers and distributors secretly subscribed to these SIM cards by themselves and sold them to others.

The NBTC now demands all mobile operators comply with the regulation that an individual must use an ID card to buy and register a maximum of five SIM cards, said Trairat Viriyasirikul, acting secretary-general of the NBTC.

Last year the NBTC passed a resolution to impose a fine of 1 million baht a day on carriers if they allow dealers to continue subscribing SIM cards themselves. Operators have complied with the rule since October, he said.

NBTC management plans to request those with more than 10 active SIM cards registered to one ID card to re-register them, said Mr Trairat, in a move to tackle online fraud.

He said once the draft emergency decree on the prevention and suppression of technology crime comes into force, the NBTC will proceed with this plan.

Additional reporting by **Somruedi Banchongduang**

บุคคลในข่าว



สร้างเครือข่าย ผศ.ดร.ภูมิสิทธิ์ มหาเวสน์ศิริ รองเลขาธิการ กสทช. เปิดการประชุมเชิงปฏิบัติการ การเครือข่ายผู้บริโภคสื่อแบบมีส่วนร่วมระดับประเทศ โดยมี ดร.วิชัย รูปขำดี, สัญญา กระจ่างศรี, ศรี บุญเจือ และ เพ็ญพร ทองนาค มาร่วมประชุมด้วย ที่โรงแรมมิราเคิล แกรนด์ วันก่อน.