**Bangkok Post**

**Bangkok Post**
**Circulation:** 70,000
**Ad Rate:** 1,400

**Section:** Business/First Page - Business
**Date:** Tuesday 26 October 2021
**Volume:** - **No:** - **Page:** B1 (Center), B2
**Col.Inch:** 267.19 **Ad Value:** 374,066 **PRValue (x3):** 1,122,198 **Clip:** Full Color
**Headline:** Conceiving safer payments

# Conceiving safer payments

After many consumers were recently defrauded, experts say users must accept heightened security methods when paying online, write **Suchit Leesa-Nguansuk** and **Somruedi Banchongduang**

Cyber threats are expected to escalate in the new normal lifestyle where people become more engaged in online shopping, digital payment and mobile wallets.

A person shows several rapid cash withdrawals, each of 34.15 baht, that appeared in her bank passbook when it was updated. Photo from the 'Sharing Experience on Unaware Cash Withdrawals' Facebook page.


## PREVENTIVE MEASURES

1. Do not enter personal information or provide sensitive transactional information via mobile phone, email or untrusted online apps and games.
2. Set an appropriate debit/credit card spending limit to limit the amount of damage.
3. Use transaction notification channels to provide you with the balance, account movements or expenses via SMS on your mobile phone.
4. Observe your own account for any unusual transactions, even if it's a small amount or a suspicious activity that is found, contact the bank.
5. If the bank informs you about an unusual activity, acknowledge the message and contact the bank's call centre to ensure that it is a real bank and watch out for any unusual activities that may arise from now on.




Source: ETDA BANGKOK POST GRAPHICS

From Page B1

## Social engineering, phishing key dangers

Related parties share a common view that the security bar must be further raised by both users and service operators to prevent cybercrime regarding online payment transactions.

Panic broke out last week after scores of bank card holders, particularly those with debit cards, complained via social media that their money had been removed without their knowledge or that they had been charged for certain online services that they didn't want.

Many of the fraudulent transactions were for small sums but occurred repeatedly.

Many victims are sharing their experiences on a Facebook page called "Sharing Experience on Unaware Cash Withdrawals", which has now attracted almost 100,000 members.

### HIGHER SECURITY BAR

The National Cyber Security Agency (NCSA) indicated that the recent spate of unauthor-

**Bangkok Post**

Bangkok Post
Circulation: 70,000
Ad Rate: 1,400

**Section:** Business/First Page - Business
**Date:** Tuesday 26 October 2021
**Volume:** - **No:** - **Page:** B1(Center), B2
**Col.Inch:** 267.19 **Ad Value:** 374,066 **PRValue (x3):** 1,122,198 **Clip:** Full Color
**Headline:** Conceiving safer payments

ised withdrawals of cash debited via the customers' credit and debit cards suggests the bar must be raised when it comes to security among both users and service operators.

Group Captain Amorn Chomchoey, acting secretary-general of the NCSA, said a one-time password (OTP) must be required for transactions of all sizes. At present, a small value transaction may not require OTP verification for the sake of customer convenience.

Some apps may currently only use an OTP during subscription.

Both businesses and technical teams may have to find a balance between security risk and users' convenience.

Users will have to accept heightened security methods, said Gp Capt Amorn.

"We have become more familiarised with the use of e-payment following the pandemic and we have barely got back to using only cash now. Users need to set a level of acceptable risk, such as a ceiling," he said.

Users should not use one account for all the services they receive, he said.

During the recent mass unauthorised withdrawals from bank accounts, he said, perpetrators were likely to use bots to randomly check the validity of card data, including the card number, expiry date and CVC.

Therefore, financial institutions need to detect such automated bot attacks and fraud to minimise risk, he said.

Gp Capt Amorn said consumers must accept more inconveniences through an OTP requirement for every transaction.

Consumers need to avoid using the same pass codes for every log in, such as smartphone access and mobile bank apps.

They need to link their emails with bank apps to receive notifications of transaction details and avoid using the same email passwords with all social media and online services they engage with because if the passwords were leaked, those accounts would be all gone, he said.

In the long run, the country may need as many as 100,000 cybersecurity experts with the knowledge required to detect and prevent cyber attacks and restore data following such incidents.

By next year, NCSA aims to increase the number of cybersecurity staff who have the Certified Information Systems Security Professional (CISSP) status from 250 to 300, Gp Capt Amorn added.

> **A one-time password must be required for transactions of all sizes.**
>
> **GROUP CAPTAIN AMORN CHOMCHOEY**
> Acting secretary-general, National Cyber Security Agency

## PREVENTIVE MEASURES

Yeo Siang Tiong, general manager for Southeast Asia at Kaspersky, a global cybersecurity firm, suggested various measures to prevent users from falling prey to cybercriminals.

"Each extra level of protection makes it harder for scammers to reach their goal, and ultimately minimises your losses," he said.

"You should enable 3D-Secure [MasterCard SecureCode, Verified by Visa] for all online payments and two-step authentication in your online banking tool, choose terminals with chip and PIN support and say 'no' to those requiring only a swipe and signature," said Mr Yeo.

He suggested online payment be done through secure WiFi networks and the installation of a robust antivirus solution on PCs.

Paying with a credit card at large retailers can be potentially dangerous, if a special trojan had infected their systems. This specifically applies to many retailers because often they use outdated point of sale (POS) terminals.

A leak of payment data from online merchants is another concern.

"A criminal could have somehow managed to track down the shop, which used an outdated processing system with no support for 3D-Secure, and therefore charge the victim's card," said Mr Yeo.

"To minimise risks, it is also best to not store your financial credentials with merchants."

When finding out card details have been compromised and malicious transactions have been done, users must quickly report to the banks and have their cards blocked.

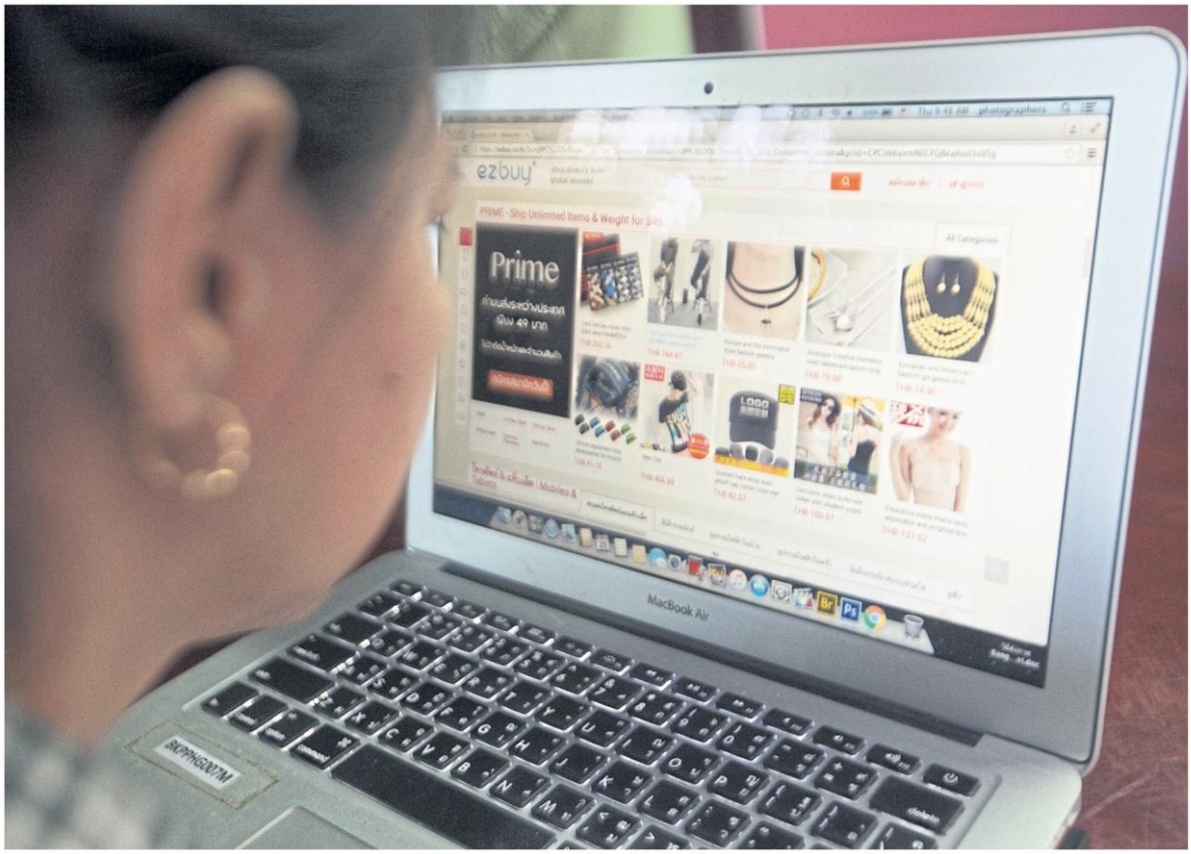
"This is because someone who stole your card credentials can also resell it to various people," he said.

According to Mr Yeo, users should have

**Bangkok Post**

Bangkok Post
Circulation: 70,000
Ad Rate: 1,400

**Section:** Business/First Page - Business
**Date:** Tuesday 26 October 2021
**Volume:** - **No:** - **Page:** B1(Center), B2
**Col.Inch:** 267.19 **Ad Value:** 374,066 **PRValue (x3):** 1,122,198 **Clip:** Full Color
**Headline:** Conceiving safer payments




**Exposure to cyber threats may increase as people become more engaged in online shopping.**
PAWAT LAOPAISARNTAKSIN

a minimum of between two and four cards.

"One dedicated card should be used only for online payments and you should avoid storing large sums on it," he added.

## CYBER THREAT CONCERNS

Cyber threats are expected to escalate in the new normal lifestyle, in which people have become more engaged in online shopping, digital payment and mobile wallets.

According to the Electronic Transactions Development Agency (ETDA), the value of

**Continued on Page B2**

e-commerce in Thailand stood at 3.78 trillion baht in 2020, but it is expected to surge 6.1% to 4 trillion baht this year.

The value of the e-commerce industry in Thailand is expected to register a compound annual growth rate (CAGR) of 9.7% between 2017 and 2021.

This highlights the surging engagement of e-commerce among customers in Thailand, which could also make them more exposed to the threats.

Prinya Hom-anek, a cybersecurity expert, indicated that most of the cyber threats in Thailand lie in social engineering and phishing where people fall prey to criminals who trick them using fear or greed tactics into clicking malicious links, such as SMS messages and emails.

There is also a growing concern about ransomware and business email compromise (BEC), an attack in which a perpetrator obtains access to a business email account and imitates executives' identity to defraud the company, its employees, customers or partners.

Regarding BEC, spoof emails of company executives may be sent to financial officers with an instruction to transfer money to an account controlled by criminals.

"BEC in Thailand costs organisations hundreds of millions of baht," said Mr Prinya.

He said financial institutions have become the top target of cyber attacks during the pandemic as staff members from financial institutions have to work from home, making them vulnerable to attacks.

Citing the "IBM Security Cost and Data Breach 2021" report, he said it took an average of 212 days to identify a breach and an average of 75 days to contain the breach.

BEC saw the highest average total cost of US$5 million, followed by phishing with $4.65 million, malicious insiders at $4.61 million and social engineering at $4.47 million.

"To mitigate cyber risks, using proper technology and creating cyber immunity among people is key," said Mr Prinya.

## STEPPING UP SECURITY MEASURES

A financial industry source, who requested anonymity, said that the banks are upgrading their security systems for online payment

**Bangkok Post**

Bangkok Post
Circulation: 70,000
Ad Rate: 1,400

**Section:** Business/First Page - Business
**Date:** Tuesday 26 October 2021
**Volume:** - **No:** - **Page:** B1(Center), B2
**Col.Inch:** 267.19 **Ad Value:** 374,066 **PRValue (x3):** 1,122,198 **Clip:** Full Color
**Headline:** Conceiving safer payments

transactions via plastic cards and will ask all e-commerce platform operators to set up a verification system on their platforms to prevent cases of fraud.

The move follows last week's meeting with the Bank of Thailand (BoT) to seek ways to deal with the spate of unauthorised withdrawals of cash debited via customers' credit and debit cards.

He added that the banks would also alert the cardholders for all online payment transactions via debit and credit cards.

Currently, the banks have different criteria in terms of alerting cardholders of their payment transactions.

The source said that earlier the number of debit card fraud cases was low as debit card spending was not popular in Thailand. The rising popularity of debit cards was in line with the fast growth of online shopping in Thailand.

The source added that these fraud cases, especially with debit card transactions, had occurred in Europe and European banks have improved their security systems to prevent this kind of fraud. This improvement in the security system has driven card scammers to switch to exploit loopholes in other countries.

Regarding the spate of unauthorised withdrawals of cash debited via customers' credit and debit cards, the Thai Bankers' Association (TBA) last week disclosed that during Oct 1-17, this kind of fraud involved 10,700 cards, of which 5,900 were credit cards accounting for transactions worth 100 million baht. The remaining 4,800 cases were debit cards with transactions worth 31 million baht.

Last week, the BoT's assistant governor for payment systems policy and financial technology group, Siritida Panomwon Na Ayudhya, said most of the cases that took place recently were small-ticket size payments via debit cards and occurred with card payments at overseas-based merchants.

> **To mitigate cyber risks, using proper technology and creating cyber immunity among people is key.**
>
> **PRINYA HOM-ANEK**
> Cybersecurity expert

The perpetrators used a robotic algorithm method to randomly select the card numbers and expiration dates when making payment transactions. The BoT confirmed that the fraud was not caused by the banks' data leak.

Miss Siritida said the BoT would also collaborate with other regulators, including the Digital Economy and Society (DES) Ministry, the National Broadcasting and Telecommunications Commission (NBTC) and the Royal Thai Police to prevent cyber risks.

Last week, the BoT and the TBA jointly set guidelines for all banks to step up measures to prevent unauthorised withdrawals of cash debited through bank cards. One guideline is all the banks will have to step up their monitoring of suspicious transactions by extending the monitoring to cover low value transactions and the highly frequent transactions made.

According to the BoT, in general online payment requires the use of an OTP to verify a cardholder's identity. However, some online shops do not require an OTP when paying for low value goods in order to provide convenience to customers.

**กรุงเทพธุรกิจ**
Krungthep Turakij
Circulation: 160,000
Ad Rate: 1,600

**Section:** การเงิน-ลงทุน/-
**วันที่:** อังคาร 26 ตุลาคม 2564
**ปีที่:** 35 **ฉบับที่:** 11975 **หน้า:** 19(ซ้าย)
**Col.Inch:** 27.02 **Ad Value:** 43,232 **PRValue (x3):** 129,696 **คลิป:** สี่สี
**คอลัมน์:** Biz Movement

กรุงเทพธุรกิจ
# Biz Movement


พล.อ.รังษี กิติญาณทรัพย์

● พร้อมแล้ว! สถานีวิทยุโทรทัศน์กองทัพบก (ททบ.5) เปลี่ยนหมายเลขช่องเป็น **"เลข 5"** ดีเดย์ 25 พ.ย. เป็นต้นไป **พล.อ.รังษี กิติญาณทรัพย์** กรรมการผู้อำนวยการใหญ่ ททบ. 5 ระบุว่า ททบ. 5 เป็นทีวีดิจิทัลประเภททีวีบริการสาธารณะเพื่อความมั่นคงและได้ใช้หมายเลข 1 ในกลุ่มของทีวีดิจิทัล ตั้งแต่ปี 2557 ซึ่งการออกอากาศที่ผ่านมา ผู้ชมยังเกิดความคลาดเคลื่อนในการเข้าถึง และยังเข้าใจแบบเดิม คือ หากต้องการรับชมรายการของ ททบ. 5 ต้องกดหมายเลข 5 ส่งผลให้ฐานผู้ชมลดลง! และเสียโอกาสในการรับชมรายการที่มีประโยชน์ ดังนั้นเพื่อให้ผู้ชมจดจำเลขหมายของช่องได้อย่างแม่นยำพร้อมการคงอัตลักษณ์ของสถานีไว้อย่างชัดเจน จึงได้ยื่นขอเปลี่ยนหมายเลขช่อง จากหมายเลข 1 เป็นหมายเลข **"5"** ต่อบอร์ด กสทช. ซึ่งได้รับการอนุมัติเป็นที่เรียบร้อย ตั้งแต่ 11 ส.ค. 2564

● ซัคเซสมอร์ เขย่าตลาดเวลเนส ส่งตัวช่วย **"PHYTOVY PROBIOTIC"** ด้วยนวัตกรรมพิเศษเจาะสายรักสุขภาพ **นพกฤษฎ์ นิธิเลิศวิจิตร** ซีอีโอ ซัคเซสมอร์ บีอิ้งค์ บอกว่า **ตลาดสุขภาพเป็นอุตสาหกรรมขนาดใหญ่ของไทย มูลค่ากว่า 65,000 ล้านบาท มีแนวโน้มเติบโตขึ้นอย่างต่อเนื่อง จากปัจจุบันขยายตัวเฉลี่ยปีละ 6.7-6.8%** สอดรับพฤติกรรมของผู้คนที่หันมาสนใจสุขภาพมากขึ้นจากหลากหลายปัจจัย ไม่ว่าจะปัญหามลภาวะฝุ่น PM 2.5 การเกิดโรคอุบัติใหม่โควิด-19 ประกอบกับประเทศไทย ถือเป็นจุดหมายของนักท่องเที่ยวที่มาเยือนและใช้บริการเวลเนส! PHYTOVY PROBIOTIC เหมาะกับผู้บริโภคที่ใส่ใจสุขภาพ โดยเฉพาะกลุ่มมิลเลนเนียลส์ หรือเจนเนอเรชั่นวาย ที่มีการหาข้อมูลเกี่ยวกับการดูแลสุขภาพเชิงลึกทั้งเรื่องการบริโภคอาหาร การออกกำลังกาย ควบคุมน้ำหนัก เสริมสร้างภูมิคุ้มกัน

● เน็ตฟลิกซ์ ร่วมกับ **"คานิวัล"** แบรนด์สตรีทแฟชั่นของไทย เผยโฉมคอลเลกชัน **"GU TING YANG WA"** ที่อัดแน่นด้วยเครื่องแต่งกายสายสตรีทและไอเทมสุดคูล ประกาศศักดาความเป็นแฟนพันธุ์แท้ของคอนเทนท์เกาหลีบนเน็ตฟลิกซ์ที่ฮิตติดลมบนจนเป็นกระแสไปทั้งบนโซเชียลและออฟไลน์ โดยคอลเลกชันนี้เตรียมเปิดให้จับจองเป็นเจ้าของพร้อมกันทั่วประเทศ 30 ต.ค.นี้ ราคาเริ่มต้น 890 บาท ผ่านเว็บไซต์ carnivalbkk.com หรือแอพพลิเคชั่น Carnival และร้าน Carnival สาขาเซ็นทรัลเวิลด์

● เตรียมพบกับประสบการณ์ใหม่ที่**เอ็ม บี เค เซ็นเตอร์** แหล่งรวมความพิเศษเข้าถึงทุกไลฟ์สไตล์! พร้อมปักหมุดรอช้อปรอชมสาขาใหม่ของร้านดอง ดอง ดองกิ (DON DON DONKI) ที่ เอ็ม บี เค เซ็นเตอร์ ศูนย์กลางของเทรนด์ใหม่จากญี่ปุ่น ซึ่งเวลานี้เริ่มติดป้ายโดยรอบตกแต่งสะดุดตาโชว์จุดขายของสินค้าและความน่ารักของ**ดองเปง** จะเป็นอีกจุดเช็คอินให้หายคิดถึงญี่ปุ่น งานนี้เจแปนนิสเลิฟเวอร์ทั้งหลายห้ามพลาด