TB-CERT
Thailand Banking Sector CERT

TB-CERT – NCSA Virtual Summit
แนวโน้มภัยคุกคามไซเบอร์และการป้องกันสำหรับภาคธนาคาร

28 November 2022

Agenda

1

ABOUT TB-CERT

Thailand Banking Sector Computer Emergency Response

ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร

- Mission
- Organization structure & Collaboration
- Member

2

Top Cyber Threat Trend in Banking Sector 2022

แนวโน้มภัยคุกคามทางไซเบอร์ภาคการธนาคาร

- Cyber Threat in the News
- How does the threat actor attack
- Fake SMS-LINE-Website-FB App
- TB-CERT Role

3

5 Pillars Activities Lead to Mission

5 เสาหลักนำไปสู่พันธกิจในปี 2022

- Professional Development
- Standard Guideline
- Security Awareness
- Research Activities
- Services Result

- Key Take away for public

TB-CERT
Thailand Banking Sector CERT

1

ABOUT TB-CERT

Thailand Banking Sector Computer Emergency Response

ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร

- Mission
- Organization structure & Collaboration
- Member

TB-CERT
Thailand Banking Sector CERT

1 Mission

TB-CERT
Thailand Banking Sector CERT

*"Be a **Neutral** and **Trusted Advisor**, an **Expertise** hub in Cybersecurity for Thailand Banking Sector"*

Thailand Banking Sector CERT (TB-CERT) was established with the approval of senior executives of commercial banks in Thailand, in order to support group members who are bank employees. The exchange of information and experience of the members is a key for beneficial of financial organizations in Thailand. This is especially useful for the prevention of cyber threats that may affect the service, resources, or personnel of an organization. The TB-CERT has four main tasks including data exchange, incident response, standardization, and human resources development.

PEOPLE

Human Development
-Training, -Workshop
-Cyber combat, -Cyber Drill

STANDARDIZATION

Develop standard for members

AWARENESS

Building awareness for public in terms of Cyber security

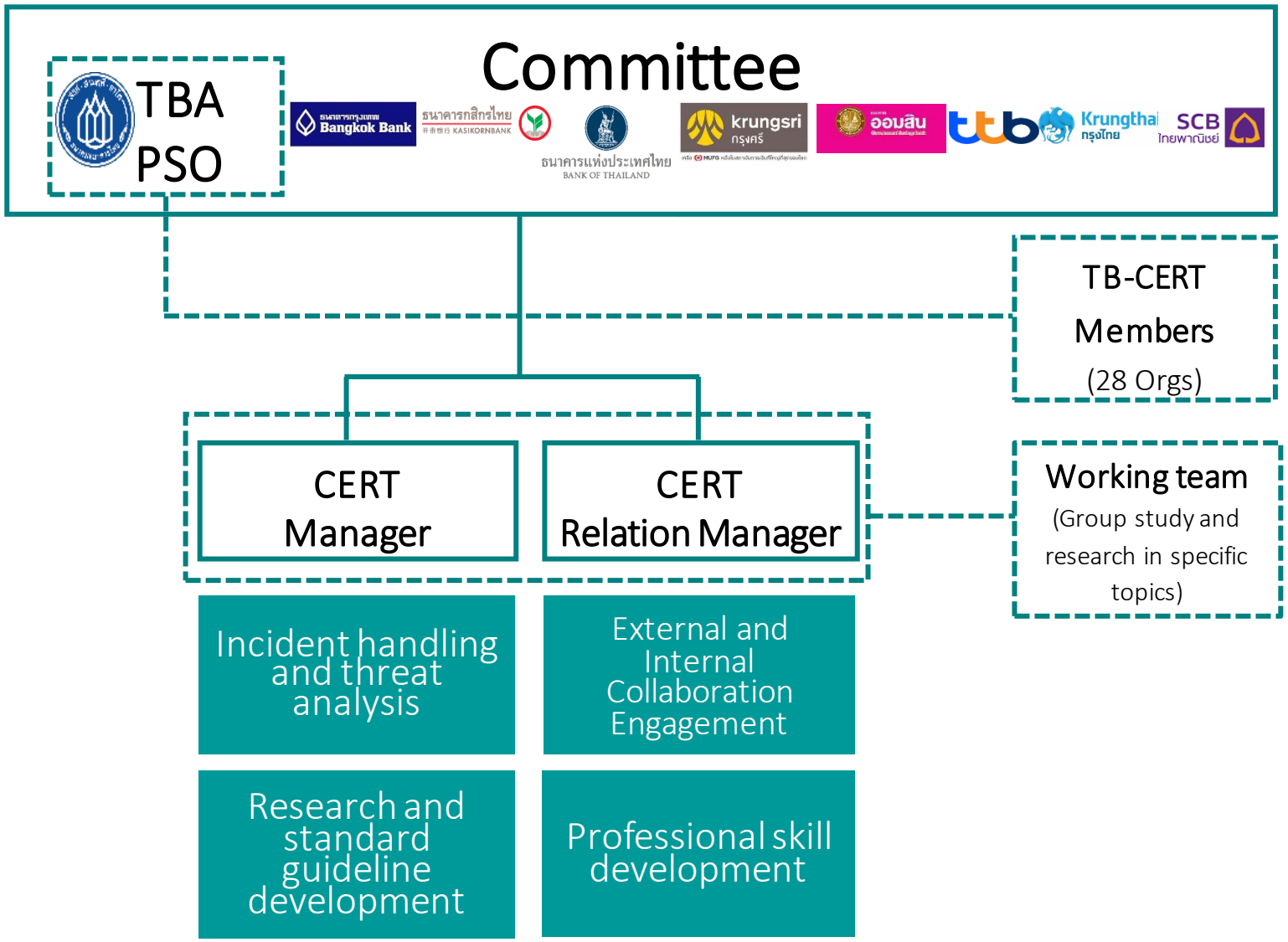
RESEARCH & DEVELOPMENT

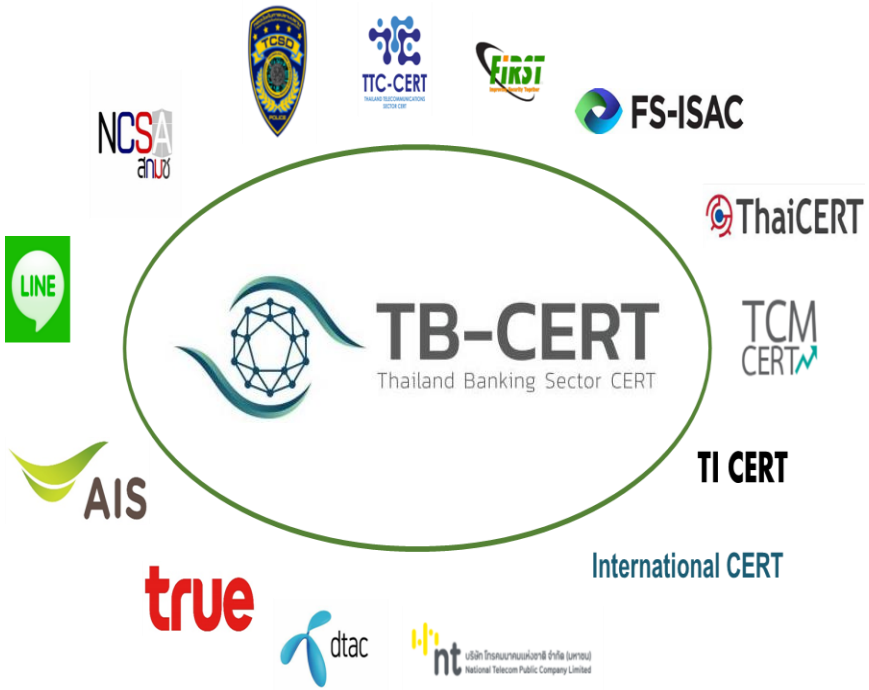
Do research and study new technologies

SERVICES

Provide service to members such as incident handling, News alerts, Technical recommendation

1 Organization Structure & Collaboration





1 TB-CERT Current Members (28)


TB-CERT
Thailand Banking Sector CERT

2

Top Cyber Threat Trend in Banking Sector 2022

แนวโน้มภัยคุกคามทางไซเบอร์ภาคการธนาคาร

- Cyber Threat in the News
- How does the threat actor attack
- Fake SMS-LINE-Website-FB App
- TB-CERT Role

TB-CERT
Thailand Banking Sector CERT

2 Top Cyber Threat Trend in Banking Sector 2022

1. Ransomware
2. Phishing
3. Account Abuse
4. API Abuse
5. Supply Chain
6. Emerging Threats
7. Future of Work
8. Evolving Cloud Risks

1. Ransomware
2. Phishing
4. API Abuse

Pre-incident

Technical Recommendation
Threat Intelligence sharing
Proactive Incident Response

Cross sector collaboration
User awareness
Threat Intelligence

API Standard

Post-incident

- Take Down
- Recommendation
- Monitoring
- Update IR Playbook

Reference: Gartner - How to Respond to the 2022 Cyberthreat Landscape

TB-CERT
Thailand Banking Sector CERT

2 Cyber Threats in the News

2 Phishing

ศูนย์ต่อต้านข่าวปลอม ประเทศไทย
Anti-Fake News Center Thailand

ข่าวปลอม อย่าแชร์! กรมสรรพากรให้เจ้าหน้าที่ทักไลน์มาแนะนำขั้นตอนการขอรับเงินคืน หากจ่ายภาษีเกินยอดที่ต้องชำระ

18 สิงหาคม 2022 | 17:00

Share | Facebook | Twitter | Link | Email

ตามที่ได้มีข้อมูลปรากฏในสื่อออนไลน์ต่าง ๆ เกี่ยวกับประเด็นเรื่อง**กรมสรรพากรให้เจ้าหน้าที่ทักไลน์มาแนะนำขั้นตอนการขอรับเงินคืน หากจ่ายภาษีเกินยอดที่ต้องชำระ** ทางศูนย์ต่อต้านข่าวปลอมได้ตรวจสอบข้อเท็จจริงโดยกรมสรรพากร กระทรวงการคลัง พบว่าข้อมูลดังกล่าวนั้น **เป็นข้อมูลเท็จ**

จากกรณีที่มีข้อมูลปรากฏในสื่อสังคมออนไลน์เกี่ยวกับประเด็นเรื่องกรมสรรพากรให้เจ้าหน้าที่ทักไลน์มาแนะนำขั้นตอนการขอรับเงินคืน หากจ่ายภาษีเกินยอดที่ต้องชำระ ทางกรมสรรพากร กระทรวงการคลัง ได้ออกมาชี้แจงว่าเป็นมิจฉาชีพแอบอ้างสนทนาผ่านช่องทาง line โดยใช้ชื่อ RD Intelligence 1161 โปรดอย่าได้หลงเชื่อ เนื่องจากปัจจุบัน RD Intelligence Center 1161 ยังไม่มีบริการสนทนาผ่านช่องทาง line หรือ Chat ส่วนตัวแต่อย่างใด

ดังนั้นขอให้ประชาชนอย่าหลงเชื่อ และขอความร่วมมือไม่ส่ง หรือแชร์ข้อมูลดังกล่าวต่อในช่องทางสื่อสังคมออนไลน์ต่างๆ และเพื่อให้ประชาชนได้รับข้อมูลข่าวสารเพิ่มเติมจากกรมสรรพากร กระทรวงการคลัง สามารถติดตามได้ที่เว็บไซต์ www.rd.go.th หรือโทร. 02 2729529

บทสรุปของเรื่องนี้คือ : เป็นมิจฉาชีพแอบอ้างสนทนาผ่านช่องทาง line โดยใช้ชื่อ RD Intelligence 1161 โปรดอย่าได้หลงเชื่อ

172 ผลการค้นหา

- Feb 6, 2022 : ออมสิน ส่ง SMS ให้ประชาชนกดรับสิทธิ์ขอสินเชื่อ GSB จำนวน 60,000 บาท
- Feb 19, 2022 : ธ.ก.ส. ส่ง SMS เข้ามือถือเบอร์ส่วนตัว เพื่อให้คลิกลิงก์เข้าระบบ
- Feb 21, 2022 : ธ.กรุงไทย ให้ยืมเงินปิดหนี้ตามนโยบายรัฐ ดอกเบี้ยต่ำ ยืมได้ทุกอาชีพ
- Mar 2, 2022 : แอปเป๋าตัง ให้กู้เงิน 1 หมื่นบาท ลงทะเบียนได้ทุกอาชีพ
- Mar 6, 2022 : ธ.กรุงไทย ส่งSMS มอบสิทธิ์เงินกู้ผ่านไลน์ และโครงการสนับสนุนเงินกู้ฉุกเฉินของธนาคาร
- Mar 12, 2022 : ธ. กรุงไทย ร่วมกับ Money Back ปล่อยเงินกู้ 300,000 บาท ดอก 100 ละ 2 บาท
- Mar 13, 2022 : ธ.กรุงไทย ปล่อยสินเชื่อประชาชนสุขใจ วงเงินสูงสุด 200,000 บาท อนุมัติภายใน 30 นาที
- Apr 2, 2022 : กรุงไทยและออมสิน ร่วมกับบริษัทเอกชน ปล่อยสินเชื่อเงินกู้ 24 เดือน วงเงิน 5,000-500,000 บาท
- Aug 13, 2022 : ธ. กรุงไทย ธ. ออมสิน ปล่อยสินเชื่อเพื่อคุณ สูงสุด 500,000 บาท ผ่าน WWW.สินเชื่อเพื่อคุณ.NET และไลน์
- Sep 19, 2022 : เจ้าหน้าที่กรมสรรพากรโทรติดต่อร้านค้าที่เข้าร่วมคนละครึ่งเรื่องภาษี และให้แอดไลน์เพื่อส่งลิงก์ให้กดยืนยัน
- Sep 24, 2022 : ธกส. ส่ง SMS ปล่อยสินเชื่อฉุกเฉินธกส. ผ่านลิงก์

TB-CERT
Thailand Banking Sector CERT

2 How does the threat actor attack?

2 Phishing

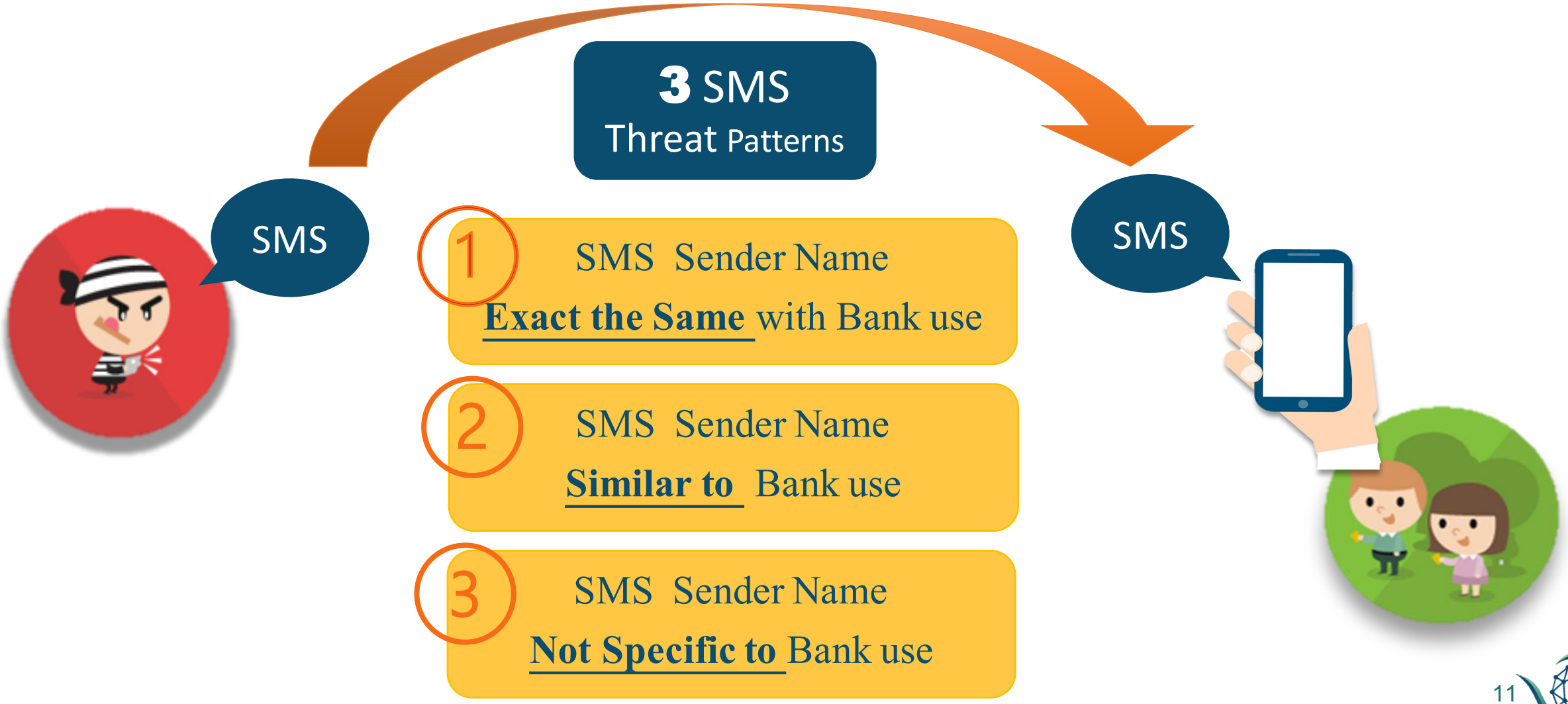
คนร้ายหลอกถามข้อมูลโดย

- ให้กรอกฟอร์ม
- ให้ลงโปรแกรม RAT

2 Observation on Suspicious Activities:

Fake SMS- Fake LINE – Fake Website – Fake Facebook App

2 Phishing

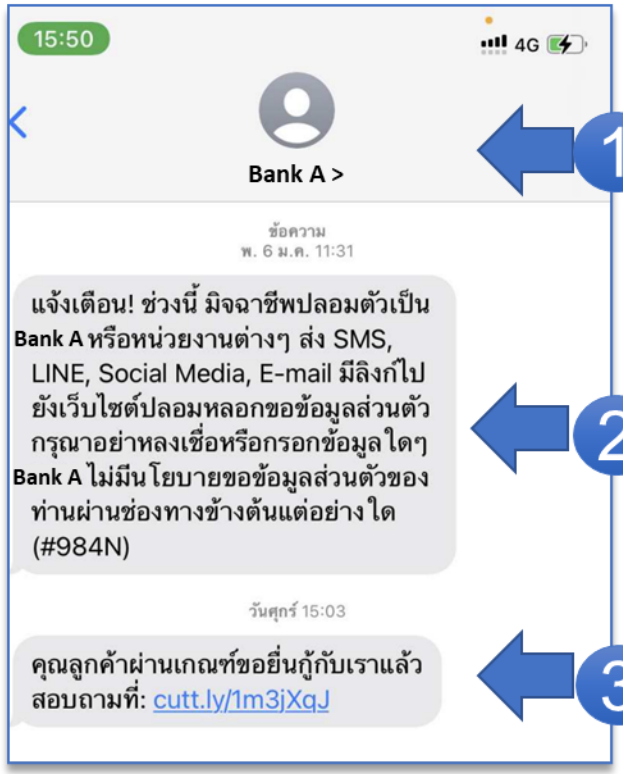


2 Observation on Suspicious Activities:

Fake SMS- Fake LINE – Fake Website – Fake Facebook App

2 Phishing

1 SMS Sender Name
Exact the Same with Bank use



1 **SMS Sender Name** ของ ธนาคาร **Bank A**

2 **SMS** ข้อความจริงที่ส่งจาก ธนาคาร **Bank A** ถึง ประชาชน

3 **SMS** ปลอมที่คนร้าย ส่งโดยใช้ชื่อ **SMS Sender Name** เหมือนของ ธนาคาร

SMS Threat Pattern #1
(ใช้ SMS Sender Name เหมือนของ ธนาคาร)

- มีผลกระทบมากเพราะเป็นรูปแบบ **SMS** ที่มีความยากสำหรับประชาขนในการสังเกตและแยกแยะระหว่าง **SMS** จริงจากธนาคาร กับ **SMS** ปลอมจากคนร้าย

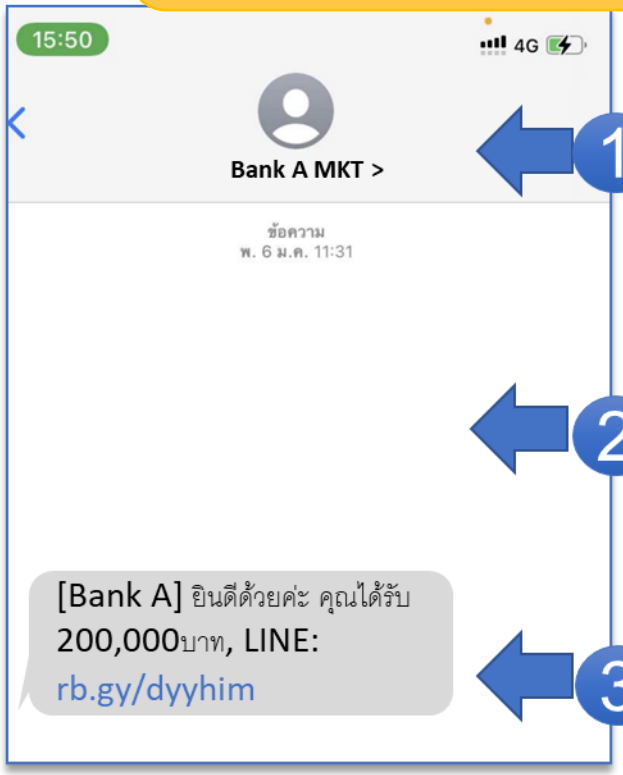
2 Observation on Suspicious Activities:

Fake SMS- Fake LINE – Fake Website – Fake Facebook App

2 Phishing

2 SMS Sender Name **Similar to** Bank use

SMS



1 SMS ปลอมที่คนร้ายใช้ Sender Name คล้ายของ ธนาคาร Bank A Bank A ≠ Bank A MKT

2 ไม่มี SMS ข้อความจริงที่ส่งจากธนาคาร Bank A

3 SMS ปลอมที่คนร้าย ส่งโดยมีเนื้อหาให้เข้าใจว่า เป็นธนาคารเสนอเงินกู้

SMS

SMS Threat Pattern #2
(ใช้ SMS Sender Name คล้ายของ ธนาคาร)

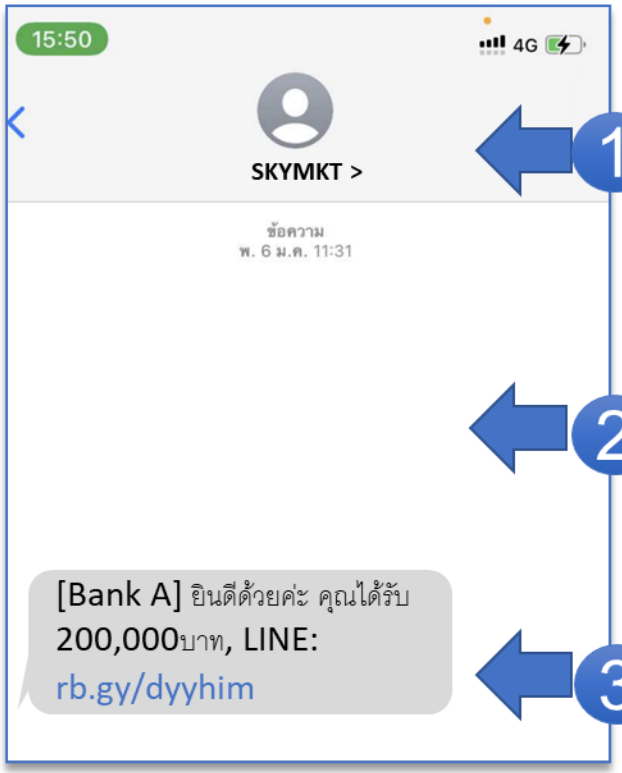
- มีผลกระทบมากเพราะเป็นรูปแบบ SMS ที่มีความยากรองลงมาสำหรับประชาชนในการสังเกตและแยกแยะ เนื่องจากมีจุดสังเกตคือ ชื่อต่าง และไม่มีข้อความจริงมาผสม

2 Observation on Suspicious Activities:

Fake SMS- Fake LINE – Fake Website – Fake Facebook App

2 Phishing

3 SMS Sender Name **Not Specific to** Bank use



1 SMS ปลอมที่คนร้ายใช้ Sender Name ไม่เจาะจงธนาคาร Bank A Bank A ≠ SKYMKT

2 ไม่มี SMS ข้อความจริงที่ส่งจากธนาคาร Bank A

3 SMS ปลอมที่คนร้าย ส่งโดยมีเนื้อหาให้เข้าใจว่า เป็นธนาคารเสนอเงินกู้

SMS Threat Pattern #3

(ใช้ SMS Sender Name ทั่วไปไม่เจาะจงธนาคาร)

- แม้คนร้ายไม่ได้ใช้ SMS Sender Name เหมือนของธนาคาร แต่ใช้เนื้อหาที่ทำให้เข้าใจว่าเป็นธนาคาร เป็นรูปแบบที่ประชาชนสามารถสังเกตความแตกต่างได้

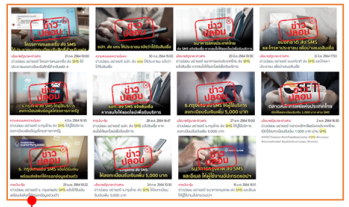
2 Observation on Suspicious Activities:

Fake SMS- Fake LINE – Fake Website – Fake Facebook App

2 Phishing

Attacker start using SMS attack to Thai bank customers

Current Incident Response Process are NOT enough to deal with new type of attacks



Sep – Oct 2020 (via Email)
Oct- Dec 2020 (via SMS)

Jan-Mar 2021 – Fake SMS impact overall Banking Sector

Apr-Oct 2021 – Fake SMS keep impact to the other areas

Executive Summary:

- Detected/Reported SMS Threat Pattern1
- SMS Registration process and White-List for Bank's SMS Sender
- Incident Response process

Zero

Attack timeline

OCBC Bank makes goodwill payouts to SMS Phishing victims

17 January 2022

MAS and ABS Announce Measures to Bolster the Security of Digital Banking

Media Releases | Published Date: 19 January 2022

Jan-Mar 2021

Feasibility analysis with BOT, AIS, NT
Jan 22, 2021: TBCERT with BOT
Feb 9, 2021: TBCERT with AIS (1)
Mar 10, 2021: TBCERT with AIS (2)
Mar 19, 2021: TBCERT with NT(CAT+TOT)

Apr 1, 2021

Agree in concept
NBTC and BOT agree in concept and assign TB-CERT, TTC-CERT including operators to work in details:
1. SMS Registration process and White-List for Bank's SMS Sender
2. Incident Response process

May-Jun 2021

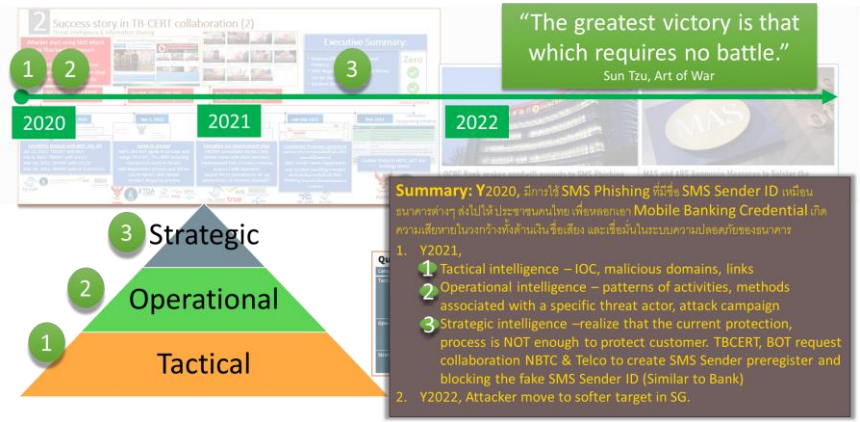
Execution our improvement plan
1. TBCERT consolidate Banks's SMS Sender name with Bank members
2. Implemented SMS incident response protocol with Operators
3. Deploy list to Operators to set up protections – Protection Started!!!

Jun-Sep 2021

Completed Proposed procedure
(SMS Sender name Registration and Incident Handling Process)

Nov 2021

Update Status to NBTC, BOT and workings teams



(สรุปวิเคราะห์แนวโน้มของ SMS Threat)

Type of SMS Threat	SMS sent from	Apr	May	Jun	Aug	Sep	Oct	Grand Total
SMS Threat Type 1	Telco C		1		3			4
	Unknown		1					1
Total SMS Threat Type 1			2		3			5
SMS Threat Type 2	Telco C		1					1
	Unknown	4	1					5
Total SMS Threat Type 2		4	2					6
SMS Threat Type 3	Telco A						1	1
	Telco B					2		2
	Telco C	1	7	1	1			10
	Unknown	2	4					6
Total SMS Threat Type 3		3	11	1	1	2	1	19
Grand Total		7	15	1	4	2	1	30

Status	Type of SMS Threat	SMS sent from	Apr	May	Jun	Aug	Sep	Oct	Grand Total
Closed	SMS Threat Type 1	Telco C		1		3			4
	SMS Threat Type 2	Telco C		1					1
	SMS Threat Type 3	Telco A						1	1
		Telco B					2		2
		Telco C	1	7	1	1			10
Closed Total			1	9	1	4	2	1	18
Open	SMS Threat Type 1	unknown		1					1
	SMS Threat Type 2	unknown	4	1					5
	SMS Threat Type 3	unknown	2	4					6
Open Total			6	6					12
Grand Total			7	15	1	4	2	1	30

Executive Summary: SMS Threat landscape in Thailand during Apr – Oct 2021

1. Total 30 incidents in 7 months have been reported and response by CERT
2. SMS Threat type 1 (Same Bank SMS Sender Name) have significant **reduced** after deploy "Bank's SMS Sender White-list". (Only 3 incidents from TRUE reported in Aug 2021)
3. Threat Actors have **changed SMS pattern to Type 3** (Not even close to Bank SMS Sender Name: **63% (19 of 30) of SMS Threat is type 3.)**

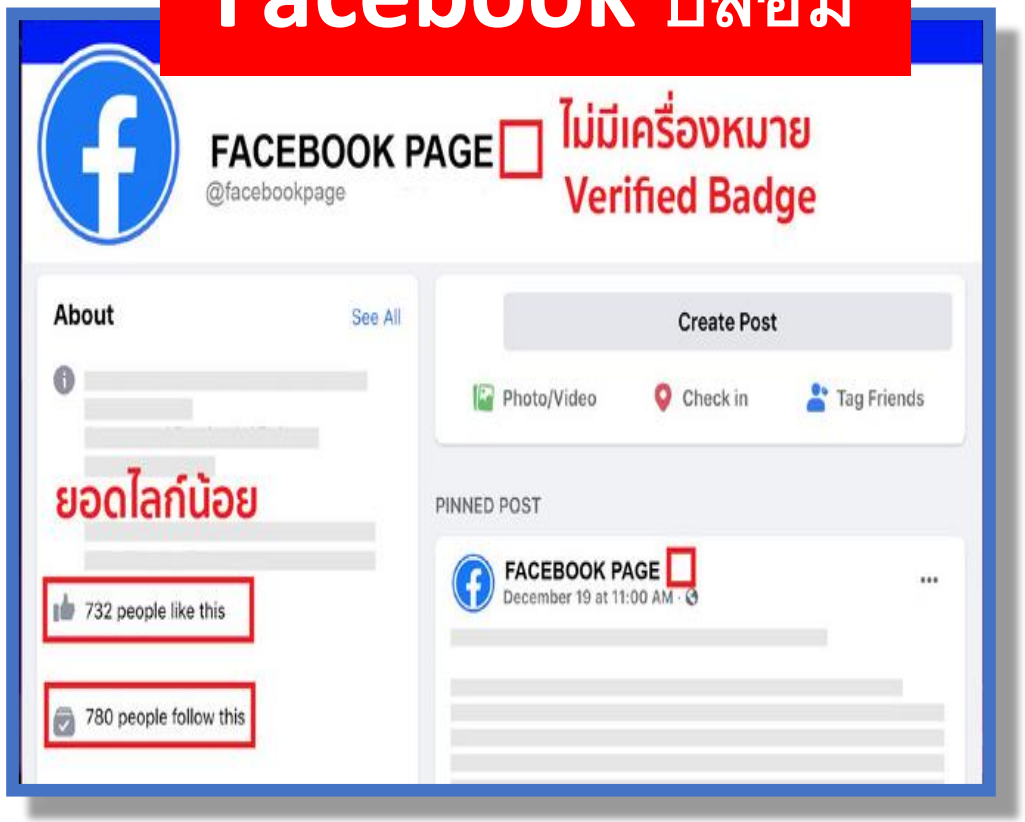
TB-CERT Thailand Banking Sector CERT

2 Observation on Suspicious Activities:

Fake SMS- Fake LINE – Fake Website – Fake Facebook App

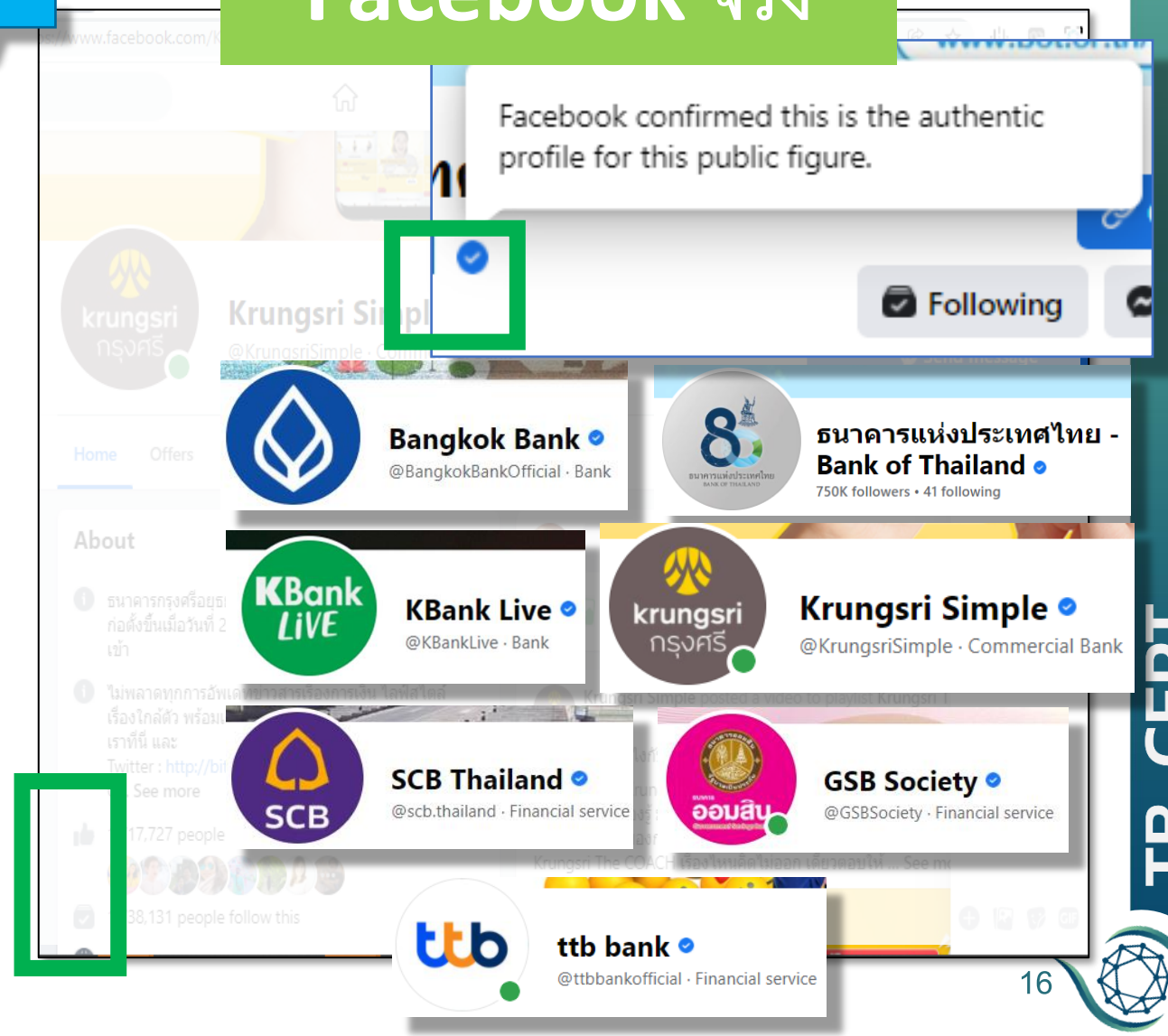
2 Phishing

Facebook ปลอม



≠

Facebook จริง



เพจ Facebook ‘ปลอม’ มักไม่มีเครื่องหมาย Verified Badge ยอดไลก์น้อย

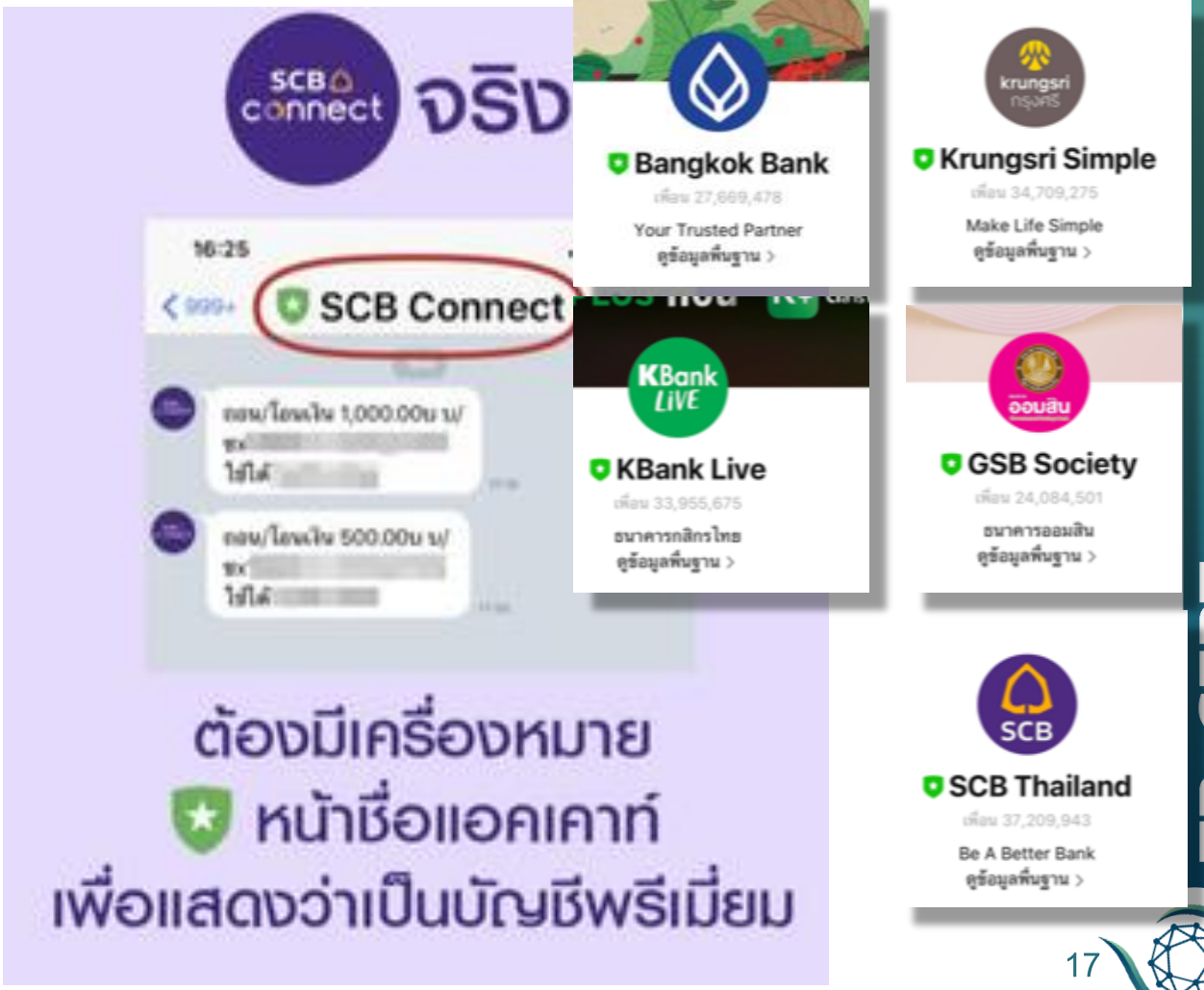
Ref: https://www.scb.co.th/th/personal-banking/stories/tips-for-you/fake-sms.html

2 Observation on Suspicious Activities:

Fake SMS- Fake LINE – Fake Website – Fake Facebook App

2 Phishing

LINE ปลอม ≠ **LINE จริง**



LINE ‘ปลอม’ ใช้โล่สีเทา

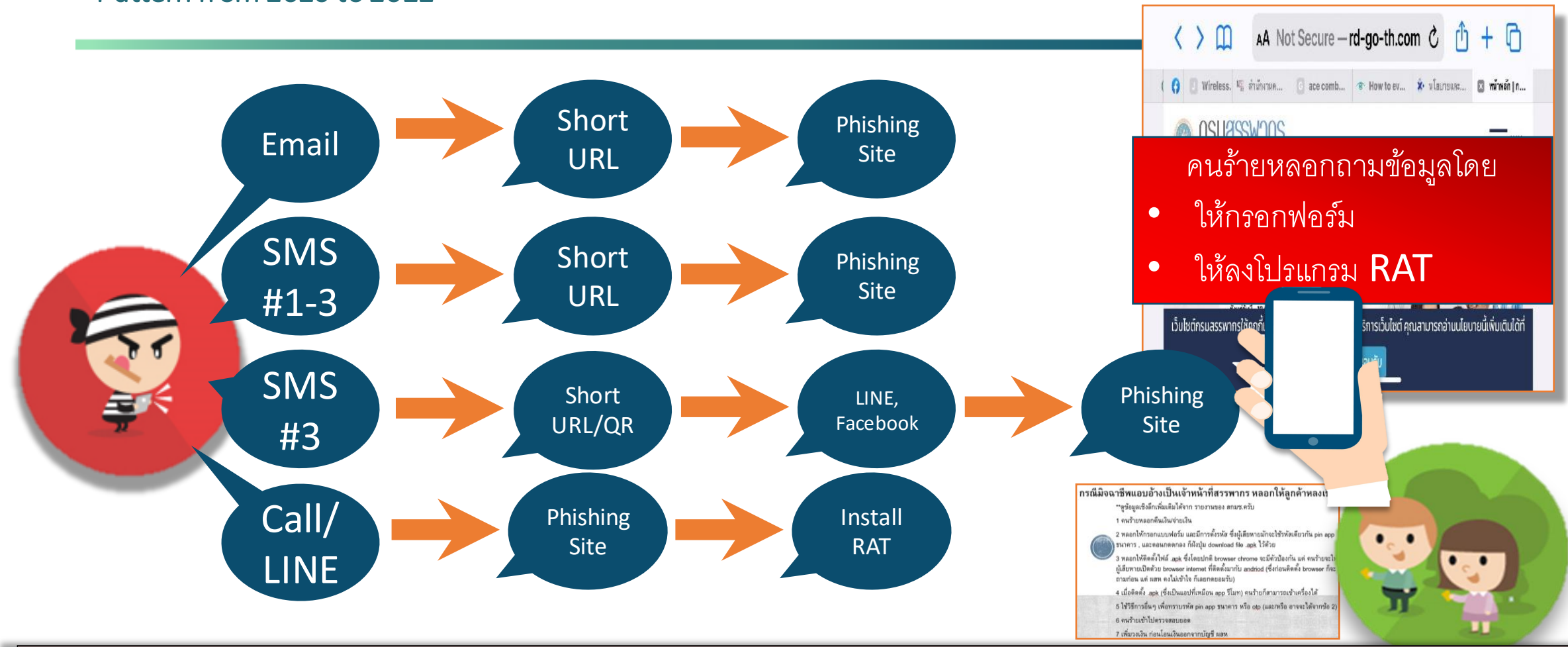
LINE จริงต้องมี ‘โล่เขียว’ นำหน้าชื่อแอ็กเคานต์

Ref: https://www.scb.co.th/th/personal-banking/stories/tips-for-you/fake-sms.html

2 How does the threat actor attack?

Pattern from 2020 to 2022

2 Phishing



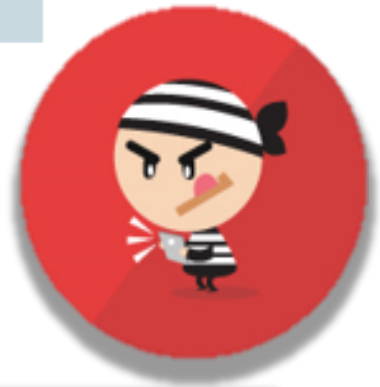
วิธีการโจมตีของแกงด์ Call Center, SMS, Line เป็นกลยุทธของการทำ Digital Fraud (กลโกงทางดิจิทัล) โดยใช้ผสมกันระหว่าง “ใช้ช่องทางไซเบอร์”+Social Engineer มาหลอกให้กรอกข้อมูล เพื่อให้โอนเงิน

2 TB-CERT Role

ความท้าทาย และ บทบาทหน้าที่ของ TB-CERT

Sample: Courses of Action Matrix

		ตรวจจับ	ป้องกัน	รบกวน	ลดประสิทธิภาพ	หลอกให้สับสน	ทำลายแล้วกู้คืน
		Goals Defined in 2006 version of JP 3-13 (Desired Effects on the Adversary)					
		Detect	Deny	Disrupt	Degrade	Deceive	Destroy
เก็บข้อมูลเป้าหมาย	Recon		Firewall ACL	Interupt spidering		False addresses	
หาเครื่องมือวิธีเจาะระบบ	Weaponization	NIDS					
ส่ง Malicious Payload มาทาง อีเมล์ USB	Delivery	Awareness	Proxy /Sender Block	Mail quarantine/AV	Queuing	Re-route suspicious emails	
เจาะระบบ	Exploitation	HIDS	Patch	DEP			
ติดตั้งมัลแวร์บนเครื่องเป้าหมาย	Installation	HIDS	Privilege restriction	AV, Sandboxing			
สร้างช่องทางรับส่งคำสั่ง	C2	HIDS	Firewall ACL	NIPS		DNS/IP redirection	
เก็บผลประโยชน์	Action on Objective	Audit log			QoS Deception	Honeypot /Deception	



การรับมือการโจมตีทางไซเบอร์ สู่ระบบสามารถทำได้หลายรูปแบบ

Controlled Environment ไม่ว่าจะทำที่ Network, Email และ Endpoint

2 TB-CERT Role

ความท้าทาย และ บทบาทหน้าที่ของ TB-CERT

Sample: Courses of Action Matrix

		ตรวจจับ	ป้องกัน	รบกวน	ลดประสิทธิภาพ	หลอกให้สับสน	ทำลายแล้วกู้คืน
		Goals Defined in 2006 version of JP 3-13 (Desired Effects on the Adversary)					
		Detect	Deny	Disrupt	Degrade	Deceive	Destroy
เก็บข้อมูลเป้าหมาย	Recon		Firewall	Interupt		False	
หาเครื่องมือวิธีเจาะระบบ	Weaponization						
ส่ง Malicious Payload มาทาง อีเมล์ USB	Delivery						
เจาะระบบ	Exploitation						
ติดตั้งมัลแวร์บนเครื่องเป้าหมาย	Installation		restriction	Sandboxing			
สร้างช่องทางรับส่งคำสั่ง	C2	HIDS	Firewall ACL	NIPS		DNS/IP redirection	
เก็บผลประโยชน์	Action on Objective	Audit log			QoS Deception	Honeypot /Deception	

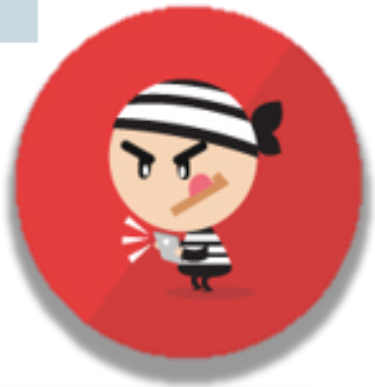
Awareness

Report it - การแจ้งเหตุจากประชาชน

ความร่วมมือ จากทุกภาคส่วนที่เกี่ยวข้อง

Digital Fraud

Digital fraud is when criminals try to use email, websites, malicious software or other methods to learn your personal details or trick you into paying them. e.g. Phishing, Malware, Identity takeover

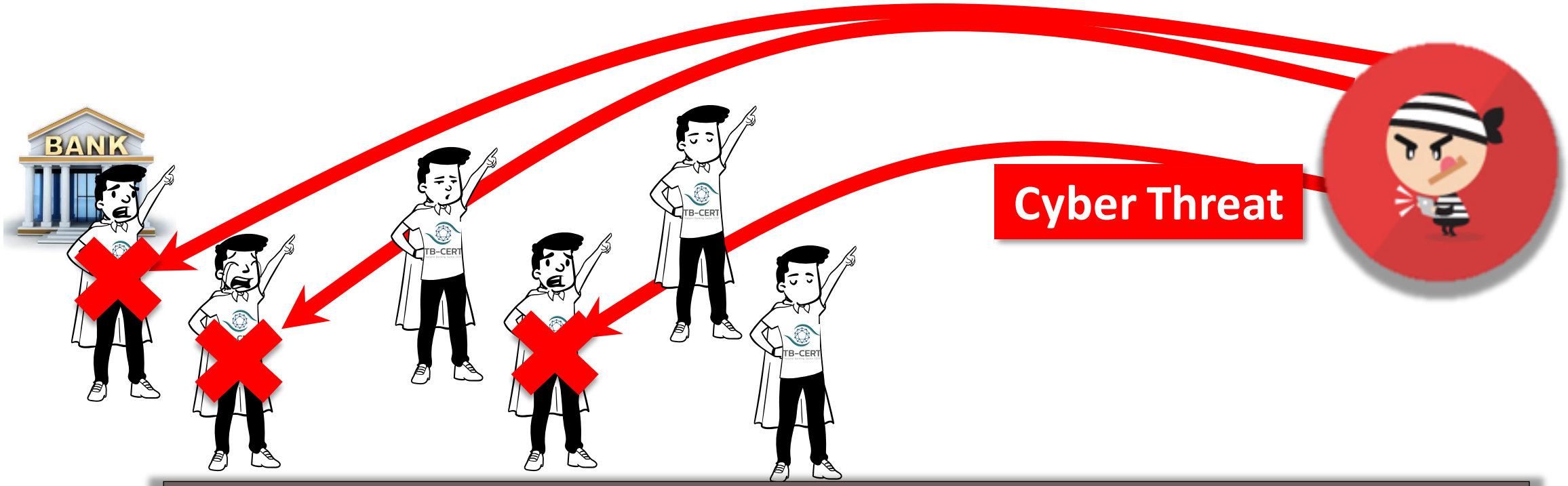


การรับมือกลโกงทางดิจิทัล

Uncontrolled Environment การเฝ้าระวังป้องกันสามารถทำได้บน ความเข้าใจ + ความร่วมมือ

2 TB-CERT Role

ความท้าทาย และ บทบาทหน้าที่ของ TB-CERT



ถ้าทุกคนไม่ Share Information เมื่อเกิด Advanced Cyber Attack
การรับมือ ป้องกันภัยในภาพรวมจะใช้เวลานานขึ้น เพราะขาดข้อมูล เพื่อป้องกัน เฝ้าระวัง
จะเกิดความเสียหายกับทั้งแต่ละธนาคาร และภาคธนาคารมากขึ้น
และพวกเราก็ไม่อาจไปสู่ TB-CERT MISSION

2 TB-CERT Role

ความท้าทาย และ บทบาทหน้าที่ของ TB-CERT

TB-CERT take key role to drive collaboration and information sharing between financial institutions, other CERTs and other international agencies both domestic and international.

3

5 Pillars Activities Lead to Mission

5 เสาหลักนำไปสู่พันธกิจในปี 2022

- Professional Development
- Standard Guideline
- Security Awareness
- Research Activities
- Services Result

- Key Take away for public

TB-CERT
Thailand Banking Sector CERT

3 5 Pillars Activities Lead to Mission

TB-CERT
Thailand Banking Sector CERT

MISSION

1	2	3	4	5
PEOPLE	STANDARDIZATION	AWARENESS	RESEARCH & DEVELOPMENT	SERVICES
พัฒนาบุคลากรด้าน Cybersecurity ของภาคธนาคาร	กำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคการธนาคาร	สร้างความตระหนักถึงภัยคุกคามด้าน Cybersecurity สำหรับภาคการธนาคาร	วิจัยและพัฒนาด้าน Cybersecurity ให้กับภาคการธนาคาร	การให้บริการแก่ธนาคารสมาชิก

3 Professional Development

1 PEOPLE

Security Talk & Workshop

Webinar and workshop provide the knowledge on many topics which are the trends of cybersecurity professional should **up to date** in the following key area

- **Cybersecurity & ESG**
- **Cyber Threat intelligence**
- **Handling ransomware**
- **Cloud security**
- **People development in cybersecurity**

Cyber Brain (E-Learning)

Cybersecurity hands on Lab with career path

Student can develop skills for their career path step by step. There are a group of skill set that students have developed are:

- **Cyber Defense Operation**
- **Management, Audit, and Legal**
- **Penetration Testing**
- **Incident Response and Digital Forensics**
- **Cloud Security**
- **Security Development**
- **Operation and Maintenance**

Cyber Combat & Cybersecurity Annual Conference

Next Chapter of Building Trust and Collaboration

As a theme of the conference the focus area is **on preparation for post covid**

There are **418** people, **7** sectors, **7** countries participating the event

42 teams join combat obtain skills in the areas of threat hunting, service attacking, protecting and maintaining available service

Banking Cyber Drill

Key Result: Understand on the Preparation and communication Especially **media handling** which is the key area to focus this year

RATTANAKOSIN -Exercise-

3 Standard Guideline

2 STANDARDIZATION

1. Update Obsolete Mobile OS

Elevate the minimum mobile OS

2. API Security Standard

Work with BOT to develop API standard

3. Phishing Handling Guideline

Develop Guideline for TB-CERT Members to be able to do first aid

3 Security Awareness

3 AWARENESS

The focused topic is “Digital fraud & Cyber crime” related to the current situation. There are 13 topics released but we found that **10 topics are about Call Center fraud**

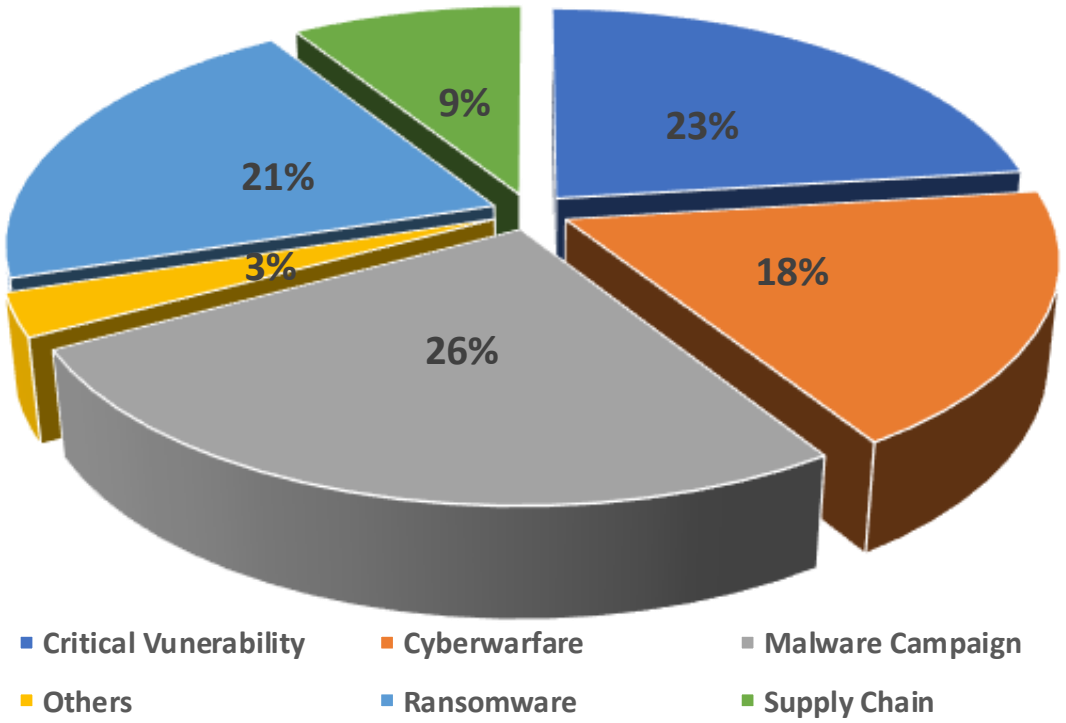
ลำดับ	เรื่อง
1	เตือนภัยแก๊งคอลเซ็นเตอร์โทรหลอกลวงให้โอนเงิน
2	คนไทยรวมพลัง รับมือแก๊งคอลเซ็นเตอร์หลอกลวง
3	6 สิ่งที่ต้องทำ เมื่อข้อมูลส่วนตัวรั่วไหลจากผู้ให้บริการ
4	Fake News รับมืออย่างไร
5	รู้ยัง มุกใหม่ ของแก๊งคอลเซ็นเตอร์
6	หลักการกลโกงครั้งใหม่ (ภาค 1) มิจฉาชีพเห็นช่องทางนี้ในการหลอกลวงได้อย่างไร มาดูกัน
7	หลักการกลโกงครั้งใหม่ (ภาค 2) ของเหล่าแก๊งคอลเซ็นเตอร์กับมือถือ Android
8	เอ๊ะ! สักนิดก่อนคิดจะสแกน หลักการคิดง่ายๆ เพื่อให้คุณเอ๊ะ! ก่อนตกเป็นเหยื่อมิจฉาชีพ
9	QR Code ปลอม หรือ Fake QR Code คืออะไร
10	เช็คง่าย ๆ ว่า Slip ที่เราได้มานั้น จริงหรือปลอม
11	รู้ทันและรับมือ Pegasus Spyware
12	รู้ไว้ปลอดภัยห่างไกลแก๊งมิจฉาชีพ-1
13	รู้ไว้ปลอดภัยห่างไกลแก๊งมิจฉาชีพ-2

3 Research Activities

4 RESEARCH & DEVELOPMENT

1. Information Categorization

Identify trends of cyber attack led to technical recommendation and awareness program development



2. Threat Intelligence Study Group

- Analyzing phishing technique capture by banking sector

- Strategic Threat Intelligence: study result motivate to rethink processes of sharing more reported phishing emails
- Operational Intelligence: improve proactive hunting program and develop detection methodology

- Detection method for unauthorized vulnerability Scan from external

Ref. ข้อมูลจาก Alert และ Technical recommendation TB-CERT

TB-CERT Thailand Banking Sector CERT

3 Services Result

5 SERVICES

ALERTS
TECHNICAL RECOMMENDATION(TR)

Alert and release technical recommendation
To members

- Critical vulnerabilities are increasing
- State-sponsor attacks has become significant monitored
- Ransomwares by several groups are still active

INCIDENT
HANDLING

Handle the incident for members and analysis the data

- The number of incidents have been increasing
- Fake Official LINE and Official SMS Sender Name change from Type 1 to Type 3 (Not Specific to Bank use)

CERT
COLLABORATION

Build relationship and collaborate with both Thai and International CERT for collecting more information and threats

TB-CERT is a sectorial CERT under Cybersecurity Act. and support for many sectors who must set up CERT

TB-CERT
Thailand Banking Sector CERT

3 Key Take away สำหรับภาคประชาชน

3 ส. เตือนใจ ระวังภัย SMS Phishing

สงสัย ชื่อผู้ส่งที่ไม่ใช่ชื่อธนาคาร หรือที่ใช้ชื่อคล้ายธนาคาร

สังเกต เนื้อหาข้อความเชิญชวนเกินจริง และมีลิงก์แนบ

ส่งข่าว ให้ธนาคารที่ถูกปลอมแปลงทราบ เพื่อยับยั้งความเสียหาย

= Protect ตัวเอง

= Protect ผู้อื่นและภาพรวมของประเทศ

TB-CERT Thailand Banking Sector CERT

TB-CERT
Thailand Banking Sector CERT