ธนาคารแห่งประเทศไทย
BANK OF THAILAND

การตรวจสอบการบริหารจัดการ Third Party

29 พฤษภาคม 2566

ภิญโญ ตรีเพชราภรณ์
ผู้อำนวยการ ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ธนาคารแห่งประเทศไทย

Third Party Trend

71% of organizations report their third-party network contains more third parties than it did three years ago.

The same percentage reports their third-party network will grow even larger in the next three years.

Gartner.

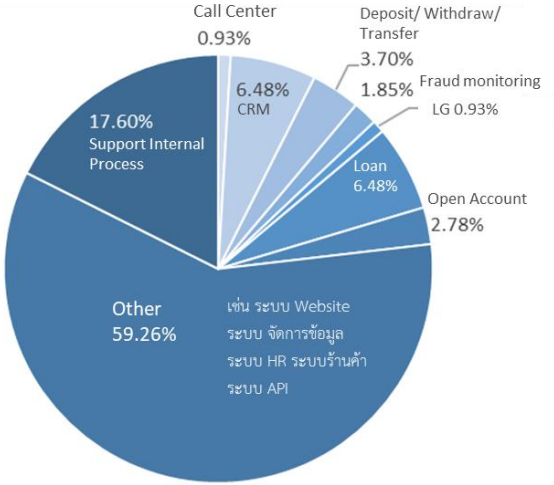
Table 1. Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

	2022	2023	2024
Cloud Application Infrastructure Services (PaaS)	111,976	138,962	170,355
Cloud Application Services (SaaS)	167,342	197,288	232,296
Cloud Business Process Services (BPaaS)	59,861	65,240	71,063
Cloud Desktop-as-a-Service (DaaS)	2,525	3,122	3,535
Cloud Management and Security Services	34,487	42,401	51,871
Cloud System Infrastructure Services (IaaS)	114,786	150,310	195,446
Total Market	**490,977**	**597,325**	**724,566**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding.
Source: Gartner (April 2023)

Cloud Service Provider

aws, Azure, Google Cloud, Alibaba Cloud, salesforce, DELL, IBM, Digital Ocean, Dropbox



ข้อมูลจาก ธปท. ณ ปี 2565

Case Study: Supply Chain Attack

Supply Chain Attack process

MEDIA AND TELECOMS FEBRUARY 15, 2021 / 8:50 AM / UPDATED A YEAR AGO

SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president

By Reuters Staff 2 MIN READ

FILE PHOTO: Microsoft's President Brad Smith speaks at the Web Summit, in Lisbon, Portugal, November 6, 2019. REUTERS/Pedro Nunes/File Photo

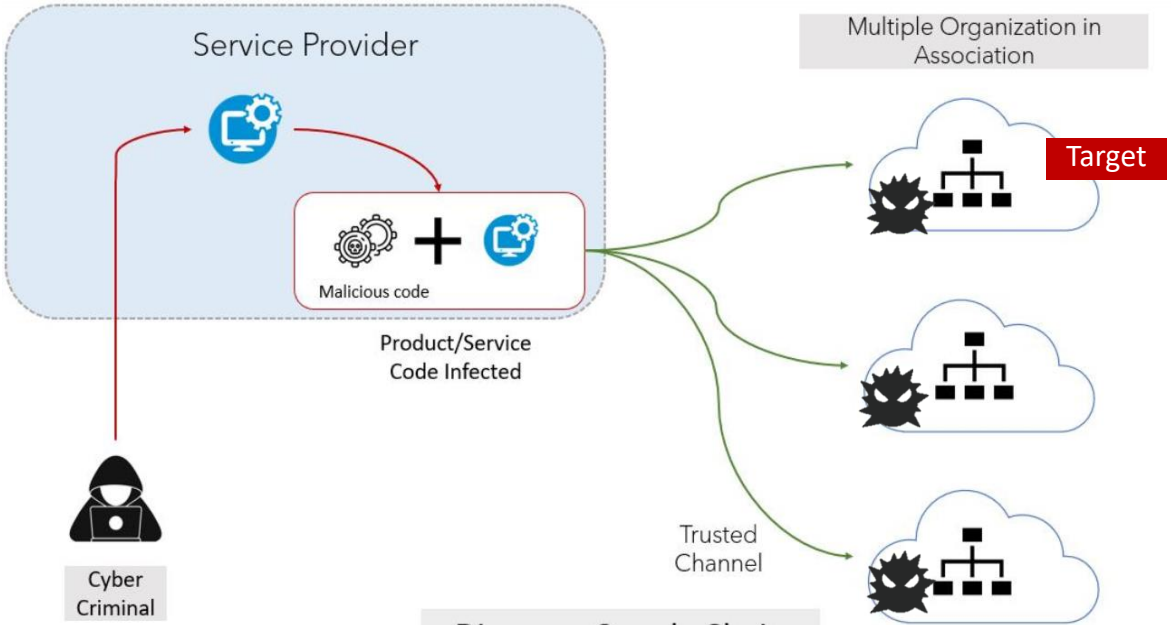
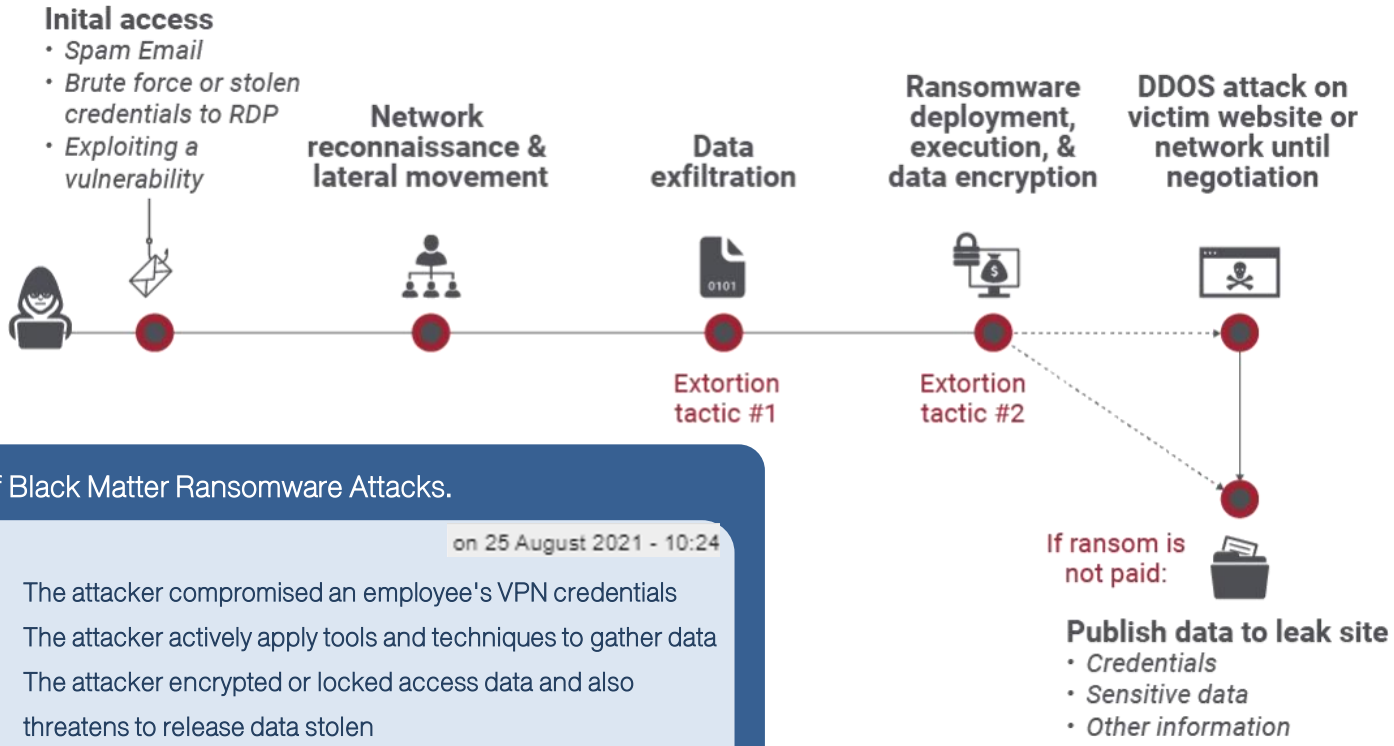


Diagram: Supply Chain Attack

ภาพจาก https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R และ https://www.blognone.com/node/120144

Case Study : Ramsomware



G-ABLE victim of Black Matter Ransomware Attacks.

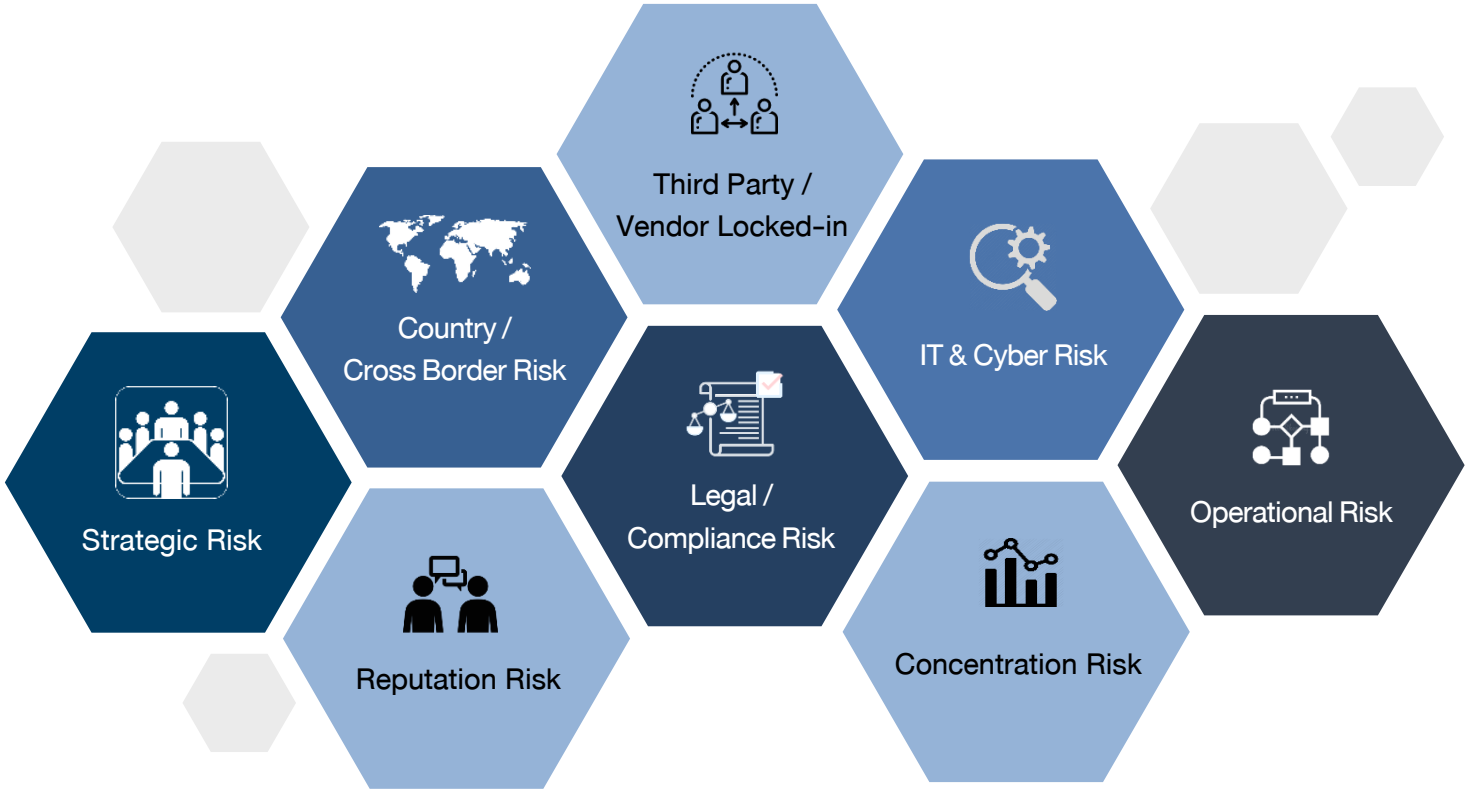
on 25 August 2021 - 10:24

- The attacker compromised an employee's VPN credentials
- The attacker actively apply tools and techniques to gather data
- The attacker encrypted or locked access data and also threatens to release data stolen

Ref : https://www.blognone.com/node/124406

Ref : Zscaler

Third Party Risk



ธนาคารแห่งประเทศไทย
BANK OF THAILAND

หลักเกณฑ์การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management)

กรอบหลักเกณฑ์การกำกับดูแลความเสี่ยงด้าน IT

Confidentiality – Integrity – Availability

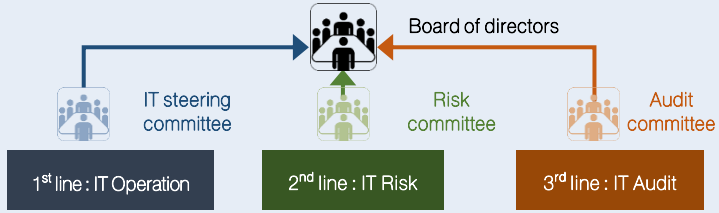
1. IT Governance

1.1 คณะกรรมการบริษัท

กำกับดูแลความเสี่ยงด้าน IT ในภาพรวม มีความรู้หรือประสบการณ์ด้าน IT อย่างเพียงพอที่จะกำกับดูแลและสนับสนุนให้องค์กรมีการบริหารความเสี่ยงด้าน IT ที่เหมาะสมและสอดคล้องกับการดำเนินธุรกิจ

1.2 โครงสร้างการกำกับดูแล

- ถ่วงดุลอย่างอิสระ ตามหลัก 3 LOD
- มีผู้รับผิดชอบด้าน IT Security



1.3 การบริหารจัดการบุคลากร

- มีความรู้ ความชำนาญเพียงพอในการปฏิบัติงาน และมีปริมาณบุคลากรเพียงพอ

1.4 นโยบายการกำกับดูแลความเสี่ยงด้าน IT

(1) IT Risk Management (2) IT Security

1.5 การสร้างความตระหนักถึงความเสี่ยงด้าน IT

- ส่งเสริมให้ตระหนักถึงความเสี่ยงด้าน IT

2. IT Security

- IT Asset Management
- Information Security
- Access Control
- Physical and Environmental Security
- Communications Security
- IT Operations Security
- System Acquisition and Development
- IT Incident and Problem mangement
- Disaster Recover Plan
- Third Party Management

3. IT Project management

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

การบริหารจัดการความเสี่ยงจากบุคคลภายนอก

3rd Party ตามนิยาม ธปท.

- **01** ผู้ให้บริการด้าน IT (IT Outsourcing)
- **02** ผู้ที่มีการเชื่อมต่อกับระบบ IT ของ สง.
- **03** ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของ สง.

ประกาศ IT Risk

- กำหนดบทบาทหน้าที่และความรับผิดชอบที่ชัดเจนระหว่าง สง. และ 3rd party รวมทั้ง**จัดทำสัญญาการเข้าตรวจสอบของ IT outsourcing ที่มีนัยสำคัญ**
- มีการกำกับดูแล ติดตาม บริหารจัดการความเสี่ยงเพียงพอกับความเสี่ยงที่เผชิญ และ Risk Tolerance
- รักษาความมั่นคงปลอดภัย (IT security และ Cyber security) ตามมาตรฐานสากล
- พร้อมรองรับเหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญ เพื่อให้บริการได้อย่างต่อเนื่อง และมีข้อมูลลูกค้าพร้อมใช้งาน
- กรณีใช้บริการ Public Cloud Computing กับระบบงานสำคัญ ต้องดำเนินการทุกข้อ NEW

แนวปฏิบัติ Third party risk management

ส่วนที่ 1 : การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Risk Governance)

- Oversight / 3 lines of defence
- Policy / Procedure
- Human Resource Mgt
- Audit
- Consumer Protection

ส่วนที่ 2 : การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (3rd Party Risk Management)

3rd Party Management Life Cycle

Risk Assessment → Due Diligence → Contract → Ongoing Monitoring → Exit/ Termination

IT security
Asset/ Access/ Data/ Network/ Change/ Config/ Capacity/ Log/ VA/ Pentest/ Back-up data/ BCP

Cyber security
Identify/ Protect/ Detect/ Response/ Recovery

การใช้บริการ Public Cloud Computing กับระบบงานสำคัญ

ต้องดำเนินการทุกข้อ กรณีใช้บริการ Public Cloud Computing กับระบบงานสำคัญ ดังต่อไปนี้

1. ประเมินระดับความเสี่ยงที่จะเกิดขึ้นจากการใช้บริการ public cloud computing
2. กำหนดปัจจัยในการคัดเลือกบุคคลภายนอกก่อนใช้บริการ
3. กรณีที่บุคคลภายนอกให้บริการในต่างประเทศ ควรจัดให้มีกระบวนการจัดเก็บข้อมูลสำรองไว้ในประเทศหรือในประเทศอื่นที่ไม่ใช่ประเทศผู้ให้บริการ
4. ต้องนำข้อมูลของ สง. หรือข้อมูลของลูกค้ากลับมาจากบุคคลภายนอก และลบหรือทำลายข้อมูลทั้งหมดที่อยู่กับบุคคลภายนอกอย่างครบถ้วน เมื่อสิ้นสุดการใช้บริการ
5. จัดให้มีกระบวนการตั้งค่าการรักษาความมั่นคงปลอดภัยด้าน IT รวมทั้งสอบทานการตั้งค่าอย่างสม่ำเสมอ
6. จัดให้มีการเข้ารหัสข้อมูลสำคัญด้วยมาตรฐานสากล
7. กำหนดให้บุคคลภายนอกระบุสถานที่ในการประมวลผล จัดเก็บข้อมูล หรือดำเนินการอื่นใดที่เกี่ยวข้องกับข้อมูลของ สง.
8. มีกระบวนการติดตามเหตุการณ์ผิดปกติและภัยคุกคามทางไซเบอร์ และมีการกำหนดแนวทางป้องกันภัยคุกคาม
9. มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

การตรวจสอบการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ขอบเขตการตรวจสอบ

ความท้าทาย

- Mobile Banking Stability
- Digital Fraud / Cyber Risk
- New Technology Risk

แนวทางการกำกับดูแลและตรวจสอบด้าน IT

Policy / Guideline

1. ประกาศ IT Risk
2. แนวปฏิบัติ

- IT Risk Management
- Third Party Management
- Mobile Banking Security
- Cyber Risk Assessment 2.0
- Data Governance
- NewTech (Blockchain, Biometric, AI, API) New
- Digital Fraud New

Ongoing Monitoring

เครื่องมือและข้อมูลที่ใช้

1. Incident Monitoring
2. IT Risk Dashboard & Data Set
3. Self-Assessment (CRAF)

Annual Examination

ขอบเขตการตรวจสอบ

1. กลยุทธ์และการเปลี่ยนแปลงสำคัญด้าน IT & Cyber
2. ความเสถียรของระบบ Mobile Banking
3. Digital Fraud / Cyber Risk
4. ความเสี่ยงจากการใช้เทคโนโลยีใหม่ (เช่น Blockchain)
5. การบริหารจัดการ Third Party

Risk Assessment → Due Diligence → Contract → Ongoing Monitoring → Exit/ Termination

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Common Gap สำคัญที่พบจากการตรวจสอบที่ผ่านมา

ข้อสังเกต

การประเมินความเสี่ยงของบุคคลภายนอก

- กรอบการประเมินความเสี่ยงบุคคลภายนอก ไม่เป็นมาตรฐาน

การบริหารจัดการการเชื่อมต่อบุคคลภายนอกผ่าน API

- กระบวนการจัดการการเชื่อมต่อบุคคลภายนอก ไม่ครอบคลุมการทดสอบ

การรายงานชุดข้อมูล Data set ไม่ตรงกับทะเบียนที่ธนาคารจัดทำ

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

การบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

สถิติภัยทางการเงิน

เส้นทางการถูกหลอกลวงของประชาชน

① หลอกลวงผ่านเครือข่ายโทรศัพท์หรือช่องทางออนไลน์

② เหยื่อหลงเชื่อโอนเงิน/แอปดูดเงิน

③ เงินถูกโอนผ่านบัญชีม้าไปยังคนร้าย

แก๊งคอลเซนเตอร์ [1/]

- แจ้งความ 20,013 คดี
- เสียหาย 3.5 พัน ลบ.

SMS หลอกลวง [2/]

- ปิดกั้น 45,743 SMS

แอปดูดเงิน

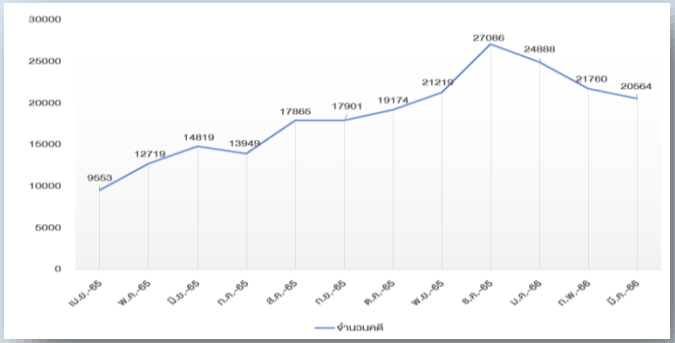
ความเสียหายลดลงจากต้นปี 30%

- ม.ค. 66 2,022 ราย / 151 ลบ.
- ก.พ. 66 1,644 ราย / 120 ลบ.
- มี.ค. 66 1,381 ราย / 107 ลบ.

บัญชีม้า [1/]

- อายัดบัญชีม้า 58,463 บัญชี
- ขออายัด 5,557.5 ลบ.
- อายัดได้ทัน 400.8 ลบ.

สถิติระบบแจ้งความออนไลน์ตำรวจ [1/]



สถิติข้อร้องเรียนผ่าน Call Center ธนาคาร (มี.ค. 66)

ประเภทเหตุการณ์	จำนวน (รายการ)
1. ถูกหลอกแอปดูดเงิน	2,150
2. ถูกหลอกให้โอนเงิน เช่น แก๊งคอลเซ็นเตอร์	3,516
3. ถูกหลอกให้ลงทุน	4,264
4. ถูกหลอกซื้อสินค้า/บริการ	2,232

1/ ข้อมูลจากสำนักงานตำรวจแห่งชาติ มี.ค. 65- มี.ค. 66
2/ ข้อมูลจากสำนักงาน กสทช. ก.ค. 65 - ธ.ค. 65

แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน

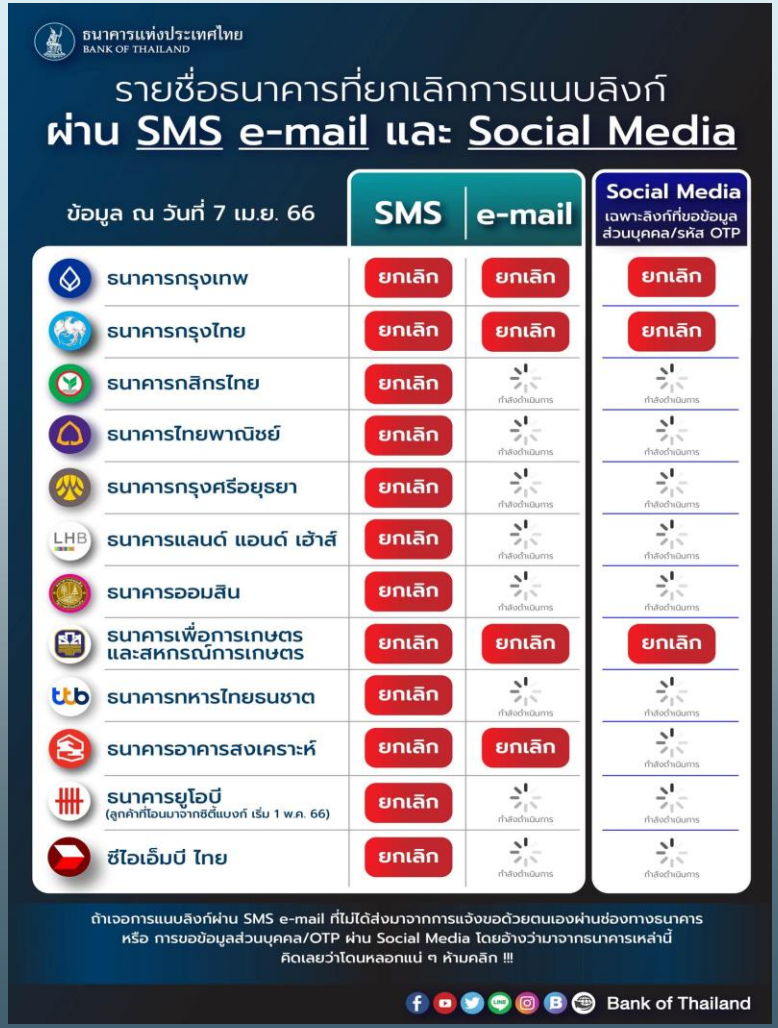
Fruad Risk Management Guideline

1. Governance
2. Management

- Protection
- Detection
- Response
- Collaboration

Appendix 1 : Fraud Risk Management for Card Payment

Appendix 2 : Fraud Risk Management for Mule Account


ธนาคารแห่งประเทศไทย
BANK OF THAILAND
รายชื่อธนาคารที่ยกเลิกการแนบลิงก์
ผ่าน SMS e-mail และ Social Media
ข้อมูล ณ วันที่ 7 เม.ย. 66
SMS
e-mail
Social Media
เฉพาะลิงก์ที่ขอข้อมูลส่วนบุคคล/รหัส OTP
ธนาคารกรุงเทพ ยกเลิก ยกเลิก ยกเลิก
ธนาคารกรุงไทย ยกเลิก ยกเลิก ยกเลิก
ธนาคารกสิกรไทย ยกเลิก กำลังดำเนินการ กำลังดำเนินการ
ธนาคารไทยพาณิชย์ ยกเลิก กำลังดำเนินการ กำลังดำเนินการ
ธนาคารกรุงศรีอยุธยา ยกเลิก กำลังดำเนินการ กำลังดำเนินการ
ธนาคารแลนด์ แอนด์ เฮ้าส์ ยกเลิก กำลังดำเนินการ กำลังดำเนินการ
ธนาคารออมสิน ยกเลิก กำลังดำเนินการ กำลังดำเนินการ
ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ยกเลิก ยกเลิก ยกเลิก
ธนาคารทหารไทยธนชาต ยกเลิก กำลังดำเนินการ กำลังดำเนินการ
ธนาคารอาคารสงเคราะห์ ยกเลิก ยกเลิก กำลังดำเนินการ
ธนาคารยูโอบี (ลูกค้าที่โอนมาจากซิตี้แบงก์ เริ่ม 1 พ.ค. 66) ยกเลิก กำลังดำเนินการ กำลังดำเนินการ
ซีไอเอ็มบี ไทย ยกเลิก กำลังดำเนินการ กำลังดำเนินการ
ถ้าเจอการแนบลิงก์ผ่าน SMS e-mail ที่ไม่ได้ส่งมาจากการแจ้งขอด้วยตนเองผ่านช่องทางธนาคาร
หรือ การขอข้อมูลส่วนบุคคล/OTP ผ่าน Social Media โดยอ้างว่ามาจากธนาคารเหล่านี้
คิดเลยว่าโดนหลอกแน่ ๆ ห้ามคลิก !!!
Bank of Thailand


ธนาคารแห่งประเทศไทย
BANK OF THAILAND
รวมเบอร์ศูนย์รับแจ้งเหตุ
ภัยทางการเงินจากมิจฉาชีพ
ข้อมูล ณ วันที่ 7 เม.ย. 66
สอบถาม และแจ้งเหตุได้ทันที ตลอด 24 ชั่วโมง
ธนาคาร กสิกรไทย 0-2888-8888 กด 001
ธนาคาร กรุงไทย 0-2111-1111 กด 108
ธนาคาร กรุงศรีอยุธยา 1572 กด 5
ธนาคาร กรุงเทพ 1333 หรือ 0-2645-5555 กด*3
ธนาคาร ไทยพาณิชย์ 0-2777-7575
ธนาคาร ทหารไทยธนชาต 1428 กด 03
ธนาคาร ออมสิน 1115 กด 6
ธนาคาร ซีไอเอ็มบี ไทย 0-2626-7777 กด 00
ธนาคาร ไทยเครดิต เพื่อรายย่อย 0-2697-5454
ธนาคาร แลนด์ แอนด์ เฮ้าส์ 0-2359-0000 กด 8
ธนาคาร อาคารสงเคราะห์ 0-2645-9000 กด 33
ธนาคาร เพื่อการเกษตรและสหกรณ์การเกษตร 0-2555-0555 กด*3
ธนาคาร ยูโอบี
ธนาคาร ซิตี้แบงก์
0-2344-9555
ธนาคาร เกียรตินาคินภัทร 0-2165-5555 กด 6
ธนาคาร ทีสโก้ 0-2633-6000 กด *7
ธนาคาร ไอซีบีซี (ไทย) 0-2629-5588 กด 4
TrueMoney ทรูมันนี่ 1240 กด 6
Bank of Thailand


ธนาคารแห่งประเทศไทย
BANK OF THAILAND
ยกระดับ
ความปลอดภัย
เฉพาะการทำรายการผ่านแอป Mobile Banking
ต้องยืนยันตัวตนขั้นต่ำด้วยการสแกนใบหน้า
การโอนเงิน
ตั้งแต่ 50,000 บาทขึ้นไป/ครั้ง *
ยอดสะสมทุก 200,000 บาท/วัน
การปรับเพิ่มวงเงิน
ตั้งแต่ 50,000 บาทขึ้นไป/ครั้ง
* จำนวนเงินขั้นต่ำของแต่ละแห่งอาจแตกต่างกัน
ประชาชนควรอัปเดตข้อมูลใบหน้าเพื่อเตรียมความพร้อมที่สาขาใดก็ได้ หรือช่องทาง
ตามที่ธนาคารกำหนดภายใน มิ.ย. 66 เพื่อให้สามารถทำธุรกรรมได้ ... ไม่สะดุด
ข้อมูล ณ วันที่
28 เม.ย. 66
ช่องทางสำหรับ
การ update ข้อมูล
สาขา
ตู้ ATM
รายการที่เริ่มใช้
การสแกนหน้าแล้ว
โอนเงิน
เพิ่มวงเงิน
ธนาคารกรุงไทย
ทั้งแอป Krungthai และเป้าตัง
ธนาคารกสิกรไทย
ธนาคารกรุงศรีอยุธยา
ธนาคารแลนด์ แอนด์ เฮ้าส์
ธนาคารไทยพาณิชย์
ธนาคารกรุงเทพ
ซีไอเอ็มบี ไทย
ธกส.
เฉพาะแอป A-Mobile Plus
ธนาคารออมสิน
ทรูมันนี่ (TrueMoney)
กำลังดำเนินการ
Bank of Thailand

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

3 เรื่องต้องรู้

เมื่อ พรก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีผลบังคับใช้

1. เมื่อถูกหลอกหรือมีเหตุสงสัยว่าตกเป็นเหยื่อ* ให้รีบดำเนินการดังนี้

*เช่น กรณีหลอกลวงคอลเซ็นเตอร์ และแอปดูดเงิน เป็นต้น

(1) แจ้งธนาคารทันที ผ่านเบอร์ศูนย์รับแจ้งเหตุ hotline หรือที่สาขาเพื่อให้ระงับธุรกรรมชั่วคราว ช่วยตัดตอนเส้นทางการเงิน

(2) แจ้งตำรวจอย่างรวดเร็ว ผ่านออนไลน์หรือท้องที่ใดก็ได้ **เพราะธนาคารระงับธุรกรรมชั่วคราวได้ไม่เกิน 72 ชั่วโมง** โดยตำรวจจะแจ้งให้ธนาคารทราบเพื่อระงับธุรกรรมต่อ

2. โทษบัญชีม้าและซิมม้า...หนักขึ้น แค่โฆษณาซื้อ/ขาย...ก็ผิดแล้ว

เปิดหรือยอมให้คนอื่น ใช้บัญชีเงินฝาก บัตร หรือ e-Wallet เป็นบัญชีม้า

หรือ

ให้คนอื่นใช้/ยืมใช้ซิมโทรศัพท์ เพื่อนำไปใช้ในการทุจริต หรือทำผิดกฎหมาย

ต้องรับโทษ...
- จำคุกไม่เกิน 3 ปี
- หรือ
- ปรับไม่เกิน 300,000 บาท
- หรือ
- ทั้งจำทั้งปรับ

โฆษณาเพื่อให้มีการซื้อ/ขายบัญชีม้า หรือซิมโทรศัพท์

ต้องรับโทษ...
- จำคุก 2-5 ปี
- หรือ
- ปรับตั้งแต่ 200,000-500,000 บาท
- หรือ
- ทั้งจำทั้งปรับ

3. หน่วยงานที่เกี่ยวข้องสามารถแลกเปลี่ยนข้อมูลระหว่างกัน

หน่วยงานสามารถแลกเปลี่ยนข้อมูล เพื่อใช้ในการสืบสวนสอบสวนและป้องกัน		ผลที่คาด (Outcome)
ธนาคาร	แชร์ข้อมูลทุจริตระหว่างกัน โดยไม่ติด PDPA	ลดบัญชีม้า ป้องกัน/จำกัดความเสียหาย
ตำรวจ DSI ปปง. และหน่วยงานที่ได้รับอนุญาต	ตำรวจ DSI ปปง. ได้รับแจ้งข้อมูลทุจริตที่แลกเปลี่ยนกันได้	ช่วยเหลือได้รวดเร็ว ติดตามลงโทษผู้กระทำผิด
ผู้ให้บริการเครือข่ายโทรศัพท์/โทรคมนาคม	เปิดเผย/แลกเปลี่ยนข้อมูลระหว่างกันหรือกับหน่วยงานที่เกี่ยวข้อง (ตำรวจ DSI ปปง.)	• ลดจำนวนซิมม้า • ป้องกันมิจฉาชีพเข้าถึงประชาชน