ภัยแก๊งคอลเซ็นเตอร์ จากอาชญากรรมทางเศรษฐกิจสู่อาชญากรรมทางเทคโนโลยี
The Threat of Call Center Gangs Evolving from Economic Crime to Cybercrime

สรวิศ บุญมี[1]
Sorawit Boonmee[1]
[1]คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยอีสเทิร์นเอเชีย
[1]School of Information Technology, Eastern Asia University
Received: January 31, 2023
Revised: March 22, 2023
Accepted: March 29, 2023

บทคัดย่อ

แก๊งคอลเซ็นเตอร์ เป็นอาชญากรรมทางเศรษฐกิจที่แสวงประโยชน์จากความตื่นกลัว ความโลภ ซึ่งเกิดขึ้นมานานระยะหนึ่งแล้ว แต่ได้ขยายวงอย่างกว้างขวางในประเทศไทย ตั้งแต่ พ.ศ. 2550 ในปัจจุบันเมื่อเทคโนโลยีสมาร์ทโฟนและโมบายแบงก์กิ้งได้รับความนิยมมากขึ้น แก๊งคอลเซ็นเตอร์จึงพัฒนารูปแบบการหลอกลวงเหยื่อด้วยเทคโนโลยีที่ทันสมัยขึ้นจนกลายเป็นอาชญากรรมทางเทคโนโลยี บทความนี้จะอธิบายถึงความเป็นมาของแก๊งคอลเซ็นเตอร์ กลวิธีทางวิศวกรรมสังคมในการหลอกลวงเหยื่อ การหลอกลวงรูปแบบใหม่ของแก๊งคอลเซ็นเตอร์ตามแนวคิดของ Cyber Kill Chain ปัญหาของบัญชีม้า มาตรการป้องกันโดย กสทช. ร่างพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี การทำงานของแอปพลิเคชันปลอม และการป้องกันและรับมือ เพื่อให้เข้าใจกลวิธีหลอกลวงรูปแบบใหม่ และสร้างความตระหนักรู้เพื่อลดความเสี่ยงที่จะตกเป็นเหยื่อโดนหลอกลวงจนต้องสูญเสียทรัพย์สิน

คำสำคัญ: แก๊งคอลเซ็นเตอร์ อาชญากรรมทางเทคโนโลยี ความมั่นคงปลอดภัยสารสนเทศ

Abstract

Call center gangs are economic crimes that take advantage of fear and greed. They have been going on for a long time, but they have expanded widely in Thailand since 2007. When smartphone technology and mobile banking became more popular, they developed a form of deceiving victims with modern technology that became a cyber-technological crime. This article explains the history of call center gangs, social engineering tactics to deceive victims, a new scam of call center gangs based on the concept of cyber kill chain, the problem of mule accounts, preventive measures by the NBTC Draft Royal Decree on Measures to Prevent and Suppress Cyber Crimes, the operation of fake applications, prevention, and coping to understand new deception tactics and raise awareness to reduce the risk of falling victim to being deceived until losing your property.

Keywords: call center gangs, cybercrime, information security

บทนำ

ภัยการหลอกลวงทางโทรศัพท์ หรือแก๊งคอลเซ็นเตอร์ (Call Center) เป็นอาชญากรรมทางเศรษฐกิจระหว่างประเทศรูปแบบหนึ่งในยุคดิจิทัล ซึ่งนอกจากจะก่อให้เกิดความเสียหายทางเศรษฐกิจต่อเหยื่อจำนวนมากแล้ว ยังก่อให้เกิดความเสียหายต่อเศรษฐกิจในภาพรวมระดับประเทศอีกด้วย ภัยคอลเซ็นเตอร์ถือได้ว่าเป็นอาชญากรรมทางเศรษฐกิจข้ามชาติที่เป็นภัยร้ายแรง และมีการปรับปรุงวิธีการหลอกลวงเหยื่อให้เข้ากับยุคปัจจุบันซึ่งเป็นยุคข้อมูลข่าวสารที่การติดต่อในรูปแบบดิจิทัลมีบทบาทมากขึ้นเรื่อย ๆ จนกลายเป็นอาชญากรรมทางเทคโนโลยี ตามรายงานจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศเปิดเผยว่า ประเทศไทยพบการใช้โทรศัพท์เพื่อหลอกลวงมากกว่า 6.4 ล้านครั้ง โดยเพิ่มขึ้นกว่าร้อยละ 270 จากปี 2563 และในไทยพบการส่งข้อความขนาดสั้นหรือเอสเอ็มเอส (SMS) หลอกลวงเพิ่มขึ้นถึงร้อยละ 57 และในปี 2564 ที่ผ่านมา มีผู้เสียหายเข้าแจ้งความกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กว่า 1,600 คน มูลค่าความเสียหายสูงกว่า 1,000 ล้านบาท นับแต่เดือนมกราคมถึง 15 กุมภาพันธ์ 2565 เข้าแจ้งความแล้ว 129 คดี สถิติทางคดีดังกล่าวแสดงให้เห็นถึงแก๊งคอลเซ็นเตอร์ยังคงระบาดอย่างต่อเนื่อง สำหรับมูลเหตุจูงใจการกระทำผิด คือ รายได้ที่ได้รับจากการก่อเหตุมีมูลค่าเป็นจำนวนมหาศาล ในขณะที่บทลงโทษตามกฎหมายไม่มีความรุนแรง (The Secretariat of the House of Representatives, 2022)

ที่มาของแก๊งคอลเซ็นเตอร์

แก๊งคอลเซ็นเตอร์ เป็นอาชญากรรมทางเศรษฐกิจรูปแบบหนึ่งที่ฉ้อโกงประชาชนโดยแสวงประโยชน์จากความตื่นกลัว ความโลภ และการสร้างความสัมพันธ์อันดีกับเหยื่อหรือผู้เสียหาย ซึ่งเกิดขึ้นมานานพอสมควรแล้ว แต่ระบาดอย่างกว้างขวางในประเทศไทย ตั้งแต่ พ.ศ. 2550 โดยเหยื่อมักจะเป็นผู้สูงวัย ข้าราชการเกษียณที่มีเงินเก็บสะสม หรือผู้หญิงที่มักมีความตื่นกลัวกับการหลอกลวงหรือฉ้อฉลของคนร้าย (Thailand Science Research and Innovation, 2021)

คำว่าแก๊งคอลเซ็นเตอร์ หรือที่เรียกอีกอย่างว่าคดีคอลเซ็นเตอร์นั้น มิได้เกิดขึ้นครั้งแรกในประเทศไทยแต่มีที่มาจากประเทศไต้หวัน โดยในตอนแรกไม่ได้ใช้คำว่าคอลเซ็นเตอร์ แต่ใช้คำว่า เอทีเอ็มเกมส์ (ATM Game)

เป็นการสร้างกลโกงต่อประชาชนโดยการแอบอ้างแสดงตนเป็นผู้อื่น แล้วหลอกลวงให้เหยื่อเชื่อทางโทรศัพท์เพื่อให้เหยื่อไปที่ตู้ ATM และให้ทำการโอนเงินแก่คนร้าย โดยมีรูปแบบที่ใช้ในการหลอกลวงผู้เสียหายหรือเหยื่อโดยใช้กลวิธีทางวิศวกรรมสังคม เช่น หลอกลวงด้วยความโลภ หรือหลอกลวงด้วยความกลัว (Thailand Science Research and Innovation, 2021)

กลวิธีทางวิศวกรรมสังคม (social engineering influence tactics)

ในด้านความมั่นคงปลอดภัยสารสนเทศ การโจมตีเหยื่อด้วยวิธีทางวิศวกรรมสังคม คือ ปฏิบัติการจิตวิทยา ซึ่งเป็นวิธีที่ง่ายที่สุดในการโจมตี เนื่องจากไม่จำเป็นต้องใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์มากนัก และส่วนใหญ่จะใช้ได้ผลดี การโจมตีแบบวิศวกรรมสังคมจะเกี่ยวกับการหลอกให้เหยื่อหลงกลเพื่อให้ผลประโยชน์ที่ผู้โจมตีต้องการ เช่น การหลอกถามรหัสผ่าน การหลอกให้ส่งข้อมูลที่สำคัญให้ ซึ่งการโจมตีประเภทนี้ไม่จำต้องใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์หรือการเจาะระบบเลย วิศวกรรมสังคมเป็นจุดอ่อนที่ป้องกันยากเพราะเกี่ยวข้องกับคน และมีกลวิธีในการโน้มน้าวเหยื่อหลายรูปแบบ ดังนี้ (Social-Engineer, 2022)

● **Authority** ในทางวิศวกรรมสังคม ผู้โจมตีอาจวางตัวเป็นผู้มีอำนาจเพื่อเพิ่มโอกาสที่เหยื่อจะยอมทำตาม เช่น อ้างว่าเป็นเจ้าหน้าที่ตำรวจ หรือเจ้าหน้าที่สรรพากร

● **Intimidation** ผู้โจมตี แจ้งหรือบอกเป็นนัยว่าจะมีผลในทางลบหากไม่ดำเนินการบางอย่าง ตามด้วยการข่มขู่เช่น อ้างว่าเหยื่อมีส่วนร่วมในการทำผิดกฎหมาย บัญชีถูกยกเลิก

● **Scarcity** ความขาดแคลนที่เหยื่อรับรู้จะทำให้เหยื่อเกิดความต้องการ เช่น อ้างว่ามีจำนวนจำกัด ใกล้หมดแล้ว

● **Urgency** เชื่อมโยงกับความขาดแคลน ผู้โจมตีใช้ความเร่งด่วนเป็นหลักการทางจิตวิทยาเรื่องเวลาของวิศวกรรมสังคม ตัวอย่างเช่น การพูดว่าข้อเสนอพิเศษมีให้ภายในเวลาจำกัดเท่านั้น กระตุ้นให้เหยื่อรีบตัดสินใจโดยไม่ไตร่ตรองให้ดี

● **Familiarity หรือ Liking** สร้างความคุ้นเคยให้เหยื่อรู้สึกไว้ใจ เช่น หลอกว่าจะช่วยเหลือ ตรวจสอบแก้ปัญหาให้

การหลอกลวงรูปแบบใหม่ของแก๊งคอลเซ็นเตอร์ตามแนวคิดของ Cyber Kill Chain

แก๊งคอลเซ็นเตอร์ได้พัฒนารูปแบบในการหลอกลวงเหยื่อตามเทคโนโลยีที่เปลี่ยนไป เมื่อสมาร์ทโฟนมีราคาถูกลงทำให้เป็นที่นิยมใช้กันมากขึ้น อำนวยความสะดวกให้สามารถทำธุรกรรมอย่างการโอนเงินผ่านระบบโมบายแบงก์กิ้งได้อย่างรวดเร็วไม่ต้องไปทำรายการที่เครื่องเอทีเอ็ม แก๊งคอลเซ็นเตอร์จึงได้พัฒนามาเป็นการโจมตีระบบโมบายแบงก์กิ้งของเหยื่อแทนซึ่งสอดคล้องกับแนวคิดของ Cyber Kill Chain ที่ถูกคิดค้นโดย Lockheed Martin เพื่อใช้อธิบายขั้นตอนการโจมตีไซเบอร์ ดังนี้ (Lockheed Martin, 2023)

1. **Reconnaissance** การลาดตระเวน คือ คนร้ายจะเริ่มต้นเก็บรวบรวมข้อมูลของเป้าหมายก่อนเริ่มการโจมตี โดยอาจค้นหาข้อมูลจากโลกอินเทอร์เน็ต หรือเครือข่ายสังคมออนไลน์ โดยจะเห็นได้ว่า ในหลายกรณีคนร้ายสามารถระบุข้อมูลเบื้องต้นของตัวเหยื่อได้ถูกต้องจนเหยื่อหลงเชื่อ

2. **Weaponization** เตรียมอาวุธสำหรับโจมตี เช่น สร้างเว็บไซต์ปลอมที่มีหน้าตาเหมือนเว็บจริงที่จะใช้แอบอ้างหลอกเหยื่อ สร้างแอปพลิเคชันปลอมเพื่อนำไปติดตั้งในสมาร์ทโฟนของเหยื่อเพื่อใช้เป็นเครื่องมือในการโจมตีระบบโมบายแบงก์กิ้ง

3. **Delivery** ติดต่อเหยื่อเพื่อส่งเว็บไซต์และแอปพลิเคชันปลอม ผ่านทางช่องทางสื่อสารต่าง ๆ ให้

4. **Exploitation** ใช้กลวิธีทางวิศวกรรมสังคมในการโน้มน้าวเหยื่อให้หลงเชื่อเรื่องหลอกลวงของคนร้าย

5. **Installation** เมื่อเหยื่อหลงเชื่อก็จะติดตั้งแอปพลิเคชันปลอมลงในเครื่องและเรียกใช้งาน

6. **Command & Control** แอปพลิเคชันปลอมก็จะสร้างช่องทางในการรับส่งคำสั่งจากคนร้ายผ่านอินเทอร์เน็ต เพื่อให้สามารถจัดการและควบคุมเครื่องของเหยื่อจากระยะไกลได้ตามความต้องการ

7. **Action on Objectives** จากนั้นคนร้ายจะควบคุมระบบโมบายแบงก์กิ้งของเหยื่อเพื่อโอนเงินออกไปยังบัญชีม้าต่อไป

เนื่องจาก Cyber Kill Chain เป็นขั้นตอนที่ดำเนินการอย่างต่อเนื่องเป็นลูกโซ่ นั่นหมายความว่า ถ้าสามารถทำให้ลูกโซ่ขาดไปได้ก่อนจะถึงขั้นสุดท้ายก็จะทำให้การโจมตีไม่เป็นผลสำเร็จทันที ซึ่งส่วนใหญ่แล้ว ควรจะใช้หลากหลายวิธีเข้าช่วยเพื่อพยายามตัดห่วงโซ่ทิ้งให้ได้ทุกจุด (defense in depth) (TechTalkThai, 2016)

บัญชีม้าและคริปโทเคอร์เรนซี

เมื่อคนร้ายควบคุมระบบโมบายแบงก์กิ้งของเหยื่อได้แล้วก็ทำการโอนเงินของเหยื่อไปยังบัญชีธนาคารที่เปิดเตรียมไว้ล่วงหน้าหรือที่เรียกว่าบัญชีม้า บัญชีม้า คือ บัญชีเงินฝากธนาคารของบุคคลอื่นซึ่งถูกคนร้ายนำมาใช้เป็นช่องทางในการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำความผิด เพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวได้ บัญชีม้าสามารถทำได้หลายวิธี ทั้งจากการโจรกรรมข้อมูลส่วนบุคคลเพื่อนำไปใช้เปิดบัญชีในชื่อของคนนั้น ๆ หรือจ้างให้บุคคลอื่นเปิดบัญชี หรือรับซื้อบัญชีเงินฝากธนาคารของบุคคลทั่วไปเพื่อนำไปใช้กระทำความผิด ซึ่งพบได้อย่างแพร่หลายในเครือข่ายสังคมออนไลน์ที่มีการขายบัญชีเงินฝากธนาคารอย่างเปิดเผย โดยบัญชีม้าเหล่านี้จะมาพร้อมกับสำเนาบัตรประจำตัวประชาชนและซิมการ์ดโทรศัพท์ที่เจ้าของบัญชีเปิดใช้งานด้วย เพื่อให้คนร้ายที่ซื้อบัญชีม้าไปแล้วจะสามารถนำข้อมูลส่วนบุคคลของเจ้าของบัญชีไปผูกกับ mobile banking เพื่อใช้โอนส่งต่อเงินที่ได้จากเหยื่อให้เร็วที่สุด (Bank of Thailand, 2022)

คนร้ายมักจะมีบัญชีม้าหลาย ๆ บัญชี เพื่อใช้โอนส่งเงินต่อกันไปเป็นทอด ๆ เพื่อป้องกันการถูกตำรวจตรวจสอบหรืออายัดเงินในบัญชีม้า เช่น เมื่อผู้เสียหายถูกหลอกให้โอนเงินเข้าบัญชีม้าที่ 1 แล้ว คนร้ายก็จะโอนเงินออกจากบัญชีดังกล่าวต่อไปยังบัญชีม้าที่ 2 จากบัญชีม้าที่ 2 โอนต่อไปยังบัญชีม้าที่ 3 และที่ 4 ซึ่งบางรายมีจำนวนบัญชีม้าถึง 5 บัญชี ท้ายที่สุดคนร้ายก็จะถอนเงินของเหยื่อหรือผู้เสียหายออกไป ซึ่งการโอนเงินจากบัญชีม้าหลายทอดเช่นนี้ตั้งแต่ต้นจนจบใช้เวลาเพียงไม่กี่นาทีเท่านั้น และหากถูกเจ้าหน้าที่ตำรวจอายัดบัญชีม้าบัญชีใด ก็จะเปลี่ยนไปใช้บัญชีม้าอื่น ๆ ที่ยังสามารถใช้งานแทนได้ ขณะที่ในทางการสืบสวนของเจ้าหน้าที่ จะมีขั้นตอนในการขอข้อมูลบัญชีเงินฝากจากสถาบันการเงินซึ่งมีระยะเวลาในการดำเนินการทำให้ที่ผ่านมายังไม่สามารถระงับยับยั้งการถอนเงินออกจากบัญชีเงินฝากธนาคารได้อย่างทันท่วงที เงินที่คนร้ายได้จากการกระทำความผิดจึงถูกโยกย้ายออกจากบัญชีม้าไปอย่างรวดเร็ว และต้องใช้เวลาในการติดตามเงินคืนให้กับผู้เสียหาย (Bank of Thailand, 2022)

เนื่องจากในปัจจุบันกฎหมายยังไม่ได้กำหนดให้การเปิดบัญชีธนาคารที่นำไปใช้เป็นบัญชีม้าเป็นความผิด โดยเฉพาะในทางปฏิบัติ เจ้าหน้าที่ตำรวจจะดำเนินคดีกับผู้เปิดบัญชีม้าในความผิดฐานเป็นตัวการหรือผู้สนับสนุนในการกระทำความผิดอื่น ดังนั้นเมื่อมิจฉาชีพใช้บัญชีม้าในการกระทำผิดฐานฉ้อโกง เจ้าของบัญชีเงินฝากที่เป็นผู้เปิดบัญชีม้าอาจต้องถูกดำเนินคดีฐานเป็นตัวการหรือผู้สนับสนุนการทำความผิดฐานฉ้อโกงด้วยเช่นกัน ดังคำพิพากษาศาลฎีกาที่ 2120/2563 ตัดสินลงโทษประชาชนที่รับจ้างเปิดบัญชี แม้จะอ้างในชั้นสอบสวนและศาลว่า ไม่ได้รู้เห็นการกระทำความผิด แต่ศาลเห็นว่า การเปิดบัญชีธนาคารนั้นเป็นเรื่องส่วนบุคคล ไม่ควรนำบัญชี บัตร ATM หรือรหัสมอบให้กับผู้อื่น การได้รับเงินค่าจ้างเพื่อมาเปิดนั้น ย่อมเล็งเห็นผลว่าผู้รับซื้อจะนำไปใช้ในทางผิดกฎหมาย จะอ้างว่าถูกหลอกไม่ได้ การกระทำจึงเป็นการให้ความช่วยเหลือหรือให้ความสะดวกในการที่ผู้อื่นกระทำความผิดฐานฉ้อโกง และเป็นผู้สนับสนุนการใช้บัตรอิเล็กทรอนิกส์สำหรับเบิกถอนเงินสดของผู้อื่นโดยมิชอบ จึงมีความผิดฐานเป็นผู้สนับสนุนการกระทำความผิด โดยต้องโทษ 2 ใน 3 ของโทษทั้งหมด (Nitilaw and Win Office, 2022)

นอกจากนี้ การส่งเงินให้กับเจ้าของหรือระดับหัวหน้าแก๊งในต่างประเทศ คนร้ายอาจใช้บัญชีคริปโทเคอร์เรนซีซึ่งไม่ได้เปิดใช้บริการผ่านศูนย์ซื้อขายสินทรัพย์ดิจิทัลที่ได้รับอนุญาตในประเทศไทย โดยคนร้ายอาจจะทำการโอนคริปโทเคอร์เรนซีแบบ Peer-to-Peer--P2P หรือผ่านศูนย์ซื้อขายสินทรัพย์ดิจิทัลที่อยู่ในต่างประเทศ ทำให้เกิดความล่าช้าหรืออาจไม่ได้รับความร่วมมือในการประสานงานขอข้อมูลเพื่อใช้ประโยชน์ในการสืบสวนสอบสวน รวมถึง มีความยุ่งยากซับซ้อนในขั้นตอนการสืบสวนเพื่อจับกุมผู้กระทำความผิด (Bank of Thailand, 2022)

มาตรการป้องกันโดย กสทช.

ในการติดต่อเหยื่อ กลุ่มที่ทำหน้าที่คอลเซ็นเตอร์อาจจะโทรหาเหยื่อจากต่างประเทศโดยใช้เทคโนโลยี VoIP --Voice over IP ซึ่งสามารถปลอมแปลงเลขหมายโทรศัพท์ต้นทางให้เป็นเลขหมายคอลเซ็นเตอร์ในประเทศได้ หรือใช้ซิมโทรศัพท์แบบเติมเงินเพื่อปกปิดต้นทางให้ตำรวจตามจับกุมได้ยาก ซึ่งคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือ กสทช. ได้มีมาตรการป้องกันต่าง ๆ อาทิ (Office of The National Broadcasting and Telecommunications Commission, 2023)

- ระงับการโทรเข้าจากต่างประเทศมายังเลขหมายปลายทางของประเทศไทย ซึ่งมีรูปแบบของเลขหมายที่โทรเข้าผิดปกติ เช่น ปลอมเป็นเลขหมายในประเทศโดยเฉพาะเลขหมายสี่หลักแบบคอลเซ็นเตอร์ทั่วไป
- ระงับการโทรเข้าจากต่างประเทศมายังเลขหมายปลายทางของประเทศไทย ซึ่งมีรูปแบบของเลขหมายโทรเข้าเป็นรหัสโทรศัพท์ประจำประเทศ (country code) ที่ยังไม่ได้กำหนดโดย ITU
- การโทรเข้าที่มาจากต่างประเทศที่ไม่มีการกำหนดเลขหมายต้นทาง (NonCLI) ซึ่งมาจากช่องทาง VoIP ให้ดำเนินการเพิ่ม Prefix โดยใช้เครื่องหมาย “+697” นำหน้าเลขหมายที่โทรเข้า
- กำหนดให้ผู้ให้บริการจะต้องเพิ่ม Prefix สำหรับกรณีบริการที่ระบุเลขหมายต้นทางจากต่างประเทศ CLI โดยใช้เครื่องหมาย “+698” นำหน้าเลขหมายที่เป็นการ Roaming จากต่างประเทศ
- จัดทำบริการ USSD หมายเลข *138 เพื่อให้ผู้ใช้บริการสามารถเลือกปฏิเสธการรับสายที่จากต่างประเทศได้
- มาตรการเชิงรุกโดยดำเนินการติดตามตรวจสอบการโทรจากต่างและในประเทศที่มีพฤติกรรมการใช้งานที่ผิดปกติและมีแนวโน้มการใช้งานที่อาจเข้าข่ายเป็นการกระทำผิดกฎหมาย
- การเพิ่มความเข้มงวดสำหรับการลงทะเบียนการใช้งานโทรศัพท์เคลื่อนที่ (การลงทะเบียน SIM) โดยจะกำหนดให้ผู้ที่ถือครองเลขหมายจำนวนมาก ต้องแสดงตัวตนและวัตถุประสงค์ของการถือครอง เป็นระยะ ๆ

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

เมื่อวันที่ 24 มกราคม 2566 ที่ประชุมคณะรัฐมนตรีเห็นว่า ปัจจุบัน มิจฉาชีพมีการหลอกลวงให้ประชาชนโอนเงินผ่านการติดต่อทางโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ ซึ่งขยายตัวรวดเร็วและเกิดความเสียหายเป็นวงกว้าง จากสถิติตั้งแต่ 1 มีนาคม ถึง 31 ตุลาคม 2565 มีคดีออนไลน์เกิดขึ้นกว่า 114,000 คดี คิดเป็นมูลค่าความเสียหายกว่า 22,000 ล้านบาท เฉลี่ย 800 คดีต่อวัน อีกทั้ง ยังไม่มีกฎหมายเฉพาะที่ให้อำนาจสถาบันการเงินหรือผู้ประกอบธุรกิจ สามารถระงับการทำธุรกรรมใด ๆ ที่ต้องสงสัยว่าเป็นธุรกรรมที่กระทำผิดทางอาญา โดยเฉพาะการหลอกลวงประชาชนให้โอนเงินไปยังบัญชีผู้อื่นที่อยู่ในขบวนการเป็นทอด ๆ อย่างรวดเร็ว หรือที่เรียกว่า บัญชีม้า ทำให้เจ้าหน้าที่ไม่สามารถระงับการทำธุรกรรมหรืออายัดเงินได้ทันท่วงที จึงมีมติอนุมัติร่างพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยมีสาระสำคัญเป็นการกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ที่หลอกลวงประชาชนให้โอนเงินผ่านการติดต่อทางโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ และลงโทษผู้ที่เปิดบัญชีบัตรอิเล็กทรอนิกส์หรือกระเป๋าเงินอิเล็กทรอนิกส์ เพื่อนำเงินหรือทรัพย์สินมาใช้ในการกระทำความผิดอาญา โดยมีรายละเอียด อาทิ (The Secretariat of the Prime Minister, 2023)

- กำหนดให้มีกลไก “คณะกรรมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี” เพื่อกำหนดแนวทางในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และกำหนดหน่วยงานที่ได้รับอนุญาตให้เข้าถึงข้อมูลที่มีการแลกเปลี่ยนข้อมูล โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธาน และมีกรรมการโดยตำแหน่ง 8 คน
- สถาบันการเงินและผู้ประกอบธุรกิจ มีอำนาจแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าผ่านระบบการแลกเปลี่ยนข้อมูล
- ผู้ให้บริการโทรคมนาคม มีอำนาจแลกเปลี่ยนข้อมูล และให้สำนักงานตำรวจแห่งชาติ และสำนักงาน ปปง. และหน่วยงานที่ได้รับอนุญาตเข้าถึงข้อมูลที่มีการแลกเปลี่ยนได้

● สำนักงาน กสทช. เป็นหน่วยงานจัดทำระบบฐานข้อมูลกลางเท่าที่จำเป็น เกี่ยวกับข้อมูลการลงทะเบียนผู้ใช้งาน ข้อความสั้น เพื่อใช้ในการสืบสวนสอบสวนและป้องกัน

● ขั้นตอนในการระงับการทำธุรกรรม อาทิ (1) กรณีสถาบันการเงินหรือผู้ประกอบธุรกิจพบเหตุอันควรสงสัยเองหรือได้รับแจ้งจากเจ้าพนักงาน ให้สถาบันการเงินหรือผู้ประกอบธุรกิจระงับการทำธุรกรรม แล้วแจ้งให้สถาบันการเงินหรือผู้ประกอบธุรกิจที่รับโอนระงับการทำธุรกรรมต่อไปทันทีเป็นการชั่วคราว หากตรวจสอบแล้วไม่พบเหตุสงสัย ให้สามารถดำเนินการทำธุรกรรมต่อไปได้ (2) กรณีได้รับแจ้งจากผู้เสียหาย ให้สถาบันการเงินหรือผู้ประกอบธุรกิจระงับการทำธุรกรรมและแจ้งให้สถาบันการเงินหรือผู้ประกอบธุรกิจที่รับโอนระงับการทำธุรกรรมไว้ทันทีเป็นการชั่วคราว เพื่อให้ผู้เสียหายร้องทุกข์ต่อพนักงานสอบสวนภายในเวลา 48 ชั่วโมง และให้พนักงานสอบสวนดำเนินการเกี่ยวกับบัญชีและกระเป๋าเงินอิเล็กทรอนิกส์นั้นภายในเวลา 7 วัน นับแต่วันได้รับแจ้ง

● การแจ้งข้อมูลหรือหลักฐาน สามารถแจ้งผ่านทางโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ได้ กรณีแจ้งทางโทรศัพท์ให้ผู้ระงับการทำธุรกรรมบันทึกไว้เป็นลายลักษณ์อักษรและส่งให้อีกฝ่ายหนึ่งทราบเพื่อเก็บไว้เป็นหลักฐาน

● กำหนดบทลงโทษ แบ่งเป็น 2 กรณี ดังนี้ (1) ห้ามมิให้ผู้ใดเปิดบัญชี บัตรอิเล็กทรอนิกส์ หรือกระเป๋าเงินอิเล็กทรอนิกส์ โดยไม่ได้มีเจตนาใช้เพื่อตน และห้ามไม่ให้ผู้ใดยินยอมให้บุคคลอื่นใช้หรือยืมใช้ซิมโทรศัพท์ของตนในทั้งที่รู้หรือควรจะรู้ ซึ่งอาจจะนำไปใช้ในการทุจริตหรือทำผิดกฎหมาย ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ (2) ห้ามไม่ให้ผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อหรือขายบัญชี บัตรอิเล็กทรอนิกส์ กระเป๋าเงินอิเล็กทรอนิกส์ หรือซิมโทรศัพท์ ซึ่งอาจก่อให้เกิดการกระทำความผิดอาญา ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกตั้งแต่ 2 ปี ถึง 5 ปี และปรับตั้งแต่ 200,0000 บาท ถึง 500,000 บาท หรือทั้งจำทั้งปรับ

จะเห็นได้ว่าร่างพระราชกำหนดนี้มีการกำหนดความผิดของผู้ที่เปิดบัญชีม้าโดยตรง และให้สถาบันการเงินมีอำนาจระงับธุรกรรมที่ต้องสงสัยว่าเป็นการหลอกโอนเงินจากผู้เสียหายได้เองโดยไม่ต้องรอให้ผู้เสียหายร้องทุกข์ต่อพนักงานสอบสวนก่อน เพิ่มโอกาสที่จะสกัดกั้นไม่ให้เงินนั้นถูกโอนออกนอกประเทศซึ่งจะทำให้ยากต่อการติดตามทวงคืน

การทำงานของแอปพลิเคชันปลอมของคนร้าย

แอปพลิเคชันปลอมของคนร้ายโดยทั่วไปจะโจมตีสมาร์ทโฟนที่ใช้ระบบปฏิบัติการแอนดรอยด์มากกว่า เนื่องจากเป็นระบบเปิด สามารถติดตั้งแอปพลิเคชันปลอมจากการดาวน์โหลดมาเองได้ง่ายกว่าโดยไม่ต้องผ่านการตรวจสอบจากกูเกิล เพลย์ คนร้ายจะพยายามโน้มน้าวเหยื่อให้ดาวน์โหลดไฟล์สำหรับติดตั้งแอปพลิเคชันนั้นจากเว็บไซต์ปลอมที่ดูน่าเชื่อถือ โดยจะสังเกตได้ว่าชื่อโดเมนใน URL ของเว็บไซต์ปลอมนั้นจะไม่ตรงกับของจริงซึ่งได้ถูกจดทะเบียนชื่อโดเมนไปแล้ว แต่คนร้ายอาจจะจดชื่อโดเมนให้มีความคล้ายคลึงใกล้เคียงกับของจริงได้จนเหยื่อไม่ทันสังเกต

เมื่อเหยื่อติดตั้งแอปพลิเคชันปลอมสำเร็จ และเรียกใช้งาน แอปพลิเคชันปลอมจะใช้กลวิธีหลากหลายเพื่อโจมตีอาทิเช่น (Chanyavilas, 2023)

● มีการให้ตั้ง PIN หรือรหัสผ่านถึง 2 ครั้ง โดยข้อมูลนี้จะถูกคนร้ายนำไปลองใช้ในการใส่เป็น PIN ขณะเข้าแอปพลิเคชันของธนาคารต่าง ๆ ในเครื่องของเหยื่อ

● หาก PIN ที่พิมพ์ในแอปพลิเคชันปลอมใช้งานไม่ได้ บางกรณีคนร้ายจะถามเหยื่อตรง ๆ เช่น PIN ที่ใส่มาเป็นอันเดียวกับของธนาคารหรือไม่ หากไม่ใช่ให้บอก PIN ของธนาคาร เพื่อทำการตรวจสอบบัญชีให้สำเร็จ

● ถ้ายังไม่ได้ PIN คนร้ายอาจบอกให้เหยื่อโอนเงินจำนวนน้อย ๆ ระหว่างบัญชีของตนเอง ระหว่างนี้คนร้ายจะสังเกตตัวเลขที่กระพริบเวลาเหยื่อกด PIN บนหน้าจอ หรือในบางครั้งก็อาศัยจังหวะหลังจากที่เหยื่อใส่ PIN แล้วแต่ยังไม่ได้ปิดแอปพลิเคชันของธนาคาร ทำรายการโอนเงินต่อเลย

● มีการขอ Permission เช่น ขอทำตัวเป็นแอปพลิเคชันสำหรับผู้พิการ (accessibility service) เพื่อให้ตัวแอปพลิเคชันสามารถทำงานได้ตลอดเวลา 24 ชั่วโมง ถึงแม้จะปิดทิ้งไปแล้วก็ตาม และสามารถแตะหน้าจอใน

ตำแหน่งใด ๆ แทนผู้ใช้งานได้ ขอทำการถ่ายทอดหน้าจอ (screen casting) เพื่อให้แอปพลิเคชันสามารถคัดลอกหน้าจอแล้วส่งภาพวีดีโอของหน้าจอเหยื่อขึ้นไปยังระบบของคนร้าย ดังนั้นคนร้ายจะสามารถเห็นหน้าจอของเหยื่อได้ตลอดเวลาไม่ว่าจะทำอะไรอยู่ที่หน้าไหนก็ตาม ขอเขียนภาพทับโปรแกรมอื่น (system alert screen overlay) เพื่อให้แอปพลิเคชันสามารถเขียนภาพใด ๆ ทับบนหน้าจอโทรศัพท์แบบเต็มจอ เหยื่อจะมองไม่เห็นว่าคนร้ายกำลังทำอะไรอยู่บนเครื่องของตน และไม่สามารถแตะปุ่มเพื่อปิดเครื่องบนหน้าจอ หรือสลับแอปพลิเคชันได้เลย

● หลังจากที่เหยื่อถูกข่มขู่และหลอกจนหลงเชื่อเมื่อมีการให้ Permission ของผู้พิการไปแล้ว ตัวแอปพลิเคชันปลอมจะแอบไปกด Allow การถ่ายทอดหน้าจอเองโดยอัตโนมัติ เพื่อไม่ให้เหยื่อรู้ตัวว่ากำลังถูกแอบถ่ายทอดหน้าจอ

● หลังจาก Allow Permission ครบแล้ว หน้าจอโทรศัพท์จะถูกล็อกทันที เพื่อให้คนร้ายเข้ามาควบคุมและทำรายการกับแอปพลิเคชันของธนาคารได้โดยเหยื่อไม่รู้ตัว ขณะเดียวกันคนร้ายจะบอกเหยื่อให้วางโทรศัพท์นิ่ง ๆ ห้ามแตะต้อง

การป้องกันและรับมือสำหรับประชาชน

ตามแนวคิดของ Cyber Kill Chain ในแต่ละขั้นตอนข้างต้น ทำให้สามารถป้องกันรับมือแก๊งคอลเซ็นเตอร์ยุคดิจิทัลได้ ดังนี้

● ตั้งสติทุกครั้งก่อนรับโทรศัพท์จากเลขหมายที่ไม่คุ้นเคย โดยเฉพาะเลขหมายที่โทรจากต่างประเทศที่ขึ้นต้นด้วย +698 หรือ +697 ซึ่งมีความเป็นไปได้สูงที่จะเป็นเบอร์ที่โทรมาจากมิจฉาชีพ หากไม่มีความจำเป็นสามารถแจ้งผู้ให้บริการให้บล็อกการโทรจากต่างประเทศได้

● โดยทั่วไปหน่วยงานหรือสถาบันการเงินต่าง ๆ จะไม่มีนโยบายสอบถามข้อมูลส่วนบุคคลของลูกค้า หรือขอให้ทำธุรกรรมทางโทรศัพท์ จึงค่อย ๆ ไตร่ตรองว่าเรื่องที่โทรมาเกี่ยวข้องกับตนเองหรือไม่ สอบถามข้อมูลเพิ่มเติมให้แน่ชัด อย่าดำเนินการใด ๆ และวางสาย หากยังไม่แน่ใจให้ติดต่อกลับคอลเซ็นเตอร์ของหน่วยงานที่เกี่ยวข้องเองโดยตรง

● ระมัดระวังการไม่เปิดเผยข้อมูลส่วนตัวที่สำคัญ เช่น วันหมดอายุของบัตรต่าง ๆ วันเดือนปีเกิด รหัสผ่าน เนื่องจากคนร้ายอาจนำไปใช้เป็นประโยชน์ต่อการโจมตี (Pokudom, 2020)

● ห้ามโอนเงินให้ไม่ว่าจะมีการอ้างเหตุผลใด ๆ ก็ตามเพราะมีโอกาสสูงมากที่จะไม่ได้คืน

● หากต้องเข้าเว็บไซต์ของหน่วยงาน ควรค้นหา URL จาก Google เองไม่ควรคลิกลิงก์ที่ส่งมาเพราะอาจจะนำไปสู่เว็บไซต์ปลอมของคนร้ายได้

● ไม่ติดตั้งแอปพลิเคชันที่ไม่ได้อยู่ใน Google Play เพราะมีความเสี่ยงสูงที่เป็นแอปพลิเคชันปลอม หากเผลอติดตั้งไปแล้วให้ตัดการเชื่อมต่อกับเครือข่ายจนกว่าจะแน่ใจว่าได้ลบแอปพลิเคชันเหล่านี้หมดแล้ว

● พยายามแยกบัญชีสำหรับทำธุรกรรมผ่านสมาร์ทโฟนโดยเฉพาะให้คงเหลือเงินเพียงพอต่อการทำธุรกรรมเท่านั้น และจำกัดวงเงินในการทำธุรกรรมออนไลน์เพื่อลดความเสี่ยงที่จะเสียเงินทั้งหมดจากการโจมตีของคนร้าย

● หากถูกโอนเงินออกไปแล้วให้รวบรวมหลักฐานและข้อมูลสำคัญทุกอย่างที่เกี่ยวข้อง แล้วเข้าแจ้งความเพื่อขอบันทึกประจำวันไปใช้เป็นหลักฐานในการติดต่อขอความช่วยเหลือเบื้องต้นกับสถาบันการเงิน หรือแจ้งความออนไลน์ที่ thaipoliceonline.com นอกจากนี้ยังสามารถโทรแจ้งเหตุที่ศูนย์รับแจ้งเหตุภัยทางการเงินจากมิจฉาชีพของธนาคารแต่ละแห่งได้ตลอด 24 ชั่วโมง

● ติดตามข่าวสารการแจ้งเตือนเกี่ยวกับการหลอกลวงต่าง ๆ เพราะคนร้ายมักจะเปลี่ยนหรือคิดค้นรูปแบบและกลวิธีใหม่ ๆ เพื่อหลอกลวงเหยื่ออยู่เสมอ

บทสรุป

ภัยจากแก๊งคอลเซ็นเตอร์มักจะมีการพัฒนารูปแบบและกลวิธีใหม่ ๆ เพื่อหลอกลวงเหยื่ออยู่เสมอเพราะได้ผลตอบแทนที่คุ้มค่า แม้หน่วยงานที่เกี่ยวข้องจะพยายามออกมาตรการ หรือปรับเพิ่มกฎหมายเพื่อรับมือแต่ก็มักจะล้าหลังมิจฉาชีพเหล่านี้อยู่เสมอ กลุ่มที่ตกเป็นเหยื่อถูกหลอกส่วนใหญ่จะเป็นผู้สูงวัย คนที่ไม่ได้ใช้เครือข่ายสังคมออนไลน์ ไม่ติดตามข่าวสารแจ้งเตือนเกี่ยวกับการหลอกลวงต่าง ๆ หรือคนที่ไม่คุ้นเคยและไม่ค่อยได้ใช้อุปกรณ์เกี่ยวกับ

เทคโนโลยีสารสนเทศ ควรมีความตระหนักถึงภัยนี้ เพื่อลดความเสี่ยงจากความเสียหาย โดยสิ่งที่กลุ่มคนร้ายต้องการจากเหยื่อนอกจากทรัพย์สินแล้ว อาจเป็นข้อมูลส่วนตัว ของเหยื่อ และรหัสผ่านต่าง ๆ เพื่อใช้สวมรอยในการทำธุรกรรมหรือนำไปหาประโยชน์ต่อได้

References

Bank of Thailand. (2022). *Exposing horse accounts know not to be a victim*. Retrieved from https://www.bot.or.th/Thai/BOTMagazine/Pages/25650166FinancialWisdom.aspx. (in Thai)

Chanyavilas, N. (2023). *The money has been sucked out of the account. What actually happened? how?*. Retrieved from http://bit.ly/3JH9Owu. (in Thai)

Lockheed Martin. (2023). *The Cyber Kill Chain*. Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Nitilaw and Win Office. (2022). *Is it wrong to open a bank account?-Lawyer Nithipol*. Retrieved from https://bit.ly/3Y1spYg. (in Thai)

Office of The National Broadcasting and Telecommunications Commission. (2023). *The problem of crime in telecommunication technology*. Retrieved from https://drive.google.com/file/d/1CeCaW9qf1s5PGcaajAXCw3iY6OHM5IBu/view. (in Thai)

Pokudom, N. (2020). Data privacy in the digital age. *EAU Heritage Journal Science and Technology, 14*(2), 59–69. (in Thai)

Social-Engineer. (2022). *Influence tactics*. Retrieved from https://www.social-engineer.org/framework/influencing-others/influence-tactics/

TechTalkThai. (2016). *Get to know Cyber Kill Chain, the process of hacking the system to attack the target*. Retrieved from https://www.techtalkthai.com/introduction-to-cyber-kill-chain/. (in Thai)

Thailand Science Research and Innovation. (2021). *Call center crime*. Retrieved from https://researchcafe.tsri.or.th/call-center-crime/. (in Thai)

The Secretariat of the House of Representatives. (2022). *Threat of call center gangs*. Retrieved from https://library.parliament.go.th/th/radioscript/rr2565-jul7. (in Thai)

The Secretariat of the Prime Minister. (2023). *Prime Minister's picture and speech file cabinet passes bill to deal with online crime suspension of suspicious transactions, opening a horse account, severe imprisonment, and a fine of hundreds of thousands*. Retrieved from https://www.thaigov.go.th/news/contents/details/64125. (in Thai)