ปัญหาแก๊งคอลเซนเตอร์โทรหลอกลวง

CALL CENTER SCAMMER PROBLEMS

ต่อศิลป์ ตันเจริญ[1]
สมพงษ์ อัศวบุญมี[2]
Torsin Tuncharoen[1]
Somphong Assawaboonmee[2]

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) กรุงเทพฯ 10210[1และ2]
National Telecom Public Company Limited Bangkok, 10210 Thailand[1and2]

Corresponding E-mail : torsin.tun@gmail.com

Received Date July 11, 2022
Revised Date March 30, 2023
Accepted Date March 31, 2023

บทคัดย่อ

บทความนี้จัดทำขึ้นเพื่อศึกษาปัญหาการโทรหลอกลวง และเพื่อนำไปสู่แนวทางที่จะแก้ปัญหาที่มีประสิทธิภาพมากขึ้น โดยใช้แนวทางการวิจัยเชิงเอกสาร ประกอบกับกระบวนการสืบค้น และวิเคราะห์ข้อมูล โดยพบว่ามิจฉาชีพที่โทรหลอกลวงจะใช้ระบบคอลเซนเตอร์โทรผ่านระบบบริการเสียงผ่านอินเทอร์เน็ต หรือ Voice over Internet Protocol (VoIP) ซึ่งสามารถใช้งานจากที่ไหนก็ได้ทั่วโลก จึงเรียกมิจฉาชีพประเภทนี้ว่า “แก๊งคอลเซนเตอร์” โดยแก๊งคอลเซนเตอร์ส่วนใหญ่จะอยู่ต่างประเทศ แล้วโทรข้ามประเทศมายังกลุ่มเป้าหมาย เพื่อให้ยากต่อการติดตามจับกุม การโทรหลอกลวงมีกลวิธีที่หลากหลาย แต่ที่ใช้มากที่สุดคือ “การปลอมแปลงหมายเลขต้นทาง” ซึ่งหมายเลขต้นทางถูกปลอมแปลงเป็นหมายเลขท้องถิ่นหรือหมายเลขของหน่วยงานต่าง ๆ เพื่อเพิ่มโอกาสที่เหยื่อจะรับสาย แม้หลายประเทศพยายามสกัดกั้นแต่ก็ไม่สามารถระงับได้ทั้งหมดเนื่องจากแก๊งคอลเซนเตอร์จะมีการปรับเปลี่ยนรูปแบบและปลอมแปลงหมายเลขที่ใช้โทรไปเรื่อย ๆ ดังนั้นผู้ให้บริการโทรศัพท์ทุกรายอาจต้องเปิดช่องทางให้ผู้ใช้บริการสามารถสมัครปฏิเสธการรับสายเรียกเข้าจากต่างประเทศได้ หากผู้ใช้บริการไม่ได้มีญาติหรือคนรู้จักในต่างประเทศจะได้ช่วยป้องกันการโทรเข้ามาหลอกลวง โดยทำควบคู่กับการประชาสัมพันธ์ให้เข้าถึงประชาชนมากที่สุดเพื่อให้มีความรู้เท่าทันและไม่ตกเป็นเหยื่อ

คำสำคัญ: แก๊งคอลเซนเตอร์หลอกลวง หมายเลขต้นทาง โทรศัพท์มือถือ ระบบบริการเสียงผ่านอินเทอร์เน็ต ซิมบ็อกซ์

Abstract

This article aims to study and find efficient solutions to scam call problems using documentary research approach, together with heuristic process and information analysis. These scammers used Voice over Internet Protocol (VoIP), which could be operated from anywhere in the world, to make their scam calls. They were thus dubbed “Call Center Scammer”. Most scammers were based in foreign countries and made oversea calls to their target, making them difficult to be tracked and arrested. The scammers used many different methods. The most common one was “Caller ID Spoofing”, where the caller number was spoofed as a local number or an organization’s number to increase chance of answering by the victims. Despite many countries’ effort to intercept, scam call problems could not be completely eliminated as the scammers always changed the caller numbers. In a bid to prevent these scammers, mobile operators have to allow their users who have no relatives or acquaintances in foreign countries to reject oversea incoming calls. At the same time, information about these scammers should be disseminated to as many people as possible in order to prevent them from being victims.

Keywords: Call center scammers, Caller number, Mobile, Voice over Internet Protocol (VoIP), SIM box

1. บทนำ

ปัจจุบันแก๊งคอลเซนเตอร์โทรหลอกลวงเป็นปัญหาที่เกิดขึ้นและสร้างความเสียหายในทุกประเทศทั่วโลก ที่ผ่านมาพบว่าการโทรหลอกลวง (Scam call) มีแนวโน้มจะเพิ่มสูงขึ้นทั่วโลก เช่น สหรัฐอเมริกาพบการโทรหลอกลวงในปี พ.ศ. 2564 สูงกว่าสถิติในปี พ.ศ. 2563 ถึงร้อยละ 118 สอดคล้องกับผลสำรวจที่เปิดเผยว่าประชากรผู้ใหญ่จำนวนร้อยละ 40 ในสหราชอาณาจักรได้รับโทรศัพท์ต้องสงสัยในปี พ.ศ. 2564 และผลสำรวจนี้ยังเปิดเผยอีกว่ามีผู้ตกเป็นเหยื่อถึงร้อยละ 2 (Lemzy, 2022) ในส่วนของประเทศไทยพบว่าในปี พ.ศ. 2564 มีการโทรศัพท์เพื่อหลอกลวงจากแก๊งคอลเซนเตอร์ถึง 6.4 ล้านครั้ง เพิ่มขึ้นจากระยะเดียวกันของปี พ.ศ. 2563 สูงถึงร้อยละ 270 (ธนาคารแห่งประเทศไทย, 2565, น. 2) ปัญหาการโทรหลอกลวงจึงเป็นปัญหาที่ทุกประเทศควรให้ความสำคัญและหาแนวทางแก้ไขปัญหาต่อไป

2. วัตถุประสงค์

เพื่อศึกษาปัญหาการโทรหลอกลวงที่เกิดขึ้นในปัจจุบัน รวมถึงมาตรการป้องกันและสกัดกั้นของหน่วยงานรัฐที่เกี่ยวข้องกับการป้องกันและปราบปรามการหลอกลวงและผู้ให้บริการโทรศัพท์ (Operator) ทั้งในประเทศไทยและในต่างประเทศ เพื่อหาแนวทางการแก้ไขปัญหาที่ดีขึ้น

3. วิธีการศึกษา

บทความนี้ใช้แนวทางการวิจัยเชิงเอกสาร (Documentary research) โดยค้นคว้าข้อมูลที่เกี่ยวข้องกับการโทรหลอกลวงและแนวทางแก้ปัญหาในปัจจุบัน ผ่านกระบวนการสืบค้นข้อมูล โดยกำหนดขอบเขตแหล่งข้อมูลจากบทความและข่าวสารภาษาไทยและภาษาอังกฤษ จากนั้นจึงนำข้อมูลมาเรียบเรียงโดยเชื่อมโยงความรู้ด้านเทคนิคกับพฤติกรรมและรูปแบบการโทรหลอกลวงที่เกิดขึ้นในปัจจุบัน และวิเคราะห์แนวทางแก้ไขปัญหาการโทรหลอกลวงทั้งในประเทศไทยและต่างประเทศ โดยกล่าวถึงปัจจัยสนับสนุนและปัจจัยที่เป็นอุปสรรคของการแก้ปัญหาให้หมดไป และนำเสนอแนวทางแก้ไขปัญหาที่ดีกว่าต่อไป

4. ผลการศึกษา

4.1 การโทรหลอกลวง

คำว่า “หลอกลวง” เป็นคำกริยาหมายความว่า “ใช้อุบายทุจริตลวงให้เข้าใจผิด” หรือในด้านกฎหมาย คือ การแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง เพื่อให้บุคคลอื่นเข้าใจผิด (ราชบัณฑิตยสถาน, 2554) เมื่อนำมาผนวกกับคำว่า “การโทร” จึงมีความหมายว่า การใช้อุบายลวงให้เข้าใจผิดผ่านทางโทรศัพท์ “การโทรหลอกลวง” ตรงกับคำว่า “Scam call” ในภาษาอังกฤษ ซึ่งมีความหมายว่า การโทรศัพท์อันฉ้อฉล กล่าวคือ ปลอมแปลงเป็นบุคคลหรือนิติบุคคลเพื่อจะขโมยทรัพย์หรือตัวตนของคุณ (Trapcall, 2017) จึงอาจสรุปได้ว่า การโทรหลอกลวง คือ การทำทุจริต โดยใช้อุบายลวงและปลอมแปลงตัวตน ด้วยเจตนาอันฉ้อฉลเพื่อให้ได้มาซึ่งทรัพย์หรือตัวตนของผู้อื่น วิธีการหลอกลวงของคนร้ายมักจะสร้างสถานการณ์ให้เหยื่อรู้สึกตกใจ หวาดกลัว วิตกกังวล หรือรู้สึกตื่นเต้น ดีใจ เพื่อให้เหยื่อขาดสติยั้งคิด และโน้มน้าวให้เหยื่อโอนเงินเข้าบัญชี โดยมักสวมรอยเป็นเจ้าหน้าที่ของหน่วยงานหรือตัวแทนของบริษัทที่มีชื่อเสียง ทั้งนี้ ในทุกสถานการณ์ คนร้ายจะกำหนดกรอบเวลาระยะสั้นเพื่อเร่งให้เหยื่อต้องดำเนินการอย่างใดอย่างหนึ่ง โดยไม่มีเวลาคิดทบทวนหรือตรวจสอบข้อมูลเสียก่อน เช่น สวมรอยเป็นเจ้าหน้าที่ธนาคารเพื่อหลอกลวงว่าบัญชีเงินฝากของเหยื่อจะถูกอายัดภายใน 2 ชั่วโมง เนื่องจากพบว่าบัญชีนี้เกี่ยวพันกับธุรกิจที่ผิดกฎหมาย และหลอกให้เหยื่อโอนเงิน หรือฝากเงินดังกล่าวเข้าบัญชีผ่านตู้รับฝากเงินอัตโนมัติ (ตู้เอดีเอ็ม/ซีดีเอ็ม) เพื่อนำเงินไปตรวจสอบ หรือเพื่อเป็นค่าดำเนินการที่เกี่ยวข้อง (ธนาคารแห่งประเทศไทย, 2557)

แก๊งคอลเซนเตอร์จะคิดกลอุบายหรือนำเหตุการณ์ที่สอดคล้องกับสถานการณ์ที่เกิดขึ้นในปัจจุบันมาสร้างเรื่องหลอกลวงอยู่เรื่อย ๆ กลอุบายที่พบบ่อยครั้ง ได้แก่

4.1.1 การอ้างตัวเป็นเจ้าหน้าที่ธนาคาร หรือสถาบันทางการเงิน โดยหลอกว่าบัญชีเงินฝากของเหยื่อเกี่ยวข้องกับธุรกิจที่ผิดกฎหมายและจะถูกอายัด เพื่อแสดงความบริสุทธิ์จะต้องโอนเงินออกจากบัญชีให้เจ้าหน้าที่ตรวจสอบก่อนเพื่อไม่ให้ถูกอายัด หรือบางครั้งก็แนะนำให้เหยื่อไปทำรายการยืนยันตัวตนหรือปลดล็อกบัญชีที่ตู้เอทีเอ็ม แต่เป็นการทำรายการโอนเงินออกจากบัญชีโดยไม่รู้ตัว เนื่องจากแก๊งคอลเซนเตอร์จะหลอกให้ทำรายการด้วยเมนูภาษาอังกฤษ

4.1.2 การอ้างตัวเป็นเจ้าหน้าที่บริษัทขนส่งพัสดุ โดยหลอกว่าเหยื่อมีพัสดุตกค้าง ซึ่งอาจทำให้เหยื่อที่มีการส่งหรือรอรับพัสดุหลงกลได้ง่าย เนื่องจากการรับส่งพัสดุจากการซื้อของออนไลน์ในปัจจุบันเป็นที่นิยมอย่างแพร่หลาย แต่หากเหยื่อไม่ได้มีการส่งหรือรอรับพัสดุอยู่ ก็จะอ้างว่าเหยื่ออาจถูกผู้ไม่หวังดีนำข้อมูลส่วนตัวไปใช้ในการจัดส่งพัสดุที่ผิดกฎหมายจึงถูกอายัด แล้วหลอกให้เหยื่อไปแจ้งความที่สถานีตำรวจซึ่งส่วนใหญ่จะอ้างชื่อสถานีตำรวจที่อยู่ต่างจังหวัด เพื่อทำให้เหยื่อไม่สะดวกในการเดินทางไปแจ้งความเอง แล้วแสดงความหวังดีช่วยเหลือโดยการโอนสายให้คุยกับเจ้าหน้าที่ตำรวจโดยตรง และแสร้งทำการโอนสายไปยังเจ้าหน้าที่ตำรวจซึ่งเป็นตำรวจปลอม แล้วทำการสอบสวนและข่มขู่ต่าง ๆ นานาเพื่อให้เหยื่อเกรงกลัวและทำตามทุกอย่าง โดยจะหลอกล่อเหยื่อว่าจะต้องรีบโอนเงินในบัญชีทั้งหมดออกไปพักที่บัญชีของตำรวจไว้ก่อน เพื่อไม่ให้ถูกอายัด

4.1.3 การอ้างตัวเป็นเจ้าหน้าที่หน่วยงานด้านโทรคมนาคม เช่น บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) โดยหลอกว่าหมายเลขโทรศัพท์ของเหยื่อจะถูกระงับการใช้งาน หากเหยื่อหลงเชื่อ จะหลอกให้เหยื่อแจ้งรายละเอียดข้อมูลส่วนตัวเพื่อดำเนินการตรวจสอบให้ จะได้ไม่ถูกระงับบริการ

4.1.4 การแสดงตัวเป็นเจ้าหนี้ทวงหนี้นอกระบบ โดยหลอกว่าเหยื่อหรือคนใกล้ชิดของเหยื่อติดหนี้นอกระบบจำนวนมาก และข่มขู่ให้เหยื่อโอนเงินมาใช้หนี้ มิฉะนั้นจะทำร้ายหรือประจานให้เสื่อมเสีย

4.1.5 การอ้างตัวเป็นเจ้าหน้าที่กรมสรรพากร โดยหลอกว่าเหยื่อได้รับคืนเงินภาษีซึ่งเป็นเงินจำนวนมาก จึงต้องทำการยืนยันตัวตนผ่านตู้เอทีเอ็มก่อน หากเหยื่อหลงกลไปที่ตู้เอทีเอ็ม จะหลอกให้ทำรายการต่าง ๆ ผ่านเมนูภาษาอังกฤษเพื่อให้เหยื่อที่อ่านไม่ออกหรือไม่ทันสังเกตว่ารายการที่หลอกให้ทำเป็นการโอนเงินออกจากบัญชี

4.1.6 การอ้างตัวเป็นเจ้าหน้าที่สถาบันการเงินให้สินเชื่อเงินกู้ สามารถอนุมัติสินเชื่อได้สะดวกง่ายและรวดเร็ว โดยการแอบอ้างกรณีแบบนี้ แก๊งคอลเซนเตอร์จะมีข้อมูลส่วนตัวของเหยื่อค่อนข้างมากและอาจทราบว่าเหยื่อกำลังต้องการกู้เงินอยู่ด้วย จึงแสดงความหวังดีเข้ามาช่วยเหลือเหยื่อ แต่จะอ้างกับเหยื่อว่าจะต้องโอนเงินค่าธรรมเนียมเพื่อใช้ในการดำเนินการก่อน

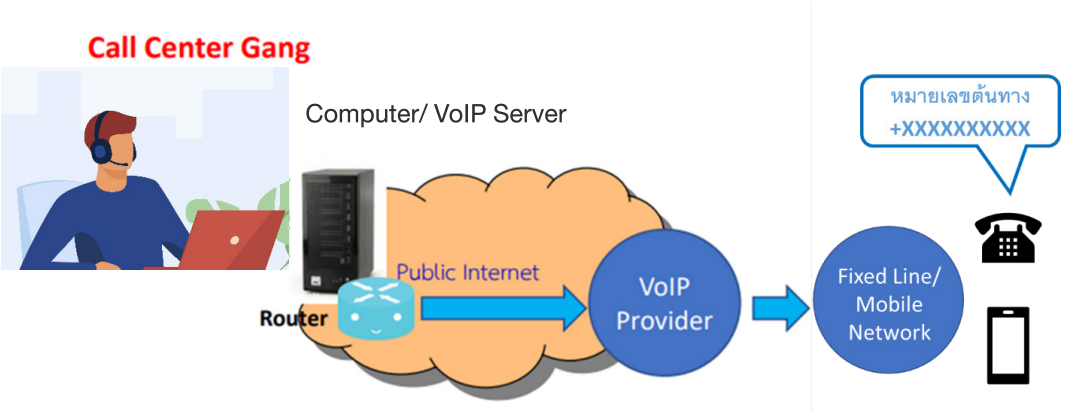
4.1.7 หลอกว่าเหยื่อเป็นผู้โชคดีและจะได้รับรางวัลใหญ่ แต่เหยื่อต้องโอนเงินจ่ายค่าภาษีก่อน (ธนาคารกรุงเทพ จำกัด (มหาชน), ม.ป.ป.)

4.1.8 หลอกว่าเป็นญาติหรือเพื่อนสนิท โดยพยายามโทรคุยด้วยความสนิทสนม และจบด้วยการขอความช่วยเหลือเรื่องเงิน

4.2 ระบบโทรศัพท์และวิธีการทางเทคนิคที่แก๊งคอลเซนเตอร์ใช้โทรหลอกลวง

แก๊งคอลเซนเตอร์ส่วนใหญ่จะโทรศัพท์ข้ามประเทศมาหาเหยื่อ ซึ่งอยู่คนละประเทศกับกลุ่มเป้าหมายในการหลอกลวง ตัวอย่างเช่น แก๊งคอลเซนเตอร์ในสาธารณรัฐอินเดียโทรหลอกลวงเหยื่อในสหรัฐอเมริกา หรือแก๊งคอลเซนเตอร์ในประเทศไทยโทรไปหลอกลวงเหยื่อในสาธารณรัฐประชาชนจีน ในหลายกรณีมีการปลอมแปลงหมายเลขต้นทาง (Caller ID spoofing) ด้วย ทั้งนี้เพื่ออำพรางพิกัดที่อยู่แท้จริง และสร้างอุปสรรคในการติดตามจับกุมตัวมาดำเนินคดี รวมทั้งเพื่อสร้างความเชื่อถือให้เหยื่อหลงกลด้วยการปลอมแปลงเป็นหมายเลขของหน่วยงานต่าง ๆ ทั้งหน่วยงานราชการและบริษัทเอกชน เช่น บริษัทบัตรเครดิต หรือธนาคารต่าง ๆ (Hopewell, 2021)

แก๊งคอลเซนเตอร์จึงเลือกใช้โทรศัพท์ระบบบริการเสียงผ่านอินเทอร์เน็ต (Voice over Internet Protocol) หรือเรียกโดยย่อว่า “VoIP” ในการโทรหลอกลวงประชาชน เนื่องจากระบบ VoIP เป็นระบบโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต (Internet) สามารถใช้งานจากที่ไหนก็ได้ เพียงแค่เชื่อมต่อระบบโทรศัพท์เข้ากับอินเทอร์เน็ตก็สามารถโทรออกไปยังหมายเลขต่าง ๆ ที่ต้องการได้ (Hale, 2022) โดยแก๊งคอลเซนเตอร์จะใช้โปรแกรมคอลเซนเตอร์สำเร็จรูปที่สามารถติดตั้งในเซิร์ฟเวอร์คอมพิวเตอร์ (Computer server) สำหรับใช้โทรออกแบบอัตโนมัติไปยังหมายเลขต่าง ๆ เมื่อโทรออกไปแล้ว หากเหยื่อรับสายจะมีข้อความเสียงจากระบบตอบรับอัตโนมัติ หรือ Interactive Voice Response (IVR) ให้เหยื่อกดเพื่อติดต่อเจ้าหน้าที่ สังเกตได้ว่าสายต่าง ๆ ที่โทรเข้ามาหลอกลวงไม่ว่าจะแอบอ้างชื่อเป็นหน่วยงานใดก็ตาม มักจะมีรูปแบบเดียวกันคือ ให้กด “9” หรือให้กด “0” เพื่อติดต่อเจ้าหน้าที่ ซึ่งโปรแกรมสำเร็จรูปที่แก๊งคอลเซนเตอร์นำมาติดตั้งในระบบโทรศัพท์ สามารถเปลี่ยนไฟล์เสียงข้อความได้ตลอดเวลาเพื่อเปลี่ยนชื่อหน่วยงานและเนื้อหาในข้อความเสียงตามแต่สถานการณ์ที่คนร้ายสร้างขึ้นเพื่อหลอกลวงประชาชน โดยองค์ประกอบต่าง ๆ ที่เกี่ยวข้องกับการโทรหลอกลวงแสดงดังภาพที่ 1



ภาพที่ 1 การโทรหลอกลวงผ่านระบบโทรศัพท์แบบบริการเสียงผ่านอินเทอร์เน็ต หรือ VoIP

ที่มา: pch.vector (2020) (ดัดแปลงโดยผู้นิพนธ์)

ในด้านอุปกรณ์และโปรแกรม แก๊งคอลเซนเตอร์ส่วนใหญ่จะใช้อุปกรณ์โทรศัพท์ระบบ VoIP โดยมีระบบคอลเซนเตอร์ที่สามารถใช้โทรออกได้ครั้งละหลาย ๆ สาย โดยปัจจุบันการสร้างระบบคอลเซนเตอร์เพื่อใช้งานโทรเข้าออกสามารถทำได้โดยง่ายเพียงแค่มีเซิร์ฟเวอร์คอมพิวเตอร์ และนำซอฟต์แวร์ที่เป็น “Opensource” เช่น โปรแกรม Asterisk ซึ่งพัฒนาโดย Mr. Mark Spencer แห่งบริษัท Digium Inc. เมื่อปี พ.ศ. 2542 (บรรจบ สุขประภาภรณ์, 2550) มาใช้ร่วมกับโปรแกรมคอลเซนเตอร์สำเร็จรูป และจัดทำไฟล์เสียงที่สามารถบันทึกเปลี่ยนแปลงเนื้อหาได้ตามที่ต้องการมาลงในเซิร์ฟเวอร์คอมพิวเตอร์ หลังจากนั้นจึงเชื่อมต่ออุปกรณ์สำหรับกระจายคู่สายโทรศัพท์ภายในไปยังพนักงาน ซึ่งถูกเกณฑ์เข้ามาทำหน้าที่คอยรับสายที่ระบบโทรออกไป การโทรออกจากระบบคอลเซนเตอร์จะเป็นการโทรออกแบบอัตโนมัติโดยโปรแกรมหรือที่เรียกว่าบอตคอล (Bot call) หรือโรโบคอล (Robocall) ซึ่งสามารถโทรออกได้หลายพันสายภายในระยะเวลา 1 นาที (Department of Agriculture, Trade and Consumer Protection, n.d.) เมื่อมีเหยื่อรับสายแล้วกด “9” หรือกด “0” จะโอนสายไปยังพนักงานที่คอยรับสายอยู่แล้วเพื่อให้พูดคุยกับเหยื่อต่อไป

4.3 แหล่งข้อมูลหมายเลขโทรศัพท์ของเหยื่อแก๊งคอลเซนเตอร์

แก๊งคอลเซนเตอร์อาจจะได้หมายเลขปลายทางของเหยื่อมาจากแหล่งซื้อขายข้อมูลที่มีการลักลอบขายกัน (Lemzy, 2022) ซึ่งอาจเป็นข้อมูลที่ได้จาก

4.3.1 การลงทะเบียนบนระบบเว็บไซต์ หรือแพลตฟอร์มต่าง ๆ (Platform)

4.3.2 การเจาะข้อมูลในระบบอิเล็กทรอนิกส์ของจดหมายอิเล็กทรอนิกส์หรือฐานข้อมูลอื่น ๆ (Email hacking)

4.3.3 การส่งจดหมายอิเล็กทรอนิกส์หลอกลวง (Phishing email)

4.3.4 การใช้วิธีเกณฑ์คนมาค้นหาข้อมูลหมายเลขโทรศัพท์จากเครือข่ายสังคมออนไลน์หรือเว็บไซต์จัดหางาน (บริษัท ดีมีเตอร์ ไอซีที จำกัด, 2565)

เมื่อได้ข้อมูลหมายเลขมาแล้ว จะนำข้อมูลเข้าระบบคอลเซนเตอร์เพื่อให้โปรแกรมดึงหมายเลขสุ่มโทรออกไป รวมทั้งยังสามารถเอาข้อมูลดังกล่าวไปขายต่อให้กับแก๊งอื่น ๆ ได้อีกด้วย

ในบางกรณีแก๊งคอลเซนเตอร์อาจป้อนคำสั่งให้โปรแกรมคอลเซนเตอร์โทรออกไปยังหมายเลขชุดเดียวกันในเวลาเดียวกัน เช่น ตั้งค่าให้โทรไปยังกลุ่มหมายเลขที่ขึ้นต้นด้วย 0812345 โปรแกรมจะสุ่มโทรออกไปหมายเลขปลายทางตั้งแต่หมายเลข 0812345000 จนถึงหมายเลข 0812345999 ในเวลาเดียวกัน ซึ่งจะพบว่าในกรณีที่ผู้รับสายใช้หมายเลขโทรศัพท์เกาะกลุ่มเรียงกัน และอยู่ในสถานที่เดียวกัน ณ เวลาที่ระบบคอลเซนเตอร์โทรออกไป จะได้รับสายเรียกเข้ามาจากหมายเลขต้นทางเดียวกันในเวลาเดียวกัน โดยวิธีนี้ แก๊งคอลเซนเตอร์คาดหวังว่าโทรออกไปพร้อมกัน 1,000 สายนั้น ต้องมีหมายเลขปลายทางที่มีตัวตนและเปิดใช้งานอยู่บ้าง และอาจรับสายแล้วมีโอกาสตกเป็นเหยื่อได้

เป็นที่น่าสังเกตเมื่อถูกแก๊งคอลเซนเตอร์โทรหลอกลวงไป 1 ครั้งแล้ว จะถูกแก๊งคอลเซนเตอร์โทรมาก่อกวนอีกอย่างต่อเนื่องได้ ทั้งนี้ เนื่องมาจากแก๊งคอลเซนเตอร์มีการจัดเก็บหมายเลขที่ติดต่อได้แล้วไว้ในฐานข้อมูลสำหรับหมายเลขที่มีตัวตน และจะมีการนำข้อมูลดังกล่าวขายต่อให้กับแก๊งคอลเซนเตอร์อื่นนำไปใช้โทรหลอกลวงต่อไป (Department of Agriculture, Trade and Consumer Protection, n.d.) ในบางกรณีเหยื่อ 1 ราย อาจได้รับสายเรียกเข้าจากแก๊งคอลเซนเตอร์มากกว่า 1 ครั้ง ภายในระยะเวลา 1 วัน ทั้งนี้ เนื่องจากแก๊งคอลเซนเตอร์มีการขายหรือส่งต่อข้อมูลระหว่างกัน แต่ละแก๊งอาจโทรไปหาเหยื่อรายเดียวกัน

4.4 รูปแบบของการโทรหลอกลวง

4.4.1 การโทรหลอกลวงโดยปลอมแปลงหมายเลขต้นทาง

โทรศัพท์ระบบ VoIP เป็นระบบที่นิยมใช้กันอย่างแพร่หลาย และมีให้บริการอยู่ในทุกประเทศทั่วโลกแก๊งคอลเซนเตอร์จึงสามารถติดต่อขอใช้บริการเพื่อนำมาเชื่อมต่อเข้าระบบคอลเซนเตอร์ผ่านเครือข่ายอินเทอร์เน็ตได้ง่ายและสะดวกรวดเร็ว ซึ่งผู้ให้บริการแต่ละรายอาจมีการกำหนดเงื่อนไขการใช้งานที่แตกต่างกันขึ้นอยู่กับหลักเกณฑ์การขอใช้บริการของแต่ละประเทศ รวมถึงนโยบายของผู้ให้บริการแต่ละรายด้วย แต่เนื่องจากปัจจุบันตลาดบริการโทรศัพท์มีการแข่งขันสูงมาก จึงพบว่ามีผู้ให้บริการบางรายที่อนุญาตให้ระบบคอลเซนเตอร์สามารถโทรออกด้วยหมายเลขต้นทางเป็นหมายเลขอะไรก็ได้ตามที่ลูกค้าต้องการ เพื่อจูงใจลูกค้าให้เลือกใช้บริการของตน ดังนั้น แก๊งคอลเซนเตอร์จึงอาศัยช่องโหว่นี้เพื่อเป็น

ช่องทางโทรหลอกลวง โดยจะพยายามติดต่อขอใช้บริการจากผู้ให้บริการที่อนุญาตให้โทรออกที่สามารถปลอมแปลงหมายเลขต้นทางให้เป็นหมายเลขอะไรก็ได้ เพื่อหลบเลี่ยงการสกัดจากโครงข่ายปลายทางที่มักจะมีระบบตรวจสอบและระงับหมายเลขต้นทางที่ถูกปลอมแปลง ในบางกรณีแก๊งคอลเซนเตอร์จะปลอมแปลงหมายเลขต้นทางเป็นหมายเลขในประเทศเพื่อให้เหยื่อคิดว่าเป็นสายเรียกเข้าปกติ หรือปลอมแปลงหมายเลขต้นทางเป็นหมายเลขของหน่วยงานราชการ รวมถึงบริษัทที่น่าเชื่อถือเพื่อเพิ่มโอกาสในการรับสายและลวงให้เหยื่อเชื่อถือ (Lemzy, 2022) และหลงกลในที่สุด โดยที่เจ้าของหมายเลขนั้น ๆ ไม่ได้มีส่วนรู้เห็นใด ๆ

4.4.2 การโทรหลอกลวงด้วยเลขหมายต่างประเทศโดยมิได้ปลอมแปลงหมายเลขต้นทาง

บางกรณีแก๊งคอลเซนเตอร์อาจขอใช้บริการโทรออกจากผู้ให้บริการในประเทศที่ระบบคอลเซนเตอร์ตั้งอยู่ เช่น การตั้งแก๊งคอลเซนเตอร์ตั้งอยู่ที่ราชอาณาจักรกัมพูชาและขอใช้บริการโทรศัพท์จากผู้ให้บริการในราชอาณาจักรกัมพูชาเหมือนลูกค้าปกติทั่วไป ซึ่งผู้ให้บริการอาจไม่ได้มีส่วนรู้เห็นใด ๆ เนื่องจากเป็นการขอใช้บริการเหมือนลูกค้าทั่วไป หรืออาจไม่ได้ตรวจสอบข้อมูลลูกค้าให้ละเอียดว่าเป็นกลุ่มมิจฉาชีพที่เคยมีประวัติอาชญากรรมหรือไม่ (Hendricks, 2020) เมื่อแก๊งคอลเซนเตอร์นำหมายเลขที่ได้จดทะเบียนขอใช้บริการมาโทรหลอกลวง ทุกสายที่โทรออกไปหาเหยื่อปลายทางจะเห็นหมายเลขต้นทางขึ้นต้นด้วย “+855” หรือหากแก๊งคอลเซนเตอร์ไปซื้อบริการ VoIP จากประเทศอื่นที่กำหนดให้มีการจดทะเบียนเปิดใช้หมายเลขสำหรับโทรออกด้วย ก็จะเห็นเป็นหมายเลขที่ขึ้นต้นด้วยเครื่องหมาย “+” ตามด้วยรหัสของประเทศนั้น ๆ เช่น กรณีใช้บริการจากสาธารณรัฐประชาชนจีน จะเห็นหมายเลขต้นทางขึ้นต้นด้วย “+86” กรณีใช้บริการจากสหราชอาณาจักรจะเห็นหมายเลขต้นทางขึ้นต้นด้วย “+44” เป็นต้น

4.4.3 การโทรหลอกลวงโดยใช้ซิมการ์ด (SIM CARD) โทรศัพท์มือถือในประเทศ

แก๊งคอลเซนเตอร์บางรายอาจตั้งอยู่บริเวณชายแดนประเทศเพื่อนบ้านที่สามารถรับสัญญาณโทรศัพท์มือถือจากประเทศไทยได้เพื่อหลีกเลี่ยงการจับกุม จึงมีการจ้างคนไปเปิดซิมการ์ด เพื่อนำซิมการ์ดไปใส่ในอุปกรณ์แปลงสัญญาณโทรศัพท์มือถือ (SIM box) แล้วนำไปเชื่อมต่อเข้ากับระบบโทรศัพท์คอลเซนเตอร์หรือ Internet Protocol Private Branch Exchange (IP PBX) เพื่อโทรออก ซึ่งหนึ่งซิมสามารถใช้โทรออกได้หลายสายพร้อมกัน และอุปกรณ์ SIM Box ที่ใช้งานสามารถใส่ซิมการ์ดเข้าไปได้เป็นจำนวนมาก ดังแสดงในภาพที่ 2 ทำให้เมื่อนำ SIM Box ไปเชื่อมต่อผ่านอุปกรณ์ IP PBX เข้ากับระบบคอลเซนเตอร์ของแก๊งคอลเซนเตอร์แล้วสามารถโทรออกไปพร้อม ๆ กันได้ครั้งละหลายร้อยสาย (“ตร.ไซเบอร์บุกรังแก๊งคอลเซ็นเตอร์”, 2565) แก๊งคอลเซนเตอร์จึงเกณฑ์คนรับจ้างเปิดซิมการ์ดไว้จำนวนมาก หากซิมการ์ดใดถูกระงับจะเปลี่ยนไปใช้ซิมการ์ดใหม่ทันที โดยวิธีการนี้ทำให้ทุกสายที่โทรออกไปจะแสดงหมายเลขต้นทางเป็นหมายเลขของซิมการ์ดซึ่งเป็นหมายเลขในประเทศไทย และไม่มีเครื่องหมาย “+” นำหน้า ทำให้การแจ้งเตือนประชาชนให้ระวังสายที่โทรเข้ามาด้วยเครื่องหมาย “+” อาจไม่ได้ผล จึงทำให้เหยื่อเข้าใจว่าเป็นหมายเลขโทรศัพท์มือถือทั่วไป โอกาสที่จะรับสายแก๊งคอลเซนเตอร์มีมากขึ้นและทำให้ถูกหลอกลวงจนสำเร็จ

อย่างไรก็ตาม เมื่อผู้ให้บริการโทรศัพท์มือถือพบว่ามีการใช้งานจากซิมการ์ดใดผิดปกติเป็นจำนวนมากจะประสานงานแจ้งข้อมูลให้สำนักงานตำรวจแห่งชาติ โดยให้ข้อมูลแหล่งที่โทรออกเพื่อทำการจับกุม หากอยู่ในประเทศไทยก็จะสามารถเข้าไปจับกุมได้ ยกเว้นกรณีอยู่แนวชายแดนประเทศเพื่อนบ้านจะทำให้ยากต่อการจับกุมได้ อาจต้องประสานงานตำรวจสากลหรือความร่วมมือจากเจ้าหน้าที่ประเทศเพื่อนบ้านช่วยจับกุม ซึ่งที่ผ่านมากรณีการใช้ซิมการ์ดที่รับจ้างเปิดต่อเข้าอุปกรณ์ SIM box และ IP PBX โดยมีแหล่งที่ตั้งอยู่ในประเทศไทยนั้น มีหลายพื้นที่สามารถจับกุมได้ด้วยความร่วมมือระหว่างผู้ให้บริการโทรศัพท์มือถือและสำนักงานตำรวจแห่งชาติ และจากการจับกุมพบว่ามีการใช้งานซิมการ์ดผ่าน SIM box ต่อเข้ากับอุปกรณ์ IP PBX เป็นจำนวนมากเพื่อเชื่อมต่อสัญญาณผ่านระบบ VoIP ไปยังแก๊งคอลเซนเตอร์ที่อยู่ในต่างประเทศ (“ตร.ภ.5 ทลายแก๊งคอลเซ็นเตอร์”, 2565)

ภาพที่ 2 อุปกรณ์แปลงสัญญาณโทรศัพท์มือถือ (SIM box)

ที่มา: Noyes (2022)

กรณีตัวอย่างของการโทรหลอกลวงในลักษณะนี้ ซึ่งทุกภาคส่วนร่วมมือกันจนนำไปสู่การจับกุมผู้ร้าย คือกรณีตำรวจเข้าตรวจค้นสถานที่ต้องสงสัย 9 จุดในพื้นที่กรุงเทพมหานครเมื่อวันที่ 6 กรกฎาคม พ.ศ. 2565 โดยในกรณีนี้ส่วนหนึ่งเกิดจากความร่วมมือของประชาชนที่แจ้งเบาะแสผ่านเว็บไซต์ Thaipoliceonline.com ที่สำนักงานตำรวจแห่งชาติเปิดขึ้นมา เพื่อเป็นช่องทางให้ประชาชนแจ้งความร้องทุกข์คดีอาชญากรรมและข้อมูลบางส่วนจากผู้ให้บริการที่รายงานการใช้งานที่เข้าข่ายโทรหลอกลวง หลังจากได้ข้อมูลเบาะแสที่ตั้งของหมายเลขซิมการ์ดที่โทรออกแล้ว กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) จึงประสานงานไปยัง กสทช. และผู้ให้บริการเจ้าของเครือข่ายเพื่อตรวจสอบรายละเอียดการใช้งานและพิกัดส่งสัญญาณ จนสามารถจับกุมเครือข่ายแก๊งคอลเซนเตอร์ในพื้นที่กรุงเทพฯ ได้ 9 จุด ทั้งนี้จากการตรวจค้น ทั้ง 9 จุด สามารถยึดอุปกรณ์ IP PBX ได้ทั้งสิ้น 48 เครื่อง

ซึ่งประมาณการจากศักยภาพของอุปกรณ์จะสามารถโทรหลอกลวงได้ถึงเดือนละ 20 ล้านครั้ง (“บุกทลาย” แก๊งคอลเซ็นเตอร์” 9 จุดทั่ว กทม.”, 2565)

4.5 ช่องทางการโทรเข้าจากต่างประเทศ

โดยปกติโทรศัพท์ระหว่างประเทศจะถูกส่งผ่านเข้ามาทางชุมสายโทรศัพท์ระหว่างประเทศของผู้ให้บริการในประเทศไทย หรือที่เรียกว่า International Direct Dialing Gateway (IDD Gateway) ซึ่งในประเทศไทยมีผู้ให้บริการหลายรายด้วยกัน ได้แก่ NT, AWN, DTN และ TIC และจะมีสัญญาการให้บริการรับส่งแทรฟฟิก (Traffic) โทรศัพท์ระหว่างประเทศกับผู้ให้บริการในต่างประเทศ กรณีผู้ให้บริการในต่างประเทศส่งแทรฟฟิกโทรศัพท์ระหว่างประเทศเข้ามาทาง IDD Gateway เมื่อส่งถึงปลายทางผู้รับสายในประเทศไทยจะเห็นหมายเลขต้นทางมีเครื่องหมาย “+” นำหน้าทุกครั้ง แต่ปัจจุบันมีผู้ให้บริการในต่างประเทศหลายรายส่งแทรฟฟิกโทรศัพท์ระหว่างประเทศผ่านผู้ให้บริการที่เป็นผู้ได้รับใบอนุญาตให้บริการ VoIP ได้ด้วย ซึ่งแทรฟฟิกที่ส่งเข้ามาบางครั้งมีหมายเลขต้นทางที่ไม่ได้เป็นหมายเลขจริงหรือไม่มีรูปแบบตามมาตรฐาน ทำให้ผู้รับปลายทางอาจเห็นหมายเลขต้นทางเป็นหมายเลขแปลก ๆ เช่น ขึ้นต้นด้วย “870” และมีจำนวนตัวเลขมากกว่า 10 หลัก หรือบางครั้งอาจไม่แสดงหมายเลขใด ๆ ส่งผลให้การโทรหลอกลวงจากแก๊งคอลเซนเตอร์ที่ผ่านมาพบหมายเลขต้นทางที่โทรเข้ามาในรูปแบบที่หลากหลาย ซึ่งยากต่อการประชาสัมพันธ์แจ้งเตือนประชาชนให้ระวังสายที่โทรเข้ามาจากหมายเลขแบบไหนบ้าง

4.6 การระงับหมายเลขต้นทางที่โทรหลอกลวง

ในทางปฏิบัติผู้ให้บริการในประเทศไทยได้พยายามตรวจจับและระงับหมายเลขต้นทางที่แปลกปลอมหรือหมายเลขที่มีรูปแบบไม่ถูกต้อง หากตรวจพบหมายเลขต้นทางเป็นหมายเลขโทรศัพท์ประจำที่ของประเทศไทยเรียกเข้ามาจากต่างประเทศ เช่น หมายเลขที่ขึ้นต้นด้วย “+662” ซึ่งเป็นหมายเลขโทรศัพท์ประจำที่ในพื้นที่กรุงเทพฯ และปริมณฑล ผู้ให้บริการจะพิจารณาระงับไม่ให้หมายเลขกลุ่มนี้เรียกเข้ามาในประเทศได้ เนื่องจากในการใช้งานจริงของโทรศัพท์ประจำที่ไม่ควรจะมีการเรียกเข้ามาจากต่างประเทศได้ แตกต่างจากหมายเลขโทรศัพท์มือถือ เช่น หมายเลขที่ขึ้นต้นด้วย “+668” ซึ่งไม่อาจจะระงับการโทรได้โดยทันที เนื่องจากจะกระทบกับคนไทยจำนวนหนึ่งที่เดินทางไปต่างประเทศแล้วเปิดใช้งานบริการข้ามแดน (International roaming) เพื่อโทรกลับมายังประเทศไทย แก๊งคอลเซนเตอร์จึงอาศัยช่องทางนี้ในการปลอมแปลงหมายเลขต้นทางเป็นหมายเลขโทรศัพท์มือถือประเทศไทยซึ่งขึ้นต้นด้วย “+666” หรือ “+668” หรือ “+669” โทรเข้ามาแทน ทำให้ระยะหลังจะพบว่า มีสายโทรหลอกลวงซึ่งมีหมายเลขต้นทางเป็นหมายเลขโทรศัพท์มือถือประเทศไทยเพิ่มมากขึ้น

4.7 การสืบหาต้นทางที่แท้จริงของแก๊งคอลเซนเตอร์

เนื่องจากเหยื่อในประเทศไทยเป็นปลายทางที่ถูกหลอกลวง ในการตรวจสอบหาแหล่งที่มาของสายที่โทรเข้ามาหลอกลวง จะต้องตรวจสอบย้อนจากปลายทางซึ่งเป็นเหยื่อว่าใช้โทรศัพท์ของผู้ให้บริการรายใด และแจ้งผู้ให้บริการรายนั้นตรวจสอบย้อนกลับไปว่ารับแทรฟฟิกมาจากโครงข่ายของผู้ให้บริการใดอีกทอดหนึ่ง โดยจะต้องทำการไล่ย้อนกลับไปเป็นทอด ๆ และส่วนใหญ่จะสิ้นสุดที่ผู้ให้บริการในต่างประเทศ ซึ่งเป็นผู้ให้บริการที่รับและส่งแทรฟฟิกดังกล่าวมาเท่านั้น ไม่สามารถไล่ย้อนต่อไปได้อีกว่าผู้ให้บริการในต่างประเทศรับมาจากที่ใด เนื่องจากเป็นข้อมูลทางด้านการค้าที่ผู้ให้บริการในต่างประเทศจะอ้างเหตุผลเพื่อปฏิเสธการตรวจสอบ และในบางกรณีผู้ให้บริการในต่างประเทศก็รับแทรฟฟิกต่อมาเป็นช่วง ๆ จึงไม่สามารถทราบได้ว่าต้นทางที่แท้จริงอยู่ที่ใด ยกเว้นกรณีที่มีการใช้งานหมายเลขจริงของประเทศต้นทางที่แก๊งคอลเซนเตอร์ตั้งอยู่ ก็อาจจะขอความร่วมมือผู้ให้บริการในประเทศนั้นตรวจสอบว่าแก๊งคอลเซนเตอร์ตั้งอยู่ที่ใดเพื่อเป็นเบาะแส ให้ตำรวจสากลเข้าไปจับกุมได้ แต่ทั้งนี้ต้องได้รับความร่วมมืออย่างดีจากผู้ให้บริการในต่างประเทศด้วย เนื่องจากบางกรณีผู้ให้บริการในต่างประเทศ ก็ไม่สามารถเปิดเผยข้อมูลการใช้งานของลูกค้าให้หน่วยงานอื่นได้ เพราะติดขัดข้อกฎหมายในลักษณะเดียวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act B.E. 2562 หรือ PDPA)

4.8 การดำเนินการแก้ไขปัญหาการโทรหลอกลวงในประเทศไทย

4.8.1 การดำเนินงานของ กสทช. ในฐานะเป็นผู้กำกับการให้บริการโทรคมนาคมของประเทศไทย

สำนักงาน กสทช. ได้แต่งตั้งคณะทำงานพหุภาคีเพื่อแก้ปัญหาแก๊งโทรศัพท์ (Call center) และข้อความสั้น (SMS) หลอกลวง โดยมีผู้แทนจากหน่วยงานต่าง ๆ เช่น สำนักงานตำรวจแห่งชาติ ธนาคารแห่งประเทศไทย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ผู้ให้บริการโทรศัพท์ทุกรายร่วมเป็นคณะทำงาน และได้มีการประชุมพิจารณากำหนดแนวทางการแก้ไขปัญหา โดยศึกษาข้อมูลจากกรณีที่เกิดขึ้นกับประเทศต่าง ๆ มาเป็นแนวทางดำเนินการ เช่น กรณีศึกษาของสหราชอาณาจักร เครือรัฐออสเตรเลีย เป็นต้น และได้ออกมาตรการต่าง ๆ โดยขอความร่วมมือจากผู้ให้บริการให้ดำเนินการ ดังนี้

4.8.1.1 การระงับสายที่เรียกเข้าจากต่างประเทศซึ่งมีหมายเลขต้นทางเป็นหมายเลขโทรศัพท์พื้นฐานของประเทศไทย

4.8.1.2 การระงับสายที่เรียกเข้าจากต่างประเทศซึ่งมีรูปแบบของหมายเลขต้นทางไม่ถูกต้อง เช่น หมายเลขสั้น รหัสประเทศที่ยังไม่ได้ถูกกำหนดให้ใช้งาน เป็นต้น

4.8.1.3 การกำหนดให้ทุกสายที่เรียกเข้ามาจากต่างประเทศ จะต้องมีเครื่องหมาย “+” นำหน้าหมายเลขต้นทางทุกครั้ง

4.8.1.4 การประชาสัมพันธ์แจ้งเตือนรูปแบบการโทรหลอกลวงและรูปแบบของหมายเลขที่โทรหลอกลวง

4.8.1.5 การจัดทำรายงานหมายเลขที่พบว่ามีการใช้โทรหลอกลวง รวมทั้งการรายงานข้อมูลการหลอกลวงผ่านทางข้อความสั้น (SMS) ด้วย

4.8.1.6 จัดทำระบบแจ้งเตือนกรณีมีสายเรียกเข้าจากต่างประเทศ เพื่อให้ผู้รับสายระมัดระวังในการสนทนากับผู้ที่โทรติดต่อเข้ามา หากไม่ได้เป็นบุคคลที่รู้จักจะได้วางสายทันที รวมทั้งให้สามารถตั้งค่าปฏิเสธสายที่เรียกเข้าจากต่างประเทศได้ด้วย โดยให้ผู้ให้บริการต่าง ๆ พิจารณาแนวทางที่สามารถดำเนินการได้รวดเร็ว ผู้ให้บริการสามารถทำเป็นแอปพลิเคชันโทรศัพท์มือถือ (Mobile application) ให้ผู้ใช้บริการดาวน์โหลดมาไว้ในมือถือเพื่อเป็นเครื่องมือช่วยแจ้งเตือนกรณีมีสายเรียกที่เรียกเข้าจากต่างประเทศ และสามารถตั้งค่าปฏิเสธการรับสายที่เรียกเข้ามาจากต่างประเทศได้ด้วย หรือผู้ให้บริการอาจทำจากระบบชุมสายโดยไม่ต้องอาศัยแอปพลิเคชันโทรศัพท์มือถือก็ได้ โดยให้ผู้ใช้บริการสมัครเลือกรับสายที่เรียกเข้าจากต่างประเทศผ่าน Unstructured Supplementary Service Data (USSD) ขึ้นอยู่กับความพร้อมของผู้ให้บริการแต่ละราย

4.8.1.7 กำหนดมาตรการจำกัดจำนวนซิมหรือหมายเลขโทรศัพท์มือถือที่ขอเปิดใช้งานคนละไม่เกิน 5 เลขหมาย เพื่อป้องกันมิจฉาชีพหรือผู้รับจ้างจากมิจฉาชีพที่ต้องการเปิดซิมการ์ดหรือหมายเลขเป็นจำนวนมาก ๆ เพื่อนำไปใช้ในการโทรหลอกลวง

โดยปัจจุบันทุกหน่วยงานที่เกี่ยวข้องได้ให้ความร่วมมือในการดำเนินการตามมาตรการต่าง ๆ ที่คณะทำงานฯ กำหนดเพื่อช่วยสกัดกั้นหรือลดการโทรหลอกลวง ทำให้แนวโน้มจำนวนเหยื่อที่ถูกโทรหลอกลวงเริ่มน้อยลง สะท้อนให้เห็นถึงความร่วมมือต่าง ๆ ที่แต่ละหน่วยงานที่เกี่ยวข้องได้ดำเนินการมาได้อย่างเหมาะสมและมีประสิทธิภาพที่น่าพึงพอใจจนเห็นผลชัดเจน ทำให้แก๊งคอลเซนเตอร์ได้หันไปใช้วิธีอื่น ๆ ในการหลอกลวงแทน เช่น การส่งจดหมายปลอมไปยังที่อยู่ของเหยื่อ

4.8.2 การดำเนินการของผู้ให้บริการโทรศัพท์ในประเทศไทย

โครงข่ายหรือผู้ให้บริการในประเทศไทยที่มีแทรฟฟิกการโทรหลอกลวงสามารถเรียกผ่านเข้ามาได้จะประกอบด้วย ผู้ให้บริการโทรศัพท์ระหว่างประเทศ (IDD) บริการโทรศัพท์ประจำที่ (Fixed line) และบริการโทรศัพท์มือถือ (Mobile) ซึ่งเป็นผู้ให้บริการที่ได้รับใบอนุญาตประเภทที่ 3 ที่มีโครงข่ายเป็นของตนเอง ได้แก่ NT, AWN, DTN, และ True รวมทั้งผู้ให้บริการ VoIP ที่ได้รับใบอนุญาตประเภทที่ 1 ซึ่งไม่มีโครงข่ายเป็นของตนเองแต่สามารถรับแทรฟฟิกโทรศัพท์ระหว่างประเทศที่โทรจากประเทศต่าง ๆ

เข้ามาได้ด้วย โดยผู้ให้บริการทุกรายได้ร่วมมือกับ กสทช. ในการตรวจสอบแทรฟฟิกที่เรียกเข้ามาจากต่างประเทศและกำหนดให้ทุกสายที่โทรเข้ามาจะต้องมีรูปแบบของหมายเลขต้นทางที่มีเครื่องหมาย “+” นำหน้า เพื่อให้ผู้รับสายได้สังเกตเห็นว่าเป็นสายที่โทรมาจากต่างประเทศและระมัดระวังในการรับสาย และมีระบบตรวจสอบการใช้งานที่ผิดปกติหรือ “Spam call” หากพบว่ามีหมายเลขใดที่โทรเข้ามาผิดปกติหรือเข้าข่าย “Spam call” เช่น โทรจากหมายเลขต้นทางเดียวกันในเวลาเดียวกันไปยังปลายทางหลายเลขหมาย จะประสานงานตรวจสอบกับหน่วยงานที่เกี่ยวข้องเพื่อยืนยันเป็นการใช้งานจริงหรือไม่ หากเป็นการโทรหลอกลวง หรือก่อกวนจะประสานงานระงับหมายเลขต้นทางนั้น ๆ หรือกลุ่มหมายเลขต้นทางนั้นไว้ เพื่อสกัดไม่ให้สามารถโทรเข้ามาได้อีก โดยตรวจสอบย้อนกลับไปยังต้นทางที่ส่งแทรฟฟิกมาเพื่อให้ดำเนินการระงับที่ต้นทางด้วย อย่างไรก็ตามแก๊งคอลเซนเตอร์ก็ยังคงพยายามหลีกเลี่ยงการตรวจสอบโดยการสุ่มโทรจากหมายเลขต้นทาง 1 เลขหมายไปยังหลายหมายเลขปลายทาง 1 เลขหมาย ไม่ซ้ำกันทำให้หลุดจากระบบตรวจสอบได้ แต่ละผู้ให้บริการจึงต้องหาวิธีสกัดเพื่อไม่ให้โทรเข้ามาหลอกลวงได้สะดวกอีก พร้อมกับพยายามหาวิธีการต่าง ๆ ที่จะช่วยปกป้องผู้ใช้งานโทรศัพท์มือถือ เช่น จัดระเบียบสายเรียกเข้าจากต่างประเทศทุกสายต้องมีเครื่องหมาย “+” นำหน้า เพื่อให้เป็นที่สังเกตว่า เป็นสายที่โทรมาจากต่างประเทศ ให้ระมัดระวังในการรับสาย รวมทั้งจัดทำระบบรองรับการปฏิเสธสายที่โทรเข้าจากต่างประเทศ โดยให้ผู้ใช้บริการสามารถเลือกปฏิเสธไม่รับสายจากต่างประเทศได้

4.9 การแก้ปัญหาของประเทศต่าง ๆ

หลายประเทศก็มีมาตรการดำเนินการที่คล้ายกับประเทศไทย คือ สกัดการโทรเข้าจากหมายเลขต้นทางที่ไม่ถูกต้อง มีระบบตรวจสอบและระงับหมายเลขที่พบว่ามีการปลอมแปลงมา หรือมีพฤติกรรมการโทรที่ผิดปกติ ตัวอย่างเช่น AT&T ซึ่งเป็นผู้ให้บริการในสหรัฐอเมริกา รายงานว่าสามารถระงับโรโบคอลได้ถึง 1 พันล้านสาย (AT&T, 2021) ในขณะที่ Telstra ซึ่งเป็นผู้ให้บริการในเครือรัฐออสเตรเลีย แจ้งว่าได้ระงับการโทรหลอกลวงไปแล้วถึง 13 ล้านสาย (Devine, 2021)

อย่างไรก็ตามพบว่า บางประเทศมีมาตรการที่เข้มงวด กล่าวคือ เมื่อพบว่ามีการโทรเข้ามาจากหมายเลขต้นทางใดซ้ำ ๆ ในเวลาเดียวกันหรือใกล้เคียงกัน จะระงับหมายเลขต้นทางนั้นทันที โดยไม่สนใจว่าจะเป็นการใช้งานจริงหรือไม่ เช่น สาธารณรัฐประชาชนจีน หากมีหมายเลขต้นทางที่โทรเข้าสาธารณรัฐประชาชนจีนด้วยหมายเลขเดิมซ้ำ ๆ จะถูกระงับหมายเลขต้นทางนั้นทันที ซึ่งในการใช้งานจริงของผู้ใช้บริการที่เป็นโรงแรมหรือบริษัทใหญ่ ๆ ส่วนใหญ่ใช้หมายเลขที่โทรออกเป็นหมายเลขนำหมู่ (Pilot number) ทำให้ได้รับผลกระทบจากมาตรการเข้มงวดดังกล่าว จะต้องแจ้งขอให้ผู้ให้บริการในสาธารณรัฐประชาชนจีนจัดทำทะเบียนหมายเลขต้นทางที่ยืนยันว่าเป็นการใช้งานจริง (Whitelist) จึงสามารถใช้งานต่อได้ และบางประเทศจะไม่อนุญาตให้หมายเลขต้นทางที่เป็นหมายเลขของประเทศตนเองโทรเข้ามาจากต่างประเทศได้ เช่น หมายเลขต้นทางเป็นหมายเลขของราชอาณาจักรกัมพูชาขึ้นต้นด้วย “+855” จะไม่อนุญาตให้เข้าไปยังหมายเลขปลายทางของหมายเลขราชอาณาจักรกัมพูชา โดยไม่คำนึงถึงผลกระทบที่อาจเกิดกับคนราชอาณาจักรกัมพูชาที่เดินทางไปต่างประเทศ ซึ่งมีความจำเป็นต้องใช้บริการโทรศัพท์ข้ามแดนอัตโนมัติเพื่อโทรกลับประเทศหรือไม่

4.10 แนวทางการป้องกันตัวเองจากแก๊งคอลเซนเตอร์

เนื่องจากเป็นการยากที่จะสามารถสกัดหรือระงับหรือปราบปรามแก๊งคอลเซนเตอร์ให้หมดสิ้นได้ ประชาชนทุกคนจึงจำเป็นจะต้องศึกษาเรียนรู้วิธีป้องการตัวเอง เพื่อไม่ให้ตกเป็นเหยื่อของแก๊งคอลเซนเตอร์ได้ โดยจะต้องติดตามข่าวสารและการแจ้งเตือนต่าง ๆ จากทั้งหน่วยงานภาครัฐและสื่อต่าง ๆ รวมทั้งศึกษาหาวิธีตรวจสอบข้อมูลให้ละเอียดรอบคอบก่อนการทำธุรกรรมใด ๆ

4.10.1 ควรศึกษาความรู้เบื้องต้นเกี่ยวกับรูปแบบของหมายเลขโทรศัพท์ต้องสงสัย เพื่อทำการวิเคราะห์และประเมินความเสี่ยงด้วยตนเองก่อนรับสายโทรศัพท์ เช่น หมายเลขต้นทางที่ขึ้นต้นด้วยเครื่องหมาย “+” เป็นโทรศัพท์มาจากต่างประเทศ หากไม่มีญาติหรือธุรกิจในต่างประเทศ ไม่ควรรับสาย

4.10.2 ใช้เครื่องมือหรือแอปพลิเคชันต่าง ๆ ตรวจสอบหมายเลขโทรศัพท์แปลกปลอมที่โทรเข้ามา เช่น กูเกิล (Google) เฟซบุ๊ก (Facebook) ไลน์ (Line) และ ฮูสคอล (Whoscall) ซึ่งแต่ละแอปพลิเคชันมีวิธีการตรวจสอบแตกต่างกัน ดังนี้

ตารางที่ 1 เครื่องมือตรวจสอบหมายเลขต้นทางและวิธีการตรวจสอบ

เครื่องมือตรวจสอบ	วิธีการตรวจสอบ
กูเกิล	นำหมายเลขโทรศัพท์ที่โทรเข้ามาค้นหา เพื่อดูว่าเคยมีประวัติถูกโพสต์แจ้งเตือนว่าเป็นมิจฉาชีพหรือไม่
เฟซบุ๊ก	นำหมายเลขโทรศัพท์ที่โทรเข้ามาค้นหาเพื่อดูว่ามีการลงทะเบียนไว้หรือไม่ ผูกบัญชีไว้กับใครและหากเคยมีประวัติการหลอกลวงก็อาจจะพบการโพสต์เตือนว่าเป็นมิจฉาชีพ
ไลน์	นำหมายเลขโทรศัพท์ที่โทรเข้ามาค้นหาเพื่อดูว่าเป็นหมายเลขที่มีตัวตนหรือไม่
ฮูสคอล	ฮูสคอลเป็นแอปพลิเคชันที่สามารถติดตั้งบนโทรศัพท์มือถือ ที่เปิดให้ผู้ใช้รายงานหมายเลขโทรศัพท์ว่าเป็นหมายเลขของใครและปลอดภัยหรือไม่ เมื่อหมายเลขที่ถูกรายงานเรียกเข้ามาแอปพลิเคชันจะแสดงข้อมูลที่ถูกรายงานไว้ทันที

ที่มา: สำนักงานตำรวจแห่งชาติ (2565)

4.10.3 หากได้มีการรับสายโทรศัพท์ที่โทรเข้ามาแล้วจะต้องมีสติในการรับฟังข้อมูลและวิเคราะห์ข้อมูลที่ได้รับอย่างมีเหตุผล ไม่ควรตื่นตระหนกตกใจ หวาดกลัวหรือตื่นเต้นไปกับข้อมูลนั้น หากข้อมูลที่ได้ฟังมาไม่ได้มีส่วนเกี่ยวข้องใด ๆ ให้วางสายทันที หรือหากไม่มั่นใจ ให้แจ้งไปที่สายต้นทางว่าจะโทรติดต่อกลับไปเอง

4.10.4 ไม่ควรให้ข้อมูลส่วนบุคคล หรือรหัสผ่านต่าง ๆ กับสายที่โทรเข้ามา เนื่องจากหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน ไม่มีนโยบายโทรสอบถามข้อมูลส่วนบุคคลของลูกค้าทางโทรศัพท์ (ธนาคารแห่งประเทศไทย, 2557)

5. การอภิปรายผล

การโทรหลอกลวงเป็นปัญหาใหญ่และสร้างความหนักใจให้กับรัฐบาล หน่วยงานต่าง ๆ ที่รับผิดชอบรวมถึงผู้ให้บริการทั่วโลก การศึกษาพบว่าแนวทางแก้ปัญหาที่ประเทศไทยดำเนินอยู่ในตอนนี้ ไม่ว่าจะเป็นการตรวจจับเพื่อระงับหมายเลขแปลกปลอม หรือการสกัดหมายเลขต้นทางที่ปลอมแปลงไม่ให้สามารถโทรเข้ามาหลอกลวงได้ ยังไม่สามารถแก้ปัญหาการโทรหลอกลวงให้หมดสิ้นไปได้ เป็นเพียงการสกัดไว้ได้ชั่วขณะเท่านั้น โดยมีปัจจัยที่สนับสนุนการแก้ปัญหานี้คือ

1. หน่วยงานผู้กำกับดูแลที่ให้แนวทางและนโยบายที่เกี่ยวข้อง กำหนดแนวทางและนโยบายต่าง ๆ อย่างรัดกุมและเท่าทันต่อสถานการณ์ของปัญหา

2. ผู้ให้บริการที่ดำเนินการตรวจสอบ คัดกรองและสกัดกั้นอย่างจริงจัง

3. เจ้าหน้าที่ผู้บังคับใช้กฎหมายที่ติดตามและจับกุมคนร้ายอย่างสุดความสามารถ

อย่างไรก็ตาม ปัจจัยที่เป็นอุปสรรคต่อการแก้ปัญหา คือ

1) คุณสมบัติของระบบโทรศัพท์แบบ VoIP ที่สามารถกำหนดให้แสดงหมายเลขต้นทางเป็นหมายเลขใด ๆ ก็ได้ ซึ่งทำให้แก๊งคอลเซนเตอร์สามารถสร้างหมายเลขโทรศัพท์ใหม่แทนหมายเลขที่ถูกสกัดได้ทันที

2) การปลอมแปลงหมายเลขที่โทรหลอกลวงเป็นหมายเลขโทรศัพท์มือถือของประเทศไทยและใช้เทคนิคการสุ่มโทรออกจากหมายเลขต้นทางที่หลากหลายโดยไม่ซ้ำกันในเวลาเดียวกัน ทำให้ยากต่อการแยกว่าเป็นการใช้งานจริงจากคนไทยที่เดินทางไปต่างประเทศแล้วใช้บริการโทรข้ามแดนระหว่างประเทศโทรกลับมาหรือไม่

3) แหล่งที่ตั้งของระบบคอลเซนเตอร์ เนื่องจากแก๊งคอลเซนเตอร์มักก่อเหตุนอกเขตอำนาจของหน่วยงานในประเทศที่เหยื่ออาศัยอยู่ จึงเป็นอุปสรรคในการสืบหาและติดตามตัวคนร้ายมาดำเนินคดี

4) การรับรู้ข่าวสารของคน เนื่องจากยังมีคนจำนวนหนึ่งที่ไม่ได้ติดตามข่าวสารใด ๆ ทำให้ตกเป็นเหยื่อของแก๊งคอลเซนเตอร์ได้ง่าย

6. บทสรุป

ความก้าวหน้าทางเทคโนโลยีของระบบโทรศัพท์ในปัจจุบัน ซึ่งสามารถใช้งานผ่านเครือข่ายอินเทอร์เน็ต หรือ Voice over Internet Protocol หรือ VoIP นั้น ทำให้สามารถใช้งานได้ง่ายและสะดวกทุกที่ที่สามารถเข้าถึงอินเทอร์เน็ต นอกจากนี้ ยังช่วยประหยัดค่าใช้จ่ายและตอบสนองการใช้งานได้หลากหลาย แต่ก็มีมิจฉาชีพอาศัยคุณสมบัติของเทคโนโลยีดังกล่าวมาเป็นช่องทางในการโทรหลอกลวง สร้างความเสียหายให้กับประเทศต่าง ๆ เป็นจำนวนมาก และเป็นการยากที่จะสามารถสกัดหรือระงับให้หมดไปได้ เนื่องจากมิจฉาชีพจะพยายามปรับเปลี่ยนรูปแบบเพื่อเลี่ยงการจับกุมหรือการสกัดทุกวิธี ด้วยผลจากการหลอกลวงแต่ละครั้งสามารถได้รับเงินจากเหยื่อแต่ละรายเป็นจำนวนมาก จึงทำให้มิจฉาชีพยังคงแสวงหาช่องทางที่จะหลอกลวงต่อไป สำหรับแนวทางแก้ไขปัญหาที่เกิดขึ้นในประเทศไทยปัจจุบันยังไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพมากนัก ดังนั้น เพื่อให้การแก้ไขปัญหาเกิดประสิทธิภาพมากยิ่งขึ้น หน่วยงานต่าง ๆ อาจต้องพิจารณาทางอื่นเพิ่มเติมเพื่อสกัดกั้นการโทรเข้าจากต่างประเทศที่เข้าข่ายการโทรหลอกลวง เช่น จะต้องกำหนดให้ผู้ให้บริการโทรศัพท์เปิดช่องการให้ผู้ใช้บริการสามารถสมัครการปฏิเสธรับสายที่เรียกเข้ามาจากต่างประเทศได้ด้วยตนเอง และกำหนดให้ผู้ให้บริการโทรศัพท์ระหว่างประเทศที่รับทราฟฟิกโทรศัพท์ระหว่างประเทศเข้ามา ต้องให้มีรูปแบบหมายเลขต้นทาง (Caller ID format) เป็นมาตรฐานโดยต้องมีเครื่องหมาย “+” นำหน้าทุกครั้ง เพื่อให้ผู้ใช้บริการทราบว่าเป็นสายที่เรียกเข้ามาจากต่างประเทศ และสามารถปฏิเสธการรับสายได้อัตโนมัติเมื่อได้สมัครใช้บริการปฏิเสธการรับสายที่เรียกเข้าจากต่างประเทศไว้ นอกจากนี้ หน่วยงานต่าง ๆ ทุกภาคส่วน จะต้องร่วมมือกันประชาสัมพันธ์ให้เข้าถึงประชาชนให้มากที่สุด เพื่อให้ระมัดระวังและสามารถป้องกันตัวเองจากแก๊งคอลเซนเตอร์ได้

7. ข้อเสนอแนะ

7.1 ข้อเสนอแนะสำหรับการศึกษาในอนาคต

ด้วยคุณสมบัตินานาประการของระบบโทรศัพท์แบบ VoIP คงไม่อาจจะเลิกใช้ระบบโทรศัพท์แบบ VoIP แล้วกลับไปใช้ระบบโทรศัพท์แบบแอนะล็อก (Analog) ตามเดิมได้ ดังนั้น แนวทางป้องกันความเสียหายที่จะเกิดกับผู้ใช้บริการที่ง่ายและทำได้ทันที นอกจากหน่วยงานที่เกี่ยวข้อง ได้แก่ กสทช. ผู้ให้บริการ สำนักงานตำรวจแห่งชาติ และธนาคารได้ร่วมมือกันสกัดกั้นแทรฟฟิกหลอกลวง และจับกุมทั้งซิมการ์ดและบัญชีรับจ้างแล้ว ยังต้องอาศัยความร่วมมือจากทุกภาคส่วนในการช่วยกันประชาสัมพันธ์แจ้งเตือนอย่างต่อเนื่อง เพื่อให้เข้าถึงประชาชนได้มากที่สุด

7.2 ข้อเสนอแนะเชิงนโยบายสำหรับกิจการสื่อสาร

แก๊งคอลเซนเตอร์ส่วนใหญ่จะตั้งอยู่นอกประเทศใช้โทรศัพท์ระบบ VoIP โทรเข้ามา ดังนั้น หน่วยงานผู้ให้บริการทุกรายจำเป็นจะต้องจัดระเบียบแทรฟฟิกโทรศัพท์ระหว่างประเทศที่เรียกเข้ามาจากประเทศต่าง ๆ ทั้งระบบปกติและระบบ VoIP ให้มีรูปแบบการแสดงหมายเลขต้นทางที่เรียกเข้าเป็นรูปแบบมาตรฐาน คือ จะต้องมีเครื่องหมาย “+” นำหน้าทุกครั้ง และผู้ให้บริการอาจต้องพัฒนาระบบโครงข่ายให้สามารถรองรับการปฏิเสธสายเรียกเข้าจากต่างประเทศสำหรับผู้ใช้บริการที่ไม่เคยมีญาติหรือคนรู้จักอยู่ในต่างประเทศ โดยกรณีที่สามารถระบุชัดเจนได้ว่าสายที่โทรเข้ามาเป็นสายที่มาจากต่างประเทศ เช่น มีเครื่องหมาย “+” นำหน้า ทั้งนี้จะต้องให้ผู้ใช้บริการสามารถเลือกสมัครหรือยกเลิกการปฏิเสธสายเรียกเข้าจากต่างประเทศได้ด้วยตนเอง ซึ่งอาจเปิดช่องทางให้ผู้ใช้บริการสมัครผ่าน USSD เช่น กดเครื่องหมาย “*” ตามด้วยรหัสบริการ นอกจากนี้ ทุกโครงข่ายอาจต้องมีระบบตรวจสอบการโทรใช้งานที่ผิดปกติหรือเข้าข่ายการโทรหลอกลวง เพื่อแจ้งเตือนให้ผู้ให้บริการสามารถทำการระงับได้รวดเร็ว โดยหากสามารถเก็บรูปแบบการใช้งานที่ผิดปกติหรือรูปแบบเดิมซ้ำ ๆ (Pattern) เพื่อให้ระบบเรียนรู้แบบปัญญาประดิษฐ์ (Artificial Intelligence: AI) แล้วต่อยอดเพื่อให้สามารถแจ้งเตือนและระงับได้รวดเร็วได้ ก็จะยิ่งช่วยให้การป้องกันและแก้ไขปัญหาการโทรหลอกลวงได้อย่างมีประสิทธิภาพมากขึ้น

รายการเอกสารอ้างอิง

ตำรวจไซเบอร์บุกรังแก๊งคอลเซ็นเตอร์ 14 แห่งเมืองชลบุรี ยึดของกลางเพียบ. (2565, 12 กรกฎาคม). *เดลินิวส์ออนไลน์*. https://www.dailynews.co.th/news/1241856/

ตำรวจภูธรภาค 5 ทลายแก๊งคอลเซ็นเตอร์เช่าพูลวิลล่าหรูเชียงใหม่หลอกเหยื่อคนไทย. (2565, 11 พฤษภาคม). *ไทยรัฐออนไลน์*. https://www.thairath.co.th/news/crime/2389781

ธนาคารกรุงเทพ จำกัด (มหาชน). (ม.ป.ป.). *รู้ทันภัยร้าย อันตรายแก๊ง Call Center*. https://www.bangkokbank.com/th-TH/Personal/Tips-and-Insights/Gang-CallCenter

ธนาคารแห่งประเทศไทย. (2557, เมษายน). *กลโกงทางโทรศัพท์*. ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน. www.1213.or.th/th/finfrauds/callcenter/Pages/Callcenter.aspx

ธนาคารแห่งประเทศไทย. (2565). Financial Fraud: กลโกงทางการเงินใกล้ตัวกว่าที่คิด. *PAYMENT INSIGHT : Bi-monthly Report, 14*, 2. https://bit.ly/3yvluMW

บรรจบ สุขประภาภรณ์. (2550). *เทคโนโลยีการสื่อสารโทรศัพท์ด้วยระบบ VoIP*. คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏเชียงราย. https://www.intech.crru.ac.th/articleind/36.pdf

บริษัท ดีมีเตอร์ ไอซีที จำกัด. (2565, 4 เมษายน). *เผย 7 ช่องทางสำรวจแก๊งมิจฉาชีพอย่าง call center เอาเบอร์โทรศัพท์ของคุณมาจากไหน? พร้อมแนวทางป้องกัน*. https://www.dmit.co.th/th/google-workspace-updates-th/7-channels-that-give-info-to-fake-call-center/

บุกทลาย “แก๊งคอลเซ็นเตอร์” 9 จุดทั่วกทม. อึ้ง!โทรป่วนได้ 20 ล้าน ครั้ง/เดือน. (2565, 6 กรกฎาคม). *คมชัดลึกออนไลน์*. https://www.komchadluek.net/news/521456

ราชบัณฑิตยสถาน. (2554). *พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. ๒๕๕๔*. https://dictionary.orst.go.th

สำนักงานตำรวจแห่งชาติ. (2565, 5 มีนาคม). วิธีตรวจสอบเบอร์โทรมิจฉาชีพ [แนบรูปภาพ] [อัปเดตสถานะ]. Facebook. https://www.facebook.com/photo/?fbid=326152719558025&set=a.306545458185418

AT&T. (2021, June 22). *AT&T now blocking or labeling more than 1 billion Robocalls per month.* https://about.att.com/story/2021/robocalls.html

Department of Agriculture, Trade and Consumer Protection. (n.d.). *DATCP home consumer protection fact sheet - Robocalls*. https://datcp.wi.gov/Pages/Publications/Robocalls300.aspx

Devine, N. (2021, June 15). *We’re now blocking over 13 million scam calls a month*. Telstra Exchange. https://exchange.telstra.com.au/were-now-blocking-over-13-million-scam-calls-a-month

Hale, J. (2022, June 18). *What is a non-fixed VoIP phone system?*. Business News Daily. https://www.businessnewsdaily.com/articles/non-fixed-voip

Hendricks, K. (2020, June 10). *Investigating scam phone calls*. FBI: Law Enforcement Bulletin. https://leb.fbi.gov/articles/featured-articles/investigating-scam-phone-calls

Hopewell, L. (2021, August 26). *What is call spoofing? How scammers are using your phone number for fake calls*. Telstra Exchange. https://exchange.telstra.com.au/fake-calls- what-is-call-spoofing/

Lemzy, A. (2022, March 15). *How do Scammers get your cellphone number and how to protect yourself*. TextMagic. https://www.textmagic.com/blog/how-do-scammers-get-your-cellphone-number/

Noyes, J. (2020, August 11). *Phishing fraudsters used SIM box to fleece hundreds of victims, police allege*. The Sydney Morning Herald. https://www.smh.com.au/national/nsw/phishing-fraudsters-used-sim-box-to-fleece-hundreds-of-victims-police-allege-20220811-p5b8xv.html

pch.vector. (2020, June 30). *Customer support representatives working in call center*. Freepik.com. https://www.freepik.com/free-vector/customer-support-Representatives-working-callcenter_9174514.htm#page=2&query=call&position=30&from_View=search&track=sph

TrapCall. (2017, August 12). *How to stop spam calls: The tricks Scammers don't want you to know*. Trapcall. https://www.trapcall.com/blog/how-to-stop-spam-calls/