# การหลอกลวงทางไซเบอร์: กรณีแก๊งคอลเซ็นเตอร์

ศรัณย์รัฐ เนาวอุไรรัตนา

งานนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรรัฐศาสตรมหาบัณฑิต
สาขาวิชาการบริหารงานยุติธรรมและสังคม
คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา
2567

มหาวิทยาลัยบูรพา
BURAPHA UNIVERSITY

มหาวิทยาลัยบูรพา
BURAPHA UNIVERSITY

# การหลอกลวงทางไซเบอร์: กรณีแก๊งคอลเซ็นเตอร์

ศรัณย์รัฐ เนาวอุไรรัตนา

งานนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรรัฐศาสตรมหาบัณฑิต
สาขาวิชาการบริหารงานยุติธรรมและสังคม
คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา
2567

# CYBER SCAM: CASE OF THE SCAM CALL CENTER

SARANRAT NAOWAURAIRATTANA

AN INDEPENDENT STUDY SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR MASTER DEGREE OF POLITICAL SCIENCE
IN JUSTICE AND SOCIAL ADMINISTRATION
FACULTY OF POLITICAL SCIENCE AND LAWS
BURAPHA UNIVERSITY
2024

คณะกรรมการควบคุมงานนิพนธ์และคณะกรรมการสอบงานนิพนธ์ได้พิจารณางานนิพนธ์ของ ศรัณย์รัฐ เนาวอุไรรัตนา ฉบับนี้แล้ว เห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรรัฐศาสตรมหาบัณฑิต สาขาวิชาการบริหารงานยุติธรรมและสังคม ของมหาวิทยาลัยบูรพาได้

| | |
|---|---|
| คณะกรรมการควบคุมงานนิพนธ์ | คณะกรรมการสอบงานนิพนธ์ |
| อาจารย์ที่ปรึกษาหลัก | |
| ..... | ..... ประธาน |
| (ผู้ช่วยศาสตราจารย์ ดร.ธีระ กุลสวัสดิ์) | (ผู้ช่วยศาสตราจารย์ ดร.สนิทเดช จินตนา) |
| | ..... กรรมการ |
| | (ผู้ช่วยศาสตราจารย์ ดร.สุปราณี ธรรมพิทักษ์) |
| | ..... กรรมการ |
| | (ผู้ช่วยศาสตราจารย์ ดร.ธีระ กุลสวัสดิ์) |

..... คณบดีคณะรัฐศาสตร์และนิติศาสตร์

(ผู้ช่วยศาสตราจารย์ ร้อยตำรวจเอก ดร. วิเชียร ตันศิริคงคล)

วันที่.....เดือน.....พ.ศ.....

บัณฑิตวิทยาลัย มหาวิทยาลัยบูรพา อนุมัติให้รับงานนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรรัฐศาสตรมหาบัณฑิต สาขาวิชาการบริหารงานยุติธรรมและสังคม ของมหาวิทยาลัยบูรพา

..... คณบดีบัณฑิตวิทยาลัย

(รองศาสตราจารย์ ดร.วิทวัส แจ้งเอี่ยม)

วันที่.....เดือน.....พ.ศ.....

65920197: สาขาวิชา: การบริหารงานยุติธรรมและสังคม; ร.ม. (การบริหารงานยุติธรรมและสังคม)

คำสำคัญ: อาชญากรรมไซเบอร์, แก๊งคอลเซ็นเตอร์

ศรัณย์รัฐ เนาวอุไรรัตนา : การหลอกลวงทางไซเบอร์: กรณีแก๊งคอลเซ็นเตอร์. (CYBER SCAM: CASE OF THE SCAM CALL CENTER ) คณะกรรมการควบคุมงานนิพนธ์: ธีระ กุลสวัสดิ์ ปี พ.ศ. 2567.

การศึกษานี้มีวัตถุประสงค์เพื่อศึกษาถึงการกระทำอันเป็นลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์ เพื่อศึกษาถึงปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ และเพื่อเสนอแนะการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยการสัมภาษณ์เชิงลึกกับกลุ่มผู้ให้ข้อมูลหลักจำนวน 18 คน ได้แก่ ประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์จำนวน 12 คน และเจ้าหน้าที่ที่ให้การช่วยเหลือหรือป้องกันประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์จำนวน 6 คน

ผลการศึกษา พบว่า ลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์มี 2 รูปแบบ ซึ่งแต่ละรูปแบบมีปัจจัยที่ทำให้ประชาชนถูกหลอกลวงแตกต่างกัน คือ 1) รูปแบบการหลอกลวงทางโทรศัพท์ ผู้หลอกลวงมักใช้วิธีการแอบอ้างเป็นเจ้าหน้าที่รัฐ หรือคนรู้จัก และให้ผู้ตกเป็นเหยื่อดำเนินการตามคำสั่งภายในระยะเวลาในการให้ตัดสินใจที่จำกัดส่งผลให้เกิดการตัดสินใจที่ผิดพลาด ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางโทรศัพท์พบว่า มี 3 ปัจจัย คือ ปัจจัยด้านความกลัว ปัจจัยด้านการรู้ไม่เท่าทันการหลอกลวง ปัญหาด้านการใช้เทคโนโลยี และ 2) รูปแบบการหลอกขายสินค้า ผู้ตกเป็นเหยื่อส่วนใหญ่มักหลงเชื่อโฆษณาผ่านแพลตฟอร์มโซเชียลมีเดียที่ใช้โปรโมชั่นดึงดูดความสนใจ แต่เมื่อทำธุรกรรมให้อีกฝ่ายเสร็จสิ้นกลับไม่ได้รับสินค้า หรือได้รับสินค้าไม่ตามที่ต้องการ ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงขายสินค้าพบว่ามี 3 ปัจจัย คือ ปัจจัยด้านความโลภ ปัจจัยด้านการรู้ไม่เท่าทันการหลอกลวง ปัญหาด้านการใช้เทคโนโลยีและอินเตอร์เน็ต สำหรับแนวทางการแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ ได้แก่ ส่งเสริมการประชาสัมพันธ์ข้อมูลข่าวสารเพื่อป้องกันการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์อย่างต่อเนื่อง ส่งเสริมการให้ความรู้แก่ประชาชนเพื่อป้องกันไม่ให้ตกเป็นเหยื่อ จัดตั้งหน่วยงานที่มีความเชี่ยวชาญในการเฝ้าระวังและตรวจสอบการกระทำผิดในโลกไซเบอร์ หน่วยงานของรัฐมีการออกมาตรการเพื่อป้องกันการหลอกลวงจากคอลเซ็นเตอร์ รวมไปถึงการบูรณาการขอความร่วมมือจากหน่วยงานที่เกี่ยวข้อง

65920197: MAJOR: JUSTICE AND SOCIAL ADMINISTRATION; M.Pol.Sc. (JUSTICE AND SOCIAL ADMINISTRATION)

KEYWORDS: CYBER CRIME, CALL CENTER GANGS

SARANRAT NAOWAURAIRATTANA : CYBER SCAM: CASE OF THE SCAM CALL CENTER . ADVISORY COMMITTEE: TEERA KULSAWAT, Ph.D. 2024.

This study aims to examine the characteristics of cyber scammers of call center gangs, which aims to study the factors that cause the individual to be deceived through cyber by call center gangs and to suggest prevention and suppression of cyber fraud by call center gangs. This is qualitative research by conducting in-depth interviews with 18 individuals, this includes 12 individuals who had fallen victim to cyber scams by call center gangs and 6 officials who have worked on assisting or preventing victimization of cyber scam.

The study revealed two main forms of cyber scams from call center gangs, each had a difference factor: 1) Telephone base-scams - preparators typically impersonate government officials or acquaintances, pressuring victims to follow instructions within the time limit, leading to make a poor decision. The three main reasons why individuals got victimized by phone calls are fear, lack of awareness of the scam, and issues with technology knowledge. 2) Product sale-scams - most of victims are often deceived by online advertisements which lure by attractive promotions. After completing the transaction, the victim would either not receive the product or get the one that didn’t meet the expectations. The three main reasons why individuals got tricked into such a scheme is greed, lack of awareness of the scam, and issue with technology knowledge. The recommended solution to prevent cyber fraud from call center gangs includes continuously promoting public awareness to prevent such scams, establishing a specialized agency to monitor and investigate in cyber space, government agencies implementing measures to prevent call center fraud, as well as fostering collaboration between agencies.

# กิตติกรรมประกาศ

งานนิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยดี เนื่องจากความกรุณาและความช่วยเหลืออย่างดียิ่งจากผู้ช่วยศาสตราจารย์ ดร.ธีระ กุลสวัสดิ์ อาจารย์ที่ปรึกษางานนิพนธ์ ซึ่งผู้วิจัยขอกราบขอบพระคุณที่ท่านได้เสียสละเวลาอันมีค่าในการให้คำปรึกษาและแนะนำ ให้ความรู้ตั้งแต่เริ่มทำงานนิพนธ์จนสำเร็จลุล่วง ตลอดจนให้กำลังใจและสนับสนุนผลักดันผู้วิจัยมาตลอด

ขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.สนิทเดช จินตนา ที่ท่านให้ความเมตตารับเป็นประธานกรรมการสอบงานนิพนธ์ และผู้ช่วยศาสตราจารย์ ดร.สุปราณี ธรรมพิทักษ์ ที่กรุณาสละเวลาอันมีค่าเป็นกรรมการสอบงานนิพนธ์ และให้คำชี้แนะที่เป็นประโยชน์ต่อการวิจัยในครั้งนี้ พร้อมทั้งให้ข้อเสนอแนะแนวทางในการแก้ไขปรับปรุงจนงานนิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี

ความสำเร็จในการศึกษาครั้งนี้ไม่อาจเกิดขึ้นได้หากไม่ได้รับความอนุเคราะห์ข้อมูลและความร่วมมือเป็นอย่างดีจากผู้ให้ข้อมูลสำคัญทุกท่าน ขอขอบคุณประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ทุกท่านที่ให้ข้อมูลและประสบการณ์ในการถูกหลอกลวง เจ้าหน้าที่ตำรวจจากกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีที่ให้ความอนุเคราะห์ให้สัมภาษณ์ถึงประสบการณ์ในการให้ความช่วยเหลือ และแนวทางในการป้องกันการหลอกลวงจากแก๊งคอลเซ็นเตอร์จนงานนิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

ขอบคุณครอบครัวที่ให้การสนับสนุนส่งเสริมให้ผู้วิจัยเสมอมา และเป็นกำลังใจสำคัญในการทำงานนิพนธ์ฉบับนี้สำเร็จลุล่วงได้เป็นอย่างดีในที่สุด

ศรัณย์รัฐ เนาวอุไรรัตนา

# สารบัญ

หน้า

# สารบัญรูปภาพ

**หน้า**

# บทที่ 1
# บทนำ

## ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารมีความก้าวหน้าอย่างต่อเนื่องและไม่มีขีดจำกัดซึ่งเป็นประโยชน์ในชีวิตประจำวันของบุคคลทั่วไป โดยเครื่องมือเหล่านี้ช่วยให้เราสามารถเข้าถึงสื่อออนไลน์จำนวนมากผ่านอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ และเชื่อมโยงการสื่อสารระหว่างบุคคลในรูปแบบต่าง ๆ ในระดับที่เป็นประโยชน์ (พิริยะ กิมาลี และนิตยา วงศ์ภินันท์วัฒนา, 2562) มนุษย์ใช้สื่อโซเชียลมีเดียเพื่อการสนทนา ค้นหาข้อมูลทำธุรกรรม และซื้อขายสินค้า ซึ่งสามารถดำเนินการได้ตลอดเวลาที่ทั่วทุกหนทุกแห่งผ่านระบบอินเตอร์เน็ตนี้ได้ส่งผลให้หน่วยงานและองค์กรต่าง ๆ ต้องปรับเปลี่ยนแนวทางการดำเนินงานให้เข้ากับการเกิดขึ้นของสื่อโซเชียลมีเดีย อย่างไรก็ตามเมื่อสื่อโซเชียลมีเดียหรือเทคโนโลยีสารสนเทศเข้ามามีอิทธิพลต่อการดำรงชีวิตก็ย่อมมีผู้ที่ไม่หวังดีที่เข้ามาหลอกลวง ขโมย และโจรกรรมข้อมูลต่าง ๆ ทางไซเบอร์เพื่อนำไปใช้ในทางการที่ผิดกฎหมายจนนำมาซึ่งอาชญากรรมทางไซเบอร์ โดยลักษณะของอาชญากรรมทางไซเบอร์นั้นส่วนหนึ่งเกิดจากความไม่ระมัดระวังของผู้ใช้งานเอง เช่น การเปิดเผยรหัสผ่านแก่บุคคลที่ไม่น่าเชื่อถือ การติดต่อสื่อสารผ่านแพลตฟอร์มโซเชียลมีเดีย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต พฤติกรรมที่อยากรู้อยากเห็น การเปิดเผยช่องโหว่ที่อาจทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลส่วนบุคคล และความไม่คำนึงถึงความเสี่ยงทางไซเบอร์ เป็นต้น (กิตติคุณ มีทองจันทร์ และวงศ์ยศ เกิดศร, 2564) และในปัจจุบันอาชญากรรมประเภทหนึ่งที่สร้างปัญหาให้กับประชาชนคือการกระทำผิดที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ที่เป็นการหลอกลวงให้กับประชาชน โดยผู้ทำการกระทำนี้ใช้วิธีการหลอกลวงทั้งที่เป็นการใช้โทรศัพท์ในการหลอกลวง หรือการใช้โทรศัพท์ผ่านอินเตอร์เน็ต (VoIP) โดยมักจะเสนอข้อเสนอที่ไม่ถูกต้องหรือมีจำนวนเงินที่หลอกลวงให้กับผู้เสียหาย โดยหวังผลเพื่อให้เข้ามาติดสอบสวน โดยการเผยแพร่ข้อมูลหรือให้ข้อความสำหรับหลอกลวง หรือรับโทรศัพท์หรือการติดต่อผ่านอินเตอร์เน็ตที่มีเจตนาไม่ดีเพื่อให้ผู้ที่ถูกเรียกหรือติดต่อตอบสนอง การกระทำความผิดเหล่านี้เกิดจากกลุ่มที่เรียกว่า “แก๊งคอลเซ็นเตอร์” นอกจากนี้ อาชญากรรมประเภทหนึ่งที่เกิดขึ้นจากแก๊งคอลเซ็นเตอร์ได้ใช้วิธีการเข้าสู่รูปแบบใหม่ตามความก้าวหน้าของเทคโนโลยี โดยตัวอย่างเช่น แก๊งคอลเซ็นเตอร์ใช้ช่องทางการเงินที่ได้มาจากการหลอกลวงผู้คนให้ลงทุนผ่านระบบสกุลเงินดิจิทัลหรือบิทคอยน์ ทำให้การรวบรวมพยานหลักฐานใน

กระบวนการดำเนินคดียากขึ้น พฤติกรรมการกระทำผิดของแก๊งคอลเซ็นเตอร์ดังกล่าวได้ทำให้เกิดปัญหาอาชญากรรมที่ก่อให้เกิดความเดือดร้อนในสังคม ซึ่งมีผู้คนหลายคนต้องเสียเงินทำลายก้อนสุดท้ายในชีวิต ซึ่งถือเป็นอันตรายต่อความมั่นคงและความผาสุกของสังคมไทย (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

จุดเริ่มต้นเกิดจากแก๊งอาชญากรรมในประเทศไต้หวันที่ใช้กลอุบายหลอกเหยื่อในประเทศเกี่ยวกับบัตรเครดิต ซึ่งต่อมาได้เข้าไปตั้งฐานในการปฏิบัติการที่ประเทศจีน และหลังจากถูกกวาดล้างอย่างหนัก ก็ตั้งฐานปฏิบัติการลอกลวงเหยื่อที่ประเทศอื่น ๆ ในแถบเอเชีย ไม่ว่าจะเป็นประเทศฟิลิปปินส์ มาเลเซีย ลาว กัมพูชา รวมถึงประเทศไทยด้วย (เดลินิวส์, 2559)

การกระทำผิดของแก๊งคอลเซ็นเตอร์ในประเทศไทยยังคงมีอย่างต่อเนื่อง ดังนั้นแก๊งคอลเซ็นเตอร์ที่เข้ามาหลอกลวงคนไทยนั้นเป็นเครือข่ายอาชญากรรมข้ามชาติที่ประสานโยงใยกันระหว่างตัวการใหญ่ซึ่งเป็นชาวไต้หวันกับแก๊งอาชญากรรมในประเทศต่าง ๆ ซึ่งแก๊งเหล่านี้จะรู้เกี่ยวข้อมูลเกี่ยวกับระบบการเงิน ข้อกฎหมาย และบริบททางสังคมของผู้คนในประเทศตนเองซึ่งเป็นกลุ่มเป้าหมายที่จะตกเป็นเหยื่อ โดยจะไปตั้งศูนย์คอลเซ็นเตอร์ในประเทศอื่นที่ไม่ใช่ประเทศของเหยื่อเพื่อป้องกันการตรวจสอบและติดตามจับกุม ซึ่งแต่ละประเทศก็จะมีแก๊งที่ดูแลโดยชาวไต้หวันและประสานกับหัวหน้าเครือข่ายที่ประเทศไต้หวัน เช่น แก๊งอาซื่อ ซึ่งอยู่ในย่านศรีเปอร์ตาลิง กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย แก๊งฉีเคอ ซึ่งอยู่ที่ดูไบ ประเทศสหรัฐอาหรับเอมิเรตส์ อุปกรณ์ที่แก๊งคอลเซ็นเตอร์ในแต่ละแห่งใช้ในการหลอกลวงเหยื่อนั้นจะมีลักษณะเดียวกันได้แก่ โทรศัพท์ คอมพิวเตอร์ เครื่องแปลงสัญญาณโทรศัพท์ VoIP ซึ่งจะแปลงสัญญาณโทรศัพท์ด้วยระบบอินเทอร์เน็ตให้เป็นหมายเลขโทรศัพท์ของหน่วยงานที่จะแอบอ้าง พร้อมทั้งหมายเลขโทรศัพท์ของเหยื่อ โดยจะมีทีมงานคอลเซ็นเตอร์จากประเทศกลุ่มเป้าหมายที่จะตกเป็นเหยื่อ โดยมีวิธีการคือ ถ้าเหยื่อเป้าหมายเป็นคนไทย แก๊งดังกล่าวจะไปเช่าบ้านหรืออาคารเพื่อตั้งศูนย์คอลเซ็นเตอร์ในประเทศเพื่อนบ้าน เช่น กัมพูชา มาเลเซีย ดูไบ แล้วให้คนไทยไปทำหน้าที่โทรศัพท์ โดยจะมีเครื่อง VoIP ซึ่งจะแปลงสัญญาณเป็นเบอร์โทร.ของหน่วยราชการต่าง ๆ ที่จะใช้ในการแอบอ้าง เช่น สถานีตำรวจ กรมสอบสวนคดีพิเศษ (ดีเอสไอ) เจ้าหน้าที่จากสำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน (ปปง.) เจ้าหน้าที่ที่ไปรษณีย์ สถาบันการเงิน เพื่อสร้างความน่าเชื่อถือเมื่อเหยื่อตรวจสอบเบอร์โทรศัพท์จะพบว่าเบอร์ที่โทรมาตรงกับเบอร์ของหน่วยราชการ โดยให้ทีมงานซึ่งเป็นคนไทยโทรศัพท์ข้ามประเทศไปหลอกให้เหยื่อโอนเงิน (สำนักงานตำรวจแห่งชาติ, 2561)

สำนักงานตำรวจแห่งชาติเผยว่า ยอดสะสมของผู้แจ้งความออนไลน์ที่ได้รับ ตั้งแต่วันที่ 1 มีนาคม พ.ศ. 2565 – 31 พฤษภาคม พ.ศ. 2566 มีจำนวนทั้งหมด 296,243 เรื่อง โดยแบ่งเป็นคดี

ออนไลน์ 270,360 เรื่อง และคดีอาญาอื่น ๆ 9,009 เรื่อง รวมมูลค่าความเสียหายทั้งหมด 38,156,125,167 บาท ซึ่งแบ่งออกมาได้ 14 อันดับ ดังนี้ (1) หลอกลวงซื้อขายสินค้าหรือบริการไม่เป็นขบวนการ 100,694 คดี (2) หลอกให้โอนเงินเพื่อทำงานฯ 36,896 คดี (3) หลอกให้กู้เงิน 33,517 คดี (4) หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ 22,740 คดี (5) ข่มขู่ทางโทรศัพท์ (Call center) 20,474 คดี (6) หลอกเป็นบุคคลอื่นเพื่อยืมเงิน 9,664 คดี (7) หลอกให้โอนเงินเพื่อรับรางวัลฯ 8,697 คดี (8) หลอกลวงซื้อสินค้าหรือบริการเป็นขบวนการ 8,107 คดี (9) หลอกให้ติดตั้งโปรแกรมควบคุมระบบฯ 4,786 คดี (10) หลอกให้ลงทุนตามพรบ.กู้ยืมเงิน 3,080 คดี (11) กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ 2,972 คดี (12) หลอกให้รักแล้วโอนเงิน 2,167 คดี (13) หลอกเกี่ยวกับทรัพย์สินดิจิทัล 1,229 คดี (14) เข้ารหัสคอมพิวเตอร์ของผู้อื่น 79 คดี ดังภาพที่ 1


ภาพที่ 1 การจัดอันดับคดีออนไลน์ (DROIDSANS, 2023)

จากสถิติการจัดอันดับคดีออนไลน์ที่ได้รับแจ้งจะเห็นได้ว่าการหลอกลวงทางไซเบอร์ในกรณีของการกระทำความผิดที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์นั้นอยู่ในอันดับที่ 5 ซึ่งมีมูลค่าความเสียหายจำนวน 4,440,554,271 บาท โดยการกระทำผิดที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ส่วนใหญ่

มักเป็นการโทรศัพท์เข้ามาหลอกลวงประชาชนในหลายรูปแบบ เช่น หลอกว่าเป็นผู้โชคดีและขอข้อมูลส่วนบุคคลเพื่อยืนยันการได้รับรางวัล จากนั้นนำข้อมูลไปโจมตีแฮกเกอร์ในระบบหรือหลอกว่าได้รับสินค้าทางไปรษณีย์จากต่างประเทศและให้มีการโอนเงินค่าภาษีเข้าไปก่อนและจึงจัดส่งสินค้าให้ รวมถึงวิธีการแชร์ลูกโซ่ก็ยังทำให้มีผู้เสียหายจำนวนมากเช่นกัน เช่น หลอกให้ลงทุนในลักษณะต่างๆ เพื่อให้ผลตอบแทนสูงในช่วงแรก จากนั้นก็จะไม่จ่ายและหนีหายไป ทำให้ส่งผลกระทบต่อประชาชนที่ตกเป็นเหยื่อจำนวนมากที่ต้องสูญเสียเงินให้กับแก๊งคอลเซ็นเตอร์ (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันฉีกุล และนัทธี จิตสว่าง, 2563) ดังนั้นจะเห็นได้ว่าปัญหาเกี่ยวกับการกระทำผิดของแก๊งคอลเซ็นเตอร์ในประเทศไทยยังคงเป็นปัญหาสำคัญที่ยังคงเกิดขึ้นอย่างต่อเนื่อง แม้แต่เจ้าหน้าที่ตำรวจและหน่วยงานที่เกี่ยวข้องจะได้ปฏิบัติการปราบปรามอย่างเต็มที่ แต่ผู้กระทำผิดที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์อาจไม่ถูกดำเนินคดีทั้งหมด สถิติการจับกุมแก๊งคอลเซ็นเตอร์ดังกล่าวข้างต้นเป็นสถิติที่มีผู้เข้าแจ้งความกับเจ้าหน้าที่ตำรวจผ่านเว็บไซต์เท่านั้น แต่ในความเป็นจริงสถิติอาชญากรรมที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์จำนวนหนึ่งอาจเป็นสถิติที่ไม่มีการแจ้งความต่อต้านนั่นเป็นเพราะอาจเห็นว่าทรัพย์สินที่สูญหายมีจำนวนไม่มากนักหรือเห็นว่าการแจ้งความเป็นเรื่องความยุ่งยากเสียเวลา หรือเห็นว่าแม้จะแจ้งความไปแล้ว จนไม่สามารถติดตามทรัพย์สินที่สูญหายไปกลับคืนมาได้ทำให้เกิดสถิติที่เป็นตัวเลขมืด (Dark Figure) ซึ่งไม่ได้สถิติที่แท้จริงของคดีที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ในประเทศไทย ดังนั้นหากไม่มีการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์อย่างมีประสิทธิภาพอาจทำให้แก๊งคอลเซ็นเตอร์หันมาใช้ประเทศไทยเป็นศูนย์กลางในการกระทำผิดอีกครั้ง ซึ่งอาจทำให้เกิดสถิติที่เป็นตัวเลขมืด (Dark Figure) ส่งผลกระทบต่อภาพลักษณ์ของประเทศไทยในแง่ที่ว่าเป็นศูนย์กลางของอาชญากรรมข้ามชาติโดยใช้ประเทศไทยเป็นฐานในการกระทำผิด ซึ่งอาจกระทำผิดต่อการท่องเที่ยวหรือการสนใจเข้ามาลงทุนของชาวต่างชาติอันเป็นอุปสรรคต่อการพัฒนาประเทศไทยอย่างแท้จริง (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันฉีกุล และนัทธี จิตสว่าง, 2563)

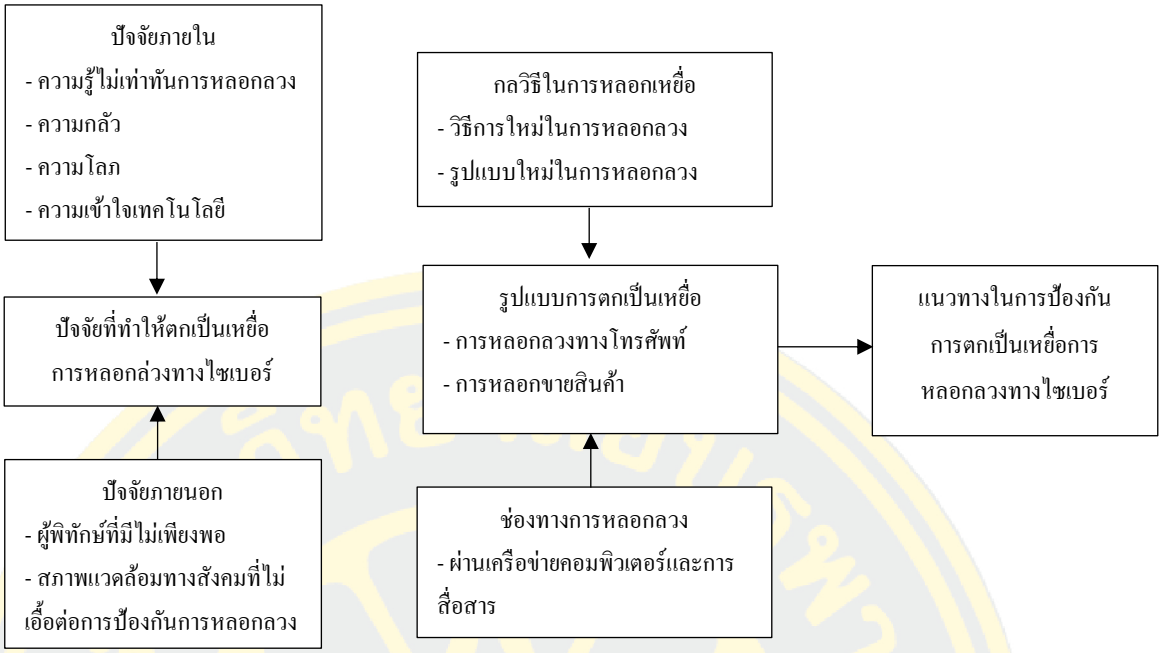
จากความเป็นมาและความสำคัญของปัญหาดังกล่าวข้างต้นจึงทำให้ผู้วิจัยมีความสนใจศึกษาถึงลักษณะของการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์ ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ ตลอดถึงหน่วยงานที่เกี่ยวข้อง และมาตรการที่เกี่ยวข้องกับการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ เพื่อป้องกันและปราบปรามปัญหาอาชญากรรมที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ได้ลดลง และเพื่อให้ทำให้ประชาชนในประเทศไทยมีคุณภาพชีวิตที่ดีขึ้นปราศจากความหวาดกลัวต่อภัยอาชกรรมประเภทแก๊งคอลเซ็นเตอร์

## วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาถึงการกระทำอันเป็นลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์
2. เพื่อศึกษาถึงปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์
3. เพื่อเสนอแนะการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์

## กรอบแนวคิดการวิจัย

ในการศึกษาครั้งนี้ มีวัตถุประสงค์เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ ศึกษาปัจจัยที่ทำให้ตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเสนอแนะแนวทางการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ จากการศึกษาถึงแนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง สรุปได้ถึงปัจจัยที่ทำให้ตกเป็นเหยื่อการหลอกลวง จากปัจจัยภายใน และปัจจัยภายนอก ซึ่งปัจจัยภายในประกอบด้วย ความรู้ไม่เท่าทันการหลอกลวง (Cohen and Felson, 1979; Deliema, 2018) ความกลัว ความโลภ (Office of Fair Trading, 2009) ความหลงรัก (Buil-Gil and Zeng, 2021) และความเข้าใจเทคโนโลยี (Dutton and Shepherd, 2004 อ้างถึงในพิทักษ์ ศิริวงษ์ และบัณฑิตา อุณหเลขจิตร, 2560) ปัจจัยภายนอกประกอบด้วย จำนวนผู้พิทักษ์ที่มีไม่เพียงพอ และสภาพแวดล้อมทางสังคมที่ไม่เอื้อต่อการป้องกันการหลอกลวง (DeLima, 2018) เช่น สภาพแวดล้อมภายในครอบครัว ชุมชน สังคม โดยการหลอกลวงมีหลายรูปแบบ โดยผู้หลอกลวงจะหาวิธีการในการหลอกลวง และรูปแบบการหลอกลวงใหม่ ๆ (สุมนทิพย์ จิตสว่าง และคณะ, 2556) มาหลอกลวงเหยื่อโดยทำผ่านเครือข่ายคอมพิวเตอร์และการสื่อสาร (Duffield and Grabowski, 2001) ซึ่งจากผลการศึกษาจะนำไปสู่แนวทางในการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ โดยผู้วิจัยนำมาสรุปเป็นกรอบแนวคิดของการวิจัยดังนี้




ภาพที่ 2 กรอบแนวคิดการวิจัย

## ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1. ประชาชนที่ได้ศึกษาเกิดความตระหนักถึงลักษณะของการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ ส่งผลให้ลดการเกิดปัญหาอาชญากรรมไซเบอร์จากแก๊งคอลเซ็นเตอร์ในสังคม

2. เพื่อเป็นข้อมูลพื้นฐานสำหรับหน่วยงานที่เกี่ยวข้องได้นำไปกำหนดมาตรการในการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์

## ขอบเขตของการวิจัย

การวิจัยครั้งนี้ ผู้วิจัยได้กำหนดขอบเขตที่จะทำการวิจัยเป็น 3 ส่วน คือ ขอบเขตด้านเนื้อหา ขอบเขตด้านประชากร และขอบเขตด้านระยะเวลา ดังนี้

**ขอบเขตด้านเนื้อหา**

ขอบเขตด้านเนื้อหา มุ่งศึกษาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ ซึ่งครอบคลุมเนื้อหาตามที่ระบุไว้ในวัตถุประสงค์ ได้แก่ รูปแบบการตกเป็นเหยื่อการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ ปัจจัยที่ทำให้ประชาชนที่มีอายุตั้งแต่ 20 – 60 ปี ถูกหลอกลวงและเสนอแนะแนวทางการป้องกันการตกเป็นเหยื่อการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ ผู้วิจัยได้กำหนดขอบเขตของการศึกษา โดยศึกษาวิเคราะห์ข้อมูลจากที่ได้มีการจัดพิมพ์เผยแพร่ ได้แก่ หนังสือ เอกสาร งานวิจัย ข้อมูลทางสถิติ มาตรการทางกฎหมาย แนวคิด ทฤษฎี และสิ่งพิมพ์หรือสื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับการหลอกลวงทางไซเบอร์

**ขอบเขตด้านผู้ให้ข้อมูลสำคัญ**

การวิจัยครั้งนี้ มุ่งผู้ที่เคยตกเป็นเหยื่อการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์และผู้ที่เกี่ยวข้อง ดังนี้

กลุ่มที่ 1 ประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ที่เคยแจ้งความดำเนินคดีภายในระยะเวลา 5 ปี (พ.ศ. 2562 - 2566) จำนวน 12 คน

กลุ่มที่ 2 เจ้าหน้าที่ที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกันประชาชนจากการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ จำนวน 6 คน

**ขอบเขตด้านระยะเวลา**

ระยะเวลาที่ใช้ในการศึกษาครั้งนี้ เริ่มดำเนินการระหว่างเดือนกันยายน พ.ศ. 2566 ถึง ตุลาคม พ.ศ. 2567 รวมระยะเวลาทั้งสิ้น 1 ปี 1 เดือน

## นิยามศัพท์เฉพาะ

อาชญากรรมไซเบอร์ หมายถึง การกระทำความผิดที่ โดยมีโครงข่ายคอมพิวเตอร์เข้ามาเกี่ยวข้อง มีวัตถุประสงค์ทางอาญา ไม่ว่าจะในฐานะเป็นเครื่องมือ หรือ เป้าหมาย หรือมีส่วนเกี่ยวข้องกับการกระทำความผิดทางอาญา และมีความมุ่งหมายในการกระทำ ความผิดที่หลากหลาย ไม่ว่าจะเพื่อผลประโยชน์ทางการเงินในทางส่วนตัว หรือเพื่อคุกคาม ต่อความมั่นคงของชาติ และความสงบเรียบร้อยของประชาชน

การหลอกลวง หมายถึง การทำให้คนอื่นหลงเชื่อหรือเข้าใจผิด หรือประสงค์ร้ายกับคนอื่นที่ก่อให้เกิดความเสียหายต่อทรัพย์สินหรือร่างกาย

การหลอกลวงทางไซเบอร์ หมายถึง การกระทำที่ใช้เทคโนโลยีสารสนเทศและการสื่อสารในการหลอกลวงหรือฉ้อโกงบุคคลหรือองค์กร โดยมักจะเกิดขึ้นผ่านทางอินเทอร์เน็ตหรือเครือข่ายคอมพิวเตอร์

แก๊งคอลเซ็นเตอร์ หมายถึง กลุ่มคน หรือขบวนการที่หลอกลวงประชาชนทางโทรศัพท์ โดยใช้วิธีการสร้างสถานการณ์ให้ประชาชนที่รับโทรศัพท์เกิดความตื่นตระหนก หรือเข้าใจผิดว่าได้รับผลประโยชน์บางอย่างที่ทางแก๊งคอลเซ็นเตอร์หลอกลวง

การป้องกันและปราบปราม หมายถึง กระบวนการและวิธีการที่ใช้เพื่อยับยั้งไม่ให้เกิดเหตุการณ์หรือการกระทำผิด และการดำเนินการเพื่อลดหรือขจัดปัญหาที่เกิดขึ้นอย่างจริงจัง

การแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์ หมายถึง การดำเนินการหรือมาตรการที่ใช้เพื่อรับมือและป้องกันการหลอกลวงทางโลกออนไลน์ ซึ่งอาจประกอบด้วยการสร้างความรู้ให้กับประชาชน การใช้เครื่องมือด้านความปลอดภัยไซเบอร์ การตรวจสอบและปราบปรามผู้กระทำผิดทางไซเบอร์ ตลอดจนการฟื้นฟูความเสียหายที่เกิดขึ้น

ปัจจัยภายใน หมายถึง ปัจจัยที่มีอยู่ในตัวบุคคลเอง เช่น ความเชื่อ บุคลิกภาพ พฤติกรรม ทัศนคติ หรือความรู้ ซึ่งส่งผลต่อการตัดสินใจและการกระทำต่าง ๆ ของบุคคลนั้น

ปัจจัยภายนอก หมายถึง ปัจจัยที่อยู่นอกตัวบุคคล เช่น สภาพแวดล้อมทางสังคม วัฒนธรรม การเงิน กฎหมาย และเทคโนโลยี ซึ่งสามารถมีอิทธิพลต่อพฤติกรรมหรือการตัดสินใจของบุคคลได้

ปัจจัยที่ทำให้ตกเป็นเหยื่อ หมายถึง ปัจจัยหรือสาเหตุที่เพิ่มความเสี่ยงให้บุคคลตกเป็นเป้าหมายของการหลอกลวงหรือการกระทำผิด อาจเป็นลักษณะนิสัย ความขาดระมัดระวัง หรือสภาพแวดล้อมที่มีความเสี่ยงสูง

กลวิธีที่ใช้ในการหลอกลวง หมายถึง เทคนิคหรือวิธีการต่าง ๆ ที่ผู้ไม่หวังดีใช้เพื่อหลอกลวงเหยื่อให้หลงเชื่อหรือตกหลุมพราง เช่น การสร้างสถานการณ์เร่งด่วน การให้ข้อมูลเท็จ หรือการปลอมตัวเป็นบุคคลหรือองค์กรที่น่าเชื่อถือ

รูปแบบการตกเป็นเหยื่อ หมายถึง ลักษณะหรือวิธีที่บุคคลถูกหลอกลวงหรือกลายเป็นเหยื่อของการกระทำผิด เช่น การตกเป็นเหยื่อทางการเงิน การถูกโจรกรรมข้อมูลส่วนตัว หรือการหลอกลวงผ่านสื่อสังคมออนไลน์

ความกลัว หมายถึง อารมณ์หรือความรู้สึกที่เกิดขึ้นเมื่อบุคคลเผชิญกับสถานการณ์ที่รู้สึกไม่ปลอดภัย หรือมีความเสี่ยงต่ออันตรายทั้งทางร่างกายและจิตใจ เป็นอารมณ์ธรรมชาติที่มีหน้าที่ช่วยป้องกันตัวบุคคลจากอันตราย

ความโลภ หมายถึง อารมณ์หรือความรู้สึกที่ต้องการหรือแสวงหาสิ่งต่าง ๆ โดยไม่มีที่สิ้นสุด หรือมีความต้องการมากเกินไป โดยทั่วไปความโลภมักเกี่ยวข้องกับการอยากได้ทรัพย์สิน เงินทอง หรือสิ่งที่มีค่าอื่น ๆ ในปริมาณที่มากกว่าที่จำเป็น หรือมากกว่าที่สมควรได้รับ

# บทที่ 2
# เอกสาร และงานวิจัยที่เกี่ยวข้อง

การศึกษาเรื่อง การหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ โดยผู้วิจัยได้รวบรวมแนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง เพื่อนำมากำหนดเป็นกรอบและแนวทางในการศึกษาดังต่อไปนี้

1. แนวคิด ทฤษฎีที่เกี่ยวข้องกับอาชญากรรมไซเบอร์
2. ลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์
3. ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์
4. กรณีที่เกี่ยวกับแก๊งคอลเซ็นเตอร์
5. งานวิจัยที่เกี่ยวข้อง

## แนวคิด ทฤษฎีที่เกี่ยวข้องกับอาชญากรรมไซเบอร์

อาชญากรรมไซเบอร์หรือการหลอกลวงทางไซเบอร์นั้นได้รับความสำคัญในยุคที่เทคโนโลยีและอินเทอร์เน็ตก้าวขึ้นอย่างรวดเร็ว การหลอกลวงทางไซเบอร์เป็นกระบวนการที่ผู้ทำผิดใช้ความชำนาญทางเทคโนโลยีและกลยุทธ์ต่าง ๆ เพื่อเอาประโยชน์ส่วนตัวหรือเข้าแทรกแซงลักษณะการทำงานของระบบที่เชื่อถือได้ โดยส่งผลให้เกิดความเสียหายทางอาญา การเมือง และสังคม การหลอกลวงทางไซเบอร์เป็นกลุ่มอาชญากรที่มีความชำนาญทางเทคโนโลยีและความรู้ในการใช้งานอินเทอร์เน็ตเป็นอย่างดี และมักใช้เทคนิคต่างๆ เพื่อก่อให้เกิดความสับสนและความเชื่อเชิงบวกในเหยื่อเพื่อให้ตัดสินใจตามที่ต้องการ นอกจากนี้ยังมีความเกี่ยวข้องกับเสรีภาพของอินเทอร์เน็ต ซึ่งทำให้การติดตามและควบคุมกิจกรรมที่เกิดขึ้นในโลกดิจิทัลไปได้ยาก นอกจากนี้ยังมีข้อเสียที่เกิดขึ้นจากการใช้เทคโนโลยีในทางไม่เหมาะสม และการละเมิดความเป็นส่วนตัวของผู้คน ซึ่งทำให้สังคมและระบบเศรษฐกิจประสบความเสียหาย (ECIPE : European Centre for International Political Economy, 2017)

ภัยคุกคามทางไซเบอร์ (Internet Threats) เป็นการกระทำที่เกิดขึ้นในระดับบุคคล องค์กร หรือรัฐซึ่งถือเป็นการก่ออาชญากรรมบนโลกไซเบอร์ (Cyber Crimes) ซึ่งมีผู้กระทำตั้งแต่มือสมัครเล่นจนถึงพวกที่ไม่เพียงแค่หวงและขโมยข้อมูล แต่อาจลามไปถึงการทำลายล้างหรือสร้างความเสียหายต่อทรัพย์สินของเป้าหมาย หรือสร้างอันตรายและผลกระทบต่อชีวิตประชาชนทั่วไปด้วยกัน การกระทำนี้สามารถดำเนินการได้หากมีอุดมคติหรือวัตถุประสงค์ทางการเมือง อาจเรียกการกระทำเช่นนี้ว่า “ภัยคุกคามทางโลกไซเบอร์” แน่นอนว่าภัยคุกคามเหล่านี้อาจไม่ได้ระทำโดย

กลุ่มบุคคลหรือผู้กระทำร้ายดานไซเบอร์ตามลำดับเพียงแค่เพราะการกระทำของบุคคลเหล่านี้อาจมีองค์กรหรือรัฐอยู่เบื้องหลังหรือให้ก้าวสนับสนุนก็ได้ทั้งนี้ก็เพื่อบรรลุเป้าหมายทางยุทธศาสตร์ในการสร้างความเสียหายต่อโครงสร้างพื้นฐานและส่งผลกระทบต่อความมั่นคงแห่งชาติฝ่ายตรงข้ามโดยเฉพาะในด้านผลประโยชน์ทางการเมือง เศรษฐกิจ สังคม จิตวิทยา ทรัพยากรธรรมชาติ และสิ่งแวดล้อม เป็นต้น (ฤทธี อินทราวุธ, 2561)

**1.1 ทฤษฎีเกี่ยวกับอาชญากรรมไซเบอร์**

อาชญากรรมทางไซเบอร์ถือเป็นหนึ่งในประเภทของการปฏิบัติการทางด้านเครือข่ายคอมพิวเตอร์ ซึ่งเป็นลักษณะของการกระทำความผิดที่ปรากฏอยู่ในอนุสัญญาว่าด้วยอาชญากรรมทางไซเบอร์ (Convention on Cybercrime) แต่คำนิยามของอาชญากรรมทางไซเบอร์จะมีความแตกต่างกันไปตามประมวลกฎหมายอาญาของแต่ละรัฐ (David Weissbrodt, ‘Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, 2013)

บางแนวคิดกำหนดให้อาชญากรรมทางไซเบอร์ หมายถึง อาชญากรรมทั่วไปที่มีการใช้คอมพิวเตอร์ในการดำเนินการ ซึ่งทำให้การดำเนินคดีกับความผิดดังกล่าวอยู่ภายใต้กฎหมายดั้งเดิมที่มีอยู่ ในขณะที่บางแนวคิดกำหนดให้อาชญากรรมทางไซเบอร์เป็นอาชญากรรมประเภทใหม่ซึ่งมีความท้าทายเฉพาะแตกต่างกับอาชญากรรมประเภทเดิมที่มีอยู่ เนื่องจากเกี่ยวข้องกับปัญหาหลายประการ ได้แก่ เขตอำนาจรัฐ ความร่วมมือระหว่างประเทศแรงจูงใจ การระบุตัวผู้กระทำความผิดเป็นต้น ซึ่งทำให้การดำเนินคดีกับความผิดนี้จำเป็นต้องมีการกำหนดกฎหมายใหม่ออกมา แต่ไม่ว่าจะเป็นการนิยามในแนวทางใดก็ตามโดยส่วนใหญ่แล้วการนิยามอาชญากรรมทางไซเบอร์ในแต่ละประเทศจะมิได้รวมถึงเพียงการแฮกข้อมูล (Hacking) และการทำลายข้อมูล (Cracking) เท่านั้น แต่ยังรวมถึง การขู่กรรโชก ภาพอนาจารเด็ก การฟอกเงิน การฉ้อโกง การละเมิดลิขสิทธิ์ซอฟต์แวร์และการจารกรรมขององค์กรอีกด้วย (จิตราภรณ์ โสตถิกุล, 2565)

การแบ่งประเภทขององค์กรอาชญากรรมทั่วไปสามารถจำแนกได้เป็น 3 ประเภทดังนี้

1. องค์กรอาชญากรรมที่เกี่ยวข้องกับการขโมยขู่ กรรโชกเงิน การลักพาตัว และเรียกความเรียกคู่ครองและหนี้นอกระบบ

2. องค์กรอาชญากรรมที่เกี่ยวข้องกับการให้บริการผิดกฎหมาย ซึ่งรวมถึงการค้ายาเสพติด การค้ามนุษย์ การพนัน การลักลอบเข้าเมือง หรือการนำเข้าหนังสือวีดีโอลามกอนาจาร

3. องค์กรอาชญากรรมที่เกี่ยวข้องกับอาชญากรรมทางเศรษฐกิจ ซึ่งรวมถึงการปลอมแปลงเอกสาร ฉ้อฉล การหลอกลวง และอาชญากรรมทางคอมพิวเตอร์

ดังนั้นแก๊งคอลเซ็นเตอร์มีความเกี่ยวข้องกับองค์กรอาชญากรรมโดยตรง เนื่องจากมีการรวมกลุ่มของอาชญากรตั้งแต่ 3 คนขึ้นไป และมีการแบ่งงานตามสายการบังคับบัญชาตามความ

เชี่ยวชาญ รวมถึงมีความเกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์และอาชญากรรมทางเศรษฐกิจโดยตรง

อนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ.2000 ได้กำหนดคำนิยามและความหมายของคำว่า “องค์กรอาชญากรรม” ไว้ว่า

1. กลุ่มอาชญากรที่จัดตั้งในลักษณะองค์กร (Organized Criminal Group) หมายถึง กลุ่มที่ประกอบด้วยบุคคลอย่างน้อย 3 คนขึ้นไปที่ค้างอยู่เป็นเวลานาน และมีการประสานงานระหว่างกันโดยมีเป้าหมายในการก่ออาชญากรรมร้ายแรงตั้งแต่หนึ่งฐานความผิดขึ้นไปตามที่กำหนดไว้ในอนุสัญญานี้ เพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงินหรือผลประโยชน์ทางวัตถุอย่างอื่น ๆ ไม่ว่าโดยทางตรงหรือทางอ้อม

2. อาชญากรรมร้ายแรง (Serious Crime) หมายถึง การกระทำที่เป็นความผิดซึ่งสามารถลงโทษโดยการทำให้สูญเสียเสรีภาพขั้นสูงสุดเป็นเวลาอย่างน้อย 4 ปีหรือโดยโทษที่รุนแรงกว่านี้

3. ทรัพย์สินที่ได้จากอาชญากรรม (Proceeds of Crime) หมายถึง ทรัพย์สินใด ๆ ที่เกิดขึ้นจากหรือได้รับมาไม่ว่าโดยทางตรงหรือทางอ้อมจากการกระทำความผิด ซึ่งเป็นผลมาจากการกระทำอาชญากรรม (United Nations Office on Drugs and Crime, 2021)

แนวคิดและทฤษฎีที่เกี่ยวข้องกับสาเหตุในการกระทำผิดที่เกี่ยวข้องกับการกระทำผิดของแก๊งคอลเซ็นเตอร์ประกอบด้วย

1. แนวคิดของสำนักคลาสสิก (Classical School) คือ หนึ่งในแนวคิดของอาชญาวิทยาที่ก่อตั้งขึ้นโดยนักปราชญ์ชาวอิตาลีชื่อ ซีซารี แบ็คคาเรีย (Cesare Beccaria) ในปี ค.ศ. 1738-1794 ซึ่งมีหลักปรัชญาสำคัญคือ เจตจำนงเสรี (Free Will) หรือเชื่อในความเสรีของมนุษย์ในการตัดสินใจและกระทำตามความเหมาะสมตามเหตุผลต่าง ๆ และคำนึงถึงผลกระทำของตนเอง กล่าวคือ มนุษย์เป็นผู้มีความเห็นอาศัยเหตุผลในการตัดสินใจและกระทำสิ่งต่างๆ เพื่อให้ได้ผลประโยชน์สูงสุดในทางวัตถุและปฏิบัติการกระทำต่าง ๆ แบ็คคาเรียเชื่อว่าถ้าหากต้องป้องกันไม่ให้คนในสังคมกระทำผิดกฎหมาย บทลงโทษจะต้องมีลักษณะที่รุนแรงและรวดเร็วเพื่อทำให้คนในสังคมเห็นว่าผลเสียที่จะได้รับจากการกระทำผิดนั้นมีมากกว่าผลประโยชน์ที่จะได้รับ ซึ่งจะส่งผลให้คนในสังคมตัดสินใจไม่ประกอบอาชญากรรมอีกต่อไป แนวคิดของสำนักคลาสสิกเน้นที่ความเสรีของมนุษย์ในการตัดสินใจและกระทำตามเหตุผล และมุ่งหมายที่จะเสริมสร้างระบบการปกครองที่ทำให้คนในสังคมไม่กลัวการถูกลงโทษมากกว่าความเสียหายจากการกระทำผิดกฎหมายที่ทำได้ ซึ่งเชื่อว่าจะส่งผลให้คนในสังคมตัดสินใจให้ถูกต้องและมีเหตุผลเพื่อประกอบอาชญากรรมให้เกิดประโยชน์สูงสุดในทางวัตถุและความสงบสุขของสังคม Freda A., & Mueller, Gerhard & Laufer, 1991) แนวคิดนี้มีหลักการสำคัญที่เชื่อว่า มนุษย์มีเจตจำนงอิสระในการตัดสินใจและเลือกการกระทำ โดย

มีการคำนึงถึงผลกระทำที่เกิดขึ้นในกรณีที่ประกอบอาชญากรรม โดยพิจารณาผลดีและผลเสียที่อาจเกิดขึ้นกับบุคคลที่กระทำผิดกฎหมาย ความเห็นนี้เกิดจากการพิจารณาว่าความเสียหายที่อาจเกิดขึ้นกับบุคคลที่กระทำผิดนั้นมากกว่าโทษที่อาจต้องได้รับ ซึ่งจะทำให้บุคคลในสังคมไม่เกรงกลัวบทลงโทษและเป็นแนวคิดที่ให้ความสำคัญกับการกระทำที่แสดงออกมาแทนที่จะสนใจถึงพฤติกรรมของบุคคล แนวคิดของสำนักคลาสสิกเกี่ยวข้องกับงานวิจัยเรื่องนี้เนื่องจากมีกรณีของคอลเซ็นเตอร์ที่เป็นชาติต่างประเทศกระทำผิดในประเทศไทย ซึ่งอาจไม่กลัวกฎหมายหรือบทลงโทษในประเทศไทย นอกจากนี้อาจมองเห็นว่ามีโอกาสหลบหลีกการถูกจับกุมจากเจ้าหน้าที่ตำรวจ ซึ่งอาจเป็นสาเหตุจูงในการกระทำผิดของคอลเซ็นเตอร์ ซึ่งเป็นแนวคิดที่สำคัญในงานวิจัยนี้ การจัดการกับแก๊งคอลเซ็นเตอร์จึงควรเน้นการบังคับใช้กฎหมายอย่างรวดเร็วและมีการติดตามดำเนินคดีอย่างจริงจัง เพื่อสร้างความมั่นใจให้สังคมว่าอาชญากรรมไซเบอร์เหล่านี้ไม่สามารถเกิดขึ้นได้โดยไม่มีผลตามมา

2. ทฤษฎีคิดก่อนกระทำผิด (Rational Choice Theory) เป็นทฤษฎีที่เชื่อว่าบุคคลมีอิสระในการเลือกที่จะกระทำผิดกฎหมาย และแนวทางในการกระทำผิดกฎหมายขึ้นอยู่กับความพึงพอใจหรือผลประโยชน์ที่ต้องการ ซึ่งไม่จำกัดเพียงในรูปของทรัพย์สินเท่านั้น แต่ยังครอบคลุมผลประโยชน์หรือความพึงพอใจด้านจิตใจด้วย ในทฤษฎีคิดนี้ การกระทำผิดกฎหมายขึ้นอยู่กับการคำนึงถึงผลที่จะตามมาหลังจากที่กระทำผิด ไม่ว่าจะเป็นผลเสียที่ได้รับหรือความพยุงพอใจในด้านต่างๆ อย่างไรก็ตามความพึงพอใจหรือผลประโยชน์ที่ต้องการสูงสุดไม่จำเป็นต้องเกี่ยวข้องเพียงแค่เงินเท่านั้น แต่ยังอาจรวมถึงด้านจิตใจด้วยทฤษฎีคิดนี้มองว่าอาชญากรมีคุณสมบัติที่แตกต่างกันไป ได้แก่ ความชำนาญในการประกอบอาชญากรรม ทรัพย์สินหรือผลประโยชน์ที่ได้รับจากการกระทำผิด และสภาพแวดล้อมโดยทั่วไปที่มีโอกาสในการกระทำผิด ซึ่งจะมีผลกระตุนหรือมูลเหตุจูงใจในการกระทำผิดของอาชญากรด้วย ดังนั้น ทฤษฎีคิดก่อนกระทำผิดมีสมมติฐานที่บุคคลเป็นผู้มีอิสระในการเลือกที่จะกระทำผิดกฎหมายและการเลือกพฤติกรรมอาชญากรรมผิดกฎหมายขึ้นอยู่กับการคำนึงถึงความพึงพอใจหรือผลประโยชน์ที่ต้องการ ซึ่งไม่จำเป็นต้องเกี่ยวข้องเพียงแค่เงินเท่านั้น แต่ยังครอบคลุมด้านจิตใจด้วย (Larry, 2006)

โดยนักคิดกลุ่มนี้ได้มองว่าอาชญากรต้องมีคุณสมบัติ 2 ประการในการที่จะประกอบอาชญากรรม คือ

1. คุณสมบัติของการประกอบอาชญากรรม อาชญากรจะมีพฤติกรรมแตกต่างกันไปตามรูปแบบของอาชญากรรม ซึ่งการประกอบอาชญากรรมอาจแตกต่างกันในด้านความชำนาญ ทรัพย์สิน ผลประโยชน์ที่จะได้รับ และจำนวนเหยื่อที่มีในกระทำอาชญากรรม

2. คุณสมบัติของอาชญากรรม โดยคำนึงถึงการตัดสินใจในการประกอบอาชญากรรม คำนึงถึงสภาพแวดล้อมได้แก่โอกาส ผลเสีย ประโยชน์ ความเสี่ยงและแรงจูงใจที่จะกระทำอาชญากรรม ซึ่งส่งผลให้อาชญากรตัดสินใจในการประกอบอาชญากรรมโดยคำนึงถึงผลตอบแทนที่มีมูลค่าสูงหรือเป็นตัวตน นอกจากนี้หากอาชญากรคำนวณระหว่างโทษและผลประโยชน์ที่จะได้รับอีกด้วย หากโทษน้อยกว่าและได้ผลประโยชน์อาชญากรก็ตัดสินใจที่จะประกอบอาชญากรรมอยู่ดี

ในทฤษฎีคิดก่อนกระทำผิด อาชญากรต้องคำนึงถึงการตัดสินใจในการประกอบอาชญากรรม คำนึงถึงสภาพแวดล้อมในการประกอบอาชญากรรม โอกาสในการกระทำผิด ผลที่จะได้รับ ประโยชน์ ความเสี่ยงเพื่อชั่งน้ำหนักที่จะกระทำความผิดและต้องมีแรงจูงใจที่จะประกอบอาชญากรรม โดยคำนึงถึงผลตอบแทนที่มีมูลค่าสูง (พรชัย ขันตี, กฤษณะพงศ์ ฟูตระกูล และจอมเดช ตรีเมฆ, 2558) ในกรณีของแก๊งคอลเซ็นเตอร์มักมีการวางแผนและดำเนินการอย่างเป็นระบบ ซึ่งสะท้อนถึงการใช้ทฤษฎีคิดก่อนกระทำผิดอย่างชัดเจน โดยพวกเขาจะประเมินถึงโอกาสที่สามารถหลอกลวงผู้คนได้สำเร็จ รวมถึงวิเคราะห์กลุ่มเป้าหมายที่มีโอกาสถูกหลอกมากที่สุด เช่น กลุ่มคนสูงอายุหรือคนที่มีความรู้ทางเทคโนโลยีน้อย ซึ่งมีแนวโน้มที่จะเชื่อในข้อมูลที่ได้รับมากกว่า และจากการคิดอย่างเป็นระบบนี้ แก๊งคอลเซ็นเตอร์จึงมุ่งเป้าหมายไปยังกลุ่มคนที่มีความเสี่ยงมากที่สุด โดยคาดหวังว่าจะได้รับผลตอบแทนสูงจากการลงมือหลอกลวง

3. ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) เป็นทฤษฎีที่ถูกพัฒนาโดย Cohen & Felson ซึ่งหมายถึง กิจวัตรหรือการกระทำที่เกิดขึ้นบ่อยครั้งและประจำ เช่น การออกไปทำงาน ปล่อยให้บ้านไม่มีคนเฝ้า การสวมใส่เครื่องประดับที่มีราคาแพง รวมถึงลักษณะของบุคคลที่อาจเป็นเหยื่ออาชญากรรมได้ง่าย เช่น เพศหญิง อายุน้อยหรืออายุมาก

ทฤษฎีกิจวัตรประจำวันมองว่ากิจกรรมประจำวันที่มนุษย์เราทำเสมอๆ มีความสัมพันธ์กับการเกิดอาชญากรรม ถ้ามีการดูแลหรือผู้ป้องกัน (Guardian) มากขึ้น เช่น มีคนเฝ้าระมัดระวังหรือสกัดหัวใจและมีการเข้าร่วมกิจกรรมประจำวันอย่างใกล้ชิด จะทำให้ลดความเสี่ยงหรือเป้าหมายของการกระทำอาชญากรรมลงได้ ในทางกลับกัน ถ้าลดจำนวนคนดูแลหรือผู้ป้องกัน สถิติอาชญากรรมจะมีโอกาสสูงขึ้น ทฤษฎีกิจวัตรประจำวันเสนอแนวคิดว่า การมีกิจกรรมประจำวันของคนที่เป็นอย่างสม่ำเสมอ ตั้งแต่เช้าออกจากบ้านไปทำงาน/โรงเรียนจนถึงกลับบ้าน ทุกวันธรรมดา จะเป็นปัจจัยที่ส่งผลต่อโอกาสในการเกิดอาชญากรรม เช่น อาชญากรรมเกิดขึ้นเช่นเดียวกันทุกสัปดาห์ กระทำเช่นนี้เหมือนกันโดยไม่เปลี่ยนแปลง อาชญากรสังเกตและวางแผนได้ว่าคนคนนี้จะทำอะไรต่อไป การทำกิจกรรมประจำวันเช่นนี้เป็นปัจจัยที่เสี่ยงในการก่ออาชญากรรม (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563) ทฤษฎีกิจวัตร

ประจำวัน (Routine Activity Theory) เป็นทฤษฎีที่ใช้อธิบายสาเหตุของการก่ออาชญากรรมหรือการกระทำความผิด โดยให้ความสำคัญกับองค์ประกอบสำคัญ 3 ประการคือ

1. เหยื่อหรือเป้าหมายที่เหมาะสม (Suitable Target) คือเหยื่อหรือเป้าหมายที่อยู่ในเงื่อนไขที่เหมาะสมในการเกิดอาชญากรรม มีความชอบที่จะเป็นเหยื่อและเสี่ยงต่อการเกิดอาชญากรรม อาจเป็นคน สิ่งของ หรือสถานที่ อย่างเช่น คนที่อยู่ในสภาพแวดล้อมที่ไม่ปลอดภัย เป็นต้น หรือสถานที่ที่มีความไม่มีคนเฝ้าระมัดระวัง

2. การขาดผู้ดูแลสถานที่นั้นๆ (Absence of a Capable Guardian) เงื่อนไขนี้หมายถึง การไม่มีผู้ดูแลหรือมีผู้ดูแลที่ไม่สามารถป้องกันอาชญากรรมได้ ผู้ดูแลสามารถเป็นคนหรืออุปกรณ์ต่างๆ เช่น ตำรวจลาดตระเวน พนักงานรักษาความปลอดภัย เพื่อนบ้าน หรือกล้องวงจรปิด

3. บุคคลที่มีแนวโน้มหรือแรงจูงใจที่จะก่อให้เกิดการกระทำผิด (Likely and Motivated Offenders) เงื่อนไขนี้เกี่ยวข้องกับบุคคลที่มีแรงจูงใจหรือเจตนาในการกระทำความผิด อาจเป็นผู้ที่ต้องการรับสิ่งของหรือเงิน แรงจูงใจส่วนบุคคล หรือความไม่พอใจต่อสถานการณ์ ซึ่งทำให้พร้อมที่จะก่ออาชญากรรม (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

ในกรณีของแก๊งคอลเซ็นเตอร์ ผู้กระทำผิดที่มีแรงจูงใจ คือแก๊งคอลเซ็นเตอร์ที่มุ่งหาผลประโยชน์จากการหลอกลวงประชาชน โดยการโทรศัพท์หลอกลวงหรือใช้เทคนิคทางจิตวิทยาเพื่อกระตุ้นให้เหยื่อทำตามคำสั่งเพื่อให้ได้ผลประโยชน์ทางการเงิน พวกเขามีแรงจูงใจสูงในการเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินของเหยื่อ และใช้เทคนิคต่าง ๆ เพื่อเพิ่มความน่าเชื่อถือในการหลอกลวง เหยื่อที่เข้าถึงได้ง่ายนั้นหมายถึงประชาชนทั่วไปที่มีการใช้โทรศัพท์หรือออนไลน์ในชีวิตประจำวัน และอาจไม่ได้ระมัดระวังตัวอยู่เสมอ โดยเฉพาะเมื่อถูกหลอกลวงให้คิดว่ามีปัญหาที่ต้องแก้ไขหรือมีผลประโยชน์ที่สามารถได้รับทันที เหยื่อส่วนใหญ่มักจะทำธุรกรรมหรือใช้เทคโนโลยีในกิจวัตรประจำวัน ซึ่งทำให้แก๊งคอลเซ็นเตอร์มีโอกาสเข้าถึงได้ง่ายผ่านการโทรศัพท์และออนไลน์ และในส่วนของการขาดแคลนผู้ป้องกัน นั้นหมายถึงการที่ประชาชนอาจไม่ได้รับการเฝ้าระวังหรือการเตือนเกี่ยวกับกลโกงอย่างเพียงพอ การขาดข้อมูลหรือความรู้เกี่ยวกับภัยไซเบอร์ทำให้พวกเขาตกเป็นเหยื่อได้ง่ายขึ้น แม้ว่าบางครั้งจะมีมาตรการป้องกันจากสถาบันการเงินหรือผู้ให้บริการโทรคมนาคม แต่ก็อาจไม่เพียงพอหรือไม่ทันต่อเทคนิคที่แก๊งคอลเซ็นเตอร์ใช้ในการโจมตี

4. แนวคิดของสำนักปฏิฐานนิยม (Positive School) จริง ๆ แล้วกลุ่มนี้มีความแตกต่างกับสำนักคลาสสิค (Classical School) โดยส่วนใหญ่คือสนับสนุนในการสำรวจประเภทของคนที่เกี่ยวข้องกับอาชญากรรมและการกระทำความผิด โดยใช้แนวคิดที่มีต้นกำเนิดจากสาเหตุและเงื่อนไขทางสังคมที่กระทำให้เกิดพฤติกรรมอาชญากรรมขึ้น ซึ่งเน้นความสัมพันธ์ระหว่าง

พฤติกรรมอาชญากรรมกับสภาพแวดล้อมและสังคมของบุคคลนั้น ๆ นักปฏิฐานนิยมน่าจะคาดคะเนหรืออธิบายพฤติกรรมอาชญากรรมด้วยการพิจารณาตัวบ่งชี้ทางสังคมและสภาพแวดล้อมที่แทรกซึมเข้ามาต่อการกระทำอาชญากรรมของบุคคล แนวคิดนี้จึงเน้นการศึกษาปัจจัยต่าง ๆ ที่อยู่ร่วมกับกระบวนการเกิดอาชญากรรม หากมีสภาพแวดล้อมที่กระตุ้นให้เกิดพฤติกรรมอาชญากรรมมากขึ้น และตัวบ่งชี้ที่บ่งชี้ถึงความเสี่ยงของบุคคลนั้น ก็จะทำให้เกิดโอกาสการกระทำอาชญากรรมได้มากขึ้นเช่นกัน

นักปฏิฐานนิยมคิดว่ามนุษย์เกิดมามีความแตกต่างกัน โดยไม่ใช่เพียงคนสามวัยและต้องสงสัยหรือมีประสิทธิภาพในการทำความผิด เนื่องจากสภาพแวดล้อมและสังคมที่มนุษย์เกิดมาอยู่จะส่งผลต่อพฤติกรรมของเขา สิ่งเหตุการณ์และสภาพแวดล้อมที่บ่งชี้ถึงความรับผิดชอบในการกระทำอาชญากรรมควรถูกสำรวจเพื่อให้เกิดความเข้าใจในกระบวนการเกิดอาชญากรรม และสามารถวางแผนการป้องกันการกระทำอาชญากรรมได้ โดยเน้นในการสร้างสภาพแวดล้อมที่เป็นสิ่งกีดขวางหรือลดความเสี่ยงในการเกิดอาชญากรรมให้น้อยลง (Freda A., & Mueller, Gerhard & Laufer, William, 1991)

ในการหลอกลวงของแก๊งคอลเซ็นเตอร์ การสร้างความเชื่อมั่นและการตีความที่เฉพาะเจาะจงจะช่วยให้เหยื่อเกิดความรู้สึกปลอดภัยและเชื่อถือได้ในสิ่งที่ผู้หลอกลวงนำเสนอ ตัวอย่างเช่น แก๊งคอลเซ็นเตอร์อาจใช้การสร้างสถานการณ์ที่น่าเชื่อถือ เช่น การอ้างถึงหน่วยงานราชการหรือบริษัทที่มีชื่อเสียง เพื่อให้เหยื่อรู้สึกว่าตนกำลังติดต่อกับผู้มีอำนาจหรือแหล่งที่เชื่อถือได้ ซึ่งการใช้แนวทางนี้ช่วยเพิ่มโอกาสในการหลอกลวงได้อย่างมีประสิทธิภาพ

5. ทฤษฎีความแตกต่างในการคบหาสมาคมหรือความสัมพันธ์ที่แตกต่าง (Theory of Differential Association) โดยซัทเธอร์แลนด์ (Sutherland) เป็นทฤษฎีที่อธิบายถึงสาเหตุของพฤติกรรมอาชญากรรมว่าเกิดขึ้นจากกระบวนการเรียนรู้และติดต่อสัมพันธ์กับผู้อื่นภายในกลุ่มที่สนิทสนมหรือคุ้นเคยกัน โดยมีหลักสำคัญดังนี้

1) เกิดจากการเรียนรู้ไม่ใช่เกิดจากการถ่ายทอดจากบรรพบุรุษ ทฤษฎีนี้เน้นว่าพฤติกรรมอาชญากรรมไม่ได้เกิดขึ้นจากกระบวนการถ่ายทอดความพยุงสอนเท่านั้น แต่เกิดจากกระบวนการเรียนรู้และติดต่อกับผู้อื่นภายในกลุ่มที่คุ้นเคยกัน

2) การเรียนรู้โดยมีปฏิกิริยาตอบโต้กับผู้อื่นในกระบวนการติดต่อสัมพันธ์ ความเชื่อในสังคมและพฤติกรรมอาชญากรรมนั้นเกิดขึ้นด้วยกระบวนการเรียนรู้และสร้างขึ้นจากปฏิกิริยากับคนอื่น ๆ ในกระบวนการติดต่อสัมพันธ์

3) ส่วนสำคัญของการเรียนรู้พฤติกรรมอาชญากรรมเกิดขึ้นภายในกลุ่มที่สนิทสนมคุ้นเคยกันความสัมพันธ์ที่คนเรียนรู้และพัฒนาพฤติกรรมอาชญากรรมเกิดขึ้นในกลุ่มที่สนิทสนมและมีความสัมพันธ์กัน

4) การเรียนรู้พฤติกรรมอาชญากรรมเรียนรู้ถึงเทคนิคในการประกอบอาชญากรรมและทิศทางของแรงจูงใจเหตุผลและทัศนคติต่างๆ คนที่เรียนรู้พฤติกรรมอาชญากรรมจะเรียนรู้เกี่ยวกับวิธีการทำอาชญากรรม แรงจูงใจและทัศนคติที่เกี่ยวข้อง

5) การที่จะมีแรงจูงใจหรือความต้องการในการกระทำอย่างไร เรียนรู้จากการกำหนดในกฎหมาย ความต้องการในการกระทำอาชญากรรมหรือแรงจูงใจของบุคคลส่วนมากเกิดจากกระบวนการเรียนรู้จากกฎหมายที่กำหนดให้กระทำอาชญากรรม

6) คนกระทำผิดกฎหมายเพราะมีการกำหนดให้ชอบที่จะละเมิดกฎหมายมากกว่าที่กำหนดไม่ให้กระทำอย่างนั้น ความพยุงสอนและเรียนรู้การกระทำอาชญากรรมมีผลต่อแรงจูงใจและความเชื่อในการละเมิดกฎหมาย คนที่เรียนรู้พฤติกรรมอาชญากรรมมากกว่าที่เรียนรู้พฤติกรรมไม่กระทำอาชญากรรมจะมีแรงจูงใจหรือความต้องการในการกระทำอาชญากรรมมากกว่าคนที่ไม่เคยเรียนรู้พฤติกรรมนั้น

7) การเข้าสมาคมกับกลุ่มที่แตกต่างกันนี้เกิดขึ้นมากน้อยต่างกันในความถี่การจัดลำดับก่อนหลังและความรู้สึกแรงกล้า การเข้าสมาคมกับกลุ่มที่มีพฤติกรรมอาชญากรรมแตกต่างกันอยู่มากน้อยและมีความรู้สึกแรงกล้าในการละเมิดกฎหมายจะมีผลต่อพฤติกรรมอาชญากรรมของบุคคลนั้น

8) กระบวนการเรียนรู้พฤติกรรมอาชญากรรมโดยการเข้าสมาคมกับผู้ที่เป็นแบบอย่างในการเป็นอาชญากรหรือผู้เป็นแบบอย่างในการเป็นประประษฐ์ต่ออาชญากร การเรียนรู้พฤติกรรมอาชญากรเกิดจากกระบวนการติดต่อกับบุคคลที่เป็นแบบอย่างในการเป็นอาชญากรหรือบุคคลที่เป็นแบบอย่างในการเป็นปษฐ์ต่ออาชญากร การติดต่อกับเหตุการณ์และการเรียนรู้พฤติกรรมอาชญากรจะเป็นนอกเหนือจากการเรียนรู้เรื่องอื่น ๆ

9) พฤติกรรมอาชญากรนั้นแสดงออกถึงความต้องการและความคาดหวังโดยทั่วไป พฤติกรรมอาชญากรรมที่แสดงออกจะสื่อถึงความต้องการและความคาดหวังของบุคคลที่กระทำ พฤติกรรมอาชญากรรมนี้สามารถเป็นตัวบ่งชี้ให้เห็นความต้องการและความคาดหวังที่อยู่ข้างในบุคคลนั้น ๆ

สรุปคือทฤษฎีความแตกต่างในการคบหาสมาคมหรือความสัมพันธ์ที่แตกต่าง (Theory of Differential Association) เน้นว่าพฤติกรรมอาชญากรรมเกิดขึ้นจากกระบวนการเรียนรู้และติดต่อสัมพันธ์กับผู้อื่นในกลุ่มที่คุ้นเคยกัน คนที่อยู่ในกลุ่มที่มีพฤติกรรมอาชญากรรมมากกว่าที่มี

พฤติกรรมไม่กระทำอาชญากรรมจะมีโอกาสในการกระทำอาชญากรรมมากกว่า และความต้องการและความคาดหวังของบุคคลนั้นๆ ส่งผลต่อพฤติกรรมอาชญากรรมด้วยเช่นกัน (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

กรณีการกระทำของแก๊งคอลเซ็นเตอร์มักเกิดขึ้นในบริบทของกลุ่มหรือเครือข่ายที่มีการฝึกอบรมและถ่ายทอดความรู้เฉพาะด้านให้แก่สมาชิกใหม่ โดยสมาชิกของแก๊งจะเรียนรู้วิธีการหลอกลวงที่มีประสิทธิภาพ เช่น การพูดจาที่โน้มน้าวใจ การสร้างเรื่องราวที่น่าเชื่อถือ และการใช้เทคโนโลยีในการเข้าถึงข้อมูลส่วนตัวของเหยื่อ พวกเขาจะได้รับการสนับสนุนจากสมาชิกในกลุ่มให้ทำการหลอกลวงอย่างต่อเนื่อง และจะได้รับการส่งเสริมให้มองว่าการกระทำเหล่านี้เป็นเรื่องปกติ ในขณะเดียวกันความสัมพันธ์ที่แตกต่างระหว่างสมาชิกในแก๊งคอลเซ็นเตอร์และสังคมภายนอกจะถูกสร้างขึ้น โดยสมาชิกในแก๊งมักมีความเชื่อร่วมกันว่าการหลอกลวงเป็นวิธีที่สามารถสร้างรายได้ได้อย่างรวดเร็ว ทำให้พวกเขามองว่าการกระทำนี้เป็นวิธีการที่มีความถูกต้องและเหมาะสมในสถานการณ์นี้ นอกจากนี้ การได้รับผลประโยชน์ทางการเงินจากการหลอกลวงยังทำให้สมาชิกในแก๊งรู้สึกว่าเป็นการประสบความสำเร็จ และจุดประกายให้พวกเขาสานต่อการกระทำผิดมากยิ่งขึ้น

6. ทฤษฎีวัฒนธรรมรอง (Sub-Cultural Theories) คือทฤษฎีที่สำรวจและอธิบายพฤติกรรมอาชญากรรมโดยให้ความสำคัญกับวัฒนธรรมหรือกลุ่มย่อยภายในสังคมที่คนส่วนใหญ่ยึดถือและปฏิบัติตาม การเรียนรู้และยอมรับวัฒนธรรมรองนี้สามารถนำไปสู่การประกอบอาชญากรรมในบางกรณี ทฤษฎีวัฒนธรรมรองมีความเกี่ยวข้องกับการเรียนรู้ทางสังคมและพฤติกรรมที่เกิดขึ้นจากการละเมิดบรรทัดฐานของสังคม การเรียนรู้วัฒนธรรมรองในการละเมิดบรรทัดฐานนี้มักจะเกิดขึ้นในกลุ่มย่อยหรือกลุ่มยากจนในสังคมที่มีความแตกต่างกัน ทฤษฎีวัฒนธรรมรองของทราสเซอร์ (Trasher) ได้กล่าวว่าในสังคมมีวัฒนธรรมหลักที่คนส่วนใหญ่ยึดถือและปฏิบัติตาม แต่ยังมีวัฒนธรรมรองที่เป็นของกลุ่มย่อยในสังคมและอาจนำไปสู่การประกอบอาชญากรรม สำคัญในทฤษฎีนี้คือต้องการผู้ที่สนับสนุนว่าพฤติกรรมดังกล่าวมีความถูกต้อง ดังนั้น การเรียนรู้วัฒนธรรมรองจึงทำให้มีพฤติกรรมเบี่ยงเบนหรือการกระทำผิดเกิดขึ้นในสังคม ทฤษฎีวัฒนธรรมรองแบบของชนชั้นกลาง (Albert Cohen) ได้กล่าวว่า วัฒนธรรมรองเป็นส่วนรวมของเหยื่อที่ต้องการรายได้ในจำนวนมาก ซึ่งมีลักษณะ 3 ประการคือ ความสามารถรอบด้าน การแสวงหาความสุขชั่วและความเป็นอิสระของกลุ่ม และอาจทำให้กลุ่มต้องการรายได้จำนวนมากจากการกระทำผิดที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์

การกระทำผิดของแก๊งคอลเซ็นเตอร์ (Gang) มักมีความเกี่ยวข้องกับแนวคิดและทฤษฎีด้านเหยื่ออาชญากรรม ตัวอย่างเช่น ทฤษฎีการมีส่วนรวมของเหยื่อ (Victim Precipitation Theory) ของ

โมร์วินก๊งกี้ (Marvin Wolfgang) ได้อธิบายว่าเหยื่อบางคนมีส่วนทำให้ตนเองเผชิญกับเหตุการณ์ที่นำไปสู่การตกเป็นเหยื่อ ตัวเหยื่ออาจใช้คำขู่หรือคำโทษทางทายหรืออาจจะเป็นผู้ยั่วยุหรือริเริ่มในการทำร้ายก่อนก็ได้ รูปแบบนี้เรียกว่า "Victim-Precipitation Crime" หรืออาชญากรรมที่เหยื่อมีส่วนรวม (มนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

แก๊งคอลเซ็นเตอร์มีลักษณะการทำงานที่เป็นระบบ มีการแบ่งหน้าที่และความรับผิดชอบอย่างชัดเจน สมาชิกในกลุ่มจะได้รับการฝึกฝนในการใช้เทคนิคการหลอกลวงที่มีประสิทธิภาพ รวมถึงการสื่อสารกับเหยื่ออย่างมีศิลปะ เพื่อสร้างความเชื่อมั่นและลดความสงสัย ซึ่งแสดงให้เห็นถึงการพัฒนาทักษะเฉพาะทางในวัฒนธรรมรองนี้ แม้จะมีผลกระทบที่เป็นอันตรายต่อเหยื่อ นอกจากนี้สมาชิกในกลุ่มนี้อาจได้รับการสนับสนุนจากเพื่อนร่วมงานหรือคนในกลุ่มเดียวกัน ทำให้พวกเขามีความเชื่อมั่นในความถูกต้องของการกระทำเหล่านี้

7. ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) เป็นทฤษฎีที่อธิบายถึงสาเหตุหรือประกอบการเกิดอาชญากรรมได้อย่างชัดเจน ทฤษฎีนี้ประกอบด้วยด้านต่าง ๆ ที่ส่งผลต่อการเกิดอาชญากรรม ซึ่งถูกนำไปใช้ในการกำหนดยุทธศาสตร์หรือกลยุทธ์ในการป้องกันและปราบปรามอาชญากรรมในพื้นที่ต่าง ๆ ตั้งแต่ด้านการปฏิบัติงานของตำรวจทุกระดับได้เพื่อลดอาชญากรรมให้เกิดขึ้นน้อยลง และเป็นที่นิยมในการใช้ในด้านการปฏิบัติงานด้านการป้องกันอาชญากรรม

ทฤษฎีสามเหลี่ยมอาชญากรรมประกอบด้วยด้านต่าง ๆ ดังนี้

1. ด้านผู้กระทำผิดหรือคนร้าย (Criminals) หมายถึงผู้ที่มีความต้องการ (Desire) จะก่อเหตุกระทำผิด ในที่นี้เป็นการอธิบายพฤติกรรมของคนที่มีความต้องการที่จะกระทำอาชญากรรม และเป็นแรงจูงใจในการกระทำผิด

2. ด้านเหยื่อ (Victims) เป้าหมาย (Target) หมายถึงบุคคล สถานที่ หรือวัตถุที่เป็นเป้าหมายของผู้กระทำผิดหรือคนร้าย ในที่นี้เป็นผู้ที่เสียหายหรือเหยื่อหรือประชาชนทั่วไปที่อยู่ในขอบเขตหรือพื้นที่ที่ผู้กระทำผิดหรือคนร้ายมุ่งหมาย และเป็นผู้ที่ต้องการของผู้กระทำผิด

3. ด้านโอกาส (Opportunity) หมายถึงช่วงเวลา (Time) และสถานที่ (Place) ที่เหมาะสมที่ผู้กระทำผิดหรือคนร้ายมีความสามารถในการกระทำผิดหรือก่ออาชญากรรม ในที่นี้เป็นการอธิบายถึงสถานการณ์ที่เหมาะสมที่คนร้ายหรือผู้กระทำผิดมีโอกาสเข้ามากระทำอาชญากรรม อาทิเช่น ช่วงเวลาที่ไม่มีคนสัญญาณอยู่ สถานที่ที่มืดและไม่มีคนเห็น เป็นต้น

เมื่อเกิดสถานการณ์หรือเหตุการณ์ที่รวมด้านต่างๆ ของทฤษฎีสามเหลี่ยมอาชญากรรมครบถ้วน กล่าวคือ ผู้กระทำผิด (Criminals) มีความต้องการ, เหยื่อ (Victims) เป้าหมาย และมีโอกาสในการกระทำผิด (Opportunity) อย่างพร้อมเป็นสิ่งสำคัญที่ส่งผลให้เกิดอาชญากรรมขึ้น การ

ป้องกันการกระทำผิดของคนร้ายต้องพยายามลดหรือควบคุมจำนวนคนร้ายในพื้นที่ที่รับผิดชอบ การปรับลงโทษเพื่อลดมูลเหตุการณ์ที่เป็นแรงจูงใจในการกระทำผิดเป็นสำคัญ สำหรับเหยื่อ ต้องรู้จักป้องกันตนเอง และเปิดเผยข้อมูลข่าวสารที่เป็นประโยชน์ต่อประชาชนในการป้องกันตนเองจากการหลอกลวงของคนร้าย ในส่วนของโอกาส ควรตัดโอกาสด้านเวลาด้วยการประชาสัมพันธ์ให้เหยื่อไม่หลงเชื่อต่อการหลอกลวงของแก๊งคอลเซ็นเตอร์ รวมทั้งตัดโอกาสด้านสถานที่โดยการป้องกันการโทรศัพท์หรือการใช้อินเตอร์เน็ตจากต่างประเทศในการหลอกลวงเหยื่อในประเทศไทย เป็นต้น (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

เมื่อพิจารณาถึงการทำงานของแก๊งคอลเซ็นเตอร์ ทฤษฎีสามเหลี่ยมอาชญากรรมสามารถใช้ในการวิเคราะห์การหลอกลวงทางไซเบอร์ได้อย่างมีประสิทธิภาพ เนื่องจากทั้งสามองค์ประกอบนี้มีความสัมพันธ์และทำงานร่วมกันในการก่อให้เกิดการหลอกลวงทางไซเบอร์ดังนี้

ผู้กระทำผิด: แก๊งคอลเซ็นเตอร์ถือเป็นผู้กระทำผิดที่มีความชำนาญในการหลอกลวงและมีการวางแผนที่ดีเพื่อเข้าถึงเหยื่อ โดยมักใช้เทคนิคการสื่อสารที่เป็นมิตรเพื่อสร้างความไว้วางใจ พวกเขาสามารถเข้าถึงข้อมูลและกลยุทธ์ที่มีประสิทธิภาพในการหลอกลวง ซึ่งทำให้การกระทำของพวกเขามีโอกาสที่จะประสบความสำเร็จสูง

เหยื่อ: เหยื่อที่ตกเป็นเป้าหมายของแก๊งคอลเซ็นเตอร์มักมีความอ่อนแอหรือไม่ระมัดระวังในการปกป้องข้อมูลส่วนตัว เช่น ความโลภที่ทำให้หลงเชื่อในข้อเสนอที่ดูน่าสนใจ หรือความกลัวที่ถูกกดดันให้ทำตามคำสั่ง โดยเฉพาะอย่างยิ่งในกรณีที่ผู้กระทำผิดใช้กลยุทธ์ที่อิงตามอารมณ์หรือจิตวิทยาในการเข้าถึงเหยื่อ

สถานที่: ในกรณีของแก๊งคอลเซ็นเตอร์หมายถึง ช่องทางการสื่อสาร เช่น โทรศัพท์ หรืออินเทอร์เน็ต ซึ่งเป็นแพลตฟอร์มที่สะดวกและมีความเสี่ยงต่ำสำหรับผู้กระทำผิดในการเข้าถึงเหยื่อ โดยมีการหลบซ่อนอยู่เบื้องหลังเทคโนโลยี ทำให้การตรวจสอบและติดตามตัวผู้กระทำผิดเป็นไปได้ยาก

สรุปได้ว่าทฤษฎีอาชญากรรมไซเบอร์โดยภาพรวมมุ่งเน้นการศึกษาและอธิบายพฤติกรรมอาชญากรรมที่เกิดขึ้นในสภาพแวดล้อมของโลกไซเบอร์ ซึ่งเกี่ยวข้องกับการใช้เทคโนโลยีและอินเทอร์เน็ต โดยอาชญากรรมไซเบอร์ครอบคลุมการกระทำผิดที่เกิดผ่านหรือใช้คอมพิวเตอร์เป็นเครื่องมือ เช่น การโจรกรรมข้อมูลส่วนตัว การหลอกลวงทางการเงิน การเผยแพร่มัลแวร์ หรือการก่อกวนระบบต่าง ๆ

**1.2 ลักษณะของการหลอกลวงทางไซเบอร์**

การหลอกลวงทางไซเบอร์นั้น นับว่าเป็นภัยคุกคามที่เป็นผลทางอ้อมจากการเข้าใช้บริการไซเบอร์ ซึ่งจะถูกชักนำนั่นโน้มน้าว ชักจูง ด้วยการแสดงให้เห็นถึงความน่าเชื่อถือในลักษณะต่าง ๆ

โดยหลอกให้หลงเชื่อว่าผู้ใช้บริการจะได้รับประโยชน์ในลักษณะต่าง ๆ โดยเฉพาะค่าตอบแทนที่เป็นเงิน ซึ่งผู้วิจัยได้รวบรวมลักษณะของการหลอกลวงทางไซเบอร์ ไว้ดังนี้

1. การประมูลสินค้าทางไซเบอร์โดยหลอกลวง (Internet Auction Fraud)

การโฆษณาขายสินค้าทางไซเบอร์ด้วยวิธีการประมูลสินค้า ผู้ซื้อที่สนใจจะเข้าร่วมการประมูลมักต้องลงทะเบียนเป็นสมาชิกของเว็บไซต์นั้น ๆ ซึ่งโดยทั่วไปจะไม่เสียค่าใช้จ่ายใด ๆ หลังจากนั้นสมาชิกจะได้รับหมายเลขสมาชิกและรหัสผ่าน (password) ผู้ซื้อจะต้องเสนอราคาซื้อแข่งขันกับผู้ซื้อรายอื่น เมื่อเสร็จสิ้นการประมูลถือว่ามีการทำสัญญาซื้อขายระหว่างผู้ประมูลและผู้เสนอขาย โดยจะมีการส่งข้อความทางอีเมล์ (e-mail) แจ้งให้ผู้ซื้อและผู้ขายทราบผลการประมูลและแจ้งรายละเอียดที่จะติดต่อกันได้เพื่อให้ทั้งฝ่ายผู้ซื้อและผู้ขายติดต่อกันในเรื่องการชำระเงินและการส่งมอบสินค้า ลักษณะการหลอกลวงการประมูลสินค้าทางไซเบอร์นั้นเป็นวิธีการซื้อขายสินค้าที่ได้รับความนิยมและเป็นช่องทางการติดต่อซื้อขายสินค้าที่สะดวกรวดเร็ว ในรายงานสำรวจที่กล่าวมาแล้วของบางประเทศพบว่าเป็นวิธีการหลอกลวงที่พบมากที่สุดเช่นกัน การหลอกลวงมีหลายรูปแบบ เช่น ผู้ขายไม่ส่งมอบสินค้าที่ผู้ซื้อประมูลได้เพราะไม่มีสินค้าอยู่จริง การหลอกลวงโดยการปั่นราคาซื้อขาย ผู้ขายหรือบุคคลที่เกี่ยวข้องกับผู้ขายจะเข้าเสนอราคาเพื่อประมูลสินค้าของตนเพื่อให้สินค้ามีราคาสูงขึ้น ทำให้ผู้ซื้อต้องซื้อสินค้าในราคาที่สูงเกินจริง เป็นต้น ผู้ซื้อได้ชำระค่าสินค้าให้แก่ผู้ขายแล้ว แต่ยังไม่ได้รับสินค้า หรือได้รับสินค้าที่ชำรุดเสียหาย หรือเป็นสินค้าที่มีลักษณะไม่ตรงกับที่มีการเสนอขายแต่แรก ด้านผู้ให้บริการประมูลทางอินเทอร์เน็ตเองก็อาจได้รับความเสียหาย เพราะผู้ใช้บริการ (ผู้ซื้อและผู้ขาย) ไม่ให้ความไว้วางใจและไม่ใช้บริการ

2. การให้บริการไซเบอร์โดยหลอกลวง (Cyber Service Provide Scams)

ผู้หลอกลวงจะส่งเช็คจำนวนหนึ่ง (เช่นราว 3.5 ดอลลาร์สหรัฐฯ) ให้แก่ ผู้ใช้บริการ เมื่อมีการเบิกเงินตามเช็คแล้ว ก็ถือว่าผู้บริโภคตกลงที่จะใช้บริการของผู้ให้บริการไซเบอร์ (Cyber Service Provider - CSP) ที่ได้รับแจ้ง ในการนี้อาจจะไม่มีการแจ้งค่าธรรมเนียมหรือค่าใช้จ่ายใด ๆ และมักเป็นการทำสัญญาให้บริการไซเบอร์ที่มีระยะเวลานาน ผู้หลอกลวงจงใจให้ผู้บริโภคหรือผู้ใช้บริการเกิดความสับสนและเข้าใจผิดในสาระสำคัญเกี่ยวกับการบริการนั้น ลักษณะการหลอกลวงนี้ผู้บริโภคจะถูกเรียกเก็บเงินค่าบริการต่าง ๆ จากผู้ให้บริการไซเบอร์ นอกจากนี้ยังอาจจะมีค่าขู่ที่กล่าวว่าถ้าหากผู้ใช้บริการต้องการเลิกสัญญาก่อนครบกำหนดสัญญา จะถูกปรับเป็นจำนวนเงินที่สูง (พระมหาธรรมทส ขนฺติพโล (พืชจันทร์), 2560)

3. การใช้บัตรเครดิตโดยไม่ได้รับอนุญาต (Credit Card Fraud)

การชำระค่าสินค้า ค่าบริการทางอินเทอร์เน็ตที่ได้รับความนิยมที่สุดวิธีหนึ่ง คือ การชำระเงินด้วยบัตรเครดิต เนื่องจากมีความสะดวกแก่ทั้งผู้ซื้อและผู้ขาย ผู้ซื้อสามารถชำระเงินโดยการให้

ข้อมูลบัตรเครดิตคือ หมายเลขบัตรเครดิต ชื่อ-สกุลของผู้ถือบัตร และวันหมดอายุแก่ร้านค้า ร้านค้าสามารถตรวจสอบได้เพียงว่า บัตรดังกล่าวเป็นบัตรที่ออกโดยผู้ออกบัตรจริง แต่ไม่สามารถตรวจสอบตัวบุคคลผู้ใช้บัตรได้ว่าเป็นบุคคลใด ลักษณะการหลอกลวงนี้ใช้วิธีการหลอกลวงเกี่ยวกับการชำระเงินด้วยบัตรเครดิตทางอินเทอร์เน็ตมีหลายวิธี ตัวอย่างเช่น การให้บริการดูภาพลามกอนาจารโดยไม่เสียค่าใช้จ่ายใด ๆ สำหรับผู้ที่มีอายุตั้งแต่ 18 ปีขึ้นไป แต่ผู้บริโภคต้องแจ้งข้อมูลบัตรเครดิตให้ผู้ให้บริการทราบเพื่อตรวจสอบความถูกต้องของข้อมูล แล้วผู้หลอกลวงจะใช้ข้อมูลนี้ไปกระทำผิดในที่อื่น ผู้ถือบัตรที่เป็นผู้บริโภคถูกเรียกเก็บเงินค่าสินค้าหรือบริการจากบริษัทหรือธนาคาร ผู้ออกบัตรทั้งที่ผู้ถือบัตรไม่ได้ใช้บัตรเครดิตชำระรายการนั้น ๆ เลย ซึ่งกฎหมายบางประเทศจะให้ความคุ้มครองผู้ถือบัตรในกรณีนี้ หรือผู้ถือบัตรรับผิดไม่เกินจำนวนเงินที่กำหนดไว้ในข้อตกลงระหว่าง ผู้ออกบัตรและผู้ถือบัตร

4. การเข้าควบคุมการใช้โมเด็มของบุคคลอื่น (International Modem Dialing/Modem Hijacking)

ลักษณะการหลอกลวงนี้เป็นการโฆษณาการให้บริการสื่อลามกอนาจารโดยไม่เสียค่าใช้จ่ายใด ผู้ใช้บริการจะต้องติดตั้งโปรแกรมคอมพิวเตอร์เพื่อดูภาพดังกล่าวหรือเรียกว่า 'viewer' หรือ 'dialer' ของผู้ให้บริการ เมื่อผู้ใช้บริการเปิดดูภาพด้วยโปรแกรมข้างต้นแล้ว การทำงานของโปรแกรมดังกล่าวจะเริ่มเมื่อมีการใช้เครื่องโมเด็ม (modem) ในขณะเดียวกันโปรแกรมฯ จะควบคุมการทำงานของโมเด็มและสั่งให้หยุดการทำงานโดยที่ผู้ใช้บริการไม่รู้ตัว แล้วจะสั่งให้มีการต่อเชื่อมผ่านโมเด็มอีกครั้งหนึ่ง โดยเป็นการใช้โทรศัพท์ทางไกลจากที่ใดที่หนึ่ง แล้วมีการใช้ไซเบอร์อินเทอร์เน็ตอีกครั้งจากที่นั้นเพื่อให้ผู้ใช้บริการสามารถดูเว็บไซต์ ผู้ใช้บริการจะถูกเรียกเก็บเงินค่าโทรศัพท์ทางไกลจำนวนมาก ทั้งที่ผู้ใช้บริการอาจไม่รับรู้ซึ่งเป็นเพราะมีบุคคลอื่นลักลอบใช้โทรศัพท์โดยอาศัยโปรแกรมคอมพิวเตอร์ (พระมหาธรรมทส ขนฺติพโล (พืชจันทร์), 2560)

5. การหลอกลวงให้ใช้บริการเกี่ยวกับเว็บไซต์ (Web Cramming)

ลักษณะของการหลอกลวง คือ การหลอกลวงว่ามีการให้บริการเปิดเว็บเพจ (web page) โดยไม่เสียค่าใช้จ่ายใด ๆ เช่น การเปิดเว็บเพจเป็นเวลา 30 วัน และไม่มีข้อผูกพันใด ๆ ถ้าไม่ใช้บริการต่อไป เมื่อมีการตกลงใช้บริการดังกล่าวแล้ว ผู้ใช้บริการจะถูกเรียกเก็บเงินค่าใช้บริการโทรศัพท์ หรือค่าใช้บริการในการมีเว็บเพจ (ค่าธรรมเนียมการใช้พื้นที่) เป็นจำนวนมากทั้งที่ตนไม่เคยใช้บริการหรือไม่ได้สมัครแต่อย่างใด ผู้ใช้บริการยังไม่สามารถแจ้งให้ผู้ให้บริการยกเลิกได้ทันทีอีกด้วย

6. การหลอกลวงโดยใช้การตลาดหรือการขายแบบตรง (Multilevel Marketing Plans/Pyramids)

ลักษณะการหลอกลวง คือ การหลอกลวงในลักษณะนี้คล้ายคลึงกับการนำสื่อโฆษณาในการทำตลาดหรือการขายตรง โดยมีการชักชวนให้บุคคลทั่วไปเข้าร่วมเป็นสมาชิกในเครือข่ายธุรกิจ โดยการกล่าวอ้างว่าผู้ขายจะได้รับสิทธิในการจำหน่ายสินค้าหลายชนิดและได้รับผลประโยชน์จากการขายสินค้าหรือชักชวนบุคคลอื่นเข้ามาเป็นตัวแทนขายตรงเป็นทอดๆ ทำให้ผู้ที่ได้รับประโยชน์จริงมีจำนวนน้อยราย

7. การหลอกลวงโดยเสนอให้เงินจากประเทศไนจีเรีย (Nigerian Money Offers)

ลักษณะการหลอกลวง คือ ผู้ใช้ไซเบอร์จะได้รับข้อความจากจดหมายหรืออีเมล์ (e-mail) จากบุคคลที่กล่าวอ้างว่ามีความสำคัญในประเทศไนจีเรียเพื่อขอช่วยเหลือในการโอนเงินจำนวนมากไปยังต่างประเทศ โดยผู้ใช้ไซเบอร์จะได้รับเงินส่วนแบ่งจำนวนนับล้านเหรียญดอลลาร์สหรัฐฯ ข้อความในจดหมายหรืออีเมล์มีเนื้อหาที่อ้างอิงว่าประชาชนในประเทศไนจีเรียไม่สามารถเปิดบัญชีเงินฝากในต่างประเทศหรือโอนเงินออกนอกประเทศที่มีมูลค่าราว 10 ล้านดอลลาร์สหรัฐฯ ได้ หรือรัฐบาลไนจีเรียต้องการทำธุรกิจกับชาวต่างชาติจึงต้องการความช่วยเหลือจากชาวต่างชาติในการเปิดบัญชีเงินฝากประเภทกระแสรายวันที่เบิกด้วยเช็ค ซึ่งผู้ใช้ไซเบอร์จะได้รับค่าตอบแทนหรือค่านายหน้า ผู้ใช้ไซเบอร์เพียงแต่แจ้งรายละเอียดของบัญชีเงินฝากของตนและกรอกเอกสารพร้อมทั้งลงลายมือชื่อของเจ้าของบัญชีเท่านั้น เมื่อมีการแจ้งข้อมูลบัญชีเงินฝากแล้ว ผู้ใช้ไซเบอร์จะถูกเรียกเก็บค่าธรรมเนียมหรือค่าใช้จ่ายในการดำเนินการตลอดเวลาโดยให้ผู้ใช้โอนเงินเข้าบัญชีที่แจ้งไว้ ผู้ที่หลอกลวงจึงสามารถเบิกเงินจากบัญชีดังกล่าวได้โดยอ้างเอกสารมอบอำนาจของเจ้าของบัญชี แต่การโอนเงินลักษณะนี้อาจทำไม่ได้ในประเทศไทย เว้นแต่จะเป็นการโอนเงินระหว่างบัญชีของธนาคารเดียวกันทางไซเบอร์ (พระมหาธรรมทส ขนฺติพโล (พืชจันทร์), 2560)

8. การหลอกลวงให้ประกอบธุรกิจที่บ้าน (Work-at-Home)

ลักษณะการหลอกลวง คือ บริษัทที่หลอกลวงจะเชิญชวนให้ผู้ต้องการประกอบธุรกิจทางไซเบอร์หรือธุรกิจด้านพาณิชย์อิเล็กทรอนิกส์สมัครเป็นสมาชิกเพื่อทำธุรกิจ โดยผู้ใช้ไซเบอร์มีเพียงเครื่องคอมพิวเตอร์และสามารถใช้อินเทอร์เน็ตจากที่บ้านได้ และมักอ้างว่าธุรกิจประเภทนี้เป็นธุรกิจที่เติบโตอย่างรวดเร็ว ในขณะที่ผู้ใช้ไซเบอร์จะไม่ได้รับคำแนะนำในการทำธุรกิจ ไม่มีข้อมูลธุรกิจที่ชัดเจนหรือไม่ทราบว่าตนอาจไม่ได้รับค่าตอบแทนใด ๆ เลย ผู้ถูกหลอกลวงจะถูกเรียกเก็บเงินค่าสมาชิกหรือซื้ออุปกรณ์ที่จำเป็นเพื่อเริ่มทำธุรกิจ ผู้ลงทุนจะไม่ได้รับเงินค่าตอบแทนตามที่มีการกล่าวอ้าง และอาจต้องสูญเสียเงินจากการลงทุนอีกด้วย

9. การหลอกลวงให้จดทะเบียนโดเมนเนม (Domain name registration scams)

ลักษณะการหลอกลวง คือ ผู้ที่ต้องการทำธุรกิจทางไซเบอร์ที่ต้องการมีเว็บไซต์และโดเมนเนมของตนเอง จะได้รับการเสนอแนะว่า ท่านสามารถได้รับสิทธิในการจดทะเบียนโดเมนเนมในระดับบนที่เรียกว่า "Generic Top-Level Domain" หรือ gTLD ได้แก่ .com, .org, .net, .int, .edu, .gov, .mil, .aero, .biz, .coop, .info, .museum, .name, และ .pro เป็นต้น ก่อนบุคคลอื่น และถูกเรียกเก็บค่าธรรมเนียมในการจองโดเมนเนมที่ต้องการ ซึ่งในความเป็นจริงไม่มีการให้บริการในลักษณะดังกล่าว ผู้ที่หลงเชื่ออาจได้รับความเสียหายเพราะได้ชำระเงินให้แก่ผู้ที่หลอกลวงโดยไม่ได้รับสิทธิหรือประโยชน์ตามที่กล่าวอ้าง

10. การหลอกลวงโฆษณาหรือขายยามหัศจรรย์ (Miracle products)

ลักษณะการหลอกลวง คือ การโฆษณาหรือขายยาทางไซเบอร์ที่อ้างสรรพคุณว่าสามารถรักษาโรคหรืออาการเจ็บป่วยด้วยโรคร้ายแรง เช่น โรคมะเร็ง, โรคภูมิคุ้มกันบกพร่อง (HIV/AIDS), โรคความดันโลหิตสูง ฯลฯ หรือสามารถบรรเทาความเจ็บป่วยได้ภายในระยะเวลาอันสั้น และมักอ้างว่ายาเหล่านี้ได้รับการรับรองหรือการพิสูจน์ทางวิทยาศาสตร์แล้ว ผู้ป่วยที่ซื้อยาดังกล่าวโดยเชื่อว่าสามารถรักษาความเจ็บป่วยได้ อาจต้องสูญเสียเงินหรือโอกาสในการได้รับการรักษาอย่างถูกต้อง นอกจากนั้น ยังอาจได้รับอันตรายจากการใช้ยาเหล่านั้นด้วย

11. การหลอกลวงเพื่อวัตถุประสงค์ด้านอื่น ๆ

การหลอกลวงเพื่อวัตถุประสงค์ด้านอื่น ๆ คือการหลอกลวงที่มีลักษณะแตกต่างกันออกไปมากมายและมีวัตถุประสงค์ที่แตกต่างกัน นอกจากการหลอกลวงตามที่กล่าวมาแล้ว การหลอกลวงเพื่อวัตถุประสงค์ด้านอื่น ๆ เช่น การหลอกลวงเพื่อเรียกค่าไถ่ การหลอลวงเพื่อการอนาจาร การหลอกลวงเพื่อนำเสียหายไปข่มขืนกระทำชิ้นเรา หรือเพื่อริดความมั่งคั่งทรัพย์สินของเหยื่อ โดยเฉพาะการหลอกลวงเพื่อการข่มขืนกระทำชิ้นเรานั้นเกิดขึ้นในสังคมไซเบอร์นั้นเป็นภัยคุกคามที่น่ากลัวมากเพราะเหยื่อมักจะเป็นเด็กที่ยังไม่บรรลุนิติภาวะซึ่งทำให้เกิดความเสียหายทั้งทางด้านสภาพร่างกายและจิตใจ (พระมหาธรรมทส ขนฺติพโล (พืชจันทร์), 2560)

## ลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์

การก่อการร้ายทางไซเบอร์เป็นหนึ่งในปฏิบัติการบนพื้นที่ไซเบอร์ที่ผิดกฎหมายนอกเหนือจากการโจมตีทางไซเบอร์และอาชญากรรมทางไซเบอร์ โดยสามารถพิจารณาความแตกต่างของการกระทำความผิดแต่ละประเภทได้จากวัตถุประสงค์และผลของการดำเนินการ (จิตราภรณ์ โสตถิกุล, 2565) การหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ถือเป็นหนึ่งในกลโกงที่อาชญากรทางไซเบอร์เลือกที่จะนำมาใช้หลอกลวง การกระทำผิดของแก๊งคอลเซ็นเตอร์มักมีลักษณะการกระทำผิด คือ กลโกงของคดีร่วมกันฉ้อโกงประชาชน รูปแบบการหลอกลวงแก๊งคอล

เซ็นเตอร์มักเปลี่ยนแปลงอย่างต่อเนื่องตามสถานการณ์ต่าง ๆ ที่เกิดขึ้น และมักจัดตั้งเป็นกลุ่มองค์กรชัดเจนเพื่อควบคุมและดำเนินการหลอกลวง พวกเขามักแบ่งหน้าที่และบทบาทในการดำเนินงาน เพื่อเพิ่มโอกาสในการสำเร็จของกิจกรรมที่ต้องการ กลุ่มแก๊งคอลเซ็นเตอร์จะแบ่งรายได้ที่ได้มาจากการหลอกลวงตามแบบฉบับของพวกเขา ซึ่งการหลอกลวงอาจแบ่งตามเปอร์เซ็นต์ของเงินเดือนหรือโบนัสที่ได้รับ การหลอกลวงดังกล่าวมักมีผลกระทบที่สำคัญต่อระบบเศรษฐกิจและสังคม เนื่องจากผู้เสียหายอาจต้องสูญเสียเงินหรือทรัพย์สินบางส่วนที่ไม่สามารถกู้คืบคืนได้ สำหรับแก๊งคอลเซ็นเตอร์ที่มีจำนวนมากมายก็มักกระทำการหลอกลวงในหลายประเทศทั่วโลก ซึ่งส่งผลกระทบให้ระบบเศรษฐกิจและสังคมประสบผลกระทบที่สำคัญโดยเฉพาะอย่างยิ่งเมื่อเหยื่อต้องสูญเสียเงินหรือทรัพย์สินอย่างมากขึ้น ในทางเดียวกัน ผลกระทบทางสังคมที่ทำให้เหยื่อเสียหายก็อาจรวมถึงความเสียหายทางจิตใจและอารมณ์ (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

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

**1. รูปแบบของแก๊งคอลเซ็นเตอร์**

รูปแบบการหลอกลวงของแก๊งคอลเซ็นเตอร์มักปรับเปลี่ยนอยู่ตลอดเวลาแล้วแต่สถานการณ์เพื่อให้ยากต่อการติดตามจับกุม มีการจัดตั้งเป็นกลุ่มองค์กรชัดเจน มีการแบ่งสายการบังคับบัญชาและหน้าที่อย่างชัดเจน ส่วนรายได้จากการหลอกลวงจะแบ่งตามเปอร์เซ็นต์โดยจะมีเงินเดือนประจำ ปัจจุบันยังมีคนตกเป็นเหยื่อออยู่เป็นระยะ ๆ จนส่งผลกระทบต่อภาพลักษณ์ประเทศอย่างร้ายแรง

1.1 การจัดองค์กร

กลุ่มมิจฉาชีพที่เกี่ยวข้องกับอาชญากรรมข้ามชาติทางด้านการโทรศัพท์ (Call center) มีลักษณะที่ถือเป็นอาชญากรรมข้ามชาติตามคำนิยามของอนุสัญญาของสหประชาชาติที่เกี่ยวกับการต่อต้านองค์กรอาชญากรรมข้ามชาติ กลุ่มมิจฉาชีพนี้มีวิธีการหลอกลวงคนไทยหรือจ้างคนไทยให้เป็นพนักงานในศูนย์โทรศัพท์นอกประเทศเพื่อทำการหลอกลวงผู้เสียหายที่เป็นคนไทยหรืออาศัยอยู่ในประเทศไทย ความเสียหายที่เกิดขึ้นนี้เป็นในประเทศไทย และมีผู้ที่จัดการถอนเงินสดจากตู้ถอนเงินสดอัตโนมัติหรือที่เรียกว่า "ม้าถอนเงิน" เพื่อดำเนินการถอนเงินสดในประเทศไทย

ประเทศไต้หวัน ประเทศมาเลเซีย หรือสาธารณรัฐประชาชนจีน เป็นต้น กลุ่มองค์กรอาชญากรรมสามารถแบ่งการทำงานออกเป็น 4 หน้าที่ด้วยกัน โดยทำหน้าที่ดังนี้

1.1.1 กลุ่มคอลเซ็นเตอร์

กลุ่มคอลเซ็นเตอร์นี้มีการตั้งศูนย์โทรศัพท์หรือ Call center ในต่างประเทศเพื่อสะดวกในการควบคุมพนักงานผู้ทำหน้าที่พูดหรือหลอกลวงเหยื่อ โดยในกระบวนการหลอกลวงนั้นมักมีการฝึกหลักการทางจิตวิทยาในการพูดโน้มน้าวและหลอกลวงเพื่อทำให้เหยื่อไม่หลบหนีหรือไม่เปิดเผยความลับรั่วไหล แม้จะไม่มีการจัดตั้งศูนย์โทรศัพท์ในประเทศที่จะทำการหลอกลวง อย่างไรก็ตาม กลุ่มคอลเซ็นเตอร์นี้มีการรับส่งกันเป็นทอดเพื่อความน่าเชื่อถือ โดยศูนย์โทรศัพท์จะติดตั้งอินเตอร์เน็ตความเร็วสูงเพื่อใช้ในระบบโทรศัพท์ผ่านทางอินเทอร์เน็ตหรือ VOIP (Voice Over Internet Protocol) การติดตามกลุ่มคอลเซ็นเตอร์นี้ค่อนข้างยาก แต่สัญญาณเสียงมักมีความชัดเจน โดยจะมีชาวไต้หวันหรือชาวจีนที่มีความชำนาญในการควบคุมระบบและการโทรศัพท์เป็นผู้ดูแล ในกระบวนการหาเหยื่อกลุ่มมิจฉาชีพนี้มักใช้โปรแกรมในการสุ่มหาเหยื่อเพื่อๆ ต่อเนื่อง ส่วนหมายเลขที่ปรากฏปลายทางจะใช้โปรแกรมในการตั้งหมายเลขให้ปรากฏเป็นหน่วยงานราชการตามที่อ้างถึงหรือเรียกว่า "Fake Number" เพื่อสร้างความน่าเชื่อถือว่าเป็นโทรศัพท์จากหน่วยงานนั้นๆ อย่างเช่น หน่วยงานตำรวจนานาชาติ (Interpol) เป็นต้น เพื่อให้เหยื่อมีความเชื่อถือในการสื่อสารกับกลุ่มคอลเซ็นเตอร์นี้

1.1.2 กลุ่มม้าถอนเงิน

ในกระบวนการหลอกลวงที่เกี่ยวข้องกับม้าถอนเงิน มักจะใช้บุคคลที่เป็นชาวไต้หวัน จีน มาเลเซีย หรือชาวไทยที่มีความสามารถในการพูดภาษาจีน ซึ่งเป็นผู้ที่ทำหน้าที่ใช้บัตรของเหยื่อในการถอนเงินสดจากตู้ถอนเงินสดอัตโนมัติ เมื่อได้รับคำสั่งจากผู้ควบคุมว่ามีเงินเข้าบัญชีธนาคารแล้ว ในกรณีที่เกิดการหลอกลวงกับคนไทย ม้าถอนเงินจะดำเนินการถอนเงินสดทั้งในประเทศไทยและต่างประเทศ เช่น ไต้หวันและสาธารณรัฐประชาชนจีน ซึ่งม้าถอนเงินนี้จะอยู่ในควบคุมของหัวหน้าชาวไต้หวัน ซึ่งจะต้องประสานงานระหว่างศูนย์โทรศัพท์ (Call center) เพื่อแจ้งให้ม้าถอนเงินไปทำการถอนเงินทันทีเพื่อป้องกันการอายัดบัญชีธนาคารจากผู้เสียหาย

1.1.3 กลุ่มจัดหาบัญชีธนาคารหรือบัตรอิเลคทรอนิกส์

กลุ่มจัดหาบัญชีธนาคารหรือบัตรอิเลคทรอนิกส์เป็นกลุ่มผู้ที่มีหน้าที่ในกระบวนการหลอกลวงเพื่อไปรวบรวมข้อมูลบัญชีและบัตรเอทีเอ็มของเหยื่อ และส่งให้กับกลุ่มม้าถอนเงิน และศูนย์โทรศัพท์ที่เป็นตัวควบคุมในกระบวนการหลอกลวงนี้ หน้าที่ของกลุ่มนี้คือให้เปิดบัญชีธนาคารประเภทสะสมทรัพย์ในชื่อเหมือนกับเจ้าของบัญชี และขอใช้บัตรเอทีเอ็มในชื่อเหมือนกัน เพื่อเก็บข้อมูลและรายละเอียดของบัญชีและบัตรเอทีเอ็มของเหยื่อ โดยในกรณีที่มีความ

จำเป็นต้องถอนเงินจำนวนมากก็อาจขอเพิ่มวงเงินในบัญชี เพื่อให้ม้าถอนเงินสามารถถอนเงินได้ตามที่กลุ่มต้องการ ในกระบวนการนี้ผู้รับจ้างในกลุ่มจัดหาบัญชีธนาคารหรือบัตรอิเลคทรอนิกส์อาจต้องถูกดำเนินคดีตามความผิดฐานในการร่วมกันฉ้อโกงประชาชนเช่นกัน เนื่องจากกิจกรรมนี้เป็นการหลอกลวงและฉ้อโกงผู้อื่นอย่างรุนแรง ซึ่งเป็นความผิดฐานทางอาญาที่มีโทษที่สูงมาก และส่งผลกระทบต่อความน่าเชื่อถือของประเทศและภาพลักษณ์ของประชาชนอย่างร้ายแรง (พันตำรวจตรีพัลลภ หริ่งรอด, 2562)

1.1.4 กลุ่มจัดการทางการเงิน

กลุ่มจัดการทางการเงินมีหน้าที่รวบรวมเงินสดจากม้าถอนเงินที่มีการถอนเงินสดจากตู้ถอนเงินสดอัตโนมัติที่ทำการหลอกลวงมาได้ และส่งเงินให้กับเจ้าของหรือระดับหัวหน้าต่อไปในกระบวนการหลอกลวงนี้ หน้าที่ของกลุ่มนี้คือการรับเงินที่ถูกหลอกลวงมาจากม้าถอนเงินและนำเงินที่ได้รับนี้ไปส่งให้กับผู้ควบคุมม้าถอนเงินหรือหัวหน้าของกลุ่มโดยตรง ดังนั้นผู้ที่เป็นส่วนหนึ่งของกลุ่มนี้จะมีบทบาทในกระบวนการในขั้นตอนของการส่งเงินแก่ผู้ควบคุมต่อไปในโครงการหลอกลวงนี้ ถ้าหากมีหลักฐานหรือสิ่งพยานที่เชื่อมโยงกลุ่มจัดการทางการเงินไปถึงผู้ควบคุมหรือระดับหัวหน้า กลุ่มนี้อาจถูกดำเนินคดีตามความผิดฐานร่วมกันฉ้อโกงประชาชนเนื่องจากกิจกรรมหลอกลวงและฉ้อโกงผู้อื่นเป็นความผิดฐานที่มีโทษที่สูงและส่งผลกระทบต่อความน่าเชื่อถือของประเทศและประชาชนอย่างรุนแรง

1.2 การหลอกลวงรูปแบบใหม่ของแก๊งคอลเซ็นเตอร์ตามแนวคิดของ Cyber Kill Chain แก๊งคอลเซ็นเตอร์ได้พัฒนารูปแบบในการหลอกลวงเหยื่อตามเทคโนโลยีที่เปลี่ยนไป เมื่อสมาร์ทโฟนมีราคาถูกลงทำให้เป็นที่นิยมใช้กันมากขึ้น อำนวยความสะดวกให้สามารถทำธุรกรรมอย่างการโอนเงินผ่านระบบโมบายแบงก์กิ้งได้อย่างรวดเร็วไม่ต้องไปทำรายการที่เครื่องเอทีเอ็มแก๊งคอลเซ็นเตอร์จึงได้พัฒนามาเป็นการโจมตีระบบโมบายแบงก์กิ้งของเหยื่อแทนซึ่งสอดคล้องกับแนวคิดของ Cyber Kill Chain ที่ถูกคิดค้นโดย Lockheed Martin เพื่อใช้อธิบายขั้นตอนการโจมตีไซเบอร์ ดังนี้

1.2.1 Reconnaissance การลาดตระเวน คือ คนร้ายจะเริ่มต้นเก็บรวบรวมข้อมูลของเป้าหมายก่อนเริ่มการโจมตี โดยอาจค้นหาข้อมูลจากโลกอินเทอร์เน็ต หรือเครือข่ายสังคมออนไลน์ โดยจะเห็นได้ว่า ในหลายกรณีคนร้ายสามารถระบุข้อมูลเบื้องต้นของตัวเหยื่อได้ถูกต้องจนเหยื่อหลงเชื่อ

1.2.2 Weaponization เตรียมอาวุธสำหรับโจมตี เช่น สร้างเว็บไซต์ปลอมที่มีหน้าตาเหมือนเว็บจริงที่จะใช้แอบอ้างหลอกเหยื่อ สร้างแอปพลิเคชันปลอมเพื่อนำไปติดตั้งในสมาร์ทโฟนของเหยื่อเพื่อใช้เป็นเครื่องมือในการโจมตีระบบโมบายแบงก์กิ้ง

1.2.3 Delivery ติดต่อเหยื่อเพื่อส่งเว็บไซต์และแอปพลิเคชันปลอม ผ่านทางช่องทางสื่อสารต่าง ๆ ให้

1.2.4 Exploitation ใช้กลวิธีทางวิศวกรรมสังคมในการโน้มน้าวเหยื่อให้หลงเชื่อเรื่องหลอกลวงของคนร้าย

1.2.5 Installation เมื่อเหยื่อหลงเชื่อก็จะติดตั้งแอปพลิเคชันปลอมลงในเครื่องและเรียกใช้งาน

1.2.6 Command & Control แอปพลิเคชันปลอมก็จะสร้างช่องทางในการรับส่งคำสั่งจากคนร้ายผ่านอินเทอร์เน็ต เพื่อให้สามารถจัดการและควบคุมเครื่องของเหยื่อจากระยะไกลได้ตามความต้องการ

1.2.7 Action on Objectives จากนั้นคนร้ายจะควบคุมระบบโมบายแบงก์กิ้งของเหยื่อเพื่อโอนเงินออกไปยังบัญชีม้าต่อไป

เนื่องจาก Cyber Kill Chain เป็นขั้นตอนที่ดำเนินการอย่างต่อเนื่องเป็นลูกโซ่ นั่นหมายความว่า ถ้าสามารถทำให้ลูกโซ่ขาดไปได้ก่อนจะถึงขั้นสุดท้ายก็จะทำให้การโจมตีไม่เป็นผลสำเร็จทันที ซึ่งส่วนใหญ่แล้ว ควรจะใช้หลากหลายวิธีเข้าช่วยเพื่อพยายามตัดห่วงโซ่ทิ้งให้ได้ทุกจุด (สรวิศ บุญมี, 2566)

เมื่อคนร้ายควบคุมระบบโมบายแบงก์กิ้งของเหยื่อได้แล้วก็ทำการโอนเงินของเหยื่อไปยังบัญชีธนาคารที่เปิดเตรียมไว้ล่วงหน้าหรือที่เรียกว่าบัญชีม้า คือ บัญชีเงินฝากธนาคารของบุคคลอื่นซึ่งถูกคนร้ายนำมาใช้เป็นช่องทางในการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำความผิด เพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวได้ บัญชีม้าสามารถทำได้หลายวิธี ทั้งจากการโจรกรรมข้อมูลส่วนบุคคลเพื่อนำไปใช้เปิดบัญชีในชื่อของคนนั้น ๆ หรือจ้างให้บุคคลอื่นเปิดบัญชีหรือรับซื้อบัญชีเงินฝากธนาคารของบุคคลทั่วไปเพื่อนำไปใช้กระทำความผิด ซึ่งพบได้อย่างแพร่หลายในเครือข่ายสังคมออนไลน์ที่มีการขายบัญชีเงินฝากธนาคารอย่างเปิดเผย โดยบัญชีม้าเหล่านี้จะมาพร้อมกับสำเนาบัตรประจำตัวประชาชนและซิมการ์ดโทรศัพท์ที่เจ้าของบัญชีเปิดใช้งานด้วย เพื่อให้คนร้ายที่ซื้อบัญชีม้าไปแล้วจะสามารถนำข้อมูลส่วนบุคคลของเจ้าของบัญชีไปผูกกับ mobile banking เพื่อใช้โอนส่งต่อเงินที่ได้จากเหยื่อให้เร็วที่สุด

คนร้ายมักจะมีบัญชีม้าหลาย ๆ บัญชี เพื่อใช้โอนส่งเงินต่อกันไปเป็นทอด ๆ เพื่อป้องกันการถูกตำรวจตรวจสอบหรืออายัดเงินในบัญชีม้า เช่น เมื่อผู้เสียหายถูกหลอกให้โอนเงินเข้าบัญชีม้าที่ 1 แล้ว คนร้ายก็จะโอนเงินออกจากบัญชีดังกล่าวต่อไปยังบัญชีม้าที่ 2 จากบัญชีม้าที่ 2 โอนต่อไปยังบัญชีม้าที่ 3 และที่ 4 ซึ่งบางรายมีจำนวนบัญชีม้าถึง 5 บัญชี ท้ายที่สุดคนร้ายก็จะถอนเงินของเหยื่อหรือผู้เสียหายออกไป ซึ่งการโอนเงินจากบัญชีม้าหลายทอด เช่นนี้ตั้งแต่ต้นจนจบใช้เวลาเพียง

ไม่กี่นาทีเท่านั้น และหากถูกเจ้าหน้าที่ตำรวจอายัดบัญชีม้าบัญชีใดก็จะเปลี่ยนไปใช้บัญชีม้าอื่น ๆ ที่ยังสามารถใช้งานแทนได้ ขณะที่ในทางการสืบสวนของเจ้าหน้าที่ จะมีขั้นตอนในการขอข้อมูลบัญชีเงินฝากจากสถาบันการเงินซึ่งมีระยะเวลาในการดำเนินการทำให้ที่ผ่านมายังไม่สามารถระงับยับยั้งการถอนเงินออกจากบัญชีเงินฝากธนาคารได้อย่างทันท่วงที เงินที่คนร้ายได้จากการกระทำความผิดจึงถูกโยกย้ายออกจากบัญชีม้าไปอย่างรวดเร็ว และต้องใช้เวลาในการติดตามเงินคืนให้กับผู้เสียหาย (Bank of Thailand, 2022)

**2. แนวคิดเกี่ยวกับการรวมกลุ่มในการกระทำผิด**

พฤติกรรมการกระทำผิดของแก๊งคอลเซ็นเตอร์เกี่ยวข้องกับแนวคิดเกี่ยวกับการรวมกลุ่มในการกระทำผิด เช่น แนวคิดเกี่ยวกับแก๊งอาชญากรรม ตามที่ Department of Public Security ประเทศสหรัฐอเมริกาได้ให้คำนิยามของ “แก๊ง” หมายถึง การรวมกลุ่มของบุคคลในการกระทำผิด ซึ่งหากเป็นกลุ่มแก๊งของเด็กและเยาวชน อาจเป็นการเกิดขึ้นอย่างเป็นธรรมชาติของวัยรุ่นในพื้นที่เมือง โดยมีการพัฒนากลุ่มแก๊งขึ้นมาเพื่อตอบสนองความต้องการของกลุ่มแก๊งเพื่อเป็นการแสดงออกซึ่งสิทธิที่ครอบครัว ชุมชนหรือรัฐบาลไม่สามารถตอบสนองความต้องการของเยาวชนดังกล่าวได้ เนื่องจากความยากจนที่เพิ่มขึ้น การถูกกีดกันและการขาดโอกาสในการดำรงชีวิตจึงได้มีการรวมกลุ่มเป็นแก๊งเพื่อปกป้องสิทธิของกลุ่มและเพื่อตอบสนองความต้องการ โดยการรวมกลุ่มที่ปราศจากผู้ควบคุม โดยมีการพัฒนากฎของแก๊งเพื่อปกป้องความปลอดภัยให้แก๊งสมาชิกของกลุ่มแก๊งได้โดยการกำหนดพื้นที่อาณาเขตและสร้างสัญลักษณ์เพื่อสร้างความหมายให้แก๊งสมาชิกของกลุ่มแก๊งรู้จักกันและสามารถระบุตัวตนในกลุ่มแก๊งได้ แก๊งคอลเซ็นเตอร์มีพฤติกรรมที่เกี่ยวข้องกับการละเมิดสิทธิของบุคคลอื่นในสังคม โดยมีการใช้ความรุนแรงหรือกระทำอาชญากรรม สำหรับแก๊งคอลเซ็นเตอร์ที่ปรากฏในปัจจุบันนั้นไม่เพียงแค่มีแก๊งที่เป็นเพศชายเท่านั้น ยังมีแก๊งที่เป็นเพศหญิงที่แสดงความแตกต่างและความไม่เท่าเทียมกันในเรื่องเพศด้วยกัน Department of Public Security ได้จำแนกแก๊งเป็น 4 ประเภทคือ 1. แก๊งที่มีอายุสั้น (Scavenger Gangs) มีลักษณะที่สำคัญคือมีขนาดเล็กถึงขนาดกลาง มีลักษณะความเป็นแก๊งไม่มากนัก สมาชิกส่วนใหญ่เป็นเพศชาย มีสมาชิกที่หลากหลายส่วนใหญ่เป็นวัยรุ่นที่มีอายุระหว่าง 13-18 ปี มีพฤติกรรมการกระทำผิดในโรงเรียนและบริเวณใกล้เคียงโรงเรียนที่เกี่ยวข้องกับอาชญากรรมพื้นฐาน การกระทำผิดที่ไม่ใช้ความรุนแรงมากนัก แสดงออกถึงการต่อต้านสังคม 2. แก๊งที่ละเมิดกฎ (Transgressor Gangs) เป็นแก๊งที่ตั้งขึ้นโดยมีวัตถุประสงค์ที่ไม่ใช้ความรุนแรง มีขนาดเล็ก โดยมีสมาชิกในกลุ่มประมาณ 40-80 คน เป็นเด็กและเยาวชนที่มีอายุระหว่าง 10-18 คน มีเพศชายมากกว่าเพศหญิง (สัดส่วน 5:1) มีการใช้ความรุนแรงกับแก๊งฝ่ายตรงข้ามหรือการใช้ความรุนแรงในพื้นที่อาณาเขตของตนเอง รวมทั้งเกี่ยวข้องกับพฤติกรรมอาชญากรรมนอกพื้นที่ ถูกก่อตั้งขึ้นเนื่องจากความยากจนของเด็กและ

เยาวชนที่ต้องการปกป้องรักษาสิทธิของตนเอง ก่อตั้งโดยไม่มีผู้บังคับบัญชา จัดตั้งกฎขึ้นมาเพื่อรักษาความสงบเรียบร้อยของกลุ่ม นอกจากนี้ยังมีการสร้างสัญลักษณ์เพื่อแสดงอัตลักษณ์ของกลุ่ม แก๊ง การที่แก๊งคอลเซ็นเตอร์มีการละเมิดสิทธิของบุคคลอื่นในสังคมและมีการใช้ความรุนแรงหรือกระทำอาชญากรรม นั้นแสดงถึงปัญหาทางสังคมที่ควรให้ความสำคัญในการก้าวหน้าและการแก้ไขปัญหาเหล่านี้เพื่อสร้างสังคมที่มีความเป็นอยู่ร่วมกันและความเท่าเทียมกันในทุกเรื่องตลอดจนเสริมสร้างสิ่งแวดล้อมที่ปลอดภัยและเชื่อมโยงกันอย่างยั่งยืนในโลกไซเบอร์

นอกจากนี้มีการรวมกลุ่มเพื่อต่อสู้กับฝ่ายตรงข้าม และกลุ่มที่ใช้ความรุนแรง (Violent Gangs) ซึ่งเป็นกลุ่มที่มีขนาดใหญ่โดยมีสมาชิกประมาณ 100-500 คน ส่วนใหญ่เป็นเพศชาย โดยมีสัดส่วนของเพศชายต่อเพศหญิงอยู่ที่ 9:1 กลุ่มนี้ก่อตั้งขึ้นเพื่อดำเนินการอาชญากรรมที่ใช้ความรุนแรงมากที่สุด และอาจเกิดเหตุการณ์ที่เกี่ยวข้องกับการฆาตกรรมหรือการกระทำอาชญากรรมที่มีความรุนแรงที่สูง การที่กลุ่มนี้มีเป้าหมายที่ไม่มีความหมายหรือการดำเนินกิจกรรมผิดกฎหมายเพื่อสร้างกำไร ยังประกอบด้วยกลุ่มผู้หญิงซึ่งเป็นกลุ่มที่ตั้งขึ้นโดยเพศหญิง โดยมีวัตถุประสงค์ที่ไม่ใช้ความรุนแรง และมีขนาดเล็กถึงขนาดกลาง มีสมาชิกประมาณ 15-40 คน และเป็นกลุ่มที่มีผู้หญิงเป็นสมาชิกเท่านั้น บางกลุ่มอาจมีความสัมพันธ์กับกลุ่มเพศชาย และมีกลุ่มเพศหญิงจำนวนไม่มากนักที่พบว่าเป็นหัวหน้ากลุ่ม หากแต่มีสมาชิกเป็นทั้งเพศหญิงและเพศชาย สมาชิกของกลุ่มส่วนใหญ่ก่อตั้งขึ้นเนื่องจากเสียใจที่ต้องเลียนแบบความมีอำนาจของกลุ่มเพศชาย และต้องการแสวงหาโอกาสในการหนีจากการถูกทำร้ายร่างกายและการถูกล่วงละเมิดทางเพศในครอบครัวและเพื่อสร้างอำนาจและการยอมรับ วัตถุประสงค์ที่สำคัญเพื่อสร้างชีวิตที่มีความหมายโดยปราศจากโอกาสในชีวิต โดยเป็นกลุ่มที่ก่อตั้งขึ้นในสหรัฐอเมริกาเนื่องจากความมีอคติทางเพศแม้ว่าจะมีการรับสมาชิกใหม่ หากแต่มีแนวโน้มที่จะหมดสิ้นไป เนื่องจากกลุ่มเพศหญิงจะมีการละทิ้งรูปแบบในการดำเนินชีวิตในรูปแบบกลุ่มมากกว่าเพศชาย อาจมีบางส่วนที่มีการรวมกลุ่มกับแก๊งที่มีผู้ชายเป็นผู้นำ (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

การแบ่งประเภทของแก๊งที่จำแนกโดย Department of Public Security เป็นแก๊งอาชญากรรม (Criminal Gangs) มีความสอดคล้องกับแก๊งคอลเซ็นเตอร์ ในแง่ของการตั้งขึ้นเพื่อประกอบอาชญากรรม มีขนาดกลางถึงขนาดใหญ่โดยมีสมาชิกประมาณ 50-200 คน ส่วนใหญ่เป็นเพศชาย และมีสมาชิกเพศหญิงจำนวนไม่มากนัก แก๊งประเภทนี้มักมีการกระทำผิดที่อาณาเขตที่ชัดเจน และบางครั้งอาจมีการประกอบอาชญากรรมนอกพื้นที่ตามคำสั่ง ในการดำเนินการของแก๊งอาชญากรรมจะประกอบด้วยการฝึกหัดในระดับที่สูงขึ้น มีกฎระเบียบ มีการวางแผน มีการจัดองค์กรและมีการดูแลในการประกอบอาชญากรรม นอกจากนี้ยังมีหน่วยที่เชี่ยวชาญในอาชญากรรมแต่ละประเภทแก๊งคอลเซ็นเตอร์เป็นกลุ่มที่เกิดขึ้นเมื่อมีการรวมกลุ่มในการประกอบอาชญากรรมที่

มีความสำคัญ และมีการประกอบอาชญากรรมที่มีความสลับซับซ้อนมากขึ้น ซึ่งอาจมีความสอดคล้องกับแก๊งอาชญากรรมที่มีลักษณะเด่นเหมือนกัน การที่แก๊งคอลเซ็นเตอร์เป็นสำคัญเกิดจากความมีอคติทางเพศ และอาจมีการรวมกลุ่มกับแก๊งที่มีผู้ชายเป็นผู้นำ ในหลายประเทศ แก๊งอาชญากรรมประเภทนี้จะเป็นที่รู้จักจากตำรวจและองค์กรอาชญากรรม เนื่องจากมีความสำคัญและมีการประกอบอาชญากรรมที่มีความสลับซับซ้อนมากขึ้น โดยสมาชิกของแก๊งอาชญากรรมในบางครั้งจะสิ้นสุดด้วยการถูกจำคุกในเรือนจำหรือการเสียชีวิตจากการใช้ความรุนแรง อาจกล่าวได้ว่าแก๊งอาชญากรรมพัฒนาเป็นองค์กรอาชญากรรมเมื่อมีการรวมกลุ่มในการประกอบอาชญากรรมที่มีความสำคัญ และมีการประกอบอาชญากรรมที่มีความสลับซับซ้อนมากขึ้น ซึ่งมีความสอดคล้องกับการกระทำของแก๊งคอลเซ็นเตอร์ที่สำคัญ (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

Bossard (1998) กล่าวว่า แก๊งอาชญากรรม (Criminal Gangs) ส่วนใหญ่มักเป็นแก๊งที่กระทำผิดเป็นครั้งคราว (Occasional Gangs) โดยเป็นการรวมกลุ่มกับเพื่อนหรือกลุ่มอดีตนักโทษ (ที่อาจเป็นผู้ที่เคยถูกเก็งข้องกับการกระทำอาชญากรรม) อาจเกิดขึ้นในสถานที่เช่นเรือนจำซึ่งเป็นสถานที่ในการฝึกหัดพฤติกรรมอาชญากรร โดยเป้าหมายของกลุ่มคือเพื่อกระทำการผิดหรือกระทำผิดอย่างต่อเนื่อง อาจมีสมาชิกที่มีความเชี่ยวชาญพิเศษหรืออาจไม่มี การรวมกลุ่มอาจเกิดขึ้นในระหว่างประเทศ กรณีที่กระทำผิดเกิดขึ้นภายใต้คำสั่งของหัวหน้าแก๊งเพียงคนเดียว กลุ่มนี้มักจะสลายตัวเมื่อหัวหน้าแก๊งถูกจับกุม ถูกดำเนินคดีหรือเสียชีวิต สมาชิกในกลุ่มอาจรวมกลุ่มกับแก๊งอื่นเพื่อกระทำผิดต่อไป ขึ้นอยู่กับทักษะและความเชี่ยวชาญของแต่ละกลุ่ม อายุของกลุ่มนี้มักไม่เป็นเวลานาน แต่การพัฒนาของกลุ่มนี้ยังคงมีความสำคัญต่อการเกิดขึ้นในสังคมนอกกฎหมาย (Bossard, 1998)

การหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์เป็นกิจกรรมที่มีผลกระทบต่อสังคมอย่างรุนแรง โดยกลุ่มมิจฉาชีพนี้มีวัตถุประสงค์ในการหลอกลวงและขโมยเงินจากบุคคลที่ไม่รู้ตัว ซึ่งผู้เสียหายที่ถูกหลอกลวงอาจเป็นประชาชนทั่วไปหรือนักลงทุนที่ไม่รู้เรื่องเกี่ยวกับกลุ่มมิจฉาชีพนี้ ผลกระทบที่เกิดขึ้นจากการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์เป็นอย่างร้ายแรง ไม่เพียงแต่ส่งผลกระทบต่อเศรษฐกิจและการเงินของบุคคลที่เสียหาย แต่ยังส่งผลกระทบต่อภาพลักษณ์และความน่าเชื่อถือของประเทศด้วย การโจมตีและหลอกลวงผ่านทางอินเทอร์เน็ตทำให้ผู้คนสังเกตถึงความเสี่ยงที่อาจเกิดขึ้นเมื่อมีการทำธุรกิจออนไลน์ และอาจทำให้ผู้คนไม่ไว้วางใจในการทำธุรกิจออนไลน์หรือดำเนินกิจกรรมทางอินเทอร์เน็ตอื่น ๆ อีกด้วย นอกจากนี้ ผู้ที่เกิดความเสียหายจากการหลอกลวงทางไซเบอร์อาจต้องเผชิญกับความเสียหายทางจิตใจและอารมณ์ การหลอกลวงทางไซเบอร์อาจสร้างความไม่สงบและความไม่มั่นคงในสังคม ซึ่งอาจทำให้ผู้คนมีความไม่ไว้วางใจในความเชื่อถือและสัญญาในสังคม โดยเฉพาะในระบบการทำธุรกิจและการทำธุรกิจ

ออนไลน์ ทั้งนี้ การหลอกลวงทางไซเบอร์เป็นปัญหาที่ต้องต่อสู้กันอย่างต่อเนื่องเพื่อความปลอดภัยและความเชื่อถือในสังคมที่สูงขึ้น ซึ่งความเสียหายที่เห็นได้อย่างชัดเจนเลย คือ ความเสียหายทางด้านทรัพย์สิน กล่าวคือ การหลอกลวงทางอินเทอร์เน็ตมีวัตถุประสงค์เพื่อผลประโยชน์ในลักษณะของทรัพย์สินหรือประโยชน์อื่น ๆ โดยที่การหลอกลวงประเภทนี้มักพบบ่อยและแพร่หลายมากที่สุด บางครั้งมิจฉาชีพเป็นบุคคลที่ไม่สามารถพบตัวหรือตรวจสอบได้ ส่งผลให้ผู้ใช้บริการที่ถูกหลอกลวงเป็นเหตุเนื่องจากความโลภและรู้เท่าไม่ถึงสถานการณ์ ขาดสติปัญญาพิจารณา เช่น กรณีการหลอกหลวงแบบแชร์ลูกโซ่ การสะสมเงิน การออมทรัพย์จากกลุ่มองค์กรหรือบริษัทที่ไม่มีอยู่จริง ซึ่งเหตุการณ์เช่นนี้อาจเป็นข่าวที่ปรากฏตามสื่อออนไลน์จำนวนมาก (พระมหาธรรมทส ขนฺติพโล (พืชจันทร์), 2560)

ดังนั้นผลกระทบของแก๊งคอลเซ็นเตอร์ที่เป็นภัยคุกคามต่อประเทศต่าง ๆ ทั่วโลก โดยมีผลกระทบทั้งต่อเศรษฐกิจระดับจุลภาค คือ เหยื่อผู้ได้รับผลกระทบจากการหลอกลวงและผลกระทบต่อเศรษฐกิจในภาพรวมของประเทศสูญเงินเป็นจำนวนมูลค่ามหาศาล ผลกระทบทางสังคม เมื่อเหยื่อที่ได้รับผลกระทบจากแก๊งคอลเซ็นเตอร์มักจะประสบกับความเครียด โดยเหยื่อบางรายคิดสั้นฆ่าตัวตาย สูญเงิน มีภาวะหนี้สิน จนนำไปสู่ปัญหาสุขภาพจิตตามมา นอกจากนั้นยังส่งผลกระทบต่อภาพลักษณ์ของประเทศอีกด้วย (อาริยา สุขโต, 2565)

สรุปได้ว่า แนวคิดการรวมกลุ่มในการกระทำผิดของแก๊งคอลเซ็นเตอร์เป็นการทำงานร่วมกันเป็นกลุ่ม เพื่อช่วยเพิ่มประสิทธิภาพในการหลอกลวงและก่ออาชญากรรมไซเบอร์ กลุ่มเหล่านี้มักมีการแบ่งบทบาทหน้าที่ชัดเจน เช่น บางคนทำหน้าที่โทรหลอกลวง บางคนทำหน้าที่ปลอมแปลงข้อมูลหรือจัดการด้านการเงิน นอกจากนี้ การทำงานเป็นทีมยังช่วยให้แก๊งเหล่านี้สามารถพัฒนาและปรับปรุงเทคนิคการหลอกลวงเพื่อหลีกเลี่ยงการตรวจจับจากเจ้าหน้าที่การรวมกลุ่มนี้ยังเอื้อให้สมาชิกสามารถแลกเปลี่ยนข้อมูล เทคนิค หรือแนวทางการหลอกลวงใหม่ ๆ ได้อย่างรวดเร็ว ทำให้การหลอกลวงมีความแนบเนียนและมีโอกาสสำเร็จมากขึ้น นอกจากนี้ การรวมกลุ่มยังช่วยกระจายความเสี่ยงในการถูกจับกุม เนื่องจากแต่ละคนจะมีหน้าที่เฉพาะเจาะจง ลดโอกาสที่แต่ละบุคคลจะถูกติดตามและระบุตัวตนได้ง่าย โดยรวมแล้วการรวมกลุ่มของแก๊งคอลเซ็นเตอร์เป็นการรวมพลังที่ทำให้สามารถดำเนินการหลอกลวงได้อย่างเป็นระบบและซับซ้อนกว่าการกระทำผิดแบบบุคคล

## ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์

ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์นั้นได้อาศัยรูปแบบของการหลอกลวงของแก๊งคอลเซ็นเตอร์ที่มักจะอาศัยปัจจัยเหล่านี้กระทำต่อผู้เสียหายหรือเหยื่อ คือ

1. การใช้ความโลภของเหยื่อ

การใช้ความโลภของเหยื่อเป็นกลไกในการหลอกลวง โดยใช้ความต้องการของเหยื่อเป็นสิ่งจูงใจในการกระทำผิด โดยแก๊งคอลเซ็นเตอร์จะหลอกลวงผู้เสียหายว่าจะได้รับเงินหรือทรัพย์สิน หากมีการดำเนินการตามที่แก๊งคอลเซ็นเตอร์ได้เสนอ อาทิ ได้รับคืนภาษีมูลค่าเพิ่ม (VAT), การถูกรางวัล, การได้รับเช็คคืนภาษี และอื่น ๆ โดยแก๊งคอลเซ็นเตอร์อ้างว่าต้องจ่ายค่าบริการเบื้องต้นเป็นค่าบริการและค่าธรรมเนียมต่าง ๆ ก่อนจึงจะได้รับเงิน เมื่อผู้เสียหายหลงเชื่อเพราะความโลภอยากได้เงินหรือทรัพย์สินจะโอนเงินเข้าบัญชีธนาคารของคนร้ายที่ได้เตรียมเปิดรองรับไว้

2. การใช้ความกลัวของเหยื่อ

แก๊งคอลเซ็นเตอร์มีการหลอกลวงโดยการใช้ความกลัวของเหยื่อในการหลอกลวงเพื่อทำให้เหยื่อรู้สึกกลัวและมีการโอนเงินให้แก่แก๊งคอลเซ็นเตอร์ โดยจะหลอกลวงผู้เสียหายว่าเป็นห นี้ค่าโทรศัพท์ เป็นหนี้บัตรเครดิตธนาคาร มีบัญชีธนาคารพัวพันกับการค้ายาเสพติด บัญชีธนาคารจะต้องถูกอายัดและถูกตรวจสอบโดยสำนักงาน ปปง. เมื่อผู้เสียหายหลงเชื่อจะทำธุรกรรมทางการเงินตามที่กลุ่มคนร้ายบอก เช่น นำบัตรอิเลคทรอนิกส์ (เอทีเอ็ม) ไปทำรายการที่ตู้ถอนเงินอัตโนมัติ (ตู้เอทีเอ็ม) ถอนเงินสดจากบัญชีธนาคารของตนเองนำไปฝากเข้าบัญชีธนาคารที่หน้าเคาน์เตอร์หรือฝากผ่านตู้รับฝากเงินอัตโนมัติ (CDM) เข้าบัญชีธนาคารที่กลุ่มคนร้ายเปิดรองรับไว้ ซึ่งในปัจจุบันลักษณะการหลอกลวงจะใช้ลักษณะทำให้ผู้เสียหายเกิดความกลัวเป็นส่วนใหญ่ (พัลลภ หริ่งรอด, 2562)

3. การใช้ความไม่รู้หรือขาดการระวังในการปกป้องทรัพย์สินของเหยื่อ

แก๊งคอลเซ็นเตอร์มีวิธีการหลอกลวงโดยใช้ความไม่รู้หรือการขาดความระมัดระวังในการปกป้องทรัพย์สินของเหยื่อ ตัวอย่างเช่นการปลอมหมายเลขโทรศัพท์ของธนาคารและแอบแฝงเป็นเจ้าหน้าที่ธนาคารเพื่อขอรหัสผ่านเพื่ออัปเดตแอปพลิเคชัน ซึ่งผู้เสียหายอาจถูกล่อให้แจ้งรหัส 6 หลักที่ส่งผ่าน SMS ให้กับพนักงานเพื่อตรวจสอบความถูกต้องและอัปเดตข้อมูลธนาคาร แต่จริง ๆ แล้วรหัสนั้นอาจถูกยกเลิกไปแล้ว ทำให้เงินในบัญชีถูกโอนออกอย่างรวดเร็ว

นอกจากนี้ แก๊งคอลเซ็นเตอร์ยังมีวิธีการทำให้เหยื่อตายใจ โดยพูดจานำเสนอขายประกันหรือโปรโมชั่นต่าง ๆ เพื่อให้เชื่อว่าเป็นเจ้าหน้าที่ของธนาคารจริง หลังจากนั้นจะหลอกให้แจ้งรหัสที่เกี่ยวข้องเพื่อทำการโอนเงินออกจากบัญชีของผู้เสียหายอย่างรวดเร็ว ในกรณีนี้ เหยื่ออาจไม่รู้ว่ากำลังโดนหลอกและขาดความระมัดระวังในการปกป้องทรัพย์สิน ทำให้แก๊งคอลเซ็นเตอร์สามารถหลอกลวงเงินจากเหยื่อได้

4. การใช้ความเชื่อหรือความศรัทธาในการหลอกลวงเหยื่อ

แก๊งคอลเซ็นเตอร์ได้ใช้ความเชื่อหรือความศรัทธาในการหลอกลวงเหยื่อ อาทิ จะเปิดเว็บไซต์หรือเปิดโปรแกรมเฟสบุ๊คและโฆษณาเพื่อชักชวนเหยื่อให้ร่วมทำบุญ จัดสร้างพระ สร้างวัด จัดงานทำบุญต่าง ๆ ทำพิธีเสริมดวงชะตา หลอกลวงคนที่ชอบเสี่ยงโชคด้วยการส่งเลขเด็ดให้ ถ้าหากถูกรางวัลจากล๊อตเตอรี่หรือหวยขอส่วนแบ่งร้อยละ 30 เป็นต้น เนื่องจากความเชื่อหรือความศรัทธา เป็นจิตวิทยาขั้นพื้นฐานที่มนุษย์มีเพื่อทำให้จิตใจรู้สึกปลอดภัยมีความสุข ซึ่งแก๊งคอลเซ็นเตอร์ได้อาศัยหลักจิตวิทยาโดยการใช้ความเชื่อและศรัทธาเป็นสิ่งสำคัญในการหลอกลวงเหยื่อจนกระทั่งประสบความสำเร็จ (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

ผู้วิจัยสามารถสรุปปัจจัยสำคัญที่ทำให้ประชาชนตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ได้ว่า เกิดจากการใช้จิตวิทยาที่มุ่งควบคุมอารมณ์ ความคิด และพฤติกรรมของเหยื่อโดยตรง ผู้หลอกลวงมักจะพยายามใช้ช่องโหว่ทางจิตใจของเหยื่อผ่านปัจจัยหลักต่าง ๆ ได้แก่ การกระตุ้นความโลภ ความกลัว ความไม่รู้ และการอาศัยความเชื่อหรือศรัทธา ซึ่งทำให้เหยื่อมีแนวโน้มที่จะหลงเชื่อและทำตามคำสั่งโดยขาดการไตร่ตรอง โดยหนึ่งในปัจจัยที่ถูกใช้มากที่สุดคือ การกระตุ้นความโลภ ซึ่งเกิดขึ้นผ่านการสร้างข้อเสนอที่น่าดึงดูด เช่น การอ้างถึงรางวัลมูลค่าสูงหรือผลประโยชน์ทางการเงิน ทำให้เหยื่อหลงคิดว่าตนกำลังจะได้รับสิ่งที่มีค่า โดยลืมระมัดระวังและตกลงเปิดเผยข้อมูลสำคัญหรือทำธุรกรรมที่เป็นอันตราย นอกจากนี้แก๊งคอลเซ็นเตอร์ยังใช้ การกระตุ้นความกลัว เพื่อข่มขู่หรือสร้างความวิตกกังวลให้แก่เหยื่อ เช่น อ้างว่ามีความเสี่ยงทางกฎหมาย หรือเหยื่ออาจถูกดำเนินคดีหากไม่ปฏิบัติตามสิ่งที่ถูกสั่ง เหยื่อที่เกิดความกลัวมักจะยอมทำตามคำสั่งเพื่อหลีกเลี่ยงปัญหา ทำให้ตกเป็นเหยื่อของการหลอกลวงได้ง่าย ส่วนในด้านของการขาดความรู้หรือความระมัดระวังถือเป็นอีกปัจจัยหนึ่งที่ทำให้ประชาชนมีโอกาสตกเป็นเหยื่อได้ เนื่องจากขาดความเข้าใจเกี่ยวกับกลโกงทางไซเบอร์และการรักษาความปลอดภัยข้อมูลส่วนตัว เมื่อผู้หลอกลวงใช้วิธีที่น่าเชื่อถือและเข้าถึงได้ง่าย ผู้คนอาจมองข้ามความเสี่ยงและตกลงให้ข้อมูลส่วนตัวโดยไม่รู้ตัว และสุดท้าย การหลอกลวงด้วยการใช้ความเชื่อหรือความศรัทธา อาศัยการสร้างภาพลักษณ์ของหน่วยงานที่น่าเชื่อถือ เช่น หน่วยงานราชการหรือสถาบันที่ประชาชนให้ความเคารพ ทำให้เหยื่อคล้อยตามได้ง่าย แก๊งคอลเซ็นเตอร์อาจใช้การอ้างตัวเป็นผู้แทนขององค์กรสำคัญเพื่อสร้างความน่าเชื่อถือและผลักดันให้เหยื่อให้ความร่วมมือ

**กรณีศึกษาที่เกี่ยวกับแก๊งคอลเซ็นเตอร์**

กรณีตัวอย่างของผลกระทบที่เกิดจากการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์

กรณีที่ 1 เป็นเกี่ยวกับผู้เสียหายที่เป็นข้าราชการบำนาญเพศหญิงอายุ 76 ปีที่ได้โอนเงินจำนวน 500,000 บาทเข้าบัญชีของเครือข่ายคอลเซ็นเตอร์ ลูกสาวของผู้เสียหายได้เปิดเผยว่า วันนั้นแม่อยู่บ้านคนเดียว ได้รับโทรศัพท์จากบุคคลที่อ้างตัวเป็นพนักงานไปรษณีย์จังหวัดขอนแก่นก่อนที่จะส่งต่อให้คุยกับบุคคลที่อ้างตัวเป็นตำรวจระดับสารวัตร กลุ่มนี้บอกว่าขอตรวจสอบเกี่ยวกับการกระทำความผิด และขอข้อมูลส่วนตัว และขอให้รวบรวมเงินไปเปิดบัญชีธนาคารในชื่อของตัวเอง แต่สุดท้ายเงินก็ถูกโอนออกไปจนเกือบหมดเหลือติดบัญชีอยู่เพียง 900 บาท ซึ่งลูกสาวของผู้เสียหายได้กล่าวว่า มันเป็นขั้นตอนง่ายมากที่จะหลอกคนอื่น ๆ กำหนดรหัสโดยใช้เลข 6 ตัวหลังของบัตรประชาชนของแม่ ซึ่งเขารู้อยู่แล้วว่าเลข 6 ตัวหลังของบัตรประชาชนของแม่คืออะไร จับเสียงได้ว่าเป็นคนแก่อยู่คนเดียว ความรู้ไม่เท่าทันของคนแก่ที่แก๊งพวกนี้ได้หลอกลวง เขาให้แม่เอากระเป๋าไว้ข้างตัวตลอดเวลา เอาโทรศัพท์ไว้ในกระเป๋าไม่ต้องเอาออกมา ไม่ต้องให้ใครรู้ว่ามีการติดต่อกับตำรวจ เพราะตอนนี้ตำรวจดำเนินการอยู่ คนแก่ต้องโอนเงินบั้นปลายชีวิต 500,000 บาทไปให้ มันไม่สงสารคนแก่ นี่คือสิ่งที่บอกว่าหลอกคนแก่เท่านั้นแหละมันเลวมากเลยนะ

ในกรณีนี้คนร้ายได้ใช้วิธีการหลอกลวงที่ง่าย ๆ แต่มีความชั่วร้าย โดยการนำเสนอตนเองให้เป็นเจ้าหน้าที่ที่สำคัญเพื่อขอข้อมูลส่วนตัวและเก็บเงินในบัญชีที่เข้าใจผู้เสียหายว่าเป็นของตนเอง การตั้งคำถามเกี่ยวกับรหัสใบประชาชนแสดงถึงความรู้จักและความเชื่อถือของคนแก๊งนอกจากนี้ยังให้ผู้เสียหายเก็บเงินอยู่ในกระเป๋าเพื่อไม่ให้คนรอบข้างรู้ว่ามีการติดต่อกับตำรวจ การหลอกลวงนี้ทำให้ผู้เสียหายเสียเงินทันทีและไม่สามารถร้องเรียนหรือแจ้งความเพื่อทำการสืบสวนได้ในทันที ความก้าวหน้าที่ชอบทำให้ผู้เสียหายหลงเชื่อและทำตามคำขอของคนแก๊งเสียเงินโดยไม่รู้ตัวว่าถูกหลอกลวง หลังจากเกิดความเสี่ยงและเสียเงินแล้ว ผู้เสียหายเพียงเพื่อนบ้านที่เล่าให้เห็นถึงว่าเป็นการหลอกลวงของเครือข่ายคอลเซ็นเตอร์ ซึ่งทำให้คนแก๊งถูกจับกุมได้ในที่สุด ความเชื่อถือและความรู้สึกปลอดภัยที่ผู้เสียหายมีอาจได้รับความเสี่ยงและเสียเงิน ด้วยเหตุนี้ ควรเสริมสร้างความระมัดระวังในการจัดการเงินและทำธุรกรรมทางการเงินที่เกี่ยวข้องเพื่อป้องกันการหลอกลวงเช่นนี้ให้เกิดขึ้นในอนาคต (สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง, 2563)

กรณีที่ 2 แก๊งคอลเซ็นเตอร์โทรหลอกผู้เสียหาย อายุ 40 ปี ชาวจังหวัดชลบุรี โดยอ้างเป็นเจ้าหน้าที่กรมการค้าภายใน หลอกให้ติดตั้งแอปพลิเคชันในโทรศัพท์มือถือ พร้อมกดลิงก์ยืนยันตัวตน สุดท้ายถูกดูดเงินเกลี้ยงทุกบัญชี เสียกว่า 16 ล้านบาท ซึ่งจากการสอบถามผู้เสียหาย เปิดเผยว่า เมื่อวานวันที่ 24 กุมภาพันธ์ 2566 ได้มีโทรศัพท์โทรเข้ามาอ้างว่าเป็นเจ้าหน้าที่จากกรมการค้าภายใน ได้โทร. มาบอกกับตนว่า ตอนนี้มีนโยบายให้ผู้ประกอบการติดตั้งแอปพลิเคชันเพื่อทำการอัปเดตข้อมูลของตัวเอง ตอนนั้นตนก็กำลังยุ่งๆ จากนั้นก็มีไลน์เด้งมาให้เรากดลิงก์ ตนก็ทำตามขั้นตอน พอเข้าได้ประมาณ 10 นาทีได้มีข้อความเด้งเข้ามาว่า เงินถูกกดออกจากบัญชีและเด้งมา

เตือนอย่างต่อเนื่องจนบัญชีกลางที่ตนดูแล ซึ่งเป็นบัญชีที่ทำธุรกิจร่วมกับพี่สาวถูกดูดเงินออกจนหมด จำนวน 9 ครั้ง หมดไปกว่า 16 ล้านบาท และมีบัญชีส่วนตัวอีก 2 บัญชี กว่า 1.5 แสนบาท ผู้เสียหายเผยว่า ตอนที่เงินกำลังถูกดูดออก ตนก็สังเกตว่าโทรศัพท์มีหน้าค้างที่แอปพลิเคชันที่ทางมิจฉาชีพให้กด ตนจึงรีบรีเซตโทรศัพท์แต่ไม่ทันแล้วและได้มีการเข้ามาแจ้งตำรวจไว้แล้ว (ไทยรัฐ, 2566)

## งานวิจัยที่เกี่ยวข้อง

พัลลภ หริ่งรอด (2562) ได้ทำการศึกษา เรื่อง มาตรการตามกฎหมายในการปราบปรามองค์กรอาชญากรรมข้ามชาติ ศึกษาเฉพาะกลุ่มคอลเซ็นเตอร์ จากการศึกษาพบว่า ปัญหาทางกฎหมายเกี่ยวกับการดำเนินคดีอาญาในความผิดที่กระทำโดยแก๊งคอลเซ็นเตอร์ ซึ่งเป็นลักษณะความผิดฐานฉ้อโกงตามมาตรา 341 แห่งประมวลกฎหมายอาญาและความไม่ชัดเจนเกี่ยวกับความหมายขององค์กรอาชญากรรมข้ามชาติ ตามมาตรา 3 แห่งพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 รวมถึงมาตรการดำเนินคดีกับอาชญากรที่มีลักษณะการกระทำดังกล่าว เนื่องจากความไม่ชัดเจนของบทบัญญัติกฎหมายและปัญหาทางกฎหมายเรื่องอัตราโทษ ทำให้เกิดปัญหาและอุปสรรคต่อการบังคับใช้กฎหมายของเจ้าหน้าที่รัฐได้

พิรุพห์รัตน์ ศรีแจ่ม (2562) ได้ทำการศึกษา เรื่อง กลโกงการทำธุรกรรมทางการเงินในยุคดิจิทัล โดยมีวัตถุประสงค์เพื่อศึกษากลโกงการทำธุรกรรมทางการเงินในยุคดิจิทัล กลุ่มตัวอย่างคือประชาชนในจังหวัดสระบุรี จำนวน 745 คน ผลการศึกษาพบว่า จากผู้ตอบแบบสอบถามที่ร่วมมือในการตอบ มีความเสียหายโดยรวมต่อการสำรวจครั้งนี้โดยเฉลี่ยคือ 14,666.98 บาท ทั้งนี้พบว่าการหลอกลวงเกี่ยวกับการทำอาชีพเสริมออนไลน์มีค่าเฉลี่ยในแง่มูลค่ามากที่สุด คือ 1,154.10 บาท รองลงมาคือการสั่งซื้อสินค้าทั้งแบบออนไลน์ หรือ แบบอื่น ๆ ที่ผู้สั่งซื้อไม่ได้รับของตรงตามที่โฆษณาไว้ หรือ มีการอวดอ้างสรรพคุณเกินจริง ค่าเฉลี่ย 895.16 ลำดับที่ 3 คือการหลอกลวงเกี่ยวกับการถูกรางวัลออนไลน์ ซึ่งมีค่าเฉลี่ย 814.26 จากการทดสอบสมมติฐาน พบว่าตัวแปรอิสระลักษณะการใช้งานด้านระยะเวลาเฉลี่ย เครื่องมือสื่อสังคมออนไลน์ที่ใช้ และ ประเภทรับรู้ข้อมูลข่าวสาร มีอิทธิพลต่อกลโกงการทำธุรกรรมทางการเงิน โดยมีค่า R Squared .324 อย่างมีนัยสำคัญทางสถิติ .05

กรกนก นิลดำ, เสริมศิริ นิลดำ, อิงดอย ศรีลำพัฒน์, ภควัฒน์ สวนงาม, วรักษณ์กมล มงคลอัศศิริ และปฐมพร ปัญญะติ (2563) ได้ทำการศึกษา เรื่อง วิธีการกลโกง ช่องทางการสื่อสาร และประสบการณ์ในการถูกมิจฉาชีพออนไลน์หลอกลวงของผู้สูงอายุในจังหวัดเชียงราย โดยมีวัตถุประสงค์เพื่อ 1) ศึกษาวิธีการกลโกงและช่องทางการสื่อสารที่มิจฉาชีพออนไลน์ใช้หลอกลวง

ผู้สูงอายุในจังหวัดเชียงราย และ 2) ศึกษาประสบการณ์ของผู้สูงอายุที่เคยถูกมิจฉาชีพออนไลน์หลอกลวงในจังหวัดเชียงราย ประชากรที่ใช้ในการศึกษา คือ กลุ่มที่มีอายุเกิน 50 ปี ขึ้นไป ในเขตอำเภอเมือง และอำเภอใกล้เคียง จังหวัดเชียงราย กลุ่มตัวอย่างจำนวน 400 คน ผลการศึกษาพบว่าผู้สูงอายุมีประสบการณ์ถูกมิจฉาชีพออนไลน์หลอกหลวงข้อมูลโดยใช้วิธีการกลโกงแบบการฉ้อโกงโดยหลอกลวงให้ร่วมลงทุนในลักษณะลูกโซ่ คิดเป็นร้อยละ 30.5 รองลงมาคือ ฉ้อโกงโดยหลอกลวง ทำให้รายการที่ตู้เอทีเอ็มเพื่อให้โอนเงินไปให้ คิดเป็นร้อยละ 27.25 ส่วนช่องทางการสื่อสารที่ผู้สูงอายุถูกหลอกลวงมากที่สุดคือช่องทางเฟซบุ๊ก คิดเป็นร้อยละ 44 รองลงมาคือ ไลน์ คิดเป็นร้อยละ 31.25 และน้อยที่สุดคือ อินสตาแกรม คิดเป็นร้อยละ 5.25 และเมื่อผู้สูงอายุรู้ว่าตนเองถูกหลอกลวงส่วนใหญ่ใช้การโพสต์หรือประกาศลงสื่อออนไลน์เพื่อเปิดเผยตัวมิจฉาชีพ คิดเป็นร้อยละ 46.75 รองลงมาคือแจ้งความกับพนักงานตำรวจ คิดเป็นร้อยละ 25.75 และน้อยที่สุดคือการตามเอาเงินคืนคิดเป็นร้อยละ 6.5

ขวัญชนก ศรีภมร (2565) ได้ทำการศึกษา เรื่อง แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม มีวัตถุประสงค์ของการวิจัยเพื่อ 1) ศึกษาปัจจัยและผลกระทบที่เกิดขึ้นจากแก๊งคอลเซ็นเตอร์ 2) ศึกษารูปแบบการหลอกลวงของแก๊งคอลเซ็นเตอร์ที่กระทบต่อความน่าเชื่อถือของหน่วยงานภาครัฐและเอกชนในประเทศไทย 3) เพื่อเปรียบเทียบแนวทางการป้องกันและมาตรการทางกฎหมายที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ของประเทศไทยและต่างประเทศ และ 4) ให้หน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องกับเรื่องแก๊งคอลเซ็นเตอร์เข้ามามีส่วน ร่วมในการร่วมมือกันหาแนวทางป้องกันแก๊งคอลเซ็นเตอร์อย่างมีประสิทธิภาพ ผลการศึกษาพบว่า ในประเทศไทยได้มีการบังคับใช้กฎหมายที่ใช้ในการปราบปรามโดยการกำหนดความผิดทางอาญาซึ่งยังไม่รวมถึงมาตรการการป้องกันอาชญากรรมโดยความร่วมมือของเอกชนประกอบกับบริบทต่าง ๆ ที่ทำให้การบังคับกฎหมายดังกล่าวยังไม่มีประสิทธิภาพเท่าที่ควรจึงทำให้ไม่สามารถจับกุมและกวาดล้างได้อย่างสมบูรณ์เนื่องจากมิจฉาชีพเหล่านี้มักมีที่อยู่ไม่เป็นหลักแหล่งและรูปแบบการหลอกลวงมีวิธีที่ซับซ้อนมากขึ้นทำให้ยากต่อการสืบสาวต้นตอประกอบกับบทกฎหมายที่ใช้ในการปราบปรามซึ่งผู้วิจัยมองว่าเป็นการแก้ปัญหาทางปลายเหตุ เนื่องจากบทกฎหมายที่เกี่ยวข้องมักเป็นบทกฎหมายทางอาญา การที่จะสามารถลงโทษผู้กระทำความผิดดังกล่าวได้จะต้องเกิดเหตุการณ์ขึ้นแล้วเท่านั้นดังนั้นการที่จะนำตัวผู้กระทำความผิดมาลงโทษแทบจะไม่ได้มีผลอะไรที่ทำให้แก๊งคอลเซ็นเตอร์ลดน้อยลง ดังนั้นประเทศไทยจึงควรหันมาให้ความสำคัญกับการป้องกันและกำกับดูแลก่อนที่จะเกิดเหตุเสียมากกว่า เพราะการหาแนวทางในการป้องกันตั้งแต่ต้นจะสามารถช่วยลดความเสียหายได้ไม่มากก็น้อยและเป็นการ

สร้างความตื่นตัวให้กับประชาชน (Public Awareness Raising) ในการระมัดระวังแก๊งคอลเซ็นเตอร์ในปัจจุบัน

ธัญพิชชา สามารถ (2565) ได้ทำการศึกษาเรื่อง การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ โดยมีวัตถุประสงค์เพื่อ 1) ศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ 2) ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และ 3) เพื่อเสนอแนะแนวทางการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ใช้วิธีการสัมภาษณ์เชิงลึกกับกลุ่มตัวอย่างผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวงทางไซเบอร์จำนวน 24 คน ผู้มีส่วนในการหลอกลวงจำนวน 5 คน และเจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกันผู้สูงอายุจากการถูกหลอกลวงทางไซเบอร์จำนวน 9 คน ผลการวิจัยแบ่งกลุ่มผู้สูงอายุที่ถูกหลอกลวงทางไซเบอร์ 4 กลุ่ม แต่ละกลุ่มมีรูปแบบและปัจจัยที่ทำให้ตกเป็นเหยื่อของการหลอกลวงแตกต่างกัน คือ 1) ผู้ที่ตกเป็นเหยื่อการ หลอกลวงให้ลงทุนมีรูปแบบการถูกหลอกลวงโดยส่วนใหญ่ถูกชักชวนจากบุคคลที่รู้จักในกลุ่มไลน์ที่เคยลงทุนด้วยกัน หรือพบเห็น โฆษณาเชิญชวนบนสื่อสังคมออนไลน์โดยมีลักษณะของผลตอบแทนที่สูงเป็นสิ่งจูงใจ มีทั้งการให้ค่าตอบแทนจากการแนะนำสมาชิก ใหม่ และไม่มีการให้ค่าตอบแทน ซึ่งผู้ที่มีส่วนในการหลอกลวงเป็นทั้งบุคคลธรรมดา และอยู่ในรูปแบบบริษัทจดทะเบียน ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่ามี 8 ปัจจัย คือ ด้านเศรษฐกิจ ด้านความโลภ ด้านเทคโนโลยีด้านการสร้างความน่าเชื่อถือของผู้ หลอกลวง ด้านความรู้ความเข้าใจในการลงทุน ด้านสภาพความเป็นอยู่ด้านการชักชวนให้ลงทุนจากญาติหรือคนรู้จัก และด้านความ เชื่อมั่นใจตนเอง 2) ผู้ที่ตกเป็นเหยื่อการหลอกลวงจากแก๊งคอลเซ็นเตอร์มีรูปแบบการหลอกลวงในการสร้างความตกใจกลัว หรือเกิด ความโลภ และมีระยะเวลาในการให้ตัดสินใจจำกัด ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่า มี4 ปัจจัย คือ ด้านความกลัว ด้านความ โลภ ด้านความไม่คุ้นเคยกับเทคโนโลยี และด้านการอยู่เพียงลำพังขณะเกิดเหตุ3)ผู้ที่ตกเป็นเหยื่อการซื้อสินค้าออนไลน์ผู้หลอกลวงจะสร้างโพรไฟล์ให้ดูมีความน่าเชื่อถือ เปิดร้านขายบนสื่อสังคมออนไลน์และขายผ่านตลาดกลางออนไลน์เพื่อสร้างความน่าเชื่อถือ สินค้าที่หลอกลวงมักจะเป็นสินค้าที่ราคาไม่สูงนัก หรือเป็นสินค้าที่มีราคาถูกกว่าท้องตลาดทั่วไป ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อ พบว่ามี 3 ปัจจัยคือ ความไว้วางใจร้านค้าออนไลน์โดยไม่ได้ตรวจสอบ การส่งเสริมการขายที่ผิดปกติและราคาสินค้าที่มีราคาไม่สูง 4) ผู้สูงอายุที่ตกเป็นเหยื่อการหลอกให้รักทางออนไลน์ มีรูปแบบการใช้จิตวิทยาในการหลอกลวง สร้างความสัมพันธ์ที่ดีและใช้ ระยะเวลาในการสร้างความไว้วางใจ เลือกเหยื่อจากการดูโพรไฟล์บนสื่อสังคมออนไลน์ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่ามี 4 ปัจจัย คือ ความรักความหลง ความน่าเชื่อถือ ด้านความเหงา และความอายของผู้ที่ถูกหลอก โดยการหลอกลวงทั้ง 4 รูปแบบมี ปัจจัยร่วมกันคือ ความรู้ไม่เท่าทันการหลอกลวง สำหรับแนวทางการแก้ไขการตกเป็นเหยื่อ

ได้แก่ การสร้างความตระหนักให้กับ ผู้สูงอายุในการรู้เท่าทันถึงรูปแบบการหลอกลวงทางไซเบอร์ การระมัดระวังการเปิดเผยข้อมูลส่วนตัวผู้อื่นที่ไม่รู้จัก การให้คำปรึกษา ในกลุ่มของครอบครัว การจัดตั้งเครือข่ายกลุ่มผู้สูงอายุเพื่อเผยแพร่ข่าวสารการหลอกลวงทางไซเบอร์ความร่วมมือของภาคเอกชนผู้ ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ในการปิดกันช่องทางการหลอกลวงจากผู้หลอกลวง ตลอดจนหน่วยงานของรัฐในการออก มาตรการทางกฎหมายตลอดจนการบังคับใช้อย่างเคร่งครัด

สรวิศ บุญมี (2566) ได้ทำการศึกษาเรื่อง ภัยแก๊งคอลเซ็นเตอร์จากอาชญากรรมทางเศรษฐกิจสู่อาชญากรรมเทคโนโลยี โดยมีอธิบายถึงความเป็นมาของแก๊งคอลเซ็นเตอร์วิธีทางวิศวกรรมสังคมในการหลอกลวงเหยื่อ การหลอกลวงรูปแบบใหม่ของแก๊งคอลเซ็นเตอร์ตามแนวคิดของ Cyber Kil Chain ปัญหาของบัญชีม้ามาตรการป้องกันโดย กสทช. ร่างพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี การทำงานของแอปพลิเคชันปลอมและการป้องกันและรับมือ เพื่อให้เข้าใจกลวิธีหลอกลวงรูปแบบใหม่ และสร้างความตระหนักรู้เพื่อลดความเสี่ยงที่จะตกเป็นเหยื่อโดนหลอกลวงจนต้องสูญเสียทรัพย์สิน

# บทที่ 3
# ระเบียบวิธีวิจัย

## วิธีดำเนินการวิจัย

การวิจัยเรื่อง การหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) มีวัตถุประสงค์เพื่อศึกษาถึงการกระทำอันเป็น ลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์ เพื่อศึกษาถึงปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ และเพื่อเสนอแนะการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ มีวิธีการดำเนินการวิจัยทั้งที่เป็นการวิจัยเชิงเอกสาร และการวิจัยเชิงคุณภาพ เพื่อให้ได้มาซึ่งความรู้ที่เกี่ยวข้องกับลักษณะการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ ปัจจัยที่ทำให้ประชาชนตกเป็นเหยื่อ และแนวทางในการป้องกันการตกเป็นเหยื่อ การสัมภาษณ์เพื่อเจาะลึกถึงมูลเหตุ ความรู้สึก และการตัดสินใจในการนำไปสู่การถูกหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ มีวิธีดำเนินการวิจัยคือ

## ผู้ให้ข้อมูลที่สำคัญ

ในการศึกษานี้มุ่งศึกษาจากประชาชนที่เคยตกเป็นเหยื่ออายุ 20 - 60 ปีขึ้นไป และเจ้าหน้าที่ที่เกี่ยวข้องในการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์

**1. ผู้ให้ข้อมูลหลัก**

โทมัส แมคมิลแลน (Thomas T. Macmillan) กล่าวไว้ว่า หากใช้ผู้ให้ข้อมูลหลักจำนวนมากกว่า 17 คนขึ้นไป ทำให้อัตราความคลาดเคลื่อนลดน้อยลง (ขวัญชัย สิทธิรัตน์ และธีระวัฒน์ จันทึก, 2559) ในการวิจัยเชิงคุณภาพ ผู้วิจัยจึงกำหนดผู้ให้ข้อมูลหลักจำนวน 18 คน โดยแบ่งผู้ให้ข้อมูลหลักเป็น 2 กลุ่ม คือ

กลุ่มที่ 1 กลุ่มประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ เพศชายและหญิง กลุ่มวัยทำงาน อายุระหว่าง 20 - 60 ปี เนื่องจากเป็นบุคคลที่มีการใช้โซเชียลมีเดียในการดำเนินชีวิต และการทำธุรกรรมต่าง ๆ และเคยแจ้งความดำเนินคดีภายในระยะเวลา 5 ปี (พ.ศ. 2562 - 2566) โดยวิธีการเลือกแบบเจาะจง (Purposive Sampling) ซึ่งเป็นการใช้วิธีการสัมภาษณ์เชิงลึกทีละคนกับประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ได้ผู้ให้สัมภาษณ์จำนวน 12 คน เพื่อหาสาเหตุเชิงลึกในการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ โดยติดต่อส่งหนังสือขอความอนุเคราะห์หน่วยงานกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ให้ช่วยส่งต่อเอกสารเชิญชวนเข้าร่วมการวิจัยและเอกสารข้อมูลสำหรับกลุ่มตัวอย่างให้กับบุคคลที่มีคุณสมบัติตามเกณฑ์ที่ผู้วิจัย

กำหนด และให้บุคคลดังกล่าวติดต่อกลับมาหาผู้วิจัยหากยินดีให้ข้อมูลตามหมายเลขโทรศัพท์ของผู้วิจัยที่ได้แจ้งไว้ในเอกสารชี้แจง ซึ่งวิธีการดังกล่าวนั้นผู้วิจัยจะไม่สามารถทราบถึงข้อมูลของกลุ่มผู้ให้ข้อมูลที่เป็นผู้เสียหายก่อนได้ ดังนั้นจึงจำเป็นต้องเป็นการตัดสินใจยินยอมให้ข้อมูลและเข้าร่วมโครงการวิจัยโดยอิสระด้วยจากตัวผู้ให้ข้อมูลเอง ซึ่งเป็นการใช้วิธีการสัมภาษณ์เชิงลึกทีละคนกับประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ จำนวน 12 คน

กลุ่มที่ 2 กลุ่มเจ้าหน้าที่ที่ให้การช่วยเหลือหรือป้องกันประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ โดยผู้ให้ข้อมูลหลักเป็นเจ้าหน้าที่รัฐระดับหัวหน้าของหน่วยงานที่ทำหน้าที่เกี่ยวกับอาชญากรรมทางเทคโนโลยี จำนวน 6 คน โดยใช้วิธีการสัมภาษณ์เชิงลึกทีละคน เพื่อหาแนวทางการป้องกันการตกเป็นเหยื่ออาชญากรรมการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ โดยติดต่อส่งหนังสือขอความอนุเคราะห์ขอสัมภาษณ์ไปยังผู้ให้ข้อมูลหลัก (Key Informant) ซึ่งผู้ให้ข้อมูลหลักเป็นเจ้าหน้าที่รัฐระดับหัวหน้าที่ทำหน้าที่เกี่ยวกับอาชญากรรมทางเทคโนโลยี ในงานวิจัยนี้ใช้คำว่า ตำรวจไซเบอร์ และปฏิบัติหน้าที่หรือมีประสบการณ์การให้ความช่วยเหลือประชาชนที่ถูกการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ เป็นระยะเวลาตั้งแต่ 4 ปีขึ้นไป

**เกณฑ์ในการคัดเข้า-คัดออก**

กลุ่มที่ 1 กลุ่มประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ เพศชายและหญิง กลุ่มวัยทำงาน อายุระหว่าง 20 - 60 ปี เนื่องจากเป็นบุคคลที่มีการใช้โซเชียลมีเดียในการดำเนินชีวิต และการทำธุรกรรมต่าง ๆ และเคยแจ้งความดำเนินคดีภายในระยะเวลา 5 ปี (พ.ศ. 2562 - 2566)

และกลุ่มที่ 2 กลุ่มเจ้าหน้าที่ที่ให้การช่วยเหลือหรือป้องกันประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ เป็นเจ้าหน้าที่รัฐระดับหัวหน้าของหน่วยงานที่ทำหน้าที่เกี่ยวกับอาชญากรรมทางเทคโนโลยี และปฏิบัติหน้าที่หรือมีประสบการณ์การให้ความช่วยเหลือประชาชนที่ถูกการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ เป็นระยะเวลาตั้งแต่ 4 ปีขึ้นไป

หากภายหลังผู้วิจัยพบว่า ผู้ให้ข้อมูลที่ถูกคัดเลือกเข้าโครงการวิจัยแล้ว แต่อาจเกิดอันตรายหรือมีโอกาสเสี่ยงกับผลแทรกซ้อนจากการวิจัยได้มากกว่าคนปกติหรือผู้ให้ข้อมูลรายอื่น เช่น เกิดภาวะผิดปกติทางร่างกายหรือจิตใจในคำถามสัมภาษณ์ทำให้ไม่สามารถเข้าร่วมการวิจัยต่อได้ ผู้วิจัยจึงจำเป็นต้องดำเนินการถอนผู้เข้าร่วมการวิจัยหรือยุติการเข้าร่วมการวิจัย

ทั้งนี้สถานที่ วันเวลาที่กำหนด หรือระบบการสัมภาษณ์ ผู้วิจัยมีแนวทางการเลือกสถานที่ที่เหมาะสม โดยเป็นสถานที่ที่เงียบสงบไม่โจ่งแจ้งหรือเป็นที่พลุกพล่าน ทั้งการสัมภาษณ์แบบออนไลน์และออฟไลน์ ซึ่งเป็นไปตามความสะดวกของผู้มีส่วนร่วมในการวิจัย ซึ่งการสัมภาษณ์

แบบออนไลน์นั้นผู้เข้าร่วมการวิจัยไม่จำเป็นต้องเปิดกล้องขณะดำเนินการสัมภาษณ์ และหากผู้เข้าร่วมการวิจัยไม่มีความประสงค์ที่จะให้ผู้วิจัยบันทึกเสียงขณะสัมภาษณ์สามารถแจ้งได้ตลอดเวลา โดยผู้วิจัยได้กำหนดตามความเหมาะสมและเอื้อต่อผู้มีส่วนร่วมในการวิจัย ซึ่งจำนวนครั้งที่เข้าสัมภาษณ์ได้ปรับให้ยืดหยุ่นตามความสมบูรณ์ของข้อมูลและประเด็นที่สำคัญ โดยผู้ให้สัมภาษณ์ให้สัมภาษณ์ด้วยความสมัครใจและสามารถปฏิเสธการตอบการสัมภาษณ์ได้ตลอดเวลา ทั้งนี้ผู้วิจัยตระหนักถึงการไม่รุกล้ำความเป็นส่วนตัว ก่อนการสัมภาษณ์จึงได้มีการติดต่อนัดหมายล่วงหน้า และส่งเอกสารชี้แจงเพื่อให้ผู้มีส่วนร่วมในการวิจัย ได้มีโอกาสพิจารณาก่อนตัดสินใจในการเข้าร่วมในการให้ข้อมูลสำหรับงานวิจัยในครั้งนี้และผู้มีสิทธิ์ในการเข้าถึงข้อมูลจะมีเฉพาะผู้ที่เกี่ยวข้องกับงานวิจัยเท่านั้น

## เครื่องมือที่ใช้ในการศึกษา

**1. แบบสัมภาษณ์**

การศึกษาวิจัยในครั้งนี้ ผู้วิจัยใช้แบบสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structured Interview) เป็นเครื่องมือในการสัมภาษณ์แบบเจาะลึก (In-depth Interview) กับผู้ให้ข้อมูลสำคัญประกอบด้วยประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ และเจ้าหน้าที่ที่เกี่ยวข้องในการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์โดยแบบสัมภาษณ์มี 2 ชุดคือ

**ชุดที่ 1 แบบสัมภาษณ์เชิงลึกประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงผ่านออนไลน์ กรณีแก๊งคอลเซ็นเตอร์** มีข้อคำถาม 2 ส่วน ได้แก่

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

ส่วนที่ 2 การถูกหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์

**ชุดที่ 2 แบบสัมภาษณ์เชิงลึกเจ้าหน้าที่ที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกันประชาชนจากการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์** มีข้อคำถาม 2 ส่วน ได้แก่

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

ส่วนที่ 2 การให้ความช่วยเหลือผู้ที่ตกเป็นเหยื่อจากการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์

**2. เครื่องบันทึกเสียง**

ผู้วิจัยอาจใช้เครื่องบันทึกเสียงประกอบการสัมภาษณ์ โดยจะมีการแจ้งและขออนุญาตผู้ให้ข้อมูลสำคัญก่อนทำการบันทึกเสียง

**3. แบบบันทึกข้อมูล (Record Form)**

ในการเก็บข้อมูลมีการใช้แบบบันทึกข้อมูล (Record Form) ประกอบการสัมภาษณ์ตามประเด็นที่ต้องการศึกษา

## วิธีการรวบรวมข้อมูล

การวิจัยครั้งนี้การวิจัยครั้งนี้ ผู้วิจัยมีวิธีการเก็บรวบรวมข้อมูล ดังนี้

1. การเก็บรวบรวมข้อมูลจากการศึกษาค้นคว้าข้อมูลจากเอกสารทางวิชาการโดยดำเนินการรวบรวมข้อมูลจากการค้นคว้าเอกสาร หนังสือ งานวิจัย ข้อมูลทางสถิติ มาตรการทางกฎหมาย แนวคิด ทฤษฎี และสิ่งพิมพ์หรือสื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ เพื่อนำมาใช้เป็นแนวทางในการสร้างแบบสัมภาษณ์เชิงลึก รวมทั้งนำมาใช้เป็นส่วนประกอบในกระบวนการวิเคราะห์และประมวลผลข้อมูลในการวิจัย

2. ผู้วิจัยส่งหนังสือขอความอนุเคราะห์ขอสัมภาษณ์ที่ออกโดยคณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา ถึงประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ จำนวน 12 คน และเจ้าหน้าที่ที่เกี่ยวข้องในการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ จำนวน 6 คน รวมทั้งสิ้น 18 คน ตามที่ได้คัดเลือกไว้แบบเจาะจง (Purposive Sampling) เพื่อเชิญเป็นผู้ให้ข้อมูลสำคัญ

3. ผู้วิจัยส่งหนังสือแจ้งผู้ให้ข้อมูลสำคัญ พร้อมทั้งแนบเอกสารแนะนำตัวประกอบหนังสือขอความอนุเคราะห์ขอสัมภาษณ์ และแบบสัมภาษณ์ เพื่อมอบให้กับผู้ให้ข้อมูลสำคัญได้ศึกษาล่วงหน้าก่อนให้สัมภาษณ์ โดยวิธีการดังกล่าวเป็นไปตามการตัดสินใจยินยอมให้ข้อมูลและเข้าร่วมโครงการวิจัยโดยความสมัครใจของผู้ให้ข้อมูลสำคัญ

4. ผู้วิจัยเข้าพบผู้ให้ข้อมูลสำคัญ ตามกำหนดวันเวลาที่ได้ติดต่อประสานไว้ เพื่อทำการสัมภาษณ์ เรื่อง การหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ โดยมีการจดบันทึกข้อมูลและบันทึกเสียงระหว่างการสัมภาษณ์ หากผู้ให้ข้อมูลสำคัญไม่ยินยอมให้ใช้เครื่องบันทึกเสียงระหว่างการสัมภาษณ์ทางผู้วิจัยจะไม่ใช้เครื่องบันทึกเสียงในการสัมภาษณ์ครั้งนั้น และจะใช้วิธีการจดบันทึกข้อมูลเพียงอย่างเดียว และการสัมภาษณ์แบบออนไลน์นั้นผู้เข้าร่วมการวิจัยไม่จำเป็นต้องเปิดกล้องขณะดำเนินการสัมภาษณ์ และหากผู้เข้าร่วมการวิจัยไม่มีความประสงค์ที่จะให้ผู้วิจัยบันทึกเสียงขณะสัมภาษณ์สามารถแจ้งได้ตลอดเวลาเช่นเดียวกับการสัมภาษณ์แบบออฟไลน์

5. การรวบรวมข้อมูลที่ได้จากการสัมภาษณ์ ผู้วิจัยเริ่มจากการถอดถ้อยคำจากการสัมภาษณ์ของผู้ให้ข้อมูลสำคัญ จากนั้นผู้วิจัยได้อ่านเอกสารที่ได้จากการถอดถอดถ้อยคำจากการสัมภาษณ์รวมกับอ่านข้อมูลที่ได้จากการจดบันทึก เพื่อหาข้อมูลที่เป็นประโยชน์ต่องานวิจัยและรวบรวมข้อมูลที่เป็นประโยชน์ของแต่ละคนไว้ เพื่อนำไปวิเคราะห์ข้อมูลและสรุปผลการวิจัยต่อไป

6. การวิเคราะห์ข้อมูลและสรุปผลการวิจัยที่ได้จากการสัมภาษณ์ ผู้วิจัยใช้วิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) เพื่อตอบวัตถุประสงค์ในการวิจัย และได้มีการตรวจสอบข้อมูลแบบสามเส้าด้านข้อมูล (Data Triangulate) ซึ่งเป็นการพิจารณาความถูกต้องของข้อมูลที่ได้จากแหล่งต่าง ๆ ผ่านการพิจารณาด้านเวลา สถานที่ และบุคคลที่มีความแตกต่างกัน

ทั้งนี้ข้อมูลต่าง ๆ ที่ได้จากการวิจัยจะถูกเก็บไว้เป็นความลับ ไม่มีการเปิดเผยชื่อ การนำเสนอข้อมูลจะเป็นในภาพรวมและใช้นามแฝงเท่านั้น และผู้มีสิทธิ์ในการเข้าถึงข้อมูลจะมีเฉพาะผู้ที่เกี่ยวข้องกับงานวิจัย ซึ่งข้อมูลจะถูกเก็บไว้ในเครื่องคอมพิวเตอร์ที่มีรหัสผ่านของผู้วิจัยเท่านั้น ส่วนเอกสารจะเก็บไว้ในตู้เอกสารที่ใส่กุญแจไว้เป็นเวลา 1 ปี หลังการเผยแพร่ผลการวิจัยและจะถูกนำไปทำลายหลังจากนั้นด้วยวิธีการย่อยเป็นเศษกระดาษหรือโดยวิธีการเผา

**การตรวจสอบคุณภาพของเครื่องมือ**

การทดสอบคุณภาพของเครื่องมือ มีขั้นตอนดังนี้

1. ผู้วิจัยได้นำแบบสัมภาษณ์เกี่ยวกับการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์เสนออาจารย์ที่ปรึกษางานนิพนธ์ เพื่อตรวจสอบความตรงเชิงเนื้อหา และความถูกต้องของภาษา

2. นำแบบสัมภาษณ์เกี่ยวกับการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์เสนอผู้เชี่ยวชาญจำนวน 3 ท่าน ได้แก่

1) รองศาสตราจารย์ ดร.พงษ์เสฐียร เหลืองอลงกต
สังกัด คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา

2) รองศาสตราจารย์ ว่าที่เรือตรี ดร.เอกวิทย์ มณีธร
สังกัด คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา

3) ดร.พิชิต รัชตพิบุลภพ
สังกัด คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา

เพื่อตรวจสอบความตรงเชิงเนื้อหา การประเมินค่าความตรงตามเนื้อหา (Content validity) ใช้การวิเคราะห์ข้อมูลเชิงคุณภาพ โดยใช้ค่าดัชนีความสอดคล้องระหว่างข้อคำถามจากการประเมินจากผู้เชี่ยวชาญจำนวน 3 ท่าน ได้ช่วยประเมินว่าข้อคำถามแต่ละข้อในแบบสอบถามมีความสอดคล้องกับเนื้อหาหรือไม่ โดยให้คะแนนตามเกณฑ์แล้วนำผลมาพิจารณาคะแนนของผู้เชี่ยวชาญในแต่ละข้อมาวิเคราะห์หาค่าดัชนีความสอดคล้อง (Item-Objective Congruence: IOC) ดังนี้

+1 หมายถึง ข้อความมีความเหมาะสมสอดคล้อง

0 หมายถึง ไม่แน่ใจว่าข้อความมีความเหมาะสมสอดคล้อง

-1 หมายถึง ข้อความไม่สอดคล้อง

หลังจากนั้นนำแบบประเมินให้ผู้ทรงคุณวุฒิประเมินความสอดคล้องของข้อคำถาม และนำมาหาค่าความสอดคล้องโดยใช้สูตร

$$IOC = \frac{\sum R}{n}$$

$\sum R$ หมายถึง ผลรวมของคะแนนจากผู้เชี่ยวชาญ

n หมายถึง จำนวนผู้เชี่ยวชาญ

3. ผลจากการประเมินจากผู้เชี่ยวชาญ

การพิจารณาความคิดเห็นของผู้เชี่ยวชาญจากการวิเคราะห์ดัชนีความสอดคล้องของเครื่องมือการวิจัย (IOC) ในทุกข้อคำถามนั้น หากข้อคำถามที่มีค่า IOC ตั้งแต่ 0.50 – 1.00 จะคัดเลือกไว้ ส่วนข้อคำถามที่มีค่า IOC ต่ำกว่า 0.50 จะพิจารณาการปรับปรุงหรือไม่คัดเลือกไว้

4. รายงานผลการประเมินจากผู้เชี่ยวชาญ

สรุปผลการประเมินจากผู้เชี่ยวชาญ พบว่า ผลรวมของคะแนนการพิจารณาจากผู้เชี่ยวชาญทั้ง 3 ท่านในแต่ละข้อคำถามเท่ากับ 3 คะแนน ผลการวิเคราะห์ดัชนีความสอดคล้องของเครื่องมือการวิจัย (IOC) จึงมีค่าเท่ากับ 1.00 แสดงว่าข้อคำถามมีความสอดคล้องกับวัตถุประสงค์การวิจัย

**การวิเคราะห์ข้อมูล**

การวิเคราะห์ข้อมูลของการศึกษาวิจัย ใช้วิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) เพื่อตอบวัตถุประสงค์ในการวิจัย การวิเคราะห์ข้อมูลผู้วิจัยใช้วิธีการถอดถ้อยคำจากการสัมภาษณ์อย่างละเอียดเพื่อให้การตีความและการกำหนดประเด็นที่สำคัญได้อย่างถูกต้อง น่าเชื่อถือได้ แล้วทำการวิเคราะห์ข้อมูลเชิงคุณภาพโดยใช้เทคนิคการวิเคราะห์เนื้อหา (Content Analysis) ในการวิเคราะห์ข้อมูลได้มีการตรวจสอบข้อมูลแบบสามเส้า (Triangulation) ซึ่งเป็นการพิจารณาความถูกต้องของข้อมูลที่ได้จากแหล่งต่าง ๆ ผ่านการพิจารณาเวลา สถานที่ และบุคคลที่มีความแตกต่างกัน พบว่า ระยะเวลาที่เหยื่อถูกหลอกลวงในแต่ละช่วงปีนั้นแก๊งคอลเซ็นเตอร์มีกลวิธีที่หลอกลวงแตกต่างกัน สถานที่เกิดเหตุในกรณีของแก๊งคอลเซ็นเตอร์สามารถหมายถึงช่องทางการสื่อสาร เช่น โทรศัพท์ หรืออินเทอร์เน็ต พบว่า เหยื่อส่วนใหญ่ถูกหลอกในลักษณะที่เหมือนกัน และบุคคลที่ตกเป็นเหยื่อแต่ละรายถูกหลอกลวงในกรณีที่แตกต่างกัน จากนั้นผู้วิจัยนำข้อมูลมาประมวลผลเพื่อสังเคราะห์หาปัจจัยของการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ รูปแบบการหลอกลวง วิธีการหลอกลวง ความเสียหายที่เกิดขึ้น จากการถูกหลอกลวง และแนวทางการป้องกันการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์กรณีแก๊งคอลเซ็นเตอร์

**จริยธรรมการวิจัยในมนุษย์**

ผู้วิจัยดำเนินการขอรับการพิจารณาจริยธรรมการวิจัยในมนุษย์ จากคณะกรรมการพิจารณาจริยธรรมการวิจัยในมนุษย์ ชุดที่ 4 กลุ่มมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยบูรพา และได้ผ่านการพิจารณารับรองเรียบร้อยแล้ว เมื่อวันที่ 2 กรกฎาคม พ.ศ. 2567 โดยในการปฏิบัติการวิจัยในครั้งนี้ผู้วิจัยได้คำนึงถึงหลักการในการปฏิบัติตามหลักจริยธรรมการวิจัยในมนุษย์ โดยเฉพาะกับบุคคลที่เคยตกเป็นเหยื่อการหลอกลวงผ่านช่องทางออนไลน์ให้ลงทุนที่เป็นผู้ร่วมในการวิจัยครั้งนี้

ผู้วิจัยเคารพในบุคคลและศักดิ์ศรีความเป็นมนุษย์ การขอความยินยอมโดยให้ข้อมูลอย่างครบถ้วนเพื่อให้ผู้ให้ข้อมูลสำคัญตัดสินใจอย่างอิสระ และเก็บรักษาความลับข้อมูลส่วนตัวของผู้ให้ข้อมูลสำคัญโดยเฉพาะประชาชนที่เคยตกเป็นเหยื่อซึ่งถือเป็นกลุ่มเปราะบาง และยังต้องรักษาไว้ซึ่งหลักคุณประโยชน์ที่จะไม่เสี่ยงให้ก่ออันตรายทั้งกายใจกับผู้ให้ข้อมูลสำคัญ โดยหากผู้ร่วมในการวิจัยรู้สึกอึดอัด หรือรู้สึกไม่สบายใจกับบางคำถามมีสิทธิ์ที่จะไม่ตอบคำถามเหล่านั้น รวมถึงมีสิทธิ์ถอนตัวออกจากโครงการนี้เมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า และการไม่เข้าร่วมหรือถอนตัวออกจากโครงการวิจัยจะไม่มีผลกระทบใด ๆ ต่อผู้ให้ข้อมูลซึ่งข้อมูลในการสัมภาษณ์จะถูกเก็บรักษาไว้ ไม่เปิดเผยต่อสาธารณะเป็นแต่จะรายงานผลการวิจัยในภาพรวมเท่านั้น และได้ดำเนินการทำลายข้อมูลที่เกี่ยวข้องหลังเสร็จสิ้นการวิจัย

โดยผู้วิจัยคัดเลือกกลุ่มตัวอย่างโดยวิธีการเลือกแบบเจาะจง ด้วยหลักความยุติธรรม โดยปราศจากอคติหรือการบังคับ และการดูแลคลนต่อสถานะทางสังคมของผู้ร่วมในการวิจัยในครั้งนี้ เป็นไปตามสถานะที่กำหนดในกลุ่มผู้ให้ข้อมูลสำคัญ 2 กลุ่ม ที่ได้กล่าวไว้แล้ว ผู้ให้สัมภาษณ์ให้สัมภาษณ์ด้วยความสมัครใจ และสามารถปฏิเสธการตอบการสัมภาษณ์ได้ตลอดเวลา

ทั้งนี้การติดต่อและวิธีการเข้าถึงผู้มีส่วนร่วมในการวิจัยครั้งนี้ ผู้วิจัยตระหนักถึงการไม่รุกล้ำความเป็นส่วนตัว โดยได้มีการติดต่อนัดหมายล่วงหน้า และส่งเอกสารชี้แจงเพื่อให้ผู้มีส่วนร่วมในการวิจัยได้มีโอกาสพิจารณาก่อนตัดสินใจในการเข้าร่วมในการให้ข้อมูลสำหรับงานวิจัยในครั้งนี้

# บทที่ 4

# ผลการวิจัย

การวิจัยเรื่อง การหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) มีวัตถุประสงค์เพื่อศึกษาถึงการกระทำอันเป็นการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์ เพื่อศึกษาถึงปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ และเพื่อเสนอแนะการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ โดยผู้วิจัยจะนำเสนอผลการศึกษา ดังนี้

1. ลักษณะของการหลอกลวงทางไซเบอร์ ลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์

2. ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์

3. ข้อเสนอแนะการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์

**ลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์**

การหลอกลวงทางไซเบอร์ในปัจจุบันได้พัฒนาไปอย่างซับซ้อนมากขึ้น โดยมีการโจมตีรูปแบบใหม่ ๆ ที่พุ่งเป้าไปยังบุคคลและองค์กรในหลากหลายอุตสาหกรรม ทำให้บุคคลตกเป็นเหยื่อมากขึ้น โดยเฉพาะการหลอกลวงทางไซเบอร์กรณีแก๊งคอลเซ็นเตอร์ที่ยังคงเป็นปัญหาที่พบเห็นได้บ่อยได้ในประเทศไทย และผู้หลอกลวงมีการใช้วิธีหลอกลวงที่ซับซ้อนมากขึ้น โดยมักปลอมเป็นเจ้าหน้าที่รัฐ เช่น ตำรวจ หรือบริษัทขนส่งต่างชาติ เพื่อสร้างเหตุการณ์ว่าเหยื่อมีส่วนเกี่ยวข้องกับคดี เช่น การค้ายาเสพติด ฟอกเงิน หรือมีพัสดุต้องสงสัย เพื่อกดดันให้โอนเงินไปแสดงความบริสุทธิ์ใจ รวมไปถึงการอ้างว่าบัญชีธนาคารของเหยื่อถูกอายัดหรือมีหนี้บัตรเครดิตที่ต้องชำระ โดยแก๊งคอลเซ็นเตอร์มักจะบังคับให้เหยื่อพูดคุยต่อเนื่อง ไม่ให้ติดต่อคนอื่นเพื่อขอคำปรึกษา และขู่ให้โอนเงิน เป็นต้น

ลักษณะการหลอกลวงของแก๊งคอลเซ็นเตอร์มีหลากหลายรูปแบบ ซึ่งผู้วิจัยสามารถค้นพบรูปแบบการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์ที่สามารถแบ่งออกเป็นทั้งหมด 2 รูปแบบ คือ การหลอกลวงทางโทรศัพท์ และการหลอกขายสินค้า ซึ่งมิจฉาชีพนั้นมักจะมีวิธีการใหม่ ๆ ในการหลอกลวง โดยการหาจุดร่วมในการสร้างความกลัว ความรีบเร่ง หรือความสับสนให้กับเหยื่อ เพื่อให้เหยื่อหลงเชื่อและกระทำตามที่มิจฉาชีพต้องการ โดยมีลักษณะการหลอกลวงที่พบบ่อยดังนี้

**1.1 รูปแบบการหลอกลวงทางโทรศัพท์**

การหลอกลวงทางโทรศัพท์โดยแก๊งคอลเซ็นเตอร์ยังคงเป็นปัญหาใหญ่ในประเทศไทย รูปแบบที่พบบ่อยคือ โดยคนร้ายมักอ้างตัวเป็นเจ้าหน้าที่ของรัฐ เพื่อสร้างเหตุการณ์ว่าเหยื่อมีการต้องหาคดี หรือเกี่ยวข้องกับการกระทำความผิด เพื่อให้เหยื่อเกิดความกลัวว่าจะถูกดำเนินคดี จากนั้นเมื่อเหยื่อเกิดความกลัว คนร้ายก็จะเสนอทางออกโดยการให้เหยื่อยอมทำตามขั้นตอนต่อไป หรือเข้าพบกับทางเจ้าหน้าที่ โดยทางออนไลน์หรือใช้วิธีการแอดไลน์เพิ่มเพื่อนเพื่อสนทนาต่อในขั้นตอนต่อไป กับคนร้ายที่รับบทบาทในขั้นตอนต่อไป โดยขั้นตอนสุดท้ายจะเกี่ยวกับการที่ให้เหยื่อทำการโอนเงินมาเพื่อทำการตรวจสอบ หรืออ้างเหตุอย่างใด ๆ เพื่อให้เหยื่อยอมทำตาม เมื่อเหยื่อหลงเชื่อก็จะสูญเสียเงินไปเป็นจำนวนมาก กล่าวคือ หากมีเงินในบัญชีมากเพียงใดก็จะสูญเงินหมดเท่านั้น

**1.1.1 แอบอ้างเป็นคนในครอบครัว** เป็นกลวิธีหนึ่งที่แก๊งคอลเซ็นเตอร์ใช้ในการเข้าหาเหยื่อและอ้างว่าเป็นสมาชิกในครอบครัว เช่น ลูกหลาน หรือพี่น้อง โดยมักใช้กลยุทธ์ต่าง ๆ เช่น การทำเสียงคล้ายกับคนในครอบครัวหรือใช้ข้อมูลส่วนตัวที่ถูกขโมยมาจากแหล่งอื่นเพื่อเพิ่มความน่าเชื่อถือ ผู้หลอกลวงอาจอ้างว่าตนอยู่ในสถานการณ์ฉุกเฉิน เช่น ประสบอุบัติเหตุหรือมีปัญหาทางการเงินและต้องการความช่วยเหลือด่วน ดังกรณีตัวอย่างต่อไปนี้

> คุณมนชิดา (นามสมมติ) อายุ 52 ปี ได้เล่าว่า *“ตอนนั้นพี่ได้รับโทรศัพท์จากหมายเลขแปลก พอรับสายเสียงของปลายสายฟังดูคุ้นเคย ปลายสายเสียงเป็นผู้หญิง เขาแนะนำตัวว่าเป็นหลานสาว พูดอย่างรีบร้อนว่ามือถือพัง ต้องการยืมเงินตอนนี้เลยเพราะจะไปซื้อเครื่องใหม่พี่ก็แปลกใจ แต่ตอนนั้นไม่ได้คิดอะไรมากเพราะฟังจากเสียงก็คุ้นมากเหมือนหลานสาวคนสนิท ด้วยความเป็นห่วงกลัวหลานลำบากพี่เลยรีบโอนเงินไปให้ตามคำขอ จำนวน 30,000 บาท หลังจากที่โอนเงินไปไม่นานก็มีสายโทรเข้าจากหมายเลขอีก โทรมาบอกว่าเงินจำนวน 30,000 บาทนั้นไม่พอที่จะซื้อมือถือเครื่องใหม่ พี่เลยโอนให้เพิ่มไปอีก 20,000 บาท แต่ตอนนั้นญาติ ๆ ก็เริ่มสงสัยและแปลกใจแล้วว่ายอดเงินที่โอนไปให้นั้นมันเยอะแปลก ๆ เลยโทรไปหาหลานสาวอีกคนที่อยู่ที่เดียวกันกับหลานสาวคนนี้ ปรากฏว่าเบอร์ที่โทรมาหาตอนแรกนั้นไม่ใช่เบอร์โทรของหลานสาวคนสนิทจริง ๆ แล้วตอนนี้โทรศัพท์มือถือก็ไม่ได้พังด้วย ตอนนั้นพี่แทบจะเป็นลมหลังจากรู้ตัวว่าโดนหลอกให้โอนเงิน เพราะยอดเงินที่โอนไปให้มิจฉาชีพก็รวม ๆ กันเป็นยอดจำนวน 50,000 บาท พี่ก็รีบไปแจ้งความทันทีหลังจากรู้เรื่อง แต่หลังจากแจ้งความเรื่องคดีของพี่คือไม่ค่อยมีความคืบหน้าอะไรเลย พี่ก็เริ่มปลงแล้ว และเหตุการณ์ครั้งนี้ถือว่าเป็นบทเรียนให้พี่ได้อย่างดีเลยว่า อย่าไว้ใจ*

*เบอร์แปลก เพราะต่อให้เราฟังแล้วเป็นน้ำเสียงที่คุ้นเคยมันก็ไม่มีอะไรมาการันตีได้ว่าปลายสายนั้นจะเป็นญาติหรือคนที่เราสนิทและไว้ใจ"*

(มนชิดา (นามสมมติ), สัมภาษณ์, 13 สิงหาคม 2567)

จากกรณีของคุณมนชิดา (นามสมมติ) จะเห็นได้ว่า ผู้หลอกลวงมีการใช้วิธีแอบอ้างเป็นคนในครอบครัวหรือคนรู้จัก เพื่อทำให้เหยื่อไว้วางใจ รู้สึกปลอดภัยและพร้อมที่จะช่วยเหลือ อีกทั้งยังสร้างสถานการณ์ที่ดูเร่งด่วน เช่น อุบัติเหตุ หรือการต้องการเงินด่วน เพื่อทำให้เหยื่อรู้สึกว่าจำเป็นต้องทำตามคำขอในทันที และเมื่อได้รับเงินตามที่ต้องการหรือผู้หลอกลวงรับรู้แล้วว่าเหยื่อรู้สึกตัวแล้วว่าถูกหลอก

**1.1.2 แอบอ้างเป็นเจ้าหน้าที่รัฐ หรือหน่วยงานที่น่าเชื่อถือ** เป็นกลวิธีที่นิยมใช้โดยแก๊งคอลเซ็นเตอร์เพื่อหลอกลวงประชาชน โดยกลุ่มผู้หลอกลวงมักจะสร้างสถานการณ์ที่ดูสมจริงและน่าเชื่อถือ ทำให้เหยื่อรู้สึกปลอดภัยและเชื่อถือในสิ่งที่ถูกเสนอ ดังกรณีตัวอย่างต่อไปนี้

คุณชัยชนะ (นามสมมติ) อายุ 30 ปี อาชีพ พนักงานประจำ เล่าว่า *"ตอนนั้นผมกำลังทำงานอยู่ก็มีสายเข้ามาจากหมายเลขแปลก ๆ ผมก็ลังเลเล็กน้อย แต่ก็ตัดสินใจกดรับสาย ปลายสายเป็นผู้หญิงที่อ้างตัวว่าเป็นเจ้าหน้าที่ธนาคาร บอกว่ามีปัญหาเกี่ยวกับบัญชีของผมและต้องการยืนยันตัวตนเพื่อแก้ไข โดยมีการพูดว่า เพื่อความปลอดภัยคุณจำเป็นต้องทำตามขั้นตอนที่เราจะแนะนำต่อไปนี้ กรุณากดลิงก์ที่ส่งให้ในข้อความเพื่อยืนยันตัวตน และตอนนั้นด้วยความรีบร้อนและกังวล ผมเปิดลิงก์ที่ส่งมาตามที่เขาบอก หลังจากนั้นไม่นาน ผมก็เริ่มได้รับข้อความแจ้งเตือนจากแอพธนาคารว่าเงินในบัญชีกำลังถูกโอนออก ตอนนั้นผมรู้สึกตกใจมาก รีบตรวจสอบแอพธนาคาร และพบว่าเงินในบัญชีของผมถูกโอนออกไปอย่างต่อเนื่องโดยที่ผมไม่สามารถทำอะไรได้ พยายามติดต่อธนาคารทันที แต่เงินก็ถูกโอนไปเรียบร้อยแล้ว ผมรู้ทันทีว่าถูกหลอกให้กดลิงก์ที่ใช้ดึงข้อมูลจากแอพธนาคาร และนั่นคือวิธีที่พวกมิจฉาชีพใช้ดูดเงินออกจากบัญชีของผมโดยไม่รู้ตัว ความประมาทเพียงแค่รับสายจากเบอร์แปลกก็กลายเป็นประสบการณ์เจ็บปวดที่ต้องเสียเงินหลักแสนไปโดยไม่สามารถทำอะไรได้ครับ"*

(ชัยชนะ (นามสมมติ), สัมภาษณ์, 13 สิงหาคม 2567)

จากกรณีของคุณชัยชนะ (นามสมมติ) พบว่า ผู้หลอกลวงใช้วิธีการแอบอ้างเป็นเจ้าหน้าที่ธนาคารช่วยสร้างความน่าเชื่อถือ เนื่องจากธนาคารมักถูกมองว่าเป็นองค์กรที่มีความน่าเชื่อถือและมีความปลอดภัย ผู้หลอกลวงมักบอกว่ามีปัญหาทางการเงินที่ต้องการการแก้ไขด่วน เช่น บัญชีถูกระงับ หรือข้อมูลส่วนตัวถูกขโมย ทำให้เหยื่อรู้สึกว่าต้องทำตามคำแนะนำทันที และ

ในกรณีนี้เพียงดำเนินตามขั้นตอนที่ผู้หลอกลวงวางแผนไว้ ใช้วิธีการแค่กดลิงก์ที่ส่งมาก็สามารถดูดเงินจนหมดบัญชีโดยที่เหยื่อไม่ทันตั้งตัวได้ทัน

นอกจากนี้ยังมีอีกเหตุการณ์หนึ่งที่ผู้หลอกลวงใช้วิธีล่อลวงเหยื่อด้วยข้อกล่าวหาว่าบัญชีผิดกฎหมาย ซึ่งเป็นวิธีการที่อันตรายและเกิดขึ้นบ่อยครั้งในสังคมปัจจุบัน เพื่อใช้ในการข่มขู่ให้เหยื่อเกิดความกลัว และยอมโอนเงินเพื่อหลีกเลี่ยงการดำเนินคดี โดยมักใช้เอกสารปลอม โลโก้ของหน่วยงาน หรืออุปกรณ์สื่อสารที่ดูมืออาชีพ เพื่อเพิ่มความน่าเชื่อถือ จากการสัมภาษณ์คุณมาลี ( นามสมมติ) อายุ 59 ปี อาชีพ ค้าขาย ถึงประสบการณ์การตกเป็นเหยื่อแก๊งคอลเซ็นเตอร์

> *“เขาบอกว่าเขาเป็นเจ้าหน้าที่รัฐ แล้วก็พูดจริงจังมาก เขาบอกว่าบัญชีของพี่มีปัญหาทางกฎหมาย ถ้าไม่รีบแก้จะต้องเดือดร้อน ถูกจับหรืออะไรสักอย่าง พี่เองก็ไม่เข้าใจทั้งหมด แต่เขาบอกว่าเรื่องนี้ร้ายแรงมาก ถ้าไม่ทำตามอาจจะเป็นปัญหาทางกฎหมายใหญ่โต เพราะพี่ก็ไม่เคยมีปัญหาทางกฎหมายมาก่อน พอได้ยินเรื่องแบบนี้ก็กลัวนะ เขาพูดเหมือนรู้ทุกอย่างเกี่ยวกับบัญชีของพี่ รู้แม้กระทั่งยอดเงินในบัญชี มันทำให้พี่รู้สึกว่าเขาต้องเป็นเจ้าหน้าที่จริง ๆ ตอนนั้นพี่ก็ไม่อยากเดือดร้อนก็เลยทำตามที่เขาบอก โดยให้พี่โอนไปให้เขา 15,000 บาท เพื่อดำเนินการ พี่เชื่อใจก็โอนไปให้ พอหลังจากโอนให้เสร็จ ฝั่งที่บอกว่าเป็นเจ้าหน้าที่ของรัฐก็เงียบหายไป จนพี่เอาเรื่องนี้ไปปรึกษาลูกหลานก็ถึงจะมารู้สึกตัวเองว่าโดนมิจฉาชีพหลอกให้โอนเงินไปเรียบร้อยแล้ว พี่รู้สึกเสียใจมากที่โอนเงินไป ซึ่งตอนนั้นไม่คิดว่าจะมีใครมาหลอกกันแบบนี้”*
>
> (มาลี (นามสมมติ), สัมภาษณ์, 15 สิงหาคม 2567)

จากกรณีของคุณมาลี (นามสมมติ) ซึ่งมีความคล้ายคลึงกับกรณีของคุณเชิดชัย (นามสมมติ) อายุ 57 ปี ที่ถูกผู้หลอกลวงแอบอ้างว่าเป็นเจ้าหน้าที่รัฐ และแจ้งว่าพัสดุส่งถึงเหยื่อเป็นของที่ผิดกฎหมาย ซึ่งจะต้องมีการโอนเงินในบัญชีทั้งหมดไปให้เพื่อตรวจสอบ ซึ่งแท้จริงแล้วเป็นเพียงกลวิธีที่ใช้หลอกลวงเหยื่อเท่านั้น เมื่อได้รับเงินตามที่ต้องการแล้วผู้หลอกลวงจึงหนีหายไป ดังคำสัมภาษณ์ที่ว่า

> *“มีสายโทรเข้ามาบอกว่า นี่โทรมาจากไปรษณีย์ปทุมธานีนะ ตอนนี้พัสดุส่งถึงผมเป็นของที่ผิดกฎหมาย ต้องมาแจ้งความกับตำรวจของปทุมธานีนะ ตอนนั้นผมก็ตกใจเลยบอกไปว่าตอนนี้ผมไม่ได้อยู่ในปทุม ผมมางานบวชหลานที่ต่างจังหวัด แต่คนที่อ้างว่าเป็นไปรษณีย์บอกว่างั้นไม่เป็นไรเพราะว่าตอนนี้มีตำรวจในชั้นผู้ใหญ่อยู่ด้วย ให้ผมแอดไลน์มาได้เลยเพื่อที่จะคุยกับทางคุณตำรวจได้สะดวก พอผมแอดไลน์*

*ไปก็โดนเชิญเข้ากลุ่มชื่อ ปปง. และในกลุ่มก็มีเจ้าหน้าที่บอกกับผมว่าทางหน่วยงานต้องตรวจสอบทรัพย์สินทั้งหมดของผม โดยที่ผมจะต้องโอนเงินในบัญชีของผมทั้งหมดไปที่บัญชีของเจ้าหน้าที่ทั้งหมด เพื่อตรวจสอบเส้นทางการเงินทั้งหมด ตอนนั้นผมก็หลงเชื่อโอนให้เขาไปหมดเลย โดยที่ในบัญชีของผมมีเงินอยู่ประมาณ 300,000 บาท พอโอนไปให้เรียบร้อย อยู่ ๆ กลุ่มในไลน์ที่มีสมาชิกเป็นเจ้าหน้าที่กับผมก็ถูกลบไปแล้ว ไม่สามารถที่จะติดต่อได้อีก รู้ตัวอีกทีว่าโดนหลอกแน่นอนเลยไปแจ้งความทันที เป็นเหตุการณ์ที่ผมจำได้ไม่ลืมเลย"*

(เชิดชัย (นามสมมติ), สัมภาษณ์, 17 สิงหาคม 2567)

คุณกัญญารัตน์ (นามสมมติ) อายุ 55 ปี อาชีพ ธุรกิจส่วนตัว ได้เล่าว่า *"ตอนเช้าของวันนั้นฉันได้รับสายโทรศัพท์ เขาอ้างว่าเป็นตำรวจบอกว่าฉันมีส่วนเกี่ยวข้องกับคดียาเสพติด ต้องตรวจสอบทรัพย์สินทั้งหมด เพราะเดี๋ยว ปปง. จะมาอายัดทรัพย์ ฉันเลยเกิดความกลัวเลยได้มีการโอนเงินไปจำนวน 650,000 บาท และหลังจากนั้นก็มีการให้ฉันเพิ่มเพื่อนในไลน์กับโรงพักที่รับผิดชอบเรื่องนี้ แชทที่คุยกันฝ่ายนั้นบอกว่าเป็นตำรวจ มีการส่งเอกสารข้อมูลต่าง ๆ ของคดีที่ฉันมีส่วนเกี่ยวข้อง มันก็ทำให้ฉันเชื่อใจเข้าไปอีกว่า เรื่องที่เกิดขึ้นนี้เป็นเรื่องจริง แล้วก็มีการบอกกับฉันว่าเดี๋ยวช่วงบ่าย ๆ จะมีตำรวจชั้นผู้ใหญ่ยศสูงวิดีโอคอลคุยด้วย แล้วพอตอนบ่ายก็มีสายวิดีโอคอลจากตำรวจจริง ๆ ซึ่งตอนที่วิดีโอคอลคุยกันตำรวจคนนั้นก็ใช้ทั้งคำขู่ คำหว่านล้อมกดดันให้ฉันรู้สึกกลัว ฉันเลยเชื่อเข้าไปอีก และถ้าถามว่าทำไมฉันถึงเชื่อสุดใจขนาดนี้ ก็เพราะก่อนหน้านี้เคยโดนสถานการณ์ตำรวจมาค้นบ้าน นั่นเลยเป็นอีกสาเหตุที่ฉันเชื่อว่าเหตุการณ์ในครั้งนี้จะเป็นเรื่องจริง แต่ตอนที่ฉันมาเอะใจคือหลังจากที่ฉันโอนเงินไปให้เกือบหมดแล้ว ทางคนที่อ้างว่าเป็นตำรวจก็มีการส่งแชทมาหาฉันว่าให้ขายทองด้วยสิ เพื่อเอามาจ่ายให้เขา เลยรู้สึกว่าเหตุการณ์ครั้งนี้เริ่มแปลก ๆ แล้ว ฉันเลยนำเรื่องนี้ไปบอกกับสามีที่ตอนนั้นเขาออกไปทำงานอยู่นอกบ้าน สามีก็บอกฉันว่าแบบนี้นี่มันมิจฉาชีพแล้ว ให้ไปแจ้งตำรวจเองที่โรงพักเลยดีกว่า จากเหตุการณ์ครั้งนี้ก็เป็นบทเรียนครั้งใหญ่ที่สูญเสียเงินเกินครึ่งล้าน"*

(กัญญารัตน์ (นามสมมติ), สัมภาษณ์, 20 สิงหาคม 2567)

จากกรณีของคุณกัญญารัตน์ (นามสมมติ) จะเห็นได้ว่า ผู้หลอกลวงใช้วิธีการสร้างสถานการณ์ว่าเหยื่อเกี่ยวข้องกับสิ่งผิดกฎหมายคล้ายคลึงกับกรณีของคุณมาลี (นามสมมติ) และคุณเชิดชัย (นามสมมติ) แต่ในกรณีนี้ผู้หลอกลวงนำวิธีการใช้วิดีโอคอลมาประกอบกับการหลอกลวงในครั้งนี้ จึงทำให้มิจฉาชีพดูเหมือนเป็นบุคคลจริง มีตัวตนที่ชัดเจน ซึ่งช่วยสร้างความ

มั่นใจให้กับเหยื่อมากขึ้น ดังนั้นการให้ข้อมูลผ่านการวิดีโอคอลที่ไม่ได้รับการรับรองจึงส่งผลให้เกิดการสูญเสียเงินจำนวนมาก

อย่างไรก็ตามมิจฉาชีพเหล่านี้มักใช้หลักจิตวิทยาในการเชิญชวนให้คนหลงเชื่อว่าเหตุการณ์ที่สร้างขึ้นนั้นเป็นเรื่องจริง และเมื่อเหยื่อหลงเชื่อจึงเริ่มกระบวนการโดยให้เหยื่อปฏิบัติตามขั้นตอนที่สั่ง แต่การหลอกลวงของกรณีนี้มิจฉาชีพใช้วิธีการสั่งด้วยน้ำเสียงสุภาพและเป็นทางการเพื่อสร้างความน่าเชื่อถือ แต่ด้วยสถานการณ์ที่กดดันจึงทำให้เหยื่อตัดสินใจโดยปราศจากความรอบคอบ จากการสัมภาษณ์คุณพบรัก (นามสมมติ) อายุ 23 ปี ถึงเหตุการณ์ที่เคยถูกหลอกลวงจากแก๊งคอลเซ็นเตอร์

> *“ตอนนั้นหนูได้รับสายโทรเข้าเป็นผู้หญิงบอกว่าเป็นเจ้าหน้าที่ของธนาคาร ตอนแรกเขาก็แนะนำตัวว่ามาจากธนาคารไหน และก็บอกกับหนูว่าตอนนี้ทางธนาคารตรวจพบว่ามีการพยายามทำธุรกรรมที่น่าสงสัยในบัญชีของหนู เพื่อความปลอดภัยทางธนาคารต้องการยืนยันข้อมูลส่วนตัวสักครู่จะได้ไหม ในใจก็คิดว่าถ้ามีการถอนเงินจากบัญชีจริงๆ ทำไมธนาคารถึงโทรมาแจ้งแบบนี้หนูไม่ได้มีประสบการณ์เกี่ยวกับเรื่องแบบนี้มาก่อน และไม่เคยได้รับการแจ้งเตือนจากธนาคารในลักษณะนี้เลย แต่ด้วยความที่กังวลเกี่ยวกับเงินในบัญชี และรู้สึกว่าทุกอย่างมันเกิดขึ้นเร็วมาก พี่คนนั้นพูดด้วยน้ำเสียงที่สุภาพและเป็นทางการ หนูก็เริ่มคิดว่าน่าจะเป็นเจ้าหน้าที่จริง ๆ เพราะเขาพูดข้อมูลเกี่ยวกับบัญชีของหนูได้ละเอียด และบอกว่าธนาคารจะส่ง SMS เพื่อยืนยันตัวตนอีกครั้ง หนูเลยคิดว่าไม่น่าจะมีปัญหาอะไร หนูก็เลยยอมให้ข้อมูลไปทั้งเลขบัตรประชาชนและเลขบัญชี โดยไม่ได้คิดอะไรมาก หลังจากที่ให้ข้อมูลไป พี่เขาก็บอกว่าตอนนี้ข้อมูลได้ยืนยันเรียบร้อยแล้ว เพื่อความปลอดภัยจะได้รับ SMS เพื่อเปลี่ยนรหัสผ่านและอัปเดตข้อมูลของภายใน 24 ชั่วโมง และวางสายไป หลังจากวางสายไปได้สักพัก หนูก็เริ่มรู้สึกไม่ค่อยสบายใจ แต่ก็คิดว่าทางธนาคารคงจัดการได้ หนูเลยไม่ได้คิดอะไรมาก แต่พอถึงช่วงดึก ๆ หนูลองเข้าแอปธนาคารของตัวเองเพื่อตรวจสอบยอดเงินในบัญชี แต่พบว่ามีการถอนเงินออกไปถึง 20,000 บาท ตกใจมากรีบโทรติดต่อไปยังธนาคารทันที แต่ธนาคารแจ้งว่ามีการทำธุรกรรมโดยใช้ข้อมูลยืนยันตัวตน และยากที่จะยกเลิกได้ เพราะเป็นธุรกรรมที่สมบูรณ์แล้ว หนูเริ่มรู้ว่าตัวเองโดนหลอกเข้าเต็ม ๆ หนูเสียใจและรู้สึกผิดที่ไม่เชื่อสัญชาตญาณของตัวเองตั้งแต่แรก และรีบไปแจ้งความที่สถานีตำรวจพร้อมแจ้งธนาคารเพื่อระงับบัญชีเพิ่มเติม”*
>
> (พบรัก (นามสมมติ), สัมภาษณ์, 23 สิงหาคม 2567)

คุณสุเมธ (นามสมมติ) อายุ 48 ปี อาชีพ รับจ้างทั่วไป *“ผมได้รับโทรศัพท์จากหมายเลขที่ไม่รู้จัก เขาบอกว่าเป็นเจ้าหน้าที่จากการไฟฟ้า และบอกว่าบ้านผมค้างชำระค่าไฟฟ้าที่สูงผิดปกติ พูดด้วยน้ำเสียงจริงจังเลยนะ ค้างจำนวนเงิน 5,000 บาท ถ้าไม่ชำระภายในวันนี้จะมีการตัดไฟและดำเนินการตามกฎหมาย ผมรู้สึกตกใจ เพราะผมไม่เคยได้รับการแจ้งเตือนใด ๆ จากการไฟฟ้า และเขาบอกต่อว่าสามารถช่วยได้โดยให้โอนเงินมาที่บัญชีที่เขาบอกเพื่อป้องกันการตัดไฟ จากนั้นผมก็พยายามที่จะสอบถามเพิ่มเติมว่าตอนนี้ผมเองก็ไม่ได้รับการแจ้งเตือนจากการไฟฟ้า แต่เขาก็ตอบกลับมาย้ำอีกว่าให้ผมไปตรวจสอบกับการไฟฟ้าสาขาใกล้บ้านได้ แต่ถ้าผมไม่โอนเงินวันนี้ ผมจะต้องเจอกับปัญหาใหญ่ ตอนนั้นผมรู้สึกสับสนและกลัวการถูกตัดไฟ ผมเลยตัดสินใจที่จะโอนเงินไปยังบัญชีที่ให้มา โดยคิดว่ามันจะช่วยป้องกันปัญหาที่จะเกิดขึ้น แต่พอหลังจากโอนเงินเสร็จ ผมก็เริ่มรู้สึกไม่สบายใจและตัดสินใจที่จะโทรไปสอบถามที่การไฟฟ้า ปรากฏว่าไม่มีข้อมูลเกี่ยวกับการค้างชำระค่าไฟฟ้าของผม เมื่อรู้ตัวว่าผมถูกหลอก ผมรู้สึกสิ้นหวังและรีบไปแจ้งความกับตำรวจ แต่เงินที่โอนไปนั้นไม่สามารถตามกลับมาได้”*

(สุเมธ (นามสมมติ), สัมภาษณ์, 27 สิงหาคม 2567)

กรณีของคุณสุเมธ (นามสมมติ) นั้น การที่ผู้หลอกลวงอ้างถึงหน่วยงานของรัฐที่มีชื่อเสียง โดยมักจะใช้ภาษาที่ดูเป็นทางการและมีน้ำเสียงที่มั่นใจ มีเป้าหมายเพื่อสร้างความน่าเชื่อถือให้กับเหยื่อ การใช้ข้อมูลที่เฉพาะเจาะจง เช่น หมายเลขโทรศัพท์ที่เหมือนจะเป็นของหน่วยงาน การให้รายละเอียดเกี่ยวกับกระบวนการตรวจสอบ หรือหากเหยื่อเกิดข้อสงสัยสามารถไปสอบถามที่สำนักงานได้ การกระทำของมิจฉาชีพในลักษณะดังกล่าวเป็นเพียงการทำให้เหยื่อเกิดความมั่นใจว่ากำลังติดต่อกับเจ้าหน้าที่จริง ๆ เมื่อหลงเชื่อจึงมีความเป็นไปได้ว่าเหยื่อจะปฏิบัติตามคำสั่ง เนื่องจากกลัวผลกระทบที่จะตามมาในภายหลังหากมีการฝ่าฝืน แม้ในภายหลังจะสามารถตรวจสอบแล้วพบว่าเป็นการหลอกลวงก็ไม่อาจได้รับเงินคืนได้ทัน แต่ในบางรายเมื่อรู้สึกตัวว่าตนกำลังถูกหลอกและเข้าแจ้งความในทันทีนั้นจึงมีความเป็นไปได้ที่จะได้รับเงินในส่วนนั้นคืน ดังคำสัมภาษณ์ของคุณเพลงรัก (นามสมมติ) อายุ 45 ปี ได้เล่าว่า

*“ได้รับสายจากเบอร์แปลกค่ะ ปลายสายบอกว่าเป็นเจ้าหน้าที่ของกรมที่ดิน และมีการแจ้งว่าตอนนี้ฉันมีปัญหาเกี่ยวกับโฉนดที่ดินที่เราซื้อไว้เมื่อปลายปีที่แล้ว และบอกต่อว่าตอนนี้ได้ตรวจสอบเอกสารและพบว่ามีการร้องเรียนเกี่ยวกับโฉนดที่ดินไม่มีความถูกต้อง ถ้าไม่ชำระค่าปรับภายใน 24 ชั่วโมง ทางกรมที่ดินจะดำเนินการยกเลิกโฉนดและดำเนินคดีทางกฎหมาย และเพื่อให้ได้ข้อมูลที่ถูกต้อง*

*จะต้องโอนเงินค่าปรับจำนวน 10,000 บาทไปยังบัญชีที่เขาบอกมาเพื่อป้องกันปัญหาที่จะเกิดขึ้น ตอนนั้นด้วยความกลัวที่จะสูญเสียที่ดิน เลยตัดสินใจโอนเงินไปยังบัญชีที่ได้รับคำแนะนำ แม้ว่าจะมีข้อสงสัยนะแต่ก็เลือกที่จะเชื่อ หลังจากโอนเงินแล้ว รู้สึกไม่สบายใจ และพยายามจะโทรไปสอบถามที่กรมที่ดิน ปรากฏว่าไม่มีการร้องเรียนหรือปัญหาใด ๆ เกี่ยวกับโฉนดที่เขาพูดถึงเลย เมื่อรู้ตัวว่าถูกหลอกรู้สึกโกรธมากค่ะ เลยรีบไปแจ้งความกับตำรวจ โชคดีที่เงินที่โอนไปสามารถตามกลับมาได้ทัน"*

(เพลงรัก (นามสมมติ), สัมภาษณ์, 27 สิงหาคม 2567)

จากผลการศึกษาแก๊งคอลเซ็นเตอร์รูปแบบการหลอกลวงทางโทรศัพท์มักใช้วิธีการหลอกลวงที่หลากหลาย โดยมีการสร้างสถานการณ์ที่ดูน่าเชื่อถือเพื่อให้เหยื่อยอมให้ข้อมูลส่วนตัวหรือทำธุรกรรมทางการเงิน ซึ่งแนวทางที่พบบ่อยในการหลอกลวงได้แก่ การอ้างว่าเป็นเจ้าหน้าที่จากหน่วยงานราชการ ธนาคาร หรือบริษัทชั้นนำ รวมถึงบุคคลในครอบครัว โดยมักจะติดต่อผู้คนผ่านทางโทรศัพท์เพื่อเสนอข้อเสนอที่ดึงดูดใจ เช่น การแจกเงินรางวัลหรือสิทธิพิเศษต่าง ๆ ที่ทำให้เหยื่อรู้สึกตื่นเต้นและต้องการรับประโยชน์ทันที

**1.2 รูปแบบการหลอกขายสินค้า**

การหลอกขายสินค้าของแก๊งคอลเซ็นเตอร์เป็นหนึ่งในวิธีการหลอกลวงที่พบบ่อยในปัจจุบัน โดยมีรูปแบบที่หลากหลาย เช่น การหลอกขายสินค้าออนไลน์ที่ไม่ตรงปก หรือการหลอกให้เหยื่อชำระเงินก่อนรับสินค้าที่ไม่มีอยู่จริง ดังกรณีตัวอย่างต่อไปนี้

คุณดนัย (นามสมมติ) อายุ 32 ปี ได้เล่าว่า *"ตอนนั้นต้องการติดตั้งแอร์ในห้องนอนเพราะอากาศที่ร้อนมาก ผมเลยโพสต์ขอคำแนะนำเรื่องแอร์ในเฟซบุ๊ก มันเป็นกลุ่มที่คอยให้คำแนะนำกันอ่ะครับ จนวันหนึ่งผมได้รับโทรศัพท์จากชายที่อ้างว่ามาจากบริษัทแอร์ชื่อดัง ซึ่งผมก็เคยได้ยินชื่อบริษัทนี้มาก่อน เขาบอกว่าตอนนี้ทางบริษัทมีโปรโมชั่นพิเศษสำหรับลูกค้าที่สั่งซื้อแอร์ในราคาลด 30% พร้อมบริการติดตั้งฟรี และผมเห็นว่าเป็นโอกาสที่ดี ทำให้ผมสนใจและสอบถามรายละเอียดเพิ่ม ฝ่ายคนขายพูดคุยอย่างเป็นมืออาชีพและดูเป็นมิตร แต่เขาบอกว่าต้องชำระเงินมัดจำจำนวน 15,000 บาทก่อนเพื่อยืนยันการจองและทำให้สามารถส่งทีมมาติดตั้งได้เร็ว ผมเลยตัดสินใจตกลงและโอนเงินไปยังบัญชีที่เขาให้ หลังจากนั้นเขาก็ยืนยันวันติดตั้งและบอกว่าจะมีทีมงานติดต่อมาในอีก 3 วัน แต่เมื่อถึงวันนัดหมาย ผมก็รอทีมช่างมาติดตั้งแอร์ แต่ไม่มีใครมาเลย ผมเลยลองโทรกลับไปยังหมายเลขที่คนนั้นใช้ติดต่อกับผม แต่โทรไม่ติดและไม่สามารถติดต่อได้ ผมจึงรู้สึกไม่สบายใจและลองค้นหาข้อมูลเกี่ยวกับบริษัทนี้ในอินเตอร์เน็ต จนพบว่าเป็นกลโกงที่มีคนโดนหลอกมาแล้วหลาย*

*ราย บางคนเสียเงินไปมากกว่าผมเสียอีก พอผมรู้ตัวว่าผมโดนหลอก ผมรีบไปแจ้งความกับเจ้าหน้าที่ตำรวจ พร้อมนำหลักฐานการโอนเงินและข้อความที่เคยคุยกับคนขายไปให้ตำรวจตรวจสอบ ตำรวจบอกว่าเคสลักษณะนี้เกิดขึ้นบ่อยมาก เพราะคนร้ายจะเลือกเหยื่อที่ไม่ระวัง และใช้วิธีการขายสินค้าในราคาพิเศษเพื่อจูงใจ และเหตุการณ์ที่ผมโดนในครั้งนี้ผมก็ไม่มีการได้รับเงินคืนเลย"*

(ดนัย (นามสมมติ), สัมภาษณ์, 10 สิงหาคม 2567)

สำหรับกรณีของคุณดนัย (นามสมมติ) จะเห็นได้ว่า การที่คุณดนัยโพสต์ขอคำแนะนำเรื่องแอร์ในเฟซบุ๊กซึ่งเป็นพื้นที่สาธารณะ บุคคลภายในกลุ่มสามารถเห็นถึงโพสต์ดังกล่าวได้ การกระทำลักษณะนี้จึงถือว่าเป็นการเปิดโอกาสให้มิจฉาชีพช่องทางหนึ่งในการหลอกลวง โดยแอบอ้างสวมรอยเป็นเจ้าหน้าที่หรือพนักงานที่เกี่ยวข้องกับด้านนั้นโดยตรง และเมื่อเหยื่อหลงเชื่อในคำพูดนำไปสู่การถูกหลอกลวงในที่สุด ซึ่งคล้ายคลึงกับกรณีของคุณเฟื่องรัตน์ (นามสมมติ) อายุ 25 ปี เพียงแต่เป็นเหตุการณ์ที่สั่งสินค้าไปแล้วแต่สิ่งที่ได้รับนั้นพบว่าไม่ตรงตามที่โฆษณา จึงทำให้เกิดความผิดหวังและสูญเสียความเชื่อมั่นในตลาด ดังคำสัมภาษณ์ที่ว่า

*"เคยโดนหลอกจากการสั่งซื้อสินค้าผ่านทางแอปพลิเคชันค่ะ มันเป็นการโกงแบบซับซ้อนและน่าเชื่อถือ เริ่มต้นจากการที่เราเห็นโพสต์โฆษณาสินค้าราคาถูก ซึ่งสินค้านั้นเป็นของที่กำลังมองหาอยู่พอดี ผู้ขายมีรีวิวดี มีผู้ติดตามเยอะ ทำให้เชื่อใจและตัดสินใจสั่งซื้อสินค้า แต่หลังจากโอนเงินเพื่อชำระค่าสินค้าอ่ะค่ะ เขาแจ้งว่าต้องรอสินค้าพรีออเดอร์ และจะส่งให้ภายในสองสัปดาห์ ตัวเราเองก็ไม่ได้เอะใจอะไร เพราะมีการอัปเดตสถานการณ์ส่งของอยู่เป็นระยะ ๆ แต่พอเวลาผ่านไปเกินกำหนดที่จะต้องได้รับสินค้ากลับยังไม่ได้รับสินค้า เลยลองสอบถามไปยังผู้ขาย แต่ก็ไม่ได้รับคำตอบ และบัญชีผู้ขายก็เริ่มมีพฤติกรรมแปลก ๆ เขาปิดการตอบกลับข้อความและเปลี่ยนชื่อ นอกจากเราก็ยังมีผู้เสียหายหลายคนที่เจอสถานการณ์เดียวกันค่ะ บางคนก็เพิ่งสั่งซื้อสินค้าจากผู้ขายรายนี้ไปไม่นาน และยังมีคนใหม่ ๆ ตกเป็นเหยื่ออยู่เรื่อย ๆ และทำให้คนใหม่ ๆ หลงเชื่อและสั่งซื้อสินค้าจากเขา เราก็เลยรวมตัวกันแจ้งความส่วนผู้ขายปิดบัญชีหนีไปพร้อมกับเงิน บางคนเสียหลักหมื่นถึงหลักแสน จากเหตุการณ์นี้ทำให้เราสำนึกได้ว่าการซื้อสินค้าผ่านโซเชียลมีเดียมีความเสี่ยงสูงมาก ครั้งต่อ ๆ ไปจะต้องตรวจสอบให้รอบคอบทุกครั้ง"*

(เฟื่องรัตน์ (นามสมมติ), สัมภาษณ์, 15 สิงหาคม 2567)

คุณลลิตตา (นามสมมติ) อายุ 28 ปี อาชีพ พนักงานประจำ ได้เล่าว่า *"เหตุการณ์ที่โดนโกงคือเห็นโฆษณาขายโทรศัพท์มือถือในเพจร้านค้าออนไลน์ค่ะ ซึ่งร้านนี้*

*ขายมือถือในราคาถูกมาก มีจำนวนผู้กดติดตามเพจเยอะอยู่พอสมควร และมีรีวิวการันตีจากลูกค้าท่านอื่นว่ามีการส่งสินค้าจริง ๆ และสินค้าก็ได้ตรงตามที่สั่ง เลยเป็นโอกาสที่ดีเกินกว่าจะปล่อยผ่านไป และด้วยราคาที่ลดลงเกือบครึ่งจากปกติ ทำให้ตัดสินใจสั่งซื้อมือถือยี่ห้อไอโฟนหนึ่งเครื่องในราคา 25,000 บาท ที่โดยปกติโทรศัพท์มือถือรุ่นนี้จะอยู่ที่ประมาณราคา 30,000 กว่าบาท แต่พอเห็นราคาที่ร้านลดมาถึงขนาดนี้ก็เป็นสิ่งที่น่าสนใจ หลังจากรอคอยไม่กี่วัน พัสดุก็มาส่งถึงบ้าน เราก็รีบเปิดกล่องด้วยความตื่นเต้น แต่ทันทีที่เห็นสิ่งของในกล่อง ความรู้สึกมันก็เปลี่ยนเป็นความโกรธและผิดหวังแทนเลยค่ะ เพราะข้างในกล่องพัสดุนั้นกลับเป็นผงซักฟอกถุงเล็ก ๆ อยู่ 2-3 ห่อ ที่ดูแล้วราคาไม่น่าเกิน 50 บาท มันเป็นความเจ็บใจที่เกิดขึ้นไม่ใช่แค่เพียงการเสียดายเงิน 25,000 บาท แต่กลับได้ผงซักฟอกราคาถูกมาแทนโทรศัพท์ที่ตั้งใจจะซื้อ รู้สึกทั้งโดนหลอกและเสียศรัทธาในร้านค้าออนไลน์มาก ๆ มาทราบภายหลังว่าร้านนี้เคยมีประวัติการโกงแบบนี้อยู่แล้ว แต่ร้านได้ทำการเปิดบัญชีใหม่มาก่อเหตุซ้ำเลยทำให้ไม่เป็นที่น่าสงสัย นอกจากเราก็มีผู้เสียหายจำนวนมากที่ยังไม่ได้รับความเป็นธรรมเหมือนกัน ได้ข้อคิดเลยว่าอย่าเชื่อในราคาที่ถูกกว่า Shop Official ไม่งั้นจะโดนหลอกแบบเรา"*

(ลลิตตา (นามสมมติ), สัมภาษณ์, 18 สิงหาคม 2567)

สำหรับกรณีของคุณลลิตตา (นามสมมติ) นั้น ผู้ตกเป็นเหยื่อมีความต้องการสินค้าในราคาที่ถูกกว่าตามท้องตลาด จึงส่งผลให้มิจฉาชีพแอบอ้างขายสินค้าหรือบริการในราคาถูกเกินจริง หรือการจัดโปรโมชั่นหรือการให้ส่วนลดที่ดูน่าสนใจ เพื่อกระตุ้นให้ผู้บริโภคซื้อสินค้าในทันที เพื่อเป็นกลยุทธ์ในการหลอกลวงผู้บริโภค โดยมักใช้วิธีการที่ดึงดูดใจและสร้างความต้องการในตลาด จึงส่งผลให้ผู้บริโภคที่ตกเป็นเหยื่ออาจจ่ายเงินไปแล้วแต่ไม่ได้รับสินค้าหรือบริการตามที่สัญญา ซึ่งคล้ายคลึงกับกรณีของคุณสุดสายใจ (นามสมมติ) อายุ 40 ปี ที่สั่งสินค้าลดราคาแต่สิ่งที่ได้รับนั้นพบว่าไม่ตรงตามที่โฆษณา ดังคำสัมภาษณ์ที่ว่า

*"ไปเจอโฆษณากระเป๋าชิ้นหนึ่งค่ะตอนเล่นเฟซบุ๊ก เป็นกระเป๋าแบรนด์ดังที่อยากได้มานาน ราคาแค่ 3,990 บาท ซึ่งปกติราคาจะสูงกว่านั้นหลายเท่า ก็คิดในใจว่าราคาถูกขนาดนี้ ต้องรีบซื้อแล้วล่ะ เลยกดสั่งซื้อทันที ก่อนจะรีบโอนเงินอย่างรวดเร็วเพราะกลัวว่าของจะหมด หลังจากกดสั่งก็ได้รับข้อความยืนยันการสั่งซื้อพร้อมทั้งเลขติดตามพัสดุ ดูเหมือนจะไม่มีอะไรผิดปกติ แต่เมื่อถึงกำหนดส่ง พัสดุกลับยังมาไม่ถึง จึงตัดสินใจเช็กเลขพัสดุที่ได้รับ ปรากฏว่าเลขพัสดุนั้นไม่สามารถติดตามได้ ตอนนั้นรู้สึกเริ่มกังวลแล้ว เลยพยายามติดต่อร้านค้า แต่ไม่มีการตอบกลับใด ๆ*

*ทั้งสิ้นค่ะ พอผ่านไปประมาณสองสัปดาห์พัสดุก็มาถึง แต่สิ่งที่ได้รับกลับไม่ใช่กระเป๋าแบรนด์หรูที่คาดหวัง แต่เป็นกระเป๋าผ้าธรรมดา ๆ ที่ดูราคาถูกและไร้คุณภาพเหมือนของในตลาดนัด ทั้งตกใจและโกรธมาก พยายามติดต่อร้านค้าอีกครั้ง แต่บัญชีร้านก็ถูกปิดไปแล้ว พอรู้ตัวว่าโดนหลอกก็โมโหตัวเองมากที่เห็นแก่ของถูกเกินไป แต่เหตุการณ์ครั้งนี้ทำให้ได้เรียนรู้บทเรียนสำคัญเกี่ยวกับการซื้อของออนไลน์ว่าไม่ควรเชื่อราคาถูกจนเกินไป และต้องตรวจสอบความน่าเชื่อถือของร้านค้าให้ดี"*

(สุดสายใจ (นามสมมติ), สัมภาษณ์, 30 สิงหาคม 2567)

จากผลการศึกษารูปแบบการหลอกขายสินค้าของแก๊งคอลเซ็นเตอร์นั้นเริ่มต้นด้วยการสร้างความน่าเชื่อถือ แก๊งคอลเซ็นเตอร์มักจะแอบอ้างตัวเป็นบริษัทหรือแบรนด์สินค้าชั้นนำเพื่อสร้างความเชื่อมั่นให้กับเหยื่อ การใช้ชื่อเสียงของบริษัทที่มีอยู่จริงในการหลอกลวงมักทำให้เหยื่อรู้สึกปลอดภัยและกล้าซื้อสินค้ามากขึ้น นอกจากนี้ บางครั้งอาจมีการใช้หมายเลขโทรศัพท์ที่มีลักษณะคล้ายคลึงกับบริษัทที่น่าเชื่อถือเพื่อหลีกเลี่ยงความสงสัย ต่อมาจะใช้การเสนอโปรโมชั่นหรือข้อเสนอที่ดึงดูดใจ เช่น การขายสินค้าราคาถูก หรือการจัดโปรโมชั่นพิเศษที่มีเวลาจำกัด ทำให้เหยื่อรู้สึกเร่งรีบและต้องรีบตัดสินใจซื้อ ในบางกรณีอาจมีการสร้างความรู้สึกว่าเป็นโอกาสที่ไม่ควรพลาด ทำให้เหยื่อหลงเชื่อและทำการสั่งซื้อโดยไม่คิดอย่างรอบคอบ

นอกจากนี้ การหลอกขายสินค้ายังใช้กลยุทธ์การสร้างความกลัวหรือความวิตกกังวลเพื่อดึงดูดความสนใจของเหยื่อ โดยการอ้างว่าสินค้าที่เสนอเป็นของแท้และมีคุณภาพดี หากไม่ซื้อจะพลาดโอกาสในการได้รับสินค้าดี ๆ หรือจะทำให้เหยื่อเกิดความไม่พอใจจากการใช้สินค้าที่มีคุณภาพต่ำ โดยมีการเปรียบเทียบกับคู่แข่งที่ไม่ดี เพื่อผลักดันให้เหยื่อรู้สึกว่าเป็นการตัดสินใจที่จำเป็นต้องทำในขณะนั้น สุดท้ายหลังจากที่เหยื่อได้ทำการชำระเงินแล้ว มักจะเกิดปัญหา คือการไม่ส่งสินค้าหรือส่งสินค้าที่ไม่มีคุณภาพ ไม่ตรงปก ซึ่งทำให้เหยื่อไม่สามารถติดตามหรือเรียกร้องคืนเงินได้และ แก๊งคอลเซ็นเตอร์เหล่านี้มักมีวิธีการในการปิดบังตัวตน ทำให้การสืบสวนและการดำเนินคดีจึงเป็นไปได้ยาก

**ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์**

อาชญากรรมไซเบอร์ในประเทศไทยได้กลายเป็นปัญหาที่เพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะการโจมตีทางการเงิน การหลอกลวงผ่านโซเชียลมีเดีย และการโจมตีระบบคอมพิวเตอร์ของหน่วยงานรัฐและเอกชน จึงส่งผลให้ปัจจุบันผู้ที่ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในประเทศไทยมีจำนวนมากขึ้น โดยเฉพาะกลุ่มวัยทำงาน อายุระหว่าง 20 - 60 ปี เนื่องจากเป็นบุคคลที่มีการใช้โซเชียลมีเดียในการดำเนินชีวิต และการทำธุรกรรมต่าง ๆ จึงมีโอกาสที่จะตกเป็นเหยื่อการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ได้ง่าย และปัจจัยที่ทำให้บุคคลตกเป็นเหยื่อของแก๊ง

คอลเซ็นเตอร์มักมาจากการใช้กลยุทธ์ทางจิตวิทยาเพื่อกดดันและหลอกลวงผู้คนให้ทำตามคำสั่งของมิจฉาชีพ ทำให้บุคคลเกิดความกลัว ความโลภ และเกิดความเชื่อถือ เนื่องจากรู้ไม่เท่าทันกลโกง อย่างไรก็ตามผู้วิจัยสามารถวิเคราะห์ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ได้ดังต่อไปนี้

1. ปัจจัยด้านความกลัว เป็นปัจจัยสำคัญในการทำให้คนถูกหลอกลวงได้ง่ายเนื่องจากความกลัวทำให้มีการตัดสินใจอย่างรีบเร่งโดยไม่ตรวจสอบข้อเท็จจริงก่อน ส่งผลให้มีการโอนเงินหรือให้ข้อมูลสำคัญเพื่อแก้ปัญหาที่ไม่เกิดขึ้นจริง และกลายเป็นผู้เสียหายของการหลอกลวงทางโทรศัพท์ ดังคำสัมภาษณ์ที่ว่า

> *“มิจฉาชีพจะขู่ให้ตกใจกลัวว่ามีความผิด ส่วนใหญ่มิจฉาชีพจะได้ข้อมูลส่วนตัวทางการแฮ็กที่มีคนนำมาขาย เมื่อเขามีข้อมูลระดับหนึ่งแล้วเขาก็จะโทรมาและอ้างเหมือนประมาณว่า ใช่คุณ...หรือไม่ จากนั้นจึงค่อย ๆ หลอกถามพอให้รู้จุดอ่อนและเขาก็จะหลอกให้กลัวว่า อาจจะเคยทำผิดหรือตรวจสอบพบว่าเกี่ยวข้องกับการทำผิดจะต้องถูกรับการตรวจสอบประมาณนี้ เลยเป็นประเด็นว่าทำให้ตกใจกลัวก่อนแล้วจึงมีการส่งต่อให้กับบุคคลที่แอบอ้างเป็นทอด ๆ อย่างรวดเร็ว หมายความว่าเมื่อเหยื่อหลงเชื่อก็จะรีบตามติดต่อให้มีการโอนเงินครั้งแรกให้เร็ว ด้วยการโอนเงินจำนวนเงินไม่มากนัก เมื่อเหยื่ออยากจะได้คืนก็จะมีกระบวนการต้องเสียธรรมเนียมเพิ่ม คนที่เสียเงินไปแล้วก็อยากได้คืนก็ให้ลงเงินเพิ่มไปอีกหน่อย เลยกลายเป็นว่ายิ่งเยอะ จนสุดท้ายคือไม่โอนถึงจะรู้ว่าถูกหลอกจากแก๊งคอลเซ็นเตอร์แล้ว”*
>
> (ตำรวจไซเบอร์ 5, สัมภาษณ์, 17 สิงหาคม 2567)

> *“ตอนนั้นด้วยความรีบร้อนและกังวล ผมเปิดลิงก์ที่ส่งมาในทันที หลังจากนั้นไม่นานผมก็เริ่มได้รับข้อความแจ้งเตือนจากแอพธนาคารว่าเงินในบัญชีกำลังถูกโอนออก ตอนนั้นผมรู้สึกตกใจมาก”*
>
> (ชัยชนะ (นามสมมติ), สัมภาษณ์, 13 สิงหาคม 2567)

> *“คนร้ายมักใช้ระยะเวลาที่บีบคั้นเหยื่อในการให้เหยื่อตัดสินใจ ไม่ว่าจะเป็นการให้เวลาเพียงน้อยนิด หรือข่มขู่ว่าจะดำเนินคดี หรืออ้างถึงความลับทางราชการ”*
>
> (ตำรวจไซเบอร์ 6, สัมภาษณ์, 26 สิงหาคม 2567)

> *“ถ้าไม่ทำตามอาจจะเป็นปัญหาทางกฎหมายใหญ่โต เพราะพี่ก็ไม่เคยมีปัญหาทางกฎหมายมาก่อน พอได้ยินเรื่องอย่างนี้ก็กลัวนะ เขาพูดเหมือนรู้ทุกอย่างเกี่ยวกับบัญชี*

*ของพี่ รู้แม้กระทั่งยอดเงินในบัญชี มันทำให้พี่รู้สึกว่าเขาต้องเป็นเจ้าหน้าที่จริง ๆ ตอนนั้นพี่ก็ไม่อยากเดือดร้อนก็เลยทำตามที่เขาบอก”*

(มาลี (นามสมมติ), สัมภาษณ์, 15 สิงหาคม 2567)

*“ตอนนั้นด้วยความกลัวที่จะสูญเสียที่ดิน เลยตัดสินใจโอนเงินไปยังบัญชีที่ได้รับคำแนะนำ แม้ว่าจะมีข้อสงสัยนะแต่ก็เลือกที่จะเชื่อ”*

(เพลงรัก (นามสมมติ), สัมภาษณ์, 27 สิงหาคม 2567)

2. ปัจจัยด้านความโลภ เป็นสิ่งที่ช่วยผลักดันให้แก๊งคอลเซ็นเตอร์สามารถเข้าถึงเหยื่อได้ง่ายขึ้น เนื่องจากแก๊งคอลเซ็นเตอร์มักใช้กลยุทธ์การตลาดที่น่าสนใจ และทำให้ผู้คนรู้สึกว่าหากไม่เข้าร่วมจะพลาดโอกาสที่ดี ดังคำสัมภาษณ์ที่ว่า

*“ถ้าจะพูดถึงหลักพุทธศาสนานะ เขาใช้กิเลสของคน รัก โลภ โกรธ หลงมาจับพฤติกรรมของคน โดยเฉพาะเนี่ยเขามีทุนเยอะเขาก็จะซื้อข้อมูลแล้วก็เอาข้อมูลตรงนี้มาศึกษาพฤติกรรมว่าเราชอบอะไร จุดอ่อนของเราอะไร รัก โลภ โกรธ หลงเนี่ย”*

(ตำรวจไซเบอร์ 1, สัมภาษณ์, 14 สิงหาคม 2567)

*“สิ่งที่เราจะถูกหลอกลวงเนี่ยก็เพราะว่าเรื่องของความโลภ แอบหลอกให้ได้เงินพวกนี้นะครับ แล้วก็หลอกให้เกิดความกลัว ตลอดจนให้เกิดความรัก ความหลงประมาณนี้ ซึ่งตอนเนี้ยมันเป็นเรื่องของพื้นฐานจิตใจของคนนะครับที่ที่ทำไมถึงยังถูกหลอกซ้ำแล้วซ้ำอีก ในกรณีของการกระทำความผิดซ้ำของผู้เสียหายที่ไปดูแล้วก็สาเหตุเกี่ยวกับเรื่องของจิตใจเรานี่แหละ ถ้าเราไม่อยากได้ของคนอื่น เราไม่หลงเชื่อในสิ่งที่เขาให้เรามา ผมว่ามันก็เป็นแนวทางหนึ่งในการป้องกันได้”*

(ตำรวจไซเบอร์ 2, สัมภาษณ์, 14 สิงหาคม 2567)

*“เมื่อเศรษฐกิจไม่ดีบวกกับคนมีความโลภ มิจฉาชีพเขาก็ต้องการหลอก เพราะเมื่อคนต้องการของถูกก็เลยซื้อเพราะหลงเชื่อว่าของดีจริง ของราคาถูกกว่าท้องตลาดจึงโอนเงินซื้อไป แต่ก็ไม่ได้ของส่วนใหญ่เป็นประมาณนี้”*

(ตำรวจไซเบอร์ 4, สัมภาษณ์, 17 สิงหาคม 2567)

*“โอกาสที่ดีเกินกว่าจะปล่อยผ่านไป และด้วยราคาที่ลดลงเกือบครึ่งจากปกติ ทำให้ตัดสินใจสั่งซื้อมือถือยี่ห้อไอโฟนหนึ่งเครื่องในราคา 25,000 บาท ที่โดยปกติโทรศัพท์มือถือรุ่นนี้จะอยู่ที่ประมาณราคา 30,000 กว่าบาท แต่พอเห็นราคาที่ร้านลดมาถึงขนาดนี้ก็เป็นสิ่งที่น่าสนใจ”*

(ลลิตตา (นามสมมติ), สัมภาษณ์, 18 สิงหาคม 2567)

*“คนร้ายมักอาศัย ความกลัว และความโลภของเหยื่อในการหาโอกาสต่อไปในการหลอกลวงเพื่อให้ได้ทรัพย์สินจากเหยื่อ ซึ่งหากจะตัดปัจจัยส่วนนี้ออกไปเพื่อไม่ให้มีการเกิดอาชญากรรมขึ้นนั้น”*

(ตำรวจไซเบอร์ 6, สัมภาษณ์, 26 สิงหาคม 2567)

*“กระเป๋าแบรนด์ดังที่อยากได้มานาน ราคาแค่ 3,990 บาท ซึ่งปกติราคาจะสูงกว่านั้นหลายเท่า ก็คิดในใจว่าราคาถูกขนาดนี้ ต้องรีบซื้อแล้วล่ะ เลยกดสั่งซื้อทันที ก่อนจะรีบโอนเงินอย่างรวดเร็วเพราะกลัวว่าของจะหมด”*

(สุดสายใจ (นามสมมติ), สัมภาษณ์, 30 สิงหาคม 2567)

3. ปัจจัยด้านความรู้ไม่เท่าทันการหลอกลวง ผู้หลอกลวงพยายามเปลี่ยนรูปแบบและวิธีการในการหลอกลวง ทำให้เหยื่อเชื่อว่าการหลอกลวงนั้นเป็นเรื่องจริง ดังนั้นจึงทำให้ตกเป็นเหยื่อของการถูกหลอกลวงได้ง่าย ดังคำสัมภาษณ์ที่ว่า

*“ปลายสายเสียงเป็นผู้หญิงคนนั้นแนะนำตัวว่าเป็นหลานสาว พูดอย่างรีบร้อนว่ามือถือพัง ต้องการยืมเงินตอนนี้เลยเพราะจะไปซื้อเครื่องใหม่พี่ก็แปลกใจ แต่ตอนนั้นไม่ได้คิดอะไรมากเพราะฟังจากเสียงก็คุ้นมากเหมือนหลานสาวคนสนิท ด้วยความเป็นห่วงกลัวหลานลำบากพี่เลยรีบโอนเงินไปให้ตามคำขอ”*

(มนชิดา (นามสมมติ), สัมภาษณ์, 13 สิงหาคม 2567)

*“เหยื่อเป้าหมายตอนนี้ก็ผู้สูงอายุที่อยู่ตามบ้านโดยลำพังและไม่ค่อยสนใจเทคโนโลยีและปัจจัยที่ทำให้เขาถูกหลอกลวงนี่ก็คือเพราะเขารู้รู้ไม่เท่าทัน รวมถึงคนเกษียณที่มีเงินเกษียณ”*

(ตำรวจไซเบอร์ 3, สัมภาษณ์, 16 สิงหาคม 2567)

*“เริ่มแรกโทรมาแอบอ้างว่าเป็นคนรู้จัก ถ้าเราเผลอทายโดยการเรียกชื่อ เขาก็จะสวมรอยเป็น แล้วก็บอกว่าเปลี่ยนเบอร์โทรศัพท์นะแอดไลน์ใหม่ โปรไฟล์ไลน์เป็นแบบนี้นะ และทำทีเป็นยืมเงิน หรือไม่ก็บอกว่ารถชน อุบัติเหตุด่วนจำเป็นต้องใช้เงิน การหลอกลวงแบบนี้ยอดเงินจะไม่สูง แต่ถ้าคอลเซ็นเตอร์ที่ยอดสูง ๆ จะเป็นพวกที่เข้าควบคุมเครื่อง หรือหลอกให้กลัวแล้วโอนไปตรวจสอบ ซึ่งถ้าเรารู้ไม่เท่าทันก็จะโดนพวกนี้หลอกง่าย ๆ เลย”*

(ตำรวจไซเบอร์ 5, สัมภาษณ์, 17 สิงหาคม 2567)

*“พี่คนนั้นพูดด้วยน้ำเสียงที่สุภาพและเป็นทางการ หนูก็เริ่มคิดว่าน่าจะเป็นเจ้าหน้าที่จริง ๆ เพราะเขาพูดข้อมูลเกี่ยวกับบัญชีของหนูได้ละเอียด และบอกว่าธนาคารจะส่ง SMS เพื่อยืนยันตัวตนอีกครั้ง หนูเลยคิดว่าไม่น่าจะมีปัญหาอะไร หนูก็เลยยอมให้ข้อมูลไปทั้งเลขบัตรประชาชนและเลขบัญชี โดยไม่ได้คิดอะไรมาก”*

(พบรัก (นามสมมติ), สัมภาษณ์, 23 สิงหาคม 2567)

*“เขาบอกว่าเป็นเจ้าหน้าที่จากการไฟฟ้า และบอกว่าบ้านผมค้างชำระค่าไฟฟ้าที่สูงผิดปกติ พูดด้วยน้ำเสียงจริงจังเลยนะ ค้างจำนวนเงิน 5,000 บาท ไม่ชำระภายในวันนี้จะมีการตัดไฟและดำเนินการตามกฎหมาย”*

(สุเมธ (นามสมมติ), สัมภาษณ์, 27 สิงหาคม 2567)

4. ปัจจัยด้านการใช้เทคโนโลยีและอินเตอร์เน็ต คอลเซ็นเตอร์ใช้วิธีการสร้างเว็บไซต์ปลอมที่มีลักษณะคล้ายคลึงกับเว็บไซต์จริง เพื่อหลอกลวงผู้ใช้ให้สมัครสมาชิกหรือให้ข้อมูลทางการเงิน โดยมักจะแอบอ้างเป็นบริษัทหรือหน่วยงานที่มีชื่อเสียง เพื่อให้ดูน่าเชื่อถือ เช่น ธนาคาร หรือหน่วยงานรัฐบาล ทำให้ผู้คนตกใจและให้ข้อมูลส่วนตัว ดังคำสัมภาษณ์ที่ว่า

*“พอเรากดลิงก์มันก็เป็นหน้าเว็บของหน่วยงานของรัฐที่มิจฉาชีพสร้างขึ้นมา หลังจากนั้นเขาจะให้กรอกข้อมูลส่วนบุคคลเข้าไปคนก็จะหลงเชื่อคิดว่าหน่วยงานของรัฐจริง ๆ ก็จะกรอกข้อมูลส่วนบุคคลทั้งหมด แม้กระทั่งบัญชีที่มีอยู่ โดยอ้างเหตุผลที่น่าเชื่อถือ”*

(ตำรวจไซเบอร์ 3, สัมภาษณ์, 16 สิงหาคม 2567)

*“ช่วงนั้นเลยเป็นข่าวว่าร้านค้าโวยเนื่องจากมีการเรียกเก็บภาษี มิจฉาชีพจึงแปลงรูปแบบว่าตนก็เป็นสรรพากร ผู้ที่ตกเป็นเหยื่อจะเป็นร้านค้าที่มีการลงทะเบียนคนละครึ่งไว้ โดยจะโทรไปก็หลอกว่าเราตรวจสอบว่าเหยื่อต้องเสียเงินลงทะเบียนอาจจะเสียภาษีเพิ่ม แต่ถ้าอยากจะลดการเสียภาษีต้องติดต่อเจ้าหน้าที่ทำประเมินใหม่แล้วก็มีการโอนเงินเพื่อชดใช้หรือวิ่งเต้นก็จะหลอกไปรูปแบบนี้”*

(ตำรวจไซเบอร์ 5, สัมภาษณ์, 17 สิงหาคม 2567)

*“ให้ผมแอดไลน์มาได้เลยเพื่อที่จะคุยกับทางคุณตำรวจได้สะดวก พอผมแอดไลน์ไปก็โดนเชิญเข้ากลุ่มชื่อ ปปง. และในกลุ่มก็มีเจ้าหน้าที่บอกกับผมว่าทางหน่วยงานต้องตรวจสอบทรัพย์สินทั้งหมดของผม โดยที่ผมจะต้องโอนเงินในบัญชีของผมทั้งหมด*

*ไปที่บัญชีของเจ้าหน้าที่ทั้งหมดเพื่อตรวจสอบเส้นทางการเงินทั้งหมด*"

(เชิดชัย (นามสมมติ), สัมภาษณ์, 17 สิงหาคม 2567)

*"ตอนบ่ายก็มีสายวิดีโอคอลจากตำรวจจริง ๆ ซึ่งตอนที่วิดีโอคอลคุยกันตำรวจคนนั้นก็ใช้ทั้งคำขู่คำหว่านล้อมกดดันให้ฉันรู้สึกกลัว ฉันเลยเชื่อเข้าไปอีก"*

(กัญญารัตน์ (นามสมมติ), สัมภาษณ์, 20 สิงหาคม 2567)

**ข้อเสนอแนะการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์**

การป้องกันไม่ให้ตกเป็นเหยื่อของแก๊งคอลเซ็นเตอร์จำเป็นต้องอาศัยความระมัดระวังและการรับรู้ถึงกลยุทธ์ที่มิจฉาชีพมักใช้ในการหลอกลวง จากการศึกษาผู้วิจัยสามารถสรุปเป็นแนวทางแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ทั้งหมด 3 ประเด็นที่ได้มาจากการวิเคราะห์จากข้อมูลที่สัมภาษณ์ และได้ข้อเสนอแนะจากผู้ให้คำสัมภาษณ์ประกอบกันดังนี้

1. ส่งเสริมการประชาสัมพันธ์เพื่อป้องกันปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ โดยให้หน่วยงานที่เกี่ยวข้องจำเป็นต้องร่วมมือกันในการเผยแพร่ข้อมูลที่ถูกต้องและเป็นประโยชน์เกี่ยวกับความเสี่ยงและวิธีการป้องกัน และหน่วยอาจจะมีการจัดอบรมให้ความรู้หรือเวิร์กช็อปสำหรับประชาชน เพื่อให้ความรู้เกี่ยวกับการป้องกันการหลอกลวงทางไซเบอร์ ซึ่งการจัดอบรมให้ความรู้เกี่ยวกับการป้องกันการหลอกลวงทางไซเบอร์ไม่เพียงแต่ช่วยเสริมสร้างความรู้ให้กับประชาชน แต่ยังส่งผลให้ประชาชนความตระหนักรู้และสามารถป้องกันตนเองได้อย่างมีประสิทธิภาพในยุคดิจิทัลที่เต็มไปด้วยความเสี่ยงและภัยคุกคามจากการหลอกลวงทางไซเบอร์ ดังคำสัมภาษณ์ที่ว่า

*"เรื่องของรูปแบบอาชญากรรมที่จะต้องประชาสัมพันธ์ให้กับพี่น้องประชาชนได้รับทราบทั่วถึงกันว่า ในเทรนด์ปัจจุบันรูปแบบการหลอกลวงไปในรูปแบบไหนอย่างไรซึ่งเราจะได้รู้เท่าทัน แล้วก็จะได้ลดการเกิดอีกนะครับ"*

(ตำรวจไซเบอร์ 2, สัมภาษณ์, 14 สิงหาคม 2567)

*"ต้องประชาสัมพันธ์ให้ให้มากกว่านี้ให้ทุกคนทราบ โดยเฉพาะคนสูงอายุให้รู้เท่าทันกลลวงของมิจฉาชีพ เพราะว่าแก๊งคอลเซ็นเตอร์พยายามที่จะพัฒนาเปลี่ยนรูปแบบไปเรื่อย ๆ เพื่อให้ทันกับเหตุการณ์ปัจจุบัน จึงต้องประชาสัมพันธ์ก่อนที่จะโดนหลอกเพิ่มขึ้น"*

(ตำรวจไซเบอร์ 3, สัมภาษณ์, 16 สิงหาคม 2567)

*“สร้างการรับรู้ แต่ก็ต้องเข้าใจว่าแต่การหลอกลวงมีการเปลี่ยนรูปแบบตามยุคสมัย โดยอ้างอิงกับสิ่งที่มีจริงในสังคมจึงทำให้เหยื่อหลงเชื่อได้ง่าย ถามว่าการจะป้องกันหรือการที่จะช่วยเหลือเหยื่อได้อย่างแรก คือ การแจ้งเตือน ทั้งเป็นคลิปสั้นลงเพจประชาสัมพันธ์ แต่ต้องยอมรับว่าของพวกนี้ไม่สามารถทั่วถึงได้ทุกคนโดยเร็ว ถ้ารูปแบบเก่า ๆ อย่างเช่น บอกว่าส่งพัสดุมาหรือหลอกเป็นเพื่อน หลัง ๆ พอคนโดนเยอะ ๆ ก็มีการประกาศสัมพันธ์ไป คนก็จะไม่ตกเป็นเหยื่อ แต่เขาก็จะเปลี่ยนรูปแบบไป จนบางครั้งกว่าจะตามทันรูปแบบใหม่ประชาชนหลายคนก็ตกเป็นเหยื่อแล้ว จึงจำเป็นต้องประชาสัมพันธ์อย่างต่อเนื่องด้วย”*

(ตำรวจไซเบอร์ 5, สัมภาษณ์, 17 สิงหาคม 2567)

2. การส่งเสริมการควบคุมอารมณ์และตัดสินใจอย่างมีสติก่อนกระทำการใด ๆ เนื่องจากมิจฉาชีพมักสร้างความรู้สึกเร่งด่วนให้เหยื่อตัดสินใจโดยไม่ทันคิด เช่น การข่มขู่ว่าจะถูกดำเนินคดีทันที หากเผชิญกับสถานการณ์เช่นนี้ควรตั้งสติและไม่รีบดำเนินการใด ๆ ควรสอบถามข้อมูลอย่างละเอียดและใช้เวลาตรวจสอบความถูกต้อง ดังคำสัมภาษณ์ที่ว่า

*“ผมก็เชื่อว่าทุก ๆ ท่านมีโทรศัพท์มือถือในโลกปัจจุบัน เคยถูกมิจฉาชีพ ส่ง SMS หรือโทรศัพท์มาหา ผมเชื่อว่าจากทุกคนโดนบ่อยครั้ง แต่ถ้าเรายึดมั่นในสิ่งที่เรามีอยู่ 1) ไม่อยากได้ของคนอื่น 2) ไม่เชื่อในสิ่งที่เขาให้ข้อมูลมาหรือเรามีการเช็คข้อมูลก่อนที่จะตัดสินใจทำอะไรลงไปครับ อันเนี้ยผมเชื่อว่ามันก็เป็นส่วนหนึ่งในการที่จะป้องกันตนไม่ให้ตกหลุมพรางของแก๊งคอลเซ็นเตอร์ได้ครับ”*

(ตำรวจไซเบอร์ 2, สัมภาษณ์, 14 สิงหาคม 2567)

*“เหตุการณ์ครั้งนี้ถือว่าเป็นบทเรียนให้พี่ได้อย่างดีเลยว่า อย่าไว้ใจเบอร์แปลก เพราะต่อให้เราฟังแล้วเป็นน้ำเสียงที่คุ้นเคยมันก็ไม่มีอะไรมาการันตีได้ว่าปลายสายนั้นจะเป็นญาติหรือคนที่เราสนิทและไว้ใจ”*

(มนชิดา (นามสมมติ), สัมภาษณ์, 13 สิงหาคม 2567)

*“ที่ดีที่สุดคือ ต้องตระหนักรู้ ไม่เชื่อ ไม่โอน อะไรที่ผ่านทางโซเชียลทางที่ไม่เห็นตัวก็ต้องพึงระวังหากคิดจะต้องโอนอะไร และที่สำคัญหลายอย่าง ๆ เลย คือ ไม่โลภ บางคนก็เห็นแก่ผลประโยชน์ที่ได้ผลตอบแทนสูงก็โลภ มีหลายรูปแบบแล้วแต่รูปแบบที่จะเจอ”*

(ตำรวจไซเบอร์ 5, สัมภาษณ์, 17 สิงหาคม 2567)

*“ความประมาทเพียงแค่รับสายจากเบอร์แปลก กลายเป็นประสบการณ์เจ็บปวดที่ต้องเสียเงินหลักแสนไปโดยไม่สามารถทำอะไรได้ครับ”*

(ชัยชนะ (นามสมมติ), สัมภาษณ์, 13 สิงหาคม 2567)

*“หากประชาชนมีความรู้ไม่ว่าจะเป็นเหตุบ้านการเมือง หรือการเตือนภัยต่างๆ ความรู้เกี่ยวกับการลงทุน ด้านการเงิน ซึ่งการลงทุนใด ๆ ก็แล้วแต่ ไม่ได้มีอะไรในโลกนี้ที่ได้มาโดยง่าย แม้ว่าคนที่รวยที่สุดในโลกก็ยังใช้ระยะเวลาหลายสิบปีในการก่อร่างสร้างตัวและทรัพย์สิน ดังนั้นจึงยากที่จะมีการลงทุนใดๆที่มีผลตอบแทนมหาศาลเช่นดังที่คนร้ายมักใช้ในการหลอกลวงเหยื่อ ซึ่งหากประชาชนศึกษาหาความรู้มากขึ้นก็จะทำให้ประชาชนหรือเหยื่อที่ถูกคนร้ายหลอกลวงน้อยลง ฉะนั้นก่อนเชื่ออะไรนั้นจะต้องตรวจสอบแหล่งที่มาที่ไป และตรวจสอบหาความชัดเจนก่อน ไม่ว่าปลายสายเป็นผู้ใด ควรสอบถาม หาข้อมูล ซึ่งหากเป็นหน่วยงานราชการจริงก็จะสามารถให้ข้อมูลหรือเปิดเผยข้อมูลที่จำเป็นกับทางเหยื่อได้ รวมทั้งควรตรวจสอบข้อมูลจากหน่วยงานกลาง หรือส่วนราชการที่เชื่อถือได้ก่อนเสมอเพื่อไม่ให้ตกหลุมพรางจากคนร้ายได้”*

(ตำรวจไซเบอร์ 6, สัมภาษณ์, 26 สิงหาคม 2567)

*“เหตุการณ์ครั้งนี้ทำให้ได้เรียนรู้บทเรียนสำคัญเกี่ยวกับการซื้อของออนไลน์ว่าไม่ควรเชื่อราคาถูกจนเกินไป และต้องตรวจสอบความน่าเชื่อถือของร้านค้าให้ดี”*

(สุดสายใจ (นามสมมติ), สัมภาษณ์, 30 สิงหาคม 2567)

3. การป้องกันและปราบปรามการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ โดยหน่วยงานที่เกี่ยวข้องกับการปราบปรามอาชญกรรมทางไซเบอร์ควรจะมีการร่วมมือกันระหว่างหน่วยงานในสภาพแวดล้อมที่มีการเปลี่ยนแปลงรวดเร็ว รวมไปถึงการบูรณาการการทำงานร่วมกันระหว่างผู้เสียหาย ธนาคาร และเจ้าหน้าที่ตำรวจ เพื่อเป็นการประสานงานกันในการแก้ปัญหาให้รวดเร็วขึ้น ดังคำสัมภาษณ์ที่ว่า

*“ที่ผ่านมาที่จะมีการล้มเสาการสื่อสารของแก๊งคอลเซ็นเตอร์นี่แหละ แล้วก็ให้เจ้าหน้าที่ธนาคารต่าง ๆ เนี่ยมาคุยกันว่า ถ้ามันมีการเงินที่โอนผิดปกติให้ระงับธุรกรรม รวมถึงให้หน่วยงานที่เกี่ยวข้องเนี่ยมาร่วมประชุม ซึ่งมีตำรวจเนี่ยเป็นตัวกลางคอยประสาน ต่อไปก็อาจจะดีขึ้นได้ และที่สำคัญรัฐบาลก็ต้องเอาจริงเอาจังในเรื่องของการออกกฎหมาย ซึ่งเมื่อเอาจริงเอาจังแล้วก็มีกฎหมายให้เจ้าหน้าที่ได้เข้มข้นอย่างเนี้ยมันก็จะทำได้ เพราะว่าเราไม่เหมือนบางประเทศที่ตำรวจสามารถ*

*จะไปดูข้อมูลทุกได้ทุกจุดได้ ควบคุมเซ็นเตอร์ได้หมดเลยธนาคาร มือถือ อะไรต่ออะไรเนี่ย ซึ่งข้อมูลพวกนี้แป๊บเดียวก็สามารถลิงก์ได้ เราก็จะตามจับได้ง่ายขึ้น แต่ตอนนี้มันยังไม่ได้ถึงตรงนั้นถ้าในอนาคตทำได้เนี่ยมันจะดีขึ้น"*

(ตำรวจไซเบอร์ 1, สัมภาษณ์, 14 สิงหาคม 2567)

*"แนวทางตอนนี้ก็มีโครงการของระบบไซเบอร์ก็มีโครงการชื่อว่าวัคซีนไซเบอร์ จะเป็นการออกบรรยายตามสถานที่ต่าง ๆ โดยกล่าวถึงวิธีการรู้ให้เท่าทันมิจฉาชีพ แล้วก็โปรโมทโฆษณาป้องกันเป็นโปสเตอร์"*

(ตำรวจไซเบอร์ 3, สัมภาษณ์, 16 สิงหาคม 2567)

*"การเปิดบัญชีควรมีมาตรการที่เข้มงวดกว่านี้ เดี๋ยวนี้มันเปิดออนไลน์ง่าย แล้วมีการขายบัญชีม้าง่ายเช่นเดียวกัน จึงคิดว่าถ้าใครเปิดบัญชีก็ต้องมาแสดงตัวตนที่ธนาคาร แล้วก็จำกัดว่าสามารถเปิดได้กี่บัญชีแค่นั้นเอง และเปิดเพื่อนำเอาไปทำอะไรก็ต้องตรวจสอบ แล้วก็ธนาคารจะรู้ว่าบัญชีนี้มีการเคลื่อนไหวสำหรับมีการโอนเข้าโอนออก ถ้าเป็นธุรกรรมผิดปกติจะมีเงินเข้าและออกทันที ซึ่งอันนี้คือบัญชีทีม้าของแก๊งคอลเซ็นเตอร์ ธนาคารจึงควรระงับการโอนบางอย่างโดยให้อำนาจทางกฎหมายแก่ธนาคารเพื่อระงับการโอนไว้ชั่วคราว และให้เจ้าของบัญชีมาชี้แจงรายได้จะสามารถช่วยได้"*

(ตำรวจไซเบอร์ 4, สัมภาษณ์, 17 สิงหาคม 2567)

*"ต้องสร้างการเรียนรู้ให้มากขึ้น แล้วก็ต้องร่วมมือระหว่างรัฐกับเอกชนในการประชาสัมพันธ์สื่อต่าง ๆ ไม่ให้คนตกเป็นเหยื่อ ต่อมากฎหมายก็ต้องเท่าทัน เช่นตอนนี้หลายธนาคารเริ่มปิดโมบายแบงก์กิ้งเพราะว่ามันสะดวก แต่ตามไม่ทันหากเกิดความเสียหายเพราะเขามีส่วนได้รับผลกระทบด้วย ไม่แน่อาจจะต้องย้อนกลับไปใช้วิธีเดิม ๆ ก่อนหน้า"*

(ตำรวจไซเบอร์ 5, สัมภาษณ์, 17 สิงหาคม 2567)

*"ปัจจุบันทางสำนักงานตำรวจแห่งชาติได้จัดให้มีการให้ความรู้ในรูปแบบต่างๆ ทั้งสื่อสังคมออนไลน์ หรือไม่ว่าจะเป็นการจัดอบรมให้ความรู้ทางด้านอาชญากรรมในรูปแบบต่างๆในแต่ละมิติ เพื่อเพิ่มวัคซีนในการป้องกันคนร้าย ที่จะมาในรูปแบบต่างๆ ซึ่งสามารถเข้าถึงข้อมูลและความรู้เพื่อป้องกันเหตุการณ์ดังกล่าวได้จาก www.thaipoliceonline.go.th. หรือ โทรสอบถาม 1441 ตลอด 24 ชั่วโมง"*

(ตำรวจไซเบอร์ 6, สัมภาษณ์, 26 สิงหาคม 2567)

# บทที่ 5
# สรุปอภิปรายผลและข้อเสนอแนะ

การวิจัยเรื่อง การหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ มีวัตถุประสงค์เพื่อศึกษาถึงการกระทำอันเป็นลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์ เพื่อศึกษาถึงปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ และเพื่อเสนอแนะการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยการสัมภาษณ์เชิงลึก (In-depth Interview) กับผู้ให้ข้อมูลสำคัญ โดยวิธีการเลือกแบบเจาะจง (Purposive Sampling) ผู้ให้ข้อมูลเป็นผู้สมัครใจให้ข้อมูล ผู้ให้ข้อมูลสำคัญจำนวน 18 คน แบ่งเป็น 2 ส่วน คือ กลุ่มประชาชนที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์จำนวน 12 คน และเจ้าหน้าที่ที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกันประชาชนจากการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ จำนวน 6 คน ซึ่งการนำเสนอผลการศึกษาผู้วิจัยใช้กระบวนการวิเคราะห์ข้อมูลจากการถ่ายทอดเรื่องราว ประสบการณ์ของผู้ที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ และเจ้าหน้าที่ที่ให้การช่วยเหลือหรือป้องกันประชาชนจากการหลอกลวงทางไซเบอร์ กรณีแก๊งคอลเซ็นเตอร์ โดยสรุปผลการศึกษาและข้อเสนอแนะของการวิจัย ดังนี้

## สรุปผลการวิจัย

ผลการวิจัยแบ่งกลุ่มการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์ได้ 2 รูปแบบ คือ

1. การหลอกลวงทางโทรศัพท์
2. การหลอกขายสินค้า

สรุปผลการวิจัยตามวัตถุประสงค์ดังนี้

จากการศึกษาการหลอกลวงของแก๊งคอลเซ็นเตอร์ทั้ง 2 รูปแบบนั้นมีความเหมือนกันในการมุ่งหวังให้เหยื่อเปิดเผยข้อมูลหรือทำธุรกรรม แต่แตกต่างกันในวิธีการติดต่อ รูปแบบการหลอกลวง และประเภทข้อมูลที่ต้องการ ดังนี้

**1. ลักษณะการหลอกลวงทางไซเบอร์ของแก๊งคอลเซ็นเตอร์**

**รูปแบบการหลอกลวงทางโทรศัพท์** เป็นรูปแบบที่พบได้บ่อยในปัจจุบัน ซึ่งมิจฉาชีพมักใช้วิธีการแอบอ้างเป็นเจ้าหน้าที่รัฐ หรือคนรู้จัก เพื่อให้เหยื่อเกิดความหลงเชื่อภายในระยะเวลาในการให้ตัดสินใจที่จำกัดและภายใต้ความรู้สึกที่เชื่อว่าการหลอกลวงนั้นเป็นของจริง ส่งผลให้นำไปสู่

การตัดสินใจที่ผิดพลาดและตกเป็นเหยื่อได้ง่าย เมื่อเหยื่อหลงเชื่อและปฏิบัติตามคำสั่ง มิจฉาชีพจะหายไปพร้อมกับเงิน ส่งผลให้เกิดความสูญเสียเงินจำนวนมาก

**รูปแบบการหลอกขายสินค้า** มิจฉาชีพมักใช้แพลตฟอร์มโซเชียลมีเดีย เพื่อโฆษณาสินค้าในรูปแบบของโพสต์หรือการส่งข้อความส่วนตัว โดยมีการใช้ภาพถ่ายสินค้าที่สวยงามและราคาโปรโมชั่นดึงดูดให้ผู้คนคลิกเข้าไปสั่งซื้อ แต่เมื่อทำธุรกรรมไปให้อีกฝ่ายเสร็จสิ้นกลับไม่ได้รับสินค้า หรือได้รับสินค้าไม่ตามที่ต้องการ นอกจากจะเป็นการสูญเสียเงินแล้วยังทำให้เกิดความผิดหวังและสูญเสียความเชื่อมั่นในตลาดอีกด้วย

**2. ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์**

จากการศึกษาผู้วิจัยสามารถค้นพบลักษณะการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ โดยแบ่งออกเป็นทั้งหมด 2 รูปแบบ คือ การหลอกลวงทางโทรศัพท์ และการหลอกขายสินค้า ซึ่งทั้ง 2 รูปแบบนั้นมีปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ ดังนี้

**ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางโทรศัพท์**

1. ปัจจัยด้านความกลัว ผู้ตกเป็นเหยื่อส่วนใหญ่เมื่อถูกแก๊งคอลเซ็นเตอร์ใช้วิธีการโทรสุ่มมาหลอกลวงมีความตกใจกลัว เนื่องจากผู้หลอกลวงใช้วิธีการแอบอ้างเป็นบุคคลหรือหน่วยงานที่น่าเชื่อถือ เช่น การหลอกลวงว่าพัสดุมีสิ่งต้องสงสัยผิดกฎหมาย การหลอกลวงว่าบัญชีธนาคารมีการทำธุรกรรมที่น่าสงสัย โดยมีระยะเวลาอันสั้นในการตัดสินใจ ส่งผลให้เกิดการตัดสินใจที่ผิดพลาด นำไปสู่ความเสียหายทางการเงิน

2. ปัจจัยด้านการรู้ไม่เท่าทันการหลอกลวง ผู้ตกเป็นเหยื่อรู้ไม่เท่าทันกลโกงของผู้หลอกลวง เนื่องจากผู้หลอกลวงพยายามเปลี่ยนรูปแบบและวิธีการในการหลอกลวงเพื่อให้ทันกับสถานการณ์ปัจจุบัน และผู้ตกเป็นเหยื่อบางรายอาจขาดการเข้าถึงข้อมูลเกี่ยวกับการหลอกลวงที่เกิดขึ้นในปัจจุบัน หรือขาดการศึกษาเกี่ยวกับวิธีป้องกันตนเองจากการหลอกลวง ทำให้ไม่สามารถแยกแยะความเสี่ยงได้

3. ปัจจัยด้านการใช้เทคโนโลยีและอินเตอร์เน็ต ข้อมูลส่วนตัวของผู้คนมักจะถูกเผยแพร่ทางออนไลน์ โดยเฉพาะในโซเชียลมีเดีย ทำให้มิจฉาชีพสามารถนำข้อมูลเหล่านี้ไปใช้ในการหลอกลวงหรือสร้างความน่าเชื่อถือ นอกจากนี้ผู้ตกเป็นเหยื่อบางรายอาจไม่คุ้นเคยกับการใช้เทคโนโลยีหรืออินเทอร์เน็ต ทำให้ไม่สามารถแยกแยะหรือระบุการหลอกลวงได้ เช่น ไม่รู้วิธีตรวจสอบความน่าเชื่อถือของแหล่งข้อมูล

**ปัจจัยที่ทำให้ประชาชนถูกหลอกลวงขายสินค้า**

1. ปัจจัยด้านความโลภ ลักษณะการหลอกลวงเหยื่องโดยอาศัยความโลภโดยใช้วิธีการดึงดูดความสนใจของผู้ที่มีความโลภและต้องการประหยัดเงิน โดยจะเน้นไปที่สินค้าที่มีความต้องการสูง เช่น เสื้อผ้า กระเป๋าแบรนด์ดัง หรืออุปกรณ์อิเล็กทรอนิกส์

2. ปัจจัยด้านการรู้ไม่เท่าทันการหลอกลวง ผู้ตกเป็นเหยื่อส่วนใหญ่มักมีความเชื่อมั่นในเทคโนโลยีและแพลตฟอร์มออนไลน์ ซึ่งอาจนำไปสู่การละเลยในการตรวจสอบความน่าเชื่อถือและไม่ระมัดระวังในการให้ข้อมูลส่วนตัวหรือทำการซื้อขาย มิจฉาชีพมักใช้เทคนิคต่าง ๆ เพื่อสร้างความน่าเชื่อถือ เช่น การใช้ภาพถ่ายหรือวิดีโอที่ดูมืออาชีพ การสร้างเว็บไซต์ที่มีลักษณะคล้ายบริษัทจริง หรือการใช้รีวิวปลอมจากผู้ที่ดูเหมือนมีประสบการณ์ที่ดี ทำให้ผู้คนเชื่อใจง่ายขึ้น

3. ปัจจัยด้านการใช้เทคโนโลยีและอินเตอร์เน็ต การใช้เทคโนโลยีสมาร์ตโฟนในการดำเนินชีวิตประจำวันนั้นมีความเสี่ยงสูงที่จะตกเป็นเหยื่อของการหลอกลวงออนไลน์ เนื่องจากมิจฉาชีพมีการใช้ช่องทางออนไลน์เพื่อเข้าถึงเหยื่อในรูปแบบต่าง ๆ เช่น การนำเสนอการส่งเสริมการขายโดยการจัดโปรโมชั่นที่น่าสนใจ

**3. แนวทางการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์**

จากการศึกษา ผู้วิจัยสามารถสรุปเป็นแนวทางแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ทั้งหมด 3 ประเด็น ได้มาจากการวิเคราะห์จากข้อมูลที่สัมภาษณ์ และได้ข้อเสนอแนะจากผู้ให้คำสัมภาษณ์ประกอบกัน ดังนี้

1. ส่งเสริมการประชาสัมพันธ์ข้อมูลข่าวสารเพื่อป้องกันการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์อย่างต่อเนื่อง และเพิ่มการมีส่วนร่วม เพื่อให้หน่วยงานที่เกี่ยวข้องร่วมกันดูแลและป้องกันการตกเป็นเหยื่อของกลุ่มอาชญากรทางไซเบอร์

2. ส่งเสริมการให้ความรู้แก่ประชาชนเพื่อป้องกันไม่ให้ตกเป็นเหยื่อการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ และสามารถควบคุมอารมณ์และตัดสินใจอย่างมีสติก่อนกระทำการใด ๆ

2.1 การสนับสนุนความรู้ความเข้าใจเรื่องการเงินส่วนบุคคลกับประชาชนทั่วไป

2.2 การให้ความรู้และวิจารณญาณในการซื้อสินค้าออนไลน์

2.3 การรักษาข้อมูลและความลับส่วนบุคคล

3. การป้องกันและปราบปรามการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ในระดับประเทศ

3.1 การบูรณาการการทำงานร่วมกันระหว่างผู้เสียหาย ธนาคาร และเจ้าหน้าที่ตำรวจ เพื่อเป็นการประสานงานกันในการแก้ปัญหาให้รวดเร็วขึ้น

3.2 การเพิ่มเจ้าหน้าที่ที่เกี่ยวข้องกับการช่วยเหลืออาชญากรรมทางไซเบอร์ให้เพิ่มมากขึ้น เพื่อที่จะรองรับคดีความที่มีจำนวนมาก

**อภิปรายผลการวิจัย**

ปัจจุบันมีการใช้เทคโนโลยีสารสนเทศกันอย่างแพร่หลาย การหาข้อมูลส่วนบุคคลจึงสามารถกระทำได้ง่าย ไม่ว่าจะเป็นการค้นหาจาก Social Media ที่มีบุคคลส่วนใหญ่ได้ทำการโพสต์ข้อมูลต่าง ๆ ที่เกี่ยวข้องกับตนเอง หรือกลุ่มการซื้อขายสินค้าออนไลน์บน Facebook หรือ Instagram ซึ่งการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวสู่สาธารณะโดยเกินความจำเป็นนั้นอาจส่งผลให้ถูกขโมยข้อมูลสำคัญและทำให้ข้อมูลส่วนบุคคลของผู้ใช้งานรั่วไหลออกไปสู่กระบวนการในการก่ออาชญากรรมทางเทคโนโลยีได้ง่าย สอดคล้องกับงานวิจัยของสุมนทิพย์ จิตสว่าง และคณะ (2563) ที่อธิบายว่า ข้อมูลลูกค้าจากสถาบันการเงินหรือหน่วยงานที่เกี่ยวข้องกับการเก็บข้อมูลลูกค้าทั้งหมดจะถูกปกปิดเป็นความลับ แต่ข้อมูลส่วนหนึ่งอาจมีการรั่วไหลได้เนื่องจากการถูกขโมยหรือแฮกส์ทางอินเตอร์เน็ตหรือเจ้าหน้าที่บางคนอาจมีการทุจริตแอบขายข้อมูลบางส่วนให้แก่แก๊งคอลเซ็นเตอร์ ทั้งที่เป็นการกระทำโดยเจตนาหรือไม่เจตนา โดยแก๊งคอลเซ็นเตอร์ได้นำข้อมูลจากลูกค้าไปใช้สร้างความน่าเชื่อถือ จนกระทั่งเหยื่อยอมโอนเงินให้อันเป็นปัญหาและอุปสรรคต่อการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์

งานวิจัยชิ้นนี้ได้นำทฤษฎีทางอาชญาวิทยาและเหยื่อวิทยาร่วมกันอธิบายถึงปัจจัยที่ทำให้ประชาชนถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ ซึ่งผู้วิจัยได้กำหนดตัวแปรที่นำมาสู่กรอบแนวคิดการวิจัยโดยจำแนกเป็นปัจจัยภายใน และปัจจัยภายนอก ซึ่งปัจจัยภายในสอดคล้องกับแนวคิดของลอร์เรน โคเฮน และมาร์คัส เฟลสัน (1979) ประกอบด้วย ความรู้ไม่เท่าทันการหลอกลวง ความกลัว ความโลภ และยังสอดคล้องกับพิทักษ์ ศิริวงษ์ และบัณฑิตา อุณหเลขจิตร (2560) ในเรื่องความเข้าใจเทคโนโลยี และปัจจัยภายนอกสอดคล้องกับ DeLima (2018) ประกอบด้วย จำนวนผู้พิทักษ์ที่มีไม่เพียงพอ และสภาพแวดล้อมทางสังคมที่ไม่เอื้อต่อการป้องกันการหลอกลวง ซึ่งสอดคล้องกับผลการศึกษาที่ว่าลักษณะการหลอกลวงเหยื่อของแก๊งคอลเซ็นเตอร์ส่วนใหญ่ผู้หลอกลวงมักใช้วิธีการสร้างสถานการณ์ทำให้เหยื่อรู้สึกตื่นตกใจกลัวหรือโลภ จนทำให้ตัดสินใจโดยไม่ระมัดระวัง เนื่องจากคิดว่าเรื่องที่เกิดขึ้นนั้นเป็นเรื่องจริง สอดคล้องกับงานวิจัยของสุมนทิพย์ จิตสว่าง และคณะ (2563) ในเรื่องของเนื้อหาที่แก๊งคอลเซ็นเตอร์ใช้ในการสนทนากับเหยื่อ ส่วนใหญ่จะเกี่ยวกับการทำธุรกรรมทางการเงินหรือขอข้อมูลส่วนบุคคลของเหยื่อ เช่น

หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัตรเครดิต เป็นต้น โดยใช้จิตวิทยาโน้มน้าวให้เหยื่อตกใจ รู้สึกหวาดกลัวหรือเกิดความโลภ รวมทั้งความไม่รู้ทำให้เหยื่อหลงเข้าใจผิดแล้วรีบเร่งให้เหยื่อทำธุรกรรมหรือให้ข้อมูลส่วนตัวเหล่านั้นไปแบบไม่ทันได้ตั้งตัว และยังสอดคล้องกับงานวิจัยของธัญพิชชา สามารถ (2566) ที่อธิบายว่า การตกเป็นเหยื่อแก๊งคอลเซ็นเตอร์ อาศัยเรื่องของความโลภ ความกลัว และการสวมรอยเป็นบุคคลที่รู้จัก ประกอบกับเวลาที่จำกัดในการตัดสินใจเป็นปัจจัยเร่งในการนำไปสู่การตัดสินใจที่ผิดพลาดได้ง่าย และปัจจัยที่สำคัญที่พบจากการศึกษา คือ ผู้ตกเป็นเหยื่อบางรายขาดความเข้าใจในเทคโนโลยี ส่งผลให้เกิดการตัดสินใจโดยขาดความรู้ความเข้าใจ จึงทำให้ตกเป็นเหยื่อแก๊งคอลเซ็นเตอร์ได้ง่าย สอดคล้องกับงานวิจัยของขวัญชนก ศรีภมร (2565) ที่อธิบายว่า มิจฉาชีพมักอาศัยช่องทางความตื่นกลัวและความโลภของคนเป็นปัจจัยหลักในการหลอกลวง และกลุ่มเป้าหมายที่เป็นที่นิยมของมิจฉาชีพ ได้แก่เหยื่อมักจะเป็นผู้สูงวัยที่ไม่เข้าใจในเทคโนโลยีมากพอ ข้าราชการเกษียณที่มีเงินเก็บสะสมหรือแม้กระทั่งข้าราชการระดับสูง เป็นต้น การทำงานของแก๊งคอลเซ็นเตอร์มีการอัปเดต ข้อมูลตามเทรนด์ในช่วงระยะเวลานั้นตลอดเวลาซึ่งจะทำให้เห็นว่าการหลอกลวงแต่ละครั้งจะเปลี่ยนเรื่องราวไปเรื่อย ๆ มีการทำบัญชีม้า หรือการรับจ้างเปิดบัญชีเพื่อให้โอนเงินเป็นทอด ๆ ตามรอยได้ยาก

การหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ เป็นอาชญากรรมทางเศรษฐกิจระหว่างประเทศรูปแบบหนึ่งในยุคดิจิทัล และนอกจากจะก่อให้เกิดความเสียหายทางเศรษฐกิจต่อเหยื่อจำนวนมากแล้ว ยังก่อให้เกิดความเสียหายต่อเศรษฐกิจในภาพรวมระดับประเทศ ซึ่งที่ผ่านมาแก๊งคอลเซ็นเตอร์ได้แอบอ้างเป็นเจ้าหน้าที่หน่วยงานของรัฐ โทรศัพท์หรือส่งข้อความสั้นหลอกลวงประชาชน เพื่อชักจูงให้ประชาชนหลงเชื่อกดลิงก์ติดตั้งแอปพลิเคชันควบคุมเครื่องโทรศัพท์แล้วโอนเงินออกจากบัญชีธนาคารไป หรือส่งเอกสารปลอมข่มขู่ให้ประชาชนกลัวเป็นเหตุให้ประชาชนได้รับความเสียหายเป็นจำนวนมาก และด้วยสภาพแวดล้อมสังคมที่เปลี่ยนไปส่งผลให้รูปแบบการหลอกลวงรูปแบบใหม่ ๆ มีการพัฒนามาควบคู่กัน จะเห็นได้จากแก๊งคอลเซ็นเตอร์พยายามที่จะแอบอ้างเป็นบุคคลหรือหน่วยงานที่กำลังเป็นที่นิยม เพื่อสร้างความน่าเชื่อถือให้สอดคล้องกับสภาพสังคมในปัจจุบัน ซึ่งแม้มีการประชาสัมพันธ์ถึงรูปแบบการหลอกลวงเพื่อเตือนภัยประชาชนก็ยังไม่สามารถเท่าทันกลโกงของมิจฉาชีพได้ ส่งผลให้ปัจจุบันปัญหาจากแก๊งคอลเซ็นเตอร์ยังพบเห็นได้อย่างต่อเนื่อง สอดคล้องกับผลงานของกัลป์ กรุยรุ่งโรจน์ (2564) ที่ได้ศึกษาว่าในปี 2023 คนไทยได้รับ SMS และได้รับสายจากมิจฉาชีพมากที่สุดในทวีปเอเชีย โดยได้รับ SMS จากมิจฉาชีพถึง 58 ล้านข้อความ เพิ่มขึ้นจากปีก่อน 17% ซึ่งตกเฉลี่ยแล้วคนไทยได้รับ SMS จากมิจฉาชีพคนละ 20.3 ข้อความต่อปี นอกจากนี้คนไทยยังได้รับสายจากมิจฉาชีพกว่า 20.8 ล้านสาย เพิ่มขึ้นจากปีก่อน 22% ซึ่งเฉลี่ยแล้วคนไทยหนึ่งคนต้องรับสายมิจฉาชีพประมาณ

7.3 สายต่อปี และประเทศไทยซึ่งเป็นประเทศที่ได้รับความเสียหายจากการถูกหลอกลวงออนไลน์ในระดับสูง มักจะใช้กลไกตำรวจในการจัดการกับมิจฉาชีพออนไลน์เป็นหลัก ซึ่งการใช้กลไกตำรวจดำเนินคดีมักเป็นแนวทางที่ป้องกันการหลอกลวงได้ต่ำ เนื่องจากเมื่อมิจฉาชีพได้รับเงินจากเหยื่อแล้ว ก็มักกระจายเงินผ่านบัญชีม้า ดังนั้นวิธีป้องกันที่ดีที่สุดคือการมีสติ และควรมีการประชาสัมพันธ์เตือนภัยประชาชนถึงกลโกงรูปแบบใหม่สม่ำเสมอ รวมถึงวิธีการปฏิบัติเมื่อรู้สึกตัวว่าตนนั้นได้ให้ข้อมูลส่วนตัวกับมิจฉาชีพไปด้วยความไม่รู้ เพื่อให้ลดปัญหาที่อาจเกิดขึ้นตามมา สอดคล้องกับงานวิจัยสัณห์ภพ วิทยาทอง (2564) ได้อธิบายว่า การรับข้อมูลข่าวสารเกี่ยวกับอาชญากรรมทางไซเบอร์ที่สูงจะทำให้พฤติกรรมเสี่ยงในการตกเป็นเหยื่ออาชญากรรมทางการทำธุรกรรมออนไลน์ลดลง ทั้งนี้เนื่องจากการที่นิสิตให้ความสำคัญกับคิดข้อมูลต่างๆ ที่เกี่ยวกับการทำธุรกรรมทางการเงินออนไลน์ ซึ่งทราบว่าจะได้รับความเสียหาย ถ้าข้อมูลเกี่ยวกับการทำธุรกรรมทางการเงินออนไลน์ถูกขโมย จึงต้องให้ความสนใจและติดตามข้อมูลเกี่ยวกับการรักษาความปลอดภัยคอมพิวเตอร์ ศึกษาคู่มือหรือคำแนะนำด้านความปลอดภัยที่ดีจะช่วยปกป้องหรือลดโอกาสเกิดอาชญากรรมคอมพิวเตอร์ และรู้เท่าทันว่าในปัจจุบันภัยคุกคามจากอาชญากรรมคอมพิวเตอร์มีอัตราเพิ่มขึ้น

การหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ยังคงเป็นปัญหาที่รุนแรง เนื่องจากมิจฉาชีพเหล่านี้มักมีที่อยู่ไม่เป็นหลักแหล่งและรูปแบบการหลอกลวงมีวิธีที่ซับซ้อนมากขึ้น ทำให้ยากต่อการสืบสาวต้นตอเพื่อยับยั้งกระบวนการนี้ และการที่จะสามารถลงโทษผู้กระทำความผิดได้จะต้องเกิดเหตุการณ์ขึ้นแล้วเท่านั้น ทำให้การที่จะนำตัวผู้กระทำความผิดมาลงโทษจึงไม่มีผลต่อการทำให้แก๊งคอลเซ็นเตอร์ลดน้อยลง ดังนั้นทุกหน่วยงานที่เกี่ยวข้องจึงควรหันมาให้ความสำคัญและร่วมมือกันในการป้องกันและกำกับดูแลก่อนที่จะเกิดเหตุเสียมากกว่า เพื่อที่จะได้เป็นแนวทางการป้องกันตั้งแต่ต้นในการช่วยลดความเสียหายที่อาจจะเกิดขึ้น

**ข้อเสนอแนะจากการวิจัย**

จากผลการศึกษาสรุปแนวการป้องกันและการปราบปรามแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ มีข้อเสนอแนะและแนวทางป้องกันดังนี้

1. หน่วยงานที่เกี่ยวข้องควรมีการจัดการอบรมประชาชนเพื่อเพิ่มความตระหนักรู้ และลดความกลัวและความโลภจากแก๊งคอลเซ็นเตอร์ ซึ่งเป็นสิ่งสำคัญในการสร้างสังคมที่ปลอดภัยจากการหลอกลวงทางไซเบอร์ โดยการส่งเสริมความรู้และการสร้างความมั่นใจจะช่วยให้ประชาชนสามารถปกป้องตนเองและลดโอกาสที่จะตกเป็นเหยื่อของอาชญากรรมเหล่านี้ได้อย่างมีประสิทธิภาพมากขึ้น

2. จัดตั้งหน่วยงานที่มีความเชี่ยวชาญในการเฝ้าระวังและตรวจสอบการกระทำผิดในโลกไซเบอร์ โดยมีเจ้าหน้าที่ที่มีความรู้ด้านเทคโนโลยีสารสนเทศและกฎหมายไซเบอร์

3. ธนาคารแห่งประเทศไทยควรมีการกำหนดเกณฑ์การตรวจสอบ โดยสร้างเกณฑ์ที่ชัดเจนในการกำหนดว่าเมื่อใดที่ธุรกรรมควรถูกตรวจสอบ เช่น จำนวนเงินที่สูงผิดปกติ หรือการทำธุรกรรมในเวลาที่ไม่ปกติ

4. รัฐบาลควรมีการสร้างนโยบายและกฎหมายที่เข้มแข็งเพื่อป้องกันการหลอกลวงจากแก๊งคอลเซ็นเตอร์ รวมถึงการจัดการกับผู้กระทำผิดกฎหมายอย่างเหมาะสมและมีประสิทธิภาพ การจัดทำนโยบายและกฎหมายที่เหมาะสมในการป้องกันการหลอกลวงไม่ว่าจะเป็นในด้านการเงิน การซื้อขาย หรือการเข้าถึงข้อมูลส่วนบุคคล

## ข้อเสนอแนะในการศึกษาวิจัยครั้งต่อไป

1. ศึกษาแนวโน้มและลักษณะการหลอกลวงของแก๊งคอลเซ็นเตอร์ในประเทศต่าง ๆ เพื่อทำความเข้าใจการกระจายตัวและรูปแบบที่แตกต่างกัน

2. ศึกษาแนวทางในการเยียวยาผู้ตกเป็นเหยื่ออาชญากรรมไซเบอร์ทุกประเภท ซึ่งเป็นเรื่องสำคัญที่ต้องพิจารณาอย่างจริงจัง เนื่องจากผลกระทบที่เกิดขึ้นจากอาชญากรรมไซเบอร์นั้นไม่เพียงแต่กระทบต่อทรัพย์สิน แต่ยังส่งผลกระทบต่อจิตใจและความเชื่อมั่นของผู้เสียหาย จึงควรศึกษาถึงแนวทางในการเยียวยา เพื่อให้สามารถช่วยเหลือผู้เสียหายได้อย่างมีประสิทธิภาพ

# บรรณานุกรม

# บรรณานุกรม


กรกนก นิลดำ, เสริมศิริ นิลดำ, อิงดอย ศรีลำพัฒน์, ภควัฒน์ สวนงาม, วรักษณ์กมล มงคลอัศศิริ และปฐมพร ปัญญะติ. (2563). วิธีการกลโกง ช่องทางการสื่อสาร และประสบการณ์ในการถูกมิจฉาชีพออนไลน์หลอกลวงของผู้สูงอายุในจังหวัดเชียงราย. *CRRU Journal of Communication Chiangrai Rajabhat University, 3*(3), 50-67, https://so01.tci-thaijo.org/index.php/CRRUJC/ article/view/241670/166342

กัลป์ กรุยรุ่งโรจน์. (2564). *คนไทยรวยมิจ: การหลอกลวงออนไลน์ในไทยเทียบกับต่างประเทศ*. https://www.the101.world/flash-scam-thailand-international

กิตติคุณ มีทองจันทร์ และวงศ์ยศ เกิดศร. (2564). ปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและ*ปริมณฑล*. *Journal of Criminology and Forensic Science, 7*(2), 122-135.

ขวัญชนก ศรีภมร. (2565). *แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม*. สารนิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย.

จิตราภรณ์ โสตถิกุล. (2565). *การก่อการร้ายทางไซเบอร์: ปัญหาการนิยาม เขตอำนาจ และการบังคับใช้กฎหมาย*. วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

เดลินิวส์ . (2559). *ชำแหละแก๊งโจรร้าย 'คอลเซ็นเตอร์' รู้ทันเหลี่ยม...ไม่ตกเป็นเหยื่อสูญเงิน*. https://www.dailynews.co.th › article

ไทยรัฐ. (2566). *หนุ่มวัย 40 เสียท่าแก๊งคอลเซ็นเตอร์ อ้างเป็นกรมการค้าภายใน โดนไป 16 ล้าน*. https://www.thairath.co.th/news/crime/ 2639170

พรชัย ขันตี, กฤษณะพงศ์ ฟูตระกูล และจอมเดช ตรีเมฆ. (2558). *ทฤษฎีอาชญาวิทยา: หลักการงานวิจัยและนโยบายประยุกต์*. ส.เจริญการพิมพ์.

พระมหาธรรมทส ขนฺติพโล (พืชจันทร์). (2560). *ศึกษาการประยุกต์ใช้สติเพื่อป้องกันการถูกหลอกลวงทางอินเทอร์เน็ต*. วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย.

พัลลภ หริ่งรอด. (2562). *มาตรการตามกฎหมายในการปราบปรามองค์กรอาชญากรรมข้ามชาติศึกษาเฉพาะกลุ่มคอลเซ็นเตอร์*. งานนิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยบูรพา.

พิทักษ์ ศิริวงศ์ และบัณฑิตา อุณหเลขจิตร. (2560). การใช้สื่อสังคมออนไลน์ของผู้สูงอายุในเขตตลาดตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม. ใน *การประชุมวิชาการ*

*มหาวิทยาลัยเทคโนโลยีราชมงคล*. ราชมงคลสร้างสรรค์นวัตกรรมที่ยั่งยืนสู่ประเทศไทย 4.0, (7-9 สิงหาคม 2560). ศูนย์แสดงสินค้าและการประชุม อิมแพค เมืองทองธานี.

พิริยะ กิมาลี, นิตยา วงศ์ภินันท์วัฒนา. (2562). *การศึกษาสาเหตุและผลกระทบเชิงลึกของการตกเป็นเหยื่อการกลั่นแกล้งทางไซเบอร์ในที่ทำงาน (No. 174173)*. มหาวิทยาลัยธรรมศาสตร์.

ฤทธี อินทราวุธ. (2561). *โลกไซเบอร์กับความมั่นคงของชาติ*. http://rittee1834.blogspot.com/2015/04/cyberspace-vs-national-security. html

สรวิศ บุญมี. (2566). ภัยแก๊งคอลเซ็นเตอร์ จากอาชญากรรมทางเศรษฐกิจสู่อาชญากรรมทางเทคโนโลยี. *วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชีย ฉบับวิทยาศาสตร์และเทคโนโลยี, 17*(2), 19-26.

สัณห์ภพ วิทยาทอง. (2564). ความเสี่ยงในการตกเป็นเหยื่ออาชญากรรมทางการทำธุรกรรมออนไลน์ของนักศึกษามหาวิทยาลัยศรีนครินทรวิโรฒ. *วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์, 7*(2), 31-44.

ธัญพิชชา สามารถ. (2566). *การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ*. ดุษฎีนิพนธ์ปริญญาดุษฎีบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย.

สุมนทิพย์ จิตสว่าง, ปิยะพร ตันฉีกุล และนัทธี จิตสว่าง (2563). *โครงการอาชญากรรมข้ามชาติ: ภัยคุกคามประเทศไทยเกี่ยวกับแก๊งคอลเซ็นเตอร์*. https://digital.library.tu.ac.th/tudc/frontend/Info/item/dc:175108

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

Bossard. (1998). *Mafias, Triads, Yakuza and Cartels: A Comparative Study of Organized Crime*. http://www.cjcenter.org/cjcenter/publications/cji

Buil-Gil, D., & Zeng, Y. (2021). Meeting you was a fake: Investigating the increase in romance fraud during COVID-19, *Journal of Financial Crime.* https://doi.org/10.1108/JFC-02-20210042

DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist, 58*(4), 706-718. https://pubmed.ncbi.nlm.nih. gov/28329-818

DROIDSANS. (2023). *14 อันดับภัยออนไลน์ที่คนไทยโดนหลอกสูงสุด เสียหายรวมกว่า 3 หมื่นล้านบาท วัยทำงานโดนเยอะสุด*. https:// droidsans.com/top-14-cyber-online-of-thailand

ECIPE (European Centre for International Political Economy). (2017). *The economic impact of cybercrime: No slowdown in sight.* https://ecipe.org/publications/the-economic-impact-of-cyber-crime-no-slowdown-in-sight

Freda A., & Mueller, Gerhard & Laufer. (1991). *Criminilogy*. McGrawHill.

Office of Fair Trading (2009). *The Psychology of Scams: Provoking and Committing Errors of Judgement. Office of Fair Trading.* https://ore.exeter.ac.uk/repository/handle/10871/20958?show=full

Siegel, J. Larry. (2006). *Criminology.* 9th ed. Canada: Thomson Wadsworth.

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

UNODC. (2021). *Cybercrime.* https://www.unodc. org/cybercrime

Weissbrodt, D. (2013.) Cyber-Conflict, Cyber-Crime and Cyber-Espionage, *Minnesota Journal of International Law,* 347-366.

# ประวัติย่อของผู้วิจัย

| | |
|---|---|
| **ชื่อ-สกุล** | นางสาวศรัณย์รัฐ เนาวอุไรรัตนา |
| **วัน เดือน ปี เกิด** | 7 มกราคม 2517 |
| **สถานที่เกิด** | เพชรบุรี |
| **สถานที่อยู่ปัจจุบัน** | 73/34-35 ถนนบางแวก แขวงบางไผ่<br>เขตบางแค กรุงเทพมหานคร รหัสไปรษณีย์ 10160 |
| **ตำแหน่งและประวัติการทำงาน** | 2537 - ปัจจุบัน บริษัท บางกอก ซายน์ เซ็นเตอร์ จำกัด<br>ตำแหน่ง กรรมการผู้จัดการ |
| **ประวัติการศึกษา** | 2536 อนุปริญญาวิทยาศาสตรบัณฑิต<br>มหาวิทยาลัยราชภัฏเพชรบุรี<br>2542 ศิลปศาสตรบัณฑิต<br>(วิชาเอกการจัดการทั่วไป แขนงบริหารทรัพยากรมนุษย์)<br>มหาวิทยาลัยราชภัฏเพชรบุรี<br>2567 รัฐศาสตรมหาบัณฑิต (การบริหารงานยุติธรรมและสังคม)<br>มหาวิทยาลัยบูรพา |