เอกสารวิชาการ (Concept Paper)
กิจกรรมถอดบทเรียน

เรื่อง การหลอกลวงให้ลงทุนออนไลน์
กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม

จัดทำโดย กลุ่มปาริชาต

รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรการป้องกันอาชญากรรมกับการอำนวยความยุติธรรมในสังคม
Crime Prevention รุ่นที่ 8
สถาบันพัฒนาบุคลากรในกระบวนการยุติธรรม สำนักงานกิจการยุติธรรม
ประจำปี 2568

บทคัดย่อ

ปัจจุบันอินเทอร์เน็ต (Internet) ได้รับความนิยมเป็นอย่างสูงและถูกนำไปใช้งานไปอย่างแพร่หลายในทุกภาคส่วน ทั้งภาครัฐภาคเอกชนและภาคธุรกิจ ซึ่งประเทศไทยมีการผลักดันระบบเศรษฐกิจแบบเดิมไปสู่ระบบเศรษฐกิจแบบดิจิทัล (Digital Economy) ซึ่งเป็นเศรษฐกิจรูปแบบใหม่ที่ขับเคลื่อนด้วยเทคโนโลยีดิจิทัลอยู่บนโลกออนไลน์ ซึ่งเป็นการนำเทคโนโลยีมาช่วยเพิ่มประสิทธิภาพและสร้างมูลค่าเพิ่มให้กับการดำเนินกิจกรรมทางเศรษฐกิจในด้านต่างๆ ไม่ว่าจะเป็นภาคการผลิต การขนส่ง การขาย และการบริการ โดยเฉพาะช่วงที่มีการแพร่ระบาดของไวรัส COVID-19 ทำให้โลกหมุนช้าลง เพราะต้องจำกัดการเดินทาง การเคลื่อนย้ายผู้คน หรือการพบเจอกัน แต่ในโลกของดิจิทัลนั้นกลับหมุนเร็วขึ้นกว่าเดิม และกลายมาเป็นส่วนหนึ่งของชีวิตอย่างไม่รู้ตัว ตั้งแต่การใช้งานสื่อสังคมออนไลน์ (Social Media) การซื้อขายสินค้า เล่นเกม ดูหนัง สั่งอาหาร ท่องเที่ยว หรือแม้กระทั่งการศึกษา นับว่าเป็นอรรถประโยชน์ที่ช่วยอำนวยความสะดวกในการใช้ชีวิต ในขณะเดียวกัน การก่ออาชญากรรมออนไลน์มีแนวโน้มสูงขึ้นซึ่งเป็นผลกระทบที่เกิดจากการใช้สื่อออนไลน์ คดีที่พบมากที่สุด ได้แก่ การโกงการซื้อขายสินค้าและบริการ การหลอกลวงให้โอนเงินเพื่อทำงาน การหลอกให้กู้เงิน และการหลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ตามลำดับ[i] โดยอาชญากรมักอาศัยความเป็นนิรนามในโลกเสมือนจริงกระทำความผิด ทำให้เป็นอุปสรรคในการตรวจสอบตัวตนและการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ

ปัญหาการหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม เป็นลักษณะการหลอกลวงแบบ Hybrid scam ซึ่งเป็นการผสมผสานเทคนิคการหลอกลวงผู้เสียหายให้ไว้ใจหรือเชื่อใจ โดยมุ่งเน้นความอ่อนไหวทางอารมณ์หรือความกังวลในความมั่นคงทางการเงิน จูงใจด้วยผลตอบแทนจากการซื้อขายสกุลเงินดิจิทัลที่ไม่มีราคาตลาดอ้างอิง และหลอกให้เสียทรัพย์โดยการลงทุนผ่านแพลตฟอร์มปลอมหลายรูปแบบ เช่น เว็บไซต์ แอพลิเคชั่น เป็นต้น งานวิชาการนี้เป็นการถอดบทเรียนเชิงคุณภาพ โดยทำการศึกษา 2 แบบ ได้แก่ การวิจัยเอกสาร ใช้การศึกษาข้อมูล ข้อเท็จจริง สถิติจากแหล่งข่าวเปิด (ข่าวสาร/ สำนวนคดี) และการวิจัยแบบตีความ ใช้การศึกษาข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกโดยหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง เพื่อวิเคราะห์จุดเสี่ยงและนำเสนอนวัตกรรมการป้องกันอาชญากรรมที่มุ่งเน้นการลดโอกาสการเกิดอาชญากรรมและการบังคับใช้กฎหมายที่ครอบคลุม

ผลการศึกษาพบว่ามิจฉาชีพจะสร้างตัวตนปลอมที่แสดงความมีประสบการณ์ด้านการลงทุนในสกุลเงินดิจิทัล โดยมีการทักเหยื่อผ่านสื่อสังคมออนไลน์บนแพลตฟอร์มต่าง ๆ หลังจากนั้นจะพยายามสร้างความรู้จัก พูดคุยเพื่อให้เกิดความเชื่อใจมากขึ้น นำไปสู่การแนะนำแพลตฟอร์มด้านการลงทุนเกี่ยวกับสกุลเงินดิจิทัล และส่งลิงก์ให้ดาวน์โหลดแพลตฟอร์มปลอมที่ใช้ในการลุงทุน เหยื่อจะถูกหลอกให้โอนเงินผ่านบัญชีม้าโดยอ้างว่าเพื่อโอนต่อไปยังบัญชีของแพลตฟอร์มต่างประเทศ หลังจากมีการลงทุนมีการแสดงผลกำไรที่สูงเกินควรเพื่อดึงดูดความสนใจกับเหยื่อ เมื่อลงทุนไประยะหนึ่ง มิจฉาชีพจะสร้างความเชื่อมั่นว่าเหยื่อจะไม่ถูกหลอกโดยวิธีการใดวิธีการหนึ่ง เช่น การส่งสินค้าแบรนด์เนมมาให้เหยื่อเพื่อหลอกให้ตายใจ เมื่อเหยื่อต้องการถอนผลกำไร มิจฉาชีพจะแจ้งว่าจะต้องทำการโอนเงินเข้าบัญชีซื้อ-ขายก่อนและหลอกให้เหยื่อโอนเงินเพิ่มขึ้นเรื่อย ๆ จนเหยื่อเริ่มรู้ตัวและมิจฉาชีพจะทำการตัดขาดการสื่อสารไป

แนวทางนวัตกรรมการป้องกันและแก้ไขการหลอกลวงที่นำเสนอ ได้แก่ การแสดงข้อความ pop-up ในแอพพลิเคชั่นของธนาคาร ที่ผู้ใช้บริการสามารถกดข้ามได้หลังจาก 3 วินาทีเพื่อเตือนผู้ใช้บริการให้ระวังมิจฉาชีพหลอกลงทุน ตรวจสอบบัญชีม้าได้ที่แอพพลิเคชั่น Cyber Check ที่ถูกสร้างและพัฒนาโดยตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี นอกจากนี้ยังมีการประชาสัมพันธ์ Clip VDO และ Spot สั้น 1-3 นาที ผ่านทาง Social Media โทรทัศน์ วิทยุ และเสียงตามสาย เกี่ยวกับการลงทุนในสกุลเงินดิจิทัลและการหลอกลวงให้ลงทุน เพื่อให้เข้าถึงประชาชนทั้งในชุมชนเมืองและต่างจังหวัด

สารบัญ

ส่วนที่ 1 บทนำ :

1) หลักการและเหตุผล

อาชญากรรมออนไลน์ (Cybercrime) เป็นการกระทำผิดกฎหมายที่เกิดขึ้นผ่านอินเทอร์เน็ตหรือเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการกระทำผิดที่เกี่ยวข้องกับการโจรกรรมข้อมูล การหลอกลวง การปลอมแปลงข้อมูล การเข้าถึงเครือข่ายและอุปกรณ์โดยไม่ได้รับอนุญาต การเผยแพร่ไวรัสคอมพิวเตอร์ หรือการกระทำที่ทำให้เกิดความเสียหายทางการเงินหรือชื่อเสียงในโลกออนไลน์ การพัฒนาเทคโนโลยีและการเชื่อมต่ออินเทอร์เน็ตที่ก้าวหน้าขึ้นทำให้เกิดช่องทางใหม่ ๆ สำหรับการกระทำผิดทางอาญาที่ทำให้เกิดความเสียหายทั้งในระดับบุคคลและสังคม สาเหตุหลักมาจากการเติบโตของการใช้อินเทอร์เน็ตและเทคโนโลยีสารสนเทศในชีวิตประจำวัน เพิ่มโอกาสให้กับอาชญากรในการกระทำผิดทางออนไลน์ และอาชญากรรมออนไลน์สามารถกระทำได้จากที่ใดก็ได้ในโลก และมักเกิดขึ้นในลักษณะที่ทำให้ผู้กระทำผิดยากที่จะถูกติดตามหรือจับกุม นอกจากนี้อาชญากรรมออนไลน์สามารถสร้างความเสียหายทางการเงินและชื่อเสียงให้กับบุคคลหรือองค์กรได้ โดยเฉพาะในกรณีที่มีการขโมยข้อมูลสำคัญหรือทำการหลอกลวงทางการเงิน ข้อมูลจาก Statista แสดงให้เห็นว่าในปี 2023 มีสถิติการก่ออาชญากรรมบนโลกออนไลน์ที่ได้รับแจ้งในสหรัฐอเมริกากว่า 700,000 คดี ซึ่งอาชญากรรมที่เกิดขึ้นมากสุด 5 อันดับแรก ได้แก่ การหลอกลวงแบบ Phishing การละเมิดข้อมูลส่วนบุคคล การโกงการซื้อขายทางออนไลน์ การกรรโชกทรัพย์ และการหลอกให้ลงทุน ตามลำดับ[2]

ในบริบทของประเทศไทย จากรายงานของสำนักงานตำรวจแห่งชาติ ระบุว่า ตั้งแต่วันที่ 1 มีนาคม 2565 ถึง 30 พฤศจิกายน 2567 มีคดีอาชญากรรมไซเบอร์เกิดขึ้น 739,494 คดี รวมมูลค่าความเสียหาย 77,360,070,295 บาท โดยอาชญากรรมที่มีมูลค่าความเสียหายมากที่สุด คือ การหลอกให้โอนเงินเพื่อทำงาน จำนวน 94,729 คดี มูลค่าความเสียหาย 11,876,253,771 บาท การหลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ จำนวน 50,247 คดี มูลค่าความเสียหาย 27,626,001,144 บาท การข่มขู่ทางโทรศัพท์ (Call Center) จำนวน 49,447 คดี มูลค่าความเสียหาย 10,503,524,467 ตามลำดับ ประกอบกับสภาวะเศรษฐกิจถดถอยเป็นวงกว้างที่ส่งผลกระทบต่อความเป็นอยู่และการใช้ชีวิตที่ยากลำบากมากขึ้น หลายคนเริ่มมองหาวิธีหาเงินจำนวนมากที่ง่ายและรวดเร็วเพื่อพัฒนาคุณภาพชีวิตของตนเองและครอบครัว มิจฉาชีพจึงเล็งเห็นช่องทางฉวยโอกาสและแสวงหาผลประโยชน์จากความยากลำบากนี้ ใช้กลวิธีและรูปแบบที่หลากหลายในการหลอกลวง รวมถึงการหลอกลวงที่เกี่ยวข้องกับการลงทุนทั้งการลงทุนแบบออฟไลน์และการลงทุนบนแพล็ตฟอร์มออนไลน์ เช่น สกุลเงินดิจิทัล ตลาดหุ้น ตลาดแลกเปลี่ยนเงินตราต่างประเทศ (Forex) และการลงทุนในสินทรัพย์ต่าง ๆ ผ่านแอปพลิเคชันหรือเว็บไซต์ที่ดูน่าเชื่อถือหรือแพลตฟอร์มปลอม ฯลฯ อีกทั้งความนิยมการลงทุนในสกุลเงินดิจิทัล (Cryptocurrency) ที่สะท้อนถึงโอกาสและลักษณะเฉพาะของสินทรัพย์ดิจิทัล ด้วยผลตอบแทนที่สูงในระยะเวลาสั้น เช่น Bitcoin, Ethereum และเหรียญอื่น ๆ มีการเติบโตอย่างรวดเร็วในช่วงหลายปีที่ผ่านมา ทำงานภายใต้เทคโนโลยีบล็อกเชน (Blockchain) ซึ่งช่วยให้การทำธุรกรรมเกิดขึ้นโดยไม่ต้องพึ่งพาสถาบันการเงินแบบดั้งเดิม นักลงทุนสามารถทำธุรกรรมได้อย่างอิสระ ไร้พรมแดน และดำเนินการโดยตรงระหว่างบุคคล (Peer-to-Peer) โดยไม่ต้องผ่านตัวกลางที่อาจเกิดค่าธรรมเนียม และเป็นการกระจายความเสี่ยง (Diversification) เพราะไม่มีความสัมพันธ์กับสินทรัพย์อื่น

รัฐบาลได้ให้ความสำคัญต่อการดำเนินการลดอาชญากรรมทางไซเบอร์ โดยดำเนินการปราบปรามอาชญากรรมทางเทคโนโลยี โดยมอบหมายกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ สำนักงาน กสทช. ร่วมกับหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ดำเนินการป้องกันและปราบปรามจับกุมอาชญากรรมทางเทคโนโลยีหรือการหลอกลวงประชาชน ตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ 2566 ซึ่งมีมาตรการสำคัญ ได้แก่ ให้สถาบันการเงินหรือผู้ประกอบธุรกิจมีหน้าที่ในการเปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้องในระหว่างสถาบันการเงินและผู้ประกอบธุรกิจ

ผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน และธนาคารแห่งประเทศไทยเห็นชอบร่วมกัน เมื่อพบเหตุอันควรสงสัยหรือได้รับข้อมูลจากการตรวจสอบ ให้สถาบันการเงินหรือผู้ประกอบธุรกิจมีหน้าที่ระงับธุรกรรม แจ้งสถาบันการเงินหรือผู้ประกอบธุรกิจทุกรายที่เป็นผู้รับโอนถัดไป พร้อมทั้งนำข้อมูลต่าง ๆ ที่เกิดขึ้นเข้าสู่ระบบ เพื่อให้ผู้รับโอนทุกคนทราบ และระงับธุรกรรมเหล่านี้ไว้เป็นระยะเวลา 7 วัน ซึ่งเป็นมาตรการขั้นต้นในการระงับการเคลื่อนย้ายเงินที่ต้องสงสัยว่าอาจได้มาโดยมิชอบ

กลุ่มผู้จัดทำเห็นความสำคัญของปัญหาดังกล่าวและทำการศึกษาเรื่อง “การหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม” ซึ่งเป็นการหลอกลวงแบบ Hybrid Scam[3] มิจฉาชีพจะมาในรูปแบบของนักธุรกิจมีทรัพย์สินเงินทองมากมาย เชิญชวนผู้เสียหายให้ร่วมลงทุนหรือทำธุรกิจด้วยกัน โดยอ้างว่าจะได้รับผลตอบแทนสูง นอกจากนี้อาจมีการเตรียมรายการหรือตัวอย่างรายได้ให้ผู้เสียหายหลงเชื่อและโอนเงินหรือทรัพย์สินให้ การหลอกลงทุนปัญหาหนึ่งในอาชญากรรมออนไลน์ที่ใกล้ตัวและสามารถสร้างมูลค่าความเสียหายได้จำนวนมาก เนื่องจากเป็นลักษณะของการลงทุนเพื่อผลตอบแทน มิจฉาชีพมักชักจูงผู้เสียหายว่าเป็นวิธีการหารายได้ที่ถูกจูงใจด้วยค่าตอบแทนที่สูงภายในเวลาอันรวดเร็ว และผู้เสียหายส่วนใหญ่มีความรู้ไม่ครอบคลุมในการลงทุนและเทคโนโลยีที่ซับซ้อนจึงถูกหลอกได้ง่าย นอกจากผลกระทบต่อตัวผู้เสียหายเอง การหลอกลวงประเภทนี้ยังส่งผลกระทบไปถึงครอบครัว สังคม และความเชื่อมั่นในระบบเศรษฐกิจและการลงทุนอีกด้วย แม้ว่า ในห้วงหลายปีที่ผ่านมาทั้งภาครัฐและเอกชนได้ให้ความสำคัญกับการประชาสัมพันธ์ สร้างความตระหนักรู้ เสริมภูมิคุ้มกันให้แก่ประชาชนทั่วไป และการนำเสนอวิธีการป้องกันอาชญากรรมนี้ร่วมกันโดยการออกมาตรการและกฎหมายเพื่อมาควบคุมการกระทำความผิดดังกล่าว แต่ความเสียหายก็ยังเกิดขึ้นอย่างต่อเนื่องและขยายพื้นที่ของการก่ออาชญากรรมไปเป็นวงกว้าง งานวิชาการนี้จึงมุ่งเน้นการศึกษาโดยการวิจัยเอกสาร ใช้การศึกษาข้อมูลข้อเท็จจริง สถิติจากแหล่งข่าวเปิด และการวิจัยแบบตีความ ใช้การศึกษาข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกโดยหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง เพื่อวิเคราะห์จุดเสี่ยงและนำเสนอนวัตกรรมการป้องกันอาชญากรรมที่มุ่งเน้นการลดโอกาสการเกิดอาชญากรรม มูลค่าความเสียหาย และการบังคับใช้กฎหมายที่ครอบคลุมขึ้น

พบว่า มิจฉาชีพจะสร้างตัวตนปลอมที่แสดงประสบการณ์ด้านการลงทุนในสกุลเงินดิจิทัลออนไลน์จะมีการทักเหยื่อผ่านสื่อสังคมออนไลน์บนแพลตฟอร์มต่าง ๆ หลังจากนั้นจะพยายามชวนคุย สร้างความรู้จักเพื่อให้เกิดความเชื่อใจมากขึ้น นำไปสู่การแนะนำผู้เชี่ยวชาญด้านการลงทุนเกี่ยวกับสกุลเงินดิจิทัล และส่งลิงก์ให้ดาวน์โหลดแพลตฟอร์มปลอมที่ใช้ในการซื้อ-ขายเหรียญดิจิทัล ให้เหยื่อโอนเงินผ่านบัญชีม้าโดยอ้างว่าเพื่อโอนต่อไปยังบัญชีของแพลตฟอร์มต่างประเทศ หลังจากมีการลงทุนมีการแสดงผลกำไรที่สูงเกินควรเพื่อดึงดูดความสนใจกับเหยื่อ เมื่อลงทุนไประยะหนึ่ง มิจฉาชีพจะสร้างความเชื่อมั่นว่าเหยื่อจะไม่ถูกหลอกโดยวิธีการใดวิธีการหนึ่ง เช่น การส่งสินค้าแบรนด์เนมมาให้เหยื่อเพื่อหลอกให้ตายใจ เมื่อเหยื่อต้องการถอนผลกำไรมิจฉาชีพจะแจ้งว่าจะต้องทำการโอนเงินเข้าบัญชีซื้อ-ขายก่อนและหลอกให้เหยื่อโอนเงินเพิ่มขึ้นเรื่อย ๆ จนเหยื่อเริ่มรู้ตัวและมิจฉาชีพจะทำการตัดขาดการสื่อสารไป จากตัวอย่างคดีที่กล่าวมาจะพบว่ามีผลกระทบต่อการใช้ชีวิตของประชาชนอย่างมีนัยยะสำคัญ ทั้งในแง่ความเชื่อมั่นในการใช้เงิน การลงทุน ความเชื่อมั่นในกระบวนการยุติธรรมสำหรับการจับกุมผู้กระทำความผิด การยึดทรัพย์ผู้กระทำความผิด และการชดใช้ค่าเสียหาย ซึ่งเป็นปัญหาที่มีความท้าทายในปัจจุบัน

2) วัตถุประสงค์

2.1 เพื่อศึกษาข้อเท็จจริง รูปแบบการกระทำความผิด และสาเหตุของการหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม

2.2 นำเสนอแนวทางนวัตกรรมการป้องกันและแก้ไขการหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม

3) ขอบเขตของเรื่อง

3.1 ประชากรและกลุ่มตัวอย่าง เป็นข้อมูลของผู้เสียหายที่ถูกหลอกลวงให้ลงทุนผ่านแพลตฟอร์มออนไลน์ จากแหล่งข่าวเปิด/ ตัวอย่างคดี จำนวน 4 ตัวอย่าง และบทสัมภาษณ์ของเจ้าหน้าที่จากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 1 ท่าน

3.2 ปัจจัยที่มีผลต่อการถูกหลอกลวง วิเคราะห์วิธีการเข้าถึงเหยื่อ เทคนิคจูงใจ ความรู้สึกของเหยื่อ

3.3 ผลกระทบจากการถูกหลอกลวง วิเคราะห์ผลกระทบที่เกิดขึ้นทั้งต่อเหยื่อและผู้กระทำความผิด ทั้งทางร่างกาย จิตใจ และทรัพย์สิน รวมถึงผู้เสียหายโดยอ้อม เช่น ครอบครัวและสังคม

3.4 แนวทางการพัฒนานวัตกรรมการป้องกันอาชญากรรม วิเคราะห์สาเหตุการเกิดอาชญากรรม และนำเสนอแนวนวัตกรรมการป้องกันอาชญากรรม โดยการแก้ไขกฎหมาย/ ระเบียบที่เกี่ยวข้อง

3.5 ระยะเวลาการศึกษา เดือนธันวาคม 2567 - มกราคม 2568

4) คำจำกัดความหรือนิยามต่าง ๆ

การหลอกลวงทางออนไลน์ (Online Scam)[4] หมายถึง การหลอกลวงทางออนไลน์ โดยผู้เป็นมิจฉาชีพจะทำการปลอมแปลงตัวตนเป็นผู้ให้บริการด้านต่างๆ เช่น การเงิน การธนาคาร จะมีการส่งอีเมลปลอมเพื่อหลอกให้มีการเปลี่ยนรหัสผ่านของบัญชี หรือการซื้อสินค้าออนไลน์ที่มีการชำระเงินโดยใช้บัตรเครดิต ซึ่งจะขอให้มีการเปิดเผยข้อมูลบัตร โดยอาจมีแบบฟอร์มให้กรอกข้อมูลสำคัญของบัตรนั้นๆ หรือแม้แต่การสร้างเว็บไซต์ปลอม เมื่อผู้ใช้ไม่ได้สังเกตให้ละเอียดจะส่งผลให้เกิดการเปิดเผยข้อมูล เมื่อผู้เพื่อใช้บริการถูกหลอกลวงได้

สกุลเงินดิจิทัล[5] คือ สินทรัพย์ดิจิทัล (Digital Asset) ประเภทหนึ่งที่มีการรักษาความปลอดภัยด้วยการเข้ารหัส ถูกออกแบบมาเพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยนเช่นเดียวกับสกุลเงินทั่วไป (Fiat Currency) เพียงแต่ไม่สามารถจับต้องได้ แม้ว่าตอนนี้จะยังไม่สามารถใช้ชำระหนี้ได้ตามกฎหมายดังเช่นสกุลเงินทั่วไป (ยกเว้นประเทศเอลซัลวาดอร์ซึ่งเป็นประเทศแรกในโลกที่อนุมัติให้บิตคอยน์สามารถใช้ชำระหนี้ตามกฎหมายได้) แต่ก็มีธุรกิจหลายแห่งเริ่มมีการนำเทคโนโลยีที่เกี่ยวข้องกับสกุลเงินดิจิทัลมาใช้ เพื่อปรับตัวรับโลกการเงินที่กำลังจะเปลี่ยนแปลงไป เช่น การรับชำระค่าสินค้าและบริการด้วยบิตคอยน์ หรือสกุลเงินดิจิทัลอื่น ๆ ลักษณะเฉพาะของสกุลเงินดิจิทัล ได้แก่ ทำธุรกรรมได้ง่ายและรวดเร็วเนื่องจากธุรกรรมเป็นแบบดิจิทัล ต้นทุนในการทำธุรกรรมต่ำ มีความปลอดภัยและเป็นส่วนตัวจากเทคโนโลยีที่ชื่อว่า “Blockchain” ซึ่งเป็นเทคโนโลยีที่ยากต่อการถอดรหัสทางคณิตศาสตร์ และเปิดซื้อขายแลกเปลี่ยน 24 ชั่วโมงซึ่งต่างจากการลงทุนในตลาดหุ้นปกติ

แพลตฟอร์มดิจิทัล[6] **(Digital Platform)** คือ สื่อกลางทางอิเล็กทรอนิกส์ที่มีการบริหารจัดการข้อมูลเพื่อให้เกิดการเชื่อมต่อกันโดยใช้เครือข่ายคอมพิวเตอร์ระหว่างผู้ประกอบการ ผู้บริโภค หรือผู้ใช้บริการ เพื่อให้เกิดธุรกรรมทางอิเล็กทรอนิกส์ ไม่ว่าจะคิดค่าบริการหรือไม่

ส่วนที่ 2 เนื้อเรื่อง :

1) ข้อเท็จจริง/สถิติที่แสดงถึงปัญหาอาชญากรรม

กรณีศึกษา 1

ปลายปี 2566 ตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (สอท.)[7] รับแจ้งเหตุจากกลุ่มผู้เสียหาย 5 ราย ถูกมิจฉาชีพสร้างโปรไฟล์ปลอมแล้วหลอกลวงให้ลงทุนสินทรัพย์ดิจิทัล โดยสร้างแพลตฟอร์มปลอมขึ้นมาเพื่อหลอกผู้เสียหายว่าได้กำไรจากการลงทุน Cryptocurrency หลอกล่อให้ผู้เสียหายนำเงินมาลงทุนเพิ่ม จนกระทั่งท้ายที่สุดไม่สามารถถอนคืนเงินลงทุนคืนได้ สร้างความเสียหายรวมกันมูลค่ากว่า 530 ล้านบาท 1 ในผู้เสียหายที่เป็นผู้สูงอายุโดนหลอกให้ลงทุนมากถึง 308 ล้านบาท นอกจากนี้ จากการตรวจสอบผู้เสียหายที่ถูกหลอกลวงในลักษณะเดียวกัน เบื้องต้นยังพบว่ามีอีกจำนวน 163 เคสไอดี รวมความเสียหายอีกประมาณ 168 ล้านบาท และในห้วงเวลาใกล้เคียงกัน สอท. ได้เปิดปฏิบัติการทลาย 2 เว็บพนันออนไลน์ พบยอดเงินหมุนเวียนกว่า 13,000 ล้านบาทต่อปี โดยสามารถจับกุมผู้ต้องหาได้ทั้งกลุ่มผู้รับผลประโยชน์ กลุ่มผู้จัดการเรื่องการเงิน จนไปถึงเจ้าของบัญชี พร้อมตรวจยึดเงินสดกว่า 117 ล้านบาท รถยนต์ PORSCHE รุ่น CAYANNE 1 คัน มูลค่าประมาณ 8,000,000 บาท และของกลางอีกหลายรายการ รวมมูลค่าทรัพย์สินกว่า 150 ล้านบาท

จากการสืบสวนขยายผลและวิเคราะห์เส้นทางการเงิน เจ้าหน้าที่ตำรวจได้พบสิ่งที่น่าสนใจ กล่าวคือเส้นทางการเงินของคดีหลอกลงทุนคริปโตเคอร์เรนซีดังกล่าวมีความเชื่อมโยงกับเส้นทางการเงินในคดีเว็บพนันออนไลน์ที่เคยเปิดปฏิบัติการจับกุมข้างต้น โดยพบว่าเงินที่ถูกหลอกลวงจากการการลงทุนคริปโตเคอร์เรนซีได้ถูกนำมาผ่านกระบวนการฟอกเงิน โดยมีกลุ่มคนร้ายแบ่งหน้าที่กันทำอย่างชัดเจน โดยเจ้าหน้าที่ตำรวจไซเบอร์ได้รายงานข้อมูลความเชื่อมโยงของ 2 คดีไปยังสำนักงาน ปปง.และต่อมาสำนักงาน ปปง. ได้มีคำสั่งที่ ย.93/2567 ลงวันที่ 22 เม.ย.67 เพื่อยึดและอายัดทรัพย์สินที่เกี่ยวข้องกับการกระทำความผิดไว้ชั่วคราวที่เจ้าหน้าที่จึงยึดเงินสดกว่า 117 ล้านบาท พร้อมทั้งรถยนต์ Porsche จำนวน 1 คัน มูลค่า 8 ล้านบาท รวมทรัพย์สินทั้งสิ้น มูลค่ากว่า 125 ล้านบาท เพื่อเข้าสู่กระบวนการตรวจสอบและนำมาเฉลี่ยทรัพย์คืนให้แก่ผู้เสียหายต่อไป

กรณีศึกษา 2

ปี พ.ศ. 2565 สอท. ได้รับแจ้งว่ามีกลุ่มผู้เสียหายหลายร้อยรายถูกหลอกลงทุนสกุลเงินดิจิทัล[8] ผ่านระบบแอปพลิเคชัน "bitpie" โดยมิจฉาชีพใช้วิธีการรับโอนเงินเพื่อฝากเทรดผ่านช่องทางกลุ่มไลน์โอเพนแชท ชื่อ "Carpo Trade" โดยมิจฉาชีพเรียกตัวเองว่า โค้ช แต่ละคนจะใช้วิธีการจัดโปรโมชันและแจกส่วนลดการลงทุนเพื่อหลอกล่อสมาชิกให้เกิดความโลภอยากลงทุนเพิ่ม และมีบรรดาหน้าม้าในกลุ่มไลน์โอเพนแชทคอยโชว์ยอดเงินดิจิทัล เพื่อทำให้เหยื่อเชื่อว่าหากลงทุนเพิ่มแล้วทำให้ได้กำไรมากขึ้น เมื่อเหยื่อลงทุนได้สักระยะก็เกิดการขาดทุนกระทันหัน หรือเรียกว่า "พอร์ตแตก" มีการแบ่งระดับสมาชิกตามจำนวนเงินลงทุน

1. สมาชิกกลุ่ม Silver ระดับทุน 10,000 - 80,000 บาท ทุกคน จะโดนเทรดติดลบและยอดเงินหายไป 80% จากยอดเงินในพอร์ต

2. กลุ่ม Gold ระดับเงินทุน 100,000 บาทขึ้นไป สมาชิกทุกคนจะโดนเทรดติดลบ 50% จากยอดเงินในพอร์ต

โค้ชอ้างว่าเป็นการผิดพลาดของระบบและการตัดสินใจเข้าเทรด จากนั้นโค้ชก็ชักชวนให้สมาชิกโอนเงินเพิ่มเข้าไปเพื่อเทรดให้ทุนที่หายไปกลับมา สมาชิกหลายคนจึงหลงเชื่อ และโอนเงินทบเข้าไป ส่วนสมาชิกบางส่วนที่ไม่ได้ทบเงิน และมีเงินเหลือบ้างในพอร์ต หากไม่ได้เปลี่ยนรหัสผ่านก็จะถูกเทรดจนหมดเงิน

ในวันต่อมา หลังจากนั้นต่อมาระบบดังกล่าวและกลุ่มไลน์โอเพนแชทก็ได้ปิดตัวลงเมื่อช่วงเดือนเมษายน 2565 กลุ่มผู้เสียหายหลายร้อยรายจึงเข้าแจ้งความ รวมมูลค่าความเสียหายกว่า 16,000,000 บาท

<u>กรณีศึกษา 3</u>

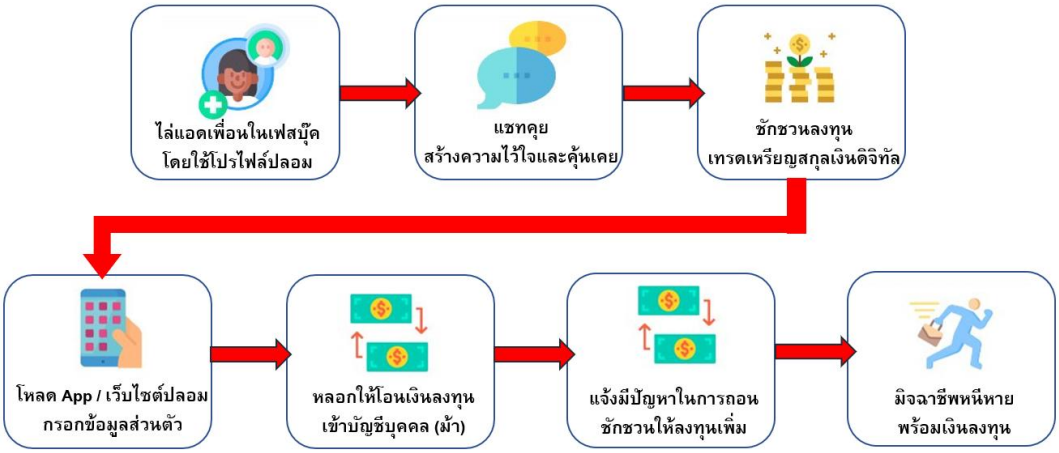
สอท. จับกุมกลุ่มคนร้ายที่ใช้โปรแกรมเทรดหุ้น[9] ชื่อ “BM TECH” ซึ่งมีที่อยู่เว็บไซต์ คือ https://mt5-www.hl058.com และกลุ่มไลน์โอเพนแชท ในการหลอกลวงกลุ่มผู้เสียให้เข้ามาทำการซื้อขายเหรียญคริปโทเคอร์เรนซี่ ชื่อเหรียญ ETH[10] ต่อมาเมื่อมีผู้เสียหายหลายรายหลงเชื่อเข้าร่วมลงทุน โดยคนร้ายจะปล่อยให้ผู้เสียหายได้กำไรในช่วงแรกของการลงทุนเมื่อผู้เสียหายหลงเชื่อและเริ่มลงทุนในจำนวนเงินที่มากขึ้น คนร้ายก็ทำการปิดกลุ่มไลน์และเว็บไซต์ลง ทำให้ไม่สามารถติดต่อกับคนร้ายได้อีกเลย ส่งผลให้มีผู้ได้รับความเสียหายที่ถูกหลอกให้ลงทุนหลายราย ภายหลังจึงได้เข้าแจ้งความร้องทุกข์ต่อพนักงานสอบสวน กก.2 บก.สอท.2 มูลค่าความเสียหายมากกว่า 1,500,000 บาท ต่อมาภายหลังได้รวบรวมพยานหลักฐานขออนุมัติออกหมายจับผู้ต้องหาต่อศาลอาญา ทั้งสิ้น จำนวน 6 ราย เพื่อดำเนินคดีตามกฎหมาย กระทั่งเจ้าหน้าที่ตำรวจ กก.2 บก.สอท.2 ได้ออกสืบสวนติดตามจับกุมผู้ต้องหาตามหมายจับแล้วจำนวน 3 ราย ในความผิดฐาน “ร่วมกันฉ้อโกงโดยแสดงตนเป็นคนอื่น และโดยทุจริตหลอกลวงร่วมกันนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่บุคคลหนึ่งบุคคลใด” เบื้องต้นผู้ต้องหาทั้งสามให้การรับสารภาพ

<u>กรณีศึกษา 4</u>

บช.สอท. ได้รับแจ้งความผ่านระบบรับแจ้งความออนไลน์[11] เกี่ยวกับคดีหลอกลงทุนไฮบริดสแกม ซึ่งคนร้ายใช้โปรไฟล์ปลอมตีสนิทผู้เสียหายผ่านช่องทางสื่อโซเชียลมีเดียต่าง ๆ ก่อนจะชวนลงทุนในแพลตฟอร์มปลอมสำหรับเทรดเงินสกุลดิจิทัลหรือสินทรัพย์ต่าง ๆ โดยมีผู้เสียหายมากกว่า 20,000 คดี มูลค่าความเสียหายมากกว่า 10,000 ล้านบาท โดยคนร้ายมีการดำเนินการที่ประเทศอื่นรวมถึงมีการใช้เทคโนโลยีที่ทันสมัยยากต่อการสืบสวน จึงได้สืบสวนหาคนร้ายตัวจริงที่ใช้บัญชีดังกล่าว โดยมีการประสานความร่วมมือกับหน่วยงานกระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐ หรือ Homeland Security Investigation (HSI) รวมถึงหน่วยงานต่างประเทศและภายในประเทศ นำไปสู่ปฏิบัติการ Trust No One เข้าตรวจค้นกว่า 40 จุด ในพื้นที่กรุงเทพมหานคร ปทุมธานี และชลบุรี สามารถจับกุม 4 ผู้ต้องหาชาวจีน และนอมินีคนไทยจดทะเบียนบริษัทและถือหุ้นแทนที่เกี่ยวข้องกับการกระทำความผิดทั้งขบวนการ ตรวจยึดทรัพย์สินเป็นโฉนดที่ดิน บ้าน ห้องชุด รถยนต์หรู ทองรูปพรรณ เงินสด และอื่นๆ รวมมูลค่าประมาณ 3,000 ล้านบาท ซึ่งสอท. จะได้ทำการประสานไปยัง ปปง. เพื่อดำเนินการตามขั้นตอนเฉลี่ยทรัพย์คืนแก่ผู้เสียหาย

จากการสังเกตรูปแบบการกระทำความผิดพบว่า แต่ละกรณีศึกษามีรูปแบบคล้ายกันหรือเป็นไปในทิศทางเดียวกัน ดังแผนภาพ

การหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม



มิจฉาชีพจะสร้างตัวตนปลอมที่แสดงประสบการณ์ด้านการลงทุนในสกุลเงินดิจิทัลออนไลน์ จะมีการทักเหยื่อผ่านสื่อสังคมออนไลน์บนแพลตฟอร์มต่าง ๆ หลังจากนั้นจะพยายามชวนคุย สร้างความรู้จักเพื่อให้เกิดความเชื่อใจมากขึ้น นำไปสู่การแนะนำผู้เชี่ยวชาญด้านการลงทุนเกี่ยวกับสกุลเงินดิจิทัล และส่งลิงก์ให้ดาวน์โหลดแพลตฟอร์มปลอมที่ใช้ในการซื้อ-ขายเหรียญดิจิทัล ให้เหยื่อโอนเงินผ่านบัญชีม้าโดยอ้างว่าเพื่อโอนต่อไปยังบัญชีของแพลตฟอร์มต่างประเทศ หลังจากมีการลงทุนมีการแสดงผลกำไรที่สูงเกินควรเพื่อดึงดูดความสนใจกับเหยื่อ เมื่อลงทุนไประยะหนึ่ง มิจฉาชีพจะสร้างความเชื่อมั่นว่าเหยื่อจะไม่ถูกหลอกโดยวิธีการใดวิธีการหนึ่ง เช่น การส่งสินค้าแบรนด์เนมมาให้เหยื่อเพื่อหลอกให้ตายใจ เมื่อเหยื่อต้องการถอนผลกำไร มิจฉาชีพจะแจ้งว่าจะต้องทำการโอนเงินเข้าบัญชีซื้อ-ขายก่อนและหลอกให้เหยื่อโอนเงินเพิ่มขึ้นเรื่อย ๆ จนเหยื่อเริ่มรู้ตัวและมิจฉาชีพจะทำการตัดขาดการสื่อสารไป จากตัวอย่างคดีที่กล่าวมาจะพบว่ามีผลกระทบต่อการใช้ชีวิตของประชาชนอย่างมีนัยยะสำคัญ ทั้งในแง่ความเชื่อมั่นในการใช้เงิน การลงทุน ความเชื่อมั่นในกระบวนการยุติธรรมสำหรับการจับกุมผู้กระทำความผิด การยึดทรัพย์ผู้กระทำความผิด และการชดใช้ค่าเสียหาย ซึ่งเป็นปัญหาที่มีความท้าทายในปัจจุบัน

<u>ข้อมูลสรุปจากการสัมภาษณ์</u> เจ้าหน้าที่จากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ความว่ากระทรวงฯ มีอำนาจดำเนินการปิดเว็บไซต์ ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กรณีที่มีการกระทำเข้าข่าย หรือมีผู้แจ้งความร้องทุกข์ ส่วนการระงับยับยั้งกรณีการโฆษณาบนสื่อสังคมออนไลน์ เป็นอำนาจของผู้ให้บริการแต่ละแพลตฟอร์ม ยกเว้นว่าเป็นการปลอมแปลงตัวตนเพื่อหลอกลวงผู้อื่นจะต้องมีผู้แจ้งความร้องทุกข์ ผู้เสียหายเป็นผู้ดำเนินการแจ้งยังกระทรวงฯ แล้วกระทรวงจะแจ้งไปยังผู้ให้บริการเพื่อดำเนินการในส่วนที่เกี่ยวข้อง แม้ว่าแต่ละแพลตฟอร์มจะนำระบบปัญญาประดิษฐ์มาใช้ในการตรวจจับผู้เข้าข่ายกระทำความผิด แต่ก็ต้องยอมรับว่ายังไม่ครอบคลุมและไม่สามารถตรวจจับได้ทั้งหมด

2) หลักการแนวคิดวิชาการที่เกี่ยวข้อง

ปัญหาการหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงสกุลเงินดิจิทัลปลอม เป็นลักษณะการหลอกลวงแบบ Hybrid scam ซึ่งเป็นการผสมผสานเทคนิคการหลอกลวงผู้เสียหายให้ไว้ใจหรือเชื่อใจ โดยมุ่งเน้นความอ่อนไหวทางอารมณ์หรือความกังวลในความมั่นคงทางการเงิน จูงใจด้วยผลตอบแทนจากการซื้อ/ขายสกุลเงินดิจิทัลที่ไม่มีราคาตลาดอ้างอิง และหลอกให้เสียทรัพย์โดยการลงทุนผ่านแพลตฟอร์มปลอมหลายรูปแบบ เช่น เว็บไซต์ แอพลิเคชั่น เป็นต้น โดยมีแนวคิดที่เกี่ยวข้อง ดังนี้

การหลอกลวงให้ลงทุน (Investment fraud)[12] หมายถึง การล่อหลอกให้เหยื่อหลงกลแล้วลงทุนเงินหรือทรัพย์สิน อาจเป็นหุ้น พันธบัตร ธนบัตร สินค้าโภคภัณฑ์ สกุลเงิน หรืออสังหาริมทรัพย์ ผู้หลอกลวงมักโกหกหรือให้ข้อมูลเท็จเกี่ยวกับการลงทุน หรืออาจแต่งเรื่องโอกาสการลงทุนปลอม ๆ ขึ้นมาเพื่อหลอกล่อเหยื่อ ตัวอย่างของการหลอกลวงให้ลงทุนที่พบได้บ่อย มีดังนี้

การฉ้อโกงจากความเกี่ยวดอง (Affinity Fraud) เป็นกลวิธีที่ผู้หลอกลวงมักอ้างความเกี่ยวดองกันเพื่อสร้างความไว้วางใจแก่เหยื่อ ไม่ว่าจะเป็นศาสนา เชื้อชาติ คนภูมิภาคเดียวกันเพราะรู้ว่าธรรมชาติของมนุษย์คือการไว้วางใจคนที่เหมือนกับเรา มักถูกใช้ในการหลอกลวงทางการเงินทั่วไป

โปรแกรมการลงทุนที่ให้ผลตอบแทนสูง (High Yield Investment Programs) ผู้หลอกลวงอ้างว่าคุณจะได้รับผลตอบแทนสูงจากเงินของคุณหากคุณลงทุนกับพวกเขา พวกเขาบอกว่าคุณรับประกันได้ว่าจะทำเงินจากการลงทุนได้ บ่อยครั้งการลงทุนเหล่านี้ไม่ใช่ของจริง หรือพวกเขาขายหุ้นที่แทบไม่มีมูลค่า มักถูกใช้ในการหลอกลวงให้ลงทุนในหุ้น หรือสกุลเงินดิจิทัลที่มีความผันผวนแต่ให้ผลตอบแทนสูง เช่น กรณีศึกษาทั้ง 4 กรณี

แชร์ลูกโซ่ (Ponzi Schemes) ผู้ชักชวนลงทุนจะใช้วิธีเสนอผลตอบแทนที่สูงในการลงทุนด้วยแนวทางหลายแบบให้คนถูกหลอกรู้สึกเชื่อถือและประทับใจ แต่แทนที่จะสร้างรายได้อย่างที่สัญญาไว้ก็จะนำเงินของผู้ลงทุนรายใหม่ไปจ่ายผลตอบแทน เงินปันผล หรือดอกเบี้ย แก่ผู้ลงทุนรายก่อน และรายงานผลตอบแทนที่ทำให้คาดหวังว่าจะได้รับผลตอบแทนที่สูงขึ้นในครั้งต่อไป เมื่อธุรกิจนั้นล่มสลาย เจ้าของธุรกิจที่ชวนลงทุนจะได้เงินมหาศาล ขณะคนที่สูญเสียเงินคือผู้ลงทุน

กลโกงปั่นแล้วเท (Pump & Dump) นักต้มตุ๋นจะหาทางเชิญชวนให้ลงทุน หรือโอนเงินกับหุ้น กองทุน สินทรัพย์ดิจิทัล หรือสกุลเงินดิจิทัล ซึ่งอาจมีอยู่จริง หรือไม่มีอยู่จริง โดยให้ข้อมูลหลอกที่น่าเชื่อถือ อ้างว่าเป็นข่าววงใน เมื่อมีราคาหุ้นที่ตอบโตอย่างรวดเร็วเกินความเป็นจริง ผู้ชักชวนก็จะเทขายเอากำไรในระยะสั้นจนราคาหุ้นตกลงไปต่ำกว่าเดิม ขณะที่ผู้ที่ถูกชวนมาลงทุนกลับขาดทุน มักถูกใช้ในการหลอกลวงให้ลงทุนในหุ้น หรือสกุลเงินดิจิทัลที่มีความผันผวนแต่ให้ผลตอบแทนสูง เช่น กรณีศึกษาทั้ง 4 กรณี

ทฤษฎีการจัดการความเสี่ยง (Risk Perception Theory)[13] มิจฉาชีพมักใช้วิธีลดทอนการรับรู้ความเสี่ยงของเหยื่อ โดยเสนอผลตอบแทนสูงในระยะเวลาอันสั้น พร้อมเน้นย้ำว่าความเสี่ยงต่ำหรือไม่มีเลย ผู้เสียหายจึงตัดสินใจลงทุนโดยไม่ได้ตรวจสอบความเสี่ยงอย่างละเอียด เช่น การลงทุนในหุ้นหรือสกุลเงินดิจิทัลที่มีความผันผวนในช่วงระยะเวลาอันสั้น จึงต้องรีบลงทุนเมื่อมีแนวโน้มที่กำไรจะเพิ่มขึ้น เป็นต้น

ทฤษฎีความคาดหวัง (Prospect Theory)[14] ทฤษฎีนี้มีอิทธิพลอย่างมากต่อการศึกษาพฤติกรรมมนุษย์ในด้านจิตวิทยาเศรษฐกิจ (Behavioral Economics) ทฤษฎีนี้อธิบายว่าผู้คนมักจะยอมรับความเสี่ยงเมื่อเผชิญกับโอกาสที่จะได้ผลตอบแทนสูง แม้จะมีความไม่แน่นอนสูง มิจฉาชีพจึงใช้วิธีการชักจูงด้วยโอกาสทำกำไรจำนวนมากในเวลาอันสั้น เพื่อให้เหยื่อตัดสินใจเร็ว และมิจฉาชีพจะใช้กระตุ้นเหยื่อที่มีความอ่อนไหวต่อการสูญเสียมากกว่ากำไรในระดับเดียวกัน เช่น การขาดทุน 100 บาท ต้องลุทนเพิ่มเป็น 2 เท่าเพื่อให้ได้ส่ วน ที่ขาดทุนคืนมา เป็นต้น ซึ่งใช้ได้กับทั้งการลงทุนและการพนัน

ทฤษฎีการโน้มน้าวใจ (Persuasion Theory)[15] ทฤษฎีการชักชวนอธิบายถึงวิธีการที่ข้อความสามารถเปลี่ยนแปลงทัศนคติหรือพฤติกรรมของบุคคลได้ โดยพิจารณาจากหลายปัจจัย เช่น ความน่าเชื่อถือของผู้ส่งสาร, เนื้อหาของข้อความ, ความสนใจของผู้รับสาร, และวิธีการที่ใช้ในการสื่อสาร มิจฉาชีพสามารถใช้เทคนิคการโน้มน้าวใจ เช่น การใช้ความน่าเชื่อถือของบุคคล การเร่งรัดเวลา และการใช้แรงกดดันจากกลุ่มทฤษฎีนี้อธิบายว่าการใช้วิธีเหล่านี้ช่วยลดความลังเลของเหยื่อ และเพิ่มโอกาสในการตัดสินใจลงทุน

ทฤษฎีความกลัวตกกระแส (Fear of Missing Out - FOMO)[16] เป็นแนวคิดที่เกิดขึ้นจากการศึกษาพฤติกรรมมนุษย์ในสังคมยุคดิจิทัล และเป็นปรากฏการณ์ทางจิตวิทยาที่อธิบายถึงความรู้สึกวิตกกังวลที่เกิดขึ้นเมื่อคนรู้สึกว่าพวกเขากำลังพลาดโอกาสหรือประสบการณ์ที่คนอื่นกำลังทำหรือได้รับ ซึ่งอาจทำให้พวกเขาตัดสินใจทำสิ่งใดสิ่งหนึ่งเพื่อไม่ให้พลาดไป มิจฉาชีพใช้กลยุทธ์กระตุ้นให้เกิดความกลัวของเหยื่อว่าจะพลาดโอกาสที่ดีในการลงทุน เช่น “ลงทุนตอนนี้ก่อนจะสายเกินไป” ทฤษฎี FOMO อธิบายว่าผู้คนมักจะตัดสินใจเร็วขึ้นเมื่อรู้สึกว่าตนเองอาจพลาดโอกาสสำคัญ

ทฤษฎีไร้ตัวตน (Theories of Anonymity) เป็นแนวคิดที่เกี่ยวข้องกับการศึกษาพฤติกรรมและปรากฏการณ์ที่เกิดขึ้นเมื่อบุคคลไม่มีการเปิดเผยตัวตนในสื่อหรือแพลตฟอร์มออนไลน์ เช่น โซเชียลมีเดีย, ฟอรัมออนไลน์, หรือการสื่อสารทางอินเทอร์เน็ตอื่นๆ ที่ทำให้บุคคลสามารถปกปิดตัวตนได้ John Suler[17] นักจิตวิทยาชาวอเมริกันได้ศึกษาเกี่ยวกับพฤติกรรมออนไลน์และเสนอแนวคิดที่เรียกว่า "The Online Disinhibition Effect" ซึ่งอธิบายถึงการที่ผู้คนแสดงพฤติกรรมที่แตกต่างไปจากการแสดงออกในชีวิตจริงเมื่อพวกเขามีความสามารถในการซ่อนตัวตนทางออนไลน์ ซึ่งสอดคล้องกับรูปแบบการกระทำความผิดของมิจฉาชีพที่หลอกลวงเหยื่อให้ลงทุนออนไลน์โดยปราศจากการพบเจอตัวตน

ทฤษฎีเปลี่ยนพื้นที่ (Space Transition Theory)[18] ทฤษฎีนี้แสดงให้เห็นว่าเมื่อบุคคลเปลี่ยนที่หรือ "ย้าย" พฤติกรรมจากโลกแห่งความจริง เช่น การหลอกลวงทางออนไลน์ การโจรกรรมข้อมูลหรือการกระทำผิดกฎหมายอื่น ๆ เนื่องจากไม่ต้องเผชิญหน้ากับผลกระทบทางสังคมและกฎหมายที่ชัดเจนเช่นเดียวกับการหลอกให้ลงทุนบนแพลตฟอร์มปลอม มิจฉาชีพไม่ต้องพบหรือรู้จักกับเหยื่อในโลกความเป็นจริงแต่สามารถสร้างความสนิทชิดเชื้อกับเหยื่อในโลกเสมือนจริงได้อย่างแนบเนียนกว่า

ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory)[19] เป็นทฤษฎีที่อธิบายถึงเงื่อนไขที่ทำให้เกิดการกระทำอาชญากรรม ซึ่งอาชญากรรมจะเกิดขึ้นเมื่อมีองค์ประกอบครบ 3 ประการดังนี้

1. เหยื่อ (Victim) หมายถึง บุคคล สถานที่ วัตถุ หรือองค์กรที่อาชญากรหมายมุ่งประกอบอาชญากรรมสร้างความเสียหายเพื่อให้ตนได้อรรถประโยชน์

2. โอกาส (Opportunity) หมายถึง ช่วงเวลาและสถานที่ ที่เหมาะสมที่อาชญากรเชื่อว่าสามารถลงมือก่ออาชญากรรมได้หรือเชื่อว่าไม่มีใครจะจับได้

3. อาชญากร (Criminal/Offender) หมายถึง ผู้ที่มีความต้องการจะก่ออาชญากรรมโดยแสวงหาโอกาสตลอดเวลาจากเหยื่อที่อ่อนแอ

กรณีการหลอกให้ลงทุนออนไลน์กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม องค์ประกอบตามสามเหลี่ยมอาชญากรรมครบถ้วน ได้แก่ มิจฉาชีพที่ใช้ข้อมูลและเครื่องมือทางออนไลน์ เหยื่อที่รู้ไม่เท่าทันโลภ และโอกาสที่เป็นช่วงเวลา สิ่งแวดล้อม และสภาวะที่ขาดการควบคุม/ตรวจสอบจากหน่วยงานที่เกี่ยวข้อง

3) วิธีการศึกษา การวิเคราะห์วิพากษ์เกี่ยวกับประเด็นที่ศึกษา

คณะผู้ศึกษาได้ใช้วิธีดำเนินการศึกษาอยู่ภายใต้วัตถุประสงค์ อันเป็นไปเพื่อศึกษาข้อเท็จจริงรูปแบบการกระทำความผิด และสาเหตุของการเกิดอาชญากรรม ตลอดทั้งเพื่อนำเสนอแนวทาง นวัตกรรมการป้องกันและแก้ไขการหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม โดยการอาศัยวิธีการรวบรวมข้อมูลต่าง ๆ อันได้แก่

- การศึกษาวิจัยเอกสาร (Documentary Research) เป็นข่าวสารกรณีการหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม จำนวน 4 คดี และงานวิจัย บทความวิชาการ บทความทางสื่อออนไลน์ในเนื้อหาทฤษฎีที่เกี่ยวข้องทั้งทางด้านอาชญวิทยา จิตวิทยา และสังคมวิทยา

- การประชุมกลุ่มจำนวน 3 ครั้ง เพื่อระดมและแลกเปลี่ยนความคิดเห็นบนพื้นฐานของทฤษฎีที่เกี่ยวข้อง และนำข้อมูลดังกล่าวมาวิเคราะห์ในประเด็นที่ศึกษาเพื่อนำมาข้อมูลที่ได้มาเสนอแนวทางในการป้องกันอาชญากรรมต่อไป

- ข้อมูลจากการสัมภาษณ์ผู้แทนจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จำนวน 1 ท่าน

3.1 การวิเคราะห์วิพากษ์เกี่ยวกับประเด็นที่ศึกษา

การหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม เมื่อวิเคราะห์เกี่ยวกับประเด็นปัญหาดังกล่าว ตามหลัก CHEERS Model แล้ว สามารถตอบคำถามพื้นฐานทั้ง 6 ข้อ ได้ดังนี้

(1) ชุมชน (Community) ส่งผลกระทบทั้งที่เป็นผู้เสียหายโดยตรง (นักลงทุน, ผู้มีความสนใจในการลงทุน ผู้เสียหายทางอ้อม (ครอบครัว, บุคคลใกล้ชิด) รวมถึงเศรษฐกิจและสังคมของประเทศ

(2) ความรุนแรงของอาชญากรรม (Harm) อาชญากรรมทางไซเบอร์ ที่มีมูลค่าความเสียหายมากที่สุด คือ การหลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ ซึ่งในส่วนของการหลอกลวงให้ลงทุนออนไลน์ กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม ซึ่งจากกรณีศึกษาจะพบว่ามีมูลค่าความเสียหายรวมกว่า 10,000 ล้านบาท ในห้วงระยะเวลาประมาณ 3 ปี

(3) ความคาดหวัง (Expectation) โดยแบ่งเป็น 2 ส่วน

(3.1) ผู้เสียหาย มีความต้องการเรียกร้องค่าเสียหายคืนจากการถูกหลอกลวง และต้องการให้ผู้กระทำความผิดได้รับโทษทางกฎหมาย

(3.2) ส่วนของประชาชนและสังคม ซึ่งมีประชาชนและสังคมบางกลุ่มเท่านั้นที่ให้ความสนใจในการป้องกัน ปรามปราบ เช่น กลุ่มนักลงทุน หรือ กลุ่มผู้ที่มีความสนใจในสกุลเงินดิจิทัล ส่วนประชาชนบางกลุ่มอาจมองว่าเป็นเรื่องไกลตัว

(4) กิจกรรม (Event) ลักษณะของการก่อเหตุ จะมีรูปแบบคือ มีการสร้างโปรไฟล์ปลอมและโฆษณาชวนเชื่อถึงผลกำไรที่เกินจริงในโซเชียล และมีการชวนคุยเพื่อตีสนิท เมื่อหลอกได้สำเร็จแล้วจะมีการแนะนำผู้เชี่ยวชาญด้านการลงทุนในเหรียญคริปโตเคอร์เรนซี พร้อมทั้งโน้มน้าวและส่งลิ้งค์แพลตฟอร์มเทรดคริปโตเคอร์เรนซีเพื่อให้เปิดบัญชีเพื่อทำการเทรดในแพลตฟอร์มปลอม จากนั้นเมื่อเหยื่อหลงเชื่อ จะโน้มน้าวให้ลงทุนเพิ่มขึ้น และไม่สามารถถอนเงินออกมาได้

(5) เหตุการณ์ที่เกิดขึ้นซ้ำๆ (Recurring) การถูกหลอกให้เทรดคริปโตเคอร์เรนซีบนแพลตฟอร์มปลอมต่าง ๆ เช่น VTPTRADE, Digitalbase, ftt token, www.sgx-ex.com, กระดานเทรด tmx.pwwb.live เป็นต้น

(6) ความคล้ายคลึงกัน (Similarity) อาชญากรรมที่มีลักษณะใกล้เคียงกัน เช่น แชร์แม่มณี แชร์ลูกโซ่น้ำมันหอมระเหย,หลอกลงทุนหุ้นในแพลตฟอร์มปลอม (แอพพลิเคชั่น Taining) เป็นต้น

สาเหตุของความเสียหายมาอาจจากหลายปัจจัย ประกอบด้วย

(1) การลงทุนกับสกุลเงินดิจิทัลเป็นเรื่องใหม่และซับซ้อน ผู้เสียหายส่วนใหญ่นอกจากจะไม่มีความรู้หรือความเข้าใจที่เพียงพอเกี่ยวกับสกุลเงินดิจิทัล (Cryptocurrency) หรือเทคโนโลยีเบื้องหลัง เช่น บล็อกเชน (Blockchain) ในการดำเนินการ ไม่มีความรู้ในการประเมินความเสี่ยง หรือการตรวจสอบว่าโครงการหรือแพลตฟอร์มนั้นถูกต้องตามกฎหมายหรือไม่ การขาดความรู้ทำให้พวกเขาไม่สามารถแยกแยะการหลอกลวงจากการลงทุนที่ถูกต้องได้ และยังมีทัศนคติต่อการลงทุนที่คาดหวังผลตอบแทนเกินจริงหรือโลภทำให้ผู้คนตกเป็นเหยื่อคือการเสนอโอกาสในการลงทุนที่ให้ผลตอบแทนสูงมากในระยะเวลาสั้น ๆ ซึ่งดูเหมือน

จะเป็นโอกาสที่ไม่สามารถพลาดได้ ผู้ลงทุนมักจะรู้สึกว่าต้องรีบลงทุนเพื่อไม่ให้พลาดโอกาสทอง และตกเป็นเป้าหมายของมิจฉาชีพได้ง่าย

(2) ผู้กระทำความผิด มีความรู้เทคนิคทางจิตวิทยาในการสร้างความเชื่อใจมักอ้างว่ามีชื่อเสียง มีประวัติการลงทุนที่ดี หรืออ้างถึงบุคคลที่น่าเชื่อถือ ทำให้ผู้คนหลงเชื่อและโอนเงินไปลงทุน หรือกลยุทธ์กดดันให้ลงทุนรวดเร็วโดยใช้ความกลัวการพลาดโอกาส (FOMO) เช่น โอกาสมีจำกัด รีบลงทุนภายในวันนี้ เพื่อกระตุ้นให้ผู้คนตัดสินใจโดยไม่คิดให้รอบคอบ รวมถึง การหลอกลวงแบบ Ponzi Scheme หรือระบบแชร์ลูกโซ่ ที่ใช้เงินของผู้ลงทุนใหม่มาจ่ายให้ผู้ลงทุนเก่า ทำให้ดูเหมือนว่าการลงทุนได้ผลกำไรจริง

(3) สภาพแวดล้อม

- แพลตฟอร์มปลอม การลงทุนในคริปโตเคอร์เรนซีต้องดำเนินการผ่านแพลตฟอร์มออนไลน์ทำให้การลงทุนเข้าถึงได้ง่าย มิจฉาชีพจึงใช้โอกาสนี้สร้างเว็บไซต์หรือแอปพลิเคชันปลอมที่ดูคล้ายแพลตฟอร์มลงทุนจริง หรือโครงการที่ไม่มีอยู่จริง แต่ดูน่าเชื่อถือ

- การใช้สื่อสังคมออนไลน์ วิจารณญาณการใช้สื่อสังคมออนไลน์และการตอบสนองต่อโฆษณาชวนเชื่อที่ชี้ชวนเรื่องการลงทุนกับสกุลเงินดิจิทัล

- เทรนด์การลงทุนโดยสกุลเงินดิจิทัล กำลังได้รับความนิยมอย่างรวดเร็วทั่วโลก เนื่องจากการเติบโตของเทคโนโลยีบล็อกเชนและสกุลเงินดิจิทัลที่ทำให้การลงทุนในสินทรัพย์ดิจิทัลเป็นที่นิยมมากขึ้น แม้ว่าตลาดที่มีความผันผวนสูง นักลงทุนจำนวนมากยังมองเห็นศักยภาพของสินทรัพย์ดิจิทัลนี้ หากเลือกลงทุนในโครงการที่มีพื้นฐานที่แข็งแกร่งและวิสัยทัศน์ที่ชัดเจน อาจได้ผลตอบแทนที่ดี

ในปัจจุบันมีแนวทางในการแก้ไขป้องกันและแก้ไขปัญหาการหลอกลวงให้ลงทุนออนไลน์ ได้แก่

(1) การหลอกลวงในการลงทุนสกุลเงินดิจิทัลบนแพลตฟอร์มปลอมในประเทศไทย เป็นอาชญากรรมที่มีบทลงโทษหลายข้อจากหลายกฎหมาย

(1.1) ประมวลกฎหมายอาญา ความผิดฐานฉ้อโกง (มาตรา 341-343) โดยมีโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 6,000 บาท หรือทั้งจำทั้งปรับ

(1.2) พระราชบัญญัติการทำธุรกรรมทางการเงินด้วยระบบอิเล็กทรอนิกส์ พ.ศ. 2562 การรับเงินจากผู้ลงทุนผ่านทางเว็บไซต์หรือแพลตฟอร์มที่ไม่ใช่ตัวแทนที่ถูกต้องตามกฎหมาย การกระทำดังกล่าวอาจถูกดำเนินคดีตามพระราชบัญญัติการทำธุรกรรมทางอิเล็กทรอนิกส์

(1.3) พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 โดยมีโทษจำคุกตั้งแต่ 1-3 ปี และ/หรือปรับไม่เกิน 2 ล้านบาท หรือทั้งจำทั้งปรับ

(1.4) พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 หากการหลอกลวงนั้นเกี่ยวข้องกับการฟอกเงินจากผลกำไรที่ได้จากการหลอกลวง (เช่น การใช้คริปโตเคอร์เรนซีเพื่อฟอกเงินจากการหลอกลวง) จะต้องรับผิดตาม พระราชบัญญัติการฟอกเงิน โดยบทลงโทษสำหรับการฟอกเงินอาจมีทั้งโทษจำคุก และปรับเป็นจำนวนมาก โดยโทษจำคุกสูงสุดไม่เกิน 10 ปี และปรับไม่เกิน 1,000,000 บาท

(1.5) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 หากมีการหลอกลวงผ่านช่องทางออนไลน์ เช่น เว็บไซต์ปลอม แอปพลิเคชัน หรือการใช้สื่อโซเชียลมีเดียในการหลอกลวง การกระทำดังกล่าวถือเป็นความผิด โทษสูงสุดอาจมีการจำคุกสูงสุดไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

(1.6) พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หากมีการหลอกลวงที่เกี่ยวข้องกับการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของผู้ลงทุนโดยไม่ได้รับการยินยอม หรือมีการใช้ข้อมูล

เพื่อจุดประสงค์ที่ไม่ถูกต้อง มีบทลงโทษที่เกี่ยวข้องกับการละเมิดสิทธิความเป็นส่วนตัว ซึ่งอาจมีโทษทั้งทางอาญาและทางแพ่ง

(2) การประชาสัมพันธ์ ได้แก่

(2.1) การแจ้งเตือนและให้ข้อมูลเพื่อไม่ให้ถูกหลอกลงทุนในแพลตฟอร์มปลอม ในลักษณะบทความ Infographic วิดีโอคลิปสั้น ข่าวสาร โดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สื่อสารมวลชน และธนาคารต่างๆ ทั้งรัฐและเอกชน

(2.2) การให้ความรู้ในเรื่องการลงทุนสกุลเงินดิจิทัล โดยหน่วยงานเอกชน เช่น Binance TH Bitkub สื่อสารมวลชน และธนาคารต่างๆ ทั้งรัฐและเอกชน

(2.3) แหล่งข้อมูลตรวจสอบแพลตฟอร์มในการเทรดสกุลเงินดิจิทัลที่ถูกต้องตามกฎหมาย โดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

อย่างไรก็ตาม ในการประชาสัมพันธ์แจ้งเตือนกลวิธีในการหลอกลงทุนบนแพลตฟอร์มปลอม และการให้ความรู้ในการเรื่องการลงทุนสกุลเงินดิจิทัล รวมทั้งการตรวจสอบแพลตฟอร์มที่ถูกต้องตามกฎหมายในการเทรดคริปโตเคอร์เรนซี ยังไม่สามารถแก้ไขปัญหาในประเด็นของเหยื่อหรือเป้าหมาย ซึ่งเป็นหนึ่งในองค์ประกอบของสามเหลี่ยมอาชญากรรมได้

ส่วนที่ 3 บทสรุปและข้อเสนอแนะ :

เพื่อเป็นการป้องกันการเกิดอาชญากรรม กลุ่มผู้จัดทำขอเสนอนวัตกรรมเน้นการป้องกันความเสียหายและลดโอกาสการเกิดอาชญากรรม ดังนี้

1. การแสดงข้อความแจ้งเตือน (pop-up) บนแอพพลิเคชันของธนาคาร ที่ผู้ใช้บริการสามารถกดข้ามได้หลังจาก 3 วินาที เพื่อเตือนผู้ใช้บริการให้ระวังมิจฉาชีพหลอกลงทุน/ตรวจสอบบัญชีม้าบนแอพพลิเคชัน Cyber Check ที่ถูกสร้างและพัฒนาโดยกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) หรือกองบัญชาการตำรวจไซเบอร์ จากการบูรณาการฐานข้อมูลร่วมกันกับทั้งหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง อาทิ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) และธนาคารแห่งประเทศไทย (ธปท.) ทั้งนี้ อาจมีการนำมาตรการหน่วงเวลาหรือการชะลอการโอนเงินมาใช้เพิ่มเติมเมื่อมีการโอนเงินจำนวนมากกว่าที่กำหนด หรือมีการโอนเงินไปยังบัญชีปลายทางที่ไม่เคยโอนมาก่อน เพื่อให้สามารถยับยั้งไม่ให้เงินถูกโอนไปยังปลายทางได้ เมื่อพบว่าบัญชีปลายทางอาจเป็นบัญชีม้าหรือบัญชีของมิจฉาชีพ

2. การประชาสัมพันธ์ด้วยแคมเปญ “**Sure ก่อน Choose**” ในลักษณะ Clip VDO และ Spot สั้น 1-3 นาที ผ่านทางสื่อสังคมออนไลน์ (Social Media) โทรทัศน์ วิทยุ และเสียงตามสาย เกี่ยวกับการลงทุนในสกุลเงินดิจิทัลและการหลอกลวงให้ลงทุน เพื่อให้เข้าถึงประชาชนทั้งในชุมชนเมืองและต่างจังหวัด โดย กรมประชาสัมพันธ์ ร่วมกับกระทรวงมหาดไทย และคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และประสานความร่วมมือกับกรุงเทพมหานครในการประชาสัมพันธ์บนขบวนรถ/ชานชลาของรถไฟฟ้าบีทีเอสและการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยในการประชาสัมพันธ์บนขบวนรถ/ ชานชลาของรถไฟฟ้ามหานคร สำหรับกลุ่มประชาชนที่อยู่ในเมือง โดยเฉพาะวัยทำงาน เพื่อช่วยลดความเสี่ยงที่อาจเกิดขึ้นจากการหลอกลวงหรือการลงทุนที่ไม่มั่นคงในพื้นที่ชุมชน ซึ่งการได้รับข้อมูลข่าวสารอย่างสม่ำเสมอ จะส่งผลให้ผู้ลงทุนเกิดความสนใจและตระหนักรู้ ด้วยการ DYOR (Do Your Own Research) ต่อยอดไปค้นคว้าศึกษา

รายละเอียดของแพลตฟอร์มการลงทุนที่ระบุในเอกสารนำเสนอข้อมูล (Whitepaper) ก่อนตัดสินใจลงทุนในแพลตฟอร์มการลงทุนมากกว่าเชื่อถือตามกระแสที่ได้รับ อีกทั้ง ผู้ลงทุนยังสามารถพิจารณาและตั้งข้อสังเกตความน่าเชื่อถือของเจ้าของแพลตฟอร์มการลงทุน มีตัวตนจริงหรือไม่ และความเป็นไปได้ของผลตอบแทนที่จะได้รับความสมเหตุสมผลของราคาซื้อขายในขณะนั้น ตลอดจนความปลอดภัยของแพลตฟอร์มที่ได้รับการตรวจสอบโค้ด (Code Audit) จากบริษัท ผู้ตรวจสอบ (Auditor) ที่น่าเชื่อถือแม้จะมีบางกรณีจะไม่สามารถตรวจสอบกลโกงที่ซ่อนไว้ได้ทั้งหมดก็ตาม

3. การฝึกอบรมให้ความรู้เรื่อง สกุลเงินดิจิทัล การประเมินความเสี่ยงในการลงทุน กลโกงในโลกคริปโตเคอร์เรนซี เป็นขั้นตอนสำคัญในการป้องกันการถูกหลอกให้ลงทุนระดับพื้นที่ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเจ้าภาพหลัก นำกลไกอาสาสมัครดิจิทัลชุมชนร่วมกับกระทรวงมหาดไทย และเจ้าหน้าที่ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ในการดำเนินการ เพื่อเสริมสร้างความเข้าใจเกี่ยวกับการลงทุนในสกุลเงินดิจิทัล และผลักดันให้เป็นกลไกการป้องกันการอาชญากรรมทางเทคโนโลยี ผ่านการอบรมให้เป็นแกนนำอาสาสมัครดิจิทัลชุมชนยกระดับเป็นผู้ที่มีองค์ความรู้ทางคอมพิวเตอร์และความเชี่ยวชาญด้านเทคโนโลยีบล็อกเชนและสินทรัพย์ดิจิทัล ผ่านเวทีการแข่งขัน พัฒนาความคิดสร้างสรรค์และสร้างนวัตกรรมแบบเร่งด่วน (Hackathon) ด้วยการให้เงินรางวัล หรือทุนสนับสนุนในบริบทของชุมชนที่มีความพร้อมและมีศักยภาพในการพัฒนาต่อไป

<u>ข้อเสนอแนะ</u>

ยุคสมัยที่เปลี่ยนแปลงอย่างรวดเร็วไปพร้อมกับกระแสเทคโนโลยีที่เปลี่ยนแปลงไปอย่างต่อเนื่องไม่มีวันสิ้นสุด และย่อมสะท้อนผลลัพธ์ออกมาเป็น ความเสี่ยงจากอาชญากรรมทางเทคโนโลยี (Cybercrime) นับวันจะทวีความเสียหายจากนักลงทุนที่ต้องสูญเสียสินทรัพย์มูลค่ามหาศาลและยากต่อการติดตาม ซึ่งประเด็นที่ทางกลุ่มได้หยิบยกนำมาเป็นเพียงแค่ส่วนหนึ่งเท่านั้น จึงเป็นประเด็นที่ต้องผลักดันเป็นวาระแห่งชาติของรัฐบาล ที่จะต้องมีมิติของการป้องกันอาชญากรรมทางเทคโนโลยีด้วยองค์ประกอบ 3 มิติ ตามหลักของทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ดังนี้

1. มิติของผู้ที่มีความสามารถในการก่ออาชญากรรม : ด้วยการเพิ่มโทษผู้กระทำผิดให้หนักขึ้น เพิ่มการรับรู้และเพิ่มความเสี่ยงการถูกจับกุมผู้ที่มีความสามารถในการก่ออาชญากรรม เมื่อมีการดำเนินการที่มากเกินกว่าประโยชน์ที่พึงได้รับและมีความกังวลต่อความเสี่ยงในการถูกจับกุม กับผลกระทบที่จะตามมาภายหลังถูกจับกุม ส่งผลให้ไม่ตัดสินใจที่จะก่ออาชญากรรมทางเทคโนโลยี

2. มิติของนักลงทุนสินทรัพย์ดิจิทัล : ประชาชนทุกภาคส่วนในสังคมจะต้องเรียนรู้จักการ DYOR (Do Your Own Research) เพื่อเสริมสร้างให้นักลงทุนมีความรู้เท่าทัน ในการเข้าไปมีส่วนร่วมในเครือข่ายทางสังคมในการปฏิสัมพันธ์ระหว่างสมาชิกในชุมชน นักลงทุนสินทรัพย์ดิจิทัล (Online Community) ด้วยกันเองและกับผู้มีอิทธิพลทางความคิด ด้านการเงิน (FinFluencer) มีการรับสารผ่านช่องทางการ (Official) ซึ่งอาจมีกิจกรรมเชิญชวน การให้คำแนะนำ ให้ข้อมูลอย่างต่อเนื่อง โฆษณาเชิญชวนให้เกิดการลงทุน เพื่อป้องกันการคล้อยตามและความไว้วางใจที่อาจเกิดขึ้น ก่อนพลั้งพลาดไป

3. มิติของผู้พิทักษ์ : ด้วยการเพิ่มศักยภาพผู้รับผิดชอบ สอดส่อง เฝ้าระวัง การกำกับดูแลบังคับใช้บังคับใช้กฎหมายที่เกี่ยวกับ สินทรัพย์ดิจิทัลที่เป็นสากลและชัดเจน พิจารณาออกกฎหมาย หรือออกบทบัญญัติเพิ่มเติม ตลอดจนการพัฒนาระบบฐานข้อมูล บนแอพพลิเคชั่น Cyber Check โดยการนำเข้าข้อมูลให้มากขึ้นและเป็นปัจจุบัน เพื่อให้ครอบคลุมการค้นหาและตรวจสอบมิจฉาชีพ จากการบูรณาการความร่วมมือระหว่างหน่วยงาน การบูรณาการร่วมกันทั้งหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง อาทิ สำนักงานคณะกรรมการกำกับ

หลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) และธนาคารแห่งประเทศไทย (ธปท.) เพื่อลดทอนโอกาสที่อาจก่อให้เกิดปัญหาอาชญากรรมทางเทคโนโลยีในอนาคต

ส่วนที่ 4 บรรณานุกรม

[1] ศูนย์บริหารรับบริการแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ. (2565-2567).

[2] Statista. (2024). *Most commonly reported cybercrime categories in the United States in 2023, by number of individuals affected.* https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-us/

[3] ThaiPBSNews. (2567). *มิจฉาชีพรูปแบบ Hybrid Scam หลอกเหยื่อโดยปลอมโปรไฟล์ | Thai PBS News* [Video]. YouTube. https://www.youtube.com/watch?v=1wmk-F835pw

[4] เรวัตร เปรมศรี. (2564). *Online Scam.* สืบค้นจาก https://www.nsm.or.th/nsm/th/node/5702

[5] Planet 46. (2567). *คริปโทเคอร์เรนซี (Cryptocurrency) คืออะไร? พามือใหม่เข้าใจครบจบในที่เดียว!* สืบค้นจาก https://www.finnomena.com/planet46/what-is-cryptocurrency/

[6] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2567). *Digital Platform (ประเด็นเกี่ยวกับกฎหมาย).* สืบค้นจาก https://www.etda.or.th/th/contact/faq/Digital-Platform.aspx

[7] ไทยรัฐออนไลน์. (2567). *ต้มคริปโต เสียหาย 530 ล้าน ล่อลวงลงทุน หมายจับมี 90 ลากคอ 23 ราย.* สืบค้นจาก https://www.thairath.co.th/news/local/central/2780445 [ค้นวันที่ 11 มกราคม 2567]

[8] กรุงเทพธุรกิจ. (2567). *ล่า! จับแก๊งหลอกเทรดสกุลเงินดิจิทัล พบเหยื่อหลายร้อยราย.* สืบค้นจาก https://www.bangkokbiznews.com/finance/cryptocurrency/1126716 [ค้นวันที่ 11 มกราคม 2567]

[9] มติชน ออนไลน์. (2566). *รวบยกแผง แก๊งหลอกลงทุนคริปโท ตุ๋นซื้อเหรียญ ETH สูญเงินกว่า 1.5 ล้าน.* สืบค้นจาก https://www.matichon.co.th/local/news_4045148 [ค้นวันที่ 11 มกราคม 2567]

[10] Ethereum. (2025). Ethereum. Ethereum.org. สืบค้นจาก https://ethereum.org

[11] สอท. (2566). *ตร.ไซเบอร์แถลงปฏิบัติการ TRUST NO ONE EP.4* [โพสต์บน Facebook]. สืบค้นจาก https://www.facebook.com/share/p/1BAnZm3JLT/

[12] Jonathan Skrmetti. (2024). *What You Need to Know about Investment Scams*. สืบค้นจาก https://www.tn.gov/attorneygeneral/working-for-tennessee/consumer/resources/materials/investment-scams.html [สืบค้นเมื่อ 16 มกราคม 2568]

[13] Slovic, P. (1987). *Perception of Risk. Science*, 236(4799), 280-285.

[14] Kahneman, D., & Tversky, A. (1979). *Prospect Theory: An Analysis of Decision under Risk. Econometrica*, 47(2), 263-291.

[15] Hovland, C., Janis, I. L., & Kelley, H. H. (1953). *Communication and Persuasion: Psychological Studies of Opinion Change.*

[16] Solomon, M. R. (2016). *Consumer Behavior: Buying, Having, and Being*. Pearson Education.

[17] Suler, J. (2004). *The Online Disinhibition Effect.* CyberPsychology & Behavior, 7(3), 321-326.

[18] Felson, M., & Cohen, L. E. (1980). *Social Change and Crime Rate Trends: A Routine Activity Approach.* American Sociological Review, 45(6), 588-608.

[19] Felson, M., & Cohen, L. E. (1980). *Social Change and Crime Rate Trends: A Routine Activity Approach.* American Sociological Review, 45(6), 588-608

[20] กุลนันทน์ ศรีเจริญ. (2566). *แนวทางการป้องกันอาชญากรรมบนเทคโนโลยีการเงินแบบกระจายศูนย์ (DeFi) : กรณีศึกษาปรากฏการณ์ล้มทั้งยืน (Rug Pull).* คณะรัฐศาสตร์:วิทยานิพนธ์ของการศึกษาระดับศิลปศาสตรดุษฎีบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย.

ส่วนที่ 5 ภาคผนวก

เอกสารนำเสนอ “One Page Summary”