นวัตกรรม เพื่อป้องกันอาชญากรรมทางเทคโนโลยี

Crime 8 PREVENTION

ประเทศไทย

37.3
(Crime Index*)
ณ 25 มกราคม พ.ศ. 2568

ดัชนีอาชญากรรม
ลำดับ 98 จาก 147 ประเทศทั่วโลก
หรือลำดับ 25 จาก 45 ประเทศ
ในภูมิภาคเอเชีย

ประเทศสิงคโปร์
ลำดับ 139 ของโลก
22.6 และลำดับที่ 39 ในภูมิภาคเอเชีย

ข้อมูลจาก: www.numbeo.com
*ดัชนีอาชญากรรม (Crime index) เป็นการนับข้อมูลแบบ update continuously

มูลค่า

ความเสียหาย (1 มกราคม - 31 ธันวาคม 267) ข้อมูลจาก: ThaiPoliceOnline

6,092,337,832 บาท

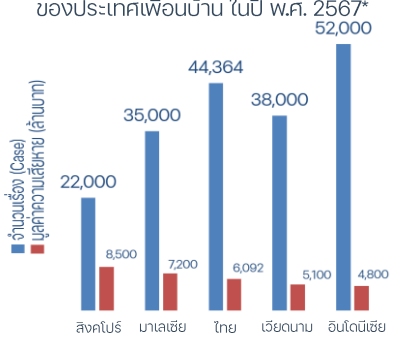
44,364 ราย* (Case)

1. โทรศัพท์ และข้อความ (SMS)
2. โซเชียลมีเดีย (Social media)
3. ข้อความผ่านสื่ออื่น ๆ (Instant messages)
4. ช่องทางอื่น ๆ
5. เว็บไซต์ (Website)

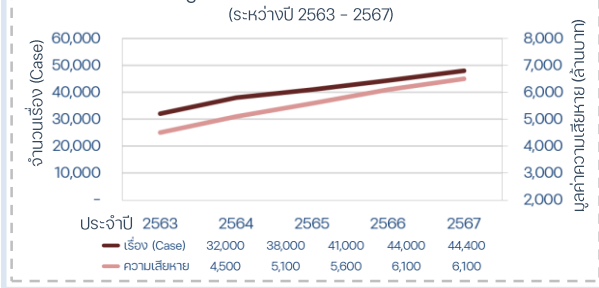
ร้อยละ 51.10 ลงทะเบียนมั่ว + ร้อยละ 22.90 ลงทะเบียนถูกต้อง + ร้อยละ 16.40 อาจเป็น passport

16,204 เบอร์โทรที่ถูกระงับ

สถิติอาชญากรรมทางเทคโนโลยีของประเทศเพื่อนบ้าน ในปี พ.ศ. 2567*



สถิติอาชญากรรมทางเทคโนโลยีของประเทศไทย* (ระหว่างปี 2563 - 2567)



ประจำปี	2563	2564	2565	2566	2567
เรื่อง (Case)	32,000	38,000	41,000	44,000	44,400
ความเสียหาย	4,500	5,100	5,600	6,100	6,100

*ประมวลผลโดยอ้างอิงข้อมูลจากสำนักงาน ปปง. Interpol cybercrime Report และ ASEAN CERT Incident Report

กลุ่ม 1 การเวก
การป้องกันอาชญากรรมทางไซเบอร์
ศึกษาเฉพาะกรณี การประทุษกรรมทางการเงิน ของเจ้าหน้าที่องค์กรปกครองส่วนท้องถิ่น

กลุ่ม 2 กาสะลอง
แนวทางการป้องกันอาชญากรรมทางเทคโนโลยี กรณีศึกษา ซิมม้า

กลุ่ม 3 จามจุรี
การหลอกลวงจากการซื้อของออนไลน์
(Online Shopping Scams)

กลุ่ม 4 ปาริชาต
การหลอกลวงให้ลงทุนออนไลน์
กรณีแพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม

กลุ่ม 5 พุทธรักษา
มาตรการป้องกันอาชญากรรมทางไซเบอร์
ศึกษาเฉพาะกรณี การประทุษร้ายบนโลกไซเบอร์ (Cyber-bullying)

ปักหมุดพื้นที่เสี่ยง

ต่อการเกิดเหตุอาชญากรรมที่มาจากการศึกษาของ 5 กลุ่ม โดยพิจารณาจาก*

1. สถิติการแจ้งความ
2. มูลค่าความเสียหาย
3. การเข้าถึงอินเตอร์เน็ต และการใช้สมาร์ทโฟน
4. กลุ่มประชากร

*ประมวลผลโดยอ้างอิงข้อมูลจากสำนักงานตำรวจแห่งชาติ ธนาคารแห่งประเทศไทย สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ สำนักงานสถิติแห่งชาติ

แผนประทุษกรรม

และความเชื่อมโยงของ 5 เหตุการณ์

(การเตรียมการ การดำเนินการ และการหลบหนี)


การประทุษกรรมทางการเงินของเจ้าหน้าที่ อปท.


ซิมม้า

การซื้อของออนไลน์


การหลอกลวงให้ลงทุน

Cyber-bullying

ปลอมแปลงเอกสาร | เข้าถึงระบบโดยมิชอบ | หลอกลวงทางโทรศัพท์ | ร้านค้าปลอม | แอบอ้างตัวตน | สร้างความน่าเชื่อถือ | คุกคามออนไลน์

ความเสียหายทางการเงิน | ความเสียหายทางจิตใจ

ป้องกัน → เฝ้าระวัง → จับกุม → ดำเนินคดี

ภายใต้การดำเนินงานยุทธศาสตร์ชาติด้านความมั่นคง "การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง"

ปัจจัยที่เกี่ยวข้อง

สารสนเทศ หมายถึง การพึ่งพาช่องโหว่หรือความอ่อนแอของระบบสารสนเทศ
สังคม หมายถึง สภาพบังคับหรือสาเหตุที่สนับสนุนให้ผู้กระทำผิดเร่งดำเนินการหรือเพิ่มแรงจูงใจ อาทิ ความกดดันทางรายได้ อัตราการว่างงาน การเติบโตทางดิจิทัล
กฎหมาย หมายถึง ความเฉพาะของกฎเกณฑ์ ข้อต้องห้าม ที่อยู่ในสภาพบังคับ

กรณีศึกษา/ปัจจัยร่วม	บุคคล	สารสนเทศ	สังคม	กฎหมาย	การดำเนินการ
การประทุษกรรมทางการเงินของเจ้าหน้าที่	☑	☑	☑	☒	*การเข้าถึงระบบ KTB Corporate*
การใช้ซิมม้า	☑	☑	☑	☒	*ใช้ซิมปลอม ปกปิดตัวตน*
การหลอกลวงจากการซื้อของออนไลน์	☑	☒	☑	☒	*หลอกขายสินค้าที่มีและไม่มีอยู่จริง*
การหลอกลวงให้ลงทุนลงทุนสกุลเงินดิจิทัล	☑	☒	☑	☒	*หลอกลงทุนโดยใช้แพลตฟอร์มปลอม*
การประทุษร้ายบนโลกไซเบอร์ (Cyber-bullying)	☑	☒	☑	☒	*ใช้ Hate Speech หรือข้อมูลส่วนตัว*

งบประมาณไปไหน

งบประมาณสะสมที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ ประจำปีงบประมาณ พ.ศ. 2566 - 2568

สำนักงานตำรวจแห่งชาติ
2,870 ล้านบาท

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
1,750 ล้านบาท

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
1,080 ล้านบาท

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
1,180 ล้านบาท

CHEERS MODEL

C **Community**
เจ้าหน้าที่ นักลงทุน ผู้ใช้ทั่วไปในระบบโทรคมนาคม ผู้ใช้สื่อสังคมออนไลน์ เด็ก และเยาวชน

H **Harm**
การสูญเสียทรัพย์สิน ในกรณีของการฉ้อโกงและการหลอกลวง

E **Expectation**
กลไกที่มีความโปร่งใส ยั่งยืน มีมาตรการเชิงรุก และการบังคับใช้กฎหมาย

E **Events**
ใช้ข้อมูลและเหตุการณ์ในอดีตมาสร้างระบบการป้องกัน

R **Recurring**
เกิดช่องโหว่ทางเทคโนโลยี และการบังคับใช้กฎหมายอย่างต่อเนื่อง

S **Similarity**
กลุ่ม 1 - 4 เป็นการหลอกลวงทางการเงิน และการหลอกลวงออนไลน์ และกลุ่ม 5 มีลักษณะคล้ายกับ Hate Speech ที่ส่งผลกระทบต่อสังคมและจิตใจ

CRIME TRIANGLE THEORY

1. ผู้กระทำความผิด (Offender)
ผู้กระทำความผิดมักเป็นบุคคลหรือกลุ่มที่มีความเชี่ยวชาญด้านเทคโนโลยี และมีแรงจูงใจทางการเงินหรือจิตวิทยา

2. เหยื่อหรือเป้าหมาย (Victim)
ผู้ใช้งานอินเทอร์เน็ตที่ขาดความรู้เกี่ยวกับความปลอดภัย หรือองค์กรที่มีระบบรักษาความปลอดภัยทางไซเบอร์ไม่เข้มงวด

3. สถานที่หรือบริบท (Place)
บริบทที่เอื้อต่ออาชญากรรม ระบบออนไลน์ หรือแพลตฟอร์มที่มีช่องโหว่ อาทิ การลงทะเบียนซิมการ์ดที่ไม่มีการตรวจสอบข้อมูลอย่างเข้มงวด โซเชียลมีเดีย หรือเว็บไซต์ที่ไม่มีกระบวนการตรวจสอบตัวตนของผู้ใช้งาน

บูรณาการข้อมูล (Integration)

บูรณาการ **ระบบศูนย์กลางข้อมูล** ที่รวบรวมข้อมูลจากผู้ให้บริการโทรคมนาคม และหน่วยงานบังคับใช้กฎหมาย เพื่อช่วยให้การเฝ้าระวังพฤติกรรม วิเคราะห์สถานการณ์ที่เกิดขึ้น และพยากรณ์

เพิ่มขีดความสามารถ (Capacities Enhancement)

1. **ด้านบุคลากร** รณรงค์ เผยแพร่ข่าวสารการปราบปราม จับกุม และให้ความรู้อย่างต่อเนื่อง เพื่อเสริมทักษะ การตระหนักรู้ และเสริมภูมิคุ้มกันต่อการเปลี่ยนแปลงทางเทคโนโลยี การเงิน การลงทุน เป็นต้น

2. **ด้านเทคโนโลยี** ให้ความสำคัญต่อการใช้ระบบสารสนเทศที่มีความเหมาะสมในการปฏิบัติงานแต่ละเรื่อง การออกแบบระบบเทคโนโลยีให้ที่มีความทันสมัยและรองรับต่อการเปลี่ยนแปลง ตรวจจับ และเฝ้าระวังความเคลื่อนไหว ปรับปรุงระบบที่มีอยู่เดิมเพื่อสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ และลงทุนในโครงการสร้างความปลอดภัยทางเทคโนโลยี (Research & Development)

3. **ด้านการใช้อำนาจรัฐ** ต่อต้าน และควบคุมอาชญากรรมโดยเด็ดขาดต่อผู้กระทำผิด และไม่ผ่อนปรน ตลอดจนการวางนโยบายที่ต่อต้านอาชญากรรม การประทุษร้ายบนโลกไซเบอร์ การบันทึกประวัติ และการจัดตั้งหน่วยงานเฉพาะเพื่อดูแลเฉพาะด้าน อาทิ e-Safety

4. **กำหนดมาตรการ** เพื่อสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ให้มีความโปร่งใส โดยทำการตรวจสอบประวัติอาชญากรรมของเจ้าหน้าที่บางตำแหน่งที่เกี่ยวข้องทางการเงิน ตลอดจนการวางนโยบายที่ต่อต้านอาชญากรรม การประทุษร้ายบนโลกไซเบอร์ การบันทึกประวัติ และการจัดตั้งหน่วยงานเฉพาะเพื่อดูแลเฉพาะด้าน หรือแม้แต่การตรวจสอบทั้งจากหน่วยงานที่มีส่วนได้ส่วนเสีย และไม่มีส่วนได้ส่วนเสีย

บังคับใช้กฎหมาย (Law Enforcement)

สนับสนุนการกำหนดมาตรการการทางกฎหมายแบบมุ่งเป้า อาทิ การออกกฎหมายหรือหลักเกณฑ์ลำดับรอง เพื่อรองรับสถานการณ์ทางเทคโนโลยี การบังคับใช้หลักการ Shared Responsibility ร่วมรับผิดชอบ ที่พุ่งเป้าไปที่ "ผู้ใช้บริการ" ที่ไม่มีความรับผิดชอบ "คนกลาง" และ "ผู้ประกอบการ"

หลักสูตร: การป้องกันอาชญากรรมกับการอำนวยความยุติธรรมในสังคม Crime Prevention

บทสรุปผู้บริหาร
(Executive summary)

ในการศึกษาสภาพปัญหาและรูปแบบของอาชญากรรมในรูปแบบออนไลน์ มีวัตถุประสงค์เพื่อร่วมระดมความคิดเห็นและเสนอแนวทางการสนับสนุนหรือแก้ไขปัญหาอย่างเป็นรูปธรรม ตลอดจนเพื่อแสดงถึงความเชื่อมโยงของเหตุการณ์ที่มีปัจจัยที่อาจส่งผลต่อการยกระดับเพื่อพัฒนาการป้องกันอาชญากรรมทางไซเบอร์ร่วมกันใน 5 กรณีศึกษา ได้แก่ การประทุษกรรมทางการเงินของเจ้าหน้าที่องค์กรปกครองส่วนท้องถิ่น การป้องกันอาชญากรรมทางเทคโนโลยีจากซิมม้า การหลอกลวงจากการซื้อของออนไลน์ หรือ Online Shopping Scams การหลอกลวงให้ลงทุนออนไลน์โดยใช้แพลตฟอร์มลงทุนสกุลเงินดิจิทัลปลอม และการประทุษร้ายบนโลกไซเบอร์ (Cyber-bullying) ผ่านกระบวนการการศึกษาที่มุ่งเน้นการเรียนรู้ด้วยวิธีการใช้ปัญหาเป็นฐาน (Problem Oriented Approach) ในการร่วมถอดบทเรียนจากผลการดำเนินงานด้านการป้องกันอาชญากรรมในอดีตจนถึงปัจจุบัน เรียนรู้การใช้ข้อมูลเชิงสถิติเพื่อวิเคราะห์ถึงสาเหตุ รูปแบบการเกิดขึ้นของอาชญากรรม และการพยากรณ์แนวโน้มของสถานการณ์ที่อาจเกิดขึ้นในอนาคต ผ่านการระดมความคิดเห็น การเปรียบเทียบ การบูรณาการนวัตกรรมเทคโนโลยี และมาตรการทางกฎหมาย ภายใต้กรอบแนวทางการป้องกันอาชญากรรมที่มีประสิทธิภาพ 6 ด้าน ตามมติคณะรัฐมนตรี เมื่อวันที่ 26 มกราคม 2560 เพื่อกำหนดแนวทางเชิงนโยบายที่มีเหมาะสมและทัดเทียมกับประเทศในกลุ่มภูมิภาค ซึ่งผลการศึกษาได้แสดงให้เห็นประเด็นเน้นย้ำเชิงนโยบายที่จำเป็นต้องให้ความสำคัญเป็นอย่างยิ่ง โดยเฉพาะ ***การบูรณาการข้อมูล (Integration)*** ที่จำเป็นต้องเริ่มจากการพัฒนาระบบฐานข้อมูลกลางเพื่อแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน งบประมาณ และสร้างเครือข่ายความร่วมมือระหว่างภาครัฐและเอกชน ***การเพิ่มศักยภาพการป้องกันและต่อเนื่อง (Capacities Enhancement)*** เพื่อพัฒนาเทคโนโลยีและนวัตกรรมในการตรวจจับและป้องกันอาชญากรรมอย่างยั่งยืน โดยการเสริมสร้างความตระหนักรู้และการมีส่วนร่วมของประชาชนในการกำหนด วางแผน แก้ไขปัญหา และเฝ้าระวัง การพัฒนาขีดความสามารถขององค์กรและเจ้าหน้าที่ให้มีองค์ความรู้ที่สอดคล้องกับการปฏิบัติงานและภารกิจ และยกระดับมาตรฐานโครงสร้างพื้นฐานด้านความปลอดภัยทางไซเบอร์ ตลอดจน ***การบังคับใช้กฎหมาย (Law Enforcement)*** เพื่อปรับปรุงกฎหมายให้ทันต่อรูปแบบอาชญากรรมที่เปลี่ยนแปลง เพิ่มประสิทธิภาพในการสืบสวนสอบสวนคดีทางไซเบอร์ และเสริมสร้างความร่วมมือระหว่างประเทศในการปราบปรามอาชญากรรม

โดยรายละเอียดของผลการศึกษาได้แสดงการศึกษาเชิงเปรียบเทียบเพื่อผลักดันการยกระดับขีดความสามารถของไทยให้ทัดเทียมกับประเทศในกลุ่มภูมิภาคเดียวกัน เช่น ประเทศสิงคโปร์ ที่ประเทศไทยจำเป็นต้องดำเนินการในลักษณะ Quick Win และ Long-term Development โดยเริ่มจากการปรับปรุงโครงสร้างการบริหารจัดการให้มีเอกภาพ การพัฒนาระบบเฝ้าระวังและป้องกันภัยคุกคามที่จำเป็นเร่งด่วน และการเสริมสร้างความร่วมมือระหว่างหน่วยงานทั้งในและต่างประเทศในการถ่ายทอดองค์ความรู้และเทคโนโลยี ควบคู่ไปกับการวางรากฐานการพัฒนาระยะยาว ทั้งด้านกฎหมาย บุคลากร และโครงสร้างพื้นฐาน ด้วยการบูรณาการข้อมูล หรือ Integration โดยเฉพาะกรณีการประทุษกรรมทางการเงินของเจ้าหน้าที่องค์กรปกครองส่วนท้องถิ่น ที่ต้องมีการเชื่อมโยงฐานข้อมูลระหว่างระบบการเงินการคลังท้องถิ่น ระบบจัดซื้อจัดจ้างภาครัฐ และระบบตรวจสอบเพื่อให้สามารถตรวจจับความผิดปกติได้แบบ Real-time นอกจากนี้ควรพัฒนาระบบ Analytics ที่สามารถ

วิเคราะห์รูปแบบการทุจริตที่ซับซ้อนได้ และหากเป็นกรณีซิมม้า หรือการหลอกลวงทางออนไลน์ ควรมีการบูรณาการข้อมูลระหว่างผู้ให้บริการโทรศัพท์เคลื่อนที่ ธนาคาร และหน่วยงานบังคับใช้กฎหมาย เพื่อให้สามารถระงับการทำธุรกรรมที่ต้องสงสัยได้ทันที รวมถึงการพัฒนาระบบแจ้งเตือนภัยที่สามารถส่งข้อมูลถึงประชาชนได้อย่างรวดเร็ว ขณะเดียวกันการเพิ่มศักยภาพด้านการป้องกันและต่อเนื่อง ทั้งด้านบุคลากรที่ต้องพัฒนาทักษะด้านดิจิทัลและความเข้าใจเกี่ยวกับอาชญากรรมทางเทคโนโลยีให้แก่เจ้าหน้าที่ทุกระดับ โดยเฉพาะเจ้าหน้าที่ด่านหน้าที่ต้องรับเรื่องร้องเรียนและให้ความช่วยเหลือประชาชน การฝึกอบรมควรครอบคลุมทั้งการสืบสวนสอบสวนคดีไซเบอร์ การรวบรวมพยานหลักฐานดิจิทัล และการป้องกันอาชญากรรมรูปแบบใหม่ และด้านเทคโนโลยี ควรลงทุนในระบบตรวจจับและป้องกันการโจมตีทางไซเบอร์ที่ทันสมัย เช่น ระบบปัญญาประดิษฐ์สำหรับวิเคราะห์พฤติกรรมต้องสงสัย ระบบติดตามธุรกรรมทางการเงินที่ผิดปกติ และระบบป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการบังคับใช้กฎหมาย ที่จำเป็นต้องมีการปรับปรุงกฎหมาย โดยต้องพัฒนากฎหมายให้ครอบคลุมอาชญากรรมทางเทคโนโลยีรูปแบบใหม่ อาทิ กรณีการหลอกลวงผ่านแพลตฟอร์มลงทุนและการกลั่นแกล้งทางไซเบอร์ รวมถึงการกำหนดบทลงโทษที่เหมาะสมและการคุ้มครองผู้เสียหาย ตลอดจนการบังคับใช้กฎหมายระหว่างประเทศที่ต้องอาศัยความร่วมมือระหว่างประเทศในการสืบสวนสอบสวนและจับกุมผู้กระทำผิด โดยเฉพาะกรณีแพลตฟอร์มลงทุนปลอมที่มีการดำเนินการจากต่างประเทศ

ขณะเดียวกัน เมื่อวิเคราะห์ถึงความเชื่อมโยงของเหตุการณ์ และรูปแบบของแผนประทุษกรรมที่เกิดขึ้นจากอาชญากรรมทางเทคโนโลยี (Technology Crime) ที่ทวีความรุนแรงและเป็นปัญหาในยุคดิจิทัลปัจจุบัน จาก 5 กรณีศึกษา ตามแนวคิดสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) และ CHEERS Model จะเห็นได้ว่า

1) แผนประทุษกรรมทางการเงินของเจ้าหน้าที่องค์กรปกครองส่วนท้องถิ่น มีขั้นตอนของการเกิดอาชญากรรมที่เริ่มจาก การเก็บข้อมูลทางการเงิน การขโมยรหัสผ่านหรือใช้ช่องโหว่ทางไซเบอร์เพื่อเข้าถึงข้อมูลทางการเงินทำธุรกรรมปลอมหรือการโอนเงินไปยังบัญชีที่ควบคุมโดยผู้กระทำผิด ซึ่งเกิดจากการใช้ช่องโหว่ของระบบบัญชีภาครัฐ การใช้เอกสารปลอมในการเข้าถึงบัญชี และการขาดระบบตรวจสอบแบบเรียลไทม์

2) การใช้ซิมม้าเพื่อก่ออาชญากรรมทางไซเบอร์ มีขั้นตอนเริ่มต้นของการก่ออาชญากรรมจากการซื้อหรือปลอมซิมการ์ดที่มาจากการใช้ข้อมูลปลอมลงทะเบียนซิมการ์ด ที่ส่งให้เกิดการสร้างหรือเปิดบัญชีธนาคารปลอม การใช้แพลตฟอร์มออนไลน์โดยใช้ซิมม้า ซึ่งเป็นสาเหตุที่เริ่มจากระบบการลงทะเบียนซิมที่ไม่เข้มงวด ขาดการติดตามพฤติกรรมซิมการ์ดที่น่าสงสัย

3) การหลอกลวงจากการซื้อของออนไลน์ (Online Shopping Scams) เกิดขึ้นจากขั้นตอนการสร้างเว็บไซต์หรือบัญชีปลอมเพื่อเปิดร้านค้าออนไลน์ที่ไม่มีสินค้าจริง โฆษณาดึงดูดเหยื่อโดยใช้โฆษณาบนโซเชียลมีเดียเพื่อกระตุ้นให้เหยื่อสนใจ หลอกลวงให้มีการชำระเงิน โดยให้เหยื่อโอนเงินโดยตรงหรือจ่ายผ่านแพลตฟอร์มที่ควบคุมโดยอาชญากร ปิดเว็บไซต์และหายตัวไป ซึ่งปัจจัยที่เกี่ยวข้องอาจเกิดจากการขาดมาตรการตรวจสอบร้านค้าออนไลน์ และการใช้บัญชีธนาคารที่ลงทะเบียนด้วยซิมม้า

4) การหลอกลวงให้ลงทุนออนไลน์โดยใช้แพลตฟอร์มลงทุนปลอม ที่มีสาเหตุจากการสร้างแพลตฟอร์มลงทุนปลอมผ่านการออกแบบเว็บไซต์หรือแอปพลิเคชันที่เลียนแบบแพลตฟอร์มลงทุนจริง ล่อลวงด้วยผลตอบแทนสูงโดยให้ข้อมูลปลอมเกี่ยวกับผลตอบแทนเกินจริง เก็บเงินจากผู้ลงทุนและหลอกให้เหยื่อโอนเงินไปยังบัญชีปลอม ปิดแพลตฟอร์มหรือทำให้ระบบไม่สามารถถอนเงินได้ ซึ่งจะเห็นได้ว่าปัจจัยที่ส่งผลต่อการเร่งทวีคูณที่เพิ่มความยุ่งยากในการติดตามอาจมาจากการใช้สกุลเงินดิจิทัลในการฟอกเงิน ความโลภและความเข้าใจผิดของผู้ลงทุน และขาดมาตรการกำกับดูแลแพลตฟอร์มออนไลน์

และ 5) การประทุษร้ายบนโลกไซเบอร์ (Cyber-bullying) ที่มีขั้นตอนการเกิดอาชญากรรมโดยมุ่งเน้นผ่านการเลือกเป้าหมายหรือค้นหาเหยื่อที่มีจุดอ่อนทางสังคมหรืออารมณ์ โจมตีทางจิตใจหรือแพร่ข่าวปลอมหรือการกระจายเนื้อหาเชิงลบ แชร์โพสต์ หรือใช้เครื่องมืออิเล็กทรอนิกส์ ในการเพิ่มการมองเห็นทำให้เหยื่อเกิดความเครียดหรือผลกระทบทางจิตใจ ซึ่งอาจมีผลมาจากอิทธิพลของโซเชียลมีเดีย การขาดมาตรการจัดการ Cyber-bullying และการไม่สามารถบังคับใช้กฎหมายกับการล่วงละเมิดทางออนไลน์ได้

นอกจากนี้ เมื่อพิจารณาในแต่ละกรณีศึกษาที่มีปัจจัยความเชื่อมโยงและเป็นปัจจัยเร้าต่อการเกิดเหตุการณ์ร่วมกัน อาทิ สถิติการแจ้งความ มูลค่าความเสียหาย การเข้าถึงอินเตอร์เน็ต และลักษณะของกลุ่มประชาชน ประกอบกับการนำข้อมูลเชิงสถิติการเกิดอาชญากรรมในแต่ประเภทเทียบเคียงข้อมูลจากสำนักงานตำรวจแห่งชาติ สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ ธนาคารแห่งประเทศไทย และสำนักงานสถิติแห่งชาติ จะพบถึงความสัมพันธ์ระหว่างรูปแบบการเกิดขึ้นของอาชญากรรมในแต่ละเหตุการณ์และลักษณะของพื้นที่ โดยเฉพาะในเขตเมืองใหญ่ เช่น เชียงใหม่ ขอนแก่น และภูเก็ต ที่มีการรายงานการหลอกลวงด้านการลงทุนและการฉ้อโกงทางการค้าออนไลน์ในสัดส่วนที่สูง ขณะที่ในเขตพื้นที่ชานเมืองและต่างจังหวัดจะพบการทุจริตในองค์กรปกครองส่วนท้องถิ่นและการหลอกลวงผ่านชิมม้าเป็นหลัก อีกทั้ง ยังพบความเชื่อมโยงระหว่างอาชญากรรมประเภทต่าง ๆ โดยพื้นที่ที่มีการรายงานการทุจริตในองค์กรปกครองส่วนท้องถิ่นสูง มักพบการรั่วไหลของข้อมูลและการนำข้อมูลไปใช้ในการก่ออาชญากรรมรูปแบบอื่นตามมา โดยผลจากการวิเคราะห์รูปแบบอาชญากรรมและความสัมพันธ์เชิงพื้นที่ดังกล่าวได้สะท้อนให้เห็นถึงความจำเป็นในการพัฒนาแนวทางการป้องกันและปราบปรามที่มีความเฉพาะเจาะจงกับบริบทของแต่ละพื้นที่ ซึ่งเป็นการแสวงหาแนวทางการป้องกันอาชญากรรมทั้งในเชิง Problem-based และ Area-based และเป็นการนำไปสู่การแก้ไขปัญหาที่ตรงประเด็นและการขับเคลื่อนนโยบายด้านการป้องกันอาชญากรรมทางไซเบอร์ที่มีประสิทธิภาพ โดยคำนึงถึงความแตกต่างของบริบทพื้นที่และความซับซ้อนของอาชญากรรมทางไซเบอร์ในปัจจุบัน เพื่อนำไปสู่การยกระดับมาตรการป้องกัน ส่งเสริมและบูรณาการ ลดโอกาสการตกเป็นเหยื่อ เฝ้าระวัง และการปราบปรามที่มีเหมาะสมกับสถานการณ์และความท้าทายในแต่ละพื้นที่

อย่างไรก็ตาม แม้การยกระดับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของไทยให้ทัดเทียมกับประเทศสิงคโปร์ที่มีการบริหารจัดการและมีค่าดัชนีอาชญากรรมในลำดับต้น ๆ ในภูมิภาค จำเป็นต้องพิจารณาและดำเนินการในหลายมิติ อาทิ **ด้านนโยบายและการบริหารจัดการ** ที่ประเทศไทยควรปรับโครงสร้างการบริหารจัดการให้มีเอกภาพมากขึ้น โดยจัดตั้งหน่วยงานระดับชาติที่มีอำนาจเบ็ดเสร็จในการกำหนดนโยบายและประสานการปฏิบัติ รวมถึงการจัดสรรงบประมาณที่เพียงพอสำหรับการดำเนินงาน **ด้านเทคโนโลยีและโครงสร้างพื้นฐาน** ที่ควรเร่งพัฒนาระบบเฝ้าระวังและป้องกันภัยคุกคามทางไซเบอร์ระดับชาติ พร้อมทั้งสร้างความร่วมมือกับภาคเอกชนในการพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยด้านความร่วมมือระหว่างประเทศและสร้างความร่วมมือทั้งในระดับทวิภาคีและพหุภาคี เพื่อแลกเปลี่ยนข้อมูลและพัฒนาขีดความสามารถร่วมกัน และ **ด้านการสร้างความตระหนักรู้** ที่ต้องมีโครงการรณรงค์และให้ความรู้แก่ประชาชนอย่างต่อเนื่องผ่านแพลตฟอร์มที่หลากหลายและเข้าถึงง่าย ประกอบกับการกระจายตัวของงบประมาณด้านความมั่นคงทางไซเบอร์ของประเทศไทยมีการกระจายตัวไปตามหน่วยงานต่าง ๆ ทำให้ขาดการบูรณาการและประสิทธิภาพในการใช้จ่าย โดยควรพิจารณารวมศูนย์งบประมาณภายใต้หน่วยงานหลักเพื่อให้เกิดการใช้งบประมาณอย่างมีประสิทธิภาพมากขึ้นและอาจจำเป็นต้องลำดับความสำคัญของการลงทุนที่มุ่งเน้นการลงทุนในโครงการที่มีความสำคัญเร่งด่วนและให้ผลตอบแทนสูง เช่น ระบบเฝ้าระวังและป้องกันภัยคุกคามระดับชาติ และการพัฒนาบุคลากรที่มีความเชี่ยวชาญเฉพาะทาง การระดมทุนจากภาคเอกชนเพื่อเพิ่มงบประมาณในการพัฒนาโครงสร้างพื้นฐานและระบบรักษาความปลอดภัยทางไซเบอร์ หรือแม้แต่การปรับปรุงกลไกการจัดสรรงบประมาณ การพัฒนาระบบการจัดสรรงบประมาณที่มีความยืดหยุ่น

และตอบสนองต่อภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว รวมถึงการจัดตั้งกองทุนพิเศษสำหรับการรับมือกับเหตุฉุกเฉินทางไซเบอร์ ดังนั้น การจัดการปัญหาอาชญากรรมทางเทคโนโลยี (Technology Crime) จึงไม่ควรเป็นบทบาทหรือหน้าที่ของคนหนึ่งคนใด แต่กลับต้องได้รับความร่วมมือในการดำเนินงานร่วมกันตั้งแต่ต้นน้ำ กลางน้ำ และปลายน้ำ อย่างเป็นระบบ

คณะผู้เข้าร่วม
หลักสูตร การป้องกันอาชญากรรมกับการอำนวยความยุติธรรมในสังคม
Crime Prevention รุ่นที่ 8 (CP 8)
มกราคม 2568