# สรุปประเด็นสำคัญจากการสัมมนา BOT Symposium 2025:

# เท่าทันภัยการเงิน – Towards Safer and More Inclusive Digital Finance (ช่วงเช้า)

**เท่าทันภัยการเงินดิจิทัล: ความท้าทายร่วมกันของสังคมไทย**

ภัยทางการเงินในยุคดิจิทัลได้กลายเป็นวิกฤตที่ส่งผลกระทบต่อคนไทยในวงกว้างและรุนแรงขึ้นอย่างต่อเนื่อง งาน BOT Symposium ได้ฉายภาพให้เห็นถึงภูมิทัศน์ของปัญหา ความท้าทาย และแนวทางที่ทุกภาคส่วนต้องร่วมมือกันเพื่อสร้างภูมิคุ้มกันให้สังคมไทยรอดพ้นจากภัยคุกคามที่ซับซ้อนและเปลี่ยนแปลงตลอดเวลา

**ภาพใหญ่ของปัญหา: ใกล้ตัวกว่าที่คิด ลุกลามในวงกว้าง และยากจะติดตามเงินคืน**

ข้อมูลเชิงประจักษ์ชี้ว่าภัยการเงินไม่ใช่เรื่องไกลตัวอีกต่อไป นับตั้งแต่ปี 2565 มีการแจ้งความคดีออนไลน์ในไทยมากกว่า 1 ล้านคดี สร้างความเสียหายกว่า 9.8 หมื่นล้านบาท การหลอกให้โอนเงินด้วยตนเอง (Authorized Push Payment – APP fraud) ในหลากหลายรูปแบบสำคัญ เช่น หลอกลงทุน หลอกทำงาน หลอกให้รัก หลอกขายของ และภัยนี้เข้าถึงคนทุกกลุ่ม โดยมีแพลตฟอร์มโซเชียลมีเดียเป็นช่องทางหลักที่มิจฉาชีพใช้ในการเข้าถึงเหยื่อ

ปัญหาถูกซ้ำเติมด้วยความรวดเร็วของระบบการชำระเงินดิจิทัล ที่ทำให้เงินของเหยื่อถูกโอนออกจากบัญชีต่อไปยังบัญชีม้าทอดถัดๆ ไปจนออกนอกระบบภายในเวลาเพียง 3 นาที ในขณะที่ผู้เสียหายใช้เวลาเฉลี่ยถึง 18 ชั่วโมงในการแจ้งความ ช่องว่างของเวลาที่ต่างกันมหาศาลนี้เองที่ทำให้การติดตามเงินคืนเป็นไปได้ยากอย่างยิ่ง อย่างไรก็ตาม ปัญหาที่น่ากังวลคือตัวเลขความเสียหายอาจสูงกว่าที่ประเมินไว้มาก เนื่องจากผู้เสียหายที่เข้าแจ้งความมีสัดส่วนเพียงประมาณ 10% เท่านั้น

**การจัดการภัยการเงิน: ข้อมูล เทคโนโลยี การกำกับดูแล และแรงจูงใจ**

**หัวใจสำคัญคือข้อมูล:** การต่อสู้กับภัยการเงินที่มีประสิทธิภาพต้องเริ่มจากการแชร์ เชื่อมโยง และใช้ข้อมูลร่วมกันอย่างทันท่วงที ประเทศไทยได้พัฒนากลไกที่ทำให้ประชาชนแจ้งความได้สะดวกขึ้น และมีศูนย์กลางข้อมูลบัญชีม้า (Central Fraud Registry - CFR) ที่เชื่อมโยงข้อมูลระหว่างสถาบันการเงินได้อย่างครอบคลุม รวม digital asset และ e-money ข้อมูลเหล่านี้ยังถูกเชื่อมต่อเพื่อสนับสนุนการทำงานของศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (AOC) ในการตรวจจับ รับมือ และป้องกันภัยได้อย่างมีประสิทธิภาพมากขึ้น

**เทคโนโลยี:** มีการนำเทคโนโลยีมาใช้ป้องกันตั้งแต่ด่านหน้า เช่น การยืนยันตัวตนด้วยข้อมูล Biometric ในการใช้งานโมบายแบงก์กิ้ง ซึ่งช่วยลดปัญหาการโจรกรรมจากเข้าถึงบัญชีโดยไม่ได้รับอนุญาต (Unauthorized fraud) ได้เกือบทั้งหมด นอกจากนี้ ข้อมูลจาก CFR ยังถูกนำมาวิเคราะห์เพื่อตรวจจับพฤติกรรมต้องสงสัยและสั่งระงับธุรกรรมได้โดยอัตโนมัติ

**การกำกับดูแล:** ประเทศไทยมีพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (พ.ร.ก. ไซเบอร์) เป็นเครื่องมือสำคัญในการกำหนดอำนาจหน้าที่และความรับผิดชอบ

ของทุกภาคส่วนที่เกี่ยวข้องอย่างครอบคลุม มีการจัดตั้งศูนย์ AOC เพื่อให้เกิดการทำงานร่วมกันระหว่างหน่วยงาน และมีการออกมาตรฐานการดำเนินการให้สถาบันการเงินปฏิบัติตาม รวมถึงการจัดการบัญชีม้าอย่างเป็นระบบ

**การสร้างแรงจูงใจ**: มีการผลักดันหลักการ "ความรับผิดชอบร่วมกัน" (Shared Responsibility) เพื่อสร้างแรงจูงใจให้ทุกฝ่าย ตั้งแต่แพลตฟอร์มดิจิทัล ผู้ให้บริการโทรคมนาคม ไปจนถึงสถาบันการเงิน ต้องเข้ามามีส่วนร่วมในการลงทุนและพัฒนาระบบป้องกันอย่างจริงจัง

**บทเรียนจากต่างประเทศ: ไทยไม่หย่อนกว่าใคร แต่ได้ต้นแบบสู่การยกระดับ**

ทุกประเทศในภูมิภาคต่างให้ความสำคัญกับการทำให้ประชาชนเท่าทันและมีภูมิคุ้มกัน โดยมีแนวทางที่น่าสนใจหลากหลายรูปแบบ ตั้งแต่การสร้างภูมิคุ้มกันให้แต่ละบุคคลผ่านแคมเปญรณรงค์ที่มีประสิทธิภาพ ไปจนถึงการออกแบบระบบการเงินที่ช่วยเตือนและป้องกันผู้ใช้งานเชิงรุก ตัวอย่างเทคโนโลยีและนโยบายที่น่าสนใจ เช่น "Scammeter" ของฮ่องกงที่ใช้เทคโนโลยีประมวลความเสี่ยงและเตือนทันที ก่อนคนทำธุรกรรม, บริการ “Money Lock” ที่สิงคโปร์ มาเลเซียและฮ่องกง ที่ให้ผู้ใช้สามารถล็อกวงเงินในบัญชีเพื่อป้องกันการโอนออกที่ไม่พึงประสงค์ หรือ**ศูนย์ประสานงานต่อต้านการหลอกลวงที่ทำหน้าที่ทั้งตรวจจับและเข้าแทรกแซงเพื่อยับยั้งความเสียหาย** เช่น การประสานงานให้พนักงานสาขาของธนาคารติดต่อพูดคุยกับลูกค้าที่กำลังจะทำธุรกรรมเสี่ยง

**บทสรุป: ทุกคนต้องมีส่วนร่วม และการป้องกันที่ดีที่สุดคือการทำให้คนเท่าทันและมีภูมิคุ้มกัน**

**ต้องเดินหน้าลดข้อจำกัดด้านข้อมูล** ทำให้การแจ้งความสะดวก และทำให้เกิดการแบ่งปันและใช้ประโยชน์จากข้อมูลร่วมกันทั้งระบบอย่างรวดเร็วและปลอดภัย

**เทคโนโลยีที่ทำงานร่วมกับคน:** ต้องพัฒนาเทคโนโลยีที่ไม่เพียงแต่ป้องกัน แต่ยังต้องช่วยให้ข้อมูลและทางเลือกแก่ผู้ใช้งานเพื่อประกอบการตัดสินใจได้อย่างเหมาะสม

**การกำกับดูแลที่ยืดหยุ่น**: กฎเกณฑ์ต้องปรับตัวให้ทันต่อภัยคุกคามรูปแบบใหม่ๆ โดยต้องสร้างสมดุลระหว่างความปลอดภัยและความสะดวกของผู้ใช้งาน เพื่อไม่ให้เกิดผลกระทบต่อผู้บริสุทธิ์เกินความจำเป็น เช่น กรณีการระงับบัญชีที่ต้องมีกระบวนการปลดล็อกที่รวดเร็วสำหรับผู้ที่ไม่เกี่ยวข้อง

**การป้องกันที่ดีที่สุดคือการทำให้ประชาชนมีความรู้เท่าทันและมีภูมิคุ้มกันทางการเงินดิจิทัลและทุกคนต้องมีส่วนร่วม** และความแน่วแน่ของภาครัฐในการผลักดันนโยบายจากระดับบนลงมา (Top-down) เพื่อให้เกิดการเปลี่ยนแปลงอย่างเป็นรูปธรรมและยั่งยืน