

เตือนภัยคอลเซ็นเตอร์

1. รูปแบบกลโกง

2. สัญญาณเตือนภัย

3. ความเสียหายที่เกิดขึ้น

4. วิธีป้องกันและปฏิบัติตัว



เตือนภัยทางสังคม ฉบับที่ 5 ปี 2569 จัดทำโดย สำนักงานส่งเสริมและสนับสนุนวิชาการ 11



วิกฤตระดับชาติ: อุตสาหกรรมการหลอกลวง

63,000+ ล้านบาท

มูลค่าความเสียหายทางเศรษฐกิจระดับประเทศ

700 - 900 เรื่อง/วัน

ปริมาณการแจ้งความผ่านระบบออนไลน์เฉลี่ย

5 ลำดับกลโกงหลัก



1. หลอกให้โอนเงิน
เพื่อทำงาน



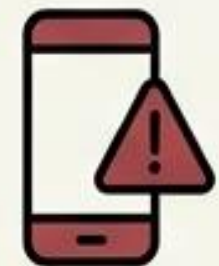
2. หลอกให้กู้เงิน



3. หลอกเป็น
เจ้าหน้าที่รัฐ



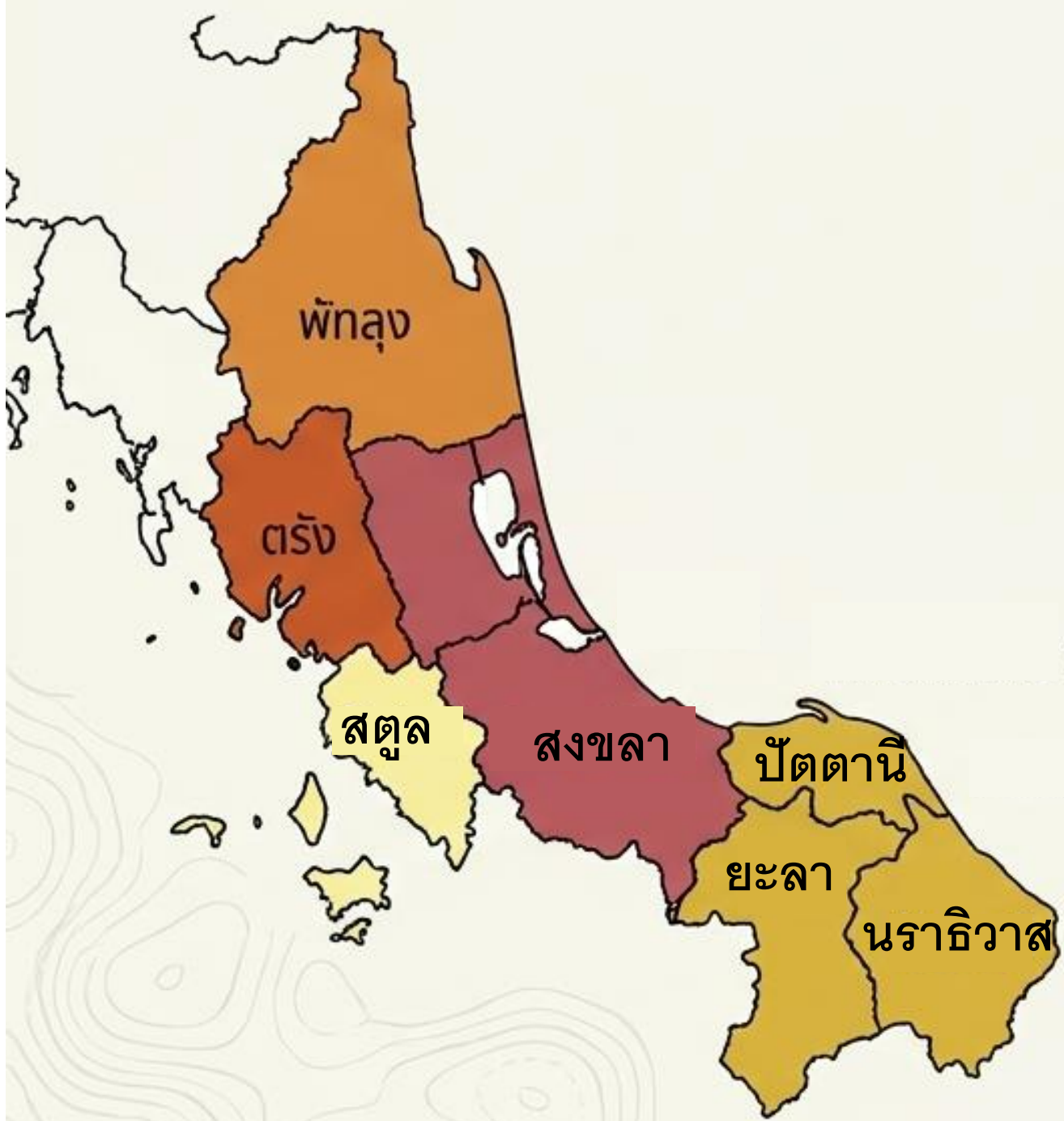
4. หลอกให้ลงทุน



5. แอปฯ ดูดเงิน

ที่มา : กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.)

แผนที่ความเสี่ยง 7 จังหวัดภาคใต้ตอนล่าง



จังหวัด (ระดับความเสี่ยง)	ลักษณะภัยคุกคามหลัก
สงขลา	หลอกลงทุน (เจาะศูนย์กลางเศรษฐกิจ), แอบอ้างศุลกากร/พัสดุ (เจาะเมืองด่านชายแดน)
ตรัง	กู้เงินออนไลน์, แอบอ้างโครงการช่วยเหลือเกษตรกรยาง/ปาล์ม
พัทลุง	หลอกติดตั้งแอปฯ ดูดเงิน (Malware) อ้างสวัสดิการรัฐ
ยะลา	แอบอ้างเจ้าหน้าที่ความมั่นคง ตรวจสอบเส้นทางการเงิน
นราธิวาส	ใช้ภาษาไทยถิ่นใต้/มลายูถิ่น หลอกขายสินค้าออนไลน์
ปัตตานี	หลอกนักศึกษาเรื่องทุน/รับสมัครงานราชการปลอม
สตูล	หลอกชาวประมง/แรงงานข้ามชาติ เรื่องต่อใบอนุญาตและภาษี

ที่มา : กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.)

รอยรั่วชายแดน

ประเทศเพื่อนบ้าน

การรั่วไหลของสัญญาณอินเทอร์เน็ตและโทรศัพท์ข้ามแดน ทำให้เจ้าหน้าที่รัฐไม่สามารถระบุตำแหน่งฐานปฏิบัติการที่แท้จริงได้

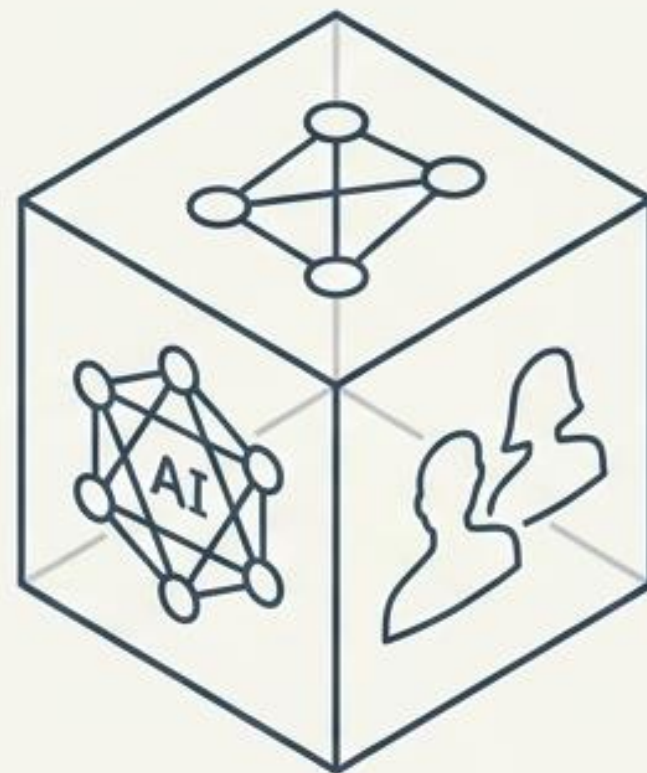
พื้นที่รอยต่อชายแดน (ด่านนอก, ปาดังเบซาร์, สุโงโก-ลก) เป็นจุดรวมพลรับจ้างเปิดบัญชีม้า เงินถูกโอนออกนอกประเทศในไม่กี่นาที

ประเทศไทย

กลโกงในระดับพื้นที่



Localizing Scams:
มิจฉาชีพไม่ได้ใช้รูปแบบเดียว
ทั้งประเทศ แต่จ้าง ‘คนในพื้นที่’
หรือใช้เทคโนโลยี AI



เจาะเกราะป้องกัน:
เลียนสำเนียงภาษาไทยถิ่นใต้
และมลายูถิ่น (ยาวิ)
เพื่อสร้างความไว้วางใจขั้นสูงสุด



เป้าหมายหลัก:
พุ่งเป้าไปที่กลุ่มผู้สูงอายุที่
สื่อสารด้วยภาษาถิ่นเป็นหลัก
ทำให้เหยื่อหลงเชื่ออย่างสนิทใจ

กลโกงออนไลน์



Data Vulnerability

ข้อมูลส่วนบุคคลรั่วไหล (ชื่อ, เบอร์โทร, เลขบัตรประชาชน)
ทำให้สคริปต์หลอกลวงมีความสมจริงและเฉพาะเจาะจง



Psychological Manipulation

การแฉกจิตวิทยาผ่าน 'ความกลัว' (อ้างคดีอาญา)
และ 'ความโลภ' (ผลตอบแทนสูงเกินจริง)



Technological Gap

ช่องว่างทางเทคโนโลยี ประชาชนขาดความเข้าใจในภัยใหม่
เช่น Deepfake (การปลอมเสียงและใบหน้า)



การวิเคราะห์ผลกระทบตามกลุ่มเป้าหมาย

กลุ่มเป้าหมาย (Target)	จุดอ่อน (Vulnerability)	ผลกระทบ (Impact)
 18 - 25 ปี (นักศึกษา / วัยเริ่มทำงาน)	ต้องการเงินด่วน อยากมี อยากได้ ตามกระแส	ด้านกฎหมาย - ถูกหลอกเปิดบัญชีม้าแลกเงินหลักร้อย นำไปสู่การถูกดำเนินคดีอาญา
 26 - 45 ปี (วัยทำงาน / หัวหน้าครอบครัว)	ภาระเศรษฐกิจ ภาวะฟุ้งฟิงในครอบครัว	ด้านทรัพย์สิน - สูญเสียเงินก่อนจากการหลอกลงทุน หรือกู้เงินออนไลน์
 50 - 70 ปี+ (กลุ่มเสี่ยงสูงสุด / เกษียณ)	ความกลัว / ไม่ทันเทคโนโลยี ความโลภ/อยากได้ต้องลงทุน	ด้านจิตใจและชีวิต - สูญเสียเงินเก็บทั้งชีวิต เกิดภาวะซึมเศร้า หรือรุนแรงถึงขั้นฆ่าตัวตาย

จุดเปลี่ยนยุทธศาสตร์: การป้องกันภัยออนไลน์

รูปแบบเดิม

National Campaign



การรณรงค์ระดับชาติเพียงอย่างเดียว
ไม่เพียงพอ สำหรับภาคใต้ตอนล่าง

รูปแบบใหม่

Hyper-Localized Defense



มีจาชีฟเจาะจงใช้ช่องโหว่ทางภูมิศาสตร์ (ด้านชายแดน)
และวัฒนธรรม (ภาษาถิ่น) ในการโจมตี ดังนั้น ยุทธศาสตร์
การป้องกันจะต้องถูกปรับแต่งให้เข้ากับบริบทของพื้นที่
ทั้งในระดับกลไกชุมชนและนโยบายโครงสร้าง

ยุทธศาสตร์การป้องกันแบบหลายระดับ

Inner Ring: กลไกชุมชน

(กำนัน, ผู้ใหญ่บ้าน, อสม. เป็นด่านหน้า)

Middle Ring: การรู้เท่าทันสื่อดิจิทัล

(สอดแทรกในมัสยิด, วัด, โรงเรียน)

Outer Ring: การควบคุมเชิงโครงสร้าง

(Task Force ระดับจังหวัด, การจัดการชายแดน)



เกราะป้องกันด้านแรก: กลไกชุมชน และแคมเปญ ‘3 ไม่ 1 แจ้ง’

ไม่เชื่อ: เบอร์แปลก
อ้างเป็นเจ้าหน้าที่



ไม่รับ: ไม่กดลิงก์
ไม่ให้ข้อมูลส่วนตัว

ไม่โอน: ไม่โอนเงินเพื่อ
ตรวจสอบเด็ดขาด



แจ้ง: โทร 1441
ทันทีเมื่อสงสัย



ผู้นำชุมชน / ภาควิเคราะห์



Deployment: มอบหมายให้ กำนัน ผู้ใหญ่บ้าน และ อสม. เป็น ‘ด่านหน้า’ เยี่ยมบ้านผู้สูงอายุ และสร้าง Digital Literacy สอดแทรกความรู้ในการประชุมชุมชน มัสยิด และวัด

การยกระดับโครงสร้าง: ข้อเสนอเชิงนโยบาย



Multi-Language Alert System

พัฒนาระบบ SMS และสื่อเตือนภัย
เป็นภาษาไทยถิ่นใต้และมลายูถิ่น



Cyber Safety Zone

ตั้ง Task Force ระดับจังหวัด สามารถอายัดบัญชี
เบื้องต้นได้ทันทีโดยไม่ต้องรอส่วนกลาง



Financial Integrity School

บรรจุหลักสูตรความเท่าทันไซเบอร์ในสถานศึกษา
เพื่อสกัดกั้นวงจรบัญชีม้าในกลุ่มเยาวชน



Telecom Border Control

ตรวจสอบการลงทะเบียนซิมล็อตใหญ่ และควบคุม
ทิศทางสัญญาณอินเทอร์เน็ตข้ามพรมแดนอย่างเข้มงวด