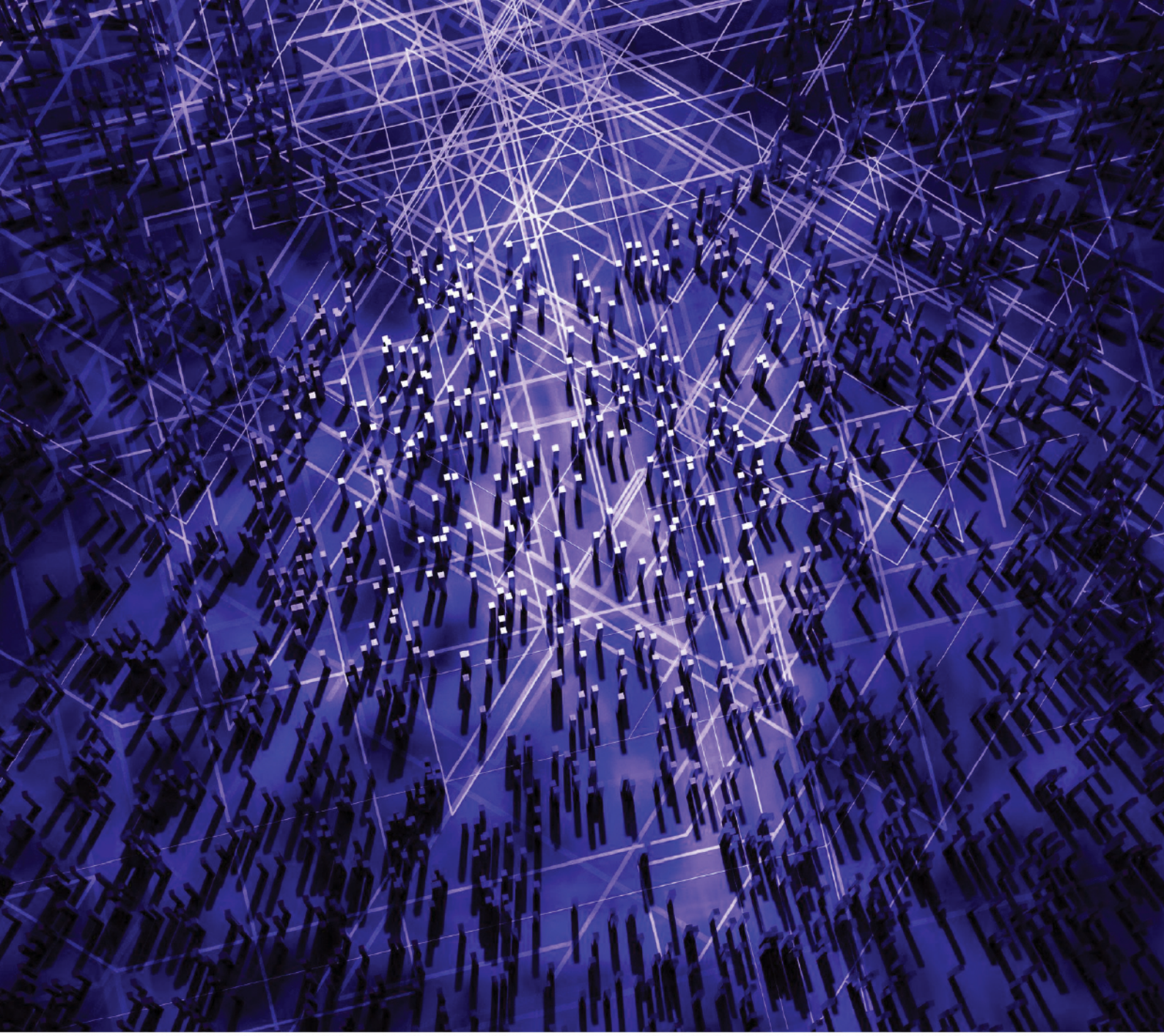


หลักฐานยืนยันความเป็นมนุษย์ (Proof of Human) : กรอบเครือข่ายมนุษย์เพื่อยกระดับความเชื่อมั่นในระบบดิจิทัลและรับมือต่อภัยการหลอกลวงทางออนไลน์ในภูมิภาคเอเชียแปซิฟิก

ธันวาคม 2568

Japan Trust & Safety Association
一般社団法人トラスト＆セーフティ協会

Southeast Asia
Public Policy Institute

คำนำ

รายงานฉบับนี้จัดทำขึ้นโดยสถาบันนโยบายสาธารณะเอเชียตะวันออกเฉียงใต้ (Southeast Asia Public Policy Institute) ร่วมกับสมาคมความเชื่อมั่นและความปลอดภัยดิจิทัลแห่งญี่ปุ่น (Japan Trust & Safety Association: JTSA) โดยได้รับการสนับสนุนจาก Tools for Humanity เพื่อศึกษาภาพรวมของสถานการณ์ด้านความเชื่อมั่นทางดิจิทัลในภูมิภาคเอเชียแปซิฟิก เนื้อหาในรายงานอ้างอิงจากการสัมภาษณ์ผู้มีส่วนเกี่ยวข้อง การทบทวนข้อมูลสาธารณะ และการวิเคราะห์ของทีมผู้เขียน นอกจากนี้ ข้อมูลและข้อคิดเห็นจาก JTSA รวมถึงคุณ Kiyotaka Tanaka ในประเด็นด้านธรรมาภิบาล ความสามารถในการทำงานร่วมกันของระบบ (interoperability) และแนวทางการปรับใช้ Proof of Human (PoH) ตามระดับความเสี่ยง (risk-based implementation) ได้มีส่วนสำคัญอย่างยิ่งต่อการจัดทำรายงานฉบับนี้

รายงานฉบับนี้ไม่ได้มีวัตถุประสงค์เพื่อสะท้อนจุดยืนหรือความคิดเห็นอย่างเป็นทางการของ Tools for Humanity และไม่ได้มุ่งหมายให้เป็นการทบทวนกฎหมาย นโยบาย หรือกฎระเบียบที่เกี่ยวข้องทั้งหมดอย่างรอบด้าน ผู้อ่านจึงควรใช้ข้อมูลและบทวิเคราะห์ในรายงานฉบับนี้ด้วยความระมัดระวัง โดยคำนึงถึงขอบเขตและข้อจำกัดของเนื้อหาอย่างเหมาะสม

สารบัญ

บทสรุปผู้บริหาร

ปัจจุบัน การหลอกลวงทางออนไลน์ได้พัฒนาไปสู่การเป็นอาชญากรรมขนาดใหญ่ที่ไร้พรมแดนและมีลักษณะเป็นระบบมากขึ้น มูลค่าทางเศรษฐกิจของอาชญากรรมไซเบอร์ทั่วโลกพุ่งสูงเกิน 10 ล้านล้านดอลลาร์สหรัฐ ขณะที่ในแต่ละปีมีความสูญเสียจากการหลอกลวงทางออนไลน์มากกว่า 1 ล้านล้านดอลลาร์สหรัฐ ผลกระทบจากปัญหานี้ไม่ได้จำกัดอยู่เพียงความเสียหายทางการเงิน หากยังส่งผลต่อสุขภาวะทางจิตใจ ความปลอดภัย และความเชื่อมั่นของประชาชนในระบบดิจิทัล อีกทั้งยังเพิ่มภาระด้านการบังคับใช้กฎหมายและการกำกับดูแลของรัฐอย่างมีนัยสำคัญ

ภูมิภาคเอเชียแปซิฟิกมีบทบาททั้งในฐานะเป้าหมายของการหลอกลวง และในฐานะพื้นที่ปฏิบัติการสำคัญของเครือข่ายอาชญากรรมออนไลน์ ศูนย์ปฏิบัติการขนาดใหญ่จำนวนมากตั้งอยู่ในเอเชียตะวันออกเฉียงใต้ โดยหลายแห่งมีความเชื่อมโยงกับการค้ามนุษย์ ในขณะเดียวกัน ประเทศที่พัฒนาแล้วในภูมิภาคอย่าญี่ปุ่นและเกาหลีใต้ ก็เผชิญกับการหลอกลวงด้านการลงทุนและการแอบอ้างตัวตนที่เพิ่มขึ้นอย่างต่อเนื่อง ปัจจัยเหล่านี้สะท้อนให้เห็นว่าการหลอกลวงทางออนไลน์เป็นปัญหาที่เชื่อมโยงกันทั้งภูมิภาค และไม่อาจจัดการได้อย่างมีประสิทธิภาพหากขาดความร่วมมือระหว่างประเทศ

ความก้าวหน้าทางเทคโนโลยียิ่งเร่งให้การหลอกลวงทางออนไลน์ขยายตัวได้รวดเร็วขึ้น ไม่ว่าจะเป็นเทคโนโลยีปัญญาประดิษฐ์ที่ทำให้การโคลนเสียงและการสร้างภาพหรือวิดีโอปลอมมีความสมจริงมากขึ้นระบบอัตโนมัติ (automation) ที่ช่วยให้สร้างบัญชีปลอมจำนวนมากได้ในเวลาอันสั้น หรือเทคโนโลยีคริปโทและระบบการชำระเงินดิจิทัลที่เอื้อต่อการเคลื่อนย้ายเงินอย่างรวดเร็วและยากต่อการติดตาม อย่างไรก็ดี เทคโนโลยีเดียวกันนี้ก็สามารถนำมาใช้เพื่อเสริมสร้างความเชื่อมั่นทางดิจิทัลได้เช่นกัน ไม่ว่าจะเป็นการยืนยันตัวตนที่แม่นยำขึ้น สัญญาณตรวจสอบความแท้จริงของเนื้อหา (authenticity signals)หรือกลไกคุ้มครองความเป็นส่วนตัวที่ช่วยลดความเสี่ยงจากภัยคุกคามรูปแบบใหม่ ทั้งนี้ การนำเทคโนโลยีเหล่านี้มาใช้จำเป็นต้องอยู่ภายใต้กรอบการกำกับดูแลที่ชัดเจนและโปร่งใส เพื่อป้องกันไม่ให้ความเสี่ยงในรูปแบบอื่นตามมา

แม้ในปัจจุบันจะมีการดำเนินมาตรการปราบปรามและการรณรงค์เพื่อยกระดับความตระหนักรู้ของประชาชนอย่างต่อเนื่อง แต่มาตรการเหล่านี้ยังไม่เพียงพอที่จะรับมือกับสถานการณ์ได้อย่างมีประสิทธิผล เมื่อผู้กระทำผิดสามารถสร้างตัวตนปลอมหรือบัญชีอัตโนมัติได้เป็นจำนวนมากด้วยต้นทุนที่ต่ำ การแก้ไขปัญหาจึงจำเป็นต้องอาศัยการพัฒนาระบบความเชื่อมั่นทางดิจิทัลในลักษณะ “สองชั้น” เพื่อปิดช่องโหว่ที่ถูกนำมาใช้ในการหลอกลวงทางออนไลน์ ซึ่งได้แก่

1.**ระบบยืนยันตัวตนทางดิจิทัล** (Digital ID) ซึ่งใช้เพื่อยืนยันว่า “ผู้ใช้งานคือใคร?” (Who are you?) ในบริบทที่มีความจำเป็นต้องระบุตัวตนของผู้ใช้งานอย่างชัดเจนสำหรับกิจกรรมที่เกี่ยวกับบริการของภาครัฐโดยตรง เช่น ภาคการเงินหรือบริการภาครัฐ อาทิ การทำธุรกรรมทางการเงินหรือบริการภาครัฐ

2.**หลักฐานยืนยันความเป็นมนุษย์** (Proof of Human : PoH): ใช้เพื่อยืนยันว่า “ผู้ใช้งานเป็นมนุษย์จริงและมีตัวตนเป็นเอกลักษณ์หรือไม่?” (Are you a real, unique human?) โดยไม่จำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้งาน ซึ่งเหมาะกับการใช้งานในพื้นที่ออนไลน์แบบเปิดและกรณีที่มีการเชื่อมต่อกันหลายแพลตฟอร์ม

ทั้งนี้ PoH ไม่ได้ถูกออกแบบมาเพื่อใช้แทน Digital ID แต่ทำหน้าที่เป็นกลไกเสริมที่ช่วยขยายความเชื่อมั่นไปยังพื้นที่ออนไลน์ซึ่งมักเป็นจุดเริ่มต้นของการหลอกลวงทางออนไลน์ เช่น โซเชียลมีเดีย บริการรับส่งข้อความ และแพลตฟอร์มซื้อขายสินค้า เป็นต้น ในบริบทเหล่านี้ PoH สามารถช่วยจำกัดการสร้างบัญชีปลอมและบัญชีที่ถูกสร้างขึ้นจำนวนมากโดยอัตโนมัติ รวมถึงลดการใช้บอตในการหลอกลวง และยังคงคุ้มครองความเป็นส่วนตัวของผู้ใช้งาน

ขณะเดียวกัน แนวโน้มในช่วงที่ผ่านมาแสดงให้เห็นว่าการนำ PoH มาใช้งานจำเป็นต้องดำเนินควบคู่กับกรอบด้านความเชื่อมั่นและความปลอดภัยที่ชัดเจน เพื่อให้สามารถรับมือกับการใช้งานระบบอัตโนมัติและการโจมตีในวงกว้างได้อย่างเหมาะสม และเพื่อหลีกเลี่ยงความเข้าใจผิดว่า PoH เป็นเครื่องมือรับรองเจตนา หรือความน่าเชื่อถือของผู้ใช้งานในเชิงพฤติกรรม

ในภูมิภาคเอเชียแปซิฟิก รัฐบาลหลายประเทศได้พัฒนาระบบยืนยันตัวตนทางดิจิทัลที่มีความเข้มแข็ง เพื่อรองรับการยืนยันตัวตนตามหลักการรู้จักลูกค้า (Know Your Customer: KYC) และเพิ่มความรับผิดชอบในภาคส่วนที่อยู่ภายใต้การกำกับดูแล อย่างไรก็ดี การหลอกลวงทางออนไลน์ส่วนใหญ่กลับเกิดขึ้นในพื้นที่ที่อยู่นอกขอบเขตการกำกับ เช่น โซเชียลมีเดีย บริการส่งข้อความและตลาดออนไลน์ เป็นต้น ซึ่งระบบยืนยันตัวตนทางดิจิทัลไม่ได้ถูกนำมาใช้หรือไม่สามารถนำมาใช้ได้อย่างเหมาะสม

ในบริบทดังกล่าว PoH จึงเข้ามามีบทบาทสำคัญในฐานะกลไกเสริมที่ช่วยเติมเต็มช่องว่างนี้ โดยอาศัยเครื่องมืออาทิ โทเคนยืนยันความเป็นมนุษย์ที่คุ้มครองความเป็นส่วนตัว (privacy-preserving human tokens) หรือการตรวจสอบผ่านอุปกรณ์ของผู้ใช้งาน (device-based verification) เพื่อจำกัดการสร้างบัญชีปลอมจำนวนมาก ขัดขวางการหลอกลวงที่อาศัยบอตทำงานเป็นระบบ และช่วยเสริมให้เครือข่ายผู้ใช้งานที่เป็นมนุษย์จริงมีความน่าเชื่อถือมากขึ้นตั้งแต่ก่อนที่เหยื่อจะถูกหลอกลวง

ทั้งนี้ การนำเทคโนโลยี PoH ไปใช้ให้เกิดผลจำเป็นต้องมีกลไกคุ้มครองที่ชัดเจน เปิดโอกาสให้ผู้ใช้งานควบคุมการใช้ข้อมูลของตนเองได้ และมีโครงสร้างการกำกับดูแลที่ป้องกันการนำไปใช้ในทางที่ผิด คุ้มครองความเป็นนิรนาม และรักษาความเชื่อมั่นของสาธารณะในระยะยาว

กรณีศึกษาในต่างประเทศ

ญี่ปุ่น – My Number : ระบบยืนยันตัวตนของรัฐที่สามารถยืนยันความเป็นเอกลักษณ์ของบุคคลได้ในวงกว้าง อย่างไรก็ตาม ปัญหาที่เกิดขึ้นจากการจัดการข้อมูลในช่วงที่ผ่านมาได้กระทบต่อความเชื่อมั่นของสาธารณะ ทำให้การขยายการใช้งานนอกภาครัฐยังมีข้อจำกัด ในบริบทนี้ ระบบ My Number อาจเป็นกรณีที่เหมาะสมที่จะถูกพัฒนาเป็นโมเดลแบบผสม (hybrid model) โดยใช้เป็นฐานของการยืนยันตัวตนจากรัฐ ควบคู่กับกลไก PoH ที่ช่วยยืนยันผู้ใช้งานในพื้นที่ออนไลน์อื่นๆ นอกเหนือจากบริการของภาครัฐโดยไม่กระทบต่อความเป็นส่วนตัว

เกาหลีใต้ – Real-name regime : เกาหลีใต้ใช้ระบบยืนยันตัวตนแบบชื่อจริงที่เชื่อมโยงข้อมูลระหว่างภาคการเงิน โทรคมนาคม และบริการภาครัฐอย่างทั่วถึง ทำให้ในทางปฏิบัติระบบชื่อจริงทำหน้าที่คล้ายกลไก PoH แต่ในขณะเดียวกันก็สร้างข้อถกเถียงด้านความเป็นส่วนตัวและสิทธิของประชาชนเมืองมากขึ้น ประสบการณ์ของเกาหลีใต้จึงสะท้อนความท้าทายของการพึ่งพาระบบรวมศูนย์ และเป็นเหตุผลที่ทำให้เริ่มมีความสนใจในแนวทางยืนยันตัวตนที่ผู้ใช้ควบคุมได้เองมากขึ้น

มาเลเซีย – MyDigital ID : มาเลเซียกำลังผลักดันระบบยืนยันตัวตนทางดิจิทัลที่เชื่อมโยงข้อมูลข้อมูลชีวภาพ (biometric data) เข้ากับทะเบียนราษฎร แนวทางดังกล่าวสอดคล้องกับหลักคิดของ PoH อย่างไรก็ดี การนำไปใช้ในวงกว้างยังขึ้นอยู่กับความเข้มแข็งของมาตรการคุ้มครองข้อมูลและระดับความเชื่อมั่นของประชาชนต่อระบบ

ฟิลิปปินส์ – PhilSys : ฟิลิปปินส์เป็นตัวอย่างของระบบยืนยันตัวตนทางดิจิทัลที่มีการลงทะเบียนและใช้งานในวงกว้างอย่างรวดเร็ว แสดงให้เห็นถึงศักยภาพในการทำหน้าที่คล้าย PoH อย่างไรก็ตาม การขยายตัวอย่างรวดเร็วยังมาพร้อมความท้าทายด้านการกำกับดูแลและการสื่อสารกับผู้ใช้งาน เพื่อให้ประชาชนเข้าใจระบบและเชื่อมั่นในการใช้งานในระยะยาว

การรับมือกับการหลอกลวงทางออนไลน์อย่างมีประสิทธิภาพจำเป็นต้องอาศัยกลไกด้านการยืนยันตัวตนของผู้ใช้ในสองระดับ โดยกิจกรรมที่เกี่ยวข้องกับบริการภาครัฐควรมีระบบการยืนยันตัวตนที่ชัดเจน ขณะที่แพลตฟอร์มออนไลน์แบบเปิดควรใช้กลไกยืนยันความเป็นมนุษย์ที่สามารถคุ้มครองความเป็นส่วนตัวของผู้ใช้ได้ โดยรูปแบบการยืนยันทั้งสองระดับจำเป็นต้องมีความโปร่งใส สามารถใช้งานข้ามระบบ (interoperable) และเปิดโอกาสให้ผู้ใช้งานสามารถควบคุมข้อมูลของตนเองได้ นอกจากนี้ การนำแนวนโยบายของภาครัฐไปปรับใช้กับแพลตฟอร์มระดับโลกไม่อาจอาศัยภาครัฐเพียงฝ่ายเดียว แต่ตัวกลางต่างๆ ไม่ว่าจะเป็นองค์กรกำหนดมาตรฐาน (standard bodies) ตัวกลางในภาคอุตสาหกรรม (industry intermediaries) หรือกรอบความร่วมมือแบบหลายภาคส่วน (multi-stakeholder frameworks) จะมีบทบาทสำคัญในการแปลงข้อกำหนดเชิงนโยบายให้แพลตฟอร์มดิจิทัลสามารถนำไปปฏิบัติได้จริง

ข้อเสนอแนะเชิงนโยบาย

ผสาน Digital ID และ PoH เข้ากับยุทธศาสตร์ป้องกันการหลอกลวงทางออนไลน์ : นำกลไกตรวจสอบความเป็นเอกลักษณ์ของผู้ใช้งานมาใช้ในกระบวนการทางการเงิน อีคอมเมิร์ซ และการสื่อสาร เพื่อลดการปลอมแปลงตัวตน บัญชีปลอม และการใช้บอต โดยกำหนดแนวทางใช้งานภายในที่ให้ความสำคัญกับความน่าเชื่อถือและความปลอดภัย เพื่อหลีกเลี่ยงการพึ่งพาเครื่องมือมากเกินไป

สนับสนุนมาตรฐานที่คุ้มครองความเป็นส่วนตัวและสามารถทำงานร่วมกันได้ระหว่างระบบ : ส่งเสริมการใช้ระบบยืนยันตัวตนและข้อมูลรับรอง (credentials) ควบคู่กับเทคนิคการเข้ารหัสข้อมูล (Cryptography) อาทิ หลักฐานแบบไม่เปิดเผยข้อมูล (zero-knowledge proofs) เพื่อคุ้มครองความเป็นนิรนามของผู้ใช้งานในกรณีที่เหมาะสม รองรับการใช้งานข้ามพรมแดน และป้องกันไม่ให้ PoH ถูกนำไปใช้เพื่อติดตามหรือจัดทำโปรไฟล์ผู้ใช้งาน

ส่งเสริมความร่วมมือและการประสานนโยบายในระดับภูมิภาค : ใช้เวทีความร่วมมือระดับภูมิภาคและพหุภาคี เช่น สภาที่ปรึกษาธุรกิจเอเปค (APEC Business Advisory Council: ABAC) หลักการระดับสูงของกลุ่ม G20 ว่าด้วยการเข้าถึงบริการการเงินดิจิทัล (G20 High-Level Principles for Digital Financial Inclusion) และกรอบงานด้านเศรษฐกิจดิจิทัลของสหประชาชาติ เพื่อกำหนดเป้าหมายร่วม แลกเปลี่ยนข้อมูลเชิงประจักษ์ และทดลองนำระบบการยืนยันตัวตนแบบ PoH ไปใช้ในภาคส่วนต่าง ๆ ผ่านกลไกพื้นที่ทดลอง (sandbox) เพื่อประเมินความสะดวกในการใช้งาน ความสามารถในการเข้าถึงเทคโนโลยีอย่างทั่วถึงของทุกกลุ่ม และความได้สัดส่วนของมาตรการ

การหลอกลวงทางออนไลน์ที่เกิดขึ้นอย่างต่อเนื่องสะท้อนว่าการสร้างความน่าเชื่อถือในโลกดิจิทัลยังเป็นเรื่องที่ท้าทาย ดังนั้น การนำระบบยืนยันตัวตนทางดิจิทัล (Digital ID) และหลักฐานยืนยันความเป็นมนุษย์ (Proof of Human) มาใช้ร่วมกันภายใต้กรอบการคุ้มครองความเป็นส่วนตัว การกำกับดูแลที่เหมาะสม และระบบที่สามารถทำงานร่วมกันได้ จะช่วยทำให้การกระทำผิดมีต้นทุนสูงขึ้น ลดการหลอกลวงในวงกว้าง โดยไม่กระทบต่อสิทธิของผู้ใช้งาน และสนับสนุนการพัฒนาเศรษฐกิจดิจิทัลของเอเชียให้ปลอดภัยและเข้าถึงได้มากขึ้น

บทนำ : การแพร่ระบาดของการหลอกลวงทางออนไลน์และช่องว่างเชิงนโยบาย

เมื่อสังคมและเศรษฐกิจพึ่งพาเทคโนโลยีดิจิทัลมากขึ้น อาชญากรรมออนไลน์ก็เพิ่มขึ้นอย่างรวดเร็วทั้งในด้านขนาดและความซับซ้อน ปัจจุบันเศรษฐกิจอาชญากรรมไซเบอร์ทั่วโลกมีมูลค่าสูงกว่า 10 ล้านล้านดอลลาร์สหรัฐ ซึ่งมีขนาดใกล้เคียงกับเศรษฐกิจที่ใหญ่เป็นอันดับสามของโลก หากเทียบตามผลิตภัณฑ์มวลรวมภายในประเทศ (GDP)[1] ในบรรดาอาชญากรรมไซเบอร์ทั้งหมด การหลอกลวงทางออนไลน์เป็นรูปแบบที่ขยายตัวอย่างต่อเนื่อง โดยผู้บริโภคทั่วโลกสูญเสียเงินมากกว่า 1 ล้านล้านดอลลาร์สหรัฐต่อปี

อย่างไรก็ตาม ผลกระทบของการหลอกลวงทางออนไลน์ไม่ได้จำกัดอยู่เพียงตัวเลขความเสียหายทางการเงินเท่านั้น เหยื่อจำนวนมากต้องเผชิญผลกระทบระยะยาวต่อสุขภาพจิตและคุณภาพชีวิต และมีความเชื่อมั่นต่อบริการดิจิทัลและเศรษฐกิจดิจิทัลน้อยลง ขณะเดียวกัน ภาครัฐยังต้องจัดสรรทรัพยากรจำนวนมากไปกับการบังคับใช้กฎหมาย การสร้างความตระหนักรู้ และการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ[2]

บทบาทสองด้านของภูมิภาคเอเชีย

ปัญหาการหลอกลวงทางออนไลน์ส่งผลกระทบต่อหลายภูมิภาคทั่วโลก แต่เอเชียแปซิฟิกเป็นพื้นที่ที่เผชิญปัญหานี้อย่างรุนแรงเป็นพิเศษ โดยรูปแบบการหลอกลวงที่พบมาก ได้แก่ การหลอกลงทุน การหลอกเชิงความสัมพันธ์ (romance scams) และการหลอกลวงแบบที่เรียกกันว่า “เชือดหมู” (pig-butchering) ซึ่งผู้กระทำผิดจะค่อย ๆ สร้างความสนิทใจและความไว้ใจ ก่อนหลอกให้เหยื่อโอนเงินหรือร่วมลงทุน การหลอกลวงลักษณะนี้มักเริ่มต้นจากโซเชียลมีเดียหรือแอปพลิเคชันส่งข้อความ และดำเนินการโดยเครือข่ายขนาดใหญ่ที่มีความเกี่ยวข้องกับกลุ่มอาชญากรรมข้ามชาติ

เอเชียตะวันออกเฉียงใต้มีบทบาทสำคัญในระบบดังกล่าว ทั้งในฐานะพื้นที่ที่มีเหยื่อจำนวนมาก ที่ตั้งของศูนย์ปฏิบัติการของผู้กระทำความผิด และแหล่งแรงงานที่ถูกดึงเข้าสู่ขบวนการเหล่านี้ โดยแรงงานจำนวนหนึ่งเป็นผู้เสียหายจากการค้ามนุษย์และไม่ได้เข้ามาเกี่ยวข้องโดยสมัครใจ[3,4]

ขณะเดียวกัน ประเทศที่พัฒนาแล้วในภูมิภาคเอเชียแปซิฟิก อาทิ ไต้หวัน ญี่ปุ่น และเกาหลีใต้ ก็มีความเกี่ยวข้องกับปัญหานี้อย่างหลีกเลี่ยงไม่ได้ ด้วยลักษณะของสังคมที่มีความเชื่อมั่นในระบบดิจิทัลสูงและมีการใช้เทคโนโลยีดิจิทัลอย่างทั่วถึง ผู้บริโภคในประเทศเหล่านี้จึงตกเป็นเป้าหมายของการหลอกลวงด้านการลงทุนและการปลอมแปลงตัวตนอยู่บ่อยครั้ง นอกจากนี้ ยังพบกรณีที่ประชาชนของประเทศเหล่านี้ถูกล่อลวงให้เดินทางไปทำงานในศูนย์หลอกลวงในต่างประเทศอีกด้วย[5] บริบทดังกล่าวสะท้อนให้เห็นว่าปัญหาการหลอกลวงทางออนไลน์ในเอเชียแปซิฟิกไม่ได้เป็นเพียงปัญหาภายในประเทศใดประเทศหนึ่ง แต่เป็นปัญหาที่เชื่อมโยงกันทั้งภูมิภาค การรับมือกับความท้าทายนี้จึงจำเป็นต้องอาศัยความร่วมมือระหว่างประเทศที่มีบริบทแตกต่างกัน ทั้งประเทศที่มีระดับการพัฒนาสูงและประเทศที่ได้รับผลกระทบจากการค้ามนุษย์ เพื่อให้สามารถจัดการปัญหาได้อย่างมีประสิทธิภาพ[6]

เทคโนโลยี: ทั้งตัวเร่งปัญหาและส่วนหนึ่งของทางออก

เทคโนโลยีได้เปลี่ยนวิธีการหลอกลวงทางออนไลน์ไปอย่างมาก จนแม้แต่รัฐบาลที่มีทรัพยากรพร้อมก็ยังตามรูปแบบการหลอกลวงใหม่ ๆ ได้ไม่ทัน

ประการแรก การโน้มน้าวเหยื่อถูกทำให้เป็นเรื่องเชิงระบบ เทคโนโลยีอย่างปัญญาประดิษฐ์ การโคลนเสียง และการสร้างภาพหรือวิดีโอปลอม (deepfakes) ถูกนำมาใช้ในการหลอกลวงมากขึ้น โดยพบว่ากรณีการหลอกลวงในภาคการเงินมากกว่าร้อยละ 42 เกี่ยวข้องกับการใช้ AI[7] ซึ่งเครื่องมือเหล่านี้ช่วยสร้างข้อความ ภาพ หรือเสียงที่ดูสมจริงในหลายภาษา ทำให้การหลอกลงทุนหรือการหลอกเชิงความสัมพันธ์ซึ่งต้องใช้เวลานาน สามารถทำได้โดยที่ผู้กระทำความผิดไม่จำเป็นต้องมีทักษะสูง เพียงทำตามรูปแบบหรือคู่มือที่ถูกพัฒนาและทดสอบมาแล้วเท่านั้น

ประการที่สอง การเข้าถึงเหยื่อทำได้ง่ายและรวดเร็วขึ้นอย่างแทบไม่มีขีดจำกัด เนื่องจากการสร้างบัญชีอัตโนมัติ ฟาร์มซิม และเครื่องมือที่สามารถใช้งานข้ามหลายแพลตฟอร์มได้ทำให้ผู้กระทำความมาผิดเพียงไม่กี่รายสามารถติดต่อผู้คนได้เป็นจำนวนมากผ่านโซเชียลมีเดีย แอปพลิเคชันส่งข้อความ และโทรศัพท์ภายในเวลาอันสั้น นอกจากนี้ บอตและระบบแนะนำเนื้อหา (recommendation systems) ยังถูกนำมาใช้เพื่อคัดเลือกกลุ่มเป้าหมายที่มีแนวโน้มจะหลงเชื่อได้ง่าย[8]

ประการที่สาม นวัตกรรมด้านการทำเงินของขบวนการอาชญากรรมมีการพัฒนาอย่างรวดเร็ว โดยโครงสร้างพื้นฐานคริปโต ช่องทางฟินเทค (fintech channels) เครือข่ายบัญชีม้า (money-mule networks) และระบบผสมธุรกรรมข้ามเครือข่าย (cross-chain mixers) ทำให้การเคลื่อนย้ายและปกปิดเส้นทางการเงินทำได้ง่ายและรวดเร็วมากขึ้น ขณะเดียวกัน ระบบชำระเงินแบบทันทีและกฎเกณฑ์การยืนยันตัวตนของลูกค้าและธุรกิจ (KYC/KYB) ที่ยังไม่เชื่อมโยงกันทั่วถึง ก็ยิ่งทำให้การสกัดกั้นธุรกรรมผิดกฎหมายทำได้ยากขึ้น[9]

ผลที่ตามมาจากพัฒนาการเหล่านี้ คือ ความเชื่อมั่นในระบบเศรษฐกิจดิจิทัลที่ลดลง เนื่องจากผู้กระทำผิดสามารถนำเทคโนโลยีใหม่มาใช้และปรับรูปแบบการหลอกลวงได้รวดเร็วกว่าที่ภาครัฐและหน่วยงานกำกับดูแลจะตอบสนองได้ทัน

อย่างไรก็ดี แม้ว่าเทคโนโลยีใหม่ๆ จะถูกใช้ในทางที่เป็นการส่งเสริมการกระทำความผิด แต่เทคโนโลยีเดียวกันนี้ก็สามารถเป็นส่วนหนึ่งของทางออกและช่วยฟื้นฟูความเชื่อมั่นได้เช่นกันหากได้รับการออกแบบและนำมาใช้อย่างเหมาะสม พร้อมมาตรการคุ้มครองที่ชัดเจน

ในด้านการยืนยันตัวตนทางดิจิทัล การพัฒนาระบบที่สามารถยืนยันตัวตนของผู้ใช้งานและตรวจสอบอุปกรณ์ และนิติบุคคลได้อย่างน่าเชื่อถือ โดยคำนึงถึงความเป็นส่วนตัว อาทิ การยืนยันตัวตนแบบไม่เปิดเผยข้อมูล การประเมินความน่าเชื่อถือของหมายเลขโทรศัพท์หรือซิมการ์ด รวมถึงการเพิ่มระดับการตรวจสอบในธุรกรรมที่มีความเสี่ยงสูง จะช่วยเพิ่มต้นทุนในการกระทำความผิด

ในด้านเนื้อหา การมีเครื่องมือที่สามารถยืนยันความถูกต้องและแท้จริงของเนื้อหา อาทิ การระบุแหล่งที่มาของภาพและวิดีโอด้วยเทคโนโลยีเข้ารหัส (cryptographic provenance) การยืนยันตัวตนผู้โทรหรือผู้ส่งข้อความ และการควบคุมความน่าเชื่อถือของโฆษณาและบัญชีผู้ใช้งานอย่างเข้มงวด จะช่วยลดโอกาสในการปลอมแปลงตัวตนและการแอบอ้างได้อย่างมีนัยสำคัญ

การแลกเปลี่ยนสัญญาณความเสี่ยง (signal-sharing) ระหว่างแพลตฟอร์มและเครือข่ายการชำระเงิน โดยออกแบบให้คุ้มครองความเป็นส่วนตัวของผู้ใช้ จะช่วยให้ตรวจจับการหลอกลวงที่ดำเนินการเป็นเครือข่ายได้ดีขึ้น และเมื่อดำเนินการร่วมกับการประเมินความเสี่ยงของธุรกรรมแบบทันที (real-time) และมาตรการชะลอการทำธุรกรรมในกรณีที่พบความผิดปกติ (cool-off) เช่น การยืนยันผู้รับเงินเพิ่มเติม หรือการเลื่อนเวลาการโอน เป็นต้น ก็จะช่วยลดความเสียหายได้ตั้งแต่จุดที่มีการโอนเงิน

การแก้ไขปัญหาการหลอกลวงจำเป็นต้องมองเหยื่อเป็นศูนย์กลางควบคู่ไปกับการบังคับใช้กฎหมาย ไม่ว่าจะเป็นการเปิดช่องทางให้สามารถระงับบัญชีหรือเนื้อหาที่เป็นอันตรายได้อย่างรวดเร็ว การเร่งกระบวนการติดตามและกู้คืนเงิน รวมถึงการมีกลไกที่ชัดเจนในการระบุและคุ้มครองแรงงานที่ถูกบังคับให้เข้ามาเกี่ยวข้องกับขบวนการหลอกลวง เพื่อยุติวงจรการแสวงหาประโยชน์อย่างแท้จริง[10]

ด้วยเหตุนี้ เทคโนโลยีจึงเป็นทั้งปัจจัยที่เอื้อต่อการก่ออาชญากรรม และเป็นส่วนสำคัญของแนวทางแก้ไขปัญหาเช่นกัน ภาครัฐ แพลตฟอร์มดิจิทัล และสถาบันการเงินจำเป็นต้องพัฒนาและปรับใช้เทคโนโลยีในเชิงป้องกัน (defensive technologies) อย่างต่อเนื่องให้ทันกับการปรับตัวของผู้กระทำผิด เนื่องจากการหลอกลวงทางออนไลน์ไม่ได้เป็นเพียงเหตุอาชญากรรมทางไซเบอร์รายกรณีเท่านั้น แต่สะท้อนถึงปัญหาเชิงโครงสร้างด้านความเชื่อมั่นในระบบเศรษฐกิจดิจิทัลในภาพรวม[11]

หากการหลอกลวงทางออนไลน์สะท้อนถึงความเปราะบางของความเชื่อมั่นในโลกออนไลน์ ระบบยืนยันตัวตนทางดิจิทัล (Digital ID) ก็เป็นหนึ่งในเครื่องมือที่สำคัญที่สุดในการช่วยฟื้นฟูความเชื่อมั่นดังกล่าว การยืนยันได้อย่างน่าเชื่อถือว่าใครอยู่เบื้องหลังธุรกรรมหรือการติดต่อสื่อสารแต่ละครั้ง จะช่วยเพิ่มต้นทุนในการกระทำผิด และสนับสนุนการพัฒนาเศรษฐกิจดิจิทัลที่ปลอดภัยยิ่งขึ้น ส่วนถัดไปของรายงานจะเป็นการวิเคราะห์ปัญหาที่ Digital ID ถูกออกแบบมาเพื่อแก้ไข เทคโนโลยีที่เกี่ยวข้อง และแนวนโยบายของประเทศต่างๆ ในภูมิภาค

การสร้างเชื่อมั่นทางดิจิทัลผ่านกลไกสองชั้น : ระบบยืนยันตัวตนทางดิจิทัล (Digital ID) และหลักฐานยืนยันความเป็นมนุษย์ (Proof of Human)

การรับมือกับการหลอกลวงทางออนไลน์อย่างมีประสิทธิผลจำเป็นต้องอาศัยระบบความเชื่อมั่นทางดิจิทัลที่ทำงานเป็นหลายชั้น แม้มาตรการบังคับใช้กฎหมายและการสร้างความตระหนักรู้จะยังคงมีความสำคัญ แต่อาจยังไม่เพียงพอ เนื่องจากการแก้ปัญหาอย่างยั่งยืนต้องอาศัยกลไกที่ช่วยยืนยันตัวตนและความแท้จริงของผู้ใช้งาน เพื่ออุดช่องโหว่ที่ผู้กระทำผิดใช้ในการขยายการหลอกลวง

ในบริบทนี้ ระบบยืนยันตัวตนทางดิจิทัล (Digital Identity: Digital ID) และหลักฐานยืนยันความเป็นมนุษย์ (Proof of Human: PoH) ถือเป็นโครงสร้างความเชื่อมั่นทางดิจิทัลสองชั้นที่มีบทบาทแตกต่างกันอย่างชัดเจน โดย Digital ID ใช้เพื่อยืนยันว่า “ผู้ใช้งานคือใคร?” (Who are you?) ผ่านการเชื่อมโยงบุคคลเข้ากับตัวตนจริงที่ได้รับการรับรองจากหน่วยงานของรัฐหรือสถาบันการเงิน ซึ่งเหมาะสำหรับการใช้งานในบริบทที่มีการกำกับดูแลและจำเป็นต้องระบุตัวตนอย่างชัดเจน เช่น การทำธุรกรรมทางการเงินหรือบริการภาครัฐ ในขณะที่หลักฐานยืนยันความเป็นมนุษย์ (Proof of Human: PoH) ใช้เพื่อยืนยันว่า “ผู้ใช้งานเป็นมนุษย์จริงและมีตัวตนเฉพาะหรือไม่?” (Are you a real, unique human?) โดยไม่จำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้งาน ซึ่งเหมาะสำหรับพื้นที่ออนไลน์แบบเปิดและเชื่อมต่อหลายแพลตฟอร์ม ซึ่งไม่จำเป็นหรือไม่เหมาะสมที่จะต้องเปิดเผยตัวตนของผู้ใช้งาน เมื่อนำทั้งสองชั้นมาใช้ร่วมกัน จะช่วยสร้างรากฐานที่สมดุล ระหว่างความรับผิดชอบและการคุ้มครองความเป็นส่วนตัวในระบบเศรษฐกิจดิจิทัล

ทั้งนี้ PoH ไม่ได้ถูกออกแบบมาเพื่อใช้แทนระบบ Digital ID แต่ทำหน้าที่เป็นกลไกเสริมที่ช่วยขยายความเชื่อมั่นไปยังพื้นที่ออนไลน์ซึ่งการยืนยันตัวตนแบบเต็มรูปแบบอาจไม่สามารถทำได้ หรือไม่เหมาะสมในทางปฏิบัติ

รูปแบบของเทคโนโลยียืนยันตัวตนทางดิจิทัล

ระบบยืนยันตัวตนทางดิจิทัล มีหลากหลายรูปแบบ โดยแต่ละรูปแบบถูกออกแบบมาเพื่อรับมือกับความเสี่ยงที่แตกต่างกัน ดังนี้

ระบบยืนยันตัวตนทางดิจิทัลที่ใช้ข้อมูลรับรอง (credential-based digital identity) เป็นระบบที่ใช้ข้อมูลในการรองรับตัวตนทางดิจิทัลซึ่งออกโดยหน่วยงานที่เชื่อถือได้ เช่น หน่วยงานภาครัฐ ธนาคาร ผู้ให้บริการโทรคมนาคม หรือสถาบันการศึกษา เป็นต้น เพื่อยืนยันข้อมูลพื้นฐานของผู้ใช้งาน อาทิ ชื่อ อายุ หรือสัญชาติ โดยข้อมูลเหล่านี้สามารถจัดเก็บไว้ในกระเป๋าเงินดิจิทัล (digital wallet) และนำไปใช้ยืนยันตัวตนกับบริการต่าง ๆ ได้ซ้ำ ๆ โดยไม่ต้องส่งเอกสารทุกครั้ง ทำให้การใช้งานมีความปลอดภัยและคุ้มครองความเป็นส่วนตัวมากกว่าการใช้เพียงสำเนาบัตรหรือภาพสแกน[12]

การยืนยันตัวตนด้วยข้อมูลชีวมิติ (biometric authentication) เป็นการตรวจสอบว่าบุคคลที่เข้าใช้งานเป็นบุคคลเดียวกับที่เคยลงทะเบียนไว้ก่อนหน้านี้หรือไม่ โดยอาศัยลักษณะเฉพาะทางกายภาพหรือพฤติกรรม อาทิ ลายนิ้วมือหรือใบหน้า วิธีนี้ช่วยลดความเสี่ยงจากการถูกสวมรอย แม้รหัสผ่านหรืออุปกรณ์ของเข้าของข้อมูลจะถูกละเมิด อย่างไรก็ดี ข้อมูลชีวมิติทำหน้าที่ยืนยันผู้ใช้งาน (user) เท่านั้น แต่ไม่สามารถระบุหรือรับรองตัวตน (identity) ที่แท้จริงของบุคคลดังกล่าวได้[13]

ระบบยืนยันตัวตนทางดิจิทัลแบบผสมผสาน (hybrid digital identity) เป็นการนำหลายปัจจัยมาใช้ร่วมกัน อาทิ ข้อมูลที่ผ่านการรับรองจากภาครัฐ และการยืนยันด้วยข้อมูลชีวมิติ เพื่อสร้างกลไกการยืนยันตัวตนที่มีความน่าเชื่อถือสูง โดยระบบลักษณะนี้ถูกออกแบบมาให้สามารถใช้งานข้ามแพลตฟอร์มได้ มีความรัดกุม และเปิดโอกาสให้ผู้ใช้งานสามารถควบคุมข้อมูลของตนเองได้มากขึ้น[14]

ระบบทั้งหมดที่กล่าวมานี้ถูกออกแบบให้รองรับกระบวนการยืนยันตัวตนตามหลัก KYC (Know-Your-Customer) และไม่ใช่ระบบแบบนิรนาม เนื่องจากมีเป้าหมายเพื่อให้สามารถตรวจสอบย้อนกลับได้ รองรับการปฏิบัติตามกฎระเบียบ และสร้างความรับผิดชอบในการดำเนินกิจกรรมที่อยู่ภายใต้การกำกับดูแล

แนวนโยบายของประเทศต่างๆ ในภูมิภาคเอเชียแปซิฟิก

การพัฒนาเทคโนโลยีการยืนยันตัวตนทางดิจิทัลไม่สามารถดำเนินไปได้อย่างมีประสิทธิภาพ หากขาดกรอบนโยบายรองรับที่เหมาะสม ระบบ Digital ID จึงต้องอาศัยการกำหนดมาตรฐานที่ชัดเจน การคุ้มครองข้อมูลส่วนบุคคล และการส่งเสริมให้เกิดการใช้งานอย่างทั่วถึงในภาคส่วนต่าง ๆ เพื่อให้สามารถทำหน้าที่ได้จริงในทางปฏิบัติ โดยแนวทางสำคัญในการดำเนินการประกอบไปด้วยปัจจัยดังต่อไปนี้

- **การรับรองสถานะทางกฎหมายของ** Digital ID เพื่อให้สามารถนำไปใช้ในธุรกรรมทางการเงิน การทำสัญญา และการเข้าถึงบริการภาครัฐได้อย่างมีผลผูกพัน
- **การกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล**ที่รัดกุม ทั้งในด้านการจัดเก็บ การจำกัดการใช้งาน และการมีช่องทางเยียวยาเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล
- **การส่งเสริมให้** Digital ID **ได้รับการยอมรับและใช้งานในทุกภาคส่วน** ไม่เพียงเฉพาะหน่วยงานรัฐ แต่รวมถึงแพลตฟอร์มดิจิทัล สถาบันการเงิน และผู้ให้บริการสาธารณูปโภค ซึ่งมักเป็นจุดแรกที่ต้องรับมือกับการหลอกลวงทางออนไลน์

หลายประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้กำลังเดินหน้าพัฒนาระบบการยืนยันตัวตนทางดิจิทัลอย่างต่อเนื่อง เพื่อส่งเสริมให้อุตสาหกรรมเศรษฐกิจดิจิทัลภายในประเทศมีความน่าเชื่อถือมากขึ้น ตัวอย่างเช่น

ประเทศไทย ได้พัฒนาแพลตฟอร์ม National Digital ID (NDID) เพื่อเชื่อมโยงระบบการยืนยันตัวตนของประชาชนระหว่างธนาคาร ผู้ให้บริการโทรคมนาคม และหน่วยงานภาครัฐ[15]

อินโดนีเซียและฟิลิปปินส์ กำลังผลักดันระบบ e-ID ระดับประเทศ โดยเชื่อมโยงกับนโยบายด้านการเข้าถึงบริการทางการเงินและสวัสดิการสังคม

เวียดนาม ได้เริ่มนำการยืนยันตัวตนด้วยข้อมูลชีวมิติมาใช้ในบริการภาครัฐผ่านระบบอิเล็กทรอนิกส์

แม้ระดับความพร้อมของแต่ละประเทศจะยังแตกต่างกัน แต่ทิศทางนโยบายของภูมิภาคกำลังขยับจากการมุ่งพัฒนาระบบภายในประเทศ ไปสู่การให้ความสำคัญกับความสามารถในการเชื่อมต่อระบบการยืนยันตัวตนระหว่างประเทศมากขึ้น แนวโน้มดังกล่าวสะท้อนให้เห็นว่าผู้กำหนดนโยบายเริ่มตระหนักว่า การเคลื่อนย้ายแรงงาน การย้ายถิ่นฐาน และการค้าในภูมิภาคเอเชียแปซิฟิกทำให้จำเป็นต้องมีระบบการยืนยันตัวตนดิจิทัลที่สามารถใช้งานข้ามพรมแดนได้ ไม่ใช่จำกัดอยู่เพียงภายในประเทศเท่านั้น

ประเทศที่พัฒนาแล้วมักมีระบบการยืนยันตัวตนทางดิจิทัลระดับประเทศที่มีคุณภาพและและถูกนำไปใช้งานในภาคส่วนต่าง ๆ มากขึ้นอย่างต่อเนื่อง ตัวอย่างสำคัญ ได้แก่

สิงคโปร์ ใช้ระบบ SingPass เป็นช่องทางหลักในการเข้าถึงบริการของทั้งภาครัฐและเอกชน ครอบคลุมบริการธนาคาร การดูแลสุขภาพ และอีคอมเมิร์ซ[16]

เกาหลีใต้ ต่อยอดระบบทะเบียนราษฎรไปสู่แพลตฟอร์มระบบการยืนยันตัวตนแบบดิจิทัลที่ครอบคลุมมากขึ้น โดยเชื่อมโยงบริการภาครัฐ ธุรกรรมทางการเงิน และการยืนยันตัวตนผ่านโทรศัพท์มือถือ

ญี่ปุ่น ใช้ระบบ “My Number” ซึ่งกำหนดหมายเลขประจำตัว 12 หลักให้แก่ประชาชนทุกคน เชื่อมโยงกับงานด้านสาธารณสุข ภาษี และงานธุรการของรัฐมากขึ้น[17] พร้อมทั้งอยู่ระหว่างการขยายการใช้งานไปสู่ภาคการเงินและการยอมรับในประเทศอื่นๆ

แม้ว่าแนวทางและความรวดเร็วในการพัฒนาของแต่ละประเทศจะแตกต่างกัน แต่ภาพรวมสะท้อนให้เห็นว่า ระบบการยืนยันตัวตนระดับประเทศ สามารถพัฒนาไปไกลกว่าการเป็นเพียงเครื่องมือสำหรับการเข้าสู่ระบบต่างๆ อย่างปลอดภัย โดยสามารถทำหน้าที่เป็นโครงสร้างพื้นฐานสำคัญของเศรษฐกิจดิจิทัลในภาพรวม รวมทั้งยังสามารถเป็นแนวทางสำหรับประเทศอาเซียนที่อยู่ระหว่างการพัฒนาระบบการยืนยันตัวตนภายในประเทศ หรือการพิจารณาแนวทางการส่งเสริมความเชื่อมโยงระหว่างระบบของประเทศต่างๆ กับประเทศอื่นในภูมิภาค

นอกจากนี้ ประสบการณ์จากประเทศเหล่านี้ยังชี้ให้เห็นว่าการดำเนินการโดยภาครัฐเพียงฝ่ายเดียวไม่เพียงพอ และความสำเร็จของระบบการยืนยันตัวตนขึ้นอยู่กับความสามารถในการนำไปใช้งานจริงในระบบนิเวศดิจิทัลโดยรวม ซึ่งต้องอาศัยความร่วมมือระหว่างภาครัฐ สถาบันการเงิน และแพลตฟอร์มเทคโนโลยีอย่างต่อเนื่อง

บทบาทของระบบการยืนยันตัวตนในการรับมือกับการหลอกลวงทางออนไลน์

ระบบการยืนยันตัวตนถือเป็นหนึ่งในเครื่องมือเชิงโครงสร้างที่มีบทบาทสำคัญในการรับมือกับการหลอกลวงและการทุจริตในโลกดิจิทัล ระบบดังกล่าวช่วยยืนยันบุคคล อุปกรณ์ และองค์กรในลักษณะที่สามารถตรวจสอบได้และไม่เปิดช่องให้ใช้งานโดยไม่ระบุตัวตน ส่งผลให้การแอบอ้างตัวตนทำได้ยากขึ้น ลดพื้นที่ของการหลบเลี่ยงความรับผิด และเพิ่มต้นทุนให้กับการกระทำผิด แม้ระบบการยืนยันตัวตนจะไม่ใช่คำตอบทั้งหมด แต่ก็ทำหน้าที่เป็นรากฐานสำคัญของความเชื่อมั่นทางดิจิทัล โดยเฉพาะในกิจกรรมที่เกี่ยวข้องกับบริการของภาครัฐ ซึ่งจำเป็นต้องผูกโยงธุรกรรมและบริการต่าง ๆ เข้ากับบุคคลหรือหน่วยงานที่มีตัวตนชัดเจนและสามารถตรวจสอบได้

การปิดช่องโหว่ที่ถูกใช้ในการหลอกลวง

การหลอกลวงทางออนไลน์มักเกิดขึ้นในภาคส่วนที่ระบบการยืนยันตัวตนยังไม่ไปถึง โดยผู้กระทำผิดสามารถอาศัยบอตและบัญชีปลอมในการส่งข้อความหรือเข้าถึงผู้ใช้งานจำนวนมากด้วยต้นทุนที่ต่ำ ใช้เทคโนโลยีสร้างภาพหรือเสียงปลอมเพื่อแอบอ้างบุคคลที่น่าเชื่อถือ หรือเข้าควบคุมบัญชีของผู้ใช้งานจริงเพื่อนำไปใช้ในการหลอกลวงเหยื่อ นอกจากนี้ เมื่อแพลตฟอร์มต่าง ๆ ใช้มาตรการยืนยันตัวตนที่ไม่เข้มแข็งหรือขาดความสอดคล้องกัน โอกาสที่การกระทำความผิดเหล่านี้จะประสบความสำเร็จก็ยิ่งเพิ่มสูงขึ้น

ระบบการยืนยันตัวตนมีบทบาทสำคัญในการช่วยลดความเสี่ยงดังกล่าวได้ในธุรกรรมที่เกี่ยวข้องกับการให้บริการของรัฐ เนื่องจากแนวทางการเชื่อมโยงการติดต่อและการทำธุรกรรมทางดิจิทัลเข้ากับตัวตนที่ผ่านการตรวจสอบแล้ว ทำให้ผู้กระทำผิดไม่สามารถดำเนินการอย่างนิรนามได้ และช่วยเสริมความเชื่อมั่นให้กับผู้ใช้งาน ภาคธุรกิจ และหน่วยงานกำกับดูแลในการทำธุรกรรมกับบุคคลอื่นๆ บนโลกออนไลน์ อย่างไรก็ดี การหลอกลวงจำนวนมากกลับเริ่มต้นในพื้นที่ที่อยู่นอกกรอบการกำกับดูแล เช่น โซเชียลมีเดีย แอปพลิเคชันรับส่งข้อความ หรือตลาดซื้อขายที่ไม่เป็นทางการ (informal marketplaces) ซึ่งไม่สามารถนำระบบการยืนยันตัวตนตามหลัก KYC มาใช้ได้โดยตรง การรับมือกับความเสี่ยงในพื้นที่เหล่านี้จึงจำเป็นต้องอาศัยแนวทางที่แตกต่างออกไป และให้ความสำคัญกับการคุ้มครองความเป็นส่วนตัวของผู้ใช้งานมากขึ้น ตัวอย่างเช่น การใช้หลักฐานยืนยันความเป็นมนุษย์ (Proof of Human)

แม้ระบบการยืนยันตัวตนจะมีความเข้มแข็งเพียงใด ก็ยังไม่สามารถแก้ไขปัญหาการหลอกลวงทั้งหมดได้ ความท้าทายดังกล่าวทำให้แนวคิดในการนำหลักฐานยืนยันความเป็นมนุษย์มาใช้ได้รับความสนใจมากขึ้น เนื่องจากเป็นกลไกที่มุ่งยืนยันว่าผู้ใช้งานเป็นมนุษย์จริง โดยไม่จำเป็นต้องเปิดเผยข้อมูลระบุตัวตนส่วนบุคคล

หลักฐานยืนยันความเป็นมนุษย์ (Proof of Human) : แนวคิดและความสำคัญเชิงนโยบาย

หลักฐานยืนยันความเป็นมนุษย์คืออะไร

หลักฐานยืนยันความเป็นมนุษย์ หรือ Proof of Human (PoH) เป็นแนวทางใหม่ที่กำลังถูกพัฒนาอย่างต่อเนื่อง เพื่อเสริมสร้างความเชื่อมั่นในโลกดิจิทัล โดย PoH หมายถึงระบบที่ออกแบบมาเพื่อป้องกันการสร้างตัวตนปลอมหรือบัญชีซ้ำจำนวนมาก และช่วยยืนยันว่า ผู้ที่ทำกิจกรรมออนไลน์เป็นมนุษย์จริง ไม่ใช่บอตหรือบัญชีปลอมที่ถูกสร้างขึ้นมา สิ่งที่ทำให้ PoH แตกต่างจากเครื่องมืออื่น ๆ อาทิ การสมัครบัญชีทั่วไปหรือการทำแบบทดสอบ CAPTCHA คือ PoH ไม่ได้ตรวจสอบเพียงครั้งเดียวแล้วจบ แต่พยายามสร้างสัญญาณยืนยันความเป็นมนุษย์ที่สามารถนำกลับมาใช้ซ้ำได้ และสามารถขยายการใช้งานไปยังหลายแพลตฟอร์ม โดยที่ยังสามารถคงคุ้มครองความเป็นส่วนตัวของผู้ใช้งาน และไม่เปิดเผยข้อมูลส่วนบุคคลมากเกินความจำเป็น

ที่สำคัญ PoH ไม่ได้ถูกออกแบบมาเพื่อใช้แทนระบบการยืนยันตัวตนของรัฐ แต่เข้ามาเติมเต็มในอีกระดับหนึ่ง กล่าวคือ PoH มุ่งที่จะยืนยันว่า “ผู้ใช้งานเป็นมนุษย์จริงหรือไม่” ไม่ใช่การระบุว่า “ผู้ใช้งานคือใคร”

ความแตกต่างหลักของ PoH เมื่อเทียบกับกลไกการยืนยันตัวตนรูปแบบอื่นๆ คือระบบการยืนยันตัวตนแบบดั้งเดิมจะใช้เพื่อตอบคำถามว่า “ผู้ใช้งานคือใคร” ผ่านการเชื่อมโยงบุคคลเข้ากับข้อมูลที่ผ่านการรับรอง อาทิ ชื่อ หรือหมายเลขประจำตัวประชาชน ในขณะที่เครื่องมืออย่างรหัสผ่านหรือการยืนยันหลายขั้นตอนช่วยป้องกันบัญชีหลังจากถูกสร้างขึ้นแล้ว แต่ไม่สามารถป้องกันการสร้างบัญชีปลอมตั้งแต่ต้นได้ ที่ผ่านมา CAPTCHA เคยถูกใช้เป็นเครื่องมือแก้ปัญหานี้ โดยอาศัยการแก้ปริศนาเพื่อทดสอบความเป็นมนุษย์ อย่างไรก็ดี เมื่อบอตและปัญญาประดิษฐ์มีความสามารถสูงขึ้น วิธีการดังกล่าวจึงได้ผลน้อยลง และยังสร้างความยุ่งยากให้กับผู้ใช้งาน ในบริบทนี้ PoH จึงเข้ามาตอบโจทย์ในจุดที่แตกต่าง โดยมุ่งยืนยันว่าผู้ใช้งาน “เป็นมนุษย์จริง” ตั้งแต่ต้น โดยแนวคิดนี้สอดคล้องกับความพยายามในหลายภาคส่วนในการลดปัญหาบอต การสร้างบัญชีปลอม รวมถึงแนวคิดเรื่องการป้องกันการสร้างตัวตนซ้ำซ้อน ที่ใช้กันในแวดวงเทคโนโลยีบล็อกเชน (sybil resistance)

กล่าวโดยสรุป PoH เป็นส่วนหนึ่งของแนวทางใหม่ในการสร้างสมดุลระหว่างความน่าเชื่อถือของผู้ใช้งาน การคุ้มครองความเป็นส่วนตัว และความสามารถในการนำไปใช้ในระบบดิจิทัลขนาดใหญ่

รูปแบบต่าง ๆ ในการยืนยันหลักฐานความเป็นมนุษย์

PoH สามารถนำไปใช้ได้หลายรูปแบบ โดยแต่ละรูปแบบให้ระดับความน่าเชื่อถือและการคุ้มครองความเป็นส่วนตัวที่แตกต่างกัน ตารางด้านล่างสรุปรูปแบบหลักของการยืนยัน PoH กลไกการทำงาน ประสบการณ์ของผู้ใช้งาน และตัวอย่างการนำไปใช้ในทางปฏิบัติ

รูปแบบการยืนยัน PoH	กลไกการทำงาน	ประสบการณ์ของผู้ใช้งาน	รูปแบบการยืนยัน PoH
การยืนยันด้วยข้อมูลชีวมิติ (ในรูปแบบที่คุ้มครองความเป็นส่วนตัว) (biometric-based)	เป็นการตรวจสอบความมีชีวิต (liveness check) เพียงครั้งเดียว อาทิ การกะพริบตาหรือหมุนศีรษะ ระบบจะออก “โทเคนยืนยันความเป็นมนุษย์” (human token) ด้วยเทคโนโลยีเข้ารหัส (cryptography) โดยไม่จัดเก็บหรือส่งต่อข้อมูลชีวมิติ	เป็นการยืนยันสั้น ๆ เพียงครั้งเดียว คล้ายการปลดล็อกโทรศัพท์ โดยไม่มีการเปิดเผยข้อมูลส่วนบุคคล	ช่วยป้องกันการสร้างบัญชีปลอมจำนวนมาก เหมาะสำหรับแพลตฟอร์มที่ต้องการหลักฐาน PoH ที่มีความน่าเชื่อถือสูง เช่น การทำธุรกรรมทางการเงินหรือกิจกรรมที่มีความเสี่ยงสูง เป็นต้น
การยืนยันจากอุปกรณ์หรือฮาร์ดแวร์ (device/hardware based)	ใช้การรับรองอุปกรณ์ (device attestation) เพื่อยืนยันว่าเป็นอุปกรณ์จริง ไม่ใช่อุปกรณ์ปลอม และสามารถผูกหลักการ “ผู้ใช้งานหนึ่งคนต่อหนึ่งอุปกรณ์” (one human = one device) โดยไม่จำเป็นต้องทราบตัวตนผู้ใช้งาน	เป็นการตรวจสอบเบื้องหลังในขั้นตอนสมัครหรือใช้งาน ไม่มีการใช้ข้อมูลชีวมิติ	ช่วยจำกัดการทำงานของฟาร์มบอต โดยทำให้การสร้างบัญชีจำนวนมากด้วยระบบอัตโนมัติทำได้ยากขึ้น ไม่ว่าจะเป็นในแอปแชต โซเชียลมีเดีย หรือแพลตฟอร์มเกม
การยืนยันผ่านปฏิสัมพันธ์หรือโจทย์ทดสอบ (interaction/challenge based)	ผู้ใช้งานทำกิจกรรมที่คล้ายการตรวจสอบความมีชีวิต (liveliness-like prompts) หรือการตอบโจทย์แบบเข้ารหัส (cryptographic challenge-response tasks) ที่บอตทำได้ยาก โดยไม่ใช้ข้อมูลชีวมิติ	เป็นการโต้ตอบง่าย ๆ ระหว่างคนกับระบบ เช่น การเคลื่อนไหวตามจังหวะ หรือการตอบสนองภายในเวลาที่กำหนด ซึ่งสร้างภาระน้อยกว่า CAPTCHA แบบดั้งเดิม	เหมาะสำหรับแพลตฟอร์มโซเชียลและพื้นที่ออนไลน์ เพื่อลดการใช้งานของบัญชีปลอม โดยไม่ต้องใช้ระบบการยืนยันตัวตนหรือ ข้อมูลชีวมิติ
การรับรองผ่านเครือข่ายความเชื่อถือทางสังคม (social/web-of-trust attestation)	ผู้ใช้งานได้รับการยืนยันความเป็นมนุษย์จากสมาชิกในเครือข่ายออนไลน์ที่น่าเชื่อถือ และแพลตฟอร์มนำการยืนยันดังกล่าวมาแปลงเป็นสัญญาณ PoH	การรับรองที่ทำได้โดยง่ายจากผู้ใช้งานหรือเครือข่ายออนไลน์ที่ผ่านการตรวจสอบแล้ว	เหมาะกับแพลตฟอร์มที่ผู้ใช้งานติดต่อกันโดยตรง (peer-to-peer marketplaces) แพลตฟอร์มรับงานอิสระ (gig platforms) หรือระบบยืนยันตัวตนที่อาศัยความร่วมมือของชุมชนผู้ใช้งาน (community-based verification environments)

ตารางที่ 3.1: รูปแบบการยืนยันหลักฐานความเป็นมนุษย์ *(Proof of Human: PoH)*

บทบาทของหลักฐานยืนยันความเป็นมนุษย์ในการรับมือกับการหลอกลวงทางออนไลน์

แม้แนวคิดเรื่อง Proof of Human (PoH) จะยังอยู่ในช่วงเริ่มต้นของการพัฒนา แต่ก็มีศักยภาพสูงในการนำมาใช้เป็นกลไกเสริมเพื่อรับมือกับปัญหาการหลอกลวงและการทุจริตในโลกดิจิทัล ปัจจุบัน การหลอกลวงทางออนไลน์ไม่ได้เกิดจากการกระทำเป็นรายกรณีเท่านั้น หากแต่ขับเคลื่อนด้วยขนาดและความรวดเร็วของการดำเนินการ เนื่องจากกลุ่มอาชญากรและเครือข่ายค้ามนุษย์สามารถสร้างบัญชีปลอมจำนวนมากได้ในเวลาอันสั้น และใช้ระบบอัตโนมัติดำเนินกลโกงหลากหลายรูปแบบ ตั้งแต่การหลอกลงทุนระยะยาวไปจนถึงการบริหารเครือข่ายบัญชีม้าเพื่อรับและโอนเงินผิดกฎหมาย ความสามารถในการสร้างตัวตนดิจิทัลปลอมได้อย่างง่ายดายและในปริมาณมากเช่นนี้ ทำให้ต้นทุนของการหลอกลวงลดลงอย่างมาก และในขณะเดียวกันก็เพิ่มภาระให้กับแพลตฟอร์มและหน่วยงานกำกับดูแลในการตรวจจับและยับยั้งพฤติกรรมที่เป็นอันตรายได้อย่างทันท่วงที

ในบริบทดังกล่าว PoH สามารถเข้ามาช่วยปรับสมดุลของระบบได้ โดยทำหน้าที่เสริมความแข็งแรงให้กับเครือข่ายผู้ใช้งานที่เป็นมนุษย์จริง และจำกัดการขยายตัวของบัญชีปลอมหรือบัญชีอัตโนมัติในวงกว้าง รวมทั้งเพิ่มการตรวจสอบในจุดสำคัญของระบบ อาทิ ขั้นตอนการสร้างบัญชีหรือการทำธุรกรรม ทำให้การสร้างบัญชีปลอมจำนวนมากภายในระยะเวลาอันสั้นทำได้ยากขึ้น แนวทางเช่นนี้ช่วยลดทั้งขนาดและความเร็วของการแพร่กระจายของกลโกงตั้งแต่ระยะเริ่มต้น ก่อนที่ความเสียหายจะลุกลามเป็นวงกว้าง

การยืนยันความเป็นมนุษย์ในรูปแบบที่สามารถตรวจสอบได้ (verifiable humanness) มีประโยชน์ได้หลายด้าน ดังนี้

ช่วยลดการสร้างบัญชีปลอมซึ่งถูกใช้เป็นเครื่องมือในการหลอกลวงของผู้กระทำผิด ไม่ว่าจะเป็นการหลอกลวงเชิงความสัมพันธ์ การหลอกสมัครงาน หรือการหลอกลงทุน โดยแทนที่จะจัดการกับบัญชีเหล่านี้หลังจากที่เหยื่อได้รับความเสียหายแล้ว PoH สามารถช่วยจำกัดจำนวนบัญชีที่ใช้ในการกระทำความผิดได้ตั้งแต่ต้น

ช่วยปกป้องระบบการเงินโดยการลดการใช้บัญชีม้าในการทำธุรกรรม เนื่องจากธนาคารและเครือข่ายการชำระเงินมักประสบความยากลำบากในการแยกแยะผู้ใช้งานทั่วไปออกจากบัญชีที่ถูกนำไปใช้ในทางทุจริต สัญญาณยืนยันความเป็นมนุษย์ (sign of humanness) ที่สามารถนำมาใช้ซ้ำได้จึงอาจช่วยเสริมการทำงานของมาตรการการรู้จักลูกค้า (Know Your Customer: KYC) และ การป้องกันและปราบปรามการฟอกเงิน (Anti-Money Laundering: AML) ที่มีอยู่โดยไม่จำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลเพิ่มเติมอยู่ตลอดเวลา

ช่วยฟื้นฟูความเชื่อมั่นในอีคอมเมิร์ซและพื้นที่ออนไลน์ ในบริบทที่การหลอกลวงทำให้ผู้ใช้งานจำนวนมากขาดความไว้วางใจในบริการทางดิจิทัล การสามารถยืนยันได้ว่าผู้ซื้อ ผู้ขาย หรือผู้ใช้งานในพื้นที่ออนไลน์เป็นบุคคลจริง อาจช่วยให้แพลตฟอร์มที่ผู้ใช้งานติดต่อกันโดยตรง (peer-to-peer marketplaces) แพลตฟอร์มรับงานอิสระ (gig platforms) และพื้นที่ทางสังคมในโลกดิจิทัล (social spaces) กลับมาน่าเชื่อถือมากขึ้นในระยะยาว

มาตรการคุ้มครองและการกำกับดูแล

การกำหนดมาตรการคุ้มครองที่เหมาะสมเป็นสิ่งจำเป็นเพื่อป้องกันไม่ให้ PoH ถูกใช้เป็นเครื่องมือในการสอดส่องประชาชนโดยไม่เหมาะสม แนวทางในการพัฒนา PoH ในปัจจุบันจึงให้ความสำคัญกับการออกแบบระบบที่คำนึงถึงการคุ้มครองความเป็นส่วนตัวเป็นหลัก (privacy-preserving design) โดยอาศัยเทคโนโลยีด้านเข้ารหัส (cryptographic proofs) และหลักฐานแบบไม่เปิดเผยข้อมูล (zero-knowledge proofs) ซึ่งช่วยให้ผู้ใช้งานสามารถแสดงความเป็นมนุษย์ได้โดยไม่ต้องเปิดเผยข้อมูลส่วนบุคคลที่สามารถระบุตัวตนของผู้ใช้งานได้ ความแตกต่างระหว่างการ “ยืนยันความเป็นมนุษย์” (ผู้ใช้งานเป็นมนุษย์หรือไม่) กับการ “เปิดเผยตัวตน” (ผู้ใช้งานคือใคร) จึงเป็นประเด็นสำคัญต่อการคุ้มครองสิทธิความเป็นส่วนตัวและการรักษาความเชื่อมั่นของผู้ใช้งานจากทุกประเทศ นอกจากการออกแบบด้านเทคนิคแล้ว ระบบ PoH ยังต้องอาศัยการกำกับดูแลที่เหมาะสม การมีบทบาทของหน่วยงานกำกับ องค์กรกำหนดมาตรฐาน หรือกลไกตรวจสอบร่วมจากหลายภาคส่วน (multi-stakeholder audits) สามารถช่วยลดความเสี่ยงที่ PoH จะถูกนำไปใช้เพื่อติดตามพฤติกรรมหรือจัดทำโปรไฟล์ของผู้ใช้งานอย่างไม่เหมาะสม

นอกจากนี้ การคุ้มครองสิทธิของผู้ใช้งานและการส่งเสริมการเข้าถึงเทคโนโลยีอย่างทั่วถึงก็เป็นประเด็นที่จำเป็นต้องให้ความสำคัญ การยืนยันตัวตนของผู้ใช้งานควรเป็นไปโดยสมัครใจ มีความโปร่งใส และสามารถยกเลิกได้ โดยผู้ใช้งานต้องเข้าใจและควบคุมได้ว่าข้อมูลหรือสัญญาณ PoH ของตนจะถูกนำไปใช้อย่างไร การมีเครื่องมือเสริมอย่างกลไกการยืนยันอายุจะสามารถช่วยคุ้มครองสิทธิของเด็กและเยาวชนได้โดยไม่ต้องเปิดเผยข้อมูลอ่อนไหวของผู้ใช้งาน นอกจากนี้ การกำหนดทางเลือกในการยืนยันหลายรูปแบบก็จะสามารถช่วยส่งเสริมการเข้าถึงเทคโนโลยีของผู้ใช้งานที่มีข้อจำกัดด้านอุปกรณ์ เทคโนโลยี หรือการเชื่อมต่ออินเทอร์เน็ต ท้ายที่สุด ความน่าเชื่อถือของ PoH จะขึ้นอยู่กับความสามารถในการสร้างสมดุลระหว่างการเพิ่มความปลอดภัยบนพื้นที่ออนไลน์ กับการเคารพความเป็นส่วนตัว การเข้าถึงอย่างทั่วถึง และความสอดคล้องกับเป้าหมายในการเสริมสร้างความเชื่อมั่นทางดิจิทัลที่ประเทศในภูมิภาคเอเชียแปซิฟิคยึดถือร่วมกัน

อย่างไรก็ดี การพึ่งพามาตรการคุ้มครองในเชิงเทคนิคเพียงอย่างเดียวอาจไม่เพียงพอ การนำ PoH มาใช้ให้ได้ผลจำเป็นต้องมีกลไกกำกับดูแลที่สอดคล้องกับการทำงานจริงของระบบนิเวศดิจิทัลในภูมิภาคเอเชียแปซิฟิก โดยปกติแล้ว ระบบยืนยันตัวตนทางดิจิทัล (digital ID) ของแต่ละประเทศมักดำเนินการตามกรอบกฎหมายและนโยบายภายในประเทศ ขณะที่การใช้งานจริงของผู้ใช้งานส่วนใหญ่ (รวมถึงบริบทที่มักความเสี่ยงด้านความเป็นส่วนตัว) มักเกิดขึ้นบนแพลตฟอร์มระดับโลก ความแตกต่างเชิงโครงสร้างนี้ทำให้เกิดความท้าทายในการเชื่อมโยงการกำกับดูแลระหว่างภาครัฐกับแพลตฟอร์ม

ด้วยเหตุนี้ จึงจำเป็นต้องมีกลไกกำกับดูแลที่เป็นตัวกลาง (neutral governance layer) ที่สามารถเชื่อมนโยบายของรัฐกับการดำเนินการของแพลตฟอร์มให้อยู่ในทิศทางเดียวกัน โดยกลไกนี้สามารถช่วยถ่ายทอดข้อกำหนดเชิงนโยบายให้เป็นแนวทางปฏิบัติที่นำไปใช้ได้จริง รวมทั้งเป็นพื้นในการรวมตัวของผู้มีส่วนได้ส่วนเสีย และสร้างพื้นที่ปลอดภัยในการทดสอบระบบ PoH ก่อนนำไปใช้ในวงกว้าง

กลไกตัวกลางดังกล่าวยังช่วยให้การนำ PoH มาปรับใช้เป็นไปอย่างเหมาะสมตามบริบทในความเป็นจริง ทั้งในด้านเทคนิคและการคุ้มครองความเป็นส่วนตัวของผู้ใช้โดยที่ยังสอดคล้องกับทั้งกรอบของระบบยืนยันตัวตนทางดิจิทัลของประเทศ และบริบทการใช้บนแพลตฟอร์ม เช่น การแปลงมาตรฐานหรือข้อกำหนดทางกฎหมายให้เป็นขั้นตอนการทำงานที่ชัดเจน การจัดพื้นที่เพื่อแลกเปลี่ยนความเห็นเกี่ยวกับประเด็นด้านความเป็นส่วนตัว และการจัดตั้งพื้นที่ทดลอง (sandbox) เพื่อทดสอบระบบ PoH อย่างปลอดภัย เพื่อลดความเสี่ยงต่อผู้ใช้งานและแพลตฟอร์ม

นอกจากกลไกที่กล่าวมาข้างต้น อีกหนึ่งปัจจัยที่ควรให้ความสำคัญคือการเสริมสร้างความเชื่อมั่นของสาธารณะต่อระบบ (public trust) ทั้งนี้ เนื่องจาก PoH เป็นแนวทางใหม่ที่แตกต่างจากระบบยืนยันตัวตนทางดิจิทัลหรือมาตรการการรู้จักลูกค้าทางอิเล็กทรอนิกส์ (electronic Know Your Customer: eKYC) ที่ผู้ใช้งานส่วนใหญ่คุ้นเคย ดังนั้น หากขาดความเข้าใจที่ถูกต้อง อาจนำไปสู่ความกังวลเรื่องการสอดส่องประชาชน หรือการใช้ข้อมูลส่วนบุคคลเกินความจำเป็น ดังนั้น การสื่อสารและการเสริมสร้างความรู้ของผู้ใช้งานจึงมีความสำคัญพอ ๆ กับการพัฒนาเทคโนโลยี โดยหน่วยงานหรือกลไกตัวกลาง ภาคธุรกิจ และภาคประชาสังคมสามารถช่วยสร้างความเข้าใจในเรื่องนี้ว่า PoH มีเป้าหมายเพื่อยืนยันเพียงว่าผู้ใช้งาน “เป็นมนุษย์จริงหรือไม่” โดยไม่ต้องเปิดเผยว่าผู้ใช้งาน “เป็นใคร” รวมถึงการแลกเปลี่ยนแนวปฏิบัติในการนำไปใช้อย่างเหมาะสมและรับผิดชอบเพื่อเพิ่มความมั่นใจของผู้ใช้งานต่อระบบใหม่

ท้ายที่สุด การนำ PoH มาใช้ควรอยู่ภายใต้กรอบการดูแลที่มุ่งส่งเสริมทั้งความเชื่อมั่นและความปลอดภัย (trust and safety) เนื่องจากการยืนยันว่าผู้ใช้งานเป็นมนุษย์จริงเพียงอย่างเดียวไม่สามารถแก้ไขปัญหาการหลอกลวงทางออนไลน์ได้ทั้งหมด ผู้ใช้งานที่เป็นมนุษย์จริงอาจไม่ได้มีเจตนาที่สุจริตเสมอไป ซึ่งเห็นได้จากการที่กลโกงจำนวนมากในภูมิภาคเอเชียแปซิฟิก อาทิ การหลอกลงทุน หรือการหลอกลวงโดยการแอบอ้าง (impersonation scam) ล้วนดำเนินการโดยมนุษย์จริงทั้งสิ้น

ด้วยเหตุนี้ PoH จึงควรถูกนำมาใช้เป็นกลไกเสริม ไม่ใช่กลไกทดแทนมาตรการด้านความปลอดภัยอื่น ๆ การอ้างอิงกรอบตามมาตรฐาน ISO/IEC 25389 (Safe Framework) สามารถช่วยกำหนดบทบาทและขอบเขตของ PoH ให้เหมาะสม และลดความเสี่ยงจากการนำไปใช้เกินวัตถุประสงค์ โดยเฉพาะในประเด็นสำคัญต่อไปนี้

- การใช้ PoH เป็นกลไกป้องกันอีกหนึ่งชั้น เพื่อลดความเสี่ยงจากการโจมตีด้วยระบบอัตโนมัติและการดำเนินการในวงกว้าง (automation and scale attacks)
- การใช้ PoH ควบคู่กับสัญญาณด้านพฤติกรรมและชื่อเสียง (behavioral and reputational signals) เพื่อช่วยตรวจจับภัยคุกคามที่เกิดจากมนุษย์จริง
- การมีแนวทางการนำไปใช้ที่ชัดเจน เพื่อลดความเสี่ยงจากการพึ่งพา PoH มากเกินไป

ดังนั้น PoH ควรถูกนำมาทดลองใช้ในฐานะนวัตกรรมเสริม ไม่ใช่กลไกที่สามารถทดแทนมาตรการด้านความปลอดภัย เพื่อช่วยเสริมความเข้มแข็งให้กับกรอบการยืนยันตัวตนที่มีอยู่ โดยหาก PoH ได้รับการออกแบบและกำกับดูแลอย่างรอบคอบ ระบบดังกล่าวอาจช่วยเปิดพื้นที่ให้เกิดการทดลองแนวทางใหม่ในการยืนยันผู้ใช้งานจริงในสภาพแวดล้อมดิจิทัลที่มีความเสี่ยงสูง และสร้างหลักฐานเชิงประจักษ์เพื่อระบุว่าจะมีกลไกแบบใดสามารถขยายผลได้ในระดับที่กว้างขึ้นในอนาคต ในภาพรวม กรอบ PoH ที่สามารถทำงานได้แบบข้ามระบบ (interoperable) เคารพสิทธิ และคำนึงถึงความเป็นส่วนตัวของผู้ใช้งาน จะสามารถทำหน้าที่เสริมระบบยืนยันตัวตนทางดิจิทัลระดับชาติ สนับสนุนการยอมรับร่วมกันระหว่างประเทศ (cross-border recognition) และสร้างฐานความเชื่อมั่นสำหรับความร่วมมือระดับภูมิภาคในการรับมือกับการหลอกลวงและการทุจริตในโลกดิจิทัลในภูมิภาคเอเชียแปซิฟิก ซึ่งจะช่วยให้ประเทศต่าง ๆ สามารถพัฒนาเครือข่ายผู้ใช้งาน (human networks) ที่เป็นมนุษย์จริง มีความยืดหยุ่น และรับมือกับอาชญากรรมออนไลน์ได้อย่างมีประสิทธิภาพ

ส่วนถัดไปของรายงานจะพิจารณาประสบการณ์ของประเทศต่าง ๆ ในภูมิภาคเอเชียแปซิฟิก เพื่อวิเคราะห์ว่าระบบ PoH จะสามารถถูกนำไปประยุกต์ใช้ในทางปฏิบัติได้อย่างไร

กรณีศึกษา : แนวทางการนำเทคโนโลยีขั้นสูงไปใช้ในทางปฏิบัติ

ในช่วงหลายปีที่ผ่านมา ประเทศต่าง ๆ ในเอเชียได้ลงทุนพัฒนาระบบยืนยันตัวตนทางดิจิทัลอย่างต่อเนื่อง เพื่อใช้ยืนยันตัวประชาชนในการให้บริการภาครัฐและบริการทางการเงิน อย่างไรก็ตาม การหลอกลวงทางออนไลน์จำนวนมากกลับเกิดขึ้นนอกระบบที่อยู่ภายใต้การกำกับดูแลเหล่านี้ โดยเฉพาะบนแพลตฟอร์มโซเชียลมีเดีย ระบบส่งข้อความ และแพลตฟอร์มเนื้อหา (content platforms) ซึ่งยังเปิดให้สามารถใช้งานอย่างนิรนามได้ ในบริบทดังกล่าว เทคโนโลยี Proof of Human (PoH) ที่กำลังพัฒนาอยู่ในปัจจุบันจึงเป็นแนวทางใหม่ที่ช่วยต่อยอดความน่าเชื่อถือของระบบยืนยันตัวตนทางดิจิทัลไปสู่พื้นที่ดิจิทัลอื่นๆ โดยมุ่งยืนยันว่าผู้ใช้งานเป็นมนุษย์จริงและมีความเป็นเอกลักษณ์ (uniqueness) โดยไม่จำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้งาน

กรณีศึกษาต่อไปนี้จะพิจารณาประสบการณ์ของ 4 ประเทศ ได้แก่ ญี่ปุ่น เกาหลีใต้ มาเลเซีย และฟิลิปปินส์ เพื่อสะท้อนให้เห็นว่าประเทศเหล่านี้นำองค์ประกอบของการยืนยันตัวตนในลักษณะ PoH มาประยุกต์ใช้ในระบบยืนยันตัวตนระดับชาติอย่างไร รวมทั้งถอดบทเรียนจากประสบการณ์ดังกล่าวเพื่อนำไปใช้ประกอบการออกแบบแนวทางรับมือกับการหลอกลวงทางออนไลน์ในอนาคต

ญี่ปุ่น: ระบบ My Number และความท้าทายด้านความเชื่อมั่นของประชาชนต่อระบบ

ระบบ My Number ของญี่ปุ่นเริ่มใช้ในปี 2559 (ค.ศ. 2016) โดยกำหนดหมายเลขประจำตัว 12 หลักให้แก่ประชาชนทุกคน เพื่อใช้ในธุรกรรมด้านภาษี ประกันสังคม และการบริหารจัดการภัยพิบัติ เดิมระบบนี้ถูกออกแบบขึ้นเพื่อเชื่อมโยงข้อมูลภาครัฐ และเพิ่มประสิทธิภาพในการบริหารงาน และต่อมาได้ขยายสู่การใช้งานในรูปแบบดิจิทัลผ่านบัตร My Number Card ซึ่งเป็นสมาร์ทการ์ด (smart card) ที่สามารถใช้ยืนยันตัวตนทางออนไลน์ของประชาชนในการเข้าถึงบริการภาครัฐ บริการด้านสาธารณสุข และธุรกรรมทางการเงิน[18] และภายในปี 2568 (ค.ศ. 2025) มีการออกบัตรดังกล่าวแล้วมากกว่า 90 ล้านใบ หรือครอบคลุมประชากรกว่า 70% ของประเทศ อย่างไรก็ดี การใช้งานในรูปแบบดิจิทัลยังคงมีข้อจำกัด เนื่องจากการเชื่อมโยงบริการที่ยังไม่ทั่วถึง และความกังวลด้านความเชื่อมั่นของประชาชนต่อระบบที่ยังคงมีอยู่[19]

แม้ระบบ My Number จะสามารถยืนยันตัวตนของประชาชนได้ในระดับประเทศ แต่ระบบดังกล่าวยังคงเป็นระบบยืนยันตัวตนแบบดั้งเดิม ไม่ใช่กรอบการทำงานในลักษณะ PoH การยืนยันภายใต้กรอบปัจจุบันอาศัยการขึ้นทะเบียนกับภาครัฐและการตรวจสอบเอกสาร โดยยังไม่ได้ออกแบบมาเพื่อคุ้มครองความเป็นส่วนตัวของเข้าของข้อมูลในระดับเดียวกับเทคโนโลยี PoH ที่ใช้กลไกเชิงเข้ารหัสหรือการพิสูจน์แบบไม่เปิดเผยข้อมูล อย่างไรก็ตาม ประสบการณ์ของญี่ปุ่นสะท้อนให้เห็นว่า การยืนยันตัวตนที่ได้รับการรับรองโดยรัฐสามารถเป็นฐานสำคัญในการต่อยอดความเชื่อมั่นทางดิจิทัลและการป้องกันการทุจริตได้ หากมีการผสานเข้ากับกลไกที่คำนึงถึงความเป็นส่วนตัวมากขึ้น

ขณะเดียวกัน ประสบการณ์ของญี่ปุ่นยังชี้ให้เห็นถึงข้อจำกัดของระบบยืนยันตัวตนแบบรวมศูนย์ในการรับมือกับการหลอกลวงทางออนไลน์ เนื่องจากกรณีการฉ้อโกงและการหลอกลวงโดยการแอบอ้างที่พบมักเกิดขึ้นบนแพลตฟอร์มที่อยู่ภายนอกการกำกับดูแลของรัฐโดยตรง เช่น โซเชียลมีเดีย ระบบส่งข้อความ และอีคอมเมิร์ซ เป็นต้น โดยแม้ว่าแพลตฟอร์มเหล่านี้จะอยู่ภายใต้กฎหมายคุ้มครองผู้บริโภคหรือกฎหมายด้านการกำกับดูแลเนื้อหา (content regulation) ทั่วไป แต่ก็ยังไม่ได้เชื่อมโยงกับกลไกการยืนยันตัวตนของรัฐโดยตรง นอกจากนี้ เหตุการณ์ด้านการจัดการข้อมูลที่มีปัญหา อาทิ กรณีการเชื่อมโยงข้อมูลประกันสุขภาพผิดพลาดในปี 2566 (ค.ศ. 2023) ยังส่งผลกระทบต่อความเชื่อมั่นของประชาชนและจุดประกายการถกเถียงเกี่ยวกับความเป็นส่วนตัวของเจ้าของข้อมูล ความรับผิดชอบในการบริหารจัดการข้อมูล และการกำกับดูแลที่เหมาะสม เหตุการณ์เหล่านี้สะท้อนให้เห็นว่าการขาดความเชื่อมั่นอาจเป็นข้อจำกัดที่มีผลกระทบมากกว่าเทคโนโลยีในการขยายการใช้ระบบยืนยันตัวตน หากพิจารณาบริบทของญี่ปุ่นซึ่งมีวัฒนธรรมด้านการคุ้มครองความเป็นส่วนตัวสูงและการบริหารจัดการข้อมูลส่วนบุคคลอย่างเหมาะสมแล้ว จะเห็นได้ว่าการยอมรับจากสังคมจึงเป็นปัจจัยสำคัญที่กำหนดความเป็นไปได้ในการนำกลไกใหม่อย่าง PoH มาปรับใช้ในทางปฏิบัติ

เพื่อตอบโจทย์ความกังวลด้านความเชื่อมั่นของประชาชน รัฐบาลญี่ปุ่นจึงเริ่มปรับปรุงกลไกกำกับดูแลและการเชื่อมโยงการทำงานของระบบต่าง ๆ โดยมุ่งขยายการใช้งานการยืนยันตัวตนผ่าน My Number Card และระบบรหัสแบบกุญแจสาธารณะของญี่ปุ่น (Japanese Public Key Infrastructure: JPKI) ไปสู่ภาคเอกชนมากขึ้น เช่น ภาคธนาคาร การลงทะเบียนซิมการ์ด และการค้าออนไลน์[20] หากการขยายการใช้งานดังกล่าวดำเนินไปอย่างโปร่งใสและคำนึงถึงความเป็นส่วนตัวของผู้ใช้งาน ญี่ปุ่นอาจพัฒนาระบบไปสู่รูปแบบผสม ซึ่งใช้การยืนยันตัวตนทางกฎหมายของรัฐเป็นฐาน ขณะเดียวกันก็เปิดให้มีการยืนยันความเป็นมนุษย์ของผู้ใช้งานในลักษณะ PoH ผ่านเทคโนโลยีการเข้ารหัสที่ไม่เปิดเผยข้อมูลส่วนบุคคล ซึ่งแนวทางนี้จะช่วยให้ญี่ปุ่นสามารถเชื่อมโยงการยืนยันตัวตนที่มีความน่าเชื่อถือเข้ากับกลไกที่ขยายการใช้งานได้ในวงกว้าง โดยไม่กระทบสิทธิด้านความเป็นส่วนตัว และช่วยเสริมทั้งการรับมือกับการหลอกลวงทางออนไลน์และความเชื่อมั่นของประชาชนต่อเศรษฐกิจดิจิทัลในภาพรวม[21]

เกาหลีใต้: การบูรณาการระบบยืนยันตัวตนดิจิทัลกับนโยบายการใช้ชื่อจริง

เกาหลีใต้มีระบบยืนยันตัวตนทางดิจิทัลที่มีความก้าวหน้าและเชื่อมโยงกันที่สุดเป็นอันดับต้นๆ ของโลก โดยมีโครงสร้างพื้นฐานบัตรประชาชนดิจิทัล (e-ID) ระดับชาติเป็นเสาหลักของระบบซึ่งเชื่อมโยงบริการสำคัญทั้งภาคการเงิน โทรคมนาคม และบริการภาครัฐ[22] ระบบดังกล่าวพัฒนาต่อยอดมาจากระบบหมายเลขประจำตัวประชาชน (Resident Registration Number: RRN) ที่ใช้มาตั้งแต่ปี 2511 (ค.ศ. 1968) และต่อมามีการต่อยอดระบบด้วยกลไกการยืนยันชื่อจริง (real-name verification) การยืนยันด้วยข้อมูลชีวมิติ และระบบรหัสแบบกุญแจสาธารณะ (public-key infrastructure) เพื่อรองรับการเติบโตอย่างรวดเร็วของเศรษฐกิจออนไลน์[23] การออกบัตร Digital ID ในปี 2563 (ค.ศ. 2020) และใบอนุญาตขับขี่ดิจิทัลในปี 2565 (ค.ศ. 2022) ถือเป็นจุดเปลี่ยนสำคัญของการเปลี่ยนผ่านจากเอกสารกระดาษสู่การยืนยันตัวตนในรูปแบบดิจิทัลอย่างเต็มรูปแบบ[24] และภายในปี 2568 (ค.ศ. 2025) ชาวเกาหลีใต้มากกว่า 50 ล้านคนใช้ระบบยืนยันตัวตนดิจิทัลในชีวิตประจำวัน ผ่านแพลตฟอร์มอย่าง PASS, Kakao, Naver และ Samsung Pass เพื่อเข้าถึงบริการทางการเงิน บริการภาครัฐ และบริการของภาคเอกชน[25]

การที่เกาหลีใต้สามารถเชื่อมโยงระบบยืนยันตัวตนของผู้ใช้งานเข้ากับแพลตฟอร์มต่าง ๆ อย่าง ทำให้การใช้ชื่อจริงและการตรวจสอบตัวตนกลายเป็นส่วนหนึ่งของการใช้งานออนไลน์ทั่วไป ผู้ใช้งานต้องยืนยันตัวตนก่อนทำธุรกรรมออนไลน์ส่วนใหญ่ ส่งผลให้กิจกรรมในโลกดิจิทัลสามารถเชื่อมโยงกลับไปยังบุคคลจริงได้อย่างชัดเจนซึ่งสอดคล้องกับแนวทางของ PoH โดยแนวทางนี้ช่วยลดปัญหาบัญชีปลอม การหลอกลวง และการใช้ระบบอัตโนมัติในทางที่ผิด (automated abuse) ได้อย่างมีประสิทธิภาพ อีกทั้งการทำงานร่วมกันระหว่างระบบต่างๆ ของหน่วยงานรัฐและภาคเอกชนยังช่วยสร้างความเชื่อมั่นในระบบโดยรวม ทำให้เกาหลีใต้มีปัญหาการทุจริตด้านตัวตนทางการเงิน (financial-identity fraud) ค่อนข้างต่ำเมื่อเทียบกับหลายประเทศ[26]

อย่างไรก็ตาม ระบบที่พึ่งพาการยืนยันตัวตนแบบรวมศูนย์เช่นนี้ก็มีข้อจำกัด เนื่องจากการบังคับใช้ระบบการยืนยันชื่อจริงและการแลกเปลี่ยนข้อมูลระหว่างภาครัฐ ผู้ให้บริการโทรคมนาคม และสถาบันการเงิน ทำให้เกิดความกังวลเกี่ยวกับความเป็นส่วนตัวและสิทธิของประชาชน เหตุการณ์ข้อมูลรั่วไหลจากองค์กรขนาดใหญ่ อาทิ หน่วยงานด้านข้อมูลเครดิต (credit bureau) หรือแพลตฟอร์มอีคอมเมิร์ซ ยิ่งทำให้สังคมตั้งคำถามถึงความเหมาะสมในการใช้ข้อมูลตามหลักการข้อมูลเท่าที่จำเป็น (data minimization)[27] เพื่อรับมือกับความท้าทายเหล่านี้ เกาหลีใต้ได้ปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection Act : PIPA) และเริ่มทดลองใช้ระบบยืนยันตัวตนดิจิทัล (Digital Identity Pilot) รูปแบบใหม่ในปี 2566 (ค.ศ. 2023) ซึ่งจะเปิดโอกาสให้ผู้ใช้งานสามารถควบคุมข้อมูลส่วนบุคคลของตนเองได้มากขึ้น[28]

ประสบการณ์ของเกาหลีใต้สะท้อนให้เห็นชัดว่า ระบบยืนยันความเป็นมนุษย์ที่รัฐเป็นแกนกลางมีทั้งจุดแข็งและข้อจำกัด ในด้านหนึ่ง การใช้การยืนยันตัวตนทางกฎหมายควบคู่กับข้อมูลชีวมิติและระบบที่เชื่อมโยงกันได้ทั่วทั้งภาครัฐและเอกชน ช่วยลดการหลอกลวงและสร้างความน่าเชื่อถือในการใช้งานดิจิทัลได้จริง แต่อีกด้านหนึ่ง การถกเถียงในสังคมก็ชี้ให้เห็นความคาดหวังที่เพิ่มขึ้นต่อระบบที่คุ้มครองความเป็นส่วนตัวมากกว่าเดิม และเปิดให้ผู้ใช้งานมีอำนาจควบคุมข้อมูลของตนเองมากขึ้น ซึ่งเป็นทิศทางเดียวกับแนวคิด PoH ที่กำลังถูกพัฒนาอยู่ในปัจจุบัน ในระยะต่อไป การพัฒนาระบบความเชื่อมั่นทางดิจิทัลของเกาหลีใต้อาจลดการพึ่งพาการบังคับใช้ระบบการยืนยันตัวตนตามชื่อจริง และหันไปสู่โมเดลที่สร้างสมดุลระหว่างการยืนยันผู้ใช้งานจริงกับการคุ้มครองสิทธิและความเชื่อมั่นของประชาชนในเศรษฐกิจดิจิทัลมากขึ้น

มาเลเซีย: MyDigital ID และเส้นทางสู่ความเชื่อมั่นผ่านข้อมูลชีวมิติ

โครงการ MyDigital ID ของมาเลเซียถือเป็นก้าวสำคัญในการพัฒนาระบบยืนยันตัวตนทางดิจิทัลของภาครัฐ โดยมีเป้าหมายเพื่อให้ประชาชนเข้าถึงทั้งบริการภาครัฐและบริการของภาคเอกชนได้โดยสะดวกและเป็นระบบมากขึ้น ระบบดังกล่าวเริ่มใช้งานอย่างเป็นทางการในปี 2567 (ค.ศ. 2024) ภายใต้กรอบ Digital Identity Blueprint และกำหนดให้ประชาชนแต่ละคนมีข้อมูลยืนยันตัวตนดิจิทัลที่เชื่อมโยงกับฐานข้อมูลของกรมทะเบียนราษฎร (National Registration Department: NRD)[29] ผ่านการยืนยันด้วยข้อมูลชีวมิติโดยการจดจำใบหน้า (facial recognition) ซึ่งระบบนี้ช่วยให้ประชาชนสามารถยืนยันตัวตนเพื่อใช้บริการออนไลน์ต่าง ๆ ได้ ไม่ว่าจะเป็นบริการภาครัฐ ธนาคาร ผู้ให้บริการโทรคมนาคม ไปจนถึงแพลตฟอร์มดิจิทัลอื่น ๆ โดยการทดลองใช้งานเบื้องต้นร่วมกับกรมสรรพากร (Inland Revenue Board : LHDN) และสถาบันการเงินบางแห่งได้ปูทางไปสู่การขยายใช้งานในระดับประเทศซึ่งคาดว่าจะเกิดขึ้นในปี 2568 (ค.ศ. 2025)[30]

MyDigital ID มีความแตกต่างจากระบบการยืนยันตัวตนอื่นๆ เนื่องจากระบบดังกล่าวถูกออกแบบให้ทำหน้าที่ทั้งเป็นข้อมูลประจำตัว (credential) และเป็นกลไกการยืนยันตัวตน (authentication) ในระบบเดียวกัน ผู้ใช้งานจึงสามารถยืนยันตัวตนได้โดยไม่จำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลซ้ำซ้อนทุกครั้ง การเชื่อมโยงตัวตนดิจิทัลเข้ากับข้อมูลชีวมิติที่ผ่านการรับรองมาแล้วยังช่วยให้มั่นใจได้ว่าบัญชีดิจิทัลมีบุคคลที่เป็นมนุษย์จริงๆ เป็นผู้ใช้งาน ซึ่งสอดคล้องกับแนวคิดของการยืนยันตัวตนตามแนวทาง PoH อย่างไรก็ดี เมื่อมาเลเซียขยายการใช้งานระบบยืนยันตัวตนไปยังหลายภาคส่วน ก็ต้องเผชิญความท้าทายเช่นเดียวกับประเทศอื่น ๆ คือการขยายความเชื่อมั่นไปสู่พื้นที่ดิจิทัลแบบเปิดที่อยู่นอกเหนือจากธุรกรรมที่เกี่ยวข้องกับภาครัฐ ซึ่งเป็นพื้นที่ที่ผู้ใช้งานจำนวนมากไม่ต้องการหรือไม่สามารถเปิดเผยข้อมูลส่วนยุคคลของตัวเองได้ ในบริบทนี้ MyDigital ID จึงอาจทำหน้าที่เป็นโครงสร้างพื้นฐานสำคัญสำหรับการพัฒนากลไก PoH ในอนาคตที่สามารถยืนยันความเป็นมนุษย์ของผู้ใช้งานได้โดยยังคงคำนึงถึงความเป็นส่วนตัวและการทำงานร่วมกันของระบบต่าง ๆ

โครงการ MyDigital ID ยังถูกพัฒนาขึ้นเพื่อตอบโจทย์ปัญหาการหลอกลวงและอาชญากรรมดิจิทัลที่เพิ่มขึ้นในมาเลเซีย ซึ่งเกิดควบคู่กับการขยายตัวของโมบายแบงก์กิ้ง (mobile banking) และอีคอมเมิร์ซ การมีระบบยืนยันตัวตนที่น่าเชื่อถือสามารถช่วยลดปัญหาการแอบอ้างและการสร้างบัญชีปลอมในระบบที่อยู่ภายใต้การกำกับดูแล ในขณะที่แนวคิดการยืนยันตัวตนตามกรอบ PoH ก็สามารถขยายการคุ้มครองไปสู่พื้นที่ดิจิทัลที่ยังไม่ถูกกำกับโดยตรง เช่น ตลาดออนไลน์ โซเชียลมีเดีย และระบบการชำระเงินดิจิทัลซึ่งมักมีความเสี่ยงด้านการหลอกลวง

ทั้งนี้ การเริ่มใช้งานระบบ MyDigital ID ก็ทำให้เกิดการถกเถียงในสังคมเกี่ยวกับความเป็นส่วนตัว การคุ้มครองข้อมูล และการกำกับดูแลเช่นกัน โดยภาคประชาสังคมได้แสดงความกังวลต่อการจัดเก็บข้อมูลชีวมิติแบบรวมศูนย์และความเสี่ยงจากการนำข้อมูลไปใช้เกินวัตถุประสงค์[31] เพื่อตอบสนองต่อข้อกังวลดังกล่าว รัฐบาลมาเลเซียได้จัดตั้งคณะกรรมการกำกับดูแลในเรื่องนี้โดยเฉพาะ (Digital ID Steering Committee) และยืนยันการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act: PDPA) รวมทั้งให้ความสำคัญกับการเชื่อมโยงการทำงานกับระบบ MySejahtera และ eKYC ภายใต้การกำกับของธนาคารกลางมาเลเซีย (Bank Negara Malaysia)[32] เพื่อให้การดำเนินโครงการเป็นไปอย่างโปร่งใส ตรวจสอบได้ และได้รับความเชื่อมั่นจากสาธารณชน

หาก MyDigital ID ถูกนำไปปรับใช้อย่างเหมาะสมโดยมีมาตรการคุ้มครองข้อมูลที่ชัดเจนและเปิดให้ผู้ใช้งานมีอำนาจควบคุมข้อมูลของตนเอง ระบบนี้อาจพัฒนาไปสู่การเป็นฐานสำคัญสำหรับนวัตกรรมด้าน PoH ในอนาคต เนื่องจากโครงสร้างของระบบปัจจุบันที่ผสานการยืนยันด้วยข้อมูลชีวมิติ การให้ความยินยอมของผู้ใช้งาน และการเชื่อมต่อระหว่างระบบต่างๆ สะท้อนให้เห็นว่าประเทศกำลังพัฒนาสามารถสร้างกรอบความเชื่อมั่นทางดิจิทัลที่ยืนยันตัวตนของผู้ใช้งานได้ โดยไม่ละเลยประเด็นความเป็นส่วนตัวและข้อจำกัดในการเข้าถึงเทคโนโลยี ประสบการณ์ของมาเลเซียเป็นตัวอย่างที่สำคัญสำหรับภูมิภาคเอเชียตะวันออกเฉียงใต้ในการชี้ให้เห็นว่าการกำกับดูแลที่เข้มแข็งของภาครัฐนั้นมีบทบาทสำคัญในการเชื่อมโยงระบบยืนยันตัวตนแบบดั้งเดิมเข้ากับแนวคิด PoH ในอนาคต และเสริมสร้างความสามารถในการรับมือกับการหลอกลวงทางออนไลน์โดยไม่บั่นทอนความเชื่อมั่นของประชาชน

ฟิลิปปินส์: การขยายขอบเขตการใช้งาน ระบบ PhilSys ในวงกว้าง

ระบบการระบุตัวตนแห่งชาติของฟิลิปปินส์ (Philippine Identification System: PhilSys) ถือเป็นหนึ่งในโครงการระบบยืนยันตัวตนทางดิจิทัลที่ขยายตัวเร็วที่สุดในเอเชียตะวันออกเฉียงใต้ โครงการนี้จัดตั้งขึ้นตามกฎหมาย Republic Act No. 11055 ในปี 2561 (ค.ศ. 2018) โดยกำหนดหมายเลขประจำตัว PhilSys จำนวน 12 หลักให้แก่พลเมืองและผู้อยู่อาศัยทุกคน พร้อมผูกกับข้อมูลชีวมิติ เช่น ภาพใบหน้า ลายนิ้วมือ และม่านตา เป็นต้น[33] ภายใต้การดูแลของสำนักงานสถิติแห่งชาติฟิลิปปินส์ (Philippine Statistics Authority: PSA) เป้าหมายหลักของ PhilSys คือการเพิ่มการเข้าถึงบริการภาครัฐ ส่งเสริมการเข้าถึงบริการทางการเงิน และยกระดับความปลอดภัยของธุรกรรมดิจิทัล ภายในปลายปี 2568 (ค.ศ. 2025) มีประชาชนลงทะเบียนแล้วมากกว่า 80 ล้านคน และบัตรประจำตัวในรูปแบบดิจิทัล ซึ่งใช้งานผ่านแอป eGovPH และเว็บไซต์ national-id.gov.ph ได้รับการยอมรับในวงกว้างจากหน่วยงานรัฐ สถาบันการเงิน และแพลตฟอร์มเอกชน[34]

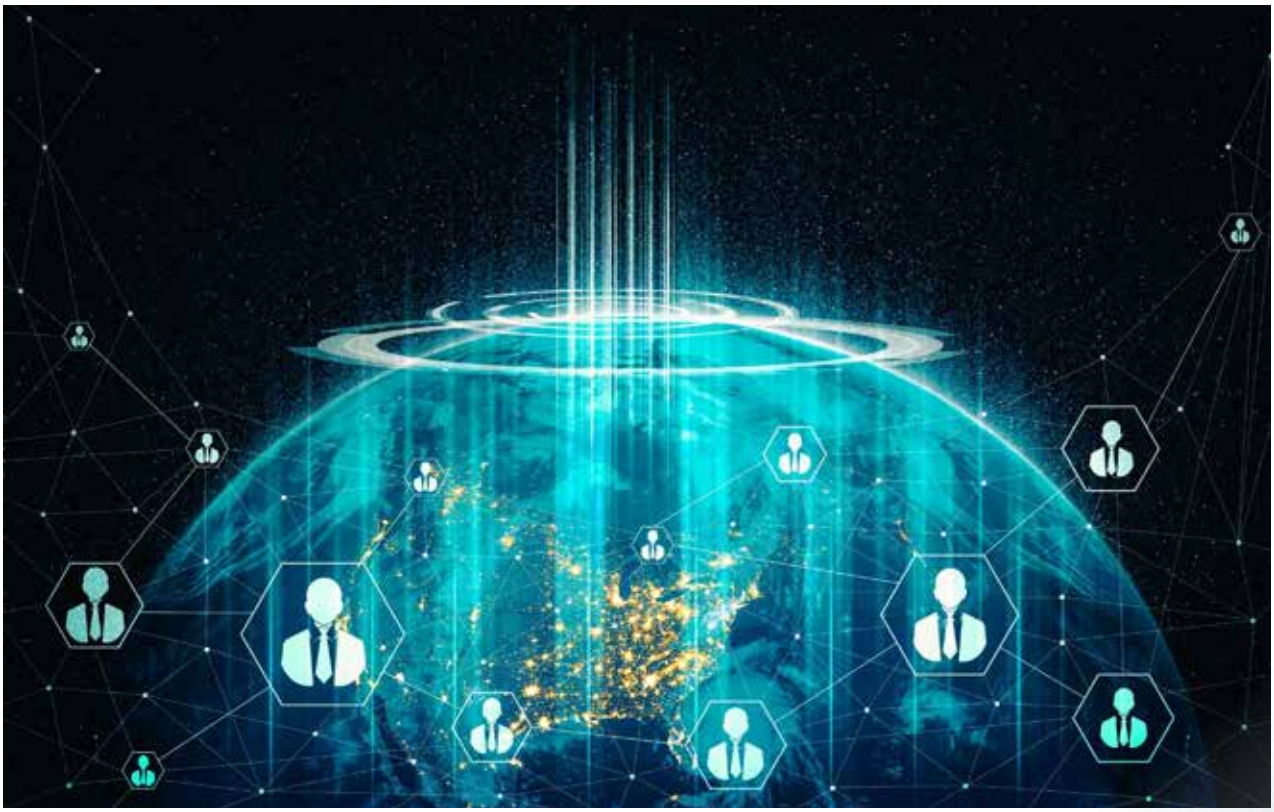
การขยายตัวของระบบ PhilSys อย่างรวดเร็วถือเป็นก้าวสำคัญของประเทศในภูมิภาคนี้ในการสร้างระบบยืนยันตัวตนที่น่าเชื่อถือในระดับประเทศ การผูกหมายเลขประจำตัวประชาชนเข้ากับข้อมูลชีวมิติที่ผ่านการตรวจสอบช่วยลดปัญหาการลงทะเบียนซ้ำ และการสร้างบัญชีปลอมได้อย่างเป็นรูปธรรม ในทางปฏิบัติ ระบบดังกล่าวทำหน้าที่คล้ายกับกลไก PoH ในการยืนยันว่าผู้ใช้งานแต่ละรายเป็นมนุษย์จริง และสามารถนำข้อมูลดังกล่าวไปใช้ต่อกับบริการสำคัญต่าง ๆ ได้ ตั้งแต่บริการภาครัฐ ธนาคาร โทรคมนาคม ไปจนถึงการรับสวัสดิการและการชำระเงินดิจิทัลผ่านระบบ eVerify ที่ตรวจสอบข้อมูลได้แบบเรียลไทม์[35]

อย่างไรก็ดี ความเร็วในการดำเนินการก็ทำให้เกิดความท้าทายหลายประการตามมา ทั้งปัญหาทางเทคนิค ความล่าช้าในการออกบัตร และข้อกังวลเกี่ยวกับการจัดเก็บและการใช้ข้อมูลชีวมิติ โดยเฉพาะการจัดเก็บข้อมูลแบบรวมศูนย์และความไม่ชัดเจนด้านแนวทางการแลกเปลี่ยนข้อมูล ประเด็นเหล่านี้ทำให้สังคมตั้งคำถามเกี่ยวกับความเป็นส่วนตัวและการคุ้มครองข้อมูลมากขึ้น[36] หน่วยงานที่เกี่ยวข้อง อาทิ สำนักงานสถิติแห่งชาติฟิลิปปินส์ (PSA) และคณะกรรมการคุ้มครองความเป็นส่วนตัว (NPC) จึงตอบสนองโดยการเพิ่มความเข้มงวดในการกำกับดูแล ปรับมาตรการด้านความปลอดภัยของข้อมูล และกำหนดให้การเข้าถึงข้อมูลต้องอยู่บนพื้นฐานของความยินยอมของผู้ใช้งาน ผ่านกรอบการทำงานของระบบ eGovPH[37]

ประสบการณ์ของฟิลิปปินส์สะท้อนให้เห็นทั้งโอกาสและความเสี่ยงของการขยายระบบอย่างรวดเร็ว ระบบ PhilSys แสดงให้เห็นว่าประเทศกำลังพัฒนาสามารถสร้างโครงสร้างพื้นฐานด้านการยืนยันตัวตนที่ช่วยเพิ่มการเข้าถึงบริการและลดการหลอกลวงได้ในระยะเวลาอันสั้น อย่างไรก็ตาม บทเรียนสำคัญคือความเชื่อมั่นของประชาชนต้องเติบโตไปพร้อมกับเทคโนโลยี และความโปร่งใสในการกำกับดูแลรวมทั้งการเปิดโอกาสให้ผู้ใช้งานควบคุมข้อมูลของตนเอง เป็นสิ่งสำคัญ หาก PhilSys มีการพัฒนาอย่างต่อเนื่อง ระบบนี้สามารถเป็นพื้นที่ในการทำลองใช้แนวทาง PoH ในอนาคต และช่วยชี้ให้เห็นว่าการยืนยันผู้ใช้งานจริงสามารถช่วยเสริมความสามารถในการรับมือกับการหลอกลวง และสร้างความเชื่อมั่นในเศรษฐกิจดิจิทัลของเอเชียตะวันออกเฉียงใต้ได้อย่างยั่งยืน

ถอดบทเรียนจากกรณีศึกษา

กรณีศึกษาทั้งสี่ประเทศสะท้อนให้เห็นเส้นทางที่แตกต่างกันในการพัฒนาโครงสร้างพื้นฐานเพื่อยืนยันความเป็นเอกลักษณ์ของผู้ใช้งานในโลกดิจิทัลของประเทศในเอเชีย ญี่ปุ่นและเกาหลีใต้แสดงให้เห็นว่าประเทศที่มีระบบกำกับดูแลและกฎระเบียบเข้มแข็งสามารถนำระบบยืนยันตัวตนที่ตรวจสอบได้มาใช้ในวงกว้างได้ อย่างไรก็ดี ผลลัพธ์กลับแตกต่างกันอย่างชัดเจน โดยกรณีของญี่ปุ่นสะท้อนให้เห็นว่าความเชื่อมั่นของประชาชนอาจสั่นคลอนได้ง่าย หากการกำกับดูแลข้อมูลไม่รัดกุม ขณะที่เกาหลีใต้แสดงให้เห็นถึงประสิทธิภาพของการเชื่อมโยงระบบยืนยันตัวตนเข้ากับภาคการเงินและเทคโนโลยีอย่างลึกซึ้ง ควบคู่กับความเสี่ยงด้านความเป็นส่วนตัวที่ตามมา ในเอเชียตะวันออกเฉียงใต้ มาเลเซียและฟิลิปปินส์สะท้อนสองแนวทางที่กำลังเกิดขึ้น มาเลเซียเลือกพัฒนาระบบโดยให้ความสำคัญกับการออกแบบกลไกกำกับดูแลและการคุ้มครองตั้งแต่ต้น ขณะที่ฟิลิปปินส์ให้ความสำคัญกับการขยายระบบอย่างรวดเร็วเพื่อเพิ่มการเข้าถึงของประชาชน เมื่อพิจารณาทั้งสี่กรณีร่วมกัน จะเห็นปัจจัยร่วมที่สำคัญคือ กลไกการยืนยันตัวตนตามแนวทาง PoH จะมีประสิทธิผลมากที่สุดเมื่อดำเนินควบคู่ไปกับความโปร่งใส การทำงานร่วมกันของระบบต่าง ๆ และการเปิดให้ผู้ใช้งานมีอำนาจควบคุมข้อมูลของตนเอง แนวทางเช่นนี้ช่วยให้ระบบยืนยันตัวตนทางดิจิทัลสามารถเสริมสร้างความปลอดภัยในโลกออนไลน์ได้จริงโดยไม่บั่นทอนความเชื่อมั่นของประชาชน



บทสรุปและข้อเสนอแนะเชิงนโยบาย

การหลอกลวงและอาชญากรรมออนไลน์ได้กลายเป็นความเสี่ยงสำคัญที่บ่อนทำลายความเชื่อมั่นในระบบดิจิทัลของภูมิภาคเอเชียแปซิฟิก แม้ประเทศต่าง ๆ จะพัฒนาระบบยืนยันตัวตนทางดิจิทัลระดับชาติขึ้นอย่างต่อเนื่อง ตั้งแต่ My Number ของญี่ปุ่นไปจนถึง PhilSys ของฟิลิปปินส์ ระบบเหล่านี้ยังถูกใช้เป็นระบบทะเบียนและฐานข้อมูลของรัฐ มากกว่าการนำมาใช้ป้องกันปัญหาในทางปฏิบัติ ดังนั้น เทคโนโลยี PoH ที่กำลังถูกพัฒนาขึ้นจึงเข้ามาเติมเต็มช่องว่างดังกล่าว โดยเปิดให้ผู้ใช้งานสามารถพิสูจน์ได้ว่าตนเป็นมนุษย์จริงบนแพลตฟอร์มดิจิทัล ระบบการเงิน และเครือข่ายการสื่อสาร โดยไม่จำเป็นต้องเปิดเผยข้อมูลระบุตัวตนส่วนบุคคล การเพิ่มสัญญาณยืนยันความเป็นมนุษย์ (signal of humanness) ในลักษณะที่คุ้มครองความเป็นส่วนตัวนี้ ช่วยรับมือกับการหลอกลวงที่อาศัยระบบอัตโนมัติหรือการดำเนินการในวงกว้าง (automated and scaled abuse) ในลักษณะที่ระบบยืนยันตัวตนแบบดั้งเดิมไม่ได้ถูกออกแบบมาเพื่อตรวจจับโดยตรง ดังนั้น การผสานเทคโนโลยี PoH เข้ากับระบบยืนยันตัวตนทางดิจิทัลจึงมีศักยภาพในการยกระดับทั้งความสามารถในการรับมือกับการหลอกลวงทางออนไลน์และความเชื่อมั่นของประชาชน โดยยังคงรักษาหลักการคุ้มครองความเป็นส่วนตัวไว้ได้

ดังที่ได้กล่าวไว้ก่อนหน้าในส่วน *มาตรการคุ้มครองและการกำกับดูแล* ของรายงาน การนำ PoH มาใช้จำเป็นต้องอาศัยการออกแบบที่คำนึงถึงความเสี่ยงที่อาจเกิดขึ้น การคุ้มครองสิทธิของผู้ใช้งานอย่างชัดเจน และความสอดคล้องกับระบบยืนยันตัวตนที่มีอยู่ โดยรัฐบาลของประเทศต่างๆ ในภูมิภาคอาจพิจารณาดำเนินการในประเด็นสำคัญต่อไปนี้

- **บูรณาการระบบยืนยันตัวตนทางดิจิทัลและ PoH เข้ากับยุทธศาสตร์ป้องกันการหลอกลวงทางออนไลน์** โดยนำกลไกการยืนยันความเป็นเอกลักษณ์ (proof of uniqueness verification) ไปใช้ในภาคการเงิน อีคอมเมิร์ซ และแพลตฟอร์มการสื่อสาร เพื่อช่วยลดการแอบอ้างบัญชีปลอม และการทุจริตที่ขับเคลื่อนด้วยบอต ทั้งนี้ควรดำเนินการอย่างเหมาะสม ไม่สร้างภาระเกินจำเป็น และสอดคล้องกับกรอบด้านความปลอดภัย เช่น ISO/IEC 25389 เป็นต้น

- **สนับสนุนมาตรฐานที่คุ้มครองความเป็นส่วนตัวและทำงานร่วมกันข้ามระบบได้ (interoperable)** โดยส่งเสริมการพัฒนากรอบระดับภูมิภาคที่ผสานการยืนยันด้วยข้อมูลชีวมิติเข้ากับกลไกการเข้ารหัส เพื่อให้การยืนยันความเป็นเอกลักษณ์ไม่กระทบต่อการไม่เปิดเผยตัวตนของผู้ใช้ รองรับการใช้งานข้ามพรมแดน และไม่เปิดช่องให้สัญญาณ PoH ถูกนำไปใช้เพื่อติดตามหรือจัดทำโปรไฟล์ผู้ใช้งาน

- **ส่งเสริมการหารือและความร่วมมือเชิงนโยบายในระดับภูมิภาค** โดยใช้เวทีที่มีอยู่แล้ว อาทิ APEC Business Advisory Council หลักการของ G20 ด้านการเข้าถึงบริการทางการเงินดิจิทัล (G20 High-Level Principles for Digital Financial Inclusion) และกรอบความร่วมมือที่สหประชาชาติสนับสนุน เพื่อแลกเปลี่ยนแนวปฏิบัติที่ดีปรับแนวนโยบายให้สอดคล้องกัน และทดลองใช้ PoH ผ่านโครงการนำร่องหรือ sandbox ก่อนการขยายผลในวงกว้าง

แนวทางเหล่านี้จะช่วยวางรากฐานให้ระบบนิเวศดิจิทัลของเอเชียแปซิฟิกมีความน่าเชื่อถือและยึดโยงกับความเป็นมนุษย์มากขึ้น โดยมีระบบที่การยืนยันตัวตนที่มีศักยภาพในการเพิ่มความปลอดภัยของผู้ใช้งานโดยไม่ละเมิดความเป็นส่วนตัว มีกรอบกำกับดูแลที่ชัดเจน และอาศัยความร่วมมือระดับภูมิภาคในการยกระดับระบบยืนยันตัวตนจากระบบทะเบียนของรัฐ ไปสู่กลไกเชิงรุกในการรับมือกับการหลอกลวงออนไลน์และส่งเสริมการเข้าถึงบริการดิจิทัลอย่างทั่วถึง

บรรณานุกรม

[1] Cybersecurity Ventures. (ไม่ปรากฏปี). “เศรษฐกิจที่ใหญ่เป็นอันดับสามของโลกกับเจตนาร้าย—และกำลังขยายตัวมากขึ้น” (“The World’s Third Largest Economy Has Bad Intentions—And It’s Only Getting Bigger”). เข้าถึงเมื่อเดือนสิงหาคม 2025. https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/

[2] GSMA. (2025). รายงานความปลอดภัยด้านการฉ้อโกงและกลโกง (Fraud and Scams Safety Report). ลอนดอน: GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2025/02/Fraud-and-scams-safety-report.pdf

[3] สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (UNODC). (2025). จุดเปลี่ยน: ผลกระทบระดับโลกของศูนย์หลอกลวง (Inflection Point: Global Implications of Scam Centres), https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf

[4] Global Initiative (พฤษภาคม 2025). “ปฏิบัติการกลโกงไซเบอร์ในเอเชียตะวันออกเฉียงใต้” (Cyber Scam Operations in Southeast Asia). https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.p

[5] The Japan Times. (2 เมษายน 2025). “แนวโน้มใหม่ของการค้ามนุษย์จากเมียนมา” (“A New Human Trafficking Trend Emerges from Myanmar”). https://www.japantimes.co.jp/news/2025/04/02/japan/crime-legal/myanmar-scam-human-trafficking/

[6] “ถูกบังคับให้หลอกลวงผู้คนทั่วโลก ขณะนี้หลายพันคนถูกควบคุมตัวบริเวณชายแดนเมียนมา” (“They Were Forced to Scam Others Worldwide. Now Thousands Are Detained on the Myanmar Border”). https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed59c821a72bd2

[7] Signicat. (2024). “ความพยายามทุจริตด้วยดีปเฟกเพิ่มขึ้นกว่า 2,137% ในช่วงสามปีที่ผ่านมา” (“Fraud Attempts with Deepfakes Have Increased by 2137% over the Last Three Years”). เข้าถึงเมื่อเดือนสิงหาคม 2025. https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year

[8] CSIS. (12 ธันวาคม 2024). การหลอกลวงไซเบอร์ขยายสู่ระดับโลก: โรงงานฉ้อโกงไฮเทคในเอเชียตะวันออกเฉียงใต้ (Cyber Scamming Goes Global: Unveiling Southeast Asia’s High-Tech Fraud Factories). https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories

[9] TRM Labs. (2022). รายงานระบบนิเวศคริปโทเคอร์เรนซีผิดกฎหมาย (The Illicit Crypto Ecosystem Report). https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022/

[10] M Meta. (21 พฤศจิกายน 2024). การปราบปรามอาชญากรรมข้ามชาติที่อยู่เบื้องหลังศูนย์หลอกลวง (Cracking Down on Organized Crime Behind Scam Centers). https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/

[11] TRM Labs. (2025). รายงานอาชญากรรมคริปโทเคอร์เรนซี ปี 2025 (2025 Crypto Crime Report). https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report

[12] ธนาคารโลก (World Bank). (ไม่ปรากฏปี). ชุดเครื่องมือระบบยืนยันตัวตนทางดิจิทัล (Digital Identity Toolkit): ส่วนว่าด้วย credential และ smart card-based eIDs. https://documents1.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf

[13] Financial Action Task Force (FATF). (มีนาคม 2020). แนวทางว่าด้วยระบบยืนยันตัวตนทางดิจิทัล (Guidance on Digital Identity). ปารีส: FATF/OECD. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf

[14] SITA และ PRISM. (2023). อัตลักษณ์ดิจิทัลด้วยข้อมูลชีวมิติ: ก้าวถัดไปของการเดินทางและบริการภาครัฐที่ไร้รอยต่อ (Biometric Digital Identity: The Next Step in Seamless Travel and Government Services). https://www.sita.aero/globalassets/docs/other/biometric-digital-identity-govt-services-prism-report.pdf

[15] OECD. (ไม่ปรากฏปี). แพลตฟอร์ม National Digital Identity ของประเทศไทย (National Digital Identity (NDID) Platform – Thailand). https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/thailand-national-digital-identity-platform.pdf

[16] Kosmos. (ไม่ปรากฏปี). ภาพรวมระบบอัตลักษณ์ดิจิทัล: สิงคโปร์ (Digital Identity Spotlight: Singapore). https://www.1kosmos.com/identity-management/digital-identity-spotlight-singapore/

[17] BiometricUpdate. (ไม่ปรากฏปี). เปรียบเทียบระบบอัตลักษณ์ดิจิทัลในเอเชีย (Digital Identity Systems around Asia Compared as Taiwan Seeks Path Forward). https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-taiwan-seeks-path-forward

[18] Ministry of Internal Affairs and Communications (MIC). (2024). "ภาพรวมระบบหมายเลขประกันสังคมและภาษี" ("Overview of the Social Security and Tax Number System").

[19] Digital Agency of Japan. (ตุลาคม 2025). "จำนวนบัตร My Number ที่ออกแล้ว" ("Number of My Number Cards Issued"); Nikkei Asia. (12 กรกฎาคม 2025). "ญี่ปุ่นออกบัตร My Number ครบ 90 ล้านใบ แต่ปัญหาความเชื่อมั่นยังคงอยู่" ("Japan's My Number Cards Hit 90m Issuance but Trust Issues Persist").

[20] The Japan Times. (9 มีนาคม 2024). "ญี่ปุ่นมีเป้าหมายเชื่อม My Number กับธนาคารและการลงทะเบียนซิมการ์ด" ("Japan Aims to Link My Number to Banking and SIM Registration").

[21] The Japan Times. (2 มิถุนายน 2023). "แก้ไขจุดบกพร่องของระบบ My Number" ("Fix the Flaws in the My Number System").

[22] Ministry of the Interior and Safety (MOIS). (2023). "ภาพรวมระบบทะเบียนราษฎร" ("Overview of the Resident Registration System").

[23] Korea Communications Commission (KCC). (2022). "นโยบายการยืนยันชื่อจริงในสภาพแวดล้อมดิจิทัล" ("Real-Name Verification Policy in the Digital Environment").

[24] Ministry of Land, Infrastructure and Transport (MOLIT). (มกราคม 2022). "การเปิดให้บริการใบอนุญาตขับขี่ดิจิทัล" ("Launch of the Mobile Driver's License Service").

[25] Korea Internet & Security Agency (KISA). (2024). "สถานะการใช้งานระบบยืนยันตัวตนดิจิทัลในเกาหลี" ("Status of Digital Authentication Use in Korea"); Yonhap News. (9 พฤษภาคม 2025). "แอป PASS มีผู้ใช้งานเกิน 50 ล้านคนในเกาหลี" ("PASS App Surpasses 50 Million Users in Korea").

[26] OECD. (2023). "รัฐบาลดิจิทัลในเกาหลี: การขับเคลื่อนสังคมอัจฉริยะและครอบคลุม" ("Digital Government in Korea: Enabling a Smart and Inclusive Society"), หน้า 45.

[27] Korea JoongAng Daily. (4 กุมภาพันธ์ 2023). "เหตุข้อมูลรั่วไหลขนาดใหญ่ตั้งคำถามต่อแนวปฏิบัติด้านความปลอดภัย" ("Massive Data Leaks Raise Questions About Security Practices"); Korea Times. (15 เมษายน 2023). "สำนักข้อมูลเครดิตถูกปรับจากเหตุข้อมูลรั่วไหลที่กระทบประชาชนจำนวนมาก" ("Credit Bureau Fined over Data Breach Affecting Millions").

[28] Ministry of the Interior and Safety (MOIS). (2023). "โครงการทดลองระบบอัตลักษณ์ดิจิทัลเพื่อการยืนยันที่ปลอดภัย" ("Digital Identity Pilot Project for Secure Authentication"); Personal Information Protection Commission (PIPC). (ธันวาคม 2023). "การแก้ไขเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล" ("Amendments to the Personal Information Protection Act").

[29] Ministry of Communications and Digital. (2024). "แผนแม่บทอัตลักษณ์ดิจิทัล" ("Digital Identity Blueprint").

[30] Department of National Registration (Jabatan Pendaftaran Negara: JPN). (มิถุนายน 2024). "การดำเนินโครงการทดลอง MyDigital ID ร่วมกับ LHDN และสถาบันการเงิน" ("Implementation of MyDigital ID Pilot with LHDN and Financial Institutions").

[31] Malay Mail. (5 เมษายน 2024). "นักรณรงค์ด้านความเป็นส่วนตัวแสดงความกังวลต่อฐานข้อมูลชีวมิติแบบรวมศูนย์" ("Privacy Advocates Raise Concerns over Centralised Biometric Database").

[32] Ministry of Communications and Digital (KKD). (15 กุมภาพันธ์ 2024). "การจัดตั้งคณะกรรมการกำกับดูแล Digital ID" ("Formation of Digital ID Steering Committee"); Bank Negara Malaysia. (2023). "แนวทางการดำเนินการ e-KYC" ("e-KYC Implementation Guidelines").

[33] "พระราชบัญญัติว่าด้วยการจัดตั้งระบบการระบุตัวตนแห่งชาติ (PhilSys)" ("An Act Establishing the Philippine Identification System (PhilSys Act)").

[34] Philippine Statistics Authority (PSA). (ตุลาคม 2025). “แดชบอร์ด PhilSys: ข้อมูลการลงทะเบียนและการออกบัตร” (“PhilSys Dashboard: Registration and Issuance Data”); Inquirer.net. (14 กันยายน 2025). “มีชาวฟิลิปปินส์ลงทะเบียนบัตรประชาชนกว่า 80 ล้านคน” (“Over 80 Million Filipinos Registered for National ID—PSA”).

[35] Philippine Statistics Authority (PSA). (2024). “การเปิดตัวพอร์ทัล PhilSys eVerify และความสามารถในการตรวจสอบด้วย QR code” (“PhilSys eVerify Portal Launch and QR Verification Capabilities”).

[36] Rappler. (22 มิถุนายน 2024). “ความกังวลด้านความเป็นส่วนตัวเพิ่มขึ้นจากการแบ่งปันข้อมูลบัตรประชาชน” (“Privacy Concerns Mount over National ID Data Sharing”); Philippine Star. (10 พฤษภาคม 2024). “ความล่าช้าและปัญหาข้อมูลของบัตรประชาชนกระตุ้นเสียงวิจารณ์” (“National ID Delays, Data Glitches Spur Criticism”).

[37] . National Privacy Commission (NPC). (2024). “คำแนะนำด้านมาตรฐานการคุ้มครองข้อมูลสำหรับระบบบัตรประชาชน” (“NPC Advisory on Data Protection Standards for the National ID System”); Philippine Statistics Authority (PSA). (2024). “มาตรการเสริมความปลอดภัยสำหรับการออก ePhilID” (“Enhanced Security Measures for ePhilID Rollout”).

www.seapublicpolicy.org