ความเสี่ยงของการยืนยันตัวตนโดยการใช้ SMS OTP ที่ส่งผ่านโครงข่ายโทรศัพท์สาธารณะ (PSTN) และแนวทางการจัดการสำหรับผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP)

1. บทนำ: การใช้ SMS OTP ในการยืนยันตัวตน

การยืนยันตัวตน (authentication) คือการยืนยันอัตลักษณ์ของบุคคลด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้นก่อนที่จะทำธุรกรรมต่างๆ ซึ่งเป็นกระบวนการที่สำคัญ โดยเฉพาะในการทำธุรกรรมที่มีความเสี่ยงสูง เช่น บริการทางการเงิน บริการภาครัฐ หรือระบบสวัสดิการประชาชน โดยหนึ่งในวิธีการยืนยันตัวตนที่เป็นที่นิยมในประเทศไทยคือ การส่งรหัส OTP (One-Time Password) ในรูปแบบข้อความสั้น (SMS) ผ่านทางโครงข่ายโทรศัพท์สาธารณะ (Public Switched Telephone Network: PSTN) วิธีนี้เป็นที่นิยมใช้กันอย่างแพร่หลาย เนื่องจากเป็นวิธีการที่สะดวกและเข้าถึงได้โดยผู้ใช้บริการหลากหลายกลุ่ม ไม่ว่าจะเป็นกลุ่มผู้สูงอายุหรือผู้ที่อาศัยในพื้นที่ชนบทที่อาจไม่มีสมาร์ตโฟนหรืออินเทอร์เน็ตความเร็วสูง

อย่างไรก็ตาม แม้ว่าการใช้ SMS OTP จะเป็นวิธีการที่สะดวกและรวดเร็ว แต่ในปัจจุบันได้มีการเล็งเห็นถึงความเสี่ยงและข้อจำกัดด้านความมั่นคงปลอดภัยที่มีแนวโน้มจะเพิ่มมากขึ้นตามการพัฒนาของเทคโนโลยีที่เกี่ยวข้อง อ้างอิงจากเอกสารมาตรฐานสากล เช่น NIST SP 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management ซึ่งได้จัดให้การยืนยันตัวตนด้วยการส่ง SMS OTP ผ่านทาง PSTN เป็นหนึ่งในกลุ่มของ "Restricted Authenticators" หรือสิ่งที่ใช้ยืนยันตัวตนที่ควรจำกัดการใช้งาน โดยเฉพาะในธุรกรรมที่ต้องการระดับความน่าเชื่อถือ (assurance level) ที่สูง

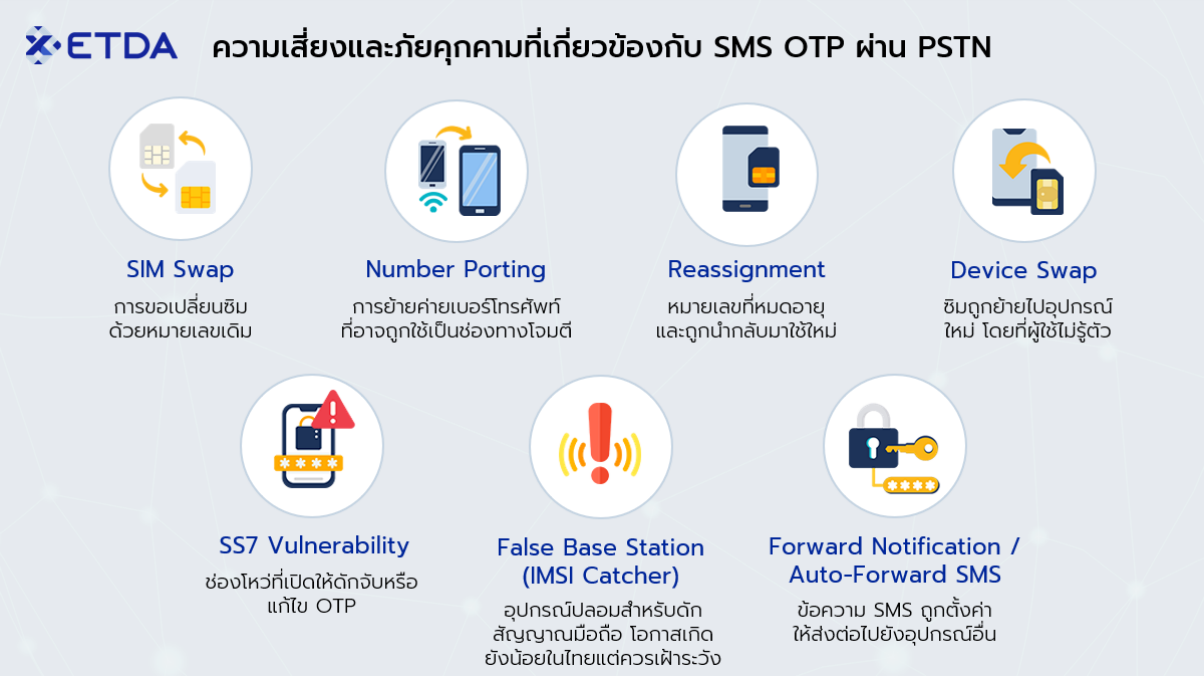
2. ทบทวนวรรณกรรม: รูปแบบการใช้ SMS OTP และข้อจำกัดด้านความปลอดภัย

ตามหลักการของ NIST SP 800-63B อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) เป็นอุปกรณ์ที่สามารถสื่อสารกับ IdP อย่างปลอดภัย ผ่านช่องทางสื่อสารรอง (secondary channel) ซึ่งแยกจากช่องทางสื่อสารหลัก (primary channel) ที่ใช้ในการยืนยันตัวตน ในกรณีที่พบเห็นได้บ่อยของการส่ง SMS OTP ผ่านทาง PSTN นั้น เริ่มต้นจาก IdP ส่ง SMS OTP ไปยังโทรศัพท์มือถือของผู้ใช้งาน (ช่องทางสื่อสารรอง) และผู้ใช้งานต้องนำ OTP ใน SMS มากรอกในหน้าเว็บไซต์ของ IdP ที่ผู้ใช้งานกำลังเข้าถึง ผ่านคอมพิวเตอร์ส่วนบุคคล (ช่องทางสื่อสารหลัก)

โครงข่ายโทรศัพท์สาธารณะ (PSTN) เป็นรากฐานของโครงข่ายโทรศัพท์แบบดั้งเดิมที่เชื่อมต่อกันทั่วโลก ซึ่งเดิมทีออกแบบมาเพื่อการส่งสัญญาณเสียงเป็นหลักผ่านสายทองแดง [1] โครงข่ายนี้อาศัยชุมสายโทรศัพท์ (telephone exchanges) ในการสร้างวงจรการเชื่อมต่อเฉพาะสำหรับการสนทนาแต่ละครั้งตลอดระยะเวลาการใช้งาน โดยพื้นฐานแล้ว PSTN แบบดั้งเดิมไม่ได้มีการออกแบบมาเพื่อรองรับการเข้ารหัสในตัว (built-in encryption) ทั้งสำหรับการสื่อสารด้วยเสียงและสำหรับการส่งข้อความ SMS [1], [2] ทำให้การใช้ SMS OTP เพื่อการยืนยันตัวตนมีความเสี่ยงที่สำคัญ โดยเฉพาะอย่างยิ่งจากช่องโหว่ในโปรโตคอล SS7 ซึ่งอาจนำไปสู่การเปลี่ยนเส้นทาง OTP หรือการดักจับข้อมูลด้วยเทคนิคการโจมตีต่าง ๆ ซึ่งจะเห็นได้ว่า ถึงแม้การใช้ SMS OTP จะให้ความสะดวกในการใช้งาน แต่ก็มีความเสี่ยงด้านความมั่นคงปลอดภัยในการใช้งาน ดังนั้น หน่วยงานผู้ให้บริการควรประเมินความเสี่ยงเหล่านี้อย่างรอบคอบและพิจารณาการนำวิธีการยืนยันตัวตนที่น่าเชื่อถือและมั่นคงปลอดภัยกว่ามาทดแทน เพื่อปกป้องข้อมูลและบัญชีของผู้ใช้งานได้ดียิ่งขึ้น

3. ความเสี่ยงและภัยคุกคามที่เกี่ยวข้องกับการส่ง SMS OTP ผ่านทาง PSTN

จากการศึกษาวรรณกรรม และการสัมภาษณ์ผู้เชี่ยวชาญด้านดิจิทัลไอดีของไทย พบว่าแม้การใช้ SMS OTP จะยังมีความจำเป็นในการใช้เพื่อยืนยันตัวตนก่อนการทำธุรกรรมในบางประเภท แต่ภัยคุกคามและความเสี่ยงต่าง ๆ ที่เกี่ยวข้องนั้น มีแนวโน้มที่เพิ่มขึ้นตามการพัฒนาของเทคโนโลยีและศักยภาพของผู้โจมตีในการโจมตีผ่านช่องโหว่ต่างๆ โดยสามารถแบ่งภัยคุกคามออกเป็นกลุ่มต่าง ๆ ได้ดังนี้



1) **SIM Swap**: คือการแอบอ้างเป็นผู้ใช้งานตัวจริง เพื่อหลอกลวงผู้ให้บริการโทรศัพท์เคลื่อนที่ให้ออกซิมการ์ดใหม่ให้ตนเอง โดยยังเป็นหมายเลขโทรศัพท์เดิมและอยู่ภายใต้ผู้ให้บริการรายเดิม ซึ่งเป็นเทคนิคที่พบในหลายประเทศ เช่น อินเดีย อังกฤษ และสหรัฐอเมริกา การโจมตีประเภทนี้อาจส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงบัญชีออนไลน์ต่างๆ ของผู้ใช้งานที่ผูกกับหมายเลขโทรศัพท์นั้นได้ เช่น บัญชีธนาคาร, บัญชีโซเชียลมีเดีย หรือบริการอื่น ๆ ที่ใช้ SMS OTP ในการยืนยันตัวตน ซึ่งอาจก่อให้เกิดความเสียหายทางการเงินและข้อมูลส่วนบุคคลอย่างร้ายแรง

   - SIM Swap ในปัจจุบันเป็นเหตุการณ์ที่อาจจะเกิดขึ้นน้อยมาก เนื่องจากการออกซิมการ์ดใหม่มีกระบวนการสแกนใบหน้า หรือการอ่าน IC Chip ของบัตรประจำตัวประชาชน แต่ก็อาจจะเกิดขึ้นได้ในกรณีที่มีบุคคลในองค์กรรู้เห็นร่วมด้วย
   - กรณีศึกษาการโจมตีด้วยวิธีการสลับซิมการ์ดในประเทศไทย: ในปี พ.ศ. 2559 ได้เกิดกรณีการโจมตีด้วยเทคนิคการสลับซิมการ์ด (SIM Swap Attack) โดยมีผู้เสียหายซึ่งเป็นผู้ประกอบการขายอุปกรณ์รถยนต์ผ่านแพลตฟอร์มโซเชียลมีเดีย Facebook ได้ตกเป็นเป้าหมายของกลุ่มผู้ไม่หวังดี โดยถูกปลอมแปลงบัตรประจำตัวประชาชน ด้วยการเปลี่ยนแปลงรูปภาพใบหน้าเพื่อแอบอ้างเป็นเจ้าของหมายเลขโทรศัพท์มือถือของผู้เสียหาย และนำบัตรประจำตัวประชาชนปลอมดังกล่าวไปติดต่อศูนย์บริการของผู้ให้บริการโทรศัพท์เคลื่อนที่เพื่อขอออกซิมการ์ดใหม่ โดยใช้หมายเลขเดิมของผู้เสียหาย ภายหลังจากได้รับหมายเลขโทรศัพท์ดังกล่าว ผู้ไม่หวังดีได้ใช้หมายเลขนั้นติดต่อไปยังศูนย์บริการลูกค้าของธนาคาร (Call Center) เพื่อดำเนินการรีเซ็ตรหัสผ่านของบัญชีธนาคาร จากนั้นได้ทำการโอนเงินออกจากบัญชีเป็นจำนวน 3 ครั้ง รวมเป็นมูลค่าทั้งสิ้นกว่า 980,000 บาท ต่อมา

ธนาคารได้ดำเนินการชดเชยความเสียหายให้แก่ผู้เสียหายเต็มจำนวน และเจ้าหน้าที่ตำรวจสามารถจับกุมตัวผู้กระทำความผิดได้ภายในปีเดียวกัน [3]

2) **Number Porting**: เป็นการโอนย้ายหมายเลขโทรศัพท์มือถือจากผู้ให้บริการโทรศัพท์เคลื่อนที่เดิมไปยังผู้ให้บริการโทรศัพท์เคลื่อนที่ใหม่ โดยหากโอนย้ายสำเร็จ ผู้ใช้งานจะได้รับซิมการ์ดใหม่ที่ยังคงเป็นหมายเลขโทรศัพท์เดิม จากผู้ให้บริการโทรศัพท์เคลื่อนที่ใหม่ หากกระบวนการยืนยันตัวตนในขั้นตอนการโอนย้ายไม่มีความเข้มงวดเพียงพอ ผู้ไม่หวังดีอาจใช้ข้อมูลปลอม เช่น บัตรประจำตัวประชาชนปลอม หรือข้อมูลส่วนบุคคลที่ได้มาโดยมิชอบ ในการดำเนินการโอนย้ายหมายเลขโทรศัพท์ของเป้าหมายมาเป็นของตน เมื่อได้หมายเลขโทรศัพท์นั้นมาแล้ว ผู้โจมตีสามารถนำไปใช้ในการเข้าถึงบริการออนไลน์ที่เชื่อมโยงกับหมายเลขโทรศัพท์นั้น เช่น การรีเซ็ตรหัสผ่านบัญชีธนาคาร การยืนยันตัวตนบนแพลตฟอร์มต่าง ๆ หรือแม้แต่การขอรหัส OTP (One-Time Password) เพื่อทำธุรกรรมที่สำคัญ

   - Number Porting ทำได้ยาก เพราะมีขั้นตอนที่ยุ่งยาก จำเป็นต้องให้เจ้าของหมายเลขโทรศัพท์ดำเนินการด้วยตนเอง รวมถึง PIN ที่ใช้ในการโอนย้ายจะมีอายุเพียง 24 ชั่วโมง และจะต้องดำเนินการในรูปแบบ Onsite เท่านั้น

3) **Reassignment**: คือกระบวนการที่ผู้ให้บริการโทรศัพท์เคลื่อนที่นำหมายเลขโทรศัพท์ที่หมดอายุหรือถูกยกเลิกแล้ว กลับมาให้บริการใหม่ เพื่อใช้ทรัพยากรหมายเลขโทรศัพท์อย่างมีประสิทธิภาพ ลักษณะของการโจมตีที่อาจเกิดขึ้นคือ ผู้ใช้บริการคนใหม่ได้รับหมายเลขที่ยังผูกกับบัญชีของผู้ใช้บริการคนเดิมที่เคยเป็นเจ้าของหมายเลขโทรศัพท์นั้น และได้รับรหัส OTP โดยไม่ตั้งใจหรือโดยเจตนา ซึ่งอาจสามารถนำไปใช้ในการเข้าถึงบัญชีของบุคคลอื่น เช่น บัญชีธนาคาร อีเมล หรือแพลตฟอร์มโซเชียลมีเดีย หากไม่มีการตรวจสอบที่รัดกุม อาจนำไปสู่การโจรกรรมข้อมูลหรือการปลอมแปลงตัวตนได้ ซึ่งมีผลกระทบจากเหตุการณ์ลักษณะนี้ ได้แก่ การสูญเสียข้อมูลส่วนบุคคล การถูกเข้าถึงระบบโดยไม่ได้รับอนุญาต และความเสียหายต่อความเชื่อมั่นของผู้ใช้ที่มีต่อระบบการพิสูจน์ตัวตนด้วยโทรศัพท์มือถือ การลดการพึ่งพา SMS OTP และการเพิ่มกลไกยืนยันตัวตนหลายปัจจัยจึงเป็นแนวทางที่ควรส่งเสริม

   - มีการกำหนดให้หมายเลขโทรศัพท์ที่ถูกยกเลิกต้องถูกพักไว้ ประมาณ 90 วัน ก่อนนำกลับมาใช้ใหม่ แต่ปัจจุบันด้วยความต้องการใช้เบอร์โทรศัพท์ที่สูงขึ้นระยะเวลาพักหมายเลขโทรศัพท์จึงลดลงมาเหลือ 30 วัน ซึ่งมีโอกาสที่มิจฉาชีพจะเล็งเป้าหมายเจาะจงเลือกหมายเลขโทรศัพท์ของบุคคลใดบุคคลหนึ่งผ่าน SIM Reuse แม้ผู้ให้บริการโทรศัพท์เคลื่อนที่บางรายอาจเปิดให้เลือกหมายเลขโทรศัพท์ได้ผ่านหน้าเว็บไซต์ แต่โอกาสที่จะได้หมายเลขโทรศัพท์ที่ต้องการแบบเฉพาะเจาะจงนั้นยังเป็นเรื่องยาก

4) **Device Swap**: ซิมการ์ดของผู้ใช้งานถูกย้ายไปใช้งานในอุปกรณ์อื่นโดยที่เจ้าของซิมการ์ดไม่รู้ตัว ซึ่งมักเกิดจากการถูกขโมยซิมการ์ด เมื่อซิมการ์ดถูกนำไปใส่ในอุปกรณ์ของผู้ไม่หวังดี ผู้ไม่หวังดีอาจสามารถควบคุมหมายเลขโทรศัพท์ของผู้เสียหายได้อย่างสมบูรณ์ ลักษณะการโจมตีที่พบบ่อย ได้แก่

การรับรหัส OTP เพื่อเข้าควบคุมบัญชีธนาคาร อีเมล หรือแพลตฟอร์มโซเชียลมีเดีย ส่งผลให้เกิดความเสียหายทั้งในแง่การเงินและความเป็นส่วนตัวของผู้ใช้

5) **SS7 Vulnerability**: Signaling System No. 7 (SS7) เป็นโพรโทคอลสำคัญในโครงข่ายโทรคมนาคมทั่วโลก ซึ่งใช้ในการจัดการการโทรและบริการต่างๆ อย่างไรก็ตาม ด้วยการออกแบบดั้งเดิมที่เน้นความเชื่อใจระหว่างเครือข่าย ทำให้ SS7 มีช่องโหว่ที่เปิดทางให้ผู้ไม่หวังดีสามารถโจมตีได้หลายรูปแบบ เช่น การดักฟังการโทรและข้อความ SMS การติดตามตำแหน่งของผู้ใช้งาน และการขัดขวางการให้บริการ ซึ่งผลกระทบที่ตามมามีความรุนแรง ตั้งแต่การละเมิดความเป็นส่วนตัว การโจรกรรมข้อมูลทางการเงินผ่านการดักจับ OTP ไปจนถึงการเข้าควบคุมบัญชีออนไลน์ต่างๆ และอาจกระทบถึงความมั่นคงในระดับที่ใหญ่ขึ้น ถึงแม้ SS7 จะเป็นเทคโนโลยีที่ถูกใช้มาอย่างยาวนาน แต่การคงอยู่ของช่องโหว่เหล่านี้ยังคงเป็นภัยคุกคามที่สำคัญในโลกดิจิทัลปัจจุบัน

    - Weakness in SS7 Security คือช่องโหว่ในระบบ Signaling System 7 (SS7) ที่ผู้โจมตีสามารถสกัดกั้นหรือดักจับข้อความ SMS ที่มีรหัส OTP ได้โดยตรง

6) **False Base Station (IMSI Catcher)**: คืออุปกรณ์ที่สามารถดักจับสัญญาณโทรศัพท์เคลื่อนที่ในพื้นที่เฉพาะ ซึ่งผู้เชี่ยวชาญไทยประเมินว่าโอกาสเกิดยังน้อยในปัจจุบัน แต่ก็ควรมีการเฝ้าระวัง

    - กรณี 2G (เช่น GSM): การทำงานด้านความปลอดภัยของ 2G ใช้การพิสูจน์ตัวตนทิศทางเดียว (เครือข่ายตรวจสอบซิมการ์ด แต่ซิมการ์ดไม่ตรวจสอบเครือข่าย) และมีการเข้ารหัสการสื่อสารทางอากาศ เช่น A5/1, A5/2 ที่ปัจจุบันถือว่าไม่ปลอดภัยและสามารถถูกบังคับให้ไม่มีการเข้ารหัสได้ (A5/0) โดยช่องโหว่หลักนี้เกิดจากการพิสูจน์ตัวตนที่ไม่สมบูรณ์ ทำให้เกิดการโจมตีโดยสถานีฐานปลอม (IMSI Catcher) เพื่อดักจับข้อมูล IMSI/IMEI, ดักฟังการสนทนา/SMS โดยเฉพาะเมื่อถูกลดระดับการเข้ารหัสหรือไม่มีการเข้ารหัส นอกจากนี้ยังเสี่ยงต่อการติดตามตำแหน่งอีกด้วย
    - กรณี 3G : การทำงานด้านความปลอดภัยของ 3G พัฒนาความปลอดภัยขึ้นมากด้วยการพิสูจน์ตัวตนสองทิศทาง (mutual authentication) ทั้งอุปกรณ์และเครือข่ายต่างตรวจสอบซึ่งกันและกัน และใช้อัลกอริทึมการเข้ารหัสที่ปลอดภัยกว่า พร้อมการปกป้องความสมบูรณ์ของข้อมูล อย่างไรก็ตาม แม้การเชื่อมต่อทางอากาศ (radio interface) ของ 3G จะปลอดภัยขึ้น แต่ก็ยังคงมีภัยคุกคามอยู่ เช่น
        i) ช่องโหว่ในโครงข่ายหลัก: การโจมตีผ่านโพรโทคอลพื้นฐานอย่าง SS7 ที่ยังคงใช้งานร่วมกัน อาจสามารถดักจับ SMS หรือติดตามตำแหน่งได้
        ii) การโจมตีแบบ Downgrade: ผู้ไม่หวังดีอาจพยายามบังคับให้อุปกรณ์ลดระดับการเชื่อมต่อลงไปเป็น 2G เพื่อใช้ประโยชน์จากช่องโหว่ของ 2G
        iii) ช่องโหว่จากการตั้งค่าหรืออุปกรณ์ปลายทาง: การตั้งค่าระบบที่ไม่ถูกต้องหรือมัลแวร์บนโทรศัพท์เคลื่อนที่ยังคงเป็นความเสี่ยง

7) **Forward Notification / Auto-Forward SMS**: การที่ข้อความ SMS หรือการแจ้งเตือนต่างๆ ที่เข้ามายังอุปกรณ์ของผู้ใช้บริการ ถูกตั้งค่าให้ส่งต่อไปยังหมายเลขโทรศัพท์อื่น, อีเมล, หรือบริการออนไลน์อื่นๆ โดยอัตโนมัติ ปัญหาสำคัญคือการตั้งค่าเหล่านี้มักเกิดขึ้นลับหลัง หรือเกิดขึ้นจากการที่ผู้ใช้บริการให้สิทธิ์ในการทำงานของแอปพลิเคชันโดยไม่ได้ตระหนักถึงขอบเขตความจำเป็นในการขอสิทธิ์ ซึ่งทำให้เกิดความเสี่ยงด้านความเป็นส่วนตัวและความปลอดภัย ตัวอย่างการตั้งค่าที่ผู้ใช้บริการอาจไม่ตระหนัก เช่น

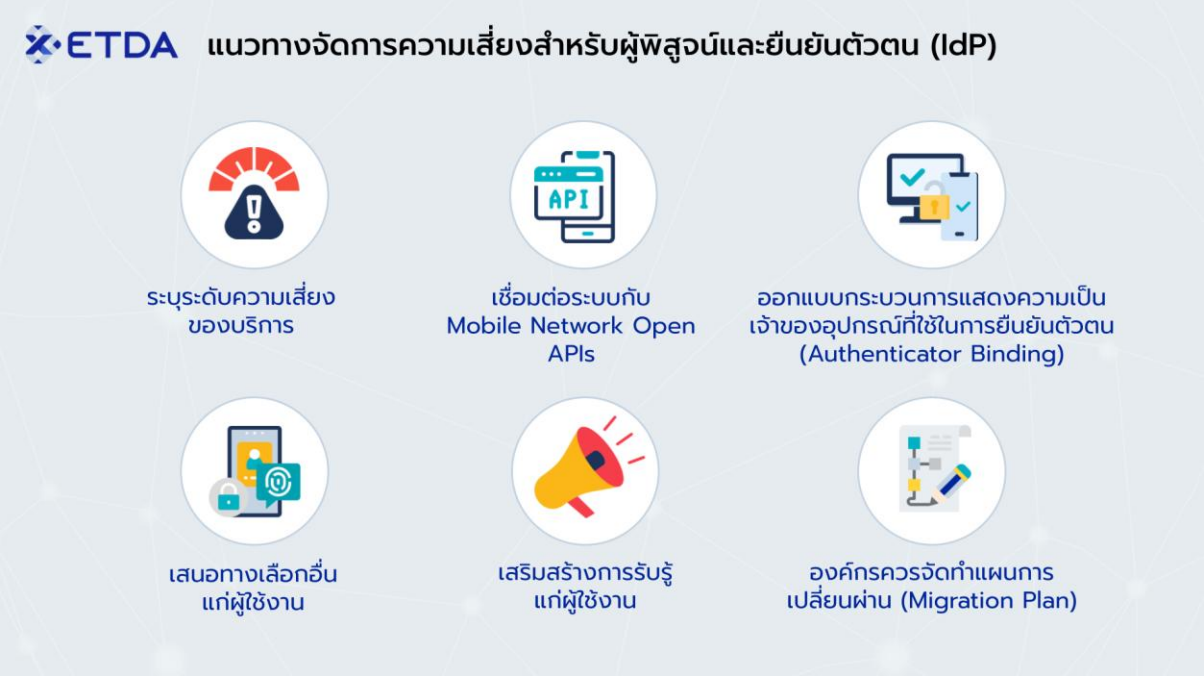
- แอปพลิเคชันอันตราย (Malware): ผู้ใช้บริการอาจถูกหลอกให้ติดตั้งแอปพลิเคชันที่มีมัลแวร์แฝงอยู่ ซึ่งแอปพลิเคชันนี้จะขอสิทธิ์เข้าถึงการใช้งานที่ผิดปกติและลอบส่งต่อข้อความ/การแจ้งเตือน ต่าง ๆ ไปยังผู้ไม่หวังดี
- การเข้าถึงอุปกรณ์โดยตรง: ผู้ไม่หวังดีอาจเข้าถึงอุปกรณ์ของผู้อื่น แล้วแอบติดตั้งแอปพลิเคชันอันตรายหรือเปลี่ยนการตั้งค่าของอุปกรณ์เพื่อส่งต่อข้อมูลกลับมาที่ตนเอง

เมื่อผู้ไม่หวังดีตั้งค่าการส่อต่อข้อมูลสำเร็จแล้ว แอปพลิเคชันดังกล่าวจะดักจับข้อความ/การแจ้งเตือนที่เข้ามา และส่งต่อไปยังปลายทางที่กำหนดไว้โดยอัตโนมัติ อาจเป็นหมายเลขโทรศัพท์อื่น ที่อยู่อีเมล หรือระบบจัดเก็บข้อมูลของผู้โจมตี ผ่านอินเทอร์เน็ตหรือผ่าน SMS อีกทอดหนึ่ง ซึ่งอาจก่อให้เกิดความเสี่ยงในการเข้าถึงข้อมูลที่ละเอียดอ่อน และนำไปสู่การโจรกรรมข้อมูลหรือการละเมิดความเป็นส่วนตัว

ช่องโหว่ของ SMS OTP มักเกิดจากพฤติกรรมโดยสมัครใจของผู้ใช้เอง เช่น การส่งต่อ OTP ให้บุคคลอื่นหรือการใช้ OTP ภายในครอบครัว ซึ่งทำให้การพิสูจน์ตัวตนผ่าน OTP มีความเสี่ยงในการถูกนำไปใช้โดยไม่ได้รับอนุญาต

4. ข้อแนะนำในการจัดการภัยคุกคาม SMS OTP ผ่าน PSTN

ผู้พิสูจน์และยืนยันตัวตน (IdP) อาจพิจารณาแนวทางดังต่อไปนี้ เพื่อเพิ่มความมั่นคงปลอดภัยของการยืนยันตัวตนที่ยังต้องใช้การส่ง SMS OTP ผ่านทาง PSTN ซึ่งยังมีความจำเป็นสำหรับประเทศไทย ที่ยังไม่สามารถละทิ้งการใช้ SMS OTP ได้โดยสิ้นเชิง ซึ่งอ้างอิงตามมาตรฐาน NIST SP 800-63B ที่ระบุว่า “Use of PSTN for out-of-band verification is restricted.” หมายถึง การใช้ SMS OTP ผ่านเครือข่าย PSTN ควรอยู่ภายใต้ข้อจำกัด และไม่ควรใช้กับระบบใหม่ที่ต้องการความน่าเชื่อถือสูง



4.1 ระบุระดับความเสี่ยงของบริการ

สำหรับบริการที่ต้องการความปลอดภัยสูง เช่น บริการด้านการเงิน หรือข้อมูลสุขภาพ ควรหลีกเลี่ยงการใช้ OTP ผ่าน SMS และเปลี่ยนไปใช้ช่องทางอื่นที่มีการผูกกับอุปกรณ์ที่น่าเชื่อถือ (device-bound) ตัวอย่างเช่น แอปพลิเคชันธนาคาร Ubank [4] ของประเทศออสเตรเลียได้เริ่มบังคับใช้การยืนยันตัวตนแบบ device-bound โดยใช้ Passkey

4.2 เชื่อมต่อระบบกับ Mobile Network Open APIs

ใช้บริการ API จากผู้ให้บริการโทรศัพท์เคลื่อนที่ เช่น SIM Swap API, Device Swap API และ Number Verification API เพื่อตรวจสอบความถูกต้อง และความเป็นเจ้าของหมายเลขโทรศัพท์และอุปกรณ์ก่อนการส่ง SMS OTP ตัวอย่างเช่น SIM Swap API ช่วยให้ IdP ตรวจสอบประวัติการเปลี่ยนซิมการ์ด, Device Swap API ช่วยระบุการเปลี่ยนแปลงอุปกรณ์ที่ใช้งาน, และ Number Verification API ช่วยยืนยันความเป็นเจ้าของหมายเลขโทรศัพท์แบบเรียลไทม์ ซึ่งช่วยเพิ่มความมั่นใจในการส่ง SMS OTP

4.3 ออกแบบกระบวนการแสดงความเป็นเจ้าของอุปกรณ์ที่ใช้ในการยืนยันตัวตน (Authenticator Binding)

การเปลี่ยนหมายเลขโทรศัพท์ที่ใช้ในการยืนยันตัวตนควรมีขั้นตอนการตรวจสอบความเป็นเจ้าของหมายเลขโทรศัพท์และอุปกรณ์ที่เข้มงวด เช่น การแสดงบัตรประชาชน ประกอบกับ การทดสอบการยืนยันตัวตน โดยการส่ง SMS OTP ไปยังอุปกรณ์ที่ผูกกับหมายเลขโทรศัพท์ใหม่ของผู้ใช้บริการ

4.4 พิจารณาทางเลือกอื่นในการยืนยันตัวตนผู้ใช้บริการ

อาทิ การใช้วิธีการอื่น ๆ สำหรับสร้าง OTP (เช่น Time-based one-time password: TOTP) การยืนยันตัวตนด้วยลายนิ้วมือหรือใบหน้า หรือการสแกน QR ผ่านแอปพลิเคชันที่มีความปลอดภัย

4.5 เสริมสร้างการรับรู้แก่ผู้ใช้งาน

โดยเฉพาะผู้สูงอายุหรือผู้ใช้ในพื้นที่ชนบท เพื่อให้รู้เท่าทันกลโกงของผู้ไม่หวังดี เช่น การขอ OTP ทางโทรศัพท์ หรือการหลอกลวงให้เปลี่ยนซิมการ์ด

4.6 การจัดทำแผนการเปลี่ยนผ่าน (Migration Plan)

เพื่อรองรับสถานการณ์ในอนาคตที่เครื่องมือยืนยันตัวตนประเภทที่ถูกจำกัดการใช้งาน (restricted authenticator) อาจไม่เป็นที่ยอมรับสำหรับการใช้งานอีกต่อไป โดยแผนการเปลี่ยนผ่านดังกล่าวจะต้องถูกผนวกเข้าไว้ใน Digital Identity Acceptance Statement ขององค์กร [5]

5. สรุป

การส่ง SMS OTP ผ่าน PSTN ไม่ใช่ผู้ร้าย ซึ่งปัจจุบันก็ยังจำเป็นต้องใช้อยู่ในบางบริการที่เหมาะสม และควรคิดถึงผลกระทบให้รอบด้าน แม้การใช้ SMS OTP ผ่าน PSTN จะยังมีความจำเป็นในบางกลุ่มผู้ใช้ โดยเฉพาะในบริบทของประเทศไทยที่การเข้าถึงเทคโนโลยีอาจยังไม่ทั่วถึง แต่หน่วยงานผู้พิสูจน์และยืนยันตัวตนและหน่วยงานที่เกี่ยวข้องควรมีการประเมินความเสี่ยงอย่างรอบคอบ พร้อมวางแนวทางในการเปลี่ยนผ่านสู่ระบบที่มีความปลอดภัยมากยิ่งขึ้น ทั้งนี้ต้องคำนึงถึง “ความมั่นคงปลอดภัย” และ “ความเท่าเทียมในการเข้าถึงบริการ” ควบคู่กันไป

อ้างอิง

[1] A. Doan, “*What Is PSTN and How Does It Actually Work?*”, (Dec. 17, 2024). Accessed: Jun. 05, 2025. [Online Video]. Available: https://www.nextiva.com/blog/what-is-pstn.html

[2] N. Voice, “What Is PSTN - A Complete Guide To The Public Phone Network”, Netlink Voice. Accessed: Jun. 05, 2025. [Online]. Available: https://netlinkvoice.com/blog/what-is-the-pstn/

[3] “รวบยกแก๊งแฮกเงิน9แสนหนุ่มประดับยนต์อยุธยา”, posttoday. Accessed: May 27, 2025. [Online]. Available: https://www.posttoday.com/politics/450606

[4] “Ubank introduces simple and secure app log in with passkeys”, Accessed: May 30, 2025. [Online]. Available: https://www.ubank.com.au/newsroom/ubank-introduces-passkeys

[5] “NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management”, Accessed: May 30, 2025. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html