



ธนาคารแห่งประเทศไทย
BANK OF THAILAND

เอกสารรับฟังความคิดเห็น

(ร่าง) หลักเกณฑ์การรักษาความมั่นคงปลอดภัย ของการให้บริการทางการเงินผ่านช่องทางดิจิทัล (Digital Channel Security)

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายกำกับสถาบันการเงิน
ธนาคารแห่งประเทศไทย
ตุลาคม 2569

ประกาศธนาคารแห่งประเทศไทย

ที่ /2569

เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินผ่านช่องทางดิจิทัล
(Digital Channel Security)

1. เหตุผลในการออกประกาศ

ช่องทางดิจิทัล (Digital Channel) เป็นช่องทางการให้บริการที่มีบทบาทสำคัญสำหรับการทำธุรกรรมทางการเงินในปัจจุบัน ขณะเดียวกันการให้บริการดังกล่าวก็นำมาซึ่งความเสี่ยงจากภัยคุกคามทางไซเบอร์ (cyber threat) และภัยทุจริตทางการเงินที่มีการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (unauthorized payment fraud) อันส่งผลกระทบต่อผู้ใช้บริการในวงกว้าง

ที่ผ่านมา ธนาคารแห่งประเทศไทยตระหนักถึงความสำคัญในการป้องกันภัยคุกคามดังกล่าว จึงได้ออกประกาศหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Mobile Banking Security) ในปี 2568 เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำที่จำเป็นสำหรับการให้บริการ Mobile Application ของสถาบันการเงิน สถาบันการเงินเฉพาะกิจ และผู้ประกอบการธุรกิจบริการเงินอิเล็กทรอนิกส์ อย่างไรก็ตาม มีฉาชีพมีการปรับเปลี่ยนรูปแบบและวิธีการโจมตีไปยังบริการผ่านช่องทางดิจิทัลอื่น อาทิ บริการ Internet Banking และบริการ Mobile Application ของผู้ให้บริการที่มีใช้สถาบันการเงิน เป็นต้น

ในครั้งนี้ ธนาคารแห่งประเทศไทย จึงได้ออกประกาศหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินผ่านช่องทางดิจิทัล (Digital Channel Security) เพื่อยกระดับการรักษาความมั่นคงปลอดภัยของบริการทางการเงินผ่านช่องทางดิจิทัล ได้แก่ บริการทางการเงินผ่าน Mobile Application และบริการ Internet Banking ให้เท่าทันภัยคุกคามทางไซเบอร์ และภัยทุจริต unauthorized payment fraud เพื่อเป็นการสร้างความเชื่อมั่นในระบบสถาบันการเงินและระบบการชำระเงินของประเทศ

2. อำนาจตามกฎหมาย

2.1 อาศัยอำนาจตามความในมาตรา 39 และ 41 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทย ออกหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนช่องทางดิจิทัล ให้สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

2.2 อาศัยอำนาจตามความในมาตรา 120/1 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และที่แก้ไขเพิ่มเติม ธนาคารแห่งประเทศไทยโดยความเห็นชอบของรัฐมนตรีว่าการ

กระทรวงการคลัง ออกหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนช่องทางดิจิทัล ให้สถาบันการเงินเฉพาะกิจถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

2.3 อาศัยอำนาจตามความในมาตรา 24 แห่งพระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560 ธนาคารแห่งประเทศไทย กำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนช่องทางดิจิทัล ให้ผู้ประกอบการธุรกิจบริการเงินอิเล็กทรอนิกส์ถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

2.4 อาศัยอำนาจตามข้อ 11 แห่งประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง ธุรกิจบัตรเครดิต) ออกหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนช่องทางดิจิทัล ให้ผู้ประกอบการธุรกิจบัตรเครดิตถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

2.5 อาศัยอำนาจตามข้อ 11 แห่งประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อส่วนบุคคลภายใต้การกำกับ) ออกหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนช่องทางดิจิทัล ให้ผู้ประกอบการธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับถือปฏิบัติตามที่กำหนด

2.6 อาศัยอำนาจตามข้อ 11 แห่งประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ) ออกหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนช่องทางดิจิทัล ให้ผู้ประกอบการธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับถือปฏิบัติตามที่กำหนด

3. ประกาศที่ยกเลิก

3.1 ประกาศธนาคารแห่งประเทศไทยที่ 4/2568 เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ สำหรับสถาบันการเงิน ลงวันที่ 31 มกราคม 2568

3.2 ประกาศธนาคารแห่งประเทศไทยที่ 17/2568 เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ สำหรับสถาบันการเงินเฉพาะกิจ ลงวันที่ 25 กรกฎาคม 2568

3.3 ประกาศธนาคารแห่งประเทศไทยที่ 18/2568 เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ สำหรับผู้ประกอบการธุรกิจบริการเงินอิเล็กทรอนิกส์ที่ให้บริการ e-Money Mobile Application ลงวันที่ 25 กรกฎาคม 2568

4. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับสถาบันการเงิน สถาบันการเงินเฉพาะกิจ ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ภายใต้การกำกับ ผู้ประกอบธุรกิจบัตรเครดิต ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคล ภายใต้การกำกับ ผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับที่ให้บริการทางการเงินผ่านช่องทางดิจิทัลตามที่ประกาศกำหนด

5. เนื้อหา

5.1 คำจำกัดความ

ในประกาศฉบับนี้

“สถาบันการเงิน” หมายความว่า สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“สถาบันการเงินเฉพาะกิจ” หมายความว่า สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์” หมายความว่า ผู้ประกอบธุรกิจที่ได้รับอนุญาตให้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ภายใต้การกำกับ ตามกฎหมายว่าด้วยระบบการชำระเงิน

“ผู้ประกอบธุรกิจบัตรเครดิต” หมายความว่า ผู้ซึ่งได้รับอนุญาตให้ประกอบธุรกิจบัตรเครดิต ตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาต ตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง ธุรกิจบัตรเครดิต)

“ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับ” หมายความว่า ผู้ซึ่งได้รับอนุญาตให้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับ ตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาต ตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อส่วนบุคคลภายใต้การกำกับ)

“ผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ” หมายความว่า ผู้ซึ่งได้รับอนุญาตให้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ ตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาต ตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ)

“ช่องทางดิจิทัล” หมายความว่า การให้บริการทางอินเทอร์เน็ต (internet banking) และอุปกรณ์เคลื่อนที่ (mobile banking)

“เครื่องอิเล็กทรอนิกส์” หมายความว่า ตู้หรือเครื่องสำหรับฝากหรือถอนเงิน หรือถายทอดเงินคงเหลือ ที่ผู้ให้บริการสามารถดำเนินการได้ด้วยตนเองโดยอัตโนมัติ เช่น เครื่องถอนเงินสดอัตโนมัติ (Automatic Teller Machine: ATM) เครื่องฝากเงินสดอัตโนมัติ (Cash Deposit Machine: CDM)”

“ผู้ให้บริการ” หมายความว่า สถาบันการเงิน สถาบันการเงินเฉพาะกิจ ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ ผู้ประกอบธุรกิจบัตรเครดิต ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับ ผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ

“ผู้ใช้บริการ” หมายความว่า บุคคลธรรมดาที่ใช้บริการทางการเงินผ่านช่องทางดิจิทัล

“บริการทางการเงินผ่านช่องทางดิจิทัล” หมายความว่า การให้บริการโอนเงินไปยังบัญชีของบุคคลอื่นที่มีอยู่กับผู้ให้บริการอื่น หรือการเบิกถอนเงินสดเพื่อรับเงินผ่านเครื่องอิเล็กทรอนิกส์ ที่ผู้ให้บริการสามารถทำการผ่านช่องทางดิจิทัล

“บริการ Mobile Application” หมายความว่า บริการทางการเงินผ่านช่องทางดิจิทัลผ่านแอปพลิเคชันของผู้ให้บริการที่ให้บริการบนอุปกรณ์เคลื่อนที่

“การสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (unauthorized payment fraud)” หมายความว่า ภัยทุจริตทางการเงินที่เกิดขึ้นจากการที่ผู้อื่นสวมรอยทำธุรกรรมแทนผู้ใช้บริการ โดยที่ผู้ใช้บริการไม่ได้ให้ความยินยอม เช่น กรณีผู้ไม่ประสงค์ดีติดตั้ง malware บนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ ทำให้สามารถเข้าถึงหรือควบคุมอุปกรณ์เคลื่อนที่และแอปพลิเคชัน หรือผู้ไม่ประสงค์ดีหลอกลวงเอารหัสผ่านของผู้ใช้บริการไปใช้สวมรอยทำธุรกรรมโดยไม่ได้รับอนุญาต เป็นต้น

5.2 หลักการ

ผู้ให้บริการที่ให้บริการทางการเงินผ่านช่องทางดิจิทัล มีหน้าที่ต้องติดตามดูแลและปรับปรุงให้บริการทางการเงินผ่านช่องทางดิจิทัลมีความมั่นคงปลอดภัยตามมาตรฐานสากล เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริต unauthorized payment fraud ที่มีพัฒนาการเปลี่ยนแปลงไปและใช้เทคนิคซับซ้อนขึ้น ครอบคลุมตั้งแต่การสมัครใช้บริการ การทำธุรกรรม ตลอดจนกระบวนการเปลี่ยนอุปกรณ์เคลื่อนที่สำหรับการใช้บริการทางการเงินผ่าน Mobile Application

5.3 หลักเกณฑ์การรักษาความมั่นคงปลอดภัยของการใช้บริการทางการเงินผ่านช่องทางดิจิทัล

หลักเกณฑ์การรักษาความมั่นคงปลอดภัยผู้ใช้บริการทางการเงินผ่านช่องทางดิจิทัล ประกอบด้วยมาตรการ 3 ส่วน ได้แก่ (1) การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ (2) การ

ป้องกันผู้ไม่ประสงค์ดีสวมรอยเป็นผู้ให้บริการ และ (3) การรักษาความปลอดภัยบริการทางการเงินผ่าน Mobile Application

5.3.1 การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ

ผู้ให้บริการต้องมีมาตรการป้องกันผู้ใช้บริการจากการถูกมิฉ้อฉลสวมรอยทำธุรกรรมแทนผ่านช่องทางดิจิทัลอย่างรัดกุมและเหมาะสม ตลอดการใช้บริการ ตั้งแต่ การสมัครใช้บริการ การติดตั้งบริการ Mobile Application บนอุปกรณ์เคลื่อนที่ และการทำธุรกรรมผ่านช่องทางดิจิทัล อย่างน้อย ดังนี้

1. การรักษาความปลอดภัยในขั้นตอนการสมัครใช้บริการ และการติดตั้ง Mobile Application บนอุปกรณ์เคลื่อนที่ใหม่

(1.1) จัดให้มีกระบวนการพิสูจน์และยืนยันตัวตนผู้ใช้บริการอย่างรัดกุม เพื่อป้องกันการสวมรอยแอบอ้างเป็นบุคคลอื่น (identity theft) มาสมัครใช้บริการทางการเงินผ่านช่องทางดิจิทัล หรือติดตั้งบริการ Mobile Application บนอุปกรณ์เคลื่อนที่ใหม่ โดยต้องดำเนินการตามกระบวนการรู้จักลูกค้า (Know Your Customer: KYC) อย่างรัดกุม หรือกระบวนการยืนยันตัวตนลูกค้า โดยใช้การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ที่มีความน่าเชื่อถือและสามารถพิสูจน์ได้ว่าเป็นผู้ใช้บริการรายนั้นจริง

(1.2) จัดให้มีการสร้างและส่งมอบปัจจัยยืนยันตัวตนไปยังผู้ใช้บริการด้วยวิธีการที่ปลอดภัยและรัดกุม โดยอย่างน้อยครอบคลุม การกำหนดให้ลูกค้าเป็นผู้สร้างหรือเปลี่ยนรหัสผ่านด้วยตนเอง การป้องกันการดักจับหรือเปลี่ยนแปลงข้อมูลยืนยันตัวตนขณะรับ-ส่ง กระบวนการและแนวทางการรักษาความปลอดภัยการลงทะเบียนอุปกรณ์เคลื่อนที่ (device binding) สำหรับบริการ mobile application เพื่อให้มั่นใจว่าข้อมูลยืนยันตัวตนไม่ถูกดัดแปลงแก้ไข และรั่วไหลไปยังบุคคลอื่น

(1.3) จำกัดการใช้บริการทางการเงินผ่านช่องทางดิจิทัลของผู้ใช้บริการไว้เพียง 1 บัญชีผู้ใช้งานต่อ 1 บริการของผู้ให้บริการ และจำกัดการใช้บริการดังกล่าว โดยให้ใช้งานบน 1 อุปกรณ์ของผู้ใช้บริการเท่านั้น เพื่อป้องกันการสวมรอยเข้าใช้งาน หรือทำธุรกรรมแทนผู้ใช้บริการ

(1.4) กรณี ผู้ใช้บริการการสมัครใช้บริการผ่านช่องทางที่ไม่พบเห็นลูกค้าต่อหน้า (non-Face-to-Face) หรือติดตั้งบริการ Mobile Application บนอุปกรณ์เคลื่อนที่ใหม่ ผู้ให้บริการต้องจัดให้มีมาตรการควบคุมความเสี่ยงจากการใช้บริการทางการเงินดิจิทัลในช่วงแรกเพิ่มเติม เพื่อลดความเสี่ยงหรือจำกัดความเสียหายจากการถูกสวมรอยทำธุรกรรม เช่น การจำกัดการใช้บริการชั่วคราวหลังสมัครบริการ (Cooling-off Period) การจำกัดให้ทำได้เฉพาะธุรกรรมเสี่ยงต่ำ การจำกัดวงเงินขั้นต่ำชั่วคราว เป็นต้น

(1.5) แจ้งเตือนผลสมัครใช้บริการ หรือติดตั้งบริการ Mobile Application บนอุปกรณ์เคลื่อนที่ใหม่ให้ผู้ให้บริการรับทราบในทันที ผ่านช่องทางที่แยกจากช่องทางหลักในการให้บริการดิจิทัล (Out-of-Band) เช่น ข้อความสั้น (SMS) อีเมล ช่องทางโซเชียลมีเดียอย่างเป็นทางการ (Official Account) โทรศัพท์ที่ผู้ให้บริการได้ลงทะเบียนไว้กับผู้ให้บริการ เป็นต้น โดยเนื้อหาการแจ้งเตือนต้องมีรายละเอียดเพียงพอให้ผู้ให้บริการสามารถตรวจสอบความถูกต้องของธุรกรรมได้

2. การรักษาความปลอดภัยขณะใช้บริการดิจิทัล

(2.1) จัดให้มีการยืนยันตัวตนผู้ใช้บริการที่ทำธุรกรรมผ่านช่องทางดิจิทัลด้วยวิธีการที่เหมาะสมตามระดับความเสี่ยงของแต่ละธุรกรรม โดยธุรกรรมที่มีความเสี่ยงสูงต้องมีการยืนยันตัวตนผู้ใช้งานแบบหลายปัจจัย (multi-factor authentication) ในขั้นตอนการอนุมัติรายการ (authorization) อย่างน้อยครอบคลุม (1) การโอนเงินไปยังบัญชีบุคคลอื่น (2) การเบิกถอนเงินสด การเบิกถอนวงเงินสินเชื่อ การเบิกถอนวงเงินบัตรเครดิตและรับเงินที่ตู้ ATM และ (3) การปรับเพิ่มวงเงินธุรกรรม โอนเงินและถอนเงินต่อวัน เพื่อป้องกันการถูกสวมรอยทำธุรกรรมแทนผู้ใช้บริการโดยไม่ได้รับอนุญาต และมั่นใจว่าผู้ทำธุรกรรมเป็นผู้ใช้บริการ

ทั้งนี้ สำหรับธุรกรรมโอนเงินที่มีความเสี่ยงต่ำ เช่น การทำธุรกรรมโอนเงินระหว่างบัญชีตนเอง ผู้ให้บริการอาจพิจารณาใช้วิธีการยืนยันตัวตนอื่นที่เหมาะสมกับความเสี่ยงแทนการยืนยันตัวตนผู้ใช้งานแบบหลายปัจจัยได้ โดยได้รับความเห็นชอบจากหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงเป็นลายลักษณ์อักษร

(2.2) จัดให้มีการใช้ปัจจัยยืนยันตัวตนผู้ใช้บริการที่มีประสิทธิภาพ ปลอดภัย และยากต่อการถูกสวมรอย รวมทั้ง ทบทวนและปรับปรุงปัจจัยยืนยันตัวตนให้เท่าทันรูปแบบภัยคุกคามจากการสวมรอยทำธุรกรรมแทนผู้ใช้บริการอย่างสม่ำเสมอ โดยมีมาตรการควบคุมปัจจัยยืนยันตัวตนในแต่ละประเภท อย่างน้อย ดังนี้

(2.2.1) ปัจจัยการยืนยันตัวตนประเภทสิ่งที่คุณรู้ (something you know) ผู้ให้บริการต้องจัดให้มีมาตรการลดความเสี่ยงจากการโจมตีในลักษณะ Brute force เช่น จำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด และระงับบัญชีผู้ใช้งานเป็นการชั่วคราว เป็นต้น

(2.2.2) ปัจจัยการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have) ผู้ให้บริการต้องใช้ปัจจัยยืนยันตัวตนที่ยากต่อการถูกปลอมแปลงและลดความเสี่ยงต่อการโจมตีแบบฟิชซิง (phishing attack) เช่น ปัจจัยที่ใช้กุญแจเข้ารหัสซึ่งลงทะเบียนกับอุปกรณ์ (Cryptographic key-based) บนอุปกรณ์ Hardware หรือ Software Token อุปกรณ์ Passkey การใช้รหัสใช้ครั้งเดียว (One Time Password-OTP) ผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ที่ลงทะเบียนไว้ล่วงหน้ากับผู้ให้บริการทางการเงิน เป็นต้น โดยให้ทดแทนการใช้รหัส OTP ที่ส่งผ่านช่องทาง SMS หรืออีเมล เป็นปัจจัยยืนยันตัวตนสำหรับการทำธุรกรรมโอนเงิน ธุรกรรมเบิกถอนเงินสด เบิกถอนวงเงินสินเชื่อ เบิกถอนวงเงินบัตรเครดิต

และรับเงินที่ตู้ ATM และการปรับเพิ่มวงเงินสำหรับการโอนเงิน เพื่อป้องกันความเสี่ยงจากการดักจับข้อมูล OTP และการสวมรอยออก SIM ใหม่ (SIM swap attack)

(2.2.3) ปัจจัยการยืนยันตัวตนประเภทสิ่งที่คุณเป็น (something you are) ผู้ให้บริการต้องใช้เทคโนโลยีชีวมิติ (biometrics) ที่มีความถูกต้องแม่นยำร่วมกับเทคนิคตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) เพื่อป้องกันการปลอมแปลงอัตลักษณ์สวมรอยทำธุรกรรมแทนผู้ให้บริการ

(2.3) แจ้งเตือนผลการทำธุรกรรมที่มีความเสี่ยงสูงทันทีผ่านช่องทาง เช่น แอปพลิเคชัน ข้อความสั้น (SMS) อีเมล ช่องทางโซเชียลมีเดียอย่างเป็นทางการ (Official Account) เป็นต้น โดยเนื้อหาการแจ้งเตือนต้องมีรายละเอียดเพียงพอให้ผู้ให้บริการสามารถตรวจสอบความถูกต้องของธุรกรรมได้

5.3.2 การป้องกันผู้ไม่ประสงค์ดีสวมรอยเป็นผู้ให้บริการ

ผู้ให้บริการต้องมีมาตรการป้องกันมิฉ้อฉลแอบอ้างสวมรอยเป็นผู้ให้บริการ เพื่อหลีกเลี่ยงขอข้อมูลสำคัญหรือหลอกลวงให้ผู้ให้บริการติดตั้งโปรแกรมไม่ประสงค์ดี (malware) ซึ่งอาจนำไปสู่การสวมรอยทำธุรกรรมแทนผู้ให้บริการได้ อย่างน้อย ดังนี้

1. งดเว้นการแนบลิงก์ผ่านช่องทางข้อความสั้น (SMS) และช่องทางอีเมล แต่สำหรับกรณีช่องทางสื่อสังคมออนไลน์ (social media) ให้ผู้ให้บริการงดแนบลิงก์เฉพาะที่มีการขอข้อมูลในการยืนยันตัวตน หรือข้อมูลส่วนบุคคลที่สำคัญ เช่น ชื่อผู้ใช้งาน รหัสผ่าน รหัสใช้ครั้งเดียว (one time password - OTP) หมายเลขบัตรประชาชน เพื่อป้องกันการสวมรอยเป็นผู้ให้บริการ การขอให้เปิดเผยข้อมูลสำคัญ (social engineering) หรือการถูกติดตั้ง malware

อย่างไรก็ดี ผู้ให้บริการสามารถแนบลิงก์ผ่านทั้ง 3 ช่องทางดังกล่าวได้ หากผู้ให้บริการดำเนินการร้องขอเอง โดยสามารถแนบลิงก์ได้เป็นรายครั้ง พร้อมทั้งต้องมีการสื่อสารย้ำให้ผู้ให้บริการทราบว่าการส่งลิงก์ดังกล่าวเป็นกรณีเฉพาะตามคำร้องขอของผู้ให้บริการเป็นรายครั้งเท่านั้น

2. มีกระบวนการติดตามและรับมืออย่างทันการณ์ต่อแอปพลิเคชันที่ปลอมแปลงหรือแอบอ้างเป็นแอปพลิเคชันของผู้ให้บริการในแพลตฟอร์มที่เป็นทางการของผู้ให้บริการดาวน์โหลดแอปพลิเคชัน (official app store) เช่น Google Play Store Apple App Store รวมทั้งมีกระบวนการรับมือและตอบสนองอย่างเหมาะสมและทันการณ์สำหรับเว็บไซต์ปลอมแปลง หรือแอปพลิเคชันปลอมแปลงที่อยู่นอกแพลตฟอร์มดังกล่าว เพื่อลดความเสี่ยงที่ผู้ให้บริการจะหลงเชื่อและเปิดเผยข้อมูลสำคัญ ถูกติดตั้ง malware หรือถูกติดตั้งแอปพลิเคชันปลอม

5.3.3 การรักษาความปลอดภัยบริการทางการเงินผ่าน Mobile Application

ผู้ให้บริการที่ให้บริการทางการเงินผ่านช่องทาง Mobile Application ต้องมีการรักษาความมั่นคงปลอดภัยบริการ Mobile Application เพิ่มเติม เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์และภัยทุจริตทางการเงิน ดังนี้

1. การรักษาความปลอดภัยข้อมูล

ผู้ให้บริการต้องรักษาความลับและความปลอดภัยข้อมูลสำคัญของผู้ใช้บริการอย่างรัดกุม เพื่อป้องกันข้อมูลสำคัญของผู้ใช้บริการรั่วไหล หรือถูกเปลี่ยนแปลงแก้ไข ทั้งขณะจัดเก็บ แสดงผล และรับ-ส่งข้อมูลระหว่างอุปกรณ์เคลื่อนที่ของผู้ใช้บริการและระบบงานของผู้ให้บริการ อย่างน้อย ดังนี้

(1.1) หลีกเลี่ยงการจัดเก็บข้อมูลสำคัญไว้ในอุปกรณ์เคลื่อนที่ เช่น ข้อมูลที่ใช้ยืนยันตัวตน ข้อมูลส่วนบุคคลโดยหากจำเป็นต้องจัดเก็บข้อมูลดังกล่าว ต้องมีกระบวนการรักษาความปลอดภัยที่รัดกุม โดยอย่างน้อยผู้ให้บริการต้องเข้ารหัสข้อมูล (data encryption) ด้วยวิธีการที่ปลอดภัยตามมาตรฐานสากล และทำลายข้อมูลเมื่อสิ้นสุดการใช้งานข้อมูล

(1.2) แอปพลิเคชันของผู้ให้บริการต้องแสดงผลข้อมูลสำคัญ (sensitive information) ของผู้ใช้บริการเท่าที่จำเป็นและเป็นไปอย่างรัดกุม โดยอย่างน้อยต้องปิดบังการแสดงผลรหัสผ่าน และปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (application blurring)

(1.3) ใช้ช่องทางสื่อสารที่ปลอดภัย (secure protocol) และยืนยันตัวตนด้วยเทคนิค certificate pinning หรือวิธีอื่นที่เทียบเท่า รวมทั้งต้องดำเนินการเข้ารหัสข้อมูลสำคัญในระดับแอปพลิเคชัน (application layer) ในการรับ-ส่งข้อมูล เพื่อป้องกันการถูกดักจับหรือแก้ไขเปลี่ยนแปลงข้อมูลระหว่างการรับส่ง (man in the middle attack)

2. การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน

ผู้ให้บริการต้องรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน และการยืนยันตัวตนผู้ใช้บริการเพื่อใช้บริการ Mobile Application รวมทั้ง ติดตามดูแลและปรับปรุงแอปพลิเคชันให้มีความมั่นคงปลอดภัยตามมาตรฐานสากลและเท่าทันภัยคุกคามรูปแบบใหม่อยู่เสมอ อย่างน้อย ดังนี้

(2.1) แอปพลิเคชันของผู้ให้บริการต้องขอสิทธิเข้าถึงทรัพยากรหรือบริการบนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ (application permission) เท่าที่จำเป็น และมีการทบทวนการขอสิทธิดังกล่าวทุกครั้งที่มีการเปลี่ยนแปลงแอปพลิเคชันอย่างมีนัยสำคัญ เพื่อป้องกันการละเมิดสิทธิความเป็นส่วนตัวของผู้ใช้บริการ รวมถึงเป็นช่องโหว่ที่อาจถูกใช้โดยผู้อื่นที่กระทำการโดยทุจริต

(2.2) ไม่ให้บริการบนแอปพลิเคชันเวอร์ชันเก่าที่อาจมีช่องโหว่ และอาจทำให้

เกิดความเสี่ยงในการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ

(2.3) ตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชันทุกครั้งในทันทีที่ผู้ใช้บริการเข้าใช้งาน (anti-tampering) และไม่อนุญาตให้ผู้ใช้บริการใช้งานแอปพลิเคชันที่ถูกเปลี่ยนแปลงแก้ไข เพื่อป้องกันไม่ให้ข้อมูลผู้ใช้บริการรั่วไหลหรือเกิดความเสียหายจากแอปพลิเคชันที่มีการดัดแปลงแก้ไข เช่น การฝัง malicious code

(2.4) จัดการการเชื่อมต่อระหว่างคอมพิวเตอร์ (session) ให้ปลอดภัย เพื่อป้องกันการสวมรอยเข้าใช้งานโดยไม่ได้รับอนุญาต (session hijacking)

(2.5) ป้องกัน source code ของแอปพลิเคชันไม่ให้อยู่ในรูปแบบที่อ่านเข้าใจโดยง่าย เช่น การทำ source code obfuscation เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงและทำการเปลี่ยนแปลงแก้ไข source code ได้

(2.6) ต้องจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้บริการเพิ่มเติมในขั้นตอนการทำธุรกรรมผ่านบริการ Mobile Application บนอุปกรณ์เคลื่อนที่ โดยใช้เทคโนโลยีเปรียบเทียบใบหน้า (face comparison) ร่วมกับการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) เพื่อให้มั่นใจว่าผู้ใช้บริการเป็นผู้ทำธุรกรรมด้วยตนเอง ซึ่งต้องจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้บริการเพิ่มเติมดังกล่าวอย่างน้อยในกรณีดังต่อไปนี้

(1) การทำธุรกรรมโอนเงินในแต่ละครั้งมีมูลค่าตั้งแต่ 50,000 บาทขึ้นไป หรือ
(2) การทำธุรกรรมโอนเงินมูลค่ารวมกัน ครบทุก 200,000 บาท ในรอบระยะเวลา 1 วัน หรือ

(3) การปรับเพิ่มวงเงินการทำธุรกรรมโอนเงินต่อวัน ตั้งแต่ 50,000 บาทขึ้นไป
ทั้งนี้ กรณีที่ผู้ใช้บริการมีข้อจำกัดในการใช้เทคโนโลยีเปรียบเทียบใบหน้า (face comparison) เช่น เป็นคนพิการทางสายตา ผู้ให้บริการอาจพิจารณาขบวนการยืนยันตัวตนเพิ่มเติมตามที่กำหนดข้างต้นได้ โดยต้องมีแนวทางลดความเสี่ยงทดแทน หรือกรณีการทำธุรกรรมที่มีความเสี่ยงต่ำ เช่น การทำธุรกรรมโอนเงินระหว่างบัญชีตนเอง การทำธุรกรรมโอนเงินประจำอัตโนมัติ (automatic recurring transfer) ที่ได้ยืนยันตัวตนไปแล้วในครั้งแรก ผู้ให้บริการอาจพิจารณาขบวนการยืนยันตัวตนเพิ่มเติมตามที่กำหนดข้างต้นได้

3. การรักษาความมั่นคงปลอดภัยของอุปกรณ์เคลื่อนที่

ผู้ให้บริการต้องให้บริการ Mobile Application ในสภาพแวดล้อมของอุปกรณ์เคลื่อนที่ที่ปลอดภัย เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีกระทำการทุจริตโดยอาศัยช่องโหว่ของระบบปฏิบัติการเข้าถึง Mobile Application และบัญชีของผู้ใช้บริการ อย่างน้อย ดังนี้

(3.1) ไม่อนุญาตให้แอปพลิเคชันของผู้ให้บริการใช้งานบนอุปกรณ์เคลื่อนที่ที่ตรวจพบว่าการเปิดสิทธิ์ให้เข้าถึงระบบปฏิบัติการ (rooted/jailbroken)

(3.2) ไม่อนุญาตให้แอปพลิเคชันของผู้ให้บริการทำงานบนอุปกรณ์เคลื่อนที่ ในขณะที่มีแอปพลิเคชันอื่นกำลังทำงานและมีพฤติกรรมการทำงานที่เสี่ยงจะก่อให้เกิดการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ เพื่อป้องกันแอปพลิเคชันของผู้ให้บริการถูกควบคุมหรือเข้าถึงโดย malware ที่ติดตั้งบนอุปกรณ์เคลื่อนที่ อย่างน้อย ดังนี้

1. แอปพลิเคชันที่ขอสิทธิช่วยเหลือคนพิการ (accessibility services) โดยไม่จำเป็น
2. แอปพลิเคชันที่สามารถควบคุมอุปกรณ์เคลื่อนที่จากระยะไกลได้ (remote control)
3. แอปพลิเคชันที่มีการปิดบังหรือขโมยข้อมูลสำคัญที่แสดงบนหน้าจอของผู้ใช้งาน

(3.3) หลักเล็งการให้บริการ Mobile Application ของผู้ให้บริการบนอุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการที่หน่วยงานด้านความมั่นคงปลอดภัยที่เป็นที่ยอมรับ เช่น Thailand Banking Sector Computer Emergency Response Team (TB-CERT) กำหนดว่ามีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ หรือการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ

กรณีผู้ให้บริการมีการให้บริการบนอุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ หรือการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ ผู้ให้บริการต้องจัดให้มีแนวทางการควบคุมความเสี่ยงเพิ่มเติม เช่น จำกัดธุรกรรมโอนเงินได้เฉพาะบัญชีตนเองเท่านั้น จำกัดวงเงินการทำธุรกรรมของกลุ่มผู้ใช้บริการดังกล่าวให้ทำธุรกรรมโอนเงินได้ไม่เกินวันละ 5,000 บาท จัดให้มีการยืนยันตัวตนโดยใช้เทคโนโลยีเปรียบเทียบกับหน้าเพิ่มเติมเมื่อทำธุรกรรมทางการเงิน รวมทั้งแจ้งเตือนผู้ใช้บริการถึงความเสี่ยงจากกรณีดังกล่าว

ทั้งนี้ ผู้ให้บริการต้องติดตามและปรับปรุงการรักษาความมั่นคงปลอดภัยของการให้บริการ Mobile Application ให้เท่าทันภัยคุกคามทางไซเบอร์และภัยทุจริตรูปแบบใหม่ เป็นไปตามมาตรฐานสากลอย่างต่อเนื่อง โดยกรณีที่พบช่องโหว่ใหม่ ผู้ให้บริการต้องเร่งดำเนินการให้มีแนวทางป้องกันเพื่อปิดช่องโหว่ภายในกรอบเวลาที่เหมาะสม หรือดำเนินการให้แล้วเสร็จภายในระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด

5.4 การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์

กรณีที่ผู้ให้บริการทางการเงินผ่านช่องทางดิจิทัล มีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้ได้ ให้ยื่นขอผ่อนผันเป็นรายกรณีต่อธนาคารแห่งประเทศไทย พร้อมแสดงเหตุผลความจำเป็นและแผนการดำเนินการ เพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนด ทั้งนี้ ธนาคารแห่งประเทศไทยจะพิจารณาให้แล้วเสร็จภายใน 30 วันทำการ นับแต่วันที่รับคำขอและเอกสารถูกต้องครบถ้วน โดย ธนาคารแห่งประเทศไทยอาจกำหนดเงื่อนไขใด ๆ ให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

6. บทเฉพาะกาล

กรณีที่ผู้ให้บริการทางการเงินผ่านช่องทางดิจิทัล มีเหตุจำเป็นหรือพฤติการณ์พิเศษที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้อยู่ก่อนที่ประกาศฉบับนี้ใช้บังคับ และประสงค์จะขอผ่อนผันการปฏิบัติตามหลักเกณฑ์ดังกล่าว ให้ผู้ให้บริการทางการเงินผ่านช่องทางดิจิทัล ยื่นคำขอผ่อนผันตามหลักเกณฑ์ข้อ 5.4 ภายใน 7 วัน นับแต่วันที่ประกาศฉบับนี้มีผลใช้บังคับ โดยให้ถือว่าการปฏิบัติในระหว่างระยะเวลาการขอผ่อนผันและการพิจารณาผ่อนผันของธนาคารแห่งประเทศไทยดังกล่าว ไม่เป็นการฝ่าฝืนหลักเกณฑ์ของประกาศนี้

7. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวัน ยกเว้นข้อ 5.3.1 (2.1) (2) ให้มีผลบังคับใช้เก้าสิบวันนับแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา

ประกาศ ณ วันที่

มกราคม 2570

(นายวิทย์ รัตนกร)

ผู้ว่าการ

ธนาคารแห่งประเทศไทย

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โทรศัพท์ 0 2283 6347, 0 2283 6346