ธนาคารแห่งประเทศไทย

12 เมษายน 2564

เรียน ผู้จัดการ

สถาบันการเงินเฉพาะกิจทุกแห่ง

ที่ ฝนส2.271/2564 เรื่อง นำส่งประกาศธนาคารแห่งประเทศไทย เรื่อง การให้สินเชื่อเพื่อผู้สูงอายุโดยมีที่อยู่อาศัยเป็นหลักประกัน (Reverse Mortgage) ของสถาบันการเงินเฉพาะกิจ ประกาศธนาคารแห่งประเทศไทย เรื่อง การส่งรายงานข้อมูลของสถาบันการเงินเฉพาะกิจ และแนวนโยบายธนาคารแห่งประเทศไทย เรื่องการรักษาความมั่นคงปลอดภัยของการใช้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ของสถาบันการเงินเฉพาะกิจ

ธนาคารแห่งประเทศไทย (ธปท.) โดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงการคลัง ได้ออกหลักเกณฑ์การกำกับดูแลสำหรับสถาบันการเงินเฉพาะกิจ (SFIs) เพื่อยกระดับการดำเนินการของ SFIs ให้มีประสิทธิภาพ มั่นคงปลอดภัย และสามารถดำเนินการตามพันธกิจได้อย่างยั่งยืนมาอย่างต่อเนื่อง โดยครั้งนี้ ธปท. เห็นควรออกหลักเกณฑ์กำกับดูแล SFIs ใน 3 เรื่อง สรุปสาระสำคัญดังนี้

1. ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 2/2564 เรื่อง การให้สินเชื่อเพื่อผู้สูงอายุโดยมีที่อยู่อาศัยเป็นหลักประกัน (Reverse Mortgage: RM) ของสถาบันการเงินเฉพาะกิจ

ตามที่คณะรัฐมนตรีมีมติเห็นชอบให้ SFIs เป็นธนาคารนำร่องในการให้สินเชื่อ Reverse Mortgage เพื่อเป็นมาตรการรองรับสังคมผู้สูงอายุของประเทศ ธปท. จึงได้ออกหลักเกณฑ์สินเชื่อ Reverse Mortgage ซึ่งเป็นธุรกรรมสินเชื่อที่ให้กับผู้กู้ที่เป็นผู้สูงอายุ โดยนำที่อยู่อาศัยที่เป็นกรรมสิทธิ์ของตนและปลอดภาระหนี้มาเป็นหลักประกัน โดยผู้กู้จะได้รับเงินให้สินเชื่อในลักษณะทยอยรับเป็นงวดจนกว่าผู้กู้จะเสียชีวิตหรือครบกำหนดอายุสัญญาสินเชื่อตามเงื่อนไขที่ได้ตกลงไว้ ทั้งนี้ ด้วยสินเชื่อ Reverse Mortgage มีลักษณะที่แตกต่างไปจากธุรกรรมสินเชื่อทั่วไป SFIs จึงควรมีการบริหารความเสี่ยงอย่างเหมาะสม เช่น การจัดทำนโยบายการให้สินเชื่อ การวิเคราะห์สินเชื่อ การจัดชั้นและกันเงินสำรอง การดำรงเงินกองทุน เป็นต้น รวมถึงควรให้ความสำคัญกับการคุ้มครองผู้บริโภค โดย SFIs ต้องมีความรู้ความเข้าใจในสินเชื่อดังกล่าว และต้องนำเสนอให้ผู้กู้และผู้ที่อาจได้รับผลกระทบมีความเข้าใจในผลิตภัณฑ์ ความเสี่ยง และสิทธิในกรณีต่าง ๆ

2. ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 3/2564 เรื่อง การส่งรายงานข้อมูลของสถาบันการเงินเฉพาะกิจ

ธปท. ปรับปรุงหลักเกณฑ์การจัดส่งรายงานข้อมูล โดยให้ SFIs ที่มีการให้สินเชื่อเพื่อที่อยู่อาศัย จัดส่งรายงานข้อมูลสินเชื่อเพื่อที่อยู่อาศัยและสินเชื่ออื่นที่เกี่ยวเนื่องกับสินเชื่อเพื่อที่อยู่อาศัย (แบบรายงานสินเชื่อเพื่อที่อยู่อาศัยจำแนกตามอัตราส่วนเงินให้สินเชื่อต่อมูลค่าหลักประกัน (แบบรายงาน LTV) และแบบรายงานสินเชื่อที่มีที่อยู่อาศัยเป็นหลักประกัน (แบบรายงาน MGL)) เพื่อให้กระทรวงการคลัง และ ธปท. มีข้อมูลเพียงพอในการติดตามคุณภาพสินเชื่อภาคอสังหาริมทรัพย์ อันเป็นประโยชน์ต่อการดำเนินนโยบายและการกำกับดูแล โดยขอให้ SFIs จัดส่งแบบรายงาน LTV เป็นรายไตรมาส ภายใน 1 เดือนนับจากวันสิ้นไตรมาส โดยเริ่มรายงานตั้งแต่งวดสิ้นไตรมาส 2 ปี 2564 เป็นต้นไป และแบบรายงาน MGL เป็นรายเดือน ภายใน 1 เดือนนับจากวันสิ้นเดือน โดยเริ่มรายงานตั้งแต่ข้อมูลเดือนพฤษภาคม 2564 เป็นต้นไป

3. แนวนโยบายธนาคารแห่งประเทศไทย เรื่องการรักษาความมั่นคงปลอดภัยของการใช้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ของสถาบันการเงินเฉพาะกิจ

ธปท. เห็นควรยกระดับการกำกับดูแลด้านมาตรฐานการรักษาความมั่นคงปลอดภัยของบริการ Mobile Banking ที่ให้บริการแก่ลูกค้ารายย่อยกับ SFIs เช่นเดียวกับที่บังคับใช้กับธนาคารพาณิชย์แล้ว

ตั้งแต่วันที่ 1 พฤษภาคม 2563 ซึ่งประกอบด้วยมาตรการ 2 ระดับ คือ (1) มาตรการขั้นต่ำที่ SFIs ต้องดำเนินการเพื่อให้บริการ Mobile Banking มีความมั่นคงปลอดภัยที่รัดกุม และ (2) มาตรการเพิ่มเติมที่ SFIs อาจพิจารณาดำเนินการเพื่อให้บริการ Mobile Banking มีความรัดกุมปลอดภัยยิ่งขึ้น

พร้อมกันนี้ ธปท. ได้ขอความร่วมมือ SFIs ในการจัดส่งรายงานข้อมูลเพิ่มเติม ดังนี้

1. ข้อมูลสินเชื่อเพื่อการอุปโภคบริโภคส่วนบุคคล (แบบรายงานสินเชื่อเพื่อการอุปโภคบริโภคส่วนบุคคล : Loans for Personal Consumption (LPC)) เพื่อให้ ธปท. มีข้อมูลภาพรวมสินเชื่อเพื่อการอุปโภคบริโภคส่วนบุคคลทั้งระบบ มาพัฒนาตัวชี้วัดความสามารถในการชำระหนี้และประเมินความเสี่ยงของภาคครัวเรือน โดยขอให้ SFIs จัดส่งแบบรายงานเป็นรายเดือน ภายใน 1 เดือนนับจากวันสิ้นเดือนนั้น และเริ่มรายงานตั้งแต่ข้อมูลงวดสิ้นเดือนพฤษภาคม 2564 เป็นต้นไป

2. ข้อมูลเพื่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (แบบรายงานชุดข้อมูลเพื่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ จำนวน 9 ชุด) เพื่อให้ ธปท. มีข้อมูลเพียงพอในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของ SFIs อย่างมีประสิทธิภาพและรวดเร็วทันการณ์ สอดรับกับความเสี่ยงที่เพิ่มขึ้นจากการที่ SFIs นำระบบเทคโนโลยีสารสนเทศมาใช้เป็นกลไกในการดำเนินธุรกิจ โดยเริ่มรายงานตั้งแต่ข้อมูลงวดไตรมาสที่ 4 ปี 2563

ธปท. จึงขอนำส่งประกาศธนาคารแห่งประเทศไทย จำนวน 2 ฉบับ ลงวันที่ 26 มีนาคม 2564 ซึ่งได้ลงประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 138 ตอนพิเศษ 80 ง ลงวันที่ 9 เมษายน 2564 และแนวนโยบาย เรื่อง การรักษาความมั่นคงปลอดภัยของการใช้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ของ SFIs พร้อมทั้ง แบบรายงาน LPC และแบบรายงานชุดข้อมูลเพื่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ มาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

สุวรรณี เจษฎาศักดิ์

(นางสาวสุวรรณี เจษฎาศักดิ์)
ผู้อำนวยการอาวุโส ฝ่ายนโยบายและกำกับสถาบันการเงิน 2
ผู้ว่าการ แทน

สิ่งที่ส่งมาด้วย
1. ประกาศธนาคารแห่งประเทศไทย จำนวน 2 ฉบับ ลงวันที่ 26 มีนาคม 2564
2. แนวนโยบายธนาคารแห่งประเทศไทย เรื่องการรักษาความมั่นคงปลอดภัยของการใช้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ของสถาบันการเงินเฉพาะกิจ
3. แบบรายงานสินเชื่อเพื่อการอุปโภคบริโภคส่วนบุคคล (แบบรายงาน LPC)
4. แบบรายงานชุดข้อมูลเพื่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ จำนวน 9 ชุด

ฝ่ายนโยบายและกำกับสถาบันการเงิน 2
โทรศัพท์ 0 2356 7520 (ประกาศ RM), 0 2283 5633 (ประกาศรายงานข้อมูล), 0 2283 5827 (แนวนโยบาย Mobile banking security)
โทรสาร 0 2283 5983

แนวนโยบายธนาคารแห่งประเทศไทย
เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ของสถาบันการเงินเฉพาะกิจ

ธนาคารแห่งประเทศไทย

จัดทำโดย
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน
ธนาคารแห่งประเทศไทย
โทรศัพท์ 0-2283-6347
e-mail: ITSupervision@bot.or.th

แนวนโยบายธนาคารแห่งประเทศไทย
เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงิน
บนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security)
ของสถาบันการเงินเฉพาะกิจ

---

1. เหตุผลในการออกแนวนโยบาย

ปัจจุบันสถาบันการเงินเฉพาะกิจหลายแห่งให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่ และการใช้บริการผ่านช่องทางดังกล่าวมีปริมาณเพิ่มขึ้นอย่างรวดเร็วและขยายตัวอย่างต่อเนื่อง ขณะเดียวกันการให้บริการผ่านช่องทางดังกล่าวทำให้ต้องเผชิญกับภัยคุกคามทางไซเบอร์ (cyber threat) ที่ปัจจุบันมีความหลากหลายและซับซ้อนมากขึ้น อาจก่อให้เกิดความเสียหายต่อลูกค้าผู้ใช้บริการได้ ธนาคารแห่งประเทศไทย (ธปท.) ได้ดูแลเรื่องดังกล่าวมาอย่างต่อเนื่องโดยได้ออกแนวนโยบายว่าด้วยการเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่ (Guiding Principles for Trusted Mobile Payments) ลงวันที่ 24 มีนาคม 2560 อย่างไรก็ตาม เพื่อยกระดับความมั่นคงปลอดภัยในการให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่ให้มั่นใจว่าสามารถป้องกัน และควบคุมความเสี่ยงจากภัยคุกคามสำคัญได้อย่างรัดกุม เพียงพอตามมาตรฐานสากล ให้ประชาชนเกิดความเชื่อมั่นในการใช้บริการ ธปท. จึงได้ออกแนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) ที่ให้บริการแก่กลุ่มลูกค้ารายย่อย ซึ่งประกอบด้วยมาตรการ 2 ระดับ คือ

1. มาตรการขั้นต่ำที่จำเป็นต้องดำเนินการเพื่อความรัดกุมด้านความมั่นคงปลอดภัยในการให้บริการ

2. มาตรการเพิ่มเติมที่อาจพิจารณาดำเนินการเพื่อให้เกิดความรัดกุมปลอดภัยยิ่งขึ้น

ทั้งนี้ ธปท. คาดหวังว่าสถาบันการเงินเฉพาะกิจที่ให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ที่ให้บริการแก่กลุ่มลูกค้ารายย่อยนำแนวนโยบายนี้มาใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยที่ครอบคลุมด้านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ ด้านอุปกรณ์เคลื่อนที่ของลูกค้า ด้านระบบเครือข่ายที่เชื่อมต่อกับผู้ใช้บริการหรือผู้ให้บริการภายนอก ด้านระบบประมวลผล และด้านการวางแอปพลิเคชันบนอุปกรณ์เคลื่อนที่บนแพลตฟอร์มอิเล็กทรอนิกส์ (e-Marketplace)

2. ขอบเขตการบังคับใช้

แนวนโยบายฉบับนี้ให้ใช้บังคับกับธนาคารออมสิน ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ธนาคารอาคารสงเคราะห์ ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย บรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม และบรรษัทตลาดรองสินเชื่อที่อยู่อาศัย ที่ให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่แก่ผู้ใช้บริการกลุ่มลูกค้ารายย่อย

3. เนื้อหา

3.1 คำจำกัดความ

ในแนวนโยบายฉบับนี้

“สถาบันการเงินเฉพาะกิจ” หมายความว่า สถาบันการเงินของรัฐที่มีกฎหมายเฉพาะจัดตั้งขึ้น ได้แก่ ธนาคารออมสิน ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ธนาคารอาคารสงเคราะห์ ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย บรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม และบรรษัทตลาดรองสินเชื่อที่อยู่อาศัย

“อุปกรณ์เคลื่อนที่” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่น เพื่อรับหรือส่งข้อมูลทางการเงิน การชำระเงิน หรือคำสั่งการชำระเงินผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง

“ผู้ให้บริการ” หมายความว่า สถาบันการเงินเฉพาะกิจที่ให้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่แก่ผู้ใช้บริการกลุ่มลูกค้ารายย่อย

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการทางการเงินและการชำระเงินโดยช่องทางการให้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่กับผู้ให้บริการ

3.2 มาตรการการรักษาความมั่นคงปลอดภัย

แนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ฉบับนี้ ประกอบด้วยมาตรการ 2 ระดับ คือ 1. มาตรการขั้นต่ำ ที่จำเป็นต้องดำเนินการเพื่อความรัดกุมด้านความมั่นคงปลอดภัยในการให้บริการ และ 2. มาตรการเพิ่มเติม ที่อาจพิจารณาดำเนินการเพื่อให้เกิดความรัดกุมปลอดภัยยิ่งขึ้น ดังนี้

1. มาตรการขั้นต่ำ เป็นมาตรการที่ป้องกันความเสี่ยงจากภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อผู้ใช้บริการและความเชื่อมั่นในวงกว้าง โดยผู้ให้บริการต้องดำเนินการปรับปรุงการรักษาความมั่นคงปลอดภัยของแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ให้เป็นไปตามมาตรการขั้นต่ำ ดังนี้

ด้านระบบ

(1) ไม่อนุญาตให้ใช้อุปกรณ์เคลื่อนที่ที่เปิดสิทธิ์ให้เข้าถึงระบบปฏิบัติการ (rooted/jailbroken) เข้าใช้งานแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลสำคัญของผู้ใช้บริการ และละเมิดหรือหลีกเลี่ยง มาตรการการรักษาความมั่นคงปลอดภัยที่ผู้ให้บริการกำหนดไว้

(2) ไม่อนุญาตให้อุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการล้าสมัย (obsolete Operating System : OS) ที่มีช่องโหว่ร้ายแรงที่ประกาศจากหน่วยงานด้านความมั่นคงปลอดภัยที่เป็นสากลและกระทบการใช้งานของผู้ใช้บริการในวงกว้างเข้าใช้งานแอปพลิเคชัน ทั้งนี้ ในกรณีที่ obsolete OS มีช่องโหว่อื่นที่ไม่กระทบผู้ใช้บริการในวงกว้าง ควรมีมาตรการรองรับเพื่อลดความเสี่ยงของผู้ให้บริการและผู้ใช้บริการตามความเหมาะสม เช่น การแจ้งเตือนผู้ใช้บริการ การจำกัดวงเงินธุรกรรม และการเพิ่มมาตรการยืนยันตัวตน

(3) ขอสิทธิ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสิทธิ์ดังกล่าวอย่างเป็นประจำ เพื่อป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของผู้ใช้บริการ

(4) ป้องกัน source code ส่วนสำคัญ เช่น การโอนเงิน การพิสูจน์ตัวตน ไม่ให้รั่วไหลจากแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีทำการแก้ไข เปลี่ยนแปลง source code ดังกล่าว

(5) ป้องกันการฝังข้อมูลสำคัญ หรือ code ที่ไม่พึงประสงค์ (malicious code) บนแอปพลิเคชัน

(6) เข้ารหัสไฟล์ข้อมูล (files encryption) ที่จัดเก็บข้อมูลสำคัญบนอุปกรณ์เคลื่อนที่ของผู้ใช้บริการ เพื่อป้องกันข้อมูลสำคัญของผู้ใช้บริการรั่วไหล

(7) ไม่อนุญาตให้ผู้ใช้บริการใช้แอปพลิเคชันเวอร์ชั่นต่ำกว่าที่ผู้ให้บริการกำหนด เพื่อให้แอปพลิเคชันมีการรักษาความมั่นคงปลอดภัยเป็นไปตามมาตรฐานของผู้ให้บริการ

(8) ป้องกันการโจมตีในลักษณะ Distributed denial-of-service (DDoS Attack) ในระดับเครือข่าย (network layer) เพื่อป้องกันระบบจากการถูกโจมตีจนไม่สามารถให้บริการได้

(9) ป้องกันภัยจากการถูกดักจับหรือแก้ไขเปลี่ยนแปลงข้อมูลระหว่างการรับส่ง (Man in the Middle Attack) โดยยืนยันตัวตนด้วยเทคนิค Certificate Pinning หรือวิธีอื่นที่เทียบเท่า และการใช้ช่องทางสื่อสารที่ปลอดภัย (secure protocol) ในการรับส่งข้อมูล

(10) ป้องกันการสวมรอยการเข้าใช้งานของลูกค้า (Session Hijacking)

(11) ป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (server) โดยไม่ได้รับอนุญาต เช่น การเข้าถึงโดยอาศัยวิธี SQL Injection, Local File Inclusion หรือ Directory Traversal เพื่อลดความเสี่ยงจากข้อมูลรั่วไหลและระบบถูกโจมตี

(12) ตรวจสอบและรับมือแอปพลิเคชันปลอมบนแพลตฟอร์มอิเล็กทรอนิกส์ที่เป็นที่ยอมรับและน่าเชื่อถือ (official e-Marketplace) เช่น Google Play Store, App Store เพื่อลดความเสี่ยงจากการที่ลูกค้า download และติดตั้งแอปพลิเคชันปลอม

ด้านการดูแลลูกค้าผู้ใช้บริการ

(1) ผู้ให้บริการต้องจัดให้มีการเสริมสร้างความรู้ความเข้าใจการใช้บริการเทคโนโลยีทางการเงินให้แก่ประชาชน ทั้งความรู้เกี่ยวกับภัยคุกคามใหม่ ๆ และวิธีการปฏิบัติตนให้ปลอดภัยในการใช้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ในเชิงรุกและต่อเนื่อง

(2) จัดให้มีแนวปฏิบัติการให้บริการลูกค้าในการใช้บริการทางการเงินและการชำระเงินผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่แก่พนักงานของสถาบันการเงินเฉพาะกิจ และดูแลให้พนักงานถือปฏิบัติอย่างรัดกุมเข้มงวด และระมัดระวังไม่ดำเนินการในลักษณะที่ก่อให้เกิดความเสี่ยง เช่น กรณีพนักงานสาขาหรือตัวแทนของสถาบันการเงินเฉพาะกิจติดตั้งแอปพลิเคชันให้ลูกค้า ควรดำเนินการเท่าที่จำเป็น ไม่เข้าถึงข้อมูลสำคัญของลูกค้า และไม่ใส่รหัสผ่านแทนลูกค้า เป็นต้น ซึ่งอาจนำไปสู่การก่อทุจริตได้

2. มาตรการเพิ่มเติม เพื่อให้การให้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่มีการรักษาความมั่นคงปลอดภัยเข้มแข็งมากยิ่งขึ้น ผู้ให้บริการควรพิจารณาดำเนินการเพิ่มเติม ดังนี้

(1) ตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชัน เมื่อผู้ใช้บริการเข้าใช้งานในทันที (Anti-Tampering) เพื่อป้องกันไม่ให้ข้อมูลผู้ใช้บริการรั่วไหลหรือเกิดความเสียหายจากแอปพลิเคชันที่มีการดัดแปลงแก้ไขโดยฝัง malicious code ไว้

(2) กำหนดให้ตั้งค่า PIN หรือ รหัสผ่านที่ซับซ้อน (PIN / password complexity) ในการเข้าใช้งานแอปพลิเคชันเพื่อให้ยากต่อการคาดเดา

(3) แสดงผลข้อมูลผู้ใช้บริการบนแอปพลิเคชันอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของลูกค้า (sensitive data masking) การปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application Blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้บริการจะรั่วไหล

(4) ป้องกันภัยคุกคามในระดับแอปพลิเคชัน (application layer) เช่น การเข้ารหัสข้อมูลสำคัญระหว่างรับ/ส่ง การป้องกัน DDOS Attack เพื่อยกระดับการป้องกันข้อมูลรั่วไหลระหว่างรับ/ส่ง หรือป้องกันระบบถูกโจมตีจนไม่สามารถให้บริการได้

(5) ตรวจสอบและรับมือแอปพลิเคชันปลอมบน website อื่น นอกเหนือจากแพลตฟอร์มอิเล็กทรอนิกส์ที่เป็นที่ยอมรับและน่าเชื่อถือ (official e-Marketplace) เช่น บน darkweb เป็นต้น

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 6347
Email : ITSupervision@bot.or.th