เจตคติต่อกลไกปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ISO/IEC 29100 และ ISO/IEC 27701[1]

มนัสนิตย์ เศรษฐาวงศ์[2] และ วศิณ ชูประยูร[3]

Received 07/09/2022 Revised 01/12/2022 Accepted 18/12/2022

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา 1) เจตคติต่อกลไกปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ 2) อิทธิพลของคุณลักษณะของผู้ใช้ต่อเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคล 3) อิทธิพลของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลต่อความเป็นส่วนตัวและความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชัน 4) อิทธิพลของความมั่นคงปลอดภัยสารสนเทศและความเป็นส่วนตัวของแอปพลิเคชันต่อความไว้วางใจของผู้ใช้ 5) อิทธิพลของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลต่อความไว้วางใจของผู้ใช้ และ 6) พัฒนาแบบจำลองอิทธิพลตามข้อค้นพบของวัตถุประสงค์ข้อ 3-5 การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ ใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ISO/IEC 29100 และ ISO/IEC 27701 เป็นทฤษฎีหลักเพื่อออกแบบการวิจัย (Personal Data Protection Act, B.E. 2562 (2019), 2019; ISO/IEC, 2011; ISO/IEC, 2019) ใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างที่เป็นผู้ใช้แอปพลิเคชันจำนวน 384 คน ได้รับแบบสอบถามกลับคืนร้อยละ 100 สถิติที่ใช้สำหรับการวิเคราะห์ข้อมูล ได้แก่ สถิติเชิงพรรณนา (ร้อยละ ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน) และ การวิเคราะห์การถดถอยเชิงเส้นแบบพหุ ผลการวิจัยพบว่า ผู้ใช้มากกว่าร้อยละ 80 มีความเห็นว่าแอปพลิเคชันที่ตนเองใช้มีกลไกปกป้องข้อมูลส่วนบุคคลที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562, ISO/IEC 29100 และ ISO/IEC 27701 ผลการทดสอบสมมติฐานพบว่า คุณลักษณะของผู้ใช้มีอิทธิพลต่อเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลที่ขนาดอิทธิพล (R^2) ระหว่าง 0.50 - 0.17 ทำให้ได้สมการอิทธิพล จำนวน 33 สมการ เจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลต่อความเป็นส่วนตัวและความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชันที่ขนาดอิทธิพล (R^2) ระหว่าง 0.08 - 0.31 ทำให้ได้สมการอิทธิพล จำนวน 8 สมการ ความมั่นคงปลอดภัยสารสนเทศและความเป็นส่วนตัวของแอปพลิเคชันมีอิทธิพลต่อความไว้วางใจของผู้ใช้ที่ขนาดอิทธิพล (R^2) ระหว่าง 0.17 - 0.36 ทำให้ได้สมการอิทธิพล จำนวน 8 สมการ เจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลต่อความไว้วางใจของผู้ใช้ที่ขนาดอิทธิพล (R^2) ระหว่าง 0.25 - 0.29 ทำให้ได้สมการอิทธิพล จำนวน 4 สมการ

คำสำคัญ: ข้อมูลส่วนบุคคล, การคุ้มครองข้อมูลส่วนบุคคล, ความเป็นส่วนตัว, ความไว้วางใจ

---

[1] บทความนี้เป็นส่วนหนึ่งของวิทยานิพนธ์ เรื่อง เจตคติต่อกลไกปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ISO/IEC 29100 และ ISO/IEC 27701

[2] วท.บ. (วิทยาการคอมพิวเตอร์), นักศึกษาหลักสูตร วท.ม. (การจัดการเทคโนโลยีสารสนเทศ) วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต, E-mail: manaznitz@gmail.com

[3] Ph.D. (Information Technology), ผู้ช่วยศาสตราจารย์, ผู้อำนวยการหลักสูตร วท.ม. (การจัดการเทคโนโลยีสารสนเทศ) วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต, E-mail: vasin@rsu.ac.th

The Position of Mobile Financial Service Application Users on Personal Data Protection Mechanisms Established by the Personal Data Protection Act B.E. 2562 (2019), ISO/IEC 29100, and ISO/IEC 27701[1]

Manasnit Setthawong[2] and Vasin Chooprayoon[3]

Received 07/09/2022 Revised 01/12/2022 Accepted 18/12/2022

Abstract

The objectives of this research were: 1) to ascertain the position of mobile financial service application users toward personal data protection guidelines set in accordance with the Personal Data Protection Act B.E. 2562 (2019), ISO/IEC 29100, and ISO/IEC 27701; 2) to investigate the association between users' characteristics and their attitudes as it pertains to privacy protection techniques used by mobile financial service applications; 3) to examine the relationship between users' attitudes regarding personal data protection mechanisms in mobile financial service applications and applicable privacy and information security standards; 4) to determine the relationship between information security and applications' privacy guidelines and users' trust; and 5) to explore the relationship between users' attitudes toward personal data protection mechanisms in mobile financial service applications and their trust in such applications; and (6) to develop a model relating to personal data protection measures in mobile financial service applications, users' characteristics, information security, as well as applications' privacy and users' trust. The study approach was quantitative in nature and utilized Thailand's Data Protection Act B.E. 2562 (2019), ISO/IEC 29100, and ISO/IEC 27701 as a framework for the purposes of its investigation. Questionnaires served as a research tool for data collection from 384 application users. The response rate was 100%. Descriptive statistics (percentage, mean, and standard deviation) and multiple linear regression analysis were employed to analyze the data. In terms of the test of hypothesis, it was discovered that users' characteristics had an effect on their perceptions regarding personal data security procedures used by mobile financial service applications (R2=0.05 - 0.31). This has led to the formulation of 33 influence equations. The study also revealed that users' attitudes regarding personal data protection systems impacted their attitudes toward applications' information security and privacy (R2 values ranging from 0.08 to 0.31), resulting in eight impact equations. Users' attitudes concerning application data security and privacy also affected their trust (R2 values ranging from 0.17 to 0.36), resulting in eight influence equations. Finally, users' positions on personal data protection procedures used by mobile financial service applications affected their trust (R2 values ranging from 0.25 to 0.29), resulting in four influence equations.

Keywords: Personal Data, Personal Data Protection, Data Privacy, Trust

---

[1]This article is part of a thesis titled "The Attitude on Personal Data Protection Mechanisms of Mobile Financial Service Application Users According to the Personal Data Protection Act B.E. 2562 (2019), ISO/IEC 29100, and ISO/IEC 27701"

[2] B.Sc (Computer Science), Student of M.S. (Information Technology Management), College of Digital Innovation Technology, Rangsit University. E-mail: manaznitz@gmail.com

3Ph.D. (Information Technology), Assistant Professor, Director of M.S. (Information Technology Management), College of Digital Innovation Technology, Rangsit University. E-mail: vasin@rsu.ac.th

บทนำ

ปัจจุบันผู้บริโภคจำนวนมากได้หันมาใช้บริการต่าง ๆ บนระบบอินเทอร์เน็ต บริการเหล่านี้มีการเก็บรวบรวม ใช้ และประมวลผลข้อมูลส่วนตัวของผู้ใช้ทั้งแบบที่ผู้ใช้ตั้งใจหรือไม่ตั้งใจให้ข้อมูล ก่อให้เกิดความเสี่ยงในการละเมิดสิทธิความเป็นส่วนตัวเพิ่มมากขึ้น เช่น การเก็บรวบรวมข้อมูลที่มีเนื้อหาไม่ถูกต้องทำให้เกิดความผิดพลาดตามมา การใช้ข้อมูลที่เก็บมาเพื่อวัตถุประสงค์หนึ่งแต่ข้อมูลนั้นถูกนำไปใช้เพื่อวัตถุประสงค์อื่นโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล การโอนข้อมูลระหว่างกันโดยไม่มีอำนาจหรือกระทำอย่างไม่เหมาะสมระหว่างองค์กร เป็นต้น (The World Bank, 2016) โดยเฉพาะเมื่อมีการเก็บรวบรวมข้อมูลจำนวนมหาศาล (Big Data) เพื่อนำมาใช้ประมวลผลและวิเคราะห์เพื่อคาดการณ์ประเมินหาประเด็นเกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลในด้านต่าง ๆ เพื่อทำความเข้าใจพฤติกรรมและความชอบส่วนบุคคลของผู้บริโภคบนโลกออนไลน์ (Profiling) และนำไปใช้เพื่อแข่งขันทางการตลาด (Fife & Orjuela, 2012; Chang, Wong, Libaque-Saenz & Lee, 2018) โดยที่เจ้าของข้อมูลไม่รู้ตัวหรือไม่ยินยอมให้ใช้ข้อมูลเหล่านั้น รายงานของ Privacy International (2018) และ Wagner (2018) พบว่า แอปพลิเคชันบนโทรศัพท์มือถือส่งข้อมูลไปยังเฟซบุ๊กโดยอัตโนมัติทันทีเมื่อผู้ใช้เปิดแอปพลิเคชันแม้ว่าผู้ใช้จะไม่มีบัญชีเฟซบุ๊กก็ตาม ในบริบทของบริการทางการเงินและการชำระเงินออนไลน์ มีการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างลูกค้าและธนาคาร เช่น ตัวตนของลูกค้า สถานะของบัญชี การโอนเงินและการชำระเงิน ฯลฯ ข้อมูลที่อ่อนไหวเหล่านี้อาจสร้างความกังวลให้กับลูกค้าต่อภัยคุกคามที่อาจเกิดขึ้น เนื่องจากธุรกิจธนาคารมีระเบียบข้อบังคับที่เข้มงวด การรั่วไหลของข้อมูลในโลกออนไลน์จึงเป็นปัญหาร้ายแรงสำหรับธนาคาร ดังนั้นการที่ลูกค้าต้องประเมินว่าธนาคารมีการจัดการกับข้อมูลของพวกเขาอย่างไรจึงเป็นเรื่องที่สำคัญยิ่ง (Chang et al., 2018) จากรายงานของ IBM Security (2019) พบว่าความเสียหายที่เกิดจากการละเมิดข้อมูลในธุรกิจประเภทการธนาคารและการเงินมีมูลค่าสูงถึง 5.86 ล้านดอลลาร์สหรัฐต่อปี ตัวอย่างเหล่านี้แสดงให้เห็นว่าในยุคแห่งการสื่อสารแบบดิจิทัลที่มีความรวดเร็วทำให้การละเมิดข้อมูลส่วนบุคคลสามารถทำได้ง่ายและรวดเร็ว ซึ่งสร้างความกังวลให้กับผู้ใช้และรัฐบาลทั่วโลก ทั้งยังส่งผลกระทบต่อความเชื่อมั่นในการพัฒนาเศรษฐกิจและสังคมดิจิทัล เพราะหากมีการรั่วไหลของข้อมูลออกไป องค์กรที่เป็นผู้เก็บรวบรวมข้อมูลอาจเสียชื่อเสียง สูญเสียความน่าเชื่อถือ และในระยะยาวจะไม่สามารถเรียกความเชื่อมั่นและความไว้วางใจจากลูกค้าให้คืนกลับมาได้ (Chang et al., 2018) ส่งผลให้องค์กรสูญเสียความสามารถในการแข่งขันทางธุรกิจตามมา การปกป้องข้อมูลส่วนบุคคลและการปฏิบัติด้านความปลอดภัยที่ไม่มีประสิทธิภาพเกิดจากการขาดความตระหนัก ความรู้ หรือความเข้าใจเกี่ยวกับวิธีการพัฒนาแอปพลิเคชัน ให้เป็นไปตามข้อกำหนดของกฎหมาย (European Union Agency for Network and Information Security [ENISA], 2017) ดังนั้น ผู้วิจัยจึงสนใจที่จะศึกษาเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ (Mobile Financial Service: MFS) หลังการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเทศไทย เพื่อนำเจตคติจากการศึกษาดังกล่าวมาช่วยให้ผู้พัฒนาซอฟต์แวร์สามารถออกแบบและสร้างกลไกการปกป้องข้อมูลส่วนบุคคลที่มีประสิทธิภาพสามารถปกป้องข้อมูลส่วนบุคคลจากการใช้ผิดวัตถุประสงค์ การใช้ไม่เหมาะสม การเข้าถึงที่ไม่ได้รับอนุญาต การดัดแปลง แก้ไข การทำให้สูญหาย และ การเปิดเผยข้อมูลโดยไม่ตั้งใจ และรวมไปถึงการขออนุญาตเจ้าของ

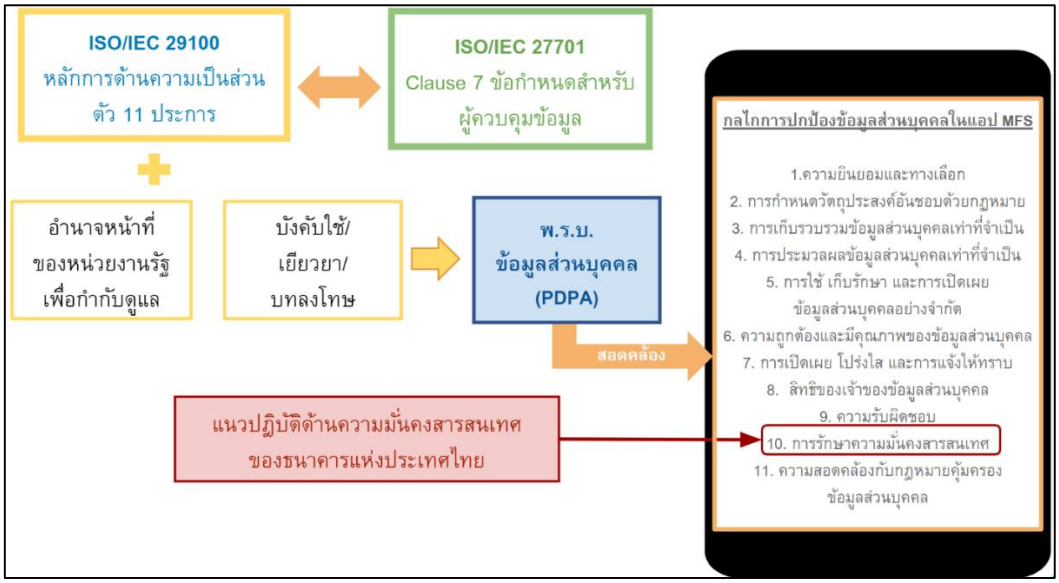
ข้อมูลก่อนนำข้อมูลเหล่านั้นไปใช้เพื่อทำการตลาดหรือนำไปใช้เพื่อวิเคราะห์ข้อมูลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และสามารถสร้างความเชื่อมั่นให้กับผู้ใช้ ซึ่งช่วยเพิ่มศักยภาพให้กับการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ในประเทศไทยสามารถก้าวไปสู่เศรษฐกิจดิจิทัลที่มีคุณภาพและช่วยขับเคลื่อนการพัฒนาประเทศได้อย่างมีประสิทธิภาพและมั่นคง

วัตถุประสงค์การวิจัย การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา

1. เจตคติต่อกลไกปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพุทธศักราช 2562 ISO/IEC 29100 และ ISO/IEC 27701
2. อิทธิพลของคุณลักษณะของผู้ใช้ต่อเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลในแอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่
3. อิทธิพลของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลต่อความเป็นส่วนตัวและความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่
4. อิทธิพลของความมั่นคงปลอดภัยสารสนเทศและความเป็นส่วนตัวของแอปพลิเคชันต่อความไว้วางใจของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่
5. อิทธิพลของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลต่อความไว้วางใจของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่
6. พัฒนาแบบจำลองอิทธิพลตามข้อค้นพบของวัตถุประสงค์ข้อ 3-5

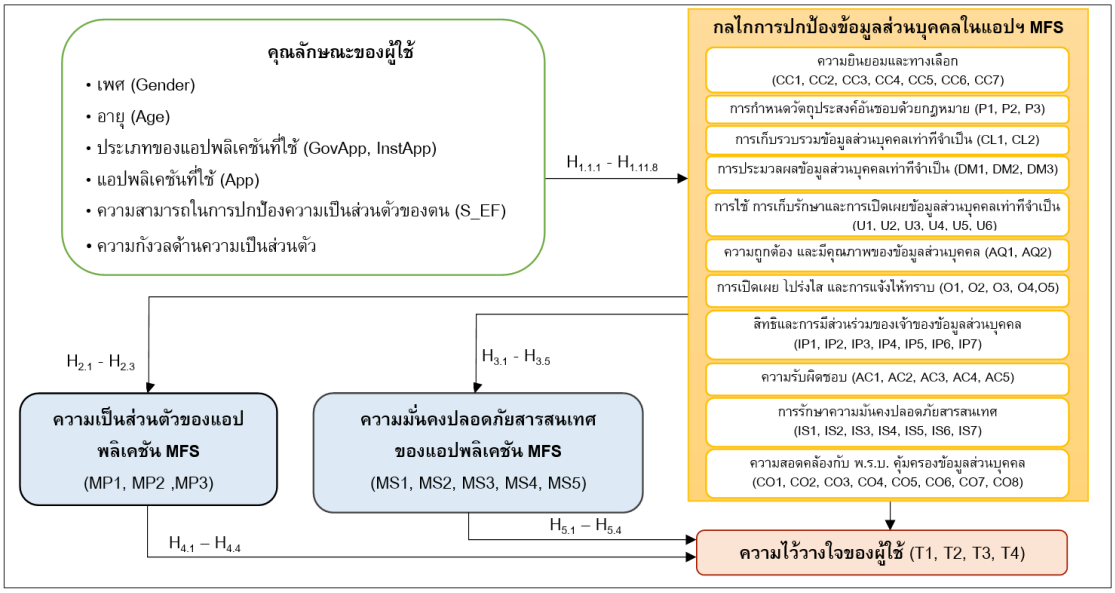
วิธีดำเนินการวิจัย

1. กรอบการวิจัย



รูปที่ 1 ขอบเขตด้านแนวคิดและทฤษฎีที่เป็นพื้นฐานของงานวิจัย

ผู้วิจัยได้พัฒนากรอบแนวคิดการวิจัยด้วยการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องกับ ISO/IEC 29100 ISO/IEC 27701 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลักของธนาคารแห่งประเทศไทย (Bank of Thailand, 2014) และศึกษาถึงกลไกการปกป้องข้อมูลส่วนบุคคลของแอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ ดังรูปที่ 1 เพื่อนำมาสังเคราะห์ตัวแปรการวิจัยจนได้กรอบการวิจัยดังรูปที่ 2



รูปที่ 2 กรอบการวิจัย

2. สมมติฐานการวิจัย

ประกอบด้วยสมมติฐานทั้งสิ้น 75 สมมติฐาน โดยจำแนกเป็น 6 กลุ่มสมมติฐานหลัก ดังนี้

สมมติฐานหลักกลุ่มที่ 1 คุณลักษณะของผู้ใช้ มีอิทธิพลต่อเจตคติของผู้ใช้ต่อกลไกการปกป้องข้อมูลส่วนบุคคลในแอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ ประกอบด้วย 55 สมมติฐานย่อย สมมติฐานหลักกลุ่มที่ 2 กลไกการปกป้องข้อมูลส่วนบุคคลในแอปพลิเคชันมีอิทธิพลต่อเจตคติด้านความเป็นส่วนตัวของผู้ใช้แอปพลิเคชัน ประกอบด้วย 3 สมมติฐานย่อย โดยตัวแปรในกลุ่มสมมติฐานที่ 1 2 และ 3 ผู้วิจัยประยุกต์มาจากศึกษาของ Fife & Orjuela (2012) ที่ศึกษาถึงความสัมพันธ์ระหว่างความกังวลเกี่ยวกับความเป็นส่วนตัวกับการใช้บริการข้อมูลบนอุปกรณ์เคลื่อนที่ที่มีความอ่อนไหวในด้านความเป็นส่วนตัวและความปลอดภัย โดยเฉพาะอย่างยิ่งแอปพลิเคชันเครือข่ายสังคมออนไลน์ การธนาคาร/การชำระเงิน และกิจกรรมด้านสุขภาพ โดยมีกลุ่มตัวอย่างเป็นผู้ใช้สมาร์ตโฟนในสหรัฐอเมริกาและญี่ปุ่น และงานวิจัยของ Chang et al. (2018) ที่ศึกษาถึงความสัมพันธ์ระหว่างความกังวลด้านความเป็นส่วนตัวของลูกค้าธนาคารออนไลน์กับนโยบายความเป็นส่วนตัวขององค์กร และงานของ Pinto (2018) ที่ศึกษาถึงทัศนคติและความตระหนักรู้ของคนรุ่นมิลเลนเนียลที่มีต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคล สมมติฐานหลักกลุ่มที่ 3 กลไกการปกป้องข้อมูล

ส่วนบุคคลในแอปพลิเคชัน มีอิทธิพลต่อเจตคติด้านความมั่นคงปลอดภัยสารสนเทศของผู้ใช้แอปพลิเคชัน ประกอบด้วย 5 สมมติฐานย่อย สมมติฐานหลักกลุ่มที่ 4 เจตคติต่อความเป็นส่วนตัวของแอปพลิเคชัน มีอิทธิพลต่อความไว้วางใจของผู้ใช้ ประกอบด้วย 4 สมมติฐานย่อย สมมติฐานหลักกลุ่มที่ 5 เจตคติต่อความมั่นคงปลอดภัยสารสนเทศของผู้ใช้แอปพลิเคชัน มีอิทธิพลต่อความไว้วางใจของผู้ใช้ ประกอบด้วย 4 สมมติฐานย่อย สมมติฐานหลักกลุ่มที่ 6 กลไกการปกป้องข้อมูลส่วนบุคคลในแอปพลิเคชันมีอิทธิพลต่อความไว้วางใจของผู้ใช้ ประกอบด้วย 4 สมมติฐานย่อย ตัวแปรในสมมติฐานกลุ่มที่ 3 4 5 และ 6 ประยุกต์มาจากการทบทวนวรรณกรรมของ Johnson, Kiser, Washington, & Torres (2017) ที่ศึกษาปัจจัยด้านความมั่นคงปลอดภัยสารสนเทศ และความเสี่ยงด้านความเป็นส่วนตัวที่มีอิทธิพลต่อการยอมรับนวัตกรรมบริการการชำระเงินบนอุปกรณ์เคลื่อนที่ และงานวิจัยของ Balapour, Nikkhah & Sabherwal (2020) ที่ศึกษาถึงอิทธิพลของความเป็นส่วนตัวของข้อมูลต่อการรับรู้ด้านความมั่นคงปลอดภัยของข้อมูลที่มีต่อพฤติกรรมและทัศนคติของผู้ใช้ และงานวิจัยของ Peikari, Ramayah, Shah, & Lo (2018) ที่ศึกษาถึงความไว้วางใจของคนไข้ที่มีต่อการรักษาความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล

3. การกำหนดประชากรและกลุ่มตัวอย่าง

ประชากรสำหรับการวิจัยครั้งนี้ คือ ผู้ใช้บริการแอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ที่มีการเปิดใช้บริการแอปพลิเคชันของผู้ให้บริการทั้งที่เป็นสถาบันการเงินและผู้ให้บริการที่มิใช่สถาบันการเงินในประเทศไทย ซึ่งมีจำนวนประมาณ 157 ล้านบัญชี (Bank of Thailand, 2020) โดยต้องดาวน์โหลดแอปพลิเคชันมาจากช่องทางที่เป็นทางการ (Official Store) เท่านั้น สำหรับงานวิจัยนี้มีประชากรจำนวนมากและไม่สามารถนับจำนวนประชากรได้แน่นอน ผู้วิจัยจึงกำหนดขนาดของกลุ่มตัวอย่างโดยใช้สูตรคำนวณของคอแครน (Cochran, 1977) โดยกำหนดระดับค่าความเชื่อมั่นที่ 95% และค่าความคลาดเคลื่อนไม่เกิน 5% ได้ขนาดตัวอย่าง 384 คน วิธีการคัดเลือกตัวอย่างเป็นการสุ่มแบบแบ่งชั้นภูมิ (Stratified Random Sampling) โดยแบ่งตามเพศ อายุ และประเภทของแอปพลิเคชันที่ใช้ สุ่มให้ได้จำนวนตัวอย่างจากแต่ละกลุ่มจำนวนใกล้เคียงกัน

4. เครื่องมือที่ใช้ในการวิจัย

ผู้วิจัยได้พัฒนาเครื่องมือวิจัยตามกรอบแนวคิดของการวิจัย ด้วยการนำวัตถุประสงค์ของการวิจัยมาขยายความเพื่อหาตัวชี้วัด ซึ่งนำไปสู่การตั้งคำถามในแบบสอบถาม ได้แบบสอบถามแบ่งเป็น 5 ตอน จำนวนข้อคำถามทั้งหมด 82 ข้อ ดังนี้ ตอนที่ 1 คุณลักษณะของผู้ใช้แอปพลิเคชัน MFS (15 ข้อ) ตอนที่ 2 ปัจจัยด้านกลไกการปกป้องข้อมูลส่วนบุคคลในแอปพลิเคชัน MFS (55 ข้อ) ตอนที่ 3 ปัจจัยด้านความเป็นส่วนตัวของข้อมูลส่วนบุคคลของแอปพลิเคชัน MFS (3 ข้อ) ตอนที่ 4 ปัจจัยด้านความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชัน MSF (5 ข้อ) ตอนที่ 5 ปัจจัยด้านความไว้วางใจของผู้ใช้ที่มีต่อแอปพลิเคชัน MFS (4 ข้อ) เมื่องานวิจัยนี้ได้ผ่านการพิจารณารับรองจากคณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิตเป็นที่เรียบร้อยแล้ว

ผู้วิจัยจึงตรวจสอบคุณภาพเครื่องมือการวิจัย โดยผู้ทรงคุณวุฒิจำนวน 5 ท่าน[1] โดยตรวจสอบความเที่ยงทั้งในเชิงโครงสร้างและเนื้อหา จากนั้นผู้วิจัยได้นำผลจากการตรวจของผู้ทรงคุณวุฒิไปคำนวณหาค่าดัชนีความเที่ยงตรงเชิงเนื้อหา (Content Validity Index : CVI) ได้ค่าเท่ากับ 0.932 ซึ่งมีค่ามากกว่า 0.8 แบบสอบถามนี้จึงมีความสอดคล้องเชิงเนื้อหาทั้งฉบับจึงสามารถนำไปเก็บข้อมูลได้ จากนั้นผู้วิจัยได้นำเครื่องมือที่ปรับปรุงแก้ไขจากข้อเสนอแนะของผู้ทรงคุณวุฒิไปทดลองใช้กับกลุ่มตัวอย่าง 30 ตัวอย่าง และได้นำคำตอบจากกลุ่มตัวอย่างดังกล่าวไปทดสอบความเชื่อน่าเชื่อถือโดยใช้สูตรคำนวณค่าสัมประสิทธิ์อัลฟา (α) ของครอนบัค (Cronbach, 1951) ได้ค่า α เท่ากับ 0.931 ซึ่งมีค่ามากกว่า 0.7 ถือว่าข้อคำถามนั้นมีความเชื่อมั่น และตัดข้อคำถามที่มี α ต่ำกว่า 0.7 ออก จึงได้แบบสอบถามที่มีคุณภาพและนำไปเก็บข้อมูลต่อไป โดยการเผยแพร่แบบสอบถามผ่านสื่อสังคมออนไลน์ต่าง ๆ เช่น เว็บไซต์พันทิป เฟสบุ๊ก ไลน์ เป็นต้น ระยะเวลาการเผยแพร่แบบสอบถามออนไลน์ตั้งแต่เมษายน – สิงหาคม 2564 และเนื่องจากช่วงเก็บข้อมูลเป็นระยะการแพร่ระบาดของโควิด-19 จึงไม่สามารถเก็บตัวอย่างทางภาคสนามได้

5. การวิเคราะห์ข้อมูล สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่

1. สถิติเชิงพรรณนา ประกอบด้วย สถิติคำนวณค่าร้อยละ ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน เพื่อพรรณนาภูมิหลังของผู้ตอบแบบสอบถาม และ เจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

2. สถิติอ้างอิง ได้แก่ การวิเคราะห์การถดถอยเชิงเส้นแบบพหุ (Multiple Linear Regression) เพื่อทดสอบสมมติฐาน ประกอบด้วยขั้นตอนวิธีดังนี้ (1) ตรวจสอบความสัมพันธ์ภายในของข้อมูล (Autocorrelation) โดยพิจารณาค่า Durbin – Watson (2) ตรวจสอบสภาวะร่วมของตัวแปรอิสระ (Multicollinearity) (3) ตรวจสอบความคลาดเคลื่อนที่เกิดจากการพยากรณ์ โดยพิจารณาจากค่าสูงสุดและค่าต่ำสุดของค่า ZResidual ที่อยู่ระหว่าง ±3 (4) ตรวจสอบการแจกแจงของความคลาดเคลื่อนที่เกิดจากการพยากรณ์ และตรวจสอบความแปรปรวนของความคลาดเคลื่อนโดยพิจารณาความเท่ากันของการกระจายของค่า ZResidual เหนือและใต้ระดับ 0 และ (5) ตรวจสอบความสัมพันธ์เชิงเส้นระหว่างตัวแปรอิสระและตัวแปรตามของสมมติฐานทั้งหมดด้วยการวิเคราะห์ความแปรปรวนทางเดียว (One – Way ANOVA)

---

[1] รายชื่อผู้ทรงคุณวุฒิจำนวน 5 ท่าน ดังนี้

1. ผศ. อัจจิมา มั่นทน รองผู้อำนวยการสำนักส่งเสริมการเรียนรู้และบริการวิชาการ มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์
2. อิทธิชัย ฉ่ำรักษ์สินธุ์ หัวหน้าฝ่ายการประกันคุณภาพซอฟต์แวร์, เอสซีบีดิจิทัล ธนาคารไทยพาณิชย์ สำนักงานใหญ่
3. ณัฐ พยงค์ศรี นักวิชาการคอมพิวเตอร์ชำนาญการกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ ปฏิบัติหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
4. ผศ.ดร. วุฒิพงษ์ ชินศรี ผู้อำนวยการหลักสูตรการจัดการความมั่นคงไซเบอร์ และผู้อำนวยการสำนักนวัตกรรมวิสาหกิจดิจิทัล มหาวิทยาลัยรังสิต
5. ดร. วรทรรศน์ มาฆะศิรานนท์ ตำแหน่งอาจารย์ประจำมหาวิทยาลัยรังสิต คณะนวัตกรรมเทคโนโลยีดิจิทัล มหาวิทยาลัยรังสิต และผู้พิพากษาสมทบในศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลาง

ผลการวิจัย

ผู้วิจัยรายงานผลตามแนววัตถุประสงค์ของการวิจัย จำแนกเป็น 6 กลุ่มข้อค้นพบ ดังนี้

1. เจตคติต่อกลไกปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562, ISO/IEC 29100 และ ISO/IEC 27701 ผลการวิจัยพบว่า

1.1 มีผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ เพื่อใช้สวัสดิการของรัฐและแอปพลิเคชันของสถาบันการเงินมากถึงร้อยละ 88.80 แอปพลิเคชันของสถาบันการเงินเพียงอย่างเดียว ร้อยละ 11.20 และไม่มีผู้ใช้ที่ใช้แอปพลิเคชันเพื่อใช้สวัสดิการของรัฐเพียงอย่างเดียว ทั้งนี้มีผู้ใช้แอปพลิเคชัน “เป๋าตังค์” มีจำนวนมากที่สุด รองลงมาได้แก่ Bualuang mBanking, กรุงไทย NEXT และ K Plus, True Money Wallet และ SCB Easy ตามลำดับ ผู้ตอบแบบสอบถามที่เป็นเพศชายทั้งหมด 192 คน คิดเป็นร้อยละ 46.6 และเป็นเพศหญิงทั้งหมด 208 คน คิดเป็นร้อยละ 53.4 โดยผู้ที่มีอายุน้อยกว่า 20 ปี ที่เป็นเพศชาย 10 คน เพศหญิง 11 คน อายุ 20-30 ปี เป็นชาย 56 คน หญิง 62 คน อายุ 41-50 ปี เป็นชาย 37 คน หญิง 52 คน อายุ 51-60 ปี เป็นชาย 15 คน หญิง 12 คน และอายุ 61 ปีขึ้นไป เป็นชาย 2 คน และ หญิง 11 คน

1.2 ผู้ตอบแบบสอบถามส่วนใหญ่มีความเชื่อมั่นในระดับสูง (3.91, 1.07)[1] ว่าตนเองสามารถควบคุมและจัดการข้อมูลส่วนบุคคลของตนเองได้ แต่ผู้ใช้ส่วนใหญ่มีความกังวลด้านความเป็นส่วนตัวมาก (3.99, 1.03) โดยผู้ใช้มีความกังวลมากที่สุดในด้านข้อมูลส่วนตัวหรือข้อมูลทางการเงินอาจรั่วไหล (4.05, 0.83) รองลงมาคือความกังวลมากว่าข้อมูลส่วนบุคคลที่แอปพลิเคชันเก็บรวบรวมไว้จะถูกละเมิด ไม่ว่าจะเป็นการนำไปใช้โดยไม่ได้รับอนุญาต หรือ การเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต นอกจากนี้ผู้ใช้ส่วนใหญ่มีความกังวลมากด้านความมั่นคงปลอดภัยสารสนเทศว่าข้อมูลทางการเงินอาจรั่วไหล (3.90, 0.87) และอาจสูญเสียเงินหากมีเหตุการณ์ผิดปกติในระหว่างทำธุรกรรม (3.95, 0.81)

1.3 เจตคติต่อกลไกปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชัน ผลการวิจัยพบว่า ผู้ใช้มีความเห็นว่าแอปพลิเคชันที่ตนเองใช้มีกลไกปกป้องข้อมูลส่วนบุคคลที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ISO/IEC 29100 และ ISO/IEC 27701 ในด้านการขอความยินยอมและให้ทางเลือก (Consent and Choice) ด้วยการทำเป็นหนังสือขอความยินยอมอย่างชัดเจน ซึ่งผู้ใช้เห็นด้วยในประเด็นนี้มากที่สุด (ร้อยละ 96.60) รองลงมาคือการกำหนดให้ตั้งค่าพิน (PIN) หรือรหัสผ่านที่มีความซับซ้อนเพื่อให้เดายาก (ร้อยละ 95.10) และการมีระบบการยืนยันตัวตนเพื่อเข้าใช้งานที่น่าเชื่อถือและปลอดภัย (ร้อยละ 94) ส่วนกลไกที่ผู้ใช้เห็นด้วยน้อยที่สุด ได้แก่ แอปพลิเคชันจะลบและทำลายข้อมูลส่วนบุคคลเมื่อวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลได้หมดอายุลงแล้ว (ร้อยละ 65.40)

1.4 ผู้ใช้เห็นด้วยในระดับสูงว่าแอปพลิเคชันสามารถปกป้องความเป็นส่วนตัวได้ โดยสามารถป้องกันการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต สามารถป้องกันการลบ ทำลาย หรือเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต มีค่าเฉลี่ยอยู่ระหว่าง 3.38-3.83

[1] ตัวเลขในวงเล็บหมายถึง ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน

1.5 ผู้ใช้เห็นว่าโดยรวมแล้วแอปพลิเคชันมีความมั่นคงปลอดภัยสารสนเทศที่ดีเพียงพอในระดับดี ค่าเฉลี่ยอยู่ระหว่าง 3.74 – 4.10 โดยเฉพาะประเด็นว่าด้วยการปกป้องข้อมูลจากภัยคุกคามทางเทคโนโลยีต่าง ๆ การป้องกันให้ข้อมูลส่วนบุคคลมีความปลอดภัยและเป็นความลับได้ในระดับดี มีมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ และเห็นว่าการทำธุรกรรมผ่านแอปพลิเคชันมีความปลอดภัย

1.6 ความไว้วางใจของผู้ใช้ ผู้ใช้มีความเชื่อในระดับสูง โดยมีค่าเฉลี่ยที่ 3.81 ต่อการที่ผู้ให้บริการแอปพลิเคชันปฏิบัติกับข้อมูลส่วนตัวของตนในแบบที่ไว้วางใจได้ ผู้ใช้ไว้วางใจในระดับสูงให้แอปพลิเคชันเก็บรวมรวมข้อมูลส่วนบุคคลโดยมีค่าเฉลี่ย 3.77 ผู้ใช้ไว้วางใจในระดับสูงให้แอปพลิเคชันใช้หรือประมวลผลข้อมูลส่วนบุคคลโดยมีค่าเฉลี่ย 3.67 ผู้ใช้ไว้วางใจในระดับสูงให้แอปพลิเคชันเปิดเผยข้อมูลส่วนบุคคลได้โดยมีค่าเฉลี่ย 3.65

2. ความสัมพันธ์ของคุณลักษณะของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ กับเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ จากการทดสอบสมมติฐานกลุ่มที่ 1 จำนวนทั้งหมด 55 สมมติฐาน พบว่าคุณลักษณะของผู้ใช้มีอิทธิพลต่อเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลที่ขนาดอิทธิพล (R2) ระหว่าง 0.05 - 0.17 ทำให้ได้สมการอิทธิพล จำนวน 33 สมการ โดยคุณลักษณะของผู้ใช้มีขนาดอิทธิพลมากที่สุดต่อเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลในประเด็นสิทธิของเจ้าของข้อมูลส่วนบุคคลสามารถยื่นร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมดำเนินการตามกฎหมาย (IP6) และ ผู้ใช้ทราบช่องทางติดต่อคณะกรรมการผู้เชี่ยวชาญเพื่อยื่นร้องเรียน (IP7) โดยมีขนาดอิทธิพล (R2) เท่ากับ 0.17 คุณลักษณะของผู้ใช้มีขนาดอิทธิพลรองลงมาต่อผู้ใช้มีสิทธิลบหรือทำลายข้อมูลส่วนบุคคลของตนได้ตาม พระราชบัญญัติคุ้มครองส่วนบุคคล พ.ศ. 2562 มาตรา 33 (CO5) (R2=0.16) คุณลักษณะของผู้ใช้มีขนาดอิทธิพลรองลงมาอันดับที่ 3 ได้แก่ ประเด็นผู้ควบคุมข้อมูลส่วนบุคคลต้องประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นสำหรับวัตถุประสงค์ที่ได้ระบุไว้ (DM1) (R2 = 0.15)

3. ความสัมพันธ์ของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่กับความเป็นส่วนตัวและความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชัน ผลการวิจัยพบว่าอิทธิพลของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลกับความเป็นส่วนตัวและความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชัน จากการทดสอบสมมติฐานกลุ่มที่ 2 และ 3 นี้จำนวนทั้งหมด 8 สมมติฐาน ทำให้ได้สมการอิทธิพลจำนวน 8 สมการ ที่ขนาดอิทธิพล (R2) ระหว่าง 0.08 - 0.31 ผลการทดสอบสมมติฐานพบว่าปัจจัยที่มีขนาดอิทธิพล (R2) มากที่สุดในกลุ่มสมมติฐานนี้ คือ เท่ากับ 0.31 ได้แก่ แอปพลิเคชันสามารถปกป้องข้อมูลส่วนบุคคลจากภัยคุกคามทางเทคโนโลยีต่าง ๆ (MS2) โดยปัจจัยย่อยในสมการที่มีอิทธิพลโดดเด่นกับ MS2 อธิบายตามลำดับ ได้แก่ ก) ค่าเริ่มต้นของแอปพลิเคชัน จะเป็น “ไม่ยินยอมให้ใช้ข้อมูล” เสมอ (CC6) ข) การป้องกันการโจมตีข้อมูลส่วนบุคคลจากผู้ไม่ประสงค์ดี (IS3) ค) ผู้ใช้ทราบช่องทางติดต่อคณะกรรมการผู้เชี่ยวชาญเพื่อยื่นร้องเรียน (IP7) จ) ผู้ให้บริการแอปพลิเคชันให้ความรู้ ความ

เข้าใจในการใช้บริการเทคโนโลยีทางการเงินอย่างปลอดภัย ทำให้มีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามในการใช้บริการเทคโนโลยีทางการเงินเบื้องต้น (IS6) และ ฉ) การใช้ การเก็บรักษา และการเปิดเผย รวมถึงการถ่ายโอนข้อมูลส่วนบุคคลให้เป็นไปตามวัตถุประสงค์ที่ระบุไว้ก่อนการเก็บข้อมูล (U1) ซึ่งสามารถแสดงสมการอิทธิพล ดังนี้

$\widehat{MS2}$ = 2.120 + .256(U1) + .419(IP7) + .438(IS3) + .457(CC6) + .379(DM1) + .400(IS6) - .280(CC5) + .267(CC7)

จากสมการอธิบายได้ว่าเมื่อ U1, IP7, IS3, CC6, DM1, IS6, CC5 และ CC7 มีค่าเท่ากับ 0 MS2 จะมีค่าเท่ากับ 2.120 ถ้า U1, IP7, IS3, CC6, DM1, IS6 และ CC7 มีค่าเพิ่มขึ้น 1 หน่วย MS2 จะมีค่าเพิ่มขึ้น 0.265, 0.419, 0.438, 0.457, 0.379, 0.400 และ 0.267 ตามลำดับ ถ้า CC5 มีค่าเพิ่มขึ้น 1 หน่วยแล้ว MS2 จะมีค่าลดลง 0.280

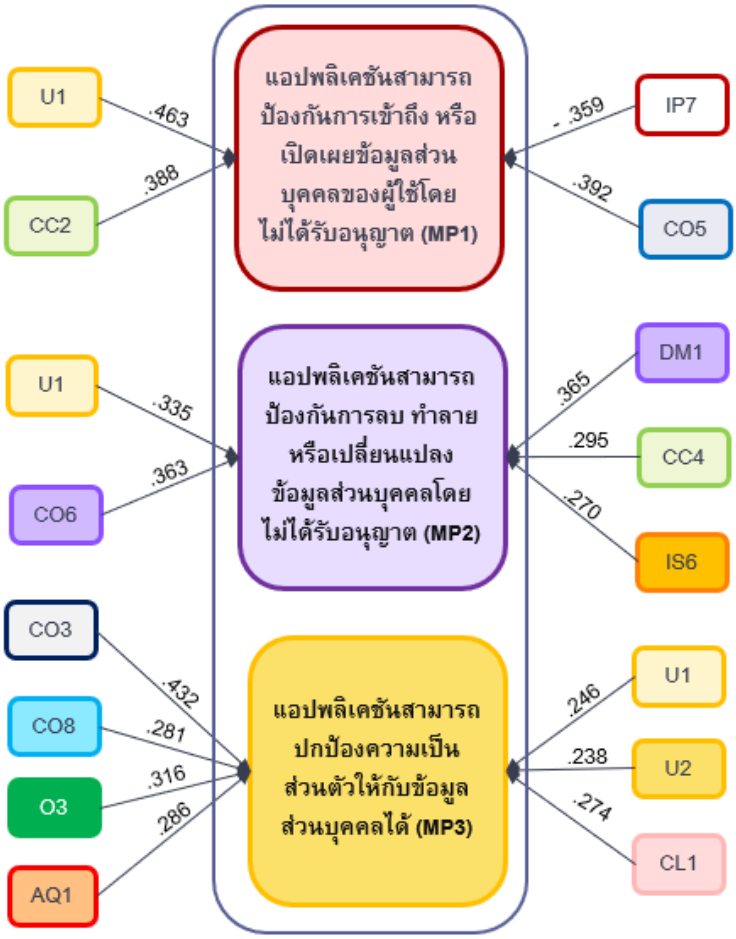
4. ความสัมพันธ์ของความมั่นคงปลอดภัยสารสนเทศและความเป็นส่วนตัวของแอปพลิเคชันต่อความไว้วางใจของผู้ใช้ ผลการวิจัยพบว่าอิทธิพลของความมั่นคงปลอดภัยสารสนเทศและความเป็นส่วนตัวของแอปพลิเคชันต่อความไว้วางใจของผู้ใช้ จากการทดสอบสมมติฐานในกลุ่มนี้จำนวนทั้งหมด 4 สมมติฐาน พบว่าผ่านเงื่อนไขการใช้การวิเคราะห์ถดถอยเชิงเส้นแบบพหุทั้งหมด มีขนาดอิทธิพล (R2) ระหว่าง 0.17 - 0.36 ทำให้ได้สมการอิทธิพล จำนวน 4 สมการ ปัจจัยที่มีขนาดอิทธิพล (R2) มากที่สุดในกลุ่มสมมติฐานนี้ คือ เท่ากับ 0.36 ได้แก่ การไว้วางใจในผู้ให้บริการแอปพลิเคชัน (T1) โดยปัจจัยย่อยในสมการที่มีอิทธิพลโดดเด่นกับ T1 อธิบายตามลำดับ ได้แก่ ก) แอปพลิเคชันสามารถปกป้องข้อมูลส่วนบุคคลจากภัยคุกคามทางเทคโนโลยีต่างๆ (MS2) ข) แอปพลิเคชันมีความมั่นคงปลอดภัยสารสนเทศที่ดีเพียงพอ (MS1) และ ค) ผู้ใช้รู้สึกปลอดภัยเมื่อทำธุรกรรมกับแอปพลิเคชัน (MS5) ซึ่งสามารถแสดงสมการอิทธิพล ดังนี้

$\widehat{T1}$ = .715 + .282(MS2) + .181(MS1) +.174(MS5) +.131(MS3)

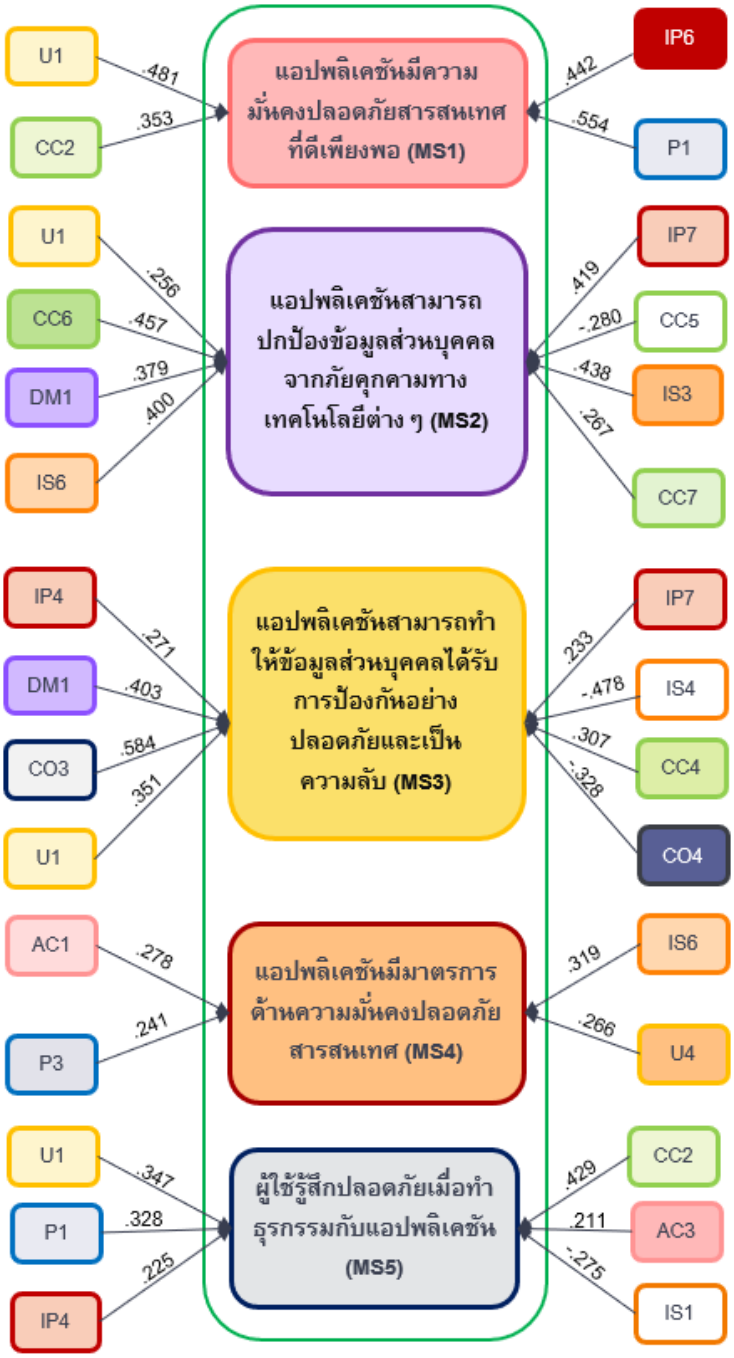
5. ความสัมพันธ์ของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่กับความไว้วางใจของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ เจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลต่อความไว้วางใจของผู้ใช้ที่ขนาดอิทธิพล (R2) ระหว่าง 0.25 - 0.29 ทำให้ได้สมการอิทธิพลจำนวน 4 สมการ ปัจจัยที่มีขนาดอิทธิพล (R2) มากที่สุดในกลุ่มสมมติฐานนี้ คือ เท่ากับ .288 ได้แก่ การไว้วางใจให้แอปพลิเคชันเก็บรวบรวมข้อมูลส่วนบุคคล (T2) โดยปัจจัยย่อยในสมการที่มีอิทธิพลโดดเด่นกับ T2 อธิบายตามลำดับ ได้แก่ ก) แอปพลิเคชันมีการกำหนดให้ตั้งรหัสผ่านที่มีความซับซ้อน (IS5) ข) การใช้ การเก็บรักษา และการเปิดเผยข้อมูลส่วนบุคคลต้องเป็นไปตามวัตถุประสงค์ที่ระบุไว้ก่อนการเก็บข้อมูลเท่านั้น (U1) และ ค) แอปพิลเคชันต้องประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นสำหรับวัตถุประสงค์ที่ได้ระบุไว้ (DM1) สามารถแสดงสมการอิทธิพล ดังนี้

$\widehat{T2}$ = 2.234 + .332(DM1) + .320(IP6) + .343(U1) + .570(IS5) + .236(AC3) + .297(CL1) + .208(IP3) - .348(IS2) + .261(P2) - .316(U3)

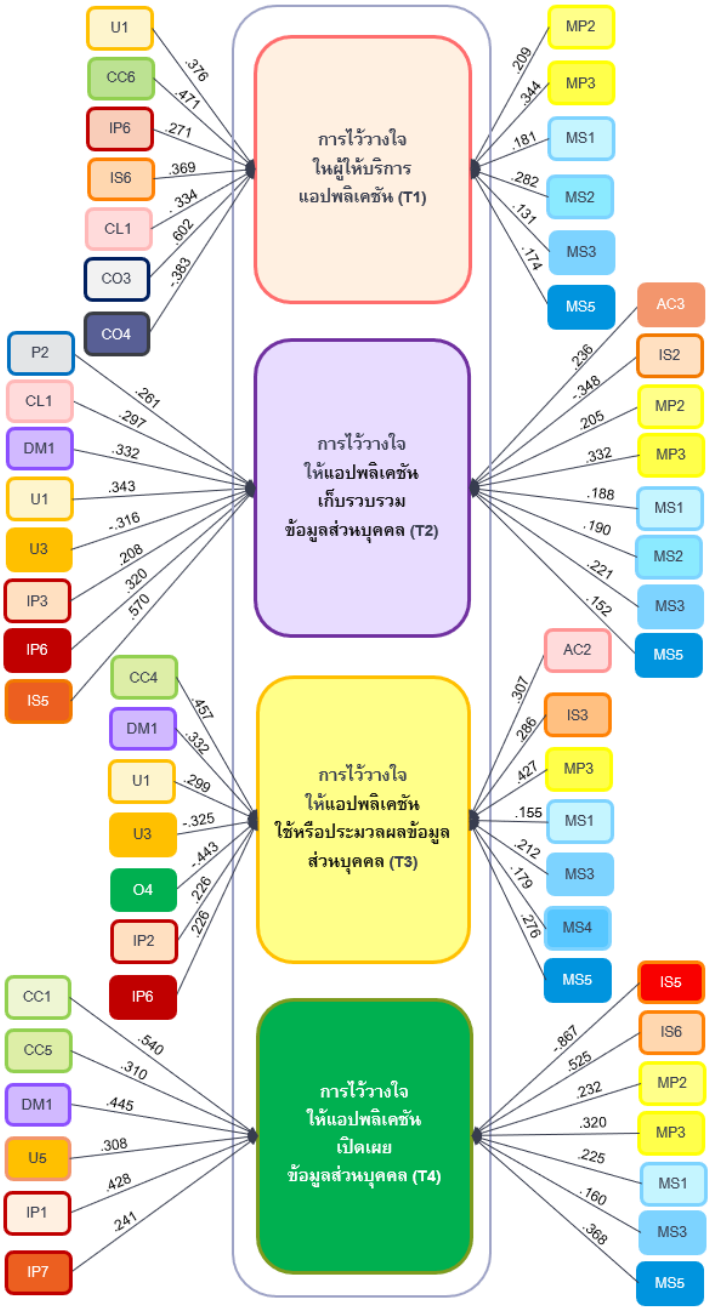
6. แบบจำลองความสัมพันธ์ระหว่างกลไกการปกป้องข้อมูลส่วนบุคคลในแอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่กับความมั่นคงปลอดภัยสารสนเทศ ความเป็นส่วนตัวของแอปพลิเคชัน และ ความไว้วางใจของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ ดังรูปที่ 3 รูปที่ 4 และ รูปที่ 5



รูปที่ 3 ตัวแบบจำลองความสัมพันธ์ของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ กับ ความเป็นส่วนตัวของแอปพลิเคชัน



รูปที่ 4 ตัวแบบจำลองความสัมพันธ์ของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่กับความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชัน



รูปที่ 5 ตัวแบบจำลองความสัมพันธ์ของเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลของผู้ใช้แอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ ความเป็นส่วนตัวของแอปพลิเคชัน และ ความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชัน ต่อ ความไว้วางใจของผู้ใช้

สรุปและอภิปรายผล

สรุปการทดสอบกลุ่มสมมติฐานที่ 1 ปัจจัยความสามารถในการปกป้องความเป็นส่วนตัวของตนมีอิทธิพลในเชิงบวกต่อเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคลในเกือบทุกประเด็น และความกังวลด้านความ

เป็นส่วนตัวในประเด็นต่าง ๆ มีอิทธิพลในเชิงลบต่อเจตคติต่อกลไกการปกป้องข้อมูลส่วนบุคคล ซึ่งหมายความว่าหากผู้ใช้มีเจตคติที่ดีต่อกลไกการปกป้องข้อมูลส่วนบุคคลของแอปพลิเคชันแล้วระดับความกังวลของผู้ใช้จะลดลง สอดคล้องกับ Pinto (2018) ที่กล่าวว่าผู้ใช้เต็มใจที่จะแลกเปลี่ยนข้อมูลส่วนบุคคลกับเว็บไซต์ที่เชื่อถือได้ และสอดคล้องกับ Chang et al. (2018) ที่พบว่า นโยบายความเป็นส่วนตัวที่มีประสิทธิผลดีจะทำให้ผู้ใช้รับรู้ว่าความเสี่ยงด้านความเป็นส่วนตัวลดลง ทำให้ความกังวลลดลง และมีบทบาทสำคัญที่ทำให้ผู้ใช้รับรู้ว่าแอปพลิเคชันมีความปลอดภัยข้อมูลส่วนบุคคลสูงขึ้น

สรุปการทดสอบสมมติฐานที่ 2 ปัจจัยด้านกลไกการปกป้องข้อมูลส่วนบุคคลที่มีอิทธิพลต่อความเป็นส่วนตัวของแอปพลิเคชันในหลายๆ ด้าน คือ ปัจจัยแอปพลิเคชัน ใช้ เก็บรักษาและเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามวัตถุประสงค์ที่ระบุไว้ตอนขอคำยินยอม (U1) ปัจจัยแอปพลิเคชันแจ้งรายละเอียดและวิธีติดต่อของผู้ให้บริการแอปพลิเคชันรวมไปถึงรายละเอียดของผู้มีส่วนได้เสียที่อาจรับรู้ข้อมูลส่วนบุคคลของผู้ใช้ (O3) มีอิทธิพลในเชิงบวกกับเจตคติต่อความเป็นส่วนตัวของแอปพลิเคชัน สอดคล้องกับ Chang et al. (2018) และ Balapour, Nikkhah & Sabherwal (2020) ที่พบว่านักพัฒนาแอปพลิเคชันควรให้ข้อมูลเกี่ยวกับมาตรการการปกป้องข้อมูลส่วนบุคคลไว้ในนโยบายความเป็นส่วนตัว เพราะรายละเอียดดังกล่าวมีบทบาทสำคัญในการกระตุ้นให้ผู้ใช้รับรู้ว่าแอปพลิเคชันมีความปลอดภัย มีความเป็นส่วนตัวและสามารถปกป้องข้อมูลส่วนบุคคลได้

สรุปการทดสอบสมมติฐานกลุ่มที่ 3 พบว่าปัจจัยด้านกลไกการปกป้องข้อมูลส่วนบุคคลในแอปพลิเคชันการให้บริการทางการเงินและการชำระเงินผ่านอุปกรณ์เคลื่อนที่ที่มีอิทธิพลมากที่สุดต่อความมั่นคงปลอดภัยสารสนเทศของแอปพลิเคชัน คือ แอปพลิเคชัน ใช้ เก็บรักษาและเปิดเผย (รวมถึงการถ่ายโอน) ข้อมูลส่วนบุคคลให้เป็นไปตามวัตถุประสงค์ที่ระบุไว้ตอนขอคำยินยอม (U1) สอดคล้องกับ Chang et al. (2018) ที่พบว่าหากแอปพลิเคชันมีนโยบายความเป็นส่วนตัวที่ระบุรายละเอียดเกี่ยวกับการใช้ เก็บรักษาและเปิดเลยข้อมูลส่วนบุคคลไว้อย่างชัดเจนนั้นมีบทบาทสำคัญที่ทำให้ผู้ใช้รับรู้ว่าแอปพลิเคชันมีความปลอดภัยของข้อมูลส่วนบุคคลสูงขึ้น

สรุปการทดสอบสมมติฐานกลุ่มที่ 4 และ 6 พบว่าปัจจัยด้านความเป็นส่วนตัวของแอปพลิเคชัน และกลไกการปกป้องข้อมูลส่วนบุคคลในแอปพลิเคชันมีอิทธิพลต่อความไว้วางใจของผู้ใช้ ซึ่งสอดคล้องกับ Deloitte (2018) ที่พบว่าหากผู้ใช้สามารถควบคุมข้อมูลส่วนบุคคลของตนเองได้ องค์กรผู้ให้บริการจะได้รับความเชื่อมั่นมากขึ้น ซึ่งสอดคล้องกับงานวิจัยของ Chueapirom & Chooprayoon (2016) ที่ว่าปัจจัยสำคัญที่มีอิทธิพลต่อโอกาสที่แอปพลิเคชันการให้บริการทางการเงินจะประสบความสำเร็จ คือ ผู้ใช้บริการสามารถควบคุมและตั้งค่าความเป็นส่วนตัวด้วยตนเองได้ และสอดคล้องกับ Albinson, Balaji, & Chu (2019) ที่ว่าหากผู้ให้บริการให้สิทธิการควบคุมการใช้ข้อมูลส่วนบุคคลให้อยู่ในมือของผู้ใช้แล้ว ผู้ให้บริการจะได้รับความไว้วางใจจากผู้ใช้ และองค์กรที่มีความโปร่งใสเกี่ยวกับการใช้ข้อมูลส่วนบุคคลจะได้รับความไว้วางใจจากผู้บริโภค คุณภาพและความชัดเจนโปร่งใสของนโยบายความเป็นส่วนตัวมีบทบาทที่สำคัญอย่างยิ่งต่อการที่องค์กรจะได้รับความไว้วางใจจากผู้ใช้

สรุปการทดสอบสมมติฐานกลุ่มที่ 5 ปัจจัยด้านความมั่นคงปลอดภัยสารสนเทศมีอิทธิพลต่อความไว้วางใจของผู้ใช้ สอดคล้องกับงานวิจัยของ Peikari, Ramayah, Shah, & Lo (2018) ที่ว่าการรับรู้ของผู้ใช้ที่มีต่อ

ความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการมีอิทธิพลในเชิงบวกต่อความไว้วางใจต่อผู้ให้บริการ ดังนั้นการสื่อสารให้ผู้ใช้ทราบถึงกลไกการรักษาความปลอดภัยข้อมูลจะช่วยเพิ่มความไว้วางใจและลดความกังวลด้านความมั่นคงปลอดภัยสารสนเทศได้ และสอดคล้องกับงานวิจัยของ Johnson, Kiser, Washington, & Torres (2017) ที่ว่าการรับรู้ของผู้ใช้ที่มีต่อความมั่นคงปลอดภัยสารสนเทศของระบบมีอิทธิพลอย่างมากต่อทัศนคติของผู้คนในการยอมรับเทคโนโลยีด้านการชำระเงินบนอุปกรณ์เคลื่อนที่

จากผลการทดสอบอิทธิพลของตัวแปรความมั่นคงปลอดภัยสารสนเทศต่อความไว้วางใจของผู้ใช้ (สมมติฐานกลุ่มที่ 5) อิทธิพลของกลไกปกป้องข้อมูลส่วนบุคคลในแอปพลิเคชันต่อความไว้วางใจของผู้ใช้ (สมมติฐานกลุ่มที่ 6) และ อิทธิพลของความเป็นส่วนตัวของแอปพลิเคชันต่อความไว้วางใจของผู้ใช้ (สมมติฐานกลุ่มที่ 4) พบว่าปัจจัยเหล่านี้มีอิทธิพลในเชิงบวกต่อความไว้วางใจของผู้ใช้ ซึ่งสอดคล้องกับงานวิจัยของ Microsoft (2019) ที่ว่าปัจจัยที่สำคัญที่สุดต่อความไว้วางใจของผู้บริโภคเรียง ได้แก่ ความมั่นคงปลอดภัยสารสนเทศ ความเป็นส่วนตัว ความน่าเชื่อถือ จริยธรรม ซึ่งสอดคล้องกับผลสำรวจของ KPGM (2011) และ Albinson, Balaji, & Chu (2019) ที่ว่ามาตรการปกป้องข้อมูลส่วนบุคคลและมาตรการความมั่นคงปลอดภัยสารสนเทศที่ดีสามารถเพิ่มความไว้วางใจของผู้บริโภคได้ เนื่องจากปัจจุบันผู้ใช้รับรู้มากขึ้นว่าในโลกไซเบอร์และการพึ่งพาอุปกรณ์อัจฉริยะที่เพิ่มขึ้นจะนำมาซึ่งความเสี่ยงที่มากขึ้น นักพัฒนาแอปพลิเคชันจึงควรมุ่งเน้นให้แอปพลิเคชันมีความมั่นคงปลอดภัยสารสนเทศที่ดีเพื่อกระตุ้นให้ลูกค้าเกิดความไว้วางใจให้องค์กร เพราะลูกค้าจะเลือกองค์กรที่ใช้เทคโนโลยีล่าสุดในการรักษาผลิตภัณฑ์และบริการให้มีความปลอดภัยและน่าเชื่อถือมากขึ้น

การประยุกต์ใช้ผลการวิจัย จากผลการวิจัย ผู้ให้บริการแอปพลิเคชันควรดำเนินการ ดังนี้

1. จากตัวแบบในรูปที่ 3 4 และ 5 ตัวแปรการมีทางเลือกในการให้หรือไม่ให้ความยินยอมแก่แอปพลิเคชันในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (CC2) มีอิทธิพลในเชิงบวกต่อเจตคติของผู้ใช้ต่อกลไกปกป้องข้อมูลของแอปพลิเคชันทั้งในด้านความเป็นส่วนตัว ความมั่นคงปลอดภัยสารสนเทศ และความไว้วางใจ แอปพลิเคชันจึงควรมีทางเลือกให้ผู้ใช้สามารถยินยอมหรือไม่ให้ความยินยอมในการเก็บรักษา ประมวลผล และเปิดเผยข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับ ISO/IEC29100 และ ISO/IEC27701 ในประเด็นความยินยอมและทางเลือก และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 19 และที่สำคัญผลการวิจัยฉบับนี้พบว่าการมีทางเลือกสำหรับการให้ความยินยอมทำให้แอปพลิเคชันได้รับความไว้วางใจจากผู้ใช้มากขึ้นด้วย

2. จากตัวแบบในรูปที่ 4 ควรพัฒนาระบบแจ้งเตือนต่าง ๆ แต่ต้องไม่เตือนเกินจำเป็นเพราะจะทำให้ผู้ใช้รู้สึกไม่ปลอดภัย (ตัวแปรแอปพลิเคชันมีระบบแจ้งเตือนในกรณีที่ผู้ใช้ใช้อุปกรณ์เคลื่อนที่มีระบบปฏิบัติการไม่ตรงตามข้อกำหนดการเข้าใช้งาน (IS1) มีอิทธิพลเชิงลบกับ MS5)

3. จากตัวแบบในรูปที่ 3 4 และ 5 ตัวแปรผู้ให้บริการแอปพลิเคชันให้ความรู้ ความเข้าใจในการใช้บริการเทคโนโลยีทางการเงินอย่างปลอดภัย ทำให้ผู้ใช้มีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามในการใช้บริการเทคโนโลยีทางการเงินเบื้องต้น (IS6) มีอิทธิพลในเชิงบวกต่อเจตคติของผู้ใช้ต่อกลไกปกป้องข้อมูลของแอป

พลิเคชันทั้งในด้านความเป็นส่วนตัว ความมั่นคงปลอดภัยสารสนเทศ และความไว้วางใจ ดังนั้นผู้ให้บริการต้องให้ความรู้และสร้างความเข้าใจในการใช้บริการเทคโนโลยีทางการเงินอย่างปลอดภัยแก่ผู้ใช้ เพื่อให้ผู้ใช้มีเจตคติที่ดีแอปพลิเคชัน

4. เพิ่มช่องทางหรือเมนูการตั้งค่าที่เน้นหรือส่งเสริมให้ผู้ใช้บริหารสิทธิของตนที่พึงมีตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมวด 3 และมีเมนูควบคุมและจัดการข้อมูลส่วนบุคคลของผู้ใช้เองให้มากขึ้น รวมทั้งมีช่องทางให้ผู้ใช้มีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับ ISO/IEC29100 และ ISO/IEC27701 ในประเด็นสิทธิและการมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล ซึ่งจะสามารถยกระดับความไว้วางใจให้แก่แอปพลิเคชันได้ นอกจากนี้ ยังต้องจัดให้มีช่องทางให้ผู้ใช้ยื่นร้องเรียนต่อคณะกรรมการ เนื่องจากการวิจัยพบว่าตัวแปรความสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (CO) ซึ่งเกี่ยวกับการให้สิทธิผู้ใช้ตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีอิทธิพลในเชิงบวกต่อเจตคติของผู้ใช้ทั้งในด้านความเป็นส่วนตัว ความมั่นคงปลอดภัยสารสนเทศ และความไว้วางใจให้แอปพลิเคชัน และยังพบว่าตัวแปรแอปพลิเคชันมีตัวเลือกที่ยืดหยุ่น ให้ผู้ใช้สามารถจัดการข้อมูลส่วนบุคคลได้ด้วยตนเอง (O4) มีอิทธิพลในเชิงบวกกับการที่ผู้ใช้ไว้วางใจให้แอปพลิเคชันใช้และประมวลผลข้อมูลส่วนบุคคล

5. แอปพลิเคชันต้องประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลของแอปพลิเคชันเท่านั้น เพราะจากตัวแบบรูปที่ 3 4 และ 5 พบว่าตัวแปรแอปพลิเคชันประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลของแอปพลิเคชันเท่านั้น (DM1) มีอิทธิพลเชิงบวกต่อเจตคติของผู้ใช้ทั้งในด้านความเป็นส่วนตัว ความมั่นคงปลอดภัยสารสนเทศ และความไว้วางใจให้แอปพิลเคชัน

6. ระบุรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูล วัตถุประสงค์อันชอบด้วยกฎหมายของการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคล วิธีติดต่อผู้ให้บริการ วิธีติดต่อคณะกรรมการผู้เชี่ยวชาญเพื่อยื่นร้องเรียน และระบุมาตรการปกป้องข้อมูลส่วนบุคคลไว้ให้ชัดเจน และเข้าใจได้ง่าย นอกจากนี้ ยังต้องจัดทำเอกสารเพื่อสื่อสารให้ผู้ใช้ทราบถึงนโยบาย ขั้นตอน แนวทางปฏิบัติ และมีการบันทึกรายการ (Log File) ที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคลไว้ในนโยบายความเป็นส่วนตัวของแอปพลิเคชัน เนื่องจากตัวแบบที่ 3 แสดงให้เห็นว่าการที่แอปพลิเคชันแจ้งรายละเอียดของผู้ให้บริการแอปพลิเคชัน รวมถึงข้อมูลเกี่ยวกับวิธีติดต่อกับผู้ให้บริการ รวมไปถึงรายละเอียดของผู้มีส่วนได้เสียที่อาจรับรู้ข้อมูลส่วนบุคคลของผู้ใช้ (O3) มีอิทธิพลเชิงบวกต่อเจตคติของผู้ใช้ว่าแอปพลิเคชันสามารถปกป้องความเป็นส่วนตัวได้

7. การวิจัยพบว่ามีผู้ใช้จำนวนร้อยละ 35 ไม่เชื่อว่าแอปพลิเคชันจะลบข้อมูลส่วนบุคคลเมื่อวัตถุประสงค์สำหรับการประมวลผลได้หมดอายุลง ดังนั้นเมื่อข้อมูลส่วนบุคคลได้หมดอายุลงหรือเมื่อไม่ได้ใช้แล้ว แอปพลิเคชันจำเป็นต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลรับทราบว่าได้ลบทำลายแล้ว

ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

เนื่องจากตัวแปรการวิจัยในครั้งนี้ยังขาดคุณลักษณะของผู้ใช้ที่ผู้วิจัยไม่ได้รวบรวมมาวิเคราะห์ด้วย เช่น รายได้/ฐานะทางเศรษฐกิจ ระดับการศึกษา เนื่องจากจริยธรรมการวิจัยในคนให้ตัดข้อคำถามที่ทำให้คนตอบรู้สึกเป็นกังวลออก

เอกสารอ้างอิง

Albinson, N., Balaji, S., & Chu, Y. (2019). Building digital trust: Technology can lead the way. Deloitte Insights. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/6320_Building-digital-trust/DI_Building-digital-trust.pdf

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*. doi: 10.1016/j.ijinfomgt.2019.102063

Bank of Thailand. (2014). IT Best Practices - Phase II. Retrieved from https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/RiskMgt_Manual/download/แนวปฏิบัติ IT Best Practices - Phase II.pdf

Bank of Thailand. (2020). Mobile Banking and Internet Banking Transactions. Retrieved from https://www.bot.or.th/English/Statistics/Pages/default.aspx

Chang, Y., Wong, F. S., Libaque-Saenz, F. C., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly, 35*(3), 445-459. Retrieved from https://doi.org/10.1016/j.giq.2018.04.002

Chueapirom, S., & Chooprayoon, V. (2016). A Multiple Regression Analysis for Prediction Factors Influencing Mobile Banking Application of Generation Y Consumers. The 11th National Graduate Research Conference 2016, National Defense Studies Institute. 22 September 2016, page 188-196.

Cochran, W. (1977). *Sampling techniques*. New York: Wiley.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika,* 16, 297–334. https://doi.org/10.1007/BF02310555

Deloitte. (2018). A new era for privacy: GDPR six months on. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf

European Union Agency for Network and Information Security (ENISA). (2017). Privacy and data protection in mobile applications. Retrieved from https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacay and security. *International Journal of Engineering Business Management, 4.* doi:https://doi.org/10.5772/51645

IBM Security. (2019). *Cost of a data breach report 2019.* Retrieved from https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.189043820.693715687.1569613662-1615529680.1569613662

ISO/IEC. (2011). ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework. Retrieved from https://www.iso.org/standard/45123.html

ISO/IEC. (2019). ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. Retrieved from https://www.iso.org/standard/71670.html

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2017). Limitations to the rapid adoption of M-payment services: Understaning the impact of privacy risk on M-Payment. *Computers in Human Behavior, 79.* 111-122. Retrieved from https://doi.org/10.1016/j.chb.2017.10.035

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons, 53*(1), 59-68. doi:https://doi.org/10.1016/j.bushor.2009.09.003

Kemp, S. (2020). Datareportal. Retrieved from https://datareportal.com/reports/digital-2020-thailand?rq=thailand

KPGM. (2011). Privacy, security issues Hamper Wider Growth of mobile banking, despite increasing consumer acceptance: KPMG survey. Retrieved from https://www.prnewswire.com/news-releases/privacy-security-issues-hamper-wider-growth-of-mobile-banking-despite-increasing-consumer-acceptance-kpmg-survey-135994438.html

Microsoft. (2019). IDC Study: Only 31% of consumers In Asia Pacific trust organizations offering digital services to protect their personal data. Retrieved from Microsoft Stories Asia: https://news.microsoft.com/apac/2019/04/16/microsoft-idc-study-only-31-of-consumers-in-asia-pacific-trust-organizations-offering-digital-services-to-protect-their-personal-data/#_ftn2

Peikari, H. R., Ramayah T., Shah, M. H., & Lo, M.C. (2018). Patients' perception of the information security management in health centers: the role of organizational and human factors. *BMC Medical Informatics and Decision Making*, 18. doi: 10.1186/s12911-018-0681-z

Personal Data Protection Act, B.E. 2562 (2019). (2019). *Government Gazette. No. 136* Chapter 69 Gor, 52-95. Retrieved from http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

Pinto, S. L. (2018). *Privacy and data protection: A study on awareness and attitudes of millennial consumers on the Internet - An Irish perspective*. Retrieved from http://norma.ncirl.ie/3386/1/salonilerisapinto.pdf

Privacy International. (2018). How apps on android share data with Facebook. Retrieved from https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf

The World Bank. (2016). Privacy by design: Current practices in Estonia, India, and Austria. Retrieved from https://id4d.worldbank.org/sites/id4d.worldbank.org/files/ PrivacyByDesign_112918web.pdf

Wagner, K. (2018). This is how Facebook collects data on you even if you don’t have an account. Retrieved from https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg