ความคิดเห็นของ Generation C เกี่ยวกับความปลอดภัยบน Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย

บุญช่วย โค้วตระกูล

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาการจัดการมหาบัณฑิต
วิทยาลัยการจัดการ มหาวิทยาลัยมหิดล
พ.ศ. 2562

สารนิพนธ์

เรื่อง

ความคิดเห็นของ Generation C เกี่ยวกับความปลอดภัยบน Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย

ได้รับการพิจารณาให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาการจัดการมหาบัณฑิต

วันที่ 10 มกราคม พ.ศ. 2562

……..……..……

นายบุญช่วย โค้วตระกูล

ผู้วิจัย

……..……..……	……..……..……
ผู้ช่วยศาสตราจารย์พลิศา รุ่งเรือง,	ผู้ช่วยศาสตราจารย์พรเกษม กันตามระ,
Ph.D.	Ed.D.
อาจารย์ที่ปรึกษาสารนิพนธ์	ประธานกรรมการสอบ สารนิพนธ์
……..……..……	……..……..……
ดวงพร อาภาศิลป์,	ตรียุทธ พรหมศิริ ,
Ph.D.	Ph.D.
คณบดีวิทยาลัยการจัดการ	กรรมการสอบสารนิพนธ์
มหาวิทยาลัยมหิดล	

กิตติกรรมประกาศ

สารนิพนธ์หัวข้อ “ความคิดเห็นของ Generation C เกี่ยวกับความปลอดภัยบน Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย” นี้จะสำเร็จลุล่วงมิได้ หากผู้วิจัยมิได้รับความเมตตา กรุณา และอนุเคราะห์ จากผู้มีส่วนเกี่ยวข้องต่างๆ ผู้วิจัยจึงขอใช้พื้นที่กิตติกรรมประกาศนี้ในการกล่าวขอบคุณผู้มีส่วนเกี่ยวข้องทุกท่าน

ผู้วิจัยขอกราบขอบพระคุณ ผศ.ดร.พลิศา รุ่งเรือง ซึ่งเสียสละเวลาอันมีค่าเพื่อเป็นอาจารย์ที่ปรึกษางานวิจัยในครั้งนี้ ให้ความรู้ ให้คำแนะนำ และให้คำปรึกษา ตลอดจนช่วยชี้แนะแนวทางในการแก้ไขให้การศึกษาวิจัยอิสระนี้สำเร็จลุล่วง ขอขอบพระคุณประธานกรรมการและคณะกรรมการสอบ ซึ่งให้คำแนะนำแนวทางในการปรับปรุงงานวิจัยให้มีความสมบูรณ์ยิ่งขึ้น

ผู้วิจัยขอกราบขอบพระคุณคณะคณาจารย์วิทยาลัยการจัดการ มหาวิทยาลัยมหิดลที่ให้ความรู้ ซึ่งได้ถูกนำมาใช้เป็นแนวทางสำคัญในการศึกษาวิจัยนี้

ขอขอบคุณเพื่อนๆ ทุกคน และพี่ๆ น้องๆ ที่ธนาคารไอซีบีซี (ไทย) จำกัด (มหาชน) สำหรับความร่วมมือเป็นอย่างสำหรับการเป็นกลุ่มตัวอย่างในการสัมภาษณ์ในงานวิจัยชิ้นนี้ หากไม่ได้รับความร่วมมือ งานชิ้นนี้คงไม่แล้วเสร็จตามเวลาที่กำหนดไว้

ขอกราบขอบพระคุณ บิดา มารดา และสมาชิกในครอบครัว ที่ให้การสนับสนุนทางการศึกษาและเป็นแรงใจในการทำงานวิจัยให้สำเร็จลุล่วง ตลอดจนขอขอบคุณเพื่อนๆทุกคน โดยเฉพาะจากวิทยาลัยการจัดการ มหาวิทยาลัยมหิดล ซึ่งได้แก่ แบงก์ เฟิร์น เนม และไนซ์ ซึ่งคอยให้กำลังใจ ช่วยเหลือซึ่งกันและกันโดยตลอดตั้งแต่เริ่มต้นจนกระทั่งงานวิจัยเสร็จสมบูรณ์

สุดท้ายนี้ผู้วิจัยหวังเป็นอย่างยิ่งว่าการศึกษาวิจัยอิสระในครั้งนี้จะสามารถเป็นแหล่งอ้างอิงที่มีประโยชน์สำหรับธุรกิจด้านการธนาคารหรือผู้ที่สนใจ และหวังว่าการศึกษาวิจัยอิสระในครั้งนี้จะสามารถนำไปต่อยอดได้ หากมีข้อผิดพลาดประการใด ผู้วิจัยขออภัยไว้ ณ ที่นี้ด้วย

บุญช่วย โค้วตระกูล

ความคิดเห็นของ Generation C เกี่ยวกับความปลอดภัยบน Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย

GENERATION C' S PERSONAL OPINIONS TOWARDS THE SECURITY ISSUES OF MOBILE BANKING APPLICATION OFFERED BY COMMERCIAL BANKS IN THAILAND

บุญช่วย โค้วตระกูล 6050063

กจ.ม.

คณะกรรมการที่ปรึกษาสารนิพนธ์: ผู้ช่วยศาสตราจารย์พลิศา รุ่งเรือง, Ph.D., ผู้ช่วยศาสตราจารย์พรเกษม กันตามระ, Ed.D., ตรียุทธ พรหมศิริ, Ph.D.

บทคัดย่อ

ปัจจุบันพบว่าในประเทศไทยมีผู้ใช้งานผ่าน Mobile Banking สูงถึง 28 ล้านคนตามสถิติของธนาคารแห่งประเทศไทย ณ เดือนกันยายน พ.ศ. 2560 ส่วนหนึ่งเป็นผลมาจากความพยายามที่จะนำประเทศไทยก้าวเข้าสู่ Cashless Society หรือสังคมไร้เงินสด ตามนโยบาย 4.0 ของภาครัฐ ธนาคารพาณิชย์ในประเทศต่างเดินหน้าพัฒนาระบบ Mobile Banking เพื่อตอบสนองความต้องการของผู้ใช้งานให้ได้มากที่สุดควบคู่ไปกับกิจกรรมทางการตลาดในวงกว้างเพื่อส่งเสริมให้คนไทยหันมาใช้งาน Mobile Banking แทนการใช้เงินสด

อย่างไรก็ตามจากงานวิจัยในอดีตพบว่า "ความปลอดภัย" ถือเป็นปัจจัยสำคัญที่ส่งผลต่อความพึงพอใจและรวมถึงการตัดสินใจเริ่มใช้บริการ Mobile Banking Application อย่างมีนัยยะสำคัญ เพื่อที่เข้าใจพฤติกรรมและความคิดเห็นของกลุ่ม Generation C ในประเด็นเรื่องความปลอดภัยของ Mobile Banking Application ที่ให้บริการโดยธนาคารพาณิชย์ในประเทศไทยมากยิ่งขึ้น ผู้วิจัยจึงได้ทำการศึกษาจากกลุ่มตัวอย่างจำนวน 30 คน ในลักษณะงานวิจัยเชิงคุณภาพโดยใช้วิธีการสัมภาษณ์แบบกึ่งโครงสร้าง จากการศึกษาพบว่า กลุ่มตัวอย่างส่วนใหญ่มีความมั่นใจในระบบ Mobile Banking Application ที่ให้บริการโดยธนาคารพาณิชย์ในประเทศ เนื่องจากระบบยืนยันตัวตนที่น่าเชื่อถือ ไม่เคยประสบเหตุการณ์เลวร้ายในการใช้งาน ระมัดระวังตัวเองในการใช้งาน และคิดว่าธนาคารพาณิชย์เองย่อมห่วงชื่อเสียงของตนเอง สำหรับการยืนยันตัวตนที่กลุ่มตัวอย่างเห็นว่ามีความเหมาะสมต่อการใช้งานนั้น ในขั้นตอนของการยืนยันตัวตนเพื่อ log-in กลุ่มตัวอย่างส่วนใหญ่เลือกวิธีการสแกนลายนิ้วมือเนื่องจาก สะดวก รวดเร็ว ง่าย ปลอมแปลงยาก ปลอดภัย มือถือส่วนใหญ่รองรับวิธีดังกล่าว และเพียงพอต่อการ log-in แต่ไม่ได้ทำรายการธุรกรรม และสำหรับการยืนยันตัวตนเพื่อยืนยันรายการธุรกรรม กลุ่มตัวอย่างส่วนใหญ่เลือกวิธี One Time Password (OTP) เนื่องจากง่าย ไม่ต้องจดจำ และปลอดภัย สำหรับความรู้ความเข้าใจการใช้งาน Mobile Banking อย่างปลอดภัยนั้น พบว่ากลุ่มตัวอย่างมีความเข้าใจคลาดเคลื่อนในสาระสำคัญที่เกี่ยวข้องในเรื่องการใช้งาน Mobile Banking ให้ปลอดภัยในหลายๆ ประเด็น และแม้ในประเด็นที่กลุ่มตัวอย่างมีความรู้ความเข้าใจเป็นอย่างดี ก็มีแนวโน้มที่จะละเลยหรือไม่ปฏิบัติตามสิ่งที่พึงปฏิบัติ เหล่านี้ถือเป็นความเสี่ยงต่อตัวผู้ใช้งานเองและรวมถึงธนาคารพาณิชย์ที่ต้องหามาตรการป้องกันเชิงรุก และสร้างความตระหนักให้เกิดขึ้นกับตัวผู้ใช้บริการดังกล่าวให้มากยิ่งขึ้น

คำสำคัญ: Mobile Banking Application / ความเชื่อมั่น / ความปลอดภัย / ระบบยืนยันตัวตน

82 หน้า

สารบัญ

		หน้า
กิตติกรรมประกาศ		**ข**
บทคัดย่อ		**ค**
สารบัญ		**ง**
สารบัญตาราง		**ช**
สารบัญรูปภาพ		**ฌ**
บทที่ 1	**บทนำ**	**1**
	1.1 ที่มาและความสำคัญ	1
	1.2 คำถามงานวิจัย	2
	1.3 วัตถุประสงค์งานวิจัย	3
	1.4 ขอบเขตงานวิจัย	3
	1.5 ประโยชน์ที่คาดว่าจะได้รับ	4
	1.6 ประพจน์	4
	1.7 นิยามศัพท์	6
บทที่ 2	**แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง**	**7**
	2.1 นิยามความเชื่อมั่นภายใต้บริบท Mobile Banking	7
	2.2 แนวนโยบายการเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่โดยธนาคารแห่งประเทศไทย	8
	2.3 ความปลอดภัยของระบบมีผลต่อการตัดสินใจใช้ Mobile Banking Application	10
	2.4 รูปแบบของภัยคุกคามสำหรับการใช้งาน Mobile Banking ในปัจจุบัน	10
	2.5 การใช้งาน Mobile Banking อย่างปลอดภัย	12
	2.6 ประเภทของสิ่งที่ใช้ยืนยันตัวตน (Credential type)	13
	2.7 งานวิจัยที่เกี่ยวเนื่องกับความปลอดภัยของ Mobile Banking Application	30
บทที่ 3	**ระเบียบวิธีวิจัย**	**31**
	3.1 รูปแบบการวิจัย	31

สารบัญ (ต่อ)

	3.2 ประชากรและการสุ่มตัวอย่าง	31
	3.3 วิธีการเก็บรวบรวมข้อมูล	32
	3.4 การวิเคราะห์ข้อมูล	32
บทที่ 4	**ผลการวิจัย**	**36**
	4.1 ระดับความเชื่อมั่นในเรื่องความปลอดภัยในการใช้งาน Mobile Banking Application ของผู้ใช้บริการ	36
	4.1.1 ภาพรวมของความเชื่อมั่นในความปลอดภัยที่มีต่อบริการ Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย	36
	4.1.2 เหตุผลหลักของความเชื่อมั่นในความปลอดภัยที่มีต่อ Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย	37
	4.1.3 แนวทางการพัฒนาความเชื่อมั่นด้านความปลอดภัยของ Mobile Banking Application	39
	4.2 ความรู้ความเข้าใจในการใช้ Mobile Banking Application ในการทำธุรกรรมทางการเงินอย่างปลอดภัย และการนำไปปฏิบัติ	41
	4.2.1 ความคิดเห็นต่อการเชื่อมต่อ Wifi ที่มีความเสี่ยงในแง่ความปลอดภัยในการเข้าใช้บริการ Mobile Banking มากกว่าการเชื่อมต่อเครือข่าย 3G และ 4G	43
	4.2.2 ความคิดเห็นต่อการทำธุรกรรมผ่าน Mobile Banking Application ที่มีความเสี่ยงน้อยกว่าการทำธุรกรรมผ่าน Website ของธนาคาร	45
	4.2.3 ความคิดเห็นในเรื่องการเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่คุ้นเคยไม่ได้ปลอดภัยกว่าการเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่ไม่คุ้นเคย	46
	4.2.4 ความคิดเห็นต่อการใช้งาน Mobile Banking Application ว่าควร log out ออกจากระบบเสมอหลังใช้งานเสร็จ	49
	4.2.5 ความคิดเห็นในเรื่องดาวน์โหลด Application จาก App Store สำหรับระบบปฏิบัติการ iOS ว่าไม่ได้ปลอดภัยจากมัลแวร์ (malware)	51
	4.2.6 ความคิดเห็นในเรื่องการพิจารณา Mobile Banking Application ของจริงว่าต้องดูที่ชื่อผู้พัฒนา (Developer) ซึ่งจะแสดงชื่อสถาบันการเงินนั้นๆ	52

สารบัญ (ต่อ)

4.2.7 ความคิดเห็นในเรื่องการดาวน์โหลดซอฟต์แวร์ฟรีบนอินเตอร์เน็ตมีส่วนเกี่ยวข้องกับการติดมัลแวร์ 54

4.2.8 ความคิดเห็นต่อการเก็บรหัสเข้าใช้งาน Mobile Banking Application เป็นความลับ 55

4.2.9 ความคิดเห็นต่อการยืนยันตัวตนเข้าใช้งาน Mobile Banking Application โดยใช้ One Time Password (OTP) ที่มีความน่าเชื่อถือสูงกว่าการใช้รหัสผ่าน 57

4.2.10 ความคิดเห็นต่อการจดรหัสผ่านเข้าใช้งาน Mobile Banking Application ไว้บนโทรศัพท์มือถือหรือเศษกระดาษ 58

4.3 ความคิดเห็นของผู้ใช้บริการเกี่ยวกับระบบการยืนยันตัวตนบน Mobile Banking Application ที่เหมาะสม 60

4.3.1 วิธีการยืนยันตัวตนที่เหมาะสมเพื่อวัตถุประสงค์ในการ log in เข้าสู่ Mobile Banking Application 60

4.3.2 วิธีการยืนยันตัวตนที่เหมาะสมเพื่อวัตถุประสงค์ในการยืนยันรายการธุรกรรมที่ทำผ่าน Mobile Banking Application 62

4.3.3 วิธีการยืนยันตัวตนแบบเดียวกันหรือแตกต่างกันสำหรับการยืนยันตัวตนเพื่อวัตถุประสงค์ในการ log in และการยืนยันรายการธุรกรรม 64

บทที่ 5 สรุป อภิปรายผล และข้อเสนอแนะ 66

5.1 สรุปและอภิปรายผลการวิจัย 66

5.1.1 ความเชื่อมั่นของผู้ใช้งาน Mobile Banking Application ในด้านความปลอดภัย 66

5.1.2 ความรู้ความเข้าใจของผู้ใช้บริการ Mobile Banking Application ในการทำธุรกรรมอย่างปลอดภัย 67

5.1.3 ความคิดเห็นของผู้ใช้บริการเกี่ยวกับระบบการยืนยันตัวตนบน Mobile Banking Application ที่เหมาะสม 70

5.2 ข้อเสนอแนะสำหรับผู้บริหาร 70

5.3 ข้อจำกัดในการวิจัย และข้อเสนอแนะสำหรับงานวิจัยในอนาคต 72

บรรณานุกรม 73

สารบัญ (ต่อ)

ภาคผนวก **77**

ภาคผนวก ก แบบสัมภาษณ์แบบกึ่งโครงสร้าง 77

ประวัติผู้วิจัย **82**

สารบัญตาราง

ตาราง		หน้า
2.1	เปรียบเทียบช่องทางการทำธุรกรรมทางการเงินบนโทรศัพท์มือถือ	13
2.2	ระดับความน่าเชื่อถือ (Levels of assurance)	14
2.3	ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ	14
3.1	แปลผลคะแนนจากการทำแบบทดสอบ	34

สารบัญภาพ

ภาพ		หน้า
2.1	วิธีการสังเกต Mobile Banking Application ที่เป็นของจริง	11
4.1	แจกแจงความถี่จำนวนคนของกลุ่มตัวอย่างในแต่ละระดับความเชื่อมั่น 1 – 10	37
4.2	แจกแจงความถี่จำนวนคนของกลุ่มตัวอย่างในแต่ละระดับคะแนนจากแบบทดสอบ	42
4.3	แจกแจงความถี่จำนวนคนของกลุ่มตัวอย่างในแต่ละระดับความรู้ความเข้าใจ	42
4.4	การโจมตีของแฮกเกอร์โดยใช้เทคนิค Man in the Middle attack	43
4.5	แสดงร้อยละของกลุ่มตัวอย่างโดยจะเลือกเชื่อมต่อ Wifi หรือไม่หากต้องทำธุรกรรม Mobile Banking ในชีวิตประจำวัน	44
4.6	แสดงร้อยละของกลุ่มตัวอย่างว่ามีการตรวจสอบ Wifi สาธารณะก่อนการเชื่อมต่อหรือไม่ในชีวิตประจำวัน	48
4.7	แสดงร้อยละของกลุ่มตัวอย่างว่ามีการ log out ออกจาก Mobile Banking Application ทุกครั้งหลังใช้งานเสร็จหรือไม่	50
4.8	แสดงร้อยละของกลุ่มตัวอย่างว่ามีการดูชื่อผู้พัฒนา Mobile Banking Application ก่อนการดาวน์โหลดหรือไม่	53
4.9	แสดงร้อยละของกลุ่มตัวอย่างว่ากล้าหรือไม่ที่จะบอกรหัสผ่าน Mobile Banking Application ให้กับคนในครอบครัว	56
4.10	แสดงร้อยละของกลุ่มตัวอย่างว่ามีการจดรหัสผ่านเข้าใช้งาน Mobile Banking Application ไว้บนโทรศัพท์มือถือหรือเศษกระดาษหรือไม่	59
4.11	แสดงร้อยละของกลุ่มตัวอย่างเรื่องความคิดเห็นของวิธีการยืนยันตัวตนเพื่อ log in เข้าใช้งาน Mobile Banking Application ที่เหมาะสม	61
4.12	แสดงร้อยละของกลุ่มตัวอย่างเรื่องความคิดเห็นของวิธีการยืนยันตัวตนในกรณียืนยันรายการธุรกรรมที่ทำผ่าน Mobile Banking Application	63
4.13	แสดงร้อยละของกลุ่มตัวอย่างเรื่องความคิดเห็นของวิธีการยืนยันตัวตนในกรณี log in และกรณียืนยันรายการธุรกรรมที่ทำผ่าน Mobile Banking Application ว่าควรเป็นวิธีการเดียวกันหรือไม่	65

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทต่อการดำเนินชีวิตประจำวันของคนในสังคม ก่อให้เกิดความสะดวกสบายในการใช้ชีวิต ซึ่งในหลายหน่วยงานทั้งภาครัฐและเอกชน ทั้งในแวดวงธุรกิจ อุตสาหกรรม การบริการ หรือแม้กระทั่งด้านการศึกษาต่างก็นำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ เพื่อให้เกิดประเกิดประสิทธิภาพ นับตั้งแต่การผลิต การจัดเก็บ การประมวลผล การเรียกใช้และการสื่อสารสารสนเทศ

ภาคธนาคารถือเป็นอีกหนึ่งธุรกิจที่มีการปรับตัวรับกับ disruptive technology ที่กำลังเกิดขึ้นอย่างรวดเร็วโดยเฉพาะอย่างยิ่งจากเทคโนโลยีสารสนเทศ หลังจากที่การใช้อินเทอร์เน็ตเป็นที่แพร่หลายของคนในสังคมประกอบกับจำนวนผู้ใช้สมาร์ทโฟนเพื่อเข้าถึงอินเทอร์เน็ตมีสัดส่วนค่อนข้างสูง หรือคิดเป็นร้อยละ 93.7 เมื่อเทียบกับการใช้คอมพิวเตอร์พีซี (ร้อยละ 45.4) โน้ตบุ๊ค (ร้อยละ 20.8) และแท็บเล็ต (ร้อยละ 10.2) (ภุชพงค์ โนดโธสง, 2561) จึงทำให้เกิดการบริการด้านธุรกรรมทางการเงินบนโทรศัพท์มือถือ

สำหรับประเทศไทยการให้บริการทางการเงินผ่านโทรศัพท์เคลื่อนที่เกิดขึ้นครั้งแรกในปีพ.ศ. 2543 เป็นการร่วมมือกันระหว่างธนาคารกสิกรไทยและดีแทค โดยใช้ SMS ในการทำรายการภายใต้ชื่อ “TFB e-Mobile Banking” ซึ่งให้บริการได้เฉพาะการสอบถามยอดเงินคงเหลือในบัญชีและการโอนเงินระหว่างบัญชี โดยผู้ใช้บริการจะต้องพิมพ์รหัสของธุรกรรมแต่ละประเภทส่งข้อมูลไปยังระบบของธนาคาร แต่ไม่ค่อยได้รับความนิยมเพราะรหัสการทำธุรกรรมแต่ละประเภทมีอักษรที่ยาวทำให้เป็นอุปสรรคต่อการใช้งาน ต่อมาในปี พ.ศ. 2545 มีการพัฒนาการให้บริการอีกครั้งในรูปแบบของ WAP (Wireless Application Protocol) แต่ก็ยังไม่เป็นที่นิยมเนื่องจากระบบการประมวลผลช้าและมีข้อจำกัดของรุ่นมือถือที่รองรับการใช้งานดังกล่าว รวมถึงผู้ใช้บริการยังขาดความเชื่อมั่นในระบบรักษาความปลอดภัยของบริการนี้ และในปี พ.ศ. 2551 การให้บริการทางการเงินผ่านโทรศัพท์เคลื่อนที่ได้ถูกนำมาพัฒนาและเสนอให้กับผู้บริโภคภายในประเทศอีกครั้งตอบรับกับกระแสความนิยมของการใช้โทรศัพท์มือถือของคนไทย ในขณะที่การให้บริการธุรกรรมทางการเงินที่สะดวก รวดเร็ว ครบวงจร และปลอดภัยเป็นหัวใจของธุรกิจธนาคาร จึงเกิดการพัฒนา

รูปแบบการให้บริการทางการเงินรูปแบบใหม่ผ่านทาง Mobile Banking Application ที่มีฟังก์ชั่นการใช้งานที่ง่ายขึ้น สะดวกและรวดเร็วขึ้น มีความสอดคล้องกับวิถีชีวิตในยุคปัจจุบัน ซึ่งผู้ใช้บริการสามารถทำธุรกรรมการเงินผ่าน Mobile Banking Application ได้แก่ การเข้าถึงบัญชีเงินฝากธนาคาร โดยผู้ใช้สามารถทำธุรกรรมได้หลายประเภทเช่นโอนเงิน ตรวจสอบยอดเงินคงเหลือซื้อขายกองทุน การชำระค่าสินค้าและบริการกับร้านค้าออนไลน์ เป็นต้น

จากข้อมูลของธนาคารแห่งประเทศไทย ณ กันยายน พ.ศ. 2560 พบว่ามีผู้ใช้งานผ่าน Mobile Banking จำนวนถึง 28 ล้านคน โดยส่วนใหญ่จะกระจุกตัวอยู่กับธนาคารพาณิชย์ขนาดใหญ่ ได้แก่ ธนาคารกสิกรไทย (K-Plus) จำนวนสูงสุดที่ 7.3 ล้านคน ตามมาด้วย ธนาคารไทยพาณิชย์ (SCB EASY) จำนวน 6.5 ล้านคน และธนาคารกรุงไทย ธนาคารกรุงเทพ ธนาคารทีเอ็มบี และธนาคารกรุงศรีอยุธยา ตามลำดับ โดยที่ธนาคารพาณิชย์ 4 ลำดับแรกมีส่วนแบ่งการตลาดสูงถึงร้อยละ 85 ของผู้ใช้งานทั้งประเทศ

อย่างไรก็ตามในช่วงที่ผ่านมาได้มีเหตุการณ์ที่กระทบความเชื่อมั่นของผู้ใช้งานเช่นข่าวเรื่องการถูกแฮกระบบ Mobile Banking จากกลุ่มมิจฉาชีพเกิดขึ้น เป็นต้น ซึ่งความปลอดภัยของการทำธุรกรรมทางการเงินผ่าน Mobile Banking Application ถือเป็นปัจจัยสำคัญที่ส่งผลต่อความพึงพอใจของผู้บริโภค สรุปได้จากงานวิจัยของ ทิพย์สุดา หมื่นหาญ (2547) ได้ศึกษาถึงปัจจัยที่มีผลต่อการตัดสินใจในการเลือกใช้ธนาคารผ่านอินเทอร์เน็ต พบว่าสิ่งที่ผู้บริโภคให้ความสำคัญเป็นลำดับแรกคือความปลอดภัยในการใช้งาน ในขณะที่วรางรัตน์ ขันคำ (2553) ได้ทำการศึกษาเรื่องการรับรู้ความเสี่ยงและปัจจัยส่วนประสมทาง การตลาด ที่มีความสำคัญต่อการตัดสินใจใช้บริการธนาคารบนอินเทอร์เน็ต เห็นว่ามีกลุ่มที่ยังไม่เริ่มใช้บริการ Mobile Banking Application เนื่องจากเหตุผลเรื่องความไม่มั่นใจในความปลอดภัยของบริการดังกล่าว

เพื่อที่จะเข้าใจความเห็นของ Generation C ในประเทศไทยมากยิ่งขึ้นในประเด็นเรื่องความปลอดภัยของ Mobile Banking Application ที่ให้บริการโดยธนาคารพาณิชย์ในประเทศไทยจึงเป็นที่มาของการศึกษาในครั้งนี้ โดยสำรวจระดับความเชื่อมั่นที่มีต่อระบบความปลอดภัยของ Mobile Banking Application ความรู้ของตัวผู้ใช้งานเอง รวมถึงขั้นตอนสำคัญที่เกี่ยวกับปลอดภัยในการใช้งานนั่นคือระบบการยืนยันตัวตน

1.2 คำถามงานวิจัย

1. ผู้ใช้บริการมีระดับความเชื่อมั่นในเรื่องความปลอดภัยในการใช้งาน Mobile Banking Application มากน้อยเพียงใด

2. ผู้ใช้บริการมีความรู้ความเข้าใจในเรื่องการใช้ Mobile Banking Application ในการทำธุรกรรมทางการเงินอย่างปลอดภัยมากน้อยเพียงใด และปกติได้ปฏิบัติตามอย่างเคร่งครัดหรือไม่

3. ผู้ใช้งานเห็นว่าระบบการยืนยันตัวตนบน Mobile Banking Application รูปแบบใดเหมาะสมที่สุด เพราะเหตุใด

1.3 วัตถุประสงค์งานวิจัย

1. เพื่อทราบถึงระดับความเชื่อมั่นในเรื่องความปลอดภัยในการใช้งาน Mobile Banking Application

2. เพื่อทราบถึงระดับความรู้ความเข้าใจของผู้ใช้บริการ Mobile Banking Application ในการทำธุรกรรมทางการเงินอย่างปลอดภัย และการนำไปปฏิบัติ

3. เพื่อเข้าใจความคิดเห็นและเหตุผลของผู้ใช้บริการเกี่ยวกับระบบการยืนยันตัวตนบน Mobile Banking Application

1.4 ขอบเขตงานวิจัย

ด้านประชากร ทำการศึกษาเฉพาะ Generation C ในประเทศไทยซึ่งเป็นผู้ที่ใช้งานเทคโนโลยีสมาร์ทโฟนและอินเทอร์เน็ตในชีวิตประจำวันและหมายรวมถึงการใช้งาน Mobile Banking Application ซึ่งไม่ได้จำกัดช่วงวัย

ด้านเนื้อหาจะมุ่งศึกษาเกี่ยวกับความคิดเห็นของกลุ่มตัวอย่าง Generation C ในประเด็นความปลอดภัยของ Mobile Banking Application ที่ให้บริการโดยธนาคารพาณิชย์ในประเทศไทย โดย โดยเป็นการศึกษาเชิงคุณภาพเพื่อทราบถึง 1) ความเชื่อมั่นของผู้ใช้งาน Mobile Banking Application ในด้านความปลอดภัย 2) ความรู้ความเข้าใจของผู้ใช้บริการ Mobile Banking Application ในการทำธุรกรรมอย่างปลอดภัยและการนำไปปฏิบัติ และ 3) ความคิดเห็นของผู้ใช้บริการการเกี่ยวกับระบบการยืนยันตัวตนบน Mobile Banking Application ที่เหมาะสม

ด้านการเก็บรวบรวมข้อมูล ดำเนินการสัมภาษณ์ในช่วงเดือน ตุลาคม – พฤศจิกายน 2561

1.5 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับจากการทำวิจัยเพื่อศึกษาความคิดเห็นที่เกี่ยวกับความปลอดภัยในการใช้บริการทำธุรกรรมผ่าน Mobile Banking Application ที่ให้บริการโดยธนาคารพาณิชย์ในประเทศ โดยสำรวจความคิดเห็นจากผู้ใช้บริการที่เป็น Generation C มีดังนี้

1. ผู้ประกอบการธนาคารพาณิชย์สามารถทราบถึงระดับความเชื่อมั่นของผู้ใช้บริาร Mobile Banking Application ในประเทศ เพื่อนำผลการวิจัยที่ได้ไปใช้ในการปรับปรุงและพัฒนาเทคโนโลยีในด้านความปลอดภัย เพื่อสามารถตอบโจทย์และเพิ่มระดับความเชื่อมั่นของผู้ใช้บริการได้ดียิ่งขึ้น

2. ผู้ประกอบการธนาคารพาณิชย์สามารถรับทราบถึงระดับความรู้ความเข้าใจของผู้ใช้บริการ Mobile Banking Application ในแง่ของการใช้งานอย่างปลอดภัย และสามารถระบุได้ว่าผู้ใช้งานส่วนใหญ่ขาดความรู้ความเข้าใจในเรื่องใดเพื่อที่จะสามารถรณรงค์ ประชาสัมพันธ์ ให้ผู้ใช้งานได้ตระหนักถึงความปลอดภัยในเรื่องดังกล่าวมากยิ่งขึ้น

3. ผู้ประกอบการธนาคารพาณิชย์สามารถประยุกต์ใช้ความคิดเห็นของผู้ใช้งานที่มีต่อวิธีการยืนยันตัวตนที่เหมาะสมในการทำธุรกรรม เพื่อใช้ในการพัฒนาระบบความปลอดภัยในการทำธุรกรรมผ่าน Mobile Banking Application ทั้งนี้การทำไปประยุกต์ใช้จริงจำเป็นต้องพิจารณาควบคู่กันกับระดับความปลอดภัยที่ธนาคารพาณิชย์สามารถยอมรับได้จากการใช้วิธีการดังกล่าว นโยบายเรื่องความปลอดภัยการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ ข้อจำกัดทางด้านเทคโนโลยี เป็นต้น

1.6 ประพจน์ (Proposition)

ในประเด็นความเชื่อมั่นในระบบความปลอดภัยของ Mobile Banking application นั้น คาดว่าประชากร Generation C ส่วนใหญ่ในประเทศจะค่อนข้างมีความเชื่อมั่นในระบบดังกล่าว จากการทบทวนวรรณกรรมเกี่ยวกับความเชื่อมั่นต่อ Mobile Banking นั้นเกิดจากสภาวะจิตใจที่จะทำไปสู่ความเต็มใจในการรับความเสี่ยงในการใช้งาน โดยที่ความเต็มใจนั้นจะยึดโยงกับความคาดหวังในการทำหน้าที่อย่างเต็มความสามารถของธนาคารพาณิชย์ ซึ่งหากกล่าวถึงสภาวะจิตใจผู้ใช้งานที่ยอมดาวน์โหลด Mobile Banking Application ลงบนโทรศัพท์มือถือนั้นต้องถือว่าได้เปิดใจในเบื้องต้นแล้ว แต่การที่จะพร้อมรับความเสี่ยงอย่างเต็มใจหรือไม่นั้นก็ขึ้นอยู่กับว่าธนาคารพาณิชย์ใน

อดีตและปัจจุบันมีการดำเนินงานโดยรัดกุมและรับผิดชอบต่อผู้ใช้งานมากน้อยแค่ไหน ซึ่งที่ผ่านมาจะพบว่าธนาคารพาณิชย์ในประเทศส่วนใหญ่จะให้ความสำคัญในเรื่องความปลอดภัยในการทำธุรกรรมผ่าน Mobile Banking Application ค่อนข้างมาก และหากเกิดปัญหาก็มิได้นิ่งนอนใจและพยายามหาวิธีการแก้ไขปัญหาและบรรเทาความเดือดร้อนให้กับผู้ใช้งานอย่างเร่งด่วน โดยมีหน่วยงานกำกับดูแลอย่าง ธปท. ในการควบคุมดูแลอย่างใกล้ชิดเพื่อสร้างความมั่นใจให้กับผู้ใช้งานสอดรับกับนโยบายรัฐบาล Thailand 4.0

ส่วนประเด็นความรู้ความเข้าใจของผู้ใช้งาน Mobile Banking Application อย่างปลอดภัยนั้น คาดว่าคนส่วนใหญ่จะมีความเข้าใจค่อนข้างดี เนื่องจากปัจจุบันสังคมได้มีการแชร์เรื่องราวเกี่ยวกับความปลอดภัยในการใช้งาน Mobile Banking ผ่านสื่อออนไลน์ในวงกว้างเพื่อสร้างความตระหนักและเตือนภัยให้กับคนในสังคม และผู้ที่ตัดสินใจใช้งาน Mobile Banking Application นั้น ส่วนใหญ่น่าจะมีความรู้พื้นฐานเกี่ยวกับคอมพิวเตอร์ อินเทอร์เน็ตพอสมควร จึงมีแนวโน้มสูงที่ผู้ใช้งานจะมีความรู้ความเข้าใจในเรื่องดังกล่าวในระดับค่อนข้างสูงแต่อาจไม่ปฏิบัติตามอย่างเคร่งครัดเนื่องจากคนส่วนใหญ่อาจยังไม่เคยมีประสบการณ์การถูกโจรกรรมข้อมูลมาก่อนเลยทำให้ไม่เกิดความระมัดระวังมากเท่าที่ควรจะเป็น

สำหรับวิธีการที่เหมาะสมในการยืนยันตัวตนทั้งในส่วนการ log in เข้าสู่ Mobile Banking Application และการยืนยันตัวตนอีกครั้งก่อนยืนยันรายการธุรกรรม จากการทบทวนวรรณกรรมเกี่ยวกับวิธีการยืนยันตัวตนในรูปแบบต่างๆ คาดว่าคนส่วนใหญ่น่าจะชอบวิธีการที่ไม่ซับซ้อนจนเกินไป และจะเลือก log in โดยวิธี Memorized Secret ที่เป็น password จำนวน 6 หลัก เนื่องจากสามารถเป็นเลขชุดเดียวกับบัตรเดบิตของหลายๆ ธนาคารซึ่งทำให้ง่ายต่อการจดจำ ส่วนการยืนยืนตัวตนอีกครั้งเพื่อยืนยันรายการธุรกรรมนั้นคาดว่าคนส่วนใหญ่จะเลือก Single-Factor One-Time Password Device โดยการใช้ OTP ที่ส่งมายังโทรศัพท์มือถือเพื่อใช้กรอกยืนยันธุรกรรมเนื่องจากมีความปลอดภัย ไม่จำเป็นต้องจดจำอะไรเพิ่มเติม อีกทั้งยังเป็นวิธีที่ใช้อย่างแพร่หลายในหลายๆ Mobile Banking Application ในปัจจุบัน

1.7 นิยามศัพท์

1. Mobile Banking Application เป็นโปรแกรมการใช้งานสำหรับการทำธุรกรรมของธนาคารผ่านโทรศัพท์เคลื่อนที่ ซึ่งผู้ใช้บริการต้องลงทะเบียนกับธนาคารเพื่อใช้บริการทางการเงินได้หลายประเภท เช่น การโอนเงินระหว่างบัญชีธนาคาร การตรวจสอบยอดบัญชี การซื้อขายตราสาร/ กองทุน และการตั้งระบบแจ้งเตือนอัตโนมัติ รวมถึงการทำธุรกรรมชำระเงินและชำระใบแจ้งหนี้ด้วย โดยในการทำธุรกรรมดังกล่าว จะทำผ่านระบบปฏิบัติการที่พัฒนาขึ้นเพื่อรองรับรับอุปกรณ์สื่อสาร เคลื่อนที่โดยเฉพาะ เช่น SMS USSD WAP M-banking application หรือเทคโนโลยีใหม่ที่จะถูกพัฒนาขึ้นในอนาคต (ธนาคารแห่งประเทศไทย, 2557)

2. Generation C กลุ่มนี้เป็นกลุ่มหรือคำใหม่ที่ Google และ Nielsen บัญญัติใช้สำหรับเรียกกลุ่มคนยุคใหม่ที่ไม่ได้แบ่งตามอายุเหมือนคนใน 7 Generation แบบเดิม หากแต่จัดกลุ่มตามพฤติกรรมการใช้โทรศัพท์มือถืออินเตอร์เน็ต และโซเชียลเน็ตเวิร์ก สำหรับคน Generation C นั้นจะมีนิสัยที่เห็นเด่นชัดมากๆ คือมีการเชื่อมต่อตลอดเวลา มีการอัพเดตข้อมูล สนใจข่าวสารที่ได้รับรู้มาในโลกไซเบอร์พร้อมจะแชร์ต่อทุกเมื่อ ติดตามดูคลิปในยูทูบมากกว่านั่งดูโทรทัศน์เหมือนกับสังคมออนไลน์กลายเป็นส่วนหนึ่งในชีวิตของตัวเองไปแล้วและคนกลุ่มนี้ก็ยังกลายเป็นผู้ขับเคลื่อนวัฒนธรรมใหม่ๆ ด้วย

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การศึกษาครั้งนี้ ผู้วิจัยได้มีการศึกษาบทความ ทฤษฎีและงานวิจัยที่เกี่ยวข้อง เพื่อให้เป็นไปตามวัตถุประสงค์ของงานวิจัย และขอบเขตของงานวิจัย โดยมีรายละเอียดดังนี้

2.1 นิยามความเชื่อมั่นภายใต้บริบท Mobile Banking

2.2 แนวนโยบายการเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่โดยธนาคารแห่งประเทศไทย

2.3 ความปลอดภัยของระบบมีผลต่อการตัดสินใจใช้ Mobile Banking Application

2.4 รูปแบบของภัยคุกคามสำหรับการใช้งาน Mobile Banking ในปัจจุบัน

2.5 การใช้งาน Mobile Banking อย่างปลอดภัย

2.6 ประเภทของสิ่งที่ใช้ยืนยันตัวตน (Credential type)

2.7 งานวิจัยที่เกี่ยวเนื่องกับความปลอดภัยของ Mobile Banking Application

2.1 นิยามความเชื่อมั่นภายใต้บริบท Mobile Banking

ความเชื่อมั่นเป็นเรื่องหนึ่งที่เกี่ยวข้องกับหลากหลายสาขาวิชา เช่น จิตวิทยา การจัดการ การเมือง และการสื่อสาร เป็นต้น อย่างไรก็ตาม คำนิยามความเชื่อมั่นนั้นไม่ว่าจะเป็นออนไลน์หรือออฟไลน์มีความหมายเข้าใจที่หลายหลายแตกต่างกันไป เนื่องด้วยความเชื่อมั่นถูกมองจากมุมมองที่แตกต่างกัน โดยนักวิจัย Gefen (2543) ให้นิยามความเชื่อมั่นว่าคือความเต็มใจที่จะทำธุรกรรมออนไลน์ในสถานการณ์ที่มีความเสี่ยง Pa and Pavlou (2545) ให้นิยามคำว่าความเชื่อมั่นว่าการที่บุคคลหนึ่งตัดสินใจเข้าทำธุรกรรมภายใต้สิ่งแวดล้อมที่มีความไม่แน่นอนอยู่ ในขณะที่ Yousafzai et al. (2546) ให้นิยามความเชื่อมั่นเกี่ยวกับธุรกรรมออนไลน์ว่าคือสภาวะจิตใจที่นำไปสู่ความเต็มใจของผู้ใช้บริการในการทำธุรกรรมทางอินเทอร์เน็ต โดยคาดหวังว่าธนาคารจะปฏิบัติหน้าที่อย่างเต็มที่ไม่ว่าผู้ใช้บริการเองจะมีความสามารถในการตรวจสอบและควบคุมการทำงานของธนาคารหรือไม่ก็ตาม

เนื่องจากการทำธุรกรรมผ่าน Mobile Banking Application ต้องใช้ข้อมูลที่มีความอ่อนไหวและมีเงินเข้ามาเกี่ยวข้อง ตัวผู้ใช้งานเองจะไม่เชื่อมั่นและใช้บริการดังกล่าวหากตนเองไม่เต็มใจที่จะรับความเสี่ยงของ Mobile Banking Application รวมถึงหากคาดการณ์ว่า Mobile Banking Application ดังกล่าวจะไม่สามารถงานได้อย่างเต็มที่และสมบูรณ์ ด้วยเหตุผลดังกล่าว การศึกษาในครั้งนี้จะประยุกต์ใช้นิยามของ Yousafzai et al. (2546) เรื่องความเชื่อมั่นในการทำธุรกรรมออนไลน์ โดยจะนำมาใช้กับ Mobile Banking โดยที่นิยามดังกล่าวจะเน้นถึงสิ่งสำคัญสามเรื่องได้แก่

1. สภาวะจิตใจ

2. สภาวะจิตใจในข้างต้นจะนำไปสู่ความเต็มใจของผู้ใช้บริการที่จะรับความเสี่ยงโดยการเข้าทำธุรกรรมออนไลน์ผ่าน Mobile Banking Application

3. ความเต็มใจดังกล่าวจะขึ้นอยู่กับความคาดหวังว่าธนาคารจะปฏิบัติหน้าที่ได้อย่างเต็มที่และสมบูรณ์

2.2 แนวนโยบายการเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่โดยธนาคารแห่งประเทศไทย

เนื่องด้วยปัจจุบันแนวโน้มการทำธุรกรรมผ่าน Mobile Banking ได้เติบโตอย่างต่อเนื่องและมีการพัฒนาเป็นช่องทางสำคัญในการชำระเงินในอนาคต อย่างไรก็ตามสิ่งที่ส่งผลต่อจำนวนผู้ใช้บริการการชำระเงินโดยอุปกรณ์เคลื่อนที่คือความเชื่อมั่นต่อระบบความปลอดภัยและกระบวนการให้บริการ และธนาคารแห่งประเทศไทย (ธปท.) พบข้อร้องเรียนของผู้ใช้งานจำนวนมากเกี่ยวกับการทำทุจริตที่อาศัยช่องโหว่หรือความไม่รัดกุมของกระบวนการให้บริการเพิ่มมากขึ้นตลอดจนภัยคุกคามทางไซเบอร์ที่นับวันจะมีความซับซ้อนและยากต่อการตรวจจับมากยิ่งขึ้น ทำให้การชำระเงินโดยอุปกรณ์เคลื่อนที่มีความเสี่ยงเพิ่มขึ้นต่อตัวผู้ใช้งาน

ธปท. จึงเห็นควรให้มีแนวนโยบาย เรื่อง การเสริมสร้างความเชื่อมั่น การชำระเงินโดยอุปกรณ์เคลื่อนที่ (Guiding Principles for Trusted Mobile Payments) เพื่อให้ผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์โดยอุปกรณ์เคลื่อนที่ (Mobile Payment Service Providers) ใช้เป็นแนวทางถือปฏิบัติในการยกระดับและสร้างมาตรฐานที่ดีของการให้บริการเพื่อให้ผู้ใช้บริการเกิดความมั่นใจและใช้ช่องทางการชำระเงินโดยอุปกรณ์เคลื่อนที่เพิ่มมากขึ้น แนวนโยบายนี้ประกอบด้วยหลักการ 6 ข้อ

หลักการที่ 1 การบริหารจัดการความเสี่ยงของผู้ให้บริการ (Risk Management) เพื่อให้ผู้ให้บริการการชำระเงินโดยอุปกรณ์เคลื่อนที่มีกระบวนการบริหารความเสี่ยงที่ครอบคลุมความ

เสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ความเสี่ยงด้านไซเบอร์ และความเสี่ยงด้านปฏิบัติการ

หลักการที่ 2 การพิสูจน์ตัวตนอย่างรัดกุม (Secure Authentication) เพื่อสร้างความเชื่อถือในการทำธุรกรรม (Trusted Relationship) โดยพิสูจน์ว่าผู้รับ หรือผู้ส่งข้อมูลธุรกรรมการชำระเงินนั้นเป็นผู้มีสิทธิ์ในการทำธุรกรรม เพื่อให้มั่นใจได้ว่าธุรกรรมนั้นไม่ได้ทำโดยบุคคลอื่นมาแอบอ้างและสวมรอยเป็นผู้ใช้บริการ (Identity Theft) โดยการพิสูจน์ตัวตนควรใช้หลายองค์ประกอบร่วมกัน (Multifactor Authentication) อย่างน้อย 2 องค์ประกอบ (Two-Factor Authentication) จากองค์ประกอบเหล่านี้ (1) องค์ประกอบสิ่งที่รู้ (What You Know) เช่น Personal Identification Number (PIN) รหัสผ่าน (Password) (2) องค์ประกอบสิ่งที่มี (What You Have) เช่น ตัวอุปกรณ์เคลื่อนที่ เครื่องโทรศัพท์มือถือ ใบรับรองอิเล็กทรอนิกส์ อุปกรณ์ Token (3) องค์ประกอบสิ่งที่เป็น (What You Are) เช่น ข้อมูลทางชีวภาพ ลายนิ้วมือ ลายม่านตา หรือน้ำเสียง

หลักการที่ 3 การคุ้มครองและการให้ความรู้แก่ผู้ใช้บริการ (Consumer Protection and Consumer Education) เพื่อคุ้มครองผู้ใช้บริการจากความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานอุปกรณ์เคลื่อนที่ในการทำธุรกรรมการชำระเงิน โดยรวมถึงการป้องกันการทำธุรกรรมการชำระเงินที่ไม่สมเหตุสมผล และเพื่อคุ้มครองข้อมูลสำคัญซึ่งไม่พึงเปิดเผยของผู้ใช้บริการ

หลักการที่ 4 การเปิดกว้างและส่งเสริมให้มีการใช้งานระหว่างกันได้ (Openness and Interoperability) เพื่อให้ธุรกิจให้บริการการชำระเงินเกิดการแข่งขันอย่างเป็นธรรม รวมทั้งเปิดกว้างให้ ผู้ใช้บริการเลือกผู้ให้บริการได้อย่างเสรี

หลักการที่ 5 การป้องกันและการปราบปรามการฟอกเงินและการสนับสนุนทางการเงินแก่การก่อการร้าย และการป้องกันการทุจริต (Anti-Money Laundering, Combating Financing Terrorism, and Fraud Protection)

หลักการที่ 6 การคำนึงถึงประสบการณ์การใช้งานของผู้ใช้บริการ (User Experience) เพื่อสร้างประสบการณ์ที่ดีในการใช้บริการการชำระเงินโดยอุปกรณ์เคลื่อนที่ ซึ่งจะช่วยเพิ่มสัดส่วนการชำระเงินผ่านช่องทางอิเล็กทรอนิกส์และลดปริมาณการใช้เงินสดลง

โดยการศึกษาในครั้งนี้นอกจากจะวัดระดับความเชื่อมั่นของผู้ใช้งาน Mobile Banking Application ในภาพรวมแล้ว ยังมุ่งศึกษาระบบการยืนยันตัวตนที่เหมาะสมในมุมมองของผู้ใช้งานซึ่งตรงกับหลักการที่ 2 รวมถึงศึกษาระดับความรู้ความเข้าใจเกี่ยวกับความปลอดภัยในการใช้ Mobile Banking Application ของผู้ใช้งาน เพื่อนำไปประยุกต์ใช้ในการให้ความรู้กับผู้ใช้บริการซึ่งตรงกับหลักการที่ 3 ของแนวนโยบายการเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่ (Guiding Principles for Trusted Mobile Payments) ของ ธปท.

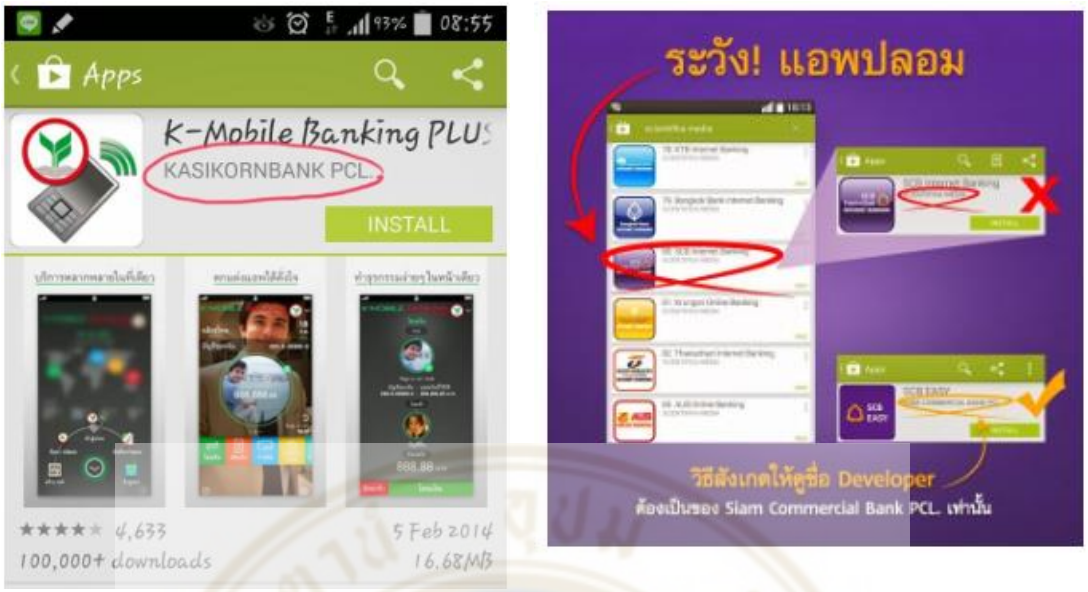
2.3 ความปลอดภัยของระบบมีผลต่อการตัดสินใจใช้ Mobile Banking Application

ความปลอดภัยของการทำธุรกรรมทางการเงินผ่าน Mobile Banking Application เป็นปัจจัยที่สำคัญและส่งผลต่อความพึงพอใจของผู้บริโภค เห็นได้จากการศึกษาเรื่องปัจจัยการใช้ธนาคารบนมือถือผ่านเทคโนโลยีโครงข่ายสื่อสาร 3G กรณีศึกษา ธนาคาร ไทยพาณิชย์ จำกัด (มหาชน) ของสามารถ แสนภิบาล (2553) พบว่ากลุ่มตัวอย่างให้ความสำคัญใน เรื่องความปลอดภัยและความเป็นส่วนตัวมากที่สุด สอดคล้องกับงานวิจัยของ สุวิสา รังสิมันต์กุล (2551) ที่ศึกษาความพึงพอใจของผู้ใช้บริการธนาคารทางอินเทอร์เน็ตของธนาคารไทยพาณิชย์ จำกัด (มหาชน) ในเขตอำเภอเมือง จังหวัดเชียงใหม่ พบว่าปัจจัยด้านผลิตภัณฑ์ ได้แก่ คุณภาพ ความถูกต้อง และความปลอดภัยส่งผลต่อความพึงพอใจของผู้บริโภคอย่างมีนัยสำคัญทางสถิติ และงานวิจัยของ ทิพย์สุดา หมื่นหาญ (2547) ได้ศึกษาถึงปัจจัยที่มีผลต่อการตัดสินใจในการเลือกใช้ธนาคารผ่าน อินเทอร์เน็ต พบว่า ความปลอดภัยในการใช้บริการเป็นปัจจัยที่ผู้บริโภคให้ความสำคัญเป็นอันดับแรก ซึ่งวราง รัตน์ ขันคำ (2553) ได้ทำการศึกษาเรื่องการรับรู้ความเสี่ยงและปัจจัยส่วนประสมทางการตลาด ที่มีความสำคัญต่อการตัดสินใจใช้บริการธนาคารบนอินเทอร์เน็ต พบว่ายังมีผู้บริโภค บางกลุ่มยังไม่ใช้บริการ Mobile Banking Application เพราะสาเหตุมาจากความไม่มั่นใจในความปลอดภัยของบริการ

2.4 รูปแบบของภัยคุกคามสำหรับการใช้งาน Mobile Banking ในปัจจุบัน

ภัยคุกคามด้านความปลอดภัยที่เกี่ยวกับ Mobile Banking สามารถแบ่งได้เป็น 2 ประเภทคือ ภัยคุกคามประเภท Non-technical เช่น การปลอมแปลงเอกสารเพื่อสมัครใช้บริการ Mobile Banking หรือการลักลอบหรือล่อลวงเพื่อให้ได้มาซึ่งข้อมูลส่วนตัวของผู้อื่น และอีกประเภทคือภัยคุกคามแบบ Technical

ภัยคุกคามแบบ Technical สามารถสร้างความเสียหายในวงกว้างได้อย่างรวดเร็ว ในปัจจุบันกลุ่มมิจฉาชีพได้มีการพัฒนารูปแบบการกระทำผิดที่หลากหลาย ตัวอย่างเช่น การสร้าง Mobile Banking Application เลียนแบบของธนาคารพาณิชย์ ทำให้เข้าใจผิดว่า Application ซึ่งอยู่บน store ของระบบปฏิบัติการโทรศัพท์มือถือเป็นของจริง โดยมีจุดประสงค์เพื่อดักจับข้อมูลทางการเงิน จุดสังเกตคือให้ดูที่ชื่อ Developer ว่าเป็นธนาคารพาณิชย์หรือไม่ ดังภาพที่ 2-1



ภาพที่ 2.1 วิธีการสังเกต Mobile Banking Application ที่เป็นของจริง

อีกวิธีการหนึ่งคือการดักจับข้อมูลผ่าน Rouge WIFI วิธีการคือ มิจฉาชีพจะใช้อุปกรณ์ปล่อยสัญญาณพร้อมกับตั้งชื่อเหมือน WIFI ของสถานที่ดังกล่าว เช่น ชื่อร้านค้า เมื่อผู้ใช้งานกดเชื่อมต่อ มิจฉาชีพก็สามารถดูดข้อมูล username และ password ที่ใช้งานอยู่ได้เพื่อนำไปใช้หาผลประโยชน์ต่อไป สำหรับวิธีป้องกันที่ทำได้ฟรีคือการดาวน์โหลดโปรแกรม SSL STRIP Guard เพื่อตรวจสอบดูว่าโทรศัพท์มือถือถูกแฮกหรือไม่ โดยจะขึ้นสถานะว่า Pass หรือ Warning

โทรศัพท์มือถือที่ทำการ Jailbreak เพื่อให้ iPhone สามารถติดตั้งโปรแกรมอื่นๆ ได้นอกเหนือจาก App Store ถือว่าเป็นการเปิดช่องทาให้แฮกเกอร์โจรกรรมข้อมูลได้ง่ายยิ่งขึ้น โดยจะนำข้อมูลความลับส่วนตัวของผู้ใช้งานไปขายต่อ หรือนำไปหาผลประโยชน์เอง หากเป็น username และ password ของธนาคารพาณิชย์ในการเข้าใช้งาน Mobile Banking Application ก็มักเข้าเข้าไปเปลี่ยน password และทำการโอนเงิน

อีกวิธีการหนึ่งคือการปล่อยมัลแวร์เข้าสู่โทรศัพท์มือถือ ซึ่งพฤติกรรมเสี่ยงที่จะทำให้ผู้ใช้งานติดมัลแวร์โดยไม่รู้ตัว อาทิเช่น การดาวน์โหลดซอฟต์แวร์ฟรีจากอินเทอร์เน็ตที่มีมัลแวร์แฝงอยู่ การเข้าชมเว็บไซต์ที่ติดเชื้อมัลแวร์ การคลิกข้อความแสดงข้อความผิดพลาดหรือหน้าต่างป๊อบอัพปลอมซึ่งเป็นการดาวน์โหลดมัลแวร์หรือการเปิดไฟล์แนบอีเมลที่มาพร้อมกับมัลแวร์ โดยที่ Symantec ได้ออกมาเปิดเผยถึงมัลแวร์ชนิดใหม่บนระบบปฏิบัติการ Android ที่สามารถดักจับ One-time Passcode (OTP) ซึ่งเป็นระบบป้องกันการทำธุรกรรมออนไลน์ที่สำคัญ

การศึกษาวิจัยมาตรการการรักษาความมั่นคงปลอดภัยระบบ Internet Banking และ Mobile Banking ในประเทศไทยโดย ACIS Cyber LAB ดำเนินการสำรวจในระหว่างวันที่ 1-31 มกราคม 2556 และมีการให้คะแนนด้านความมั่นคงปลอดภัย (Scoring) และพบว่าระบบส่วนใหญ่ยังขาดมาตรการที่จำเป็นต่อการรับมือกับภัยคุกคามที่เกิดขึ้นในปัจจุบัน ได้แก่

1. การให้ความรู้หรือข้อแนะนำในการรักษาความมั่นคงปลอดภัยให้กับผู้ใช้งาน หรือการจัดหา Anti-MalWare software ให้การทำธุรกรรมมีความมั่นคงปลอดภัย

2. การตรวจจับการถูกถอดรหัส SSL โดยโปรแกรม SSLStrip

3. อายุการใช้งานของ One Time Password (OTP) ลักษณะของการเรียกใช้ One Time Password (OTP) (เฉพาะการเพิ่มบัญชีผู้ใช้งาน หรือ ในทุกๆ ธุรกรรม)

4. การแสดงชื่อเจ้าของบัญชีที่จะโอนเงินเข้าในข้อความเดียวกับรหัส OTP ทั้งธนาคารเดียวกันและต่างธนาคาร

5. การสร้าง Link แบบ Dynamic Path ในส่วนที่มีการเรียกใช้ One Time Password (OTP) เพื่อป้องกันแฮกเกอร์นำ Static Link ไป Hardcode ในโทรจันหรือมัลแวร์

2.5 การใช้งาน Mobile Banking อย่างปลอดภัย

ผู้ใช้งาน Mobile Banking ควรเข้าใจถึงข้อพึงปฏิบัติและข้อพึงระวังเพื่อลดโอกาสในการตกเป็นเป้าหมายของกลุ่มมิจฉาชีพในการโจรกรรมข้อมูลสำคัญซึ่งจะก่อให้เกิดความเสียหายตามมา ซึ่งหากเข้าใช้งาน Mobile Banking Application ด้วย username และ password ก็ควรตั้ง password ที่ปลอดภัยยากต่อการคาดเดามีความยาวอย่างน้อย 8 ตัวอักษรผสมด้วยตัวอักษรใหญ่หรือเล็ก ตัวเลข สัญลักษณ์พิเศษ โดยที่ไม่บอกรหัสให้ผู้อื่นทราบแม้แต่คนใกล้ชิด ไม่เก็บ username และ password ไว้บนโทรศัพท์มือถือ ไม่ jailbreak เครื่อง ไม่คลิกลิงค์จาก Email หรือ SMS ที่ดูเหมือนว่าจะส่งมาจากธนาคารพาณิชย์หรือแหล่งที่ไม่น่าเชื่อถือ โหลด Mobile Banking Application จาก Developer ที่เป็นชื่อธนาคารพาณิชย์ที่ถูกต้อง หลีกเลี่ยงการเชื่อมต่อ WIFI สาธารณะในการทำธุรกรรม และเมื่อใช้งานเสร็จต้องทำการ Log out ออกจาก Mobile Banking Application ด้วยทุกครั้ง

การทำธุรกรรมทางการเงินบนโทรศัพท์มือถือใน 2 ช่องทางซึ่งได้แก่ การใช้บริการผ่านเว็บไซต์บนโทรศัพท์ (Mobile Web) และ การใช้บริการผ่านแอพพลิเคชั่นบนโทรศัพท์ (Mobile Client Application หรือ Mobile Banking Application) นั้น จะพบว่า Mobile Banking Application

จะได้เปรียบทั้งในแง่ความปลอดภัยต่อผู้ใช้งาน ความง่ายในการใช้งาน และความสวยงาม ดังตารางที่ 2.1

ตารางที่ 2.1 เปรียบเทียบช่องทางการทำธุรกรรมทางการเงินบนโทรศัพท์มือถือ

ประเภท	มีอยู่ทั่วไป	ง่ายต่อการใช้	ปลอดภัย	สวยงาม
Mobile Web	◑	◑	◑	◕
Mobile Client Application	○	◕	●	●

● แข็งมาก ◕ แข็ง ◑ ปานกลาง ◔ อ่อน ○ อ่อนมาก

ที่มา: Mobile Banking Association (2009)

2.6 ประเภทของสิ่งที่ใช้ยืนยันตัวตน (Credential type)

ในการยืนยันตัวตนทางอิเล็กทรอนิกส์ ผู้ให้บริการสิ่งที่ใช้ยืนยันตัวตนจะสร้างวิธีการ (Mechanism) ที่จะสามารถระบุเอกลักษณ์ที่สามารถเชื่อมโยงไปยังข้อมูลประจำตัวของสมาชิกแต่ละคนที่ถูกต้อง โดยใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่ต่างกันตามระดับความน่าเชื่อถือที่กำหนดไว้ สิ่งที่ใช้ยืนยันตัวตนสามารถแบ่งออกเป็น 3 ประเภทตามปัจจัยที่ใช้ในการยืนยันตัวตน (Authentication Factor) ดังนี้ (National Institute of Standards and Technology, 2017)

1. สิ่งที่คุณรู้ (Something you know) คือข้อมูลที่สมาชิกเท่านั้นที่ทราบ เช่น รหัสผ่าน (Password) และเลขรหัสส่วนตัว (PIN) เป็นต้น

2. สิ่งที่คุณมี (Something you have) คือสิ่งของที่สมาชิกเท่านั้นที่มีอยู่ในครอบครอง เช่น บัตรประจำตัว (ID Card) หนังสือเดินทาง (Passport) อุปกรณ์ที่บรรจุสิ่งที่ใช้ยืนยันตัวตน และกุญแจการเข้ารหัสลับ (Cryptographic Key) เป็นต้น

3. สิ่งที่คุณเป็น (Something you are) คือข้อมูลทางชีวภาพของสมาชิกเช่น ลายนิ้วมือ หน้า ม่านตา เสียง เป็นต้น

ประเภทปัจจัยในการยืนยันตัวตน (Authentication factor) จะมีความปลอดภัยและเข้มงวด (Strength) ที่แตกต่างกัน ความปลอดภัยของระบบการยืนยันตัวตนจะขึ้นอยู่กับจำนวนชนิดของปัจจัยในการยืนยันตัวตนที่ใช้ประกอบกันเพื่อยืนยันตัวตน วิธีการยืนยันตัวตนโดยใช้ประเภทของปัจจัยในการยืนยันตัวตนแบ่งเป็น 2 แบบ ได้แก่

1. การยืนยันตัวตนแบบปัจจัยเดี่ยว (Single-factor authentication) เป็นการยืนยันตัวตนที่ใช้ สิ่งที่ใช้ยืนยันตัวตนเพียง 1 ปัจจัย เช่น การใช้ชื่อผู้ใช้งานและรหัสผ่านในการเข้าระบบ ซึ่งรหัสผ่านเป็นสิ่งที่คุณรู้ (Something You Know)

2. การยืนยันตัวตนแบบหลายปัจจัย (Multi-factor authentication) เป็นการยืนยันตัวตนที่ใช้ ปัจจัยตั้งแต่ 2 ปัจจัยขึ้นไปเพื่อเพิ่มความน่าเชื่อถือในการยืนยันตัวตนแต่ละครั้ง เช่น การใช้บัตรเอทีเอ็ม (ATM Card) ในการถอนเงินสดจากตู้เอทีเอ็ม ซึ่งบนบัตรเอทีเอ็มจะมีชิพ (Chip) ที่ฝังกุญแจส่วนตัว (Private Key) ของเอนทิตีอยู่ ดังนั้นเมื่อเอนทิตีต้องการถอนเงินสด เอนทิตีจะต้องเสียบบัตรเอทีเอ็มเข้ากับตู้เอทีเอ็ม และใส่เลขรหัสส่วนตัว (PIN) เพื่อไปเปิดใช้งานกุญแจส่วนตัวที่ฝังอยู่ในบัตรเอทีเอ็มนั้นเพื่อใช้ยืนยันตัวตนอีกครั้งหนึ่ง ดังนั้นบัตรเอทีเอ็มเป็นสิ่งที่คุณมี และเลขรหัสเป็นสิ่งที่คุณรู้ ประกอบกันเพื่อใช้ยืนยันตัวตน

มาตรฐาน National Institute of Standards and Technology (NIST) 800-63-2 อธิบายชนิดของสิ่งที่ใช้ในการยืนยันไว้ 9 ชนิด โดยสิ่งที่ใช้ยืนยันตัวตนแต่ละชนิดจะสามารถรองรับระดับความน่าเชื่อถือได้แตกต่างกันโดยสามารถแบ่งออกได้เป็นระดับ 1 ถึง 4 ดังตารางที่ 2-2 และ 2-3

ตารางที่ 2.2 ระดับความน่าเชื่อถือ (Levels of assurance)

ระดับความน่าเชื่อถือ (LoA)	**รายละเอียด**
ระดับ 1 (ต่ำ)	ไม่มีความน่าเชื่อถือหรือมีความน่าเชื่อถือเล็กน้อยในข้อมูลประจำตัวที่ใช้ยืนยันหรืออ้างสิทธิ์
ระดับ 2 (ปานกลาง)	มีความน่าเชื่อถือพอสมควรในข้อมูลประจำตัวที่ใช้ยืนยันหรืออ้างสิทธิ์
ระดับ 3 (สูง)	มีความน่าเชื่อถือสูงในข้อมูลประจำตัวที่ใช้ยืนยันหรืออ้างสิทธิ์
ระดับ 4 (สูงมาก)	มีความน่าเชื่อถือสูงมากในข้อมูลประจำตัวที่ใช้ยืนยันหรืออ้างสิทธิ์

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ

ชนิดของสิ่งที่ยืนยันตัวตน	**รายละเอียด**	**ระดับความน่าเชื่อถือ**	**ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน**	**ข้อกำหนดของผู้ตรวจสอบ**
Memorized Secret	(1) เป็นข้อมูลความลับ (Secret) ที่ตกลงกันระหว่างสมาชิกและผู้	1	(1) รหัสผ่าน (Password) อย่างน้อย 6 ตัวอักษร	จำกัดจำนวนความพยายามในการยืนยันตัวตน

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	ให้บริการสิ่งที่ใช้ยืนยันตัวตน (2) มีลักษณะเป็นตัวอักษรหรือตัวเลข เช่น รหัสผ่าน (Password) หรือเลขรหัสส่วนตัว (PIN) ถูกใช้แสดงต่อผู้ตรวจสอบในขั้นตอนการยืนยันตัวตน (3) จัดอยู่ในประเภทสิ่งที่คุณรู้ (Something You Know)		(ผู้ใช้เลือกมาจากชุดตัวอักษรที่ประกอบด้วยอย่างน้อย 90 ตัวอักษร) หรือ (2) เลขรหัสส่วนตัว (PIN) ที่ถูกสร้างแบบสุ่มอย่างน้อย 4 ตัว (Digit)	ที่ล้มเหลวด้วยบัญชีสมาชิกผู้ใช้ 100 ครั้งภายใน 30 วัน และทำการล็อคบัญชีสมาชิกผู้ใช้เมื่อเกินจำนวนที่กำหนด
		2	(1) รหัสผ่าน (Password) อย่างน้อย 8 ตัวอักษร (ผู้ใช้เลือกมาจากชุดตัวอักษรที่ประกอบด้วยอย่างน้อย 90 ตัวอักษร) หรือ (2) เลขรหัสส่วนตัว (PIN) ที่ถูกสร้างแบบสุ่มอย่างน้อย 6 ตัว (digit) (3) ผู้ให้บริการสิ่งที่ใช้ยืนยันตัวตนจะต้องมีกฎ	จำกัดจำนวนความพยายามในการยืนยันตัวตนที่ล้มเหลวด้วยบัญชีสมาชิกผู้ใช้ 100 ครั้งภายใน 30 วัน และทำการล็อคบัญชีสมาชิกผู้ใช้เมื่อเกินจำนวนที่กำหนด

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
			ข้อบังคับในการสร้างข้อมูลความลับ (Secret)	
Pre-Registered Knowledge	(1) เป็นสิ่งที่ใช้ยืนยันตัวตนที่มีลักษณะของคำถามคำตอบโดยการถามคำถามที่เป็นความลับและรอคำตอบจากผู้อ้างสิทธิ์ (Claimant) เพื่อยืนยันตัวตน (2) คำถามจะถูกกำหนดโดยผู้ให้บริการ สิ่งที่ใช้ยืนยันตัวตน เช่น “ชื่อโรงเรียนแรกของคุณคืออะไร?” หรือกำหนดโดยสมาชิกผู้ใช้ก็ได้ และคำตอบจะถูกกำหนดไว้โดยสมาชิกผู้ใช้ (Subscriber) ตอนลงทะเบียน เช่น “อนุบาลกุ๊กไก่” (3) ในขั้นตอนยืนยันตัวตน ระบบจะถามคำถาม และผู้อ้างสิทธิ์	1	(1) ข้อมูลความลับ (Secret) มีค่าอย่างน้อย 14 บิต (Bits) (2) ผู้ใช้สามารถกำหนดคำถามเองจากความรู้ส่วนตัว (Personal Knowledge) หรือเลือกคำถาม (Question) จากชุดของคำถามที่ระบบเตรียมไว้ให้ (ชุดของคำถามจะต้องมีอย่างน้อย 5 คำถาม)	(1) จำกัดจำนวนความพยายามในการยืนยันตัวตนที่ล้มเหลวด้วยบัญชีสมาชิกผู้ใช้ 100 ครั้งภายใน 30 วัน และทำการล็อคบัญชีสมาชิกผู้ใช้เมื่อเกินจำนวนที่กำหนด (2) ผู้ตรวจสอบจะทำการตรวจสอบคำตอบที่ได้จากผู้ใช้สำหรับคำถามอย่างน้อย 3 คำถาม (3) ห้ามคำตอบว่าง
		2	(1) ข้อมูลความลับ (Secret)	(1) จำกัดจำนวนความพยายามในการยืนยันตัวตน

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	(Claimant) ก็จะใช้คำตอบที่จำไว้ตอบเพื่อยืนยันตัวตน (4) นอกจากนี้การจดจำรูปภาพก็สามารถเป็นทางเลือกหนึ่งที่สมาชิกผู้ใช้ (Subscriber) จะทำการเลือกและจำรูปภาพที่ผู้ให้บริการสิ่งที่ใช้ยืนยันตัวตน เตรียมไว้ให้เลือกตอนลงทะเบียน และเลือกรูปภาพที่จำไว้ในขั้นตอนการยืนยันตัวตนกับระบบ (5) จัดอยู่ในประเภทสิ่งที่คุณรู้ (Something You Know)		มีค่าอย่างน้อย 20 บิต (Bits) (2) ผู้ใช้สามารถกำหนดคำถามเองจากความรู้ส่วนตัว (Personal Knowledge) หรือเลือกคำถาม (Question) จากชุดของคำถามที่ระบบเตรียมไว้ให้ (ชุดของคำถามจะต้องมีอย่างน้อย 7 คำถาม)	ที่ล้มเหลวด้วยบัญชีสมาชิกผู้ใช้ 100 ครั้งภายใน 30 วัน และทำการล็อคบัญชีสมาชิกผู้ใช้เมื่อเกินจำนวนที่กำหนด (2) ผู้ตรวจสอบจะทำการตรวจสอบคำตอบที่ได้จากผู้ใช้สำหรับคำถามอย่างน้อย 5 คำถาม (3) ห้ามคำตอบว่าง
Look-up Secret	(1) เป็นสิ่งที่ใช้ยืนยันตัวตน ที่มีลักษณะทางกายภาพ (Physical) จับต้องได้หรืออิเล็กทรอนิกส์ก็ได้ (2) เก็บบันทึกชุดของความลับ	2	ข้อมูลความลับมีความยาวอย่างน้อย 64 บิต (Bits)	ถ้าข้อมูลความลับมีความยาวอย่างน้อย 20 บิต (Bits) ผู้ตรวจสอบจะต้องมีการจำกัดจำนวนความพยายามในการ

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	(Set of Secret) ที่ถูกแชร์ระหว่างผู้อ้างสิทธิ์ (Claimant) และผู้ให้บริการสิ่งที่ใช้ยืนยันตัวตน (3) ในขั้นตอนการยืนยันตัวตน ผู้อ้างสิทธิ์สามารถใช้โทเคนนี้ในการค้นหาความลับที่เหมาะสมเพื่อใช้ตอบกลับไปยังคำถามจากผู้ตรวจสอบ (Verifier) (4) ตัวอย่างเช่น ผู้อ้างสิทธิ์อาจถูกร้องขอให้แสดงตัวอักษรหรือตัวเลขที่กำหนดที่ถูกพิมพ์ไว้บนบัตร เป็นต้น (5) จัดอยู่ในประเภทสิ่งที่คุณมี (Something You Have)			ยืนยันตัวตนที่ล้มเหลวด้วยบัญชีสมาชิกผู้ใช้ 100 ครั้ง ภายใน 30 วัน และทำการล็อคบัญชีสมาชิกผู้ใช้เมื่อเกินจำนวนที่กำหนด
Out of Band Device	(1) เป็นสิ่งที่ใช้ยืนยันตัวตนที่มีลักษณะทางกายภาพ ที่สามารถกำหนดช่องทาง (Channel) และสามารถรับความลับ (Secret) ที่	2	สิ่งที่ใช้ยืนยันตัวตนจะต้องสามารถถูกระบุที่อยู่เฉพาะได้ และรองรับการติดต่อสื่อสารใน	(1) ข้อมูลความลับ (Secret) ที่ถูกสร้างโดยผู้ตรวจสอบมีค่าอย่างน้อย 64 บิต (Bits)

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	ใช้ได้ครั้งเดียว (One-Time Use) จากผู้ตรวจสอบ (Verifier) เพื่อใช้ในการยืนยันตัวตน (2) รองรับช่องทางการสื่อสารส่วนตัว (Private Communication Channel) ที่แยกต่างหากจากช่องทางหลักของระบบ (Primary Channel) ในการยืนยันตัวตน ดังนั้นเมื่อผู้อ้างสิทธิ์ได้รับความลับจากผู้ตรวจสอบผ่านทางอุปกรณ์ ผู้อ้างสิทธิ์จะต้องแสดงความลับนั้นกลับไปยังผู้ตรวจสอบผ่านช่องทางหลักของระบบเพื่อยืนยันตัวตน (3) ตัวอย่างเช่น การที่ผู้อ้างสิทธิ์ได้รับข้อความจากระบบผ่านโทรศัพท์มือถือ ผู้อ้างสิทธิ์ก็จะสามารถนำ		การยืนยันตัวตนทางอิเล็กทรอนิกส์ผ่านช่องทางส่วนตัว (Private Communication Channel) ที่แยกจากช่องทางหลัก (Primary Channel) ของระบบ	(2) ถ้าข้อมูลความลับ (Secret) ที่ถูกสร้างโดยผู้ตรวจสอบ มีค่าอย่างน้อย 20 บิต (Bits) ผู้ตรวจสอบจะต้องมีการจำกัดจำนวนความพยายามในการยืนยันตัวตนที่ล้มเหลวด้วยบัญชีสมาชิกผู้ใช้ 100 ครั้งภายใน 30 วัน และทำการล็อคบัญชีสมาชิกผู้ใช้เมื่อเกินจำนวนที่กำหนด

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	ข้อความนั้นไปใช้ล็อกอินเข้าเว็บไซต์เพื่อยืนยันตัวตน เป็นต้น อย่างไรก็ตามผู้อ้างสิทธิ์จะต้องลงทะเบียนโทรศัพท์มือถือกับผู้ให้บริการสิ่งที่ใช้ยืนยันตัวตนก่อน (4) อุปกรณ์โทเคนจะต้องถูกถือครองและถูกควบคุมโดยผู้อ้างสิทธิ์ (Claimant) (5) จัดอยู่ในประเภทสิ่งที่คุณมี (Something You Have)			
Single-Factor One-Time Password Device	(1) เป็นอุปกรณ์ฮาร์ดแวร์ (Hardware Device) ที่รองรับการสร้างรหัสผ่านที่ใช้ได้เพียงครั้งเดียว (One-Time Password) (2) เก็บความลับ (Secret) ที่ถูกใช้สำหรับสร้างรหัสผ่านที่ใช้ได้เพียงครั้งเดียว และไม่	2	(1) ต้องใช้วิธีการของ Approved Block Cipher หรือ Hash Function ในการรวมกุญแจสมมาตร (Symmetric Key) ที่ถูกเก็บบนอุปกรณ์ด้วย Nonce เพื่อสร้าง	(1) รหัสผ่านที่ใช้ได้เพียงครั้งเดียว (One-Time Password) จะต้องมีการกำหนดอายุ (Limited Lifetime) เป็นนาที (2) โมดูลที่ใช้ในกระบวนการ

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	จำเป็นต้องถูกเปิดใช้งาน (Activation) ด้วยปัจจัยอื่นเพิ่มเติม (Second Factor) (3) ตัวอย่างเช่น เอนทิตีสามารถรับรหัสผ่านที่ใช้ได้เพียงครั้งเดียวในลักษณะตัวอักษร 6 ตัวที่ถูกสร้างจากอุปกรณ์ต่อ 1 ครั้ง เพื่อใช้ยืนยันตัวตน 1 ครั้ง เป็นต้น (4) การยืนยันตัวตนจะเสร็จสมบูรณ์ได้ต่อเมื่อเอนทิตีสามารถแสดงรหัสผ่านที่ใช้ได้เพียงครั้งเดียวที่ถูกต้องได้และเอนทิตีจะต้องถือครองและควบคุมอุปกรณ์นั้น (5) จัดอยู่ในประเภทสิ่งที่คุณมี (Something You Have)		รหัสผ่านที่ใช้ได้เพียงครั้งเดียว (One-Time Password) (2) Nonce อาจจะเป็นวันที่และเวลา (Date and Time) หรือตัวนับ (Counter) ที่ถูกสร้างบนอุปกรณ์	เข้ารหัส (Cryptographic Module) จะต้องถูกทำอย่างถูกต้องตามมาตรฐาน FIPS 140-2 ระดับ 1 หรือสูงกว่า
Single-Factor Cryptographic Device	(1) เป็นอุปกรณ์ฮาร์ดแวร์(Hardware Device) ที่ดำเนินการเกี่ยวกับกระบวนการการเข้ารหัสข้อมูล	2	โมดูลที่ใช้ในกระบวนการเข้ารหัส	ข้อมูลนำเข้าของอุปกรณ์โทเคน (Token Input) ที่ถูกสร้างโดยผู้

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	(Cryptographic Operations) (2) ไม่จำเป็นต้องถูกเปิดใช้งาน (Activation) ด้วยปัจจัยอื่นเพิ่มเติม (Second Factor) (3) อุปกรณ์นี้ใช้กุญแจการเข้ารหัสลับแบบสมมาตร (Symmetric) หรืออสมมาตร (Asymmetric Cryptographic Keys) ที่ถูกเก็บไว้ในอุปกรณ์ (4) ตัวอย่างเช่น เมื่อเอนทิตีต้องการยืนยันตัวตน เอนทิตีก็สามารถเสียบอุปกรณ์นี้เข้ากับช่องอ่านหรืออุปกรณ์อ่าน(Reader) เพื่อนำกุญแจการเข้ารหัสลับจากอุปกรณ์ส่งเข้าไปในกระบวนการตรวจสอบเป็นต้น (5) การยืนยันตัวตนจะเสร็จสมบูรณ์ได้ต่อเมื่อ		(Cryptographic Module) จะต้องมีความถูกต้องตามมาตรฐาน FIPS 140-2 ระดับ 1 หรือสูงกว่า	ตรวจสอบ เช่น Nonce จะต้องมีค่าอย่างน้อย 64 บิต (Bits)

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	เอนทิตีต้องถือครองอุปกรณ์เท่านั้น (6) จัดอยู่ในประเภทสิ่งที่คุณมี (Something You Have)			
Multi-Factor Software Cryptographic Token	(1) เป็นกุญแจการเข้ารหัสลับ (Cryptographic Key) ที่ถูกเก็บไว้บนแหล่งบันทึกข้อมูล เช่น Disk ในเครื่องคอมพิวเตอร์ บราวเซอร์ หรือที่เก็บข้อมูลอิเล็กทรอนิกส์อื่นๆ (Soft Media) (2) จำเป็นจะต้องถูกเปิดใช้งาน (Activation) ด้วยปัจจัยอื่นเพิ่มเติม (Second Factor) ในการยืนยันตัวตน (3) ตัวอย่างการใช้งาน เช่น เมื่อเอนทิตีต้องการลงลายมือชื่ออิเล็กทรอนิกส์ เอนทิตีจะต้องติดตั้งใบรับรองอิเล็กทรอนิกส์ไว้ในอุปกรณ์คอมพิวเตอร์ที่	3	(1) โมดูลที่ใช้ในกระบวนการเข้ารหัส (Cryptographic Module) จะต้องมีความถูกต้องตามมาตรฐาน FIPS 140-2 ระดับ 1 หรือสูงกว่า (2) ในการยืนยันตัวตนแต่ละครั้งจะต้องมีการใส่รหัสผ่านหรือข้อมูลอื่นๆ ที่ใช้ในการเปิดใช้งาน (Other Activation Data) (3) สำเนาที่ไม่ได้ถูกเข้ารหัสของกุญแจที่ใช้ในการยืนยันตัวตน	ข้อมูลนำเข้าของอุปกรณ์โทเคน (Token Input) ที่ถูกสร้างโดยผู้ตรวจสอบ เช่น Nonce จะต้องมีค่าอย่างน้อย 64 บิต (Bits)

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	จะใช้ลงลายมือชื่ออิเล็กทรอนิกส์ เช่น เครื่องคอมพิวเตอร์พกพา (Laptop) หลังจากนั้นเอนทิตีจะใส่รหัสผ่าน (Password) หรือเลขรหัสส่วนตัว (PIN) เพื่อทำการเปิดใช้งาน (Activation) กุญแจส่วนตัวที่เป็นคู่คีย์กับกุญแจสาธารณะที่อยู่ในใบรับรองอิเล็กทรอนิกส์เพื่อใช้ลงลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น (4) การยืนยันตัวตนจะเสร็จสมบูรณ์ได้ต่อเมื่อเอนทิตีจะต้องถือครองและควบคุมกุญแจได้เท่านั้น (5) การมีกุญแจการเข้ารหัสลับจัดอยู่ในประเภทสิ่งที่คุณมี (Something You Have) และการใช้สิ่งที่ใช้ยืนยันตัวตนอื่นเพิ่มเติม เช่น รหัสผ่านหรือเลขรหัส		จะต้องถูกลบหลังจากการยืนยันตัวตนแต่ละครั้ง	

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	เพื่อเปิดใช้งานจะจัดอยู่ในประเภทสิ่งที่คุณรู้ (Something You Know) (หรืออาจจะใช้สิ่งที่ใช้ยืนยันตัวตน ประเภทสิ่งที่คุณเป็น (Something You Are) เช่น ข้อมูลชีวภาพ (Biometric) เพื่อเปิดใช้งานก็ได้)			
Multi-Factor One-Time Password Device	(1) เป็นอุปกรณ์ฮาร์ดแวร์ (Hardware Device) ที่สร้างรหัสผ่านที่ใช้ได้เพียงครั้งเดียว (One-Time Password) เพื่อใช้ในการยืนยันตัวตน (2) จำเป็นต้องถูกเปิดใช้งาน (Activation) ด้วยปัจจัยอื่นเพิ่มเติม (Second Factor) (3) ตัวอย่างเช่น การใส่รหัสผ่านหรือเลขรหัสบนแป้นพิมพ์พิเศษ (Entry Pad) การพิมพ์ลายนิ้วมือบนเครื่องอ่านลายนิ้วมือ (Fingerprint	4	(1) โมดูลที่ใช้ในกระบวนการเข้ารหัส (Cryptographic Module) จะต้องมีความถูกต้องตามมาตรฐาน FIPS 140-2 ระดับ 2 หรือสูงกว่าพร้อมด้วยความมั่นคงปลอดภัยทางกายภาพ (Physical Security) ตามมาตรฐาน FIPS 140-2 ระดับ 3 หรือสูงกว่า	รหัสผ่านที่ใช้ได้เพียงครั้งเดียว (One-Time Password) จะต้องมีการกำหนดอายุ (Limited Lifetime) น้อยกว่า 2 นาที

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	Reader) หรือการใช้อุปกรณ์อื่นๆ ผ่านช่องทาง USB Port เป็นต้น (4) โดยปกติรหัสที่ใช้ได้เพียงครั้งเดียวจะถูกแสดงบนอุปกรณ์และเอนทิตีจะต้องกรอกรหัสนั้นด้วยตนเองต่อผู้ตรวจสอบเสมือนรหัสผ่าน (การส่งข้อมูลรหัสจากอุปกรณ์ ผ่านทางอิเล็กทรอนิกส์ไปยังเครื่องคอมพิวเตอร์ก็สามารถทำได้) เช่น เอนทิตีสามารถใช้อุปกรณ์เพื่อสร้างรหัสผ่านที่ใช้ได้เพียงครั้งเดียวและเอนทิตีจะต้องใส่รหัสผ่าน หรือพิมพ์ลายนิ้วมือเพื่อเปิดใช้งานอุปกรณ์นั้นเสียก่อนอุปกรณ์จึงสร้างรหัสผ่านได้ เป็นต้น (5) การยืนยันตัวตนจะเสร็จสมบูรณ์ได้ต่อเมื่อ		(2) ต้องใช้วิธีการของ Approved Block Cipher หรือ Hash Function ในการรวมกุญแจสมมาตร (Symmetric Key) ที่ถูกเก็บบนอุปกรณ์ฮาร์ดแวร์ส่วนบุคคลด้วย Nonce เพื่อสร้างรหัสผ่านที่ใช้ได้เพียงครั้งเดียว (One-Time Password) (3) Nonce อาจจะเป็นวันที่และเวลา (Date and Time) หรือตัวนับ (Counter) ที่ถูกสร้างบนอุปกรณ์ (4) ในการยืนยันตัวตนแต่ละครั้งจะต้องมีการใส่รหัสผ่านหรือ	

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	เอนทิตีสามารถแสดงรหัสผ่านที่ใช้ได้เพียงครั้งเดียวที่ถูกต้องได้และเอนทิตีจะต้องถือครองและควบคุมอุปกรณ์นั้น (6) การมีอุปกรณ์จัดอยู่ในประเภทสิ่งที่คุณมี (Something You Have) และการใช้โทเคนอื่นเพิ่มเติมเพื่อเปิดใช้งาน อุปกรณ์ จัดอยู่ในประเภทสิ่งที่คุณรู้ (Something You Know) หรือสิ่งที่คุณเป็น (Something You Are)		ข้อมูลอื่นๆ ที่ใช้ในการเปิดใช้งาน (Other Activation Data) ผ่านวิธีการในการนำเข้าข้อมูล (Integrated Input Mechanism)	
Multi-Factor Hardware Cryptographic Device	(1) เป็นอุปกรณ์ฮาร์ดแวร์ (Hardware Device) ที่บรรจุกุญแจการเข้ารหัสลับ (Cryptographic Key) ที่ถูกป้องกันด้านความมั่นคงปลอดภัยไว้ (2) จำเป็นต้องถูกเปิดใช้งาน (Activation) ด้วยปัจจัยอื่นเพิ่มเติม (Second Factor)	4	(1) โมดูลที่ใช้ในกระบวนการเข้ารหัส (Cryptographic Module) จะต้องมีความถูกต้องตามมาตรฐาน FIPS 140-2 ระดับ 2 หรือสูงกว่าพร้อมด้วยความมั่นคง	ข้อมูลนำเข้าของอุปกรณ์โทเคน (Token Input) ที่ถูกสร้างโดยผู้ตรวจสอบ เช่น Nonce จะต้องมีค่าอย่างน้อย 64 บิต (Bits)

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	(3) โดยส่วนใหญ่ของอุปกรณ์ชนิดนี้จะเป็นอุปกรณ์พิเศษ เช่น บัตรสมาร์ทการ์ด (Smart Card) ที่ใช้เก็บใบรับรองอิเล็กทรอนิกส์ที่มีกุญแจสาธารณะ (Public Key) และกุญแจส่วนตัว (Private Key) ทั้งนี้ กุญแจส่วนตัวสามารถถูกเก็บแยกออกจากกุญแจสาธารณะได้ โดยให้เก็บไว้ในอุปกรณ์ที่เรียกว่า Hardware Security Module (HSM) หรือสิ่งที่ใช้ยืนยันตัวตนใดๆ ที่มีการป้องกันความมั่งคงปลอดภัยตามมาตรฐานที่กำหนด เป็นต้น (4) ตัวอย่างการใช้งาน เช่น เมื่อเอนทิตีต้องการยืนยันตัวตนในระบบที่ใช้บัตรสมาร์ทการ์ด เอนทิตีจะต้องรูดหรือเสียบบัตรสมาร์ทการ์ด		ปลอดภัยทางกายภาพ (Physical Security) ตามมาตรฐาน FIPS 140-2 ระดับ 3 หรือสูงกว่า (2) ในการยืนยันตัวตนแต่ละครั้งจะต้องมีการใส่รหัสผ่านเลขรหัสส่วนตัว (PIN) หรือข้อมูลชีวภาพ (Biometric) เพื่อเปิดใช้งานกุญแจที่ใช้ในการยืนยันตัวตน (Authentication Key) (3) ห้ามส่งออกกุญแจที่ใช้ในการยืนยันตัวตน	

ตารางที่ 2.3 ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดของระดับความน่าเชื่อถือ (ต่อ)

ชนิดของสิ่งที่ยืนยันตัวตน	รายละเอียด	ระดับความน่าเชื่อถือ	ข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตน	ข้อกำหนดของผู้ตรวจสอบ
	เข้ากับเครื่องอ่านบัตร (Reader) แล้วเอนทิตีจะต้องใส่รหัสผ่าน (Password) หรือเลขรหัสส่วนตัว (PIN) เพื่อทำการเปิดใช้งาน (Activation) กุญแจส่วนตัวที่เป็นคู่คีย์กับกุญแจสาธารณะที่อยู่ในใบรับรองอิเล็กทรอนิกส์ เป็นต้น (5) การยืนยันตัวตนจะเสร็จสมบูรณ์ได้ต่อเมื่อเอนทิตีจะต้องถือครองอุปกรณ์และควบคุมกุญแจได้เท่านั้น (6) การมีอุปกรณ์จัดอยู่ในประเภทสิ่งที่คุณมี (Something You Have) และการใช้โทเคนอื่นเพิ่มเติมเพื่อเปิดใช้งานอุปกรณ์ จัดอยู่ในประเภทสิ่งที่คุณรู้ (Something You Know) หรือสิ่งที่คุณเป็น (Something You Are)			

2.7 งานวิจัยที่เกี่ยวเนื่องกับความปลอดภัยของ Mobile Banking Application

จากการวิจัยในสหรัฐอเมริกาพบว่าเหตุผลที่ผู้ใช้งานโทรศัพท์มือถือส่วนใหญ่ไม่ทำธุรกรรมผ่าน Mobile Banking Application ก็คือเหตุผลด้านความปลอดภัยมาเป็นอันดับหนึ่ง รองลงมาคือไม่สนใจ และต้องการทำธุรกรรมผ่านเว็บไซต์ธนาคารแทน ตามลำดับ ซึ่งสาเหตุที่ผู้ใช้งาน Mobile Banking Application กังวลเรื่องความปลอดภัยนั้นส่วนใหญ่มาจากการเข้าใจที่ผิดๆ หรือการขาดความรู้ความเข้าใจที่เพียงพอ โดยที่พบว่าจำนวนผู้ใช้สมาร์ทโฟนทั้งหมด ร้อยละ 48 ได้ใช้งาน Mobile Banking และมีเพียงร้อยละ 24 ที่เคยชำระเงินผ่าน Mobile Banking (Federal Reserve, 2014) ซึ่งสอดคล้องกับหลายๆ งานวิจัยที่พบว่าความปลอดภัยเป็นส่วนหนึ่งในปัจจัยเรื่องความเชื่อมั่น และมีความสำคัญอย่างมากต่อการใช้งาน Mobile Banking Application (Gunsaekaran & Ngai 2003; Horton et al. 2002; Nasri 2011)

โดยรูปแบบของการยืนยันตัวตนสำหรับ Online Banking พบว่าผู้คนส่วนใหญ่นิยมรหัสผ่านที่เป็นการผสมกันระหว่างตัวเลข อักขระพิเศษ ตัวอักษรเล็ก และ ตัวอักษรใหญ่ผสมกันมากถึงร้อยละ 32.5 รองลงมาคือ การผสมกันระหว่างตัวเลขและตัวอักษรเล็ก ร้อยละ 30 และ การใช้ตัวเลขเพียงอย่างเดียว ร้อยละ 7.5 ตามลำดับ โดยเก็บข้อมูลจากกลุ่มตัวอย่างที่เป็นลูกค้าธนาคารอาศัยอยู่ในเวสท์เทิร์นออสเตรเลีย (Nattakant Utakrit, 2012)

บทที่ 3
ระเบียบวิธีวิจัย

ในการศึกษาความเห็นของ Generation C ในประเทศไทยเกี่ยวกับความปลอดภัยในการใช้งาน Mobile Banking Application ที่ให้บริการโดยธนาคารพาณิชย์ในประเทศไทย โดยมุ่งศึกษาระดับความเชื่อมั่นที่มีต่อระบบความปลอดภัยของ Mobile Banking Application ความรู้ความเข้าใจในการใช้งานอย่างปลอดภัย รวมถึงความคิดเห็นเกี่ยวกับระบบในการยืนยันตัวตนของผู้ใช้งาน มีวิธีการศึกษาดังนี้

3.1 รูปแบบการวิจัย

การศึกษาในครั้งนี้จะเป็นการวิจัยเชิงคุณภาพ (Qualitative Research) เป็นการศึกษาปรากฏการณ์ทางสังคมตามความเป็นจริงในทุกมิติ เป็นการแสวงหาความรู้โดยเน้นความสำคัญของข้อมูลด้านความรู้สึกนึกคิด ค่านิยม อุดมการณ์ ของบุคคลที่เกี่ยวข้องกับปรากฏการณ์นั้นๆ โดยมีช่วงระยะเวลา และใช้วิธีวิเคราะห์ข้อมูลแบบการตีความสร้างข้อสรุป แบบอุปนัย (induction) เป็นหลัก (สุภางค์ จันทวานิช, 2543) ทั้งนี้การเลือกใช้วิธีวิจัยเชิงคุณภาพจะต้องมีความสอดคล้องกับวัตถุประสงค์ หรือจุดมุ่งหมายของการวิจัย ซึ่งการตอบสนองอาจจะเพื่อเป็นการบรรยาย การแปลความหมายเพื่อจะได้เข้าใจอย่างลึกซึ้งในธรรมชาติของปรากฏการณ์เฉพาะอย่าง การตรวจสอบ หรือเพื่อการประเมินความสำเร็จของนโยบาย หรือ โครงการกิจกรรมต่างๆ (Leed & Ormrod, 2001)

3.2 ประชากรและการสุ่มตัวอย่าง

ประชากรที่ใช้ศึกษา คือกลุ่มคน Generation C ซึ่งจะไม่ได้จะแบ่งตามช่วงอายุ แต่จะแบ่งตามพฤติกรรมการใช้อินเทอร์เน็ต โทรศัพท์สมาร์ทโฟน และใช้โซเชียลเน็ตเวิร์ก โดยที่กลุ่มคนเหล่านี้ต้องมีประสบการณ์การใช้งาน Mobile Banking Application ของธนาคารพาณิชย์ภายในประเทศไทยเพื่อที่จะสามารถตอบคำถามวิจัยได้อย่างเหมาะสม

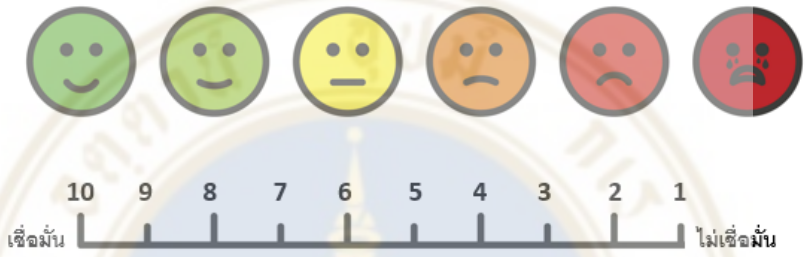
การเลือกกลุ่มตัวอย่างโดยวิธีที่ไม่อาศัยความน่าจะเป็น (Non-Probability Sampling) แบบเจาะจง (Purposive Sampling) ซึ่งเป็นการเลือกตัวอย่างโดยใช้ดุลยพินิจและการตัดสินใจของผู้วิจัยในการเลือกตัวอย่างที่สอดคล้องกับวัตถุประสงค์ของงานวิจัย ข้อดีของวิธีนี้ก็คือมีความสะดวกรวดเร็วและประหยัดค่าใช้จ่าย ส่วนข้อเสียคือ การเลือกกลุ่มตัวอย่างแบบเจาะจงต้องใช้ความรู้ ความชำนาญ และประสบการณ์ในเรื่องนั้นๆ ของผู้ทำวิจัย ดังนั้นจึงไม่มีวิธีการทางสถิติที่จะมาคำนวณความคลาดเคลื่อนที่เกิดจากการสุ่มตัวอย่างได้ (หทัยชนก พรรคเจริญ, 2555) โดยที่ผู้วิจัยทำการเก็บข้อมูลจากกลุ่มตัวอย่างจำนวนทั้งสิ้น 30 คน ใช้เวลาราว 20 นาทีต่อคน โดยใช้วิธีการศึกษาแบบเชิงพรรณนา (Descriptive Research) การกำหนดขนาดกลุ่มตัวอย่างเป็นไปแนวทางของ Nastasi และ Schensul (2005) ให้แนวทางในการเก็บรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกว่า ควรสัมภาษณ์กลุ่มตัวอย่างประมาณ 5-30 คน โดยเวลาในการสัมภาษณ์ประมาณ 20-40 นาทีต่อคน และพิจารณาถึงความอิ่มตัวของข้อมูล (Data Saturation) โดยพิจารณาข้อมูลที่ได้จากการรวบรวมว่าสามารถนำไปสู่การค้นหารูปแบบหรือสร้างข้อค้นพบตามวัตถุประสงค์ของการวิจัยหรือไม่ จนกระทั่งผู้วิจัยไม่พบแนวคิด รูปแบบ หรือข้อค้นพบอื่นๆ ที่แตกต่างจากข้อมูลเดิมที่รวบรวมได้

3.3 วิธีการเก็บรวบรวมข้อมูล

การศึกษาครั้งนี้ใช้การสัมภาษณ์แบบกึ่งโครงสร้าง (semi-structured interview) ในการเก็บรวบรวมข้อมูล การสัมภาษณ์แบบกึ่งโครงสร้างเป็นการสัมภาษณ์ที่มักไม่มีรูปแบบแน่นอน แต่จะมีลักษณะผสมผสานระหว่างโครงสร้างข้อคำถามและการกำหนดประเด็นคำถามไว้ล่วงหน้า นิยมใช้กับการวิจัยเชิงคุณภาพที่ต้องการความยืดหยุ่นเพื่อการเก็บข้อมูลในขณะที่ยังคงไว้ซึ่งเนื้อหาสาระที่ครอบคลุมประเด็นอย่างครบถ้วน (ปัญญา ธีระวิทยเลิศ, 2540) คำถามที่ใช้ในการสัมภาษณ์จะสอดคล้องไปกับคำถามวิจัยเพื่อให้ได้คำตอบในประเด็นที่ทำการศึกษา และมีการใช้เครื่องมือแบบทดสอบในการวัดความรู้ความเข้าใจของผู้ให้สัมภาษณ์ โดยคำถามที่ใช้ในการสัมภาษณ์และแบบทดสอบถูกพัฒนาบนแนวคิดและทฤษฎีที่ได้จากการทบทวนวรรณกรรม โดยแบ่งการสัมภาษณ์แบ่งออกเป็น 4 ส่วนดังนี้

ส่วนที่ 1: คำถามเกี่ยวกับข้อมูลทั่วไปของผู้ให้สัมภาษณ์ ได้แก่ อายุ อาชีพ ระดับการศึกษา Mobile Banking Application ของธนาคารที่เคยใช้ในอดีตหรือปัจจุบัน ระยะเวลาใช้งาน Mobile Banking Application จนถึงปัจจุบัน

ส่วนที่ 2: คำถามที่ให้ผู้ให้สัมภาษณ์เลือกคะแนนความเชื่อมั่นในการใช้บริการ Mobile Banking Application ในภาพรวมต่อความปลอดภัย ว่ามีระดับมากน้อยเพียงใด โดยใช้ Likert Scale ระหว่าง 1-10 โดย 1 หมายถึงเชื่อมั่นน้อยที่สุด และ 10 หมายถึงเชื่อมั่นมากที่สุด เนื่องจากเป็นการสอบถามความคิดเห็นของผู้ให้สัมภาษณ์หาก scale มีความละเอียดเพียงพอก็น่าจะสะท้อนความคิดเห็นได้ดียิ่งขึ้นและการที่ scale ที่มีทั้งหมดเป็นนับรวมเป็นเลขคู่ สามารถขจัดปัญหาที่ผู้ให้สัมภาษณ์เลี่ยงให้ความคิดเห็นแบบตรงไปตรงมาโดยการตอบในลักษณะเป็นกลางแทน หลังจากนั้นจะทำการสัมภาษณ์ต่อเนื่องถึงเหตุผลการใช้ระดับคะแนนดังกล่าวว่ามีเหตุผลสนับสนุนใดบ้าง (Jeff, 2018)



ส่วนที่ 3: เป็นการวัดความรู้ความเข้าใจของผู้ให้สัมภาษณ์ในการใช้งาน Mobile Banking Application อย่างปลอดภัยโดยจะให้ผู้ให้สัมภาษณ์ทำแบบทดสอบ หลังจากนั้นผู้วิจัยวิเคราะห์คำตอบทั้งหมดที่ได้จากการทำแบบทดสอบ เพื่อสัมภาษณ์สอบทานความรู้ความเข้าใจของผู้ทำแบบทดสอบอีกครั้ง รวมถึงการตั้งคำถามสัมภาษณ์ว่าผู้ให้สัมภาษณ์ได้นำความรู้ความเข้าใจของตนไปใช้จริงหรือไม่ เพราะเหตุใด

ส่วนที่ 4: เป็นการสอบถามความคิดเห็นเกี่ยวกับวิธีการยืนยันตัวตนผ่าน Mobile Banking Application ที่ผู้ให้สัมภาษณ์เห็นว่าเหมาะสม โดยแบ่งออกเป็น 2 ลักษณะ คือ การยืนยันตัวตนเพื่อ log in เข้าสู่ระบบ Mobile Banking Application และการยืนยันตัวตนเพื่อยืนยันรายการการทำธุรกรรม โดยก่อนการสัมภาษณ์จะแจกเอกสารสรุปรายละเอียดอย่างสั้นๆ และมีรูปภาพประกอบ เพื่อแจ้งให้ผู้ให้สัมภาษณ์ทราบถึงวิธีการยืนยันตัวตนที่มีอยู่ในปัจจุบัน

3.4 การวิเคราะห์ข้อมูล

ข้อมูลที่ได้จากการสัมภาษณ์และการทำแบบทดสอบข้างต้น จะถูกนำมาวิเคราะห์ข้อมูลแบบสร้างข้อสรุป โดยการนำคำตอบจากการสัมภาษณ์ของกลุ่มตัวอย่างมาจัดเรียงข้อมูล วิเคราะห์ผล และสรุปผล ดังนี้

1) ค่าเฉลี่ยของระดับความเชื่อมั่นที่มีต่อความปลอดภัยของ Mobile Banking Application ในภาพรวม โดยใช้สูตร

$\bar{X} = \frac{\sum x}{n}$ โดยที่ $\bar{X}$ หมายถึงค่าเฉลี่ยของระดับความเชื่อมั่นระหว่าง 1 ถึง 10

$\sum x$ หมายถึงผลรวมระดับความเชื่อมั่น

n หมายถึงจำนวนผู้ให้สัมภาษณ์ (30 คน)

อย่างไรก็ตาม ค่าเฉลี่ยดังกล่าวอาจไม่สามารถสะท้อนความคิดเห็นของกลุ่มคน Generation C ได้ทั้งหมดในเชิงสถิติ เนื่องจากเป็นข้อมูลจากผู้ที่ให้สัมภาษณ์เพียง 30 คนเท่านั้น แต่ตัวเลขดังกล่าวสามารถสื่อถึงความคิดเห็นโดยรวมของกลุ่มตัวอย่างที่มีต่อความเชื่อมั่นในเรื่องความปลอดภัยของ Mobile Banking Application

ข้อมูลที่ได้จากการสัมภาษณ์เกี่ยวกับเหตุผลสนับสนุนความเชื่อมั่นของผู้ให้สัมภาษณ์แต่ละคน จะถูกนำมาวิเคราะห์เนื้อหา (content analysis) ซึ่งเป็นการวิเคราะห์ข้อมูลเชิงบรรยายเชื่อมโยงกับสิ่งที่ศึกษา ทำการจัดประเภทข้อมูล สังเคราะห์ ค้นหาแบบแผนและตีความข้อมูลที่ได้มาเพื่อให้เข้าใจความหมายของสิ่งที่ศึกษาอยู่ โดยขั้นตอนการวิเคราะห์ข้อมูลนั้นมีลักษณะไม่ตายตัว (ณรงค์ศักดิ์ บุญยมาลิก, 2555) โดยหลังจากได้ข้อมูลจากการสัมภาษณ์และถอดความให้อยู่ในรูปแบบเอกสารแล้ว จากนั้นจัดกลุ่มคำตอบที่มีทิศทางของคำตอบไปในทางเดียวกัน ทำการกำหนดรหัส (coding) ให้กับข้อมูลเพื่อสื่อถึงคำตอบต่างๆ ที่เป็นกลุ่มเดียวกัน จากนั้นนำข้อมูลที่ได้จากการแบ่งหมวดหมู่มาวิเคราะห์เชิงเนื้อหา ตีความข้อมูลที่ได้ โดยใช้แนวคิดและทฤษฎีต่างๆ ที่เกี่ยวข้องมาประกอบและเชื่อมโยงความสัมพันธ์

2) คะแนนความรู้ความเข้าใจในเรื่องการใช้งาน Mobile Banking Application อย่างปลอดภัย ซึ่งเป็นตัวชี้วัดเบื้องต้นว่าผู้ทำแบบทดสอบมีความรู้ความเข้าใจมากน้อยเพียงใด จากแบบทดสอบทั้ง 10 ข้อ (ข้อละ 1 คะแนน) โดยผลที่ได้สามารถตีค่าได้ดังนี้

ตารางที่ 3.1 แปลผลคะแนนจากการทำแบบทดสอบ

คะแนนรวม	**ระดับความรู้ความเข้าใจ**
น้อยกว่า 7 คะแนน	น้อย
7 – 8 คะแนน	ทั่วไป
9 – 10 คะแนน	มาก

โดยที่แบบสอบถามดังกล่าวได้ถูกนำไปทดสอบกับกลุ่มคนจำนวน 20 คนซึ่งเป็นพนักงานธนาคารไอซีบีซี (ไทย) จำกัด มหาชน เพื่อใช้ในการกำหนดวิธีแปลผลคะแนนเป็นระดับความรู้ความเข้าใจ พบว่าหากเป็นพนักงานทั่วไปของธนาคารที่ไม่ได้ปฏิบัติหน้าที่อยู่ในฝ่ายกลุ่มลูกค้ารายย่อย หรือเจ้าหน้าที่ฝ่ายไอที (จำนวนทั้งสิ้น 10 คน) คะแนนจะอยู่ในช่วง 6 – 10 คะแนน แต่โดยส่วนใหญ่กว่า 70% จะอยู่ในช่วง 7 – 8 คะแนน จึงกำหนดให้ช่วงคะแนน 7-8 คะแนนแปลผลเป็นระดับความรู้ความเข้าใจอยู่ในระดับทั่วไป ในขณะที่เจ้าหน้าที่ฝ่ายกลุ่มลูกค้ารายย่อย และเจ้าหน้าที่ฝ่ายไอที (จำนวนทั้งสิ้น 10 คน) จะอยู่ที่ช่วงคะแนน 9 – 10 เท่านั้น จึงจัดให้ช่วงคะแนนดังกล่าวมีความรู้ความเข้าใจอยู่ในระดับมาก และหากต่ำกว่า 7 คะแนนจะถูกจัดให้มีระดับความรู้ความเข้าใจในระดับน้อย

ข้อมูลที่ได้จากการสัมภาษณ์เพื่อสอบทานความรู้ความเข้าใจในเรื่องการใช้งาน Mobile Banking Application อย่างปลอดภัย และการนำความรู้ความเข้าใจดังกล่าวไปปฏิบัติ จะถูกนำมาวิเคราะห์และจัดหมวดหมู่โดยวิธีการวิเคราะห์เนื้อหา (content analysis) เช่นกัน

3) ข้อมูลที่ได้จากการสัมภาษณ์ความคิดเห็นในเรื่องการยืนยันตัวตนเพื่อใช้งาน Mobile Banking Application ใน 2 ลักษณะคือ การยืนยันตัวตนเพื่อ log in เข้าสู่ระบบ Mobile Banking Application และ การยืนยันตัวตนเพื่อยืนยันรายการการทำธุรกรรม จะถูกนำมาวิเคราะห์และจัดหมวดหมู่โดยวิธีการวิเคราะห์เนื้อหา (content analysis) เช่นกัน

บทที่ 4
ผลการวิจัย

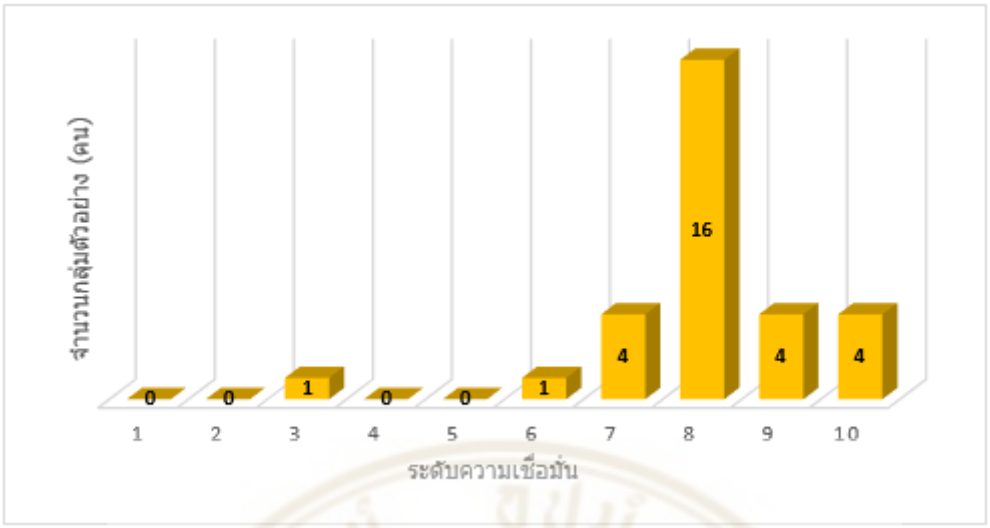
การศึกษาความเห็นของ Generation C ในประเทศไทยเกี่ยวกับความปลอดภัยในการใช้งาน Mobile Banking Application ที่ให้บริการโดยธนาคารพาณิชย์ในประเทศไทยนั้น ผู้ทำการวิจัยได้เลือกใช้วิธีวิจัยเชิงคุณภาพ (Qualitative research) โดยเก็บข้อมูลปฐมภูมิ (Primary data) ซึ่งได้จากการสัมภาษณ์กึ่งโครงสร้าง (semi-structured interview) และเลือกกลุ่มตัวอย่างแบบเจาะจง ซึ่งคือ Generation C ในประเทศไทย 30 คนที่ใช้บริการ Mobile Banking Application ผลการวิเคราะห์ข้อมูลพบประเด็นต่างๆ ดังนี้

4.1 ระดับความเชื่อมั่นในเรื่องความปลอดภัยในการใช้งาน Mobile Banking Application ของผู้ใช้บริการ

ผลการสัมภาษณ์เกี่ยวกับความคิดเห็นของผู้ใช้บริการ Mobile Banking Application ต่อระดับความเชื่อมั่นความปลอดภัยของบริการดังกล่าวโดยธนาคารพาณิชย์ในประเทศไทย สามารถสรุปสาระสำคัญได้ดังนี้

4.1.1 ภาพรวมของความเชื่อมั่นในความปลอดภัยที่มีต่อบริการ Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย

จากการสัมภาษณ์กลุ่มตัวอย่าง 30 คนต่อระดับความเชื่อมั่นที่มีต่อบริการ Mobile Banking Application โดยที่ทุกคนต่างมีประสบการณ์การใช้งานมาไม่น้อยกว่า 1 ปี โดยใช้ Likert Scale ระหว่าง 1-10 โดย 1 หมายถึงเชื่อมั่นน้อยที่สุด และ 10 หมายถึงเชื่อมั่นมากที่สุด พบว่าค่าเฉลี่ยความเชื่อมั่นของกลุ่มตัวอย่างอยู่ที่ระดับ 8.03 ซึ่งจัดว่าค่อนข้างสูงมาก โดยหากแจกแจงความถี่ในแต่ระดับความเชื่อมั่นของกลุ่มตัวอย่างได้ดังนี้ (ภาพที่ 4.1)



ภาพที่ 4.1 แจกแจงความถี่จำนวนคนของกลุ่มตัวอย่างในแต่ละระดับความเชื่อมั่น 1 – 10

4.1.2 เหตุผลหลักของความเชื่อมั่นในความปลอดภัยที่มีต่อ Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย

จากการวิเคราะห์ประเด็นที่ได้จากการสัมภาษณ์กลุ่มตัวอย่างถึงเหตุผลหลักที่ทำให้เกิดความเชื่อมั่นในความปลอดภัยของ Mobile Banking Application พบว่าสามารถแบ่งออกได้เป็น 4 เหตุผลหลักดังนี้

1. มีความมั่นใจในระบบยืนยันตัวตน (11 คน) โดยมองว่าธนาคารพาณิชย์ได้มีการใช้วิธีการยืนยันตัวตนที่มีความปลอดภัยเพียงพอในสายตาของผู้ใช้งาน อาทิเช่น การสแกนลายนิ้วมือ การใส่รหัสผ่าน การขอเลขรหัส OTP เป็นต้น

"...ส่วนตัวคิดว่าปลอดภัยดี ทีเด็ดคือมีเลขรหัส OTP ที่ส่งมาให้ทางมือถือทุกครั้งก่อนโอนเงิน" (เพศชาย, อายุ 31 ปี, ธุรกิจส่วนตัว)

"...เพราะก่อนเข้าใช้งานต้องมีทั้งสแกนลายนิ้วมือ หรือไม่ก็ใส่รหัสผ่าน เบ็ดเสร็จต้องใส่รหัสอย่างน้อย 2 รอบถึงจะโอนเงินได้ แล้วพอโอนออกแล้วก็ยังมี e-slip ให้ด้วย" (เพศชาย, อายุ 33 ปี. พนักงานบริษัทเอกชน)

2. ไม่เคยเจอเหตุการณ์เลวร้ายโดยตรง (9 คน) โดยที่กลุ่มตัวอย่างคิดเห็นว่าจากประสบการณ์ในอดีตตนเองยังไม่เคยประสบเหตุการณ์ในเชิงลบที่เกี่ยวกับเรื่องความปลอดภัยในการใช้งาน Mobile Banking Application แต่ส่วนใหญ่จะเคยได้ยินเหตุการณ์จากบุคคลอื่นในข่าว เช่น การถูกโจรกรรมข้อมูลส่วนตัว เงินในบัญชีถูกขโมยโดยอาชญากรทางคอมพิวเตอร์ เป็นต้น

“…ส่วนตัวกลัวในการใช้งาน Mobile Banking Application แต่คิดว่าไม่น่าจะแย่ขนาดนั้น แล้วที่บ้านก็ชอบเล่าข่าวแย่ๆ เกี่ยวกับเรื่องพวกนี้ให้ฟัง แต่หลังๆ ใช้แล้วก็รู้สึกสะดวกดี ไม่มีปัญหาอะไร ก็เลยใช้บ่อยเลย” (เพศหญิง, อายุ 27 ปี, พนักงานบริษัทเอกชน)

“…กลัวการโจรกรรมข้อมูล แต่ก็ไม่ค่อยรู้รายละเอียดว่าเค้าทำกันยังไงบ้าง แต่ก็ไม่เคยเกิดขึ้นกับตัวเอง แต่ถ้าธนาคารให้ยืนยันในการเข้าทำธุรกรรมหลายขั้นตอนก็จะค่อนข้างมั่นใจ เช่น ของธนาคารยูโอบี แต่บางธนาคารที่ขั้นตอนน้อย กดง่าย ก็ไม่ค่อยมั่นใจ” (เพศชาย, อายุ 30 ปี, บริษัทเอกชน)

“…เพราะไม่เคยเจอมากับตัวเลยไม่ค่อยวิตกอะไรมาก แต่ก็ไม่ประมาทเพราะได้ยินข่าวมาบ้าง เช่น มีการแฮคข้อมูลเพื่อใช้กดหรือโอนเงินในบัญชีไปที่อื่น แต่ก็ยอมรับว่าส่วนหนึ่งอาจมาจากความไม่รู้ของผู้ใช้งาน ทำตัวให้ตกอยู่ในภาวะเสี่ยงเอง” (เพศชาย, อายุ 31 ปี, พนักงานธนาคาร)

3. ระวังตนเองในการใช้บริการทุกๆ ครั้งเพื่อป้องกันความเสี่ยง (7 คน) โดยมองว่าหากตนเองไม่มีพฤติกรรมเสี่ยงในการใช้งาน Mobile Banking และรู้เท่าทันภัยคุกคามต่างๆ เป็นอย่างดีแล้ว ก็จะสามารถทำให้ใช้งานได้อย่างปลอดภัย ไร้กังวล ตัวอย่างเช่น การหลีกเลี่ยงต่อ Wifi สาธารณะเมื่อเข้าใช้งาน Mobile Banking หรือการเปลี่ยนรหัสผ่านอยู่สม่ำเสมอ เป็นต้น

“…ส่วนตัวคิดว่า app มีความน่าเชื่อถือ เราเช็คได้ตลอดเวลาว่ามีความเคลื่อนไหวของธุรกรรมยังไงบ้าง แล้วปกติก็จะมีการทำ memo ทุกครั้งที่มีการโอนเงินจะได้ตรวจสอบย้อนกลับไปได้ว่าทำธุรกรรมอะไร เพื่ออะไรในอดีต หากมีอะไรเกิดขึ้นก็มีหลักฐาน” (เพศชาย, อายุ 38 ปี, พนักงานบริษัทเอกชน)

“…เวลาใช้งานทุกครั้งจะระมัดระวังตัวเองตลอด เวลาโอนเงินเสร็จก็จะ log out ทันที” (เพศชาย, อายุ 30 ปี, พนักงานบริษัทเอกชน)

“…เพราะคิดว่าเราควร secure ได้ด้วยตัวเอง ปกติก็จะเปลี่ยนรหัสผ่านทุก 3 เดือน มีตั้ง alert ทางอีเมลเพื่อแจ้งเตือนทุกครั้งที่บัญชีเคลื่อนไหว แล้วก็ตั้ง limit วงเงินถอน โอน ต่อครั้งให้น้อยๆ” (เพศหญิง, อายุ 47 ปี, พนักงานธนาคาร)

4. ธนาคารพาณิชย์ย่อมรักษาชื่อเสียงของตนเอง (2 คน) โดยที่กลุ่มตัวอย่างมองว่าธนาคารพาณิชย์ในฐานะองค์กรขนาดใหญ่ย่อมรักษาภาพพจน์ของตนเอง โดยเฉพาะอย่างยิ่งตัวธุรกิจธนาคารความน่าเชื่อถือถือเป็นหัวใจสำคัญ ดังนั้นการให้บริการใดๆ ย่อมคำนึงถึงความเชื่อมั่นและความปลอดภัยของลูกค้าเป็นอันดับต้นๆ ทำให้ตนเองเกิดความเชื่อมั่นว่าบริการ Mobile Banking ของธนาคารพาณิชย์ย่อมมีความปลอดภัยไปโดยปริยาย

“…ปกติธนาคารพาณิชย์น่าจะต้องห่วงภาพลักษณ์ของตัวเอง เพราะถ้าแบงก์ขาดความน่าเชื่อถือแล้วใครจะกล้าเอาเงินมาฝากหรือเข้ามาทำธุรกรรมด้วย Mobile Banking ก็เหมือนกัน ถ้าเกิดปัญหาขึ้นบ่อยๆ คนก็จะยิ่งกลัวไม่กล้าใช้ ก็เลยคิดว่าธนาคารน่าจะได้คิดวิธีการที่น่าจะดีที่สุดเท่าที่จะทำได้ในการดูแลเรื่องความปลอดภัยของลูกค้า” (เพศชาย, อายุ 31 ปี, พนักงานธนาคาร)

4.1.3 แนวทางการพัฒนาความเชื่อมั่นด้านความปลอดภัยของ Mobile Banking Application

จากการสัมภาษณ์กลุ่มตัวอย่างพบว่าค่าเฉลี่ยความเชื่อมั่นในความปลอดภัยของ Mobile Banking Application อยู่ที่ระดับ 8.03 ดังที่ได้กล่าวมาแล้วข้างต้น กลุ่มตัวอย่างได้ให้ข้อเสนอแนะเพื่อเป็นแนวทางในการพัฒนาความเชื่อมั่นด้านความปลอดภัยให้ดียิ่งขึ้น โดยสามารถแบ่งออกได้เป็น 4 ประเด็นหลักดังนี้

1. วิธีการยืนยันตัวตน (7 คน) โดยกลุ่มตัวอย่างเชื่อว่าหากวิธียืนยันตัวตนด้วยวิธีที่มีความปลอดภัยโดยเฉพาะอย่างยิ่ง OTP จะช่วยสร้างความมั่นใจยิ่งขึ้นในการทำธุรกรรม หรือแม้กระทั่งการใช้ข้อมูลทางชีวภาพ (biometrics) เพื่อช่วยในการยืนยันตัวบุคคลได้ดียิ่งขึ้น

“…ถ้าระบบบังคับให้ใส่ OTP ทุกครั้ง และสแกนลายนิ้วอีกชั้นก่อนการทำธุรกรรมโดยไม่สนจำนวนเงินขั้นต่ำในการทำธุรกรรมก็ดูปลอดภัยดี คล้ายๆกับในอเมริกาที่เคยใช้ตอนไปเรียน” (เพศหญิง, อายุ 30 ปี, พนักงานบริษัทเอกชน)

“….ใช้ OTP เป็นรหัสผ่านหลักก็น่าจะดี เพราะเป็นคนลืมรหัสผ่านบ่อย ถ้าใช้ OTP อย่างเดียวไปเลยก็จะได้ไม่ต้องจำรหัส เพียงแค่มือถืออย่าหาย” (เพศหญิง, อายุ 28 ปี, พนักงานบริษัทเอกชน)

“…ใช้การยืนยันตัวตนด้วยเสียง เพราะน่าจะใช้งานง่ายและค่อนข้างแม่นยำ ถ้าเทียบกับลายนิ้วมือก็ดูเหมือนจะมีข้อจำกัดกับมือถือบางรุ่นที่จะไม่รองรับการสแกนลายนิ้วมือ” (เพศชาย, อายุ 29 ปี, ทันตแพทย์)

“…อยากให้ใช้การยืนยันตัวตนแบบ biometrics เพิ่มมากขึ้น เพราะลอกเลียนแบบได้ค่อนข้างยาก ไม่เหมือนรหัสผ่านที่ถ้าคนอื่นรู้ก็เอาไปใช้ทำธุรกรรมได้เลย” (เพศชาย, อายุ 32 ปี, พนักงานบริษัทเอกชน)

2. ระบบล่ม (3 คน) เกิดจากความกังวลที่ระบบอาจมีปัญหาระหว่างการทำธุรกรรมหรือที่เรียกว่าระบบล่มซึ่งอาจก่อให้เกิดความเสียหาย เช่น เงินในบัญชีของตนเองหายไป แต่

ปลายทางก็ยังคงไม่ได้รับเงินโอน เป็นต้น อย่างไรก็ตามกลุ่มตัวทั้งสามคนนี้ยังไม่เคยประสบปัญหาในลักษณะนี้มาก่อนกับตนเอง

“…ไม่อยากให้เกิดปัญหาระบบล่มตอนทำธุรกรรม เดี๋ยวเงินหาย ไปไม่ถึงปลายทาง เห็นออกข่าวบ่อยๆ เรื่องระบบล่ม โดยเฉพาะช่วงปลายเดือนเวลาเงินเดือนออก แล้วมีคนใช้งาน Mobile Banking เยอะๆ” (เพศหญิง, อายุ 32 ปี, ธุรกิจส่วนตัว)

“…อยากให้พัฒนาระบบให้มีความเสถียรมากกว่านี้ เห็นบางธนาคารลงทุนกับระบบค่อนข้างมาก อย่างเช่นที่ได้ยินมาคือ SCB ลงทุนกับ platform ของ Mobile Banking ประมาณ 4 พันล้าน แล้วเห็นความแตกต่างได้ชัดเลยว่าระบบดีขึ้นกว่าแต่ก่อนมาก ไม่ค้าง ไม่ล่ม มีความเสถียร ถ้าธนาคารอื่นทำตามก็น่าจะดูปลอดภัย และไว้ใจได้” (เพศหญิง, อายุ 26 ปี, พนักงานธนาคาร)

3. เหตุผลอื่นๆ (11 คน) ประกอบไปด้วยหลากหลายประเด็นที่ช่วยเพิ่มระดับความปลอดภัยในการใช้งาน Mobile Banking ในมุมมองของผู้บริโภค ตัวอย่างเช่น เพิ่มระดับความปลอดภัยของ Mobile Banking Application ให้ยากต่อการถูกแฮก มีการแจ้งเตือนความเคลื่อนไหวของบัญชีและธุรกรรมโดยฟรีค่าใช้จ่ายหากทำได้ มีการรับผิดชอบหากเกิดความเสียหายขึ้นกับผู้ใช้งานอย่างรวดเร็ว มี call center รับแจ้งเหตุโดยต้องติดต่อได้ง่ายไม่รอนาน หรือแม้กระทั่งการประยุกต์ใช้เทคโนโลยี Blockchain ในการให้บริการ Mobile Banking Application เป็นต้น

“…ต้องพัฒนาระบบให้ยากที่จะถูกแฮกโดยพวกมิจฉาชีพ เพราะบางทีเราก็ไม่ค่อยได้ระวังตัวเอง และระบบก็ควรป้องกันพวก malware ต่างๆ ได้ด้วย เช่น พวกไวรัส เวิร์ม ที่แอบมาขโมยข้อมูลส่วนตัวในมือถือ” (เพศหญิง, อายุ 29 ปี, พนักงานบริษัทเอกชน)

“…ถ้าเป็นไปได้อยากให้มี SMS alert มาแจ้งเตือนทุกความเคลื่อนไหวของบัญชี และควรที่จะฟรีด้วย เหมือนพวกบัตรเครดิตที่ปกติก็จะแจ้งการใช้บัตรให้เราฟรีผ่าน SMS” (เพศชาย, อายุ 30 ปี, พนักงานรัฐวิสาหกิจ)

“…อยากให้เมื่อเกิดเรื่องมีเจ้าหน้าที่ call center คอยรับเรื่องอย่างรวดเร็ว ไม่ใช่ว่าต้องรอนานกว่าจะรับเรื่องและต้องเคลมง่ายด้วย” (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

“…สมมุติว่าถ้าเงินความเสียหายเพราะแฮกเกอร์ที่ให้สูญเงินไป ธนาคารพาณิชย์ควรมีนโยบายชดเชยค่าเสียหายให้ลูกค้าโดยทันที ไม่ใช่ถ่วงเวลา เพราะบางทีลูกค้าก็จำเป็นต้องใช้เงินก้อนนั้นด่วน หลังจากนั้นธนาคารค่อยมาตรวจสอบหาสาเหตุทีหลังว่าความเสียหายเงินขึ้นจากใครกันแน่ ถ้าเกิดจากตัวลูกค้าเองก็ค่อยไปทวงเงินคืนตอนหลัง แต่ถ้าเป็นแฮกเกอร์ก็ค่อยแจ้งตำรวจดำเนินคดี” (เพศชาย, อายุ 31 ปี, พนักงานธนาคาร)

“…เอาเทคโนโลยี Blockchain เข้ามาใช้ เพราะปกติข้อมูลการเงินและธุรกรรมจะถูกรวมศูนย์ไว้ที่ server ของธนาคารพาณิชย์เองซึ่งก็ไม่ค่อยปลอดภัยถ้าระบบของธนาคารไม่ดีพอแล้วถูกแก๊งโจรกรรมแฮกข้อมูลได้ แต่ถ้าใช้ Blockchain ปัญหานี้ก็จะไม่เกิด เพราะข้อมูลทางการเงินจะถูกฝังไว้ในเครื่องคอมพิวเตอร์หลายๆ เครื่องในเครือข่าย ถ้าแฮกเกอร์จะแก้ไขข้อมูลก็ต้องแก้ข้อมูลที่ฝั่งอยู่ในเครื่องคอมหลายๆ เครื่องในเครือข่ายซึ่งแทบเป็นไปไม่ได้เลย” (เพศหญิง, อายุ 50 ปี, พนักงานธนาคาร)

“…อยากให้มีการ double check คล้ายๆ ของ Gmail กรณีล็อกอินใช้งาน Mobile Banking กับมือถือเครื่องอื่นในเวลาเดียวกัน เช่น ขึ้น pop-up มาถามว่าคนที่ log in อีกเครื่องที่เกิดทีหลังใช่ตัวเราจริงหรือเปล่า” (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

อย่างไรก็ตาม กลุ่มตัวอย่างจำนวน 3 คน เห็นว่าไม่มีทางทำให้ปลอดภัย 100 เปอร์เซ็นต์ โดยมองว่าภัยคุกคามเรื่องความปลอดภัยในการใช้งาน Mobile Banking ไม่สามารถทำให้สมบูรณ์แบบได้ 100 เปอร์เซ็นต์ในความเป็นจริง ผู้ใช้บริการควรปิดช่องโหว่ดังกล่าวเองโดยเพิ่มความระมัดระวังในการเข้าใช้งาน Mobile Banking

“…ไม่สามารถพัฒนาให้สมบูรณ์แบบได้อยู่แล้ว เพราะยังไงก็ต้องมีสิ่งให้แก้ไขอยู่ตลอดเวลา ยิ่งถ้าเป็นเรื่องกับกับเทคโนโลยี เงินๆทองๆ ก็จะมีพวกมิจฉาชีพคอยหาโอกาสเล่นงาน” (เพศชาย, อายุ 32 ปี, พนักงานธนาคาร)

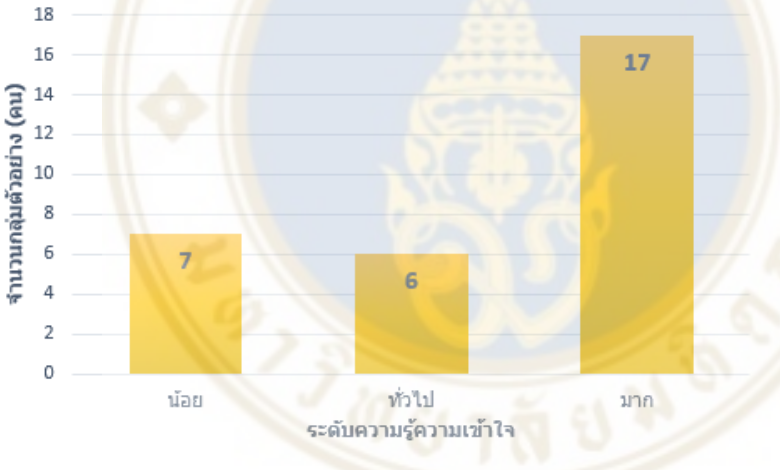
“…พูดยาก แต่ระบบน่าจะมีช่องว่างที่เจาะได้อยู่ดี แต่ก็ขึ้นอยู่กับตัวคนใช้งานด้วยที่จะช่วยปิดหรือลดความเสี่ยงอีกที ไม่ใช่หวังพึ่งธนาคารให้ดูแลรับผิดชอบเพียงฝ่ายเดียว” (เพศชาย, อายุ 30 ปี, ข้าราชการ)

4.2 ความรู้ความเข้าใจในการใช้ Mobile Banking Application ในการทำธุรกรรมทางการเงินอย่างปลอดภัย และการนำไปปฏิบัติ

ในการวัดความรู้ความเข้าใจเบื้องต้นเกี่ยวกับการใช้งาน Mobile Banking Application อย่างปลอดภัย กลุ่มตัวอย่างได้ทำแบบทดสอบจำนวน 10 ข้อ โดยที่แต่ละข้อจะมีข้อความ (statement) กล่าวถึงข้อมูลทั่วไปเกี่ยวกับ Mobile Banking Application และให้กลุ่มตัวอย่างพิจารณาว่าข้อความดังกล่าวเป็นจริงหรือเท็จ โดยเกณฑ์การให้คะแนนมีดังนี้คือ 0-6 คะแนน มีความรู้ความ

เข้าใจในระดับ “น้อย” 7-8 คะแนน มีความรู้ความเข้าใจในระดับ “ทั่วไป” และ 9-10 คะแนน มีความรู้ความเข้าใจในระดับ “มาก” สามารถสรุปผลคะแนนภาพรวมได้ตามภาพที่ 4.2

ภาพที่ 4.2 แจกแจงความถี่จำนวนคนของกลุ่มตัวอย่างในแต่ละระดับคะแนนจากแบบทดสอบ



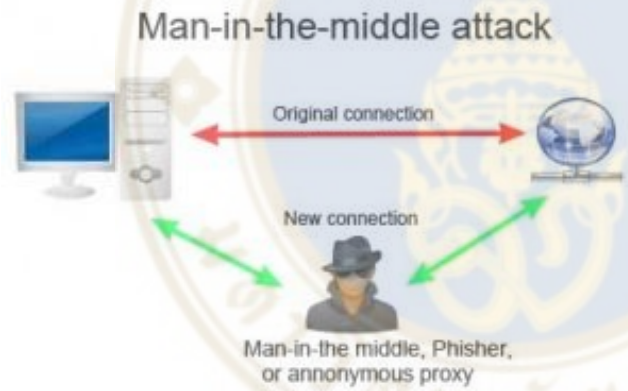
ภาพที่ 4.3 แจกแจงความถี่จำนวนคนของกลุ่มตัวอย่างในแต่ละระดับความรู้ความเข้าใจ

จากภาพที่ 4.3 การทดสอบพบว่ากลุ่มตัวอย่างส่วนใหญ่จำนวน 17 คน (ร้อยละ 57) มีความรู้ความเข้าใจอยู่ในระดับ “มาก” รองลงมาคือ 7 คน (ร้อยละ 23) มีความรู้ความเข้าใจอยู่ในระดับ “น้อย” และ 6 คน (ร้อยละ 20) มีความรู้ความเข้าใจอยู่ในระดับ “ทั่วไป”

ข้อมูลได้จากการสัมภาษณ์โดยอ้างอิงกับแบบทดสอบข้อ 1 ถึง ข้อ 10 สามารถสรุปเป็นประเด็นสำคัญได้ดังนี้

4.2.1 ความคิดเห็นต่อการเชื่อมต่อ Wifi ที่มีความเสี่ยงในแง่ความปลอดภัยในการเข้าใช้บริการ Mobile Banking มากกว่าการเชื่อมต่อเครือข่าย 3G และ 4G

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือการใช้ Wifi มีความเสี่ยงด้านความปลอดภัยในการใช้งาน Mobile Banking Application มากกว่าการเชื่อมต่อเครือข่าย 3G และ 4G เนื่องจากมีการทดสอบโดยให้แฮกเกอร์หมวกขาว (white hat hacker) ทดสอบโดยการพยายามเจาะเข้าระบบโดยอาศัยช่องโหว่ต่างๆ ที่มีอยู่แล้วพบว่าความพยายามแฮกเข้าเครือข่าย 3G และ 4G แทบไม่ประสบความสำเร็จเลยต่างจากการแฮกเข้าเครือข่าย Wifi สาธารณะที่มีโอกาสสำเร็จค่อนข้างสูง เทคนิคที่ใช้ในการทดสอบคือ Man In the Middle attacks (MITM) โดยแฮคเกอร์หมวกขาวจะปลอมเป็นคนกลางเข้ามาแทรกสัญญาณการรับส่งข้อมูลระหว่างผู้ใช้ (เบราว์เซอร์) และเซิร์ฟเวอร์ โดยใช้โปรแกรมดักฟังข้อมูลของเหยื่อ แล้วแฮกเกอร์หมวกขาวก็เป็นตัวกลางส่งผ่านข้อมูลให้ระหว่างเบราว์เซอร์กับเซิร์ฟเวอร์ดังภาพที่ 4.4 ทั้งนี้สิ่งหนึ่งที่ผู้ใช้งาน Mobile Banking Application พึงตระหนักคือไม่มีระบบหรือเครือข่ายไหนที่ปลอดภัยร้อยเปอร์เซ็นต์ (Norton, 2561)



ภาพที่ 4.4 การโจมตีของแฮกเกอร์โดยใช้เทคนิค Man in the Middle attack

หลังการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่ากลุ่มตัวอย่าง 27 คนจาก 30 คน (ร้อยละ 90) มีความรู้ความเข้าใจในเรื่องดังกล่าว

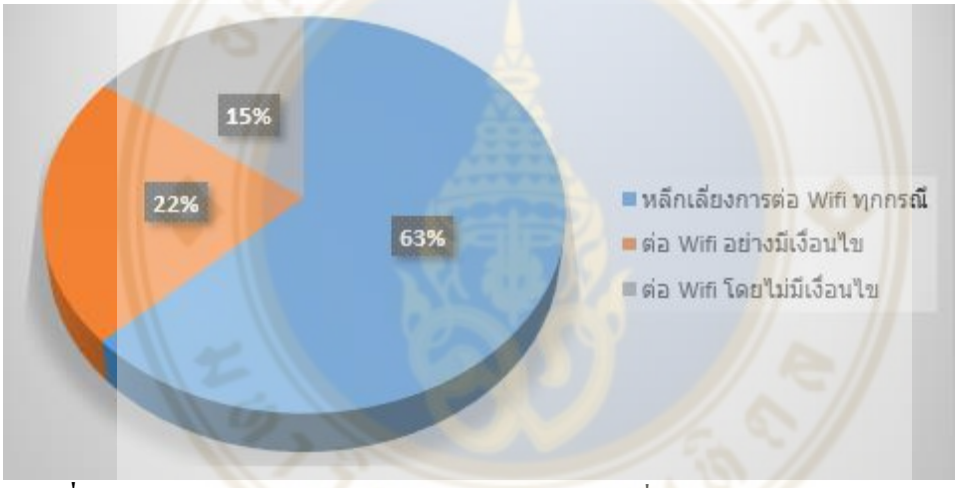
“...ถ้าใช้งานผ่าน 3G 4G ต้องปลอดภัยกว่า Wifi อยู่แล้วเพราะมันเป็นเครือข่ายส่วนตัว ไม่ใช่เครือข่ายที่ผ่านตัวกลางอย่างพวก Wifi โดยเฉพาะ Wifi สาธารณะยิ่งอันตราย เพราะเคยได้ยินว่ามีคนโดนล้วงข้อมูลไปทำธุรกรรมหมดเงินไปแบบไม่รู้ตัว” (เพศชาย, อายุ 33 ปี, พนักงานธนาคาร)

และมีเพียง 3 คน (ร้อยละ 10) ที่ขาดความรู้ความเข้าใจในเรื่องดังกล่าวและเมื่อสัมภาษณ์เพิ่มเติมพบว่าประเด็นที่มีความเข้าใจคลาดเคลื่อนมีดังนี้

“…คิดว่าการต่อผ่านเครือข่าย 3G และ 4G ไม่เป็นเครือข่ายส่วนตัวเหมือน Wifi เพราะฉะนั้นใครจะเข้ามาใช้ก็ได้ ก็น่าจะเสี่ยงที่จะถูกขโมยข้อมูลมากกว่าในความคิด” (เพศหญิง, อายุ 29 ปี, พนักงานบริษัทเอกชน)

“…ดูเหมือนว่า 3G และ 4G เป็นเครือข่าย public ที่ใครจะเข้ามาใช้ก็ได้ มันก็น่าจะถูกโจมตีได้ง่ายกว่าเครือข่าย private อยากพวก Wifi” (เพศชาย, อายุ 32 ปี, พนักงานบริษัทเอกชน)

เมื่อสัมภาษณ์เพิ่มเติมกับกลุ่มตัวอย่างที่ตอบถูกในข้อนี้จำนวน 27 คนในประเด็นการนำความรู้ความเข้าใจดังกล่าวไปใช้จริงในชีวิตประจำวันหรือไม่ พบว่า



ภาพที่ 4.5 แสดงร้อยละของกลุ่มตัวอย่างโดยจะเลือกเชื่อมต่อ Wifi หรือไม่หากต้องทำธุรกรรม Mobile Banking ในชีวิตประจำวัน

กลุ่มตัวอย่างส่วนใหญ่จำนวน 17 คน (ร้อยละ 63) หลีกเลี่ยงการต่อ Wifi ทุกกรณีเมื่อทำธุรกรรมผ่าน Mobile Banking Application (ดังภาพที่ 4.5) โดยให้เหตุผลคล้ายๆ กัน เช่น รู้ว่าไม่ปลอดภัยและได้ยินข่าวเกี่ยวกับการโดนแฮกข้อมูลทางการเงินเมื่อใช้ Wifi

“…พอรู้มาบ้างว่าถ้าใช้ Wifi ฟรีตามที่สาธารณะมีโอกาสถูกแฮกข้อมูลได้ ก็เลยเลี่ยงไม่เชื่อมต่อ Wifi เวลาใช้งาน Mobile Banking แต่จะใช้สัญญาณโทรศัพท์แทน” (เพศชาย, อายุ 33 ปี, พนักงานธนาคาร)

“…ยังไงก็ไม่ใช้ Wifi อยู่แล้วเพราะรู้ว่าไม่ปลอดภัย แล้วตัวเองก็ใช้มีเน็ต 4G อยู่แล้วก็เลยไม่มีปัญหา” (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

ในขณะที่มีกลุ่มตัวอย่างบางส่วนจำนวน 6 คน (ร้อยละ 22) เลือกที่จะเชื่อมต่อ Wifi อย่างมีเงื่อนไข โดยเหตุผลหลักคือต้องสามารถไว้ใจ Wifi ของร้านค้าหรือผู้ให้บริการนั้นๆได้ เป็น Wifi ที่ตัวเองรู้จัก และรวมถึงมีกระบวนการเข้าถึง Wifi ดังกล่าวอย่างเป็นขั้นตอน

"...ถ้ามี Wifi ให้ใช้ฟรีก็ใช้ แต่จะใช้ทำเรื่องอื่น เช่น คุยไลน์ เล่นเฟซบุค เช็คอีเมล แต่จะไม่ใช้ทำธุรกรรมผ่าน Mobile Banking เด็ดขาด" (เพศชาย, อายุ 38 ปี, พนักงานบริษัทเอกชน)

"...ปกติจะเลี่ยงทุกครั้ง แต่ถ้าเป็นร้านประจำแล้วเราก็เป็น Member มีรหัสเข้าใช้ Wifi ที่ต้องขอจากร้านก็จะสบายใจขึ้นในการทำ Mobile Banking" (เพศหญิง, อายุ 47 ปี, พนักงานธนาคาร)

"...ปกติก็ใช้ Wifi แต่ต้องมั่นใจในเครือข่าย หรือเป็นของร้านที่เรารู้จักถึงจะเชื่อมต่อ" (เพศชาย, อายุ 31 ปี, ธุรกิจส่วนตัว)

ในขณะที่กลุ่มตัวอย่างส่วนน้อยจำนวน 4 คน (ร้อยละ 15) ตัดสินใจเชื่อมต่อ Wifi เพื่อทำธุรกรรมผ่าน Mobile Banking โดยไม่ลังเล

"...ถ้ามี Wifi ฟรีให้ต่อก็ใช้ คิดว่าไม่น่าจะเป็นไร ขึ้นอยู่กับดวง" (เพศชาย, อายุ 31 ปี, ธุรกิจส่วนตัว)

"...ปกติไม่แคร์ ถ้าเครือข่ายอันไหนเร็วกว่าก็ใช้อันนั้น ถ้า Wifi เร็วกว่า 3G ก็เลือกต่อ Wifi" (เพศชาย, อายุ 32 ปี, พนักงานธนาคาร)

4.2.2 ความคิดเห็นต่อการทำธุรกรรมผ่าน Mobile Banking Application ที่มีความเสี่ยงน้อยกว่าการทำธุรกรรมผ่าน Website ของธนาคาร

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือการทำธุรกรรมผ่าน Mobile Banking และ Website ของธนาคารต่างมีความเสี่ยงทั้งคู่ แต่เนื่องจากอุปกรณ์ฮาร์ดแวร์ที่มากับพร้อมกับโทรศัพท์มือถือจึงทำให้การทำธุรกรรมผ่าน Mobile Banking มีความปลอดภัยสูงกว่า อาทิเช่น การมีเทคโนโลยีที่สามารถบอกพิกัดหรือจุดใช้งานโทรศัพท์มือถือ หรือการมีระบบสแกนนิ้วมือเพื่อการยืนยันตัวตน เป็นต้น เหล่านี้จึงทำให้การใช้งานผ่านโทรศัพท์มือถือมีความปลอดภัยมากกว่าแล็ปท็อปและคอมพิวเตอร์พีซี (ข้อมูลจากธนาคาร Starling Bank) ในการเข้า internet banking ผ่าน web browser ต้องสังเกตรูปแม่กุญแจสีเหลืองต้อง Lock อยู่เสมอ (ซึ่งหมายถึง https:// โดย s หมายถึง security) ซึ่งแปลว่ามีการเข้ารหัสและเป็นการติดต่อไปยัง Server ของธนาคารอยู่จริง แต่ถ้าเข้าผ่านโปรแกรม Mobile banking ทางมือถือ เราจะไม่เห็น URL หรือแม่กุญแจนั้นแล้ว แต่ทางธนาคารจะ

บังคับให้ต้องเข้ารหัสหรือ https อยู่เสมออยู่แล้ว ซึ่งแสดงว่าจะปลอดภัยมากขึ้น (Maybank Kim Eng Securities, 2557)

จากการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่า 25 คนจากกลุ่มตัวอย่าง (ร้อยละ 83) มีความรู้ความเข้าใจในเรื่องดังกล่าว

“...App น่าจะปลอดภัยมากกว่าเพราะเหมือนเป็น gateway โดยเฉพาะของธนาคารเพื่อให้ลูกค้าทำธุรกรรมออนไลน์ แต่ Website บางทีก็มีเว็บปลอม แล้วถ้า search หาเว็บธนาคารใน google เพื่อทำธุรกรรมยิ่งอันตรายถ้าไม่ดู URL ให้ดีดี” (เพศชาย, อายุ 30 ปี, พนักงานบริษัทเอกชน)

“...ถ้า website ปลอดภัยมากกว่า app ธนาคารคงไม่พยายามโปรโมทให้คนโหลด app ของตัวเองไปใช้งาน แล้วถ้ายิ่งมีคนใช้งาน app เยอะธนาคารเองก็น่าจะยิ่งต้องพัฒนาระบบความปลอดภัยให้ดีขึ้นไปอีก” (เพศชาย, อายุ 32 ปี, พนักงานธนาคาร)

กลุ่มตัวอย่างเพียง 5 คน (ร้อยละ 17) ขาดความรู้ความเข้าใจในเรื่องดังกล่าวและเมื่อสัมภาษณ์เพิ่มเติมพบว่าประเด็นที่มีความเข้าใจคลาดเคลื่อนมีดังนี้

“...ถ้าเข้าผ่าน Website น่าจะเสี่ยงน้อยกว่า โดยเฉพาะที่แสดง URL ว่าเป็น https:// จะมั่นใจเป็นพิเศษว่าจะไม่ถูกแฮกข้อมูล” (เพศหญิง, อายุ 29 ปี, พนักงานบริษัทเอกชน)

“…คิดว่ามี https:// ดูปลอดภัยดี แต่ Mobile Banking เคยได้ยินข่าว่ามี app ปลอมน่าจะไม่ค่อยปลอดภัย” (เพศชาย, อายุ 30 ปี, พนักงานรัฐวิสาหกิจ)

“…เคยใช้มานานก่อน Mobile Banking เลยคิดว่าน่าจะปลอดภัยดีถ้าเข้าผ่าน Website ธนาคาร” (เพศหญิง, อายุ 28 ปี, พนักงานบริษัทเอกชน)

4.2.3 ความคิดเห็นในเรื่องการเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่คุ้นเคยไม่ได้ปลอดภัยกว่าการเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่ไม่คุ้นเคย

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือแฮกเกอร์จะพยายามตั้งชื่อ Wifi ในการเชื่อมต่อเป็นชื่อร้านค้าที่คนส่วนใหญ่รู้จักเพื่อให้เหยื่อหลงกลและเชื่อมต่อ Wifi ที่เป็นของปลอมทำให้ข้อมูลที่ส่งผ่านเครือข่าย Wifi ดังกล่าวถูกดักจับโดยแฮกเกอร์เพื่อใช้ในทางที่อาจก่อให้เกิดความเสียหายแก่ผู้ใช้งาน หรือแม้กระทั่ง Wifi ของร้านค้าที่เรารู้จักเป็นอย่างดีก็ไม่ควรใช้งานหากไม่จำเป็น เพราะข้อมูลส่วนตัวบางอย่าง เช่น รหัสผ่านในการเข้าใช้บริการเว็บต่างๆ อาจถูกขโมยจากพนักงานภายในร้านที่ไม่ประสงค์ดีและมีความทักษะด้านคอมพิวเตอร์เป็นอย่างดี ดังนั้นจึงนำมาสู่

ข้อสรุปได้ว่าการเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่เรารู้จักไม่ได้ปลอดภัยกว่าการเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่เราไม่รู้จักแต่อย่างใด (Maybank Kim Eng Securities, 2557)

หลังการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่ากลุ่มตัวอย่าง 16 คน (ร้อยละ 53) มีความรู้ความเข้าใจในเรื่องดังกล่าว

"...ชื่อ Wifi จะตั้งเป็นชื่ออะไรก็ได้อยู่แล้ว ที่สำคัญคือต้องมั่นใจว่าเป็นของร้านนั้นจริงหรือเปล่า เคยได้ยินข่าวอยู่ว่ามันจะมีพวกแฮกเกอร์ปล่อย Wifi ให้ใช้ฟรีแต่พวกนี้จะเข้าไปล้วงข้อมูลเราได้" (เพศชาย, อายุ 32 ปี, พนักงานธนาคาร)

"...ร้านค้าอย่าง Starbucks ปกติก็จะถามรหัสผ่านแบบนี้ก็ดู secure ดีแต่เราจะรู้ได้ไงว่า Wifi ที่ชื่อ Starbucks มันจะเป็นของจริง เพราะชื่อ Wifi มันสามารถตั้งซ้ำกันได้ มันก็มีโอกาสให้พวกมิจฉาชีพหากินได้" (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

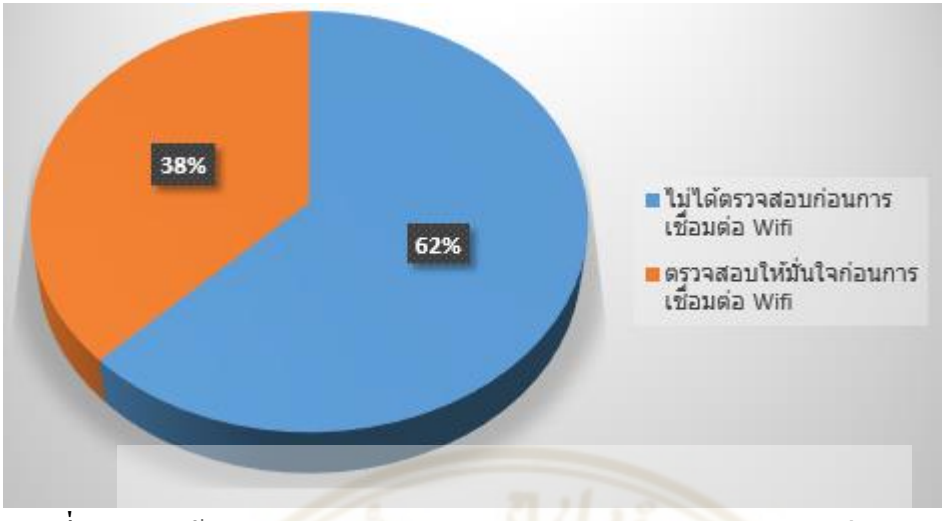
ในขณะที่กลุ่มตัวอย่าง 14 คน (ร้อยละ 47) ยังขาดความรู้ความเข้าใจในเรื่องดังกล่าว และเมื่อสัมภาษณ์เพิ่มเติมพบว่าประเด็นที่มีความเข้าใจคลาดเคลื่อนส่วนใหญ่เกิดจากความเชื่อว่า Wifi ที่แสดงชื่อร้านค้าที่รู้จักน่าจะรักษาชื่อเสียงของตนเอง สามารถไว้ใจได้ และไม่น่าจะถูกแฮก

"...ถ้า Wifi ชื่อที่เรารู้จัก เค้าเองคงไม่อยากเสียชื่อเสียง โดยส่วนใหญ่ก็จะเชื่อมต่อเลยเพราะไว้ใจ" (เพศหญิง, อายุ 32 ปี, ธุรกิจส่วนตัว)

"...คิดว่าถ้าร้านที่มีชื่อเสียง น่าจะรักษาชื่อเสียง โดยให้ความสำคัญกับเรื่องความปลอดภัย ข้อมูลส่วนตัวของลูกค้า ไม่งั้นอาจเป็นเรื่องราวใหญ่โตได้" (เพศหญิง, อายุ 50 ปี, พนักงานธนาคาร)

"...ถ้าเป็น Wifi ที่เรารู้จักน่าจะไม่โดนแฮก แต่ถ้าเป็น Wifi สาธารณะทั่วไปที่เราไม่รู้จักน่าจะมีความเป็นไปได้ที่จะถูกแฮก" (เพศชาย, อายุ 29 ปี, ทันตแพทย์)

เมื่อสัมภาษณ์เพิ่มเติมกับกลุ่มตัวอย่างที่ตอบถูกในข้อนี้จำนวน 16 คนในประเด็นการนำความรู้ความเข้าใจดังกล่าวไปใช้จริงในชีวิตประจำวันหรือไม่ พบว่า



ภาพที่ 4.6 แสดงร้อยละของกลุ่มตัวอย่างว่ามีการตรวจสอบ Wifi สาธารณะก่อนการเชื่อมต่อหรือไม่ในชีวิตประจำวัน

กลุ่มตัวอย่างส่วนใหญ่จำนวน 10 คน (ร้อยละ 62) ไม่ได้ตรวจสอบก่อนการเชื่อมต่อ Wifi หรือมีพฤติกรรมที่ค่อนข้างละเลยในเรื่องความปลอดภัยในเชื่อมต่อ Wifi สาธารณะ (ดังภาพที่ 4.6) โดยกลุ่มตัวอย่างอธิบายว่าในชีวิตจริงมีแนวโน้มเชื่อมต่อ Wifi สาธารณะอะไรก็ได้ หากจำเป็นต้องใช้ก็จะใช้ หากเป็นชื่อ Wifi ที่ใช้อยู่ประจำก็จะใช้ไม่ค่อยได้ระวังตัวเท่าไหร่ หรือหากเป็นชื่อที่คุ้นเคยก็จะเชื่อมต่อ

"...ในชีวิตจริงเป็นชื่อ Wifi อะไรก็ได้เหมือนกันหมด ส่วนใหญ่ก็จะเชื่อมต่อเลยถ้าไม่ต้องเสียเงินหรือขอรหัสผ่าน" (เพศชาย, อายุ 30 ปี, พนักงานบริษัทเอกชน)

"...สมมุติว่าถ้าแพ็คเกจอินเตอร์เน็ต 4G หมด แล้วถ้าแถวนั้นมี Wifi ให้เชื่อมต่อฟรีก็กล้าต่อ แต่อาจจะเลือกต่อ Wifi ที่แสดงชื่อเป็นร้านค้าที่เราค่อนข้างรู้จัก" (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

"...ปกติจะต่อเลย ไม่ค่อยสงสัยหรือระแวงอะไรมากในชีวิตจริง แต่ถ้าร้านมีให้กรอกรหัส Wifi ด้วยก็จะรู้สึกอุ่นใจยิ่งขึ้น" (เพศหญิง, อายุ 27 ปี, พนักงานธนาคาร)

"...ในชีวิตจริงถ้าเชื่อมต่อได้ก็เชื่อม แต่เวลาเชื่อมต่อ Wifi สาธารณะจะไม่ค่อยใช้ Mobile Banking เพื่อความปลอดภัย" (เพศชาย, อายุ 32 ปี, พนักงานธนาคาร)

ในขณะที่กลุ่มตัวอย่างจำนวน 6 คน (ร้อยละ 38) มีความตระหนักในเรื่องความปลอดภัยและจะตรวจสอบให้มั่นใจก่อนการเชื่อมต่อ Wifi สาธารณะ

“…ปกติก็ระวังตัวเรื่อง Wifi ปลอมที่หลอกแฮกข้อมูลอยู่ตลอด ปกติถ้าจะใช้งานก็จะถามพนักงานร้านค้าให้มั่นใจว่าเป็น Wifi ของร้านหรือเปล่า แล้วจะไม่ทำธุรกรรมผ่าน Mobile Banking” (เพศชาย, อายุ 31 ปี, พนักงานบริษัทเอกชน)

4.2.4 ความคิดเห็นต่อการใช้งาน Mobile Banking Application ว่าควร log out ออกจากระบบเสมอหลังใช้งานเสร็จ

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือควรมีการ log out ออกจากระบบทุกครั้ง เพราะหากมือถือถูกโจรกรรมในขณะที่เปิด Mobile Banking Application มิจฉาชีพอาจเข้าไปใช้งานและก่อให้เกิดความเสียหายขึ้นได้ ในกรณีของธนาคาร Fannin Bank ประเทศสหรัฐอเมริกาได้กล่าวว่าระบบของธนาคารเองมีหน่วงเวลาในการ log out อัตโนมัติอยู่ที่ 3 นาที ซึ่งในหลายๆครั้งสิ่งที่ไม่คาดคิดอาจเกิดขึ้นได้ภายใน 3 นาทีดังนั้นผู้ใช้งานจึงไม่ควรเปิดโอกาสนั้น (Fannin Bank, 2561) หลังการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่ากลุ่มตัวอย่าง 26 คน (ร้อยละ 87) มีความรู้ความเข้าใจในเรื่องดังกล่าว

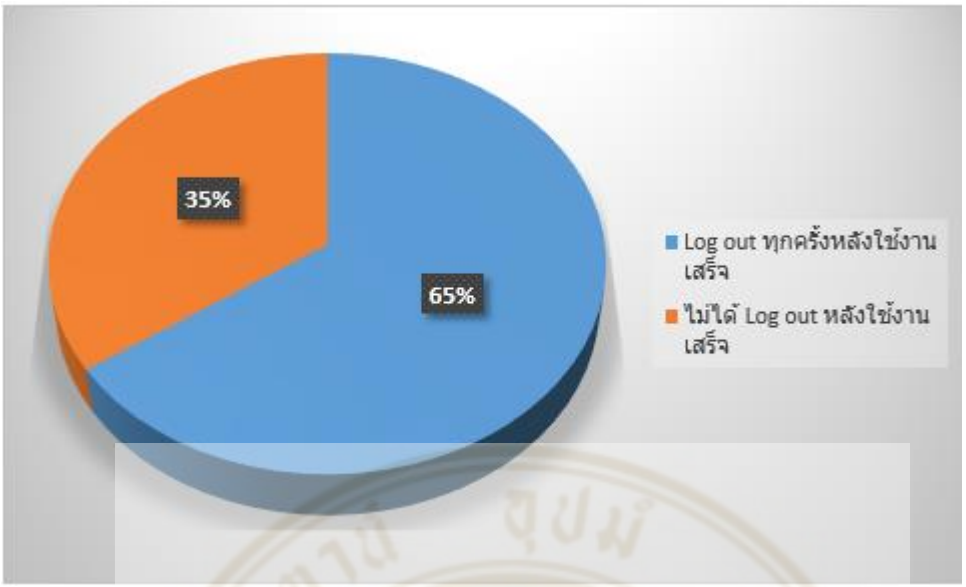
“...จริงๆ ถ้าคิดแบบรอบคอบก็น่าจะต้อง log out ออกทุกครั้ง เพราะเราไม่รู้ว่าจะเกิดอะไรขึ้น บางทีอาจลืมโทรศัพท์ทิ้งไว้แป๊บเดียวแล้วถูกขโมยไปก็มีความเสี่ยงถ้ายังเปิดใช้งาน Mobile Banking ค้างไว้อยู่” (เพศหญิง, อายุ 32 ปี, ธุรกิจส่วนตัว)

“...ปลอดภัยไว้ก่อน ยังไงก็ต้อง log out หลังใช้ Mobile Banking App เสร็จ อย่างน้อยก็ไม่ต้องกลัวว่าจะถูกขโมยหรือแอบเอาไปใช้” (เพศหญิง, อายุ 34 ปี, พนักงานธนาคาร)

ในขณะที่กลุ่มตัวอย่าง 4 คน (ร้อยละ 13) ที่ขาดความรู้ความเข้าใจในเรื่องดังกล่าวและเมื่อสัมภาษณ์เพิ่มเติมพบว่าประเด็นที่มีความเข้าใจคลาดเคลื่อนส่วนใหญ่นั้นเกิดจากความเข้าใจว่าระบบจะ log out ให้อัตโนมัติเมื่อเลิกใช้งานจึงไม่จำเป็นต้องกด log out ออกในทุกๆ ครั้ง

“... ปกติระบบก็จะ log out ให้เองโดยอัตโนมัติอยู่แล้วเวลาไม่ได้ใช้งานนานๆ สัก 2-3 นาที ถ้าจะใช้งานอีกทีก็แค่ log in เข้าไปใหม่” (เพศหญิง, อายุ 50 ปี, พนักงานธนาคาร)

เมื่อสัมภาษณ์เพิ่มเติมกับกลุ่มตัวอย่างที่ตอบถูกในข้อนี้จำนวน 26 คนในประเด็นการนำความรู้ความเข้าใจดังกล่าวไปใช้จริงในชีวิตประจำวันหรือไม่ พบว่า



ภาพที่ 4.7 แสดงร้อยละของกลุ่มตัวอย่างว่ามีการ log out ออกจาก Mobile Banking Application ทุกครั้งหลังใช้งานเสร็จหรือไม่

กลุ่มตัวอย่างส่วนใหญ่จำนวน 17 คน (ร้อยละ 65) มีการปฏิบัติตนตามสิ่งที่รู้อย่างเคร่งครัด (ดังภาพที่ 4.7) โดยกลุ่มตัวอย่างอธิบายว่า เคยชินและทำเป็นนิสัย มีความกลัวหากมือถือถูกขโมย และล็อกหน้าจอเพียงอย่างเดียวไม่น่าเพียงพอ

"…ปกติจะ log out ตลอดเพราะกลัวมือถือหายแล้วใช้งาน Mobile Banking ค้างอยู่เดี๋ยวพวกหัวขโมยจะแอบโอนเงินไปบัญชีอื่นได้" (เพศหญิง, อายุ 32 ปี, ธุรกิจส่วนตัว)

"…เคยโทรศัพท์หายแล้วกังวลมากว่าใครจะเอา Mobile Banking เราไปใช้หรือเปล่า ตอนนี้ก็เลย log out ทุกครั้งที่ใช้เสร็จเพื่อความสบายใจ" (เพศหญิง, อายุ 34 ปี, พนักงานธนาคาร)

"…log out ตลอดเพราะทำเป็นนิสัยตั้งแต่สมัยแรกๆ ที่เริ่มใช้งาน รู้สึกปลอดภัยดี" (เพศชาย, อายุ 33 ปี, พนักงานธนาคาร)

ในขณะที่กลุ่มตัวอย่างจำนวน 6 คน (ร้อยละ 38) ไม่ได้มีการ log out หลังใช้งานเสร็จ โดยให้เหตุผลว่า หน่วงเวลาของระบบในการ log out อัตโนมัติค่อนข้างสั้นน่าจะปลอดภัย และใช้วิธีปิดแอพโดยไม่ log out

"…คิดว่าหน่วงเวลาสั้น น่าจะแค่ราวๆ 1 นาที ระบบมันก็จะ log out ให้เองอัตโนมัติเลยไม่ log out" (เพศชาย, อายุ 31 ปี, พนักงานบริษัทเอกชน)

"…หลังใช้ Mobile Banking เสร็จปกติจะใช้วิธีปิดแอพไปเลย เพราะเร็วดี ไม่ต้องหาปุ่มกดปิดแอพ" (เพศชาย, อายุ 31 ปี, พนักงานธนาคาร)

4.2.5 ความคิดเห็นในเรื่องดาวน์โหลด Application จาก App Store สำหรับระบบปฏิบัติการ iOS ว่าไม่ได้ปลอดภัยจากมัลแวร์ (malware)

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือ Application บางตัวบน App Store มี malware แฝงตัวอยู่และมีหลายกรณีที่เป็นข่าวในอดีต ล่าสุดในปี พ.ศ. 2561 มีการเปิดเผยข้อมูลว่า Application หลายตัวบน App store โดยเฉพาะอย่างยิ่ง utility application มี malware แฝงตัวอยู่โดยจะดักจับข้อมูลประวัติการใช้งานเว็บไซต์ต่างๆ ซอฟต์แวร์บนมือถือที่ผู้ใช้งานติดตั้งว่ามีอะไรบ้าง ซึ่งข้อมูลทั้งหมดดูเหมือนว่าจะถูกส่งไปยังเซิฟเวอร์ในประเทศจีน แต่ในขณะที่ปี พ.ศ. 2560 Apple ได้ออกมาปรับกฎของ App Store ใหม่โดยจะไม่อนุญาตให้ Application ประเภทสแกนไวรัสและมัลแวร์ไม่สามารถอยู่บน App Store ได้อีกต่อไปโดยมีเหตุผลคือไม่ต้องการให้ผู้ใช้งานเกิดความเชื่อว่า iOS สามารถโดนไวรัสและมัลแวร์เล่นงานได้ หรือก็คือพยายามรักษาภาพพจน์ว่า iOS เป็นระบบปฏิบัติการที่ปลอดภัยจากมัลแวร์ร้อยเปอร์เซ็นต์ โดยที่คำว่ามัลแวร์ ย่อมาจากคำว่า Malicious Software ซึ่งหมายถึงโปรแกรมประสงค์ร้ายต่าง ๆ ที่ทำงานในลักษณะที่เป็นการโจมตีระบบ ทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล ซึ่งมัลแวร์แบ่งออกได้หลายประเภท เช่น ไวรัส (Virus), เวิร์ม (Worm), ม้าโทรจัน (Trojan Horse), การแอบดักจับข้อมูล (Spyware), แอ็ดแวร์ (Adware) และอื่น ๆ ดังนั้นจะถือได้ว่า มัลแวร์คือคำรวม ๆ ทั้งหมดของโปรแกรมที่มีจุดประสงค์ร้ายดังกล่าว (Paul, 2015)

หลังการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่ากลุ่มตัวอย่าง 19 คน (ร้อยละ 63) มีความรู้ความเข้าใจในเรื่องดังกล่าว

“...ตอนแรกก็คิดว่า iOS จะรอดจาก malware 100% แต่เหมือนเคยอ่านเจอข่าวว่าโทรศัพท์มือถือ iPhone ก็มีพวก malware แฝงอยู่ด้วยเหมือนกัน” (เพศชาย, อายุ 31 ปี, พนักงานธนาคาร)

“...น่าจะมีโอกาสมี malware อยู่เหมือนกัน แต่โอกาสคงจะน้อยมากๆ เพราะ Apple ไม่ได้เปิดให้ใครก็ได้มาพัฒนาหรือใส่ application ไว้ใน App Store ได้ง่ายๆ เหมือนของ Android” (เพศหญิง, อายุ 34 ปี, พนักงานธนาคาร)

ในขณะที่กลุ่มตัวอย่าง 11 คน (ร้อยละ 37) ที่ขาดความรู้ความเข้าใจในเรื่องดังกล่าว และเมื่อสัมภาษณ์เพิ่มเติมพบว่าประเด็นที่มีความเข้าใจคลาดเคลื่อนส่วนใหญ่เกิดจากการรับรู้ส่วนตัวว่า App Store ไม่มีข่าวเรื่องมัลแวร์มาก่อน ไม่เคยเห็นว่า App store มีโปรแกรม anti-virus

ให้ดาวน์โหลดเลยคิดว่าปลอดภัย จากประสบการณ์ใช้งานส่วนตัวที่ไม่เคยเจอเรื่องมัลแวร์บน App store และคิดว่า App Store น่าจะมีการตรวจสอบที่ดีก่อนนำ Application ต่างๆ ขึ้นสู่ App store

"…App store ไม่น่าจะมีปัญหาไวรัส มัลแวร์ เพราะว่าตั้งแต่ใช้งานมาไม่เคยเห็นโปรแกรม anti-virus ให้ดาวน์โหลดมาใช้ ถ้ามีปัญหาจริงก็น่าจะมีโปรแกรมพวกนี้ให้ดาวน์โหลด" (เพศหญิง, อายุ 32 ปี, ธุรกิจส่วนตัว)

"…คิดว่า iOS ปลอดภัยกว่าเยอะเพราะตั้งแต่ใช้งานมาไม่เคยเจอมัลแวร์ และก็ไม่เคยได้ยินข่าวติดไวรัสเหมือน Android" (เพศชาย, อายุ 32 ปี, พนักงานบริษัทเอกชน)

"…น่าจะมีการตรวจสอบ Application ของผู้พัฒนามาก่อนที่จะอัพโหลดขึ้น App store" (เพศหญิง, อายุ 26 ปี, พนักงานธนาคาร)

4.2.6 ความคิดเห็นในเรื่องการพิจารณา Mobile Banking Application ของจริงว่าต้องดูที่ชื่อผู้พัฒนา (Developer) ซึ่งจะแสดงชื่อสถาบันการเงินนั้นๆ

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือการตรวจสอบ Mobile Banking Application ที่เหมาะสมคือการดูที่ชื่อผู้พัฒนาก่อนการดาวน์โหลด Application ทุกครั้ง โดยที่ของจริงจะแสดงเป็นชื่อของธนาคารดังกล่าว แต่หากเป็นของปลอมจะเป็นชื่ออย่างอื่นที่ไม่มีความเกี่ยวข้องกับธนาคารดังกล่าว ซึ่งในอดีตที่ผ่านมาเคยมีตัวอย่าง Application ปลอมที่เกิดขึ้นกับธนาคารกสิกรไทย และ ธนาคารไทยพาณิชย์ ซึ่งมีผู้ใช้งาน Mobile Banking Application มากเป็นอันดับ 1 และอันดับ 2 ของประเทศตามลำดับ ซึ่งสร้างความเสียหายเป็นวงกว้างกับผู้เสียหายที่ตกเป็นเหยื่อ เพราะหากผู้เสียหายดาวน์โหลดและนำไปใช้งานจริงจะทำให้มิจฉาชีพได้ข้อมูลส่วนตัวเพื่อใช้ในการ log in เข้าใช้งาน Mobile Banking ดังกล่าว (ธนาคารแห่งประเทศไทย, 2557)

หลังการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่า 23 คนจากกลุ่มตัวอย่าง (ร้อยละ 77) มีความรู้ความเข้าใจในเรื่องดังกล่าว

"...ดูคะแนนรีวิวของคนใช้งานก็เป็นส่วนหนึ่ง แต่เท่าที่รู้มาคือต้องดูที่ชื่อ developer ว่าบริษัทอะไรเป็นคนทำ app ตัวนั้นขึ้นมา" (เพศชาย, อายุ 31 ปี, พนักงานบริษัทเอกชน)

"...เท่าที่รู้คือถ้าให้ดีสุดต้องดูตรงชื่อผู้พัฒนาว่าเป็นใคร แต่ปกติก็ควรต้องดูอย่างอื่นประกอบไปด้วย เช่น คนดาวน์โหลดกันเยอะไหม คอมเม้นท์คนใช้งานเป็นยังไงบ้าง" (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

ในขณะที่ 7 คนจากกลุ่มตัวอย่าง (ร้อยละ 23) ที่ขาดความรู้ความเข้าใจในเรื่องดังกล่าว และเมื่อสัมภาษณ์เพิ่มเติมพบว่าประเด็นที่มีความเข้าใจคลาดเคลื่อนส่วนใหญ่นั้นเกิดจากความไม่รู้ คิดว่าควรดูยอดการดาวน์โหลดเป็นหลัก ดูรีวิวของผู้ใช้งาน

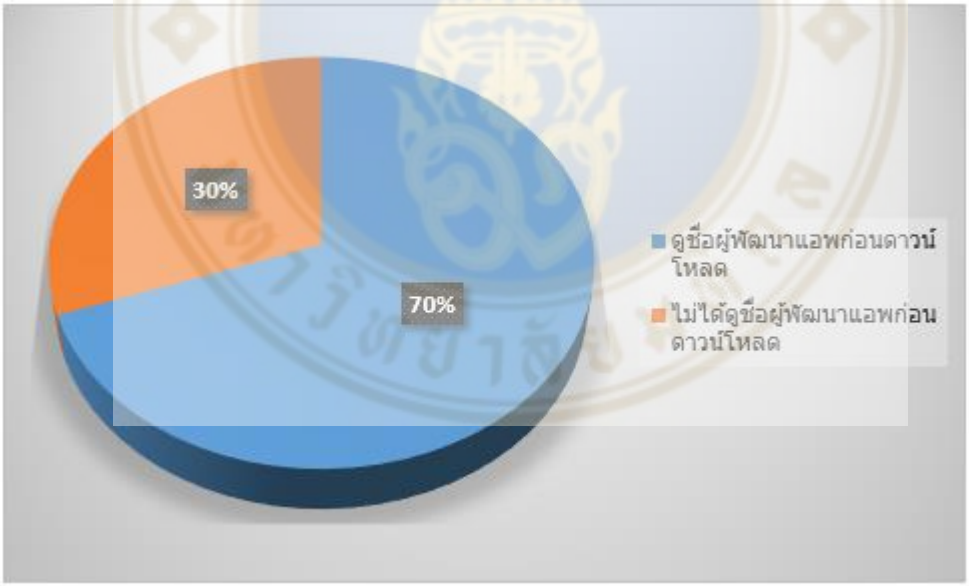
"...คิดว่าควรดูรีวิวเป็นหลัก ดูดาวที่ผู้ใช้งานให้ แล้วก็ใช้เซ็นส์ของตัวเอง" (เพศหญิง, อายุ 26 ปี, พนักงานธนาคาร)

"...บอกตามตรงว่าดูไม่ออกว่าอันไหนจริงอันไหนปลอม ดูยาก" (เพศหญิง, อายุ 34 ปี, พนักงานธนาคาร)

"...ดูไม่ค่อยออกว่าอันไหนจริงหรือปลอม แต่โดยส่วนตัวจะดูหน้าตา ดูดาว ดูภาพรวมๆ" (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

"...ดูยอดดาวน์โหลด ถ้ามากก็น่าจะเชื่อถือได้" (เพศชาย, อายุ 35 ปี, พนักงานบริษัทเอกชน)

เมื่อสัมภาษณ์เพิ่มเติมกับกลุ่มตัวอย่างที่ตอบถูกในข้อนี้จำนวน 23 คนในประเด็นการนำความรู้ความเข้าใจดังกล่าวไปใช้จริงในชีวิตประจำวันหรือไม่ พบว่า



ภาพที่ 4.8 แสดงร้อยละของกลุ่มตัวอย่างว่ามีการดูชื่อผู้พัฒนา Mobile Banking Application ก่อนการดาวน์โหลดหรือไม่

กลุ่มตัวอย่างส่วนใหญ่จำนวน 16 คน (ร้อยละ 70) มีการปฏิบัติตนตามสิ่งที่รู้ในชีวิตจริง (ดังภาพที่ 4.8) โดยกลุ่มตัวอย่างอธิบายว่านอกเหนือจากการดูชื่อผู้พัฒนาแล้ว กลุ่มตัวอย่างยังเสริมว่าต้องดู

ข้อมูลอื่นๆ ประกอบด้วย อาทิเช่น ดูยอดดาวน์โหลด เวลาดาวน์โหลดให้ไปที่เว็บไซต์หลักของธนาคารก่อน ดูรีวิว ดูภาพรวมทั้งหมด

“…ปกติจะดูชื่อ developer กับดูยอดดาวน์โหลดเป็นหลัก ถ้าของปลอมคนก็จะดาวน์โหลดไม่เยอะ” (เพศชาย, อายุ 31 ปี, พนักงานบริษัทเอกชน)

“…ถ้าจะให้มั่นใจยิ่งขึ้น ต้องเข้าเว็บไซต์หลักของธนาคาร แล้วมันจะมีให้สแกน QR Code เพื่อดาวน์โหลดแอพลงมือถืออีกที ก่อนดาวน์โหลดก็ดูชื่อ developer อีกทีเพื่อความมั่นใจ” (เพศชาย, อายุ 38 ปี, พนักงานบริษัทเอกชน)

“…นอกจากดู Developer แล้วก็จะดูรีวิว หน้าตา โลโก้ ฟีดแบคว่าเป็นยังไงบ้างก่อนดาวน์โหลด” (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

ในขณะที่กลุ่มตัวอย่างจำนวน 7 คน (ร้อยละ 30) ไม่ได้มีการสังเกตอะไรเป็นพิเศษก่อนการดาวน์โหลด Mobile Banking Application

“…ส่วนตัวไม่ค่อยสังเกต พอมัน search แล้วขึ้นอะไรมาเป็นอันแรกก็ดาวน์โหลดเลย” (เพศหญิง, อายุ 28 ปี, พนักงานบริษัทเอกชน)

4.2.7 ความคิดเห็นในเรื่องการดาวน์โหลดซอฟต์แวร์ฟรีบนอินเตอร์เน็ตมีส่วนเกี่ยวข้องกับการติดมัลแวร์

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือการดาวน์โหลดซอฟต์แวร์ฟรีบนโลกออนไลน์เปิดโอกาสเสี่ยงในการติดมัลแวร์ได้โดยไม่รู้ตัว โดยที่แฮกเกอร์จะพัฒนาซอฟต์แวร์ที่แฝงมัลแวร์โดยส่วนใหญ่จะเป็นของฟรีเพื่อดึงดูดให้คนทั่วไปตัดสินใจดาวน์โหลดได้โดยง่าย (Google Ads, 2561)

หลังการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่าทุกคนต่างตระหนักถึงข้อมูลดังกล่าวเป็นอย่างดี ไม่มีผู้ใดตอบคำถามในข้อนี้ผิด

“...ที่จริงน่าจะเกี่ยวข้องกัน เพราะของฟรีไม่มีบนโลก ส่วนใหญ่อะไรฟรีๆ ให้สงสัยไว้ก่อนว่าต้องมีอะไรแอบแฝงอยู่หรือเปล่า เช่น พวกไวรัส” (เพศชาย, อายุ 35 ปี, พนักงานบริษัทเอกชน)

“...ต้องเกี่ยวข้องกันอยู่แล้ว เพราะพวกที่พัฒนา app หรือโปรแกรมที่เป็นพวกมิจฉาชีพก็มี และถ้าจะให้เหยื่อหลงกลก็ต้องให้ดาวน์โหลดฟรีไปใช้” (เพศชาย, อายุ 29 ปี, ทันตแพทย์)

4.2.8 ความคิดเห็นต่อการเก็บรหัสเข้าใช้งาน Mobile Banking Application เป็นความลับ

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือผู้ใช้งานไม่ควรบอกรหัสเข้าใช้งาน Mobile Banking Application ให้แก่บุคคลอื่นทราบ ถึงแม้ว่าจะเป็นคนในครอบครัวก็ตาม เพราะมีหลายกรณีที่ความเสียหายเกิดขึ้นจากการไว้วางใจบุคคลใกล้ชิด ดังนั้นเพื่อความปลอดภัยสูงสุดผู้ใช้งานจึงควรเก็บรหัสผ่านเป็นความลับ (ภูมิ ภูมิรัตน์, 2561)

หลังการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่ากลุ่มตัวอย่าง 26 คน (ร้อยละ 87) มีความรู้ความเข้าใจในเรื่องดังกล่าว

"...ถ้าตอบตามหลักความปลอดภัยก็ไม่ควรจะบอกใครเลยแม้แต่คนในครอบครัว แต่ในโลกความเป็นจริงคนส่วนใหญ่ก็อาจจะมีบอกกันบ้างในบางครั้ง" (เพศชาย, อายุ 31 ปี, พนักงานบริษัทเอกชน)

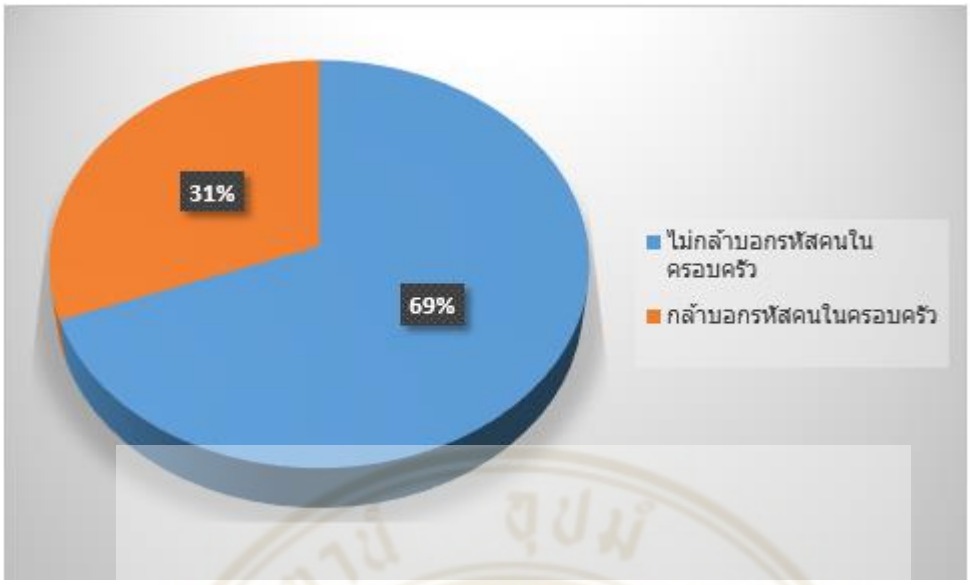
"...คนในครอบครัวก็ใช่ว่าจะไว้ใจได้ เห็นหลายครั้งที่เงินหายไปจากบัญชีก็เพราะคนใกล้ตัวก็เลยคิดว่าไม่ควรจะบอกรหัสผ่านให้กับใครเลยได้รู้" (เพศหญิง, อายุ 30 ปี, พนักงานบริษัทเอกชน)

ในขณะที่กลุ่มตัวอย่าง 4 คน (ร้อยละ 13) ที่ขาดความรู้ความเข้าใจในเรื่องดังกล่าวและเมื่อสัมภาษณ์เพิ่มเติมพบว่าประเด็นที่มีความเข้าใจคลาดเคลื่อนส่วนใหญ่นั้นเกิดจากความเข้าใจว่าการบอกรหัสแก่คนในครอบครัวจะช่วยทำธุรกรรมแทนกันได้ในกรณีจำเป็น และเป็นบุคคลที่สามารถไว้ใจได้

"…คิดว่าน่าจะบอกคนในครอบครัวได้ เพราะถ้าเกิดเหตุฉุกเฉินเร่งด่วนต้องรีบใช้เงินแล้วอยู่นอกบ้าน ก็สามารถขอให้คนที่บ้านโอนเงินแทนกันได้ อีกอย่างถ้าเป็นคนในครอบครัวก็ไม่น่าจะเป็นอะไร" (เพศชาย, อายุ 35 ปี, พนักงานบริษัทเอกชน)

"…บอกคนในครอบครัวไม่น่าจะเป็นไร คิดว่าบอกได้ แต่ส่วนตัวก็ไม่ได้บอกใคร แต่ถ้าให้บอกก็กล้าบอก" (เพศหญิง, อายุ 29 ปี, พนักงานบริษัทเอกชน)

เมื่อสัมภาษณ์เพิ่มเติมกับกลุ่มตัวอย่างที่ตอบถูกในข้อนี้จำนวน 26 คนในประเด็นการนำความรู้ความเข้าใจดังกล่าวไปใช้จริงในชีวิตประจำวันหรือไม่ พบว่า



ภาพที่ 4.9 แสดงร้อยละของกลุ่มตัวอย่างว่ากล้าหรือไม่ที่จะบอกรหัสผ่าน Mobile Banking Application ให้กับคนในครอบครัว

กลุ่มตัวอย่างส่วนใหญ่จำนวน 18 คน (ร้อยละ 69) มีการปฏิบัติตนตามสิ่งที่รู้อย่างเคร่งครัด (ดังภาพที่ 4.9) โดยกลุ่มตัวอย่างอธิบายว่าจะไม่บอกรหัสแก่สมาชิกในครอบครัวทุกกรณี และบางกรณีหากจำเป็นจริงๆ ก็จะบอกรหัสผ่านให้คนในครอบครัวทราบแต่จะรีบเปลี่ยนรหัสโดยทันที

"...ปกติจะไม่บอกรหัสของตัวเองให้คนอื่นในครอบครัวรู้เลย แต่จะรู้รหัสของคนอื่นในบ้านบางคน แต่ถ้ามาขอก็ไม่กล้าบอก" (เพศชาย, อายุ 31 ปี, พนักงานบริษัทเอกชน)

"...ไม่บอกรหัสอยู่แล้ว ถึงแม้ว่าจะสนิทกันแค่ไหนหรือเป็นคนในครอบครัว กลัวเหมือนละคนเลือดข้นคนจาง" (เพศหญิง, อายุ 30 ปี, พนักงานบริษัทเอกชน)

"...ถึงแม้จะเป็นคนในครอบครัวก็ไม่ไว้ใจ ยกเว้นว่ามีเหตุจำเป็นจริงๆ อาจจะต้องบอกแต่ก็จะเปลี่ยนรหัสผ่านให้เร็วที่สุด กลัวเงินในบัญชีหาย" (เพศหญิง, อายุ 26 ปี, พนักงานธนาคาร)

ในขณะที่กลุ่มตัวอย่างจำนวน 8 คน (ร้อยละ 31) กล้าบอกรหัสให้กับคนในครอบครัวทราบโดยเฉพาะพ่อแม่พี่น้องเพราะคิดว่าสามารถไว้ใจได้ หรือบางกรณีเป็นธุรกิจกงสีใช้บัญชีที่เป็นชื่อของตนเองแต่เป็นเงินของทางบ้านเพราะฉะนั้นจะมีการบอกรหัสให้บุคคลในครอบครัวได้รับทราบ

"...ถ้าเป็นพ่อแม่พี่น้องบอกได้เชื่อใจกัน แต่ถ้าเป็นญาติไม่กล้าบอก" (เพศหญิง, อายุ 27 ปี, พนักงานบริษัทเอกชน)

“…ปกติบัญชีเงินฝากชื่อตัวเองใช้เป็นบัญชีกงสีของที่บ้าน ก็เลยมีคนอื่นรู้รหัสผ่าน Mobile Banking ด้วย แต่เงินในบัญชีจะเป็นของทางบ้าน แล้วถ้าให้บอกรหัสของตัวเองให้กับคนในครอบครัวก็คิดว่ากล้าบอกถ้าเป็นพ่อ แม่ พี่น้อง แต่ถ้าเป็นญาติจะไม่กล้าบอก” (เพศชาย, อายุ 31 ปี, ธุรกิจส่วนตัว)

4.2.9 ความคิดเห็นต่อการยืนยันตัวตนเข้าใช้งาน Mobile Banking Application โดยใช้ One Time Password (OTP) ที่มีความน่าเชื่อถือสูงกว่าการใช้รหัสผ่าน

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือตามมาตรฐาน National Institute of Standards and Technology (NIST) 800-63-2 ได้กล่าวถึงสิ่งที่ใช้ยืนยันตัวตนแต่ละชนิดและระดับความน่าเชื่อถือที่แตกต่างกันไป รหัสผ่านถือเป็นสิ่งที่คุณรู้ (something you know) ซึ่งระดับความน่าเชื่อถืออยู่ที่ระดับต่ำสุดคือ 1 เพราะหากผู้อื่นล่วงรู้รหัสดังกล่าวก็สามารถนำไปใช้งานได้เลยไม่ว่าจะอยู่ ณ ที่ใด สำหรับ OTP ถือเป็นสิ่งที่คุณมี (something you have) ซึ่งในกรณีนี้คือเบอร์โทรศัพท์มือถือโดยระบบจะส่งรหัสผ่านแบบใช้ครั้งเดียวเข้ามือถือของผู้ใช้งานโดยตรง วิธีดังกล่าวระดับความน่าเชื่อถือจะอยู่ที่ระดับ 2 (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2560) หลังการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่ากลุ่มตัวอย่าง 25 คน (ร้อยละ 83) มีความรู้ความเข้าใจในเรื่องดังกล่าว

“...เท่าที่คิดคือ OTP น่าจะปลอดภัยกว่ารหัสผ่าน เพราะไม่อย่างนั้นทำไมหลาย app ของธนาคารถึงให้ใช้ OTP ก่อนโอนเงินออก แต่รหัสผ่านส่วนใหญ่จะใช้แค่ log in เฉยๆ” (เพศหญิง, อายุ 27 ปี, พนักงานบริษัทเอกชน)

“...ถ้าเป็นรหัสผ่านถ้าคนอื่นรู้ก็จบ เอาไปใช้ทำธุรกรรมได้เลย แต่ถ้าเป็น OTP คือต้องเป็นเจ้าของมือถือเครื่องนั้นจริงๆ ถึงจะใช้งานได้ ดูแล้ว OTP ก็น่าจะปลอดภัยมากกว่ารหัสผ่าน” (เพศชาย, อายุ 30 ปี, ข้าราชการ)

ในขณะที่กลุ่มตัวอย่าง 5 คน (ร้อยละ 17) ที่ขาดความรู้ความเข้าใจในเรื่องดังกล่าวและเมื่อสัมภาษณ์เพิ่มเติมพบว่าประเด็นที่มีความเข้าใจคลาดเคลื่อนส่วนใหญ่นั้นเกิดจากความไม่รู้ และมองว่า password มีความปลอดภัยกว่าถ้าคนอื่นไม่ทราบรหัสของเรา

“…จริงๆ คิดว่า password น่าจะช่วยในเรื่องความปลอดภัยมากกว่าถ้าไม่แชร์ก็ไม่น่าเป็นไร แต่ OTP น่าจะช่วยเหมือนกันแต่น้อยกว่า password” (เพศหญิง, อายุ 34 ปี, พนักงานธนาคาร)

“…ตอบว่า password ปลอดภัยกว่าในข้อนี้ เดาเอา แต่ก็แอบลังเลว่า OTP น่าจะปลอดภัยกว่าหรือเปล่า เพราะทุกวันนี้ธนาคารมักจะเลือกใช้ OTP ในการยืนยันการโอนเงินเวลาทำ Mobile Banking” (เพศชาย, อายุ 30 ปี, ข้าราชการ)

4.2.10 ความคิดเห็นต่อการจดรหัสผ่านเข้าใช้งาน Mobile Banking Application ไว้บนโทรศัพท์มือถือหรือเศษกระดาษ

จากการทบทวนวรรณกรรม ข้อเท็จจริงที่พบคือควรหลีกเลี่ยงการบันทึกรหัสผ่านเข้าทำธุรกรรม Mobile Banking ไว้ในโทรศัพท์มือถือเช่นเดียวกันการจดรหัสผ่านไว้บนเศษกระดาษ เพราะหากมือถือโดนแฮกระบบจากผู้ไม่หวังดีหรือติดมัลแวร์ก็จะทำให้ข้อมูลรหัสผ่านของเรานั้นรั่วไหลออกไปได้เช่นเดียวกัน (Octopatr, 2015)

หลังการทำแบบทดสอบและสัมภาษณ์กลุ่มตัวอย่างพบว่ากลุ่มตัวอย่าง 26 คน (ร้อยละ 87) มีความรู้ความเข้าใจในเรื่องดังกล่าว

“...จดใส่มือถือหรือใส่กระดาษก็เสี่ยงทั้งคู่ ปกติเค้าก็สอนกันว่าห้ามจดรหัสผ่านเอาไว้เพื่อความปลอดภัย แต่เอาจริงๆ คนส่วนใหญ่ก็น่าจะจดไว้สักที่เพราะสมัยนี้รหัสผ่านที่ต้องใช้เยอะแยะไปหมด จำไม่ไหว” (เพศชาย, อายุ 30 ปี, ข้าราชการ)

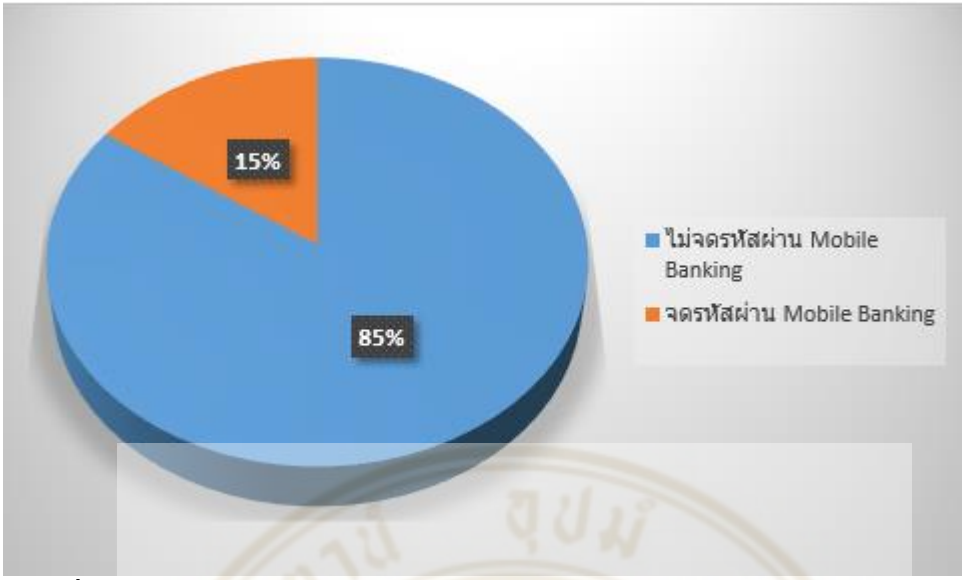
“...จดใส่มือถือก็ไม่น่าจะปลอดภัยมากกว่า เพราะถ้ามือถือหายหรือถูกแฮกน่าจะอันตรายมากกว่าด้วยซ้ำ” (เพศหญิง, อายุ 30 ปี, พนักงานบริษัทเอกชน)

ในขณะที่กลุ่มตัวอย่าง 4 คน (ร้อยละ 13) ขาดความรู้ความเข้าใจในเรื่องดังกล่าวและเมื่อสัมภาษณ์เพิ่มเติมพบว่าประเด็นที่มีความเข้าใจคลาดเคลื่อนส่วนใหญ่นั้นเกิดจากความคิดเห็นว่าโทรศัพท์มือถือนั้นมีรหัสผ่านทำให้การบันทึกรหัสผ่านลงบนเครื่องน่าจะปลอดภัยมากกว่าการจดใส่เศษกระดาษหรือสมุด

“…มองว่าบันทึกรหัสไว้บนมือถือน่าจะดีกว่ากระดาษ เพราะมือถือมันมีรหัสเข้าเครื่องอยู่แล้ว” (เพศหญิง, อายุ 26 ปี, พนักงานธนาคาร)

“…คิดว่าสมุดมันหายได้ แต่ถ้าเป็นมือถือมันติดตัวตลอดเวลา แถมมีรหัสเข้าเครื่องด้วยก็น่าจะปลอดภัยมากกว่า” (เพศหญิง, อายุ 27 ปี, พนักงานบริษัทเอกชน)

และเมื่อสัมภาษณ์เพิ่มเติมกับกลุ่มตัวอย่างที่ตอบถูกในข้อนี้จำนวน 26 คนในประเด็นการนำความรู้ความเข้าใจดังกล่าวไปใช้จริงในชีวิตประจำวันหรือไม่ พบว่า



ภาพที่ 4.10 แสดงร้อยละของกลุ่มตัวอย่างว่ามีการจดรหัสผ่านเข้าใช้งาน Mobile Banking Application ไว้บนโทรศัพท์มือถือหรือเศษกระดาษหรือไม่

กลุ่มตัวอย่างส่วนใหญ่จำนวน 22 คน (ร้อยละ 85) มีการปฏิบัติตนตามสิ่งที่รู้อย่างเคร่งครัด (ดังภาพที่ 4.10) โดยกลุ่มตัวอย่างอธิบายว่าจะไม่จดรหัสผ่าน Mobile Banking ไว้ในเศษกระดาษหรือโทรศัพท์มือถือโดยเด็ดขาดเหตุผลส่วนใหญ่เพราะสามารถจำรหัสได้ มีเทคนิคในการจดจำรหัส หากลืมรหัสค่อยแจ้งขอรหัสใหม่ เคยมีประสบการณ์ถูกมิจฉาชีพโมยกดเงินสด และเริ่มระวังตัวเมื่อเงินออมเริ่มเยอะขึ้น

"...ไม่จดเพราะมีเทคนิคการจำ ทุกธนาคารจะใช้รหัสไม่ซ้ำกัน ต้องนี้ขี้ระแวงเพราะเคยมีประสบการณ์กระเป๋าสตางค์หายแล้วบัตรเอทีเอ็มโดยกดเงินออกไป 60,000 บาทที่ไทยเพราะตั้งรหัสเป็น พ.ศ. เกิด ตอนหลังเลยระวังตัวเรื่องรหัสผ่าน" (เพศหญิง, อายุ 30 ปี, พนักงานบริษัทเอกชน)

"...ตอนแรกเคยจด แต่ตอนนี้ไม่จดแล้วเพราะเงินในบัญชีเริ่มเยอะขึ้น พฤติกรรมก็เริ่มเปลี่ยน" (เพศชาย, อายุ 30 ปี, ข้าราชการ)

"...ปกติไม่จด แต่ก็จำรหัสไม่ได้ค่อยได้ ถ้าหากลืมก็แค่แจ้งธนาคารขอรหัสผ่านใหม่" (เพศหญิง, อายุ 31 ปี, พนักงานบริษัทเอกชน)

ในขณะที่กลุ่มตัวอย่างจำนวน 4 คน (ร้อยละ 15) มีการจดลงบนเศษกระดาษ หรือบันทึกไว้ในโทรศัพท์ หรือทั้งสองอย่าง โดยให้เหตุผลคือเป็นคนขี้ลืม

“…จดใส่กระดาษเพราะรหัสใช้ Mobile Banking ของแต่ละธนาคารไม่ซ้ำกันเลย จำไม่ค่อยได้” (เพศชาย, อายุ 31 ปี, ธุรกิจส่วนตัว)

“…บันทึกไว้ในมือถือ เพราะขี้ลืม จำรหัสไม่ค่อยจะได้” (เพศหญิง, อายุ 28 ปี, พนักงานบริษัทเอกชน)

4.3 ความคิดเห็นของผู้ใช้บริการเกี่ยวกับระบบการยืนยันตัวตนบน Mobile Banking Application ที่เหมาะสม

เครื่องมือสำคัญอย่างหนึ่งที่ช่วยให้การใช้งาน Mobile Banking เกิดความปลอดภัยก็คือระบบการยืนยันตัวตนของผู้ใช้งาน ผู้ให้บริการจะสร้างวิธีการที่สามารถระบุเอกลักษณ์ที่สามารถเชื่อมโยงไปยังฐานลูกค้าของธนาคารได้อย่างถูกต้อง โดยสิ่งที่จะสามารถใช้ยืนยันตัวตนได้นั้นสามารถแบ่งออกได้เป็น 3 ปัจจัยได้แก่

1. สิ่งที่คุณรู้ (Something you know) คือข้อมูลที่ผู้ใช้งานเท่านั้นที่ทราบ เช่น รหัสผ่าน (Password) และเลขรหัสส่วนตัว (PIN) เป็นต้น

2. สิ่งที่คุณมี (Something you have) คือสิ่งของที่ผู้ใช้งานเท่านั้นที่มีอยู่ในครอบครอง เช่น บัตรประจำตัว (ID Card) หนังสือเดินทาง (Passport) อุปกรณ์ที่บรรจุสิ่งที่ใช้ยืนยันตัวตน และกุญแจการเข้ารหัสลับ (Cryptographic Key) เป็นต้น

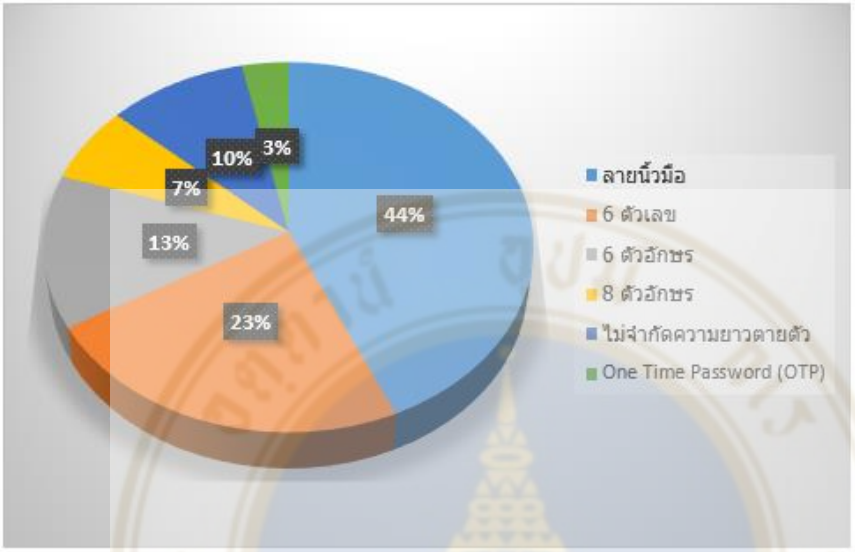
3. สิ่งที่คุณเป็น (Something you are) คือข้อมูลทางชีวภาพของผู้ใช้งานเช่น ลายนิ้วมือ หน้า ม่านตา เสียง เป็นต้น

เพื่อทราบถึงทัศนะของกลุ่มตัวอย่างซึ่งเป็นผู้ใช้งาน Mobile Banking Application เกี่ยวกับวิธีการยืนยันตัวตนที่คิดว่าเหมาะสมพร้อมเหตุผลสนับสนุน ทางผู้วิจัยจึงแบ่งการสัมภาษณ์เรื่องความคิดเห็นดังกล่าวออกเป็น 2 ส่วนคือวิธีการยืนยันตัวตนเพื่อวัตถุประสงค์ในการ log in เข้าสู่ระบบ Mobile Banking Application และวิธีการยืนยันตัวตนเพื่อวัตถุประสงค์ในการยืนยันรายการการทำธุรกรรม

4.3.1 วิธีการยืนยันตัวตนที่เหมาะสมเพื่อวัตถุประสงค์ในการ log in เข้าสู่ Mobile Banking Application

จากการสัมภาษณ์กลุ่มตัวอย่างทั้งสิ้น 30 คนพบว่าผู้คนส่วนใหญ่คิดว่าการยืนยันตัวตนด้วยวิธีการสแกนลายนิ้วมือมีความเหมาะสมที่สุดคิดเป็นจำนวน 13 คน (ร้อยละ 44) รองลงมาคือ

การใช้รหัสผ่านตัวเลขหกหลักจำนวน 7 คน (ร้อยละ 23) รหัสผ่านหกตัวอักษรจำนวน 4 คน (ร้อยละ 13) รหัสผ่านแบบไม่จำกัดความยาวตายตัวจำนวน 3 คน (ร้อยละ 10) รหัสผ่านแปดตัวอักษรจำนวน 2 คน (ร้อยละ 7) และการใช้ One Time Password (OTP) จำนวน 1 คน (ร้อยละ 3) ตามลำดับ (ภาพที่ 4.11)



ภาพที่ 4.11 แสดงร้อยละของกลุ่มตัวอย่างเรื่องความคิดเห็นของวิธีการยืนยันตัวตนเพื่อ log in เข้าใช้งาน Mobile Banking Application ที่เหมาะสม

โดยเหตุผลสนับสนุนความคิดเห็นของกลุ่มตัวอย่างสามารถสรุปได้ดังนี้

วิธีการยืนยันตัวตน	**เหตุผลสนับสนุน**
ลายนิ้วมือ	- สะดวก - รวดเร็ว - ง่าย - ปลอมแปลงยาก - ปลอดภัย - มือถือรุ่นใหม่ส่วนใหญ่รองรับการสแกนนิ้ว - เพียงพอต่อการ log in แต่ไม่ได้ทำรายการธุรกรรม
รหัสผ่านตัวเลขหกหลัก	- สะดวก - รวดเร็ว - จำง่าย
รหัสผ่านหกตัวอักษร	- ยากต่อการคาดเดา

วิธีการยืนยันตัวตน	เหตุผลสนับสนุน
	- ปลอดภัย - ไม่ยาวไม่สั้นเกินไป
รหัสผ่านแบบไม่จำกัดความยาวตายตัว	- คาดเดายาก
รหัสผ่านแปดตัวอักษร	- จำยาก - ยากต่อการคาดเดา
One Time Password (OTP)	- ไม่ต้องจดจำ

"…อยากให้เหมือนที่อเมริกา ที่ผู้นธนาคารเค้าไม่กำหนดจำนวนตัวอักษรว่าต้อง 6 ตัว หรือ 8 ตัว แต่เค้าจะให้เราสามารถกำหนดตัวอักษรกี่ตัวเองก็ได้ อาจจะเป็น 1-15 ตัวอักษรอะไรประมาณนี้ ถ้าดูความน่าจะเป็นก็ทำให้พวกมิจฉาชีพคาดเดารหัสได้ยากขึ้น เพราะสมมุติถ้ากำหนดไปเลยเช่น 4 ตัว โจรก็จะเดาได้ว่าน่าจะเป็นปี พ.ศ. เกิดอะไรประมาณนี้" (เพศหญิง, อายุ 30 ปี, พนักงานบริษัทเอกชน)

"…ถ้าแค่ log in เป็นลายนิ้วมือก็ง่ายดี สะดวกด้วยและก็เป็น identity ของแต่ละบุคคลลอกเลียนแบบได้ยาก" (เพศหญิง, อายุ 32 ปี, ธุรกิจส่วนตัว)

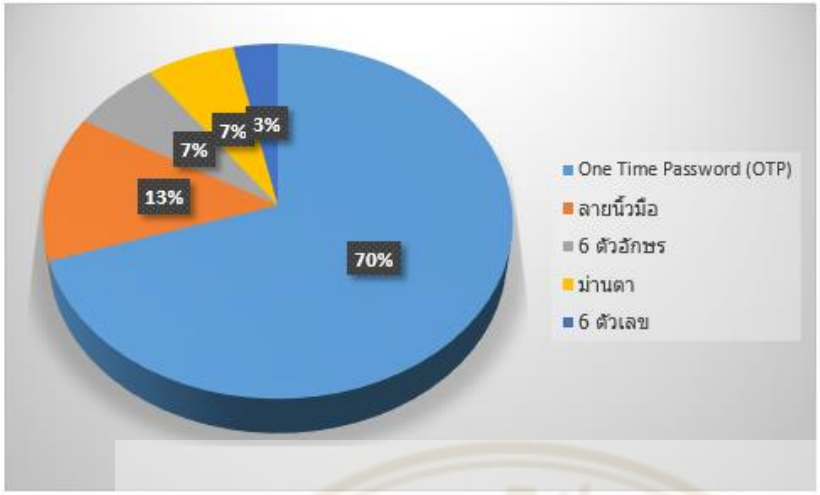
"…ลายนิ้วมือ เพราะว่าสะดวก รวดเร็ว และปลอดภัยดี มีเพียงคนเดียวที่เข้าได้" (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

"…อยากได้ตัวเลข 6 ตัวใช้ log in เพราะอยากได้ความรวดเร็ว แล้วก็ลดความเสี่ยงที่จะลืมรหัสเพราะไม่ยาวเกินไป" (เพศชาย, อายุ 31 ปี, พนักงานบริษัทเอกชน)

"…ขอเลือกแบบ 6 ตัวอักษร เพราะมันดูยากดี ตั้งก็ยาก จำก็ยาก แล้วก็ดูปลอดภัยกว่าแค่ 6 ตัวเลข" (เพศหญิง, อายุ 32 ปี, พนักงานบริษัทเอกชน)

4.3.2 วิธีการยืนยันตัวตนที่เหมาะสมเพื่อวัตถุประสงค์ในการยืนยันรายการธุรกรรมที่ทำผ่าน Mobile Banking Application

จากการสัมภาษณ์กลุ่มตัวอย่างทั้งสิ้น 30 คนพบว่าผู้คนส่วนใหญ่คิดว่าการยืนยันตัวตนด้วยการใช้ One Time Password (OTP) มีความเหมาะสมที่สุดคิดเป็นจำนวน 21 คน (ร้อยละ 70) รองลงมาคือการใช้ลายนิ้วมือจำนวน 4 คน (ร้อยละ 13) รหัสผ่านหกตัวอักษรจำนวน 2 คน (ร้อยละ 7) เท่ากับการสแกนม่านตาจำนวน 2 คน (ร้อยละ 7) และรหัสผ่านหกตัวเลขจำนวน 1 คน (ร้อยละ 3) ตามลำดับ โดยสามารถสรุปตามภาพที่ 4.12



ภาพที่ 4.12 แสดงร้อยละของกลุ่มตัวอย่างเรื่องความคิดเห็นของวิธีการยืนยันตัวตนในกรณียืนยันรายการธุรกรรมที่ทำผ่าน Mobile Banking Application

โดยเหตุผลสนับสนุนความคิดเห็นของกลุ่มตัวอย่างสามารถสรุปได้ดังนี้

วิธีการยืนยันตัวตน	**เหตุผลสนับสนุน**
One Time Password (OTP)	- ไม่ต้องจดจำ - ปลอดภัย - ง่าย
ลายนิ้วมือ	- ง่าย - สะดวก - รวดเร็ว - ยืนยันตัวตนได้ดี - กรณีย้ายเครื่องเปลี่ยนเบอร์โทรศัพท์ยังสามารถใช้งานได้
รหัสผ่านหกตัวอักษร	- สะดวก - ไม่ยาวไม่สั้นเกินไป - จำง่าย
ม่านตา	- ปลอดภัย - สะดวก
รหัสผ่านหกตัวเลข	- จำง่าย

“…เลือก One Time Password เพราะดูปลอดภัย สมมุติว่าโดนแฮกก็จะใช้รหัสเดิมเข้าไม่ได้เพราะรหัสจะเปลี่ยนไปทุกๆ ครั้ง แต่ถ้าใช้ password ยังน่าจะยังเข้าได้อยู่ดี” (เพศชาย, อายุ 31 ปี, พนักงานบริษัทเอกชน)

“…OTP เพราะส่วนตัวรู้สึกว่าปลอดภัยกว่า password ใช้ได้เป็นครั้งๆ ไป ถ้า password โดนขโมยก็ยังสามารถใช้ได้อยู่เรื่อยๆ กว่าเราจะรู้ตัว” (เพศชาย, อายุ 30 ปี, ข้าราชการ)

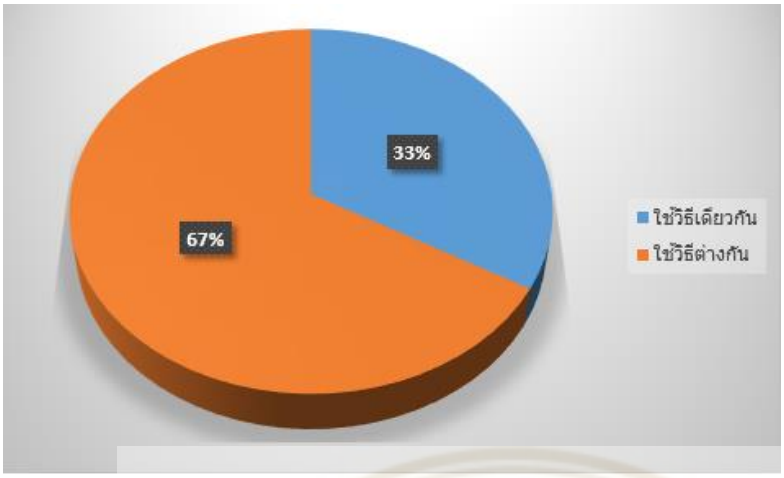
“…ใช้เป็นลายนิ้วมือ เพราะสะดวกดี ที่สำคัญเวลาจะย้ายเครื่องเปลี่ยนเบอร์โทรศัพท์ก็ยังสามารถใช้ได้ปกติไม่เหมือนกับ OTP” (เพศหญิง, อายุ 32 ปี, ธุรกิจส่วนตัว)

“…เอา password หกตัวอักษรน่าจะพอจำได้ ถ้าแปดตัวก็ดูเยอะไป แต่วิธี biometric ไม่เอาเพราะว่าถ้าเค้าแอบทำให้เราสลบก็สามารถเอาอวัยวะเรามาสแกนทำธุรกรรมได้อยู่ดี” (เพศชาย, อายุ 35 ปี, พนักงานบริษัทเอกชน)

“…วิธีสแกนม่านตา เพราะคิดว่าเป็นวิธีที่ดูปลอดภัยกว่าลายนิ้วมือ แล้วก็สะดวกด้วย” (เพศหญิง, อายุ 27 ปี, พนักงานบริษัทเอกชน)

4.3.3 วิธีการยืนยันตัวตนแบบเดียวกันหรือแตกต่างกันสำหรับการยืนยันตัวตนเพื่อวัตถุประสงค์ในการ log in และการยืนยันรายการธุรกรรม

จากการสัมภาษณ์กลุ่มตัวอย่างทั้งสิ้น 30 คนเกี่ยวกับประเด็นวิธีการยืนยันตัวตนว่าควรจะเหมือนหรือต่างกันสำหรับกรณีการ log in และการยืนยันรายการธุรกรรม พบว่ากลุ่มตัวอย่าง 20 คน (ร้อยละ 67) คิดว่าควรใช้วิธีการยืนยันตัวตนที่ต่างกัน โดยมีเหตุผลสนับสนุนคือ เรื่องความปลอดภัยที่มากกว่า สามารถยืนยันตัวตนได้ดีกว่า ในขณะที่กลุ่มตัวอย่างจำนวน 10 คน (ร้อยละ 33) มองว่าควรใช้วิธีในลักษณะเดียวกันพร้อมเหตุผลสนับสนุนคือมีความสะดวก ไม่ต้องจดจำเยอะ และหากเป็นวิธีการที่ปลอดภัยก็น่าจะปลอดภัย โดยสรุปได้ตามภาพที่ 4.13



ภาพที่ 4.13 แสดงร้อยละของกลุ่มตัวอย่างเรื่องความคิดเห็นของวิธีการยืนยันตัวตนในกรณี log in และกรณียืนยันรายการธุรกรรมที่ทำผ่าน Mobile Banking Application ว่าควรเป็นวิธีการเดียวกันหรือไม่

"...ถ้าเลือกได้ อยากให้ใช้วิธีการเดียวกัน คนแก่ก็จะใช้ได้ไม่ยาก ไม่ต้องจำเยอะ จริงๆ แล้วอะไรที่เป็น application ควรใช้งานง่าย" (เพศชาย, อายุ 30 ปี, ข้าราชการ)

"...เลือกวิธีการเดียวกันน่าจะดีกว่า เพราะจะได้ไม่ต้องจำ ปกติชีวิตทุกวันนี้ก็ต้องจำรหัสเยอะแยะอยู่แล้ว ถ้ายิ่งมีหลายตัวก็ยิ่งยาก" (เพศชาย, อายุ 31 ปี, ธุรกิจส่วนตัว)

"...วิธีเดียวกันก็ได้ เพราะถ้าวิธีที่ใช้เป็นวิธีที่มีความปลอดภัยสูงอยู่แล้ว ใช้วิธีการเดียวกันก็ไม่น่าจะมีปัญหาอะไร" (เพศหญิง, อายุ 27 ปี, พนักงานบริษัทเอกชน)

"...ควรจะต่างกันเพื่อความปลอดภัย ถ้าแค่ log in เอาวิธีง่ายๆก็พอ เพราะแค่เข้าไปดูประวัติธุรกรรมย้อนหลังเฉยๆ แต่ถ้าจะ confirm ธุรกรรม อันนี้ก็ต้องเป็นอีกวิธีที่ต้องซับซ้อนเป็นการป้องกันไว้ก่อน" (เพศชาย, อายุ 32 ปี, พนักงานบริษัทเอกชน)

บทที่ 5
สรุปผลการวิจัย อภิปราย และข้อเสนอแนะ

จากบทที่ 3 ซึ่งได้นำเสนอกระบวนการในการเก็บรวบรวมข้อมูลในเชิงคุณภาพสำหรับการศึกษาวิจัยในครั้งนี้และมีการนำเสนอข้อมูลที่จัดเก็บได้จากกลุ่มตัวอย่างในบทที่ 4 สำหรับบทที่ 5 ผู้วิจัยจะสรุปผลการวิจัยที่ได้โดยละเอียด พร้อมทั้งอภิปรายผลที่ได้จากการเก็บรวมรวมข้อมูลในครั้งนี้เมื่อเปรียบเทียบกับทฤษฎีและผลงานการวิจัยอื่นๆ ที่เกี่ยวข้อง เพื่อนำไปสู่ข้อเสนอแนะที่เป็นประโยชน์ต่อผู้ที่สนใจและรวมไปถึงการศึกษาต่อยอดงานวิจัยในครั้งนี้ในอนาคต โดยมีรายละเอียดดังนี้

5.1 สรุปและอภิปรายผลการวิจัย

จากการวิจัยเรื่องความคิดเห็นของ Generation C เกี่ยวกับความปลอดภัยบน Mobile Banking Application ที่ให้บริการโดยธนาคารพาณิชย์ในประเทศไทย สามารถแบ่งอภิปรายผลได้ 3 ส่วน ดังนี้

1. ความเชื่อมั่นของผู้ใช้งาน Mobile Banking Application ในด้านความปลอดภัย
2. ความรู้ความเข้าใจของผู้ใช้บริการ Mobile Banking Application ในการทำธุรกรรมอย่างปลอดภัยและการนำไปปฏิบัติ
3. ความคิดเห็นของผู้ใช้บริการเกี่ยวกับระบบการยืนยันตัวตนบน Mobile Banking Application ที่เหมาะสม

ซึ่งสามารถอภิปรายผลการวิจัยเป็นดังนี้

5.1.1 ความเชื่อมั่นของผู้ใช้งาน Mobile Banking Application ในด้านความปลอดภัย

ผู้วิจัยได้สัมภาษณ์กลุ่มตัวอย่าง 30 คน โดยความคิดเห็นของกลุ่มตัวอย่างส่วนใหญ่หากเทียบเคียงระดับความเชื่อมั่นตาม Likert Scale จาก 1 (น้อยที่สุด) ถึง 10 (มากที่สุด) พบว่าค่าเฉลี่ยของความเชื่อมั่นของกลุ่มตัวอย่างจะอยู่ที่ระดับ 8.03 ซึ่งถือว่าค่อนข้างสูงมาก โดยที่ Yousafzai et al. (2546) ให้นิยามความเชื่อมั่นเกี่ยวกับธุรกรรมออนไลน์ว่าคือสภาวะจิตใจที่นำไปสู่ความเต็มใจของผู้ใช้บริการในการทำธุรกรรมทางอินเทอร์เน็ตที่จะรับความเสี่ยงในการเข้าทำธุรกรรมผ่าน Mobile

Banking Application โดยความเต็มใจดังกล่าวจะขึ้นอยู่กับคาดหวังว่าธนาคารจะปฏิบัติหน้าที่อย่างเต็มที่ไม่ว่าผู้ใช้บริการเองจะมีความสามารถในการตรวจสอบและควบคุมการทำงานของธนาคารหรือไม่ก็ตาม

เมื่อสอบถามกลุ่มตัวอย่าง 30 คนถึงเหตุผลหลักของความเชื่อมั่นดังกล่าวพบว่าสอดคล้องกับนิยามความเชื่อมั่นด้านธุรกรรมออนไลน์ข้างต้น เนื่องจากเหตุผลหลักของกลุ่มตัวอย่างคือระบบการยืนยันตัวตนที่ค่อนข้างรัดกุมของธนาคารพาณิชย์ในประเทศไทยซึ่งเป็นสถาบันที่มีหน้าที่หลักในการให้บริการธุรกรรม Mobile Banking Application แก่ผู้ใช้งาน และโดยภาพรวมในปัจจุบันถือว่าธนาคารเองได้ปฏิบัติหน้าที่ได้ค่อนข้างสมบูรณ์ โดยเหตุผลรองลงมาคือกลุ่มตัวอย่างไม่เคยเจอเหตุการณ์เลวร้ายกับตัวเองมาก่อน

อย่างไรก็ตามเมื่อให้กลุ่มตัวอย่างเสนอแนะวิธีการเพิ่มระดับความเชื่อมั่นต่อ Mobile Banking Application ด้านความปลอดภัยเพื่อใช้ในการปรับปรุงพัฒนาและยกระดับความเชื่อมั่นให้สูงขึ้น พบว่าข้อเสนอแนะหลักจากกลุ่มตัวอย่างคือเรื่องระบบการยืนยันตัวตนอีกเช่นเดียวกัน อาจกล่าวได้ว่าผู้ใช้งานให้ความสำคัญในระบบการยืนยันตัวตนมากเป็นพิเศษ และมีผลอย่างยิ่งต่อความเชื่อมั่นในการใช้บริการ Mobile Banking Application ซึ่งสอดคล้องกับงานวิจัยของ ชัญญาพัทธ์ จงทวี (2558) ที่พบว่าความปลอดภัยในการใช้งานเป็นหนึ่งในปัจจัยที่มีผลต่อความพึงพอใจในการใช้บริการ Mobile Banking

5.1.2 ความรู้ความเข้าใจของผู้ใช้บริการ Mobile Banking Application ในการทำธุรกรรมอย่างปลอดภัย

ผู้วิจัยได้ใช้แบบทดสอบ 10 ข้อเพื่อใช้วัดความรู้ความเข้าใจในการใช้ Mobile Banking Application เพื่อนำไปสู่การสัมภาษณ์ประเด็นที่น่าสนใจเพิ่มเติม โดยตามเกณฑ์การจัดกลุ่มคะแนนของกลุ่มตัวอย่างทั้งสิ้น 30 คนพบว่ามีความรู้ความเข้าใจอยู่ระดับ “มาก” จำนวน 17 คน โดยกลุ่มคนตัวอย่าง รองลงมาคือระดับ “น้อย” จำนวน 7 คน และระดับ “ทั่วไป” จำนวน 6 คน อย่างไรก็ตามจากการสัมภาษณ์พบว่ามีสาระสำคัญบางประเด็นที่กลุ่มตัวอย่างยังคงเข้าใจคลาดเคลื่อนเกี่ยวกับการใช้งาน Mobile Banking Application ซึ่งสามารถสรุปได้ดังนี้

ข้อเท็จจริง	ความเข้าใจคลาดเคลื่อน
การเชื่อมต่อ Wifi มีความเสี่ยงในแง่ความปลอดภัยในการเข้าใช้บริการ Mobile Banking มากกว่าการเชื่อมต่อเครือข่าย 3G และ 4G	- การเชื่อมต่อผ่านเครือข่าย 3G และ 4G ไม่เป็นเครือข่ายส่วนตัวจึงปลอดภัยน้อยกว่า Wifi

ข้อเท็จจริง	ความเข้าใจคลาดเคลื่อน
การทำธุรกรรมผ่าน Mobile Banking Application มีความเสี่ยงน้อยกว่าการทำธุรกรรมผ่าน Website ของธนาคาร	- หากเข้าผ่านเว็บไซต์ https:// จะมีความปลอดภัยมากกว่า Mobile Banking Application - มี Application ปลอมจึงปลอดภัยน้อยกว่าเข้าใช้งานผ่านเว็บไซต์
การเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่เรารู้จักไม่ได้ปลอดภัยกว่าการเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่เราไม่รู้จัก	- หากเป็น Wifi ที่แสดงชื่อร้านค้าที่รู้จักน่าจะรักษาชื่อเสียงของตนเอง สามารถไว้ใจได้ และไม่น่าจะถูกแฮก
หลังการใช้งาน Mobile Banking Application ควร log out ออกจากระบบเสมอ	- ระบบจะ log out ให้อัตโนมัติเมื่อเลิกใช้งานจึงไม่จำเป็นต้องกด log out ออกในทุกๆ ครั้ง
ดาวน์โหลด Application จาก App Store สำหรับระบบปฏิบัติการ iOS ไม่ได้ปลอดภัยจากมัลแวร์ (malware) ร้อยเปอร์เซ็นต์	- App Store ไม่มีข่าวเรื่องมัลแวร์มาก่อน - App store ไม่มีโปรแกรม anti-virus ให้ดาวน์โหลดจึงคิดว่าปลอดภัยกว่า - จากประสบการณ์ใช้งานส่วนตัวที่ไม่เคยเจอเรื่องมัลแวร์บน App store - App Store มีการตรวจสอบที่ดีก่อนนำ Application ต่างๆ ขึ้นสู่ App store
การพิจารณา Mobile Banking Application เป็นของจริงหรือไม่นั้นให้ดูที่ชื่อผู้พัฒนา (Developer) ซึ่งจะแสดงชื่อสถาบันการเงินนั้นๆ	- ควรดูยอดการดาวน์โหลดเป็นหลัก - อ่านรีวิวของผู้ใช้งาน
ไม่ควรบอกรหัสเข้าใช้งาน Mobile Banking Application ให้คนอื่นได้รับทราบรวมถึงบุคคลในครอบครัว	- การบอกรหัสแก่คนในครอบครัวจะช่วยทำธุรกรรมแทนกันได้ในกรณีจำเป็น - คนในครอบครัวเป็นบุคคลที่สามารถไว้ใจได้
การยืนยันตัวตนเข้าใช้งาน Mobile Banking Application โดยใช้ One Time Password (OTP) มีความน่าเชื่อถือสูงกว่าการใช้รหัสผ่าน	- การใช้รหัสผ่านน่าจะปลอดภัยมากกว่าหากคนอื่นไม่รู้รหัสผ่านของเรา
การจดรหัสผ่านเข้าใช้งาน Mobile Banking Application ไว้บนโทรศัพท์มือถือไม่ได้ปลอดภัยกว่าการจดลงสมุดหรือเศษกระดาษ	- โทรศัพท์มือถือนั้นมีรหัสผ่านทำให้การบันทึกรหัสผ่านลงบนเครื่องน่าจะปลอดภัยมากกว่าการจดใส่เศษกระดาษหรือสมุด

ทั้งนี้จากแบบทดสอบทั้งสิ้น 10 ข้อมีจำนวน 6 ข้อที่ผู้วิจัยสามารถสัมภาษณ์เพิ่มเติมเชิงพฤติกรรมในกรณีที่ผู้ให้สัมภาษณ์สามารถตอบคำถามนั้นๆ ได้อย่างถูกต้องว่าได้มีการนำไปปฏิบัติจริงในชีวิตประจำวันหรือไม่ พบว่ามีกลุ่มตัวอย่างจำนวนหนึ่งนำไปใช้จริง แต่ในขณะเดียวกันก็พบว่ามีกลุ่มตัวอย่างจำนวนไม่น้อยที่ละเลยและไม่ปฏิบัติตามสิ่งที่ตนเองมีความรู้ความเข้าใจ โดยสามารถสรุปเป็นประเด็นสาระสำคัญได้ดังนี้

ข้อเท็จจริงที่ทราบ	**เหตุผลที่ไม่ปฏิบัติตาม**
การเชื่อมต่อ Wifi มีความเสี่ยงในแง่ความปลอดภัยในการเข้าใช้บริการ Mobile Banking มากกว่าการเชื่อมต่อเครือข่าย 3G และ 4G	- หากส่วนตัวคิดว่าสามารถไว้ใจ Wifi ของร้านค้าหรือผู้ให้บริการนั้นๆ ได้ - หากมีกระบวนการเข้าถึง Wifi ดังกล่าวอย่างเป็นขั้นตอน เช่น การกรอกรหัสผ่าน - เชื่อมต่อ Wifi เพื่อทำธุรกรรมผ่าน Mobile Banking โดยไม่ลังเลทั้งที่รู้ว่ามีความเสี่ยง
การเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่เรารู้จักไม่ได้ปลอดภัยกว่าการเชื่อมต่อ Wifi ที่แสดงชื่อร้านค้าที่เราไม่รู้จัก	- ไม่ได้ระวังตัวเองมากนัก - หากจำเป็นต้องใช้ก็จะใช้ - หากเป็นชื่อ Wifi ที่ใช้อยู่ประจำก็จะใช้ไม่ค่อยได้ระวังตัวเท่าไหร่
หลังการใช้งาน Mobile Banking Application ควร log out ออกจากระบบเสมอ	- หน่วงเวลาของระบบในการ log out อัตโนมัติค่อนข้างสั้น
การพิจารณา Mobile Banking Application เป็นของจริงหรือไม่นั้นให้ดูที่ชื่อผู้พัฒนา (Developer) ซึ่งจะแสดงชื่อสถาบันการเงินนั้นๆ	- ปกติไม่ได้สังเกตก่อนการดาวน์โหลด
ไม่ควรบอกรหัสเข้าใช้งาน Mobile Banking Application ให้คนอื่นได้รับทราบรวมถึงบุคคลในครอบครัว	- กล้าบอกรหัสให้กับคนในครอบครัวทราบโดยเฉพาะพ่อแม่พี่น้องเพราะคิดว่าสามารถไว้ใจได้ - เป็นธุรกิจกงสีใช้บัญชีที่เป็นชื่อของตนเองแต่เป็นเงินของทางบ้านเพราะฉะนั้นจะมีการบอกรหัสให้บุคคลในครอบครัวได้รับทราบ
การจดรหัสผ่านเข้าใช้งาน Mobile Banking Application ไว้บนโทรศัพท์มือถือไม่ได้ปลอดภัยกว่าการจดลงสมุดหรือเศษกระดาษ	- เป็นคนขี้ลืม

5.1.3 ความคิดเห็นของผู้ใช้บริการเกี่ยวกับระบบการยืนยันตัวตนบน Mobile Banking Application ที่เหมาะสม

จากการสัมภาษณ์ความคิดเห็นของกลุ่มตัวอย่างพบว่าวิธีการยืนยันตัวตนที่คิดว่าเหมาะสมเพื่อวัตถุประสงค์ในการ log in เข้าสู่ Mobile Banking Application คือ ลายนิ้วมือ รหัสผ่านตัวเลขหกหลัก และรหัสผ่านหกตัวอักษรตามลำดับ โดยที่เหตุผลหลักที่ผู้ให้สัมภาษณ์เลือกวิธีลายนิ้วมือเนื่องจากมีความสะดวก รวดเร็ว ง่าย ปลอมแปลงยาก ปลอดภัย อุปกรณ์มือถือรุ่นใหม่รองรับการสแกนลายนิ้วมือ และเพียงพอต่อการ log in ซึ่งเหตุผลดังกล่าวถือว่าค่อนข้างกว้างและครอบคลุมเหตุผลของกลุ่มตัวอย่างที่เลือกใช้วิธีรหัสผ่านตัวเลขหกหลัก ในขณะที่มีข้อเสนอแนะที่น่าสนใจและเป็นวิธีการยืนยันตัวตนที่ยังไม่ได้นำมาประยุกต์ใช้กับระบบการยืนยันตัวตนของธนาคารพาณิชย์ในประเทศนั่นคือรหัสผ่านแบบไม่จำกัดความยาวตายตัวซึ่งสามารถคาดเดารหัสผ่านได้ยาก

ในขณะที่วิธีการยืนยันตัวตนที่กลุ่มตัวอย่างคิดว่าเหมาะสมเพื่อวัตถุประสงค์ในการยืนยันรายการธุรกรรมที่ทำผ่าน Mobile Banking Application อันดับหนึ่งคือ One Time Password (OTP) และรองลงมาคือลายนิ้วมือ โดยเหตุผลหลักของการเลือกวิธียืนยันตัวตนแบบ OTP คือไม่ต้องจดจำ ปลอดภัย และง่าย ซึ่งเหตุผลสนับสนุนของผู้ให้สัมภาษณ์สำหรับการเลือกใช้สองวิธีนี้ถือว่าใกล้เคียงกันมากจะต่างเพียงลายนิ้วมือจะมีความสะดวก และกรณีย้ายเครื่องเปลี่ยนเบอร์โทรศัพท์ยังสามารถใช้งานได้ เป็นเหตุผลเพิ่มเติม

ในขณะที่งานวิจัยเชิงปริมาณในอดีตโดยเก็บข้อมูลจากกลุ่มตัวอย่างที่เป็นลูกค้าธนาคารอาศัยอยู่ในเวสท์เทิร์นออสเตรเลียพบว่าผู้คนส่วนใหญ่นิยมรหัสผ่านที่เป็นการผสมกันระหว่างตัวเลข อักขระพิเศษ ตัวอักษรเล็ก และ ตัวอักษรใหญ่ผสมกันมากถึงร้อยละ 32.5 รองลงมาคือ การผสมกันระหว่างตัวเลขและตัวอักษรเล็ก ร้อยละ 30 และ การใช้ตัวเลขเพียงอย่างเดียว ร้อยละ 7.5 ตามลำดับ โดยเก็บข้อมูลจากกลุ่มตัวอย่างที่เป็นลูกค้าธนาคารอาศัยอยู่ในเวสท์เทิร์นออสเตรเลีย (Nattakant Utakrit, 2012)

5.2 ข้อเสนอแนะสำหรับผู้บริหาร (Managerial Implications)

เพื่อให้ธนาคารพาณิชย์ที่เป็นผู้ให้บริการ Mobile Banking Application แก่ลูกค้าในประเทศสามารถตอบสนองความเชื่อมั่นในด้านความปลอดภัยแก่ผู้ใช้บริการดังกล่าว จากผลการวิจัยครั้งนี้ผู้วิจัยจึงมีข้อเสนอแนะดังนี้

ธนาคารควรมีการชี้แนะและสร้างความตระหนักเพิ่มเติมให้แก่ผู้ใช้งานเพื่อให้เกิดงานใช้งาน Mobile Banking Application อย่างปลอดภัยในวงกว้าง เนื่องจากพบว่ากลุ่มตัวอย่างหลายคนยังคงมีความเข้าใจผิดในบางประการเกี่ยวกับการใช้งานระบบดังกล่าว อาทิเช่น การเข้าใจข้อเท็จจริงคลาดเคลื่อนในกรณีเครือข่าย Wifi ปลอดภัยเพราะเป็นระบบส่วนบุคคลในขณะที่เครือข่าย 3G และ 4G เป็นเครือข่ายเปิดแบบสาธารณะจึงปลอดภัยน้อยกว่าในการเข้าใช้งาน Mobile Banking เป็นต้น อีกทั้งยังมีกลุ่มตัวอย่างจำนวนไม่น้อยที่ถึงแม้ว่าจะทราบถึงข้อพึงปฏิบัติในการใช้งาน Mobile Banking อย่างปลอดภัยแต่ก็ได้ละเลยและเลือกที่จะไม่ปฏิบัติตามสิ่งที่ตนเองรู้ เหล่านี้หากเกิดความเสียหายเกิดขึ้นแก่ผู้ใช้งานอาจนำไปสู่ความเสียหายต่อชื่อเสียงของธนาคารเองเนื่องจากผู้ใช้งานอาจกล่าวโทษว่าเป็นความผิดที่เกิดจากระบบของธนาคารที่ไม่รัดกุมเพียงพอ ทั้งๆที่ข้อเท็จจริงนั้นอาจเกิดจากพฤติกรรมเสี่ยงของตัวผู้ใช้งานเอง ดังนั้นมาตรการป้องกันเหตุจึงควรถูกนำมาพิจารณาโดยธนาคารพาณิชย์

นอกจากนี้เพื่อเสริมสร้างภาพลักษณ์ที่ดีของธนาคารเกี่ยวกับความเชื่อมั่นในด้านความปลอดภัยในการใช้งาน Mobile Banking Application ธนาคารควรให้ความสำคัญกับระบบการยืนยันตัวตนของธนาคารเนื่องจากมีกลุ่มตัวอย่างจำนวนมากกล่าวว่าสิ่งที่ทำให้ตนเองมีความเชื่อมั่นในด้านความปลอดภัยนั้นเกิดจากความเชื่อมั่นในระบบการยืนยันตัวตนของธนาคาร และในขณะเดียวกันก็มีกลุ่มตัวอย่างจำนวนไม่น้อยที่เสนอแนะให้มีการพัฒนาปรับปรุงระบบยืนยันตัวตนเพิ่มเติมเพื่อยกระดับความเชื่อมั่นด้านความปลอดภัยให้สูงขึ้น อาทิเช่น การนำ OTP มาใช้ในการยืนยันตัวตนจะช่วยสร้างความมั่นใจยิ่งขึ้นในการทำธุรกรรม หรือแม้กระทั่งการใช้ข้อมูลทางชีวภาพ (biometrics) จะช่วยในการยืนยันตัวบุคคลได้ปลอดภัยยิ่งขึ้นในมุมมองของตัวผู้ใช้งานที่เป็น Generation C ในขณะเดียวกันเมื่อกล่าวถึงวิธีการที่เหมาะสมในการยืนยันตัวตนเมื่อแบ่งแยกตามวัตถุประสงค์การใช้งานระหว่าง (1) การยืนยันตัวตนเพื่อ log-in เข้าสู่ระบบและ (2) การยืนยันตัวตนเพื่อยืนยันการทำธุรกรรมพบว่า วิธีการยืนยันตัวตนเพื่อ log-in ที่กลุ่มตัวอย่างกล่าวถึงมาที่สุดคือลายนิ้วมือ และรองลงมาคือรหัสผ่านตัวเลขหกหลัก โดยที่เหตุผลหลักที่เลือกลายนิ้วมือคือมีความสะดวก รวดเร็ว ง่าย ปลอมแปลงยาก ปลอดภัย อุปกรณ์มือถือรุ่นใหม่รองรับการสแกนลายนิ้วมือและความปลอดภัยเพียงพอต่อวัตถุประสงค์การใช้งานเพื่อ log in ซึ่งเหตุผลดังกล่าวถือว่ากว้างและครอบคลุมเหตุผลของการใช้รหัสผ่านตัวเลขหกหลัก ในขณะที่มีกลุ่มตัวอย่างบางส่วนเสนอนำความคิดในการประยุกต์ใช้รหัสผ่านแบบไม่จำกัดความยาวตายตัวซึ่งไม่เคยมีมาก่อนในประเทศไทยเพราะเห็นว่าคาดเดารหัสผ่านได้ยากและน่าจะมีความปลอดภัยสูง

สำหรับวิธีการที่เหมาะสมในการยืนยันตัวตนเพื่อยืนยันการทำธุรกรรมอันดับหนึ่งคือ OTP และรองลงมาคือลายนิ้วมือ หากพิจารณาเหตุผลสนับสนุนในการใช้ OTP ของกลุ่มตัวอย่าง

พบว่า ไม่ต้องจดจำ ปลอดภัย และง่าย ซึ่งเหตุผลสนับสนุนของผู้ให้สัมภาษณ์สำหรับการเลือกใช้สองวิธีนี้ถือว่าใกล้เคียงกันมากจะต่างเพียงลายนิ้วมือจะมีความสะดวก และกรณีย้ายเครื่องเปลี่ยนเบอร์โทรศัพท์ยังสามารถใช้งานได้

5.3 ข้อจำกัดในการวิจัย และข้อเสนอแนะสำหรับงานวิจัยในอนาคต

จากการทำวิจัยในครั้งนี้ มีข้อจำกัดในการวิจัยและข้อเสนอแนะสำหรับงานวิจัยในอนาคตดังนี้

1. เนื่องจากงานวิจัยนี้เป็นการศึกษาเกี่ยวกับความคิดเห็นของ Generation C ด้านความปลอดภัยบน Mobile Banking Application ที่ให้บริการโดยธนาคารพาณิชย์ในประเทศไทย คนกลุ่มนี้จะมีความรู้ความเข้าใจในด้านเทคโนโลยีสารสนเทศอยู่พอสมควรเนื่องจากมีการใช้งานอยู่ในชีวิตประจำวัน ดังนั้นงานวิจัยในอนาคตสามารถศึกษาความคิดเห็นของ Generation อื่นๆ เพราะความคิดเห็นที่ได้น่าจะมีความแตกต่างจากกลุ่มคนที่เป็น Generation C เนื่องจากมีความหลากหลายของประสบการณ์ ความรู้ความเข้าใจต่อเทคโนโลยีสารสนเทศในแต่ละช่วงวัยที่แตกต่างกัน

2. เนื่องจากงานวิจัยในครั้งนี้เป็นเชิงคุณภาพเพื่อศึกษาถึงเหตุผลที่ทำให้ Generation C เชื่อมั่นในด้านความปลอดภัยในการใช้งาน Mobile Banking Application ของ Generation C แต่ยังไม่สามารถบ่งชี้ได้ชัดในเชิงสถิติได้ว่าปัจจัยใดมีผลอย่างเป็นนัยยะสำคัญ รวมถึงกระบวนการในการยืนยันตัวตนที่สามารถบอกได้เพียงว่าวิธีการใดบ้างที่กลุ่มตัวอย่างเห็นว่าเหมาะสมในการใช้งานจริง ดังนั้น งานวิจัยในอนาคตจึงควรหาคำตอบในเชิงลึกว่าปัจจัยใดมีผลต่อความเชื่อมั่นด้านความปลอดภัยในการใช้งาน Mobile Banking Application อย่างมีนัยยะสำคัญ และรวมถึงวิธีการยืนยันตัวตนวิธีการใดที่คนส่วนใหญ่คิดว่าเหมาะสมในทางสถิติ โดยคำตอบเหล่านี้สามารถหาได้โดยงานวิจัยเชิงปริมาณ

3. การนำผลการศึกษาที่ได้จากงานวิจัยในครั้งนี้ไปประยุกต์ใช้ในธุรกิจการเงินที่เกี่ยวข้องยังต้องคำนึงถึงข้อจำกัดบางประการ เช่น ความเป็นไปได้เชิงเทคนิค ระดับความปลอดภัยที่ได้รับการยอมรับและเหมาะสม และบริบทอื่นๆ ควบคู่กันไป เนื่องจากการทำการวิจัยในครั้งนี้ผู้วิจัยให้อิสระแก่กลุ่มตัวอย่างในการแสดงความคิดเห็นในการตอบคำถามโดยไม่จำเป็นต้องคำนึงถึงข้อจำกัดกล่าวสำหรับระบบยืนยันตัวตน Mobile Banking Application เหล่านี้ถือเป็นข้อจำกัดในงานวิจัย

บรรณานุกรม

กุหลาบ ปุริสาร. (2556). วิธีวิทยาการวิจัยเชิงคุณภาพ (Qualitative Research Methodology). *วารสารวิทยาลัยบัณฑิตเอเชีย, 3(1)*, 1-15.

ทิพย์สุดา หมื่นหาญ. (2547). ปัจจัยที่มีผลต่อการตัดสินใจเลือกใช้บริการธนาคารผ่านอินเตอร์เน็ตของผู้ใช้บริการในเขตกรุงเทพมหานคร (วิทยานิพนธ์ปริญญาโท). มหาวิทยาลัยเชียงใหม่, เชียงใหม่.

ทีมวิเคราะห์ระบบการชำระเงิน ฝ่ายนโยบายระบบการชำระเงิน. ธนาคารแห่งประเทศไทย. (2557). *รายงานบริการทางการเงินผ่านโทรศัพท์เคลื่อนที่ Mobile Financial Service*. กรุงเทพฯ

ธนาคารธนชาต. (2561). *7 วิธีป้องกันไว้ ทุกครั้งที่ใช้ Mobile Banking ปลอดภัยไร้กังวลแน่นอน*. ค้นเมื่อวันที่ 20 ตุลาคม 2561, จาก https://thanachartcsr.com/project/7-วิธีป้องกันไว้-ทุกครั้งที่ใช้-mobile-banking-ปลอดภัย-ไร้กังวลแน่นอน/

บริษัทหลักทรัพย์ฟินันเซีย ไซรัส. (2561). *FINANSIA ชี้ Mobile Banking ทำให้ตลาดกังวลต่อการปรับลดลงของรายได้ค่าธรรมเนียมหุ้นกลุ่มแบงก์*. ค้นเมื่อวันที่ 15 ตุลาคม 2561, จาก https://mgronline.com/stockmarket/detail/9610000031270

ประพนธ์ หาญหริรักษ์. (2559). ความมั่นคงปลอดภัยของแอปพลิเคชันธนาคารบนมือถือ (วิทยานิพนธ์ปริญญาโท). มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ, กรุงเทพฯ.

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ สายกำกับสถาบันการเงิน. ธนาคารแห่งประเทศไทย. (2557). *แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices)*. กรุงเทพฯ

ฝ่ายนโยบายระบบการชำระเงิน. ธนาคารแห่งประเทศไทย. (2560). *แนวนโยบายเรื่อง การเสริมสร้างความเชื่อมั่นการชำระเงินโดยอุปกรณ์เคลื่อนที่*. กรุงเทพฯ

บรรณานุกรม (ต่อ)

ภุชพงค์ โนดไธสง. (2561). *สำนักงานสถิติแห่งชาติ เปิดตัวแอป Thai Stat ดูสถิติรอบด้าน ที่คนไทยจำเป็นต้องรู้*. ค้นเมื่อวันที่ 15 ตุลาคม 2561, จาก https://www.it24hrs.com/2017/nso-thai-stat-app-announce/

ภูมิ ภูมิรัตน์. (2561). *Mobile Banking ใช้อย่างไรให้ปลอดภัย*. ค้นเมื่อวันที่ 20 ตุลาคม 2561. จาก https://www.g-able.com/digital-review/digital-transformation/cybersecurity/mobile-banking-ใช้ให้ปลอดภัย/

วรางรัตน์ ขันคำ. (2553). การรับรู้ความเสี่ยงและปัจจัยส่วนประสมทางการตลาดที่มีความสำคัญต่อการตัดสินใจใช้บริการธนาคารบนอินเทอร์เน็ต (วิทยานิพนธ์ปริญญาโท). มหาวิทยาลัยเกษตรศาสตร์, กรุงเทพฯ.

สามารถ แสนภิบาล. (2553). ปัจจัยการใช้ธนาคารบนมือถือผ่านเทคโนโลยีโครงข่ายสื่อสาร 3G กรณีศึกษาธนาคารไทยพาณิชย์ จำกัด (มหาชน) (วิทยานิพนธ์ปริญญาโท). มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

สุภางค์ จันทวานิช. (2543). *การวิเคราะห์ข้อมูลในการวิจัยเชิงคุณภาพ* (พิมพ์ครั้งที่ 3). กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

สุรีย์พร เหมืองหลิ่ง. (2559). ปัจจัยที่มีผลต่อความเชื่อมั่นในการใช้บริการทางการเงินผ่าน Mobile Banking Application ของผู้ใช้บริการในเขตกรุงเทพมหานครและปริมณฑล (วิทยานิพนธ์ปริญญาโท). มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

สุวิสา สุรังสิมันต์กุล. (2551). ความพึงพอใจของผู้ใช้บริการธนาคารทางอินเตอร์เน็ตของธนาคารไทยพาณิชย์ จำกัด (มหาชน) ในเขตอำเภอเมือง จังหวัดเชียงใหม่ (วิทยานิพนธ์ปริญญาโท). มหาวิทยาลัยเชียงใหม่, เชียงใหม่.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2560). *ร่างข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการยืนยันตัวตนทางอิเล็กทรอนิกส์*. กรุงเทพฯ

บรรณานุกรม (ต่อ)

หทัยชนก พรรคเจริญ. (2555). เทคนิคการเลือกตัวอย่าง. เอกสารบรรยายสำนักนโยบายและวิชาการ สถิติ สำนักสถิติแห่งชาติ

ACIS Professional Center. (2556). *Information Security Research on Thailand' s Internet Banking/ Mobile Banking.* ค้นเมื่อวันที่ 20 ตุลาคม 2561, จาก https://www.acisonline.net/?p=908

Fannin Bank. (2561). *Mobile Banking Security Tips*. ค้นเมื่อวันที่ 15 ตุลาคม 2561, จาก https://www.fanninbank.com/mobile-banking-security.php

Fusionsport. (2017). *How Many Likert Scale Points are Optimal?*. ค้นเมื่อวันที่ 20ตุลาคม 2561. จาก https://www.fusionsport.com/blog/agree-to-disagree-how-many-likert-scale-points-is-optimal/

Gefen, D. (2000). E-Commerce: The Role of familiarity and trust. *Omega, 28(6)*, 725-737.

Google Ads. (2561). *ป้องกันตนเองจากมัลแวร์*. ค้นเมื่อวันที่ 20 ตุลาคม 2561. จาก https://support.google.com/google-ads/answer/2375413?hl=th

Jeff Toister. (2018). *Should survey rating scales be even or odd?*. ค้นเมื่อวันที่ 20 ตุลาคม 2561, จาก https://www.toistersolutions.com/blog/2017/12/28/should-customer-service-survey-scales-be-even-or-odd

Maybank Kim Eng Securities (ประเทศไทย). (2014). *ใช้งาน Internet Banking และ Mobile Banking อย่างไรให้ปลอดภัย*. ค้นเมื่อวันที่ 15 ตุลาคม 2561, จาก https://www.it24hrs.com/2014/mobile-banking-safety/

Nastasi, B. K. and Schensul, S. L. (2005). "Contributions of qualitative research to the validity of intervention research", *Journal of School Psychology. 43(3)*, 177-195.

Nattakant Utakrit. (2012). Security awareness by online banking users in Western Australian of phishing attacks (Publised doctoral dissertation). Edith Cowan University, Australia

บรรณานุกรม (ต่อ)

Norton. (2561). *Wifi: What is a man-in-the-middle attack?*. ค้นเมื่อวันที่ 15 ตุลาคม 2561, จาก https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

Octopatr. (2015). *ระวังมิจฉาชีพมาหลอกเอา password (รหัสผ่าน) ของคุณไปง่ายๆ ในไม่กี่วินาที*. ค้นเมื่อวันที่ 20 ตุลาคม 2561. จาก https://droidsans.com/people-tricked-to-give-their-password/

OKnation. (2560). *การใช้สื่อของคน Gen C*. ค้นเมื่อวันที่ 15 ตุลาคม 2561, จาก http://oknation.nationtv.tv/blog/print.php?id=1022632

Paul Wagenseil. (2015). *Malware-Infected iPhone Apps: What You Need to Know*. ค้นเมื่อวันที่ 20 ตุลาคม 2561. จาก https://www.tomsguide.com/us/malware-iphone-app-store-faq,news-21613.html

Yousafzai, S.Y., Pallister, J.G. & G.R. Foxal (2003). A proposed model of e-trust for electronic banking. *Technovation*, *23(11)*, 847–860.

ภาคผนวก ก

แบบสัมภาษณ์แบบกึ่งโครงสร้าง

สำหรับ Generation C ที่ใช้ Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย

งานวิจัยเรื่อง

ความคิดเห็นเกี่ยวกับความปลอดภัยบน Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย

ผู้วิจัย: นายบุญช่วย โค้วตระกูล
นักศึกษาปริญญาโท สาขาการจัดการธุรกิจ วิทยาลัยการจัดการ มหาวิทยาลัยมหิดล

แบบสัมภาษณ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาการจัดการมหาบัณฑิต สาขาวิชาการจัดการธุรกิจ วิทยาลัยการจัดการ มหาวิทยาลัยมหิดล

แบบสัมภาษณ์นี้เป็นแนวทางสำหรับใช้ในการสัมภาษณ์กลุ่มตัวอย่างที่เป็น Generation C ที่ใช้ Mobile Banking Application เพื่อเก็บรวบรวมข้อมูลสำหรับงานวิจัยเรื่อง “ความคิดเห็นเกี่ยวกับความปลอดภัยบน Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย” โดยมีวัตถุประสงค์เพื่อศึกษาว่า

- ความเชื่อมั่นของผู้ใช้บริการ Mobile Banking Application ที่มีต่อความปลอดภัย
- ความรู้ความเข้าใจของผู้ใช้บริการ Mobile Banking Application ในการทำธุรกรรมทางการเงินอย่างปลอดภัย และการนำไปปฏิบัติ
- ความคิดเห็นของผู้ใช้บริการเกี่ยวกับระบบการยืนยันตัวตนบน Mobile Banking Application ที่เหมาะสม

ข้อมูลที่ได้รับจะถูกรักษาไว้เป็นความลับและจะถูกนำไปใช้เพื่อประโยชน์ทางการศึกษาเท่านั้น

แบบคำถามที่ใช้ในการสัมภาษณ์

ชื่อผู้ให้สัมภาษณ์: …… อายุ: …… ปี

อาชีพ: …… ระดับการศึกษา: ……

Mobile Banking Application ที่ใช้อยู่ในอดีตหรือปัจจุบัน: ……..

ระยะเวลาใช้งาน Mobile Banking Application จนถึงปัจจุบัน (โดยประมาณ): …… ปี ……. เดือน

ระดับความเชื่อมั่นของผู้ใช้งาน Mobile Banking Application ในเรื่องความปลอดภัย

☐ ระดับความเชื่อมั่นในความปลอดภัยในภาพรวมของ Mobile Banking Application ของธนาคารพาณิชย์ในประเทศไทย ท่านให้คะแนนในระดับใดระหว่าง 1 ถึง 10 โดยที่ 1 หมายถึงเชื่อมั่นน้อยที่สุด และ 10 หมายถึงเชื่อมั่นมากที่สุด

☐ เหตุผลที่ท่านให้คะแนนความเชื่อมั่นดังกล่าว คือ ……..

ระดับความรู้ความเข้าใจของผู้ใช้บริการ Mobile Banking Application ในการทำธุรกรรมทางการเงินอย่างปลอดภัย

☐ กรุณาทำ**แบบทดสอบ**วัดความรู้ความเข้าใจเรื่องความปลอดภัยที่เกี่ยวกับ Mobile Banking Application จำนวนทั้งสิ้น 10 ข้อ โดยให้เลือก X ตรงช่องถูก หรือ ผิด อย่างใดอย่างหนึ่ง

☐ ทำไมท่านถึงเลือกตอบข้อ ……. เป็นคำตอบนี้ ท่านมีความมั่นใจในคำตอบมากน้อยแค่ไหน กรุณาช่วยอธิบายขยายความคำตอบดังกล่าว

☐ โดยปกติ ท่านได้นำความรู้ความเข้าใจดังกล่าวไปใช้จริงมากน้อยเพียงใด โปรดยกตัวอย่าง

ความคิดเห็นของผู้ใช้บริการเกี่ยวกับระบบการยืนยันตัวตนบน Mobile Banking Application ที่เหมาะสมที่สุด

- ☐ ท่านสามารถศึกษารายละเอียดเกี่ยวกับวิธีการยืนยันตัวตนจากเอกสารสรุปวิธีการยืนยันตัวตนบน Mobile Banking Application ที่ได้มอบให้
- ☐ โดยส่วนใหญ่แล้วการยืนยันตัวตนบน Mobile Banking Application จะทำใน 2 ลักษณะคือ การยืนยันตัวตนในขั้นตอนการ log in เข้าสู่ Mobile Banking Application และการยืนยันรายการธุรกรรม
  - ○ ท่านเห็นการยืนยันตัวตนในขั้นตอนการ log in ควรใช้วิธีการใด **เพราะเหตุผลใด**
  - ○ ท่านเห็นว่าการยืนยันรายการธุรกรรม ควรใช้วิธีการใด เพราะเหตุ**ใด**
- ☐ **ท่**านเห็นว่าการยืนยันตัวตนในขั้นตอนการ log in และการยืนยันรายการธุ**รกรรม ควรใช้วิธีการเดียวกัน หรือใช้การยืนยันตัวตน 2 ชั้น** เพราะเหตุใด

แบบทดสอบ

กรุณาทำเครื่องหมายกากบาท (X) ในช่อง “ถูก” หรือ “ผิด” หลังข้อความ (Statement)

ข้อความ (Statement)	ถูก	ผิด
1. การเชื่อมต่อเครือข่าย 3G และ 4G เพื่อใช้งาน Mobile Banking Application มีความเสี่ยงด้านความปลอดภัย**มากกว่า**การเชื่อมต่อผ่าน WIFI		
2. การเข้าทำธุรกรรมออนไลน์ผ่าน website ของธนาคารจะมีความเสี่ยง**น้อยกว่า** Mobile Banking Application		
3. การเชื่อมต่อ WIFI ที่แสดงชื่อร้านค้าที่เรารู้จักตามที่สาธารณะมีความปลอดภัย**มากกว่า**การเชื่อมต่อกับ WIFI แสดงชื่อที่เราไม่รู้จัก		
4. การ log in เข้าใช้งาน Mobile Banking Application เมื่อใช้งานเสร็จแล้ว เรา**ไม่จำเป็น**ต้อง log out ก็ได้		
5. หากดาวน์โหลดแอพจาก App Store (สำหรับระบบปฏิบัติการ iOS) **ไม่ต้องกังวล**เรื่องแอพที่มีมัลแวร์แฝงอยู่เหมือนการดาวน์โหลดจาก Play Store (สำหรับระบบปฏิบัติการ Android)		
6. หากอยากทราบว่า Mobile Banking Application เป็นของจริงหรือของปลอมให้ดูได้ที่คะแนนรีวิวจากผู้ใช้งานคนอื่นๆ		
7. การดาวน์โหลดซอฟต์แวร์ฟรีบนอินเทอร์เน็ต**ไม่เกี่ยวข้อง**กับการติดมัลแวร์		
8. **ไม่ควร**บอกรหัสเข้าใช้งาน Mobile Banking Application ให้กับคนอื่นได้รับทราบ ยกเว้นบุคคลในครอบครัวเท่านั้น		
9. การยืนยันตัวตนเข้าใช้งาน Mobile Banking Application โดยใช้ One Time Password (OTP) มีระดับความน่าเชื่อถือ**สูงกว่า**การใช้รหัสผ่าน (Password)		
10. ไม่ควรจดรหัสผ่านเข้าใช้งาน Mobile Banking Application ไว้ในสมุดหรือเศษกระดาษ แต่ควรบันทึกไว้ในโทรศัพท์มือถือซึ่งจะมีความปลอดภัย**มากกว่า**		

เฉลย:

ถูก	ข้อความที่ 9
ผิด	ข้อความที่ 1, 2, 3, 4, 5, 6, 7, 8, 10

เอกสารสรุปชนิดของสิ่งที่ใช้ยืนยันตัวตน

สำหรับผู้ให้สัมภาษณ์

สิ่งที่ใช้ยืนยันตัวตน	ภาพประกอบ
รหัสผ่าน 4 ตัวเลข	1234
รหัสผ่าน 6 ตัวเลข	123456
รหัสผ่าน 6 ตัวอักษร	123AbC
รหัสผ่าน 8 ตัวอักษร	1234AbCd
One-time password (OTP)	
ลายนิ้วมือ	
ม่านตา	
Face recognition	
Token