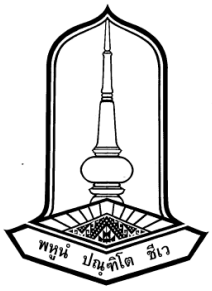


การวิเคราะห์ความปลอดภัยและความมั่นคงสำหรับระบบธนาคาร ผ่านโทรศัพท์มือถือในประเทศไทย

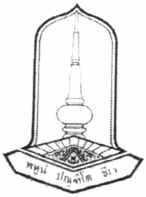
นิภาพร แสงทวี

เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
กรกฎาคม 2559

การวิเคราะห์ความปลอดภัยและความมั่นคงสำหรับระบบธนาคาร ผ่านโทรศัพท์มือถือในประเทศไทย

นิภาพร แสงทวี

เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
กรกฎาคม 2559



คณะกรรมการสอบการศึกษาค้นคว้าอิสระ ได้พิจารณาการศึกษาค้นคว้าอิสระ ของนางสาวนิภาพร แสงทวี แล้วเห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยมหาสารคาม

คณะกรรมการสอบการศึกษาค้นคว้าอิสระ

.....	ประธานกรรมการ
(อาจารย์ ดร.รพีพร ซ่ำชอง)	(กรรมการบัณฑิตศึกษาภายนอกภาควิชา)
.....	กรรมการ
(อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์)	(อาจารย์ที่ปรึกษาการศึกษาค้นคว้าอิสระ)
.....	กรรมการ
(ผศ.ดร.จิรัฏฐา ภูบุญอบ)	(อาจารย์บัณฑิตศึกษาประจำคณะ)

มหาวิทยาลัยอนุมัติให้รับการศึกษาค้นคว้าอิสระฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยมหาสารคาม

.....	.....
(ผศ.ดร.สุจิน บุตรดีสุวรรณ)	(ศ.ดร.ประดิษฐ์ เทอดทูล)
คณบดีคณะวิทยาการสารสนเทศ	คณบดีบัณฑิตวิทยาลัย
	วันที่ 29 เดือน ก.ค. พ.ศ. 2559

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จสมบูรณ์ได้ด้วยความกรุณาและความช่วยเหลืออย่างสูงยิ่งจาก อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์ ประธานกรรมการควบคุมวิทยานิพนธ์ อาจารย์ ดร.รพีพร ช่ำชอง ประธานกรรมการสอบ และผู้ช่วยศาสตราจารย์ ดร.จิรัฏฐา ภูบุญอบ กรรมการสอบ

ขอขอบพระคุณ อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์ ที่ถ่ายทอดความรู้วิชาตลอดจนคอยพร่ำสอนศิษย์ ด้วยเมตตาจิต ผู้ซึ่งมีจิตวิญญาณของความเป็นครูโดยแท้จริง

ขอบคุณผู้เชี่ยวชาญที่ช่วยตรวจเครื่องมือการวิจัย

ขอขอบพระคุณคณะวิทยาการสารสนเทศและมหาวิทยาลัยมหาสารคามที่เป็นสถาบันการศึกษาให้ความรู้

ขอขอบพระคุณ บิดามารดา ที่คอยสนับสนุนค่าใช้จ่ายในการเล่าเรียนและเป็นกำลังใจจนทำให้งานการศึกษาค้นคว้าอิสระครั้งนี้สำเร็จไปได้ด้วยดี

ขอขอบคุณพี่ๆ เพื่อนๆ และผู้ช่วยวิจัย ISAN ที่คอยให้คำปรึกษาและคอยช่วยเหลือเกื้อกูลมาโดยตลอด

ขอขอบพระคุณ คณะผู้บริหารสำนักงานธนารักษ์พื้นที่ จังหวัดมหาสารคาม ที่เห็นความสำคัญของการศึกษาโดยเปิดให้โอกาสใช้เวลาราชการเพื่อมาติดต่อประสานงานที่มหาวิทยาลัยมหาสารคาม

นิภาพร แสงทวี

ชื่อเรื่อง การวิเคราะห์ความปลอดภัยและความมั่นคงสำหรับระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย
ผู้ศึกษา นางสาวนิภาพร แสงทวี
ปริญญา ปริญญาวิทยาศาสตรมหาบัณฑิต **สาขาวิชา** เทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์
มหาวิทยาลัย มหาวิทยาลัยมหาสารคาม **ปีที่พิมพ์** 2559

บทคัดย่อ

Mobile Banking (m-banking) เป็นบริการธนาคารออนไลน์ผ่านทางแอปพลิเคชันบนสมาร์ทโฟน ซึ่งเป็นทางเลือกที่ต่างจากระบบธนาคารผ่านเครือข่ายอินเทอร์เน็ต (i-banking) ซึ่งใช้โปรแกรมเว็บแอปพลิเคชันผ่านเบราว์เซอร์ เมื่อเทียบกับ i-banking แล้ว m-banking คาดว่าน่าจะความปลอดภัยและมั่นคงมากกว่า แต่ยังมีรายงานเกี่ยวกับคดีความด้านการโจมตีระบบธนาคารเพิ่มมากขึ้น ในช่วงไม่กี่ปีที่ผ่านมา ดังนั้นงานวิจัยหลายชิ้นก่อนหน้านี้ ได้วิเคราะห์ปัญหาความมั่นคงความปลอดภัยของระบบ i-banking แต่ส่วนใหญ่ยังไม่ได้มุ่งเน้นในส่วนของระบบ m-banking โดยมีเพียงบางส่วนที่ได้ทำการสำรวจเกี่ยวกับระบบ m-banking แต่ส่วนใหญ่เน้นทางด้านเทคนิคหรือด้านความมั่นคง แต่ยังขาดการสำรวจด้านการจัดการหรือด้านความปลอดภัยของระบบ m-banking และที่สำคัญงานเหล่านั้น ยังไม่ได้วิเคราะห์ในประเด็นที่สำคัญต่อไปนี้คือ: กรณีคดีที่เคยเกิดขึ้น การสังเกตการณ์ในรายละเอียดของการให้บริการจริง การทดลองเพื่อทะลวงระบบ m-banking จากฝั่งของผู้ใช้จริง ดังนั้น บทความนี้จึงเสนอการวิเคราะห์ทั้งด้านความปลอดภัยและความมั่นคงของระบบ m-banking โดยครอบคลุมประเด็นสำคัญที่กล่าวไปแล้ว จากการตรวจสอบธนาคาร 6 แห่งในประเทศไทย ได้พบจุดอ่อนของระบบ m-banking หลายอย่าง โดยผลจากงานวิจัยนี้สามารถใช้เป็นทิศทางและแนวทางในการปรับปรุงความปลอดภัยและความมั่งคงของระบบ m-banking ต่อไป

คำสำคัญ: ธนาคารผ่านโทรศัพท์มือถือ, ความปลอดภัย, ความมั่นคง, วิศวกรรมสังคม

TITLE An Analysis of Safety and Security for Mobile Banking Systems in Thailand
AUTHOR MissNipaporn Seangtawee
DEGREE Master of Science **MAJOR** Information Technology
ADVISOR Dr. Somnuk Puangpronpitag
UNIVERSITY Mahasarakham University **YEAR** 2016

ABSTRACT

Mobile banking (m-banking) is an online banking service via a smartphone application. It is an alternative to internet banking (i-banking), which use a web application via a web browser. In comparison to i-banking, m-banking has been expected to be safer and securer. However, several bank-hacking crimes have been increasingly reported during the last few years. So, several previous studies have analyzed the i-banking security/safety issues. Yet, most of them have not yet focused on the m-banking. Some of them have investigated on m-banking only on the technical (security) but not the management (safety) side. Significantly, most of them have not yet analyzed according to the following critical points: the occurred crime cases, the detailed observation on the real services, the experiments to break the real mobile banking systems on the user side. Hence, in this paper, we propose to analyze both safety & security and cover all the aforementioned significant points. By investigating on six banks in Thailand, we have found several weaknesses of the m-banking systems. The contribution from this work can be a guiding direction to improve the security and safety of the m-banking systems.

Keyword: Mobile Banking, Safety, Security, Social Engineer

สารบัญ

หน้า

กิตติกรรมประกาศ ..... ก
บทคัดย่อ ..... ข
สารบัญตาราง ..... ช
สารบัญรูป ..... ซ

บทที่ 1 บทนำ 1
1.1 หลักการและเหตุผล 1
1.2 วัตถุประสงค์ 2
1.3 ขอบเขตของการศึกษา 2
1.4 ความสำคัญของการศึกษา 3
1.5 นิยามศัพท์เฉพาะ 3

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 4
2.1 Mobile Banking vs. Internet Banking 4
2.2 Safety vs. Security 4
2.3 แนวโน้มของระบบธนาคารผ่านโทรศัพท์มือถือ 5
2.4 จำนวนผู้ใช้งานระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย 5
2.5 ความเป็นมาของการทำธุรกรรมการเงินผ่านโทรศัพท์มือถือ 6
2.5.1 K-Mobile Banking ATM SIM: ธนาคารกสิกรไทย จำกัด (มหาชน) 6
2.5.2 KTB Online Mobile: ธนาคารกรุงไทย จำกัด (มหาชน) 7
2.5.3 SCB Mobile Banking: ธนาคารไทยพาณิชย์ จำกัด (มหาชน) 8
2.5.4 TMB M-Banking: ธนาคารทหารไทย จำกัด (มหาชน) 8
2.5.5 Bualuang M-Banking: ธนาคารกรุงเทพ จำกัด (มหาชน) 9
2.5.6 Krungsri M-Banking: ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) 9
2.6 ระบบปฏิบัติการบนสมาร์ทโฟน 10
2.7 เทคโนโลยีที่เกี่ยวข้องในการใช้งานระบบ m-banking 11
2.8 ภัยคุกคามการใช้งานระบบธนาคารบนโทรศัพท์มือถือในปัจจุบัน 12
2.8.1 วิเคราะห์ปัญหา Social Engineering 12
2.8.2 วิเคราะห์ปัญหา SMS Spoofing 13
2.8.3 การโจมตีด้วย Mobile Phone Trojans 14
2.8.4 เตือนผู้ใช้ Android อย่าโหลดลิงค์ APK ใน SMS 15
2.8.5 ลักษณะ SMS delay 16
2.8.6 วิเคราะห์ปัญหามัลแวร์ 16

หน้า

2.8.7 ช่องโหว่ของซิมการ์ดที่ทำให้ผู้ไม่ประสงค์ดีสามารถสำเนาซิมการ์ดได้โดยง่าย 18
2.8.8 Masque Attack ภัยคุกคามใหม่บน iPhone และ iPad 18
2.8.9 เตือนภัย “Internet Banking” ปล้นวันละแสน 19
2.8.10 เตือนผู้ใช้ Apple ระวังมัลแวร์สายพันธุ์ใหม่ ระบาดบน iOS และ OS X 20
2.8.11 เตือนระวังลงแอปพลิเคชันไฟฉายบนมือถือก็โดนขโมยข้อมูล 20
2.9 ความมั่นคงของระบบ m-banking 21
2.9.1 Triple Lock Security 21
2.9.2 Two Factor Authentication (2FA) 21
2.10 การโจมตีแบบแทรกกลางการสื่อสาร 22
2.10.1 การโจมตีแบบแทรกกลางการสื่อสารด้วยเครื่องมือ Cain & Abel 22
2.10.2 การโจมตีแบบ SSL Strip 24
2.11 ดัชนีความสอดคล้อง (Index of Consistency) 24
2.12 งานวิจัยที่เกี่ยวข้อง 25

บทที่ 3 วิธีดำเนินการวิจัย 31
3.1 ภาพรวมการดำเนินการศึกษา 31
3.2 ด้านความปลอดภัยของ m-banking 32
3.3 ด้านความมั่นคงของ m-banking 38
3.4 ด้านความปลอดภัยของผู้ให้บริการ Mobile Sim 41
3.5 ด้านการวิเคราะห์พฤติกรรมของผู้ใช้ Smartphone 41
3.6 ข้อจรรยาบรรณในการวิจัย 43

บทที่ 4 ผลการดำเนินงาน 44
4.1 ผลด้านความปลอดภัยระบบ m-banking 44
4.1.1 การเปิดบัญชีธนาคาร 44
4.1.2 การสมัครใช้งานระบบ m-banking 46
4.1.3 ลักษณะการ Login เข้าสู่ระบบ 48
4.1.4 ลักษณะการ Reset ข้อมูล 50
4.1.5 ลักษณะการเปลี่ยนเบอร์มือถือ 52
4.1.6 ลักษณะของ OTP 53
4.1.7 ลักษณะการเชื่อมต่ออินเทอร์เน็ต 54
4.1.8 มาตรการความปลอดภัยอื่นๆ 54
4.1.9 การยกเลิกการใช้งานระบบ m-banking 55
4.1.10 การปิดบัญชี 56
4.2 ผลด้านความมั่นคงของระบบ m-banking 56

หน้า

4.2.1 ผลการทดสอบการโจมตีแบบ SSL Sniff 56
4.2.2 ผลการทดสอบการโจมตีแบบ SSL Strip 57
4.2.3 รูปแบบการโจมตีด้วยวิธีแทรกกลางการสื่อสาร 59
4.3 ผลด้านความปลอดภัยของผู้ให้บริการ Mobile Sim 60
4.4 ผลด้านการวิเคราะห์พฤติกรรมของผู้ใช้ Smartphone 61

บทที่ 5 สรุปอภิปรายผล และข้อเสนอแนะ 64
5.1 สรุปอภิปรายผล 64
5.1.1 ผลด้านความปลอดภัยของระบบ m-banking 64
5.1.2 ผลด้านความมั่นคงระบบ m-banking 66
5.1.3 ผลด้านความปลอดภัยของผู้ให้บริการ Mobile Sim 67
5.1.4 ผลการวิเคราะห์พฤติกรรมผู้ใช้ Smartphone 67
5.2 ผลสัมฤทธิ์ที่ได้จากการศึกษา 68
5.2.1 ผลการศึกษาปัญหา 68
5.2.2 ผลการวิเคราะห์ปัญหา 68
5.3 ข้อเสนอแนะ 68

เอกสารอ้างอิง 69

ภาคผนวก 73
ภาคผนวก ก ตารางการหาค่า IOC จากความเห็นผู้เชี่ยวชาญ 74
ภาคผนวก ข แบบสอบถาม 76

ประวัติย่อผู้ศึกษา 79

สารบัญตาราง

หน้า

ตารางที่ 2.1 ส่วนแบ่งการตลาดของสมาร์ทโฟนทั่วโลก....11
ตารางที่ 2.2 ตัวอย่างปัญหา การโจมตีที่พบและแนวทางการป้องกันที่เกิดขึ้นกับการรักษาความปลอดภัยในการใช้งานอินเทอร์เน็ตแบงก์กิ้ง....26
ตารางที่ 2.3 เปรียบเทียบประเด็นด้านความปลอดภัยและความมั่นคงของงานวิจัยที่เกี่ยวข้อง....30
ตารางที่ 3.1 ตัวอย่างตารางที่ใช้ในการแสดงผลด้านความปลอดภัยของ m-banking....37
ตารางที่ 3.2 ผลการสำรวจผู้ให้บริการ Mobile Sim....41
ตารางที่ 4.1 ผลการสำรวจการเปิดบัญชีธนาคาร....44
ตารางที่ 4.2 ผลการสำรวจการสมัครใช้งานระบบ m-banking....46
ตารางที่ 4.3 ผลการสำรวจลักษณะการ Login เข้าสู่ระบบ....49
ตารางที่ 4.4 ผลการสำรวจลักษณะการ Reset ข้อมูล....50
ตารางที่ 4.5 ผลการสำรวจลักษณะการเปลี่ยนเบอร์มือถือ....52
ตารางที่ 4.6 ผลการสำรวจลักษณะของ OTP....53
ตารางที่ 4.7 ผลสำรวจการเชื่อมต่ออินเทอร์เน็ตของระบบ m-banking....54
ตารางที่ 4.8 ผลการสำรวจมาตรการความปลอดภัยอื่นๆ....55
ตารางที่ 4.9 ผลการสำรวจการยกเลิกการใช้งานระบบ m-banking....55
ตารางที่ 4.10 ผลการสำรวจการปิดบัญชี....56
ตารางที่ 4.11 ผลการสำรวจผู้ให้บริการ Mobile Sim....60

สารบัญรูป

หน้า

รูปที่ 2.1 Global mobile banking users 5
รูปที่ 2.2 สถิติเกี่ยวกับช่องทางการทำธุรกรรมทางออนไลน์ของธนาคารในประเทศไทย 6
รูปที่ 2.3 K-Mobile Banking PLUS 7
รูปที่ 2.4 KTB netbank 7
รูปที่ 2.5 SCB Easy 8
รูปที่ 2.6 TMB Touch 9
รูปที่ 2.7 Bualuang mbanking 9
รูปที่ 2.8 Krungsri Mobile Application 10
รูปที่ 2.9 The Faked Document 13
รูปที่ 2.10 เอสเอ็มเอสปลอม 14
รูปที่ 2.11 เอสเอ็มเอสที่แฝงไฟล์มัลแวร์บนระบบปฏิบัติการแอนดรอยด์ 15
รูปที่ 2.12 แอปพลิเคชันจริงและปลอมของ Google Services Framework 16
รูปที่ 2.13 แจ้งเตือนวิธีการโหลดแอปพลิเคชันให้ปลอดภัย 17
รูปที่ 2.14 Faked Mobile Banking Applications by Scientifika Media 17
รูปที่ 2.15 แจ้งเตือนการส่งเอสเอ็มเอสแอบอ้างดาวน์โหลดแอปพลิเคชันของธนาคาร 19
รูปที่ 2.16 ตัวอย่างแอปพลิเคชันไฟฉายที่ขอสิทธิ์มากเกินไป 21
รูปที่ 2.17 ลักษณะการใช้งานระบบ 2FA 22
รูปที่ 2.18 การกำหนดการ์ดเครือข่าย 23
รูปที่ 2.19 ปุ่ม Start/Stop เพื่อเริ่มใช้งาน 23
รูปที่ 2.20 ค้นหาเป้าหมายที่ต้องการโจมตี 23
รูปที่ 3.1 ภาพรวมของการศึกษาค้นคว้าอิสระ 31
รูปที่ 3.2 ประเด็นที่นำมาใช้ในการวิเคราะห์ด้านความปลอดภัยของ m-banking 32
รูปที่ 3.3 การใส่รหัส PIN Lock ก่อนเข้าสู่ระบบของธนาคาร 34
รูปที่ 3.4 การนำ Limit Login มาตรวจสอบการเข้าสู่ระบบ 34
รูปที่ 3.5 ลักษณะการ Reset Password 35
รูปที่ 3.6 ลักษณะยืนยันการโอนเงินด้วยรหัส OTP 36
รูปที่ 3.7 ประเด็นที่จะใช้ในการวิเคราะห์ด้านความมั่นคงของ m-banking 38
รูปที่ 3.8 วิเคราะห์โครงสร้างการโจมตีระบบ m-banking ผ่าน 3G และ 4G 38
รูปที่ 3.9 วิเคราะห์สถานการณ์จำลองการโจมตีระบบ m-banking ผ่าน Wi-Fi 39
รูปที่ 4.1 ผลการดักจับข้อมูลด้วยเทคนิค SSL Sniff ผ่าน Browser 57
รูปที่ 4.2 ผลการดักจับข้อมูลด้วยเทคนิค SSL Strip ผ่าน Application 58
รูปที่ 4.3 ผลการดักจับข้อมูลด้วยเทคนิค SSL Strip ผ่าน Browser 58
รูปที่ 4.4 SSL Sniff 59
รูปที่ 4.5 SSL Strip 59

บทที่ 1

บทนำ

1.1 หลักการและเหตุผล

จากเดิมการทำธุรกรรมการเงินจะต้องไปที่สาขาหรือตู้เอทีเอ็ม ซึ่งทำให้เสียเวลาในการเดินทางและการต่อคิว ธนาคารจึงเริ่มนำเทคโนโลยีมาอำนวยความสะดวกให้กับลูกค้า โดยเริ่มมีการใช้ระบบ Internet Banking (i-banking) ผ่านเว็บเบราว์เซอร์บนอุปกรณ์คอมพิวเตอร์และสมาร์ทโฟน ต่อมาเนื่องจากการใช้สมาร์ทโฟน เริ่มมีบทบาทในชีวิตประจำวันมากขึ้น เพราะเป็นอุปกรณ์ที่มีขนาดเล็กพกพาสะดวก ธนาคารต่างๆ จึงมีการพัฒนาจาก i-banking มาเป็นระบบ Mobile Banking (m-banking) หรือ การทำธุรกรรมการเงินทางธนาคารผ่านโทรศัพท์มือถือ โดยใช้งานผ่าน Mobile Application ที่มีการออกแบบให้ง่ายต่อการใช้งานและมีระบบความปลอดภัยมั่นคงที่สูงขึ้น ระบบ m-banking [1] ถูกพัฒนาให้มีความปลอดภัยมั่นคงมากขึ้นกว่าการใช้งานผ่านเว็บเบราว์เซอร์ เพราะระบบจะกำหนดค่าความปลอดภัยมั่นคงจากธนาคารที่พัฒนาแอปพลิเคชัน ซึ่งโปรแกรมที่เป็นแอปพลิเคชันบนสมาร์ทโฟน จะสามารถควบคุมกลไกความมั่นคงปลอดภัยได้ดีกว่าการเขียนโปรแกรมเพื่อรันผ่านเว็บเบราว์เซอร์ ตัวอย่างเช่น กลไกการบังคับใช้ HTTPS, การใช้ระบบ Personal Identity Number (PIN) Code, การใช้ระบบ One Time Password (OTP) เป็นต้น ซึ่งสามารถช่วยลดความผิดพลาดของผู้ใช้จากการกรอก URL ผ่านเว็บเบราว์เซอร์ ลดปัญหาการ Phishing Attack [2] อีกทั้งมีการเติบโตของเครือข่ายการให้บริการอินเทอร์เน็ตผ่านโทรศัพท์เคลื่อนที่ ได้ขยายจาก 3G ไปสู่ 4G ทำให้มีความเร็วในการรับส่งข้อมูลรวดเร็วขึ้นและระบบเหล่านี้ ยังมีการเข้ารหัสที่สามารถป้องกันการโจมตีด้วยวิธีแทรกกลางการสื่อสาร (Man In The Middle (MITM) Attack) ได้ดีกว่าการใช้ Wi-Fi อีกด้วย

จากงานวิจัยก่อนหน้านี้ [2-7] ได้มีการศึกษาปัญหาและทดสอบความปลอดภัยมั่นคงของระบบ i-banking พบว่ายังมีปัญหาคือ การใช้งานบนเว็บเบราว์เซอร์สามารถถูกดักจับบัญชีผู้ใช้และรหัสผ่านได้ โดยการโจมตีด้วยวิธีแทรกกลางการสื่อสาร และการจู่โจม HTTPS [2] เช่น SSL Sniff และ SSL Strip จากปัญหาดังกล่าวได้ส่งผลเสียต่อการทำธุรกรรมบนเว็บเบราว์เซอร์ระบบ i-banking นอกจากนี้ ยังมีงานวิจัยก่อนหน้านี้จำนวนหนึ่ง ที่ได้ทำการศึกษาความมั่นคงของระบบ m-banking ที่น่าจะมีความปลอดภัยมากกว่าระบบ i-banking แต่งานวิจัยเหล่านี้ ส่วนใหญ่ยังเป็นการศึกษาเฉพาะด้านความมั่นคง ซึ่งเน้นเทคนิควิธีแต่ยังไม่ได้ครอบคลุมถึงการวิจัยด้านความปลอดภัย ทั้งนี้ Schmeh [8] ได้ชี้ให้เห็นว่าความปลอดภัย ซึ่งเป็นด้านการบริหารจัดการ มีความสำคัญไม่น้อยกว่าด้านเทคนิควิธี ซึ่งเป็นด้านความมั่นคงและต้องมีการดูแลควบคู่กันไป

ดังนั้นในการศึกษาค้นคว้าอิสระนี้ จึงได้เสนอวิเคราะห์ทั้งด้านความปลอดภัยและความมั่นคงของระบบ m-banking ในกลุ่มลูกค้าบุคคล โดยใช้ธนาคารพาณิชย์ในประเทศไทย 6 แห่ง เป็นกรณีศึกษา โดยทำการสำรวจทั้งสองประเด็นคือ 1) ประเด็นด้านความปลอดภัย (Safety) คือการบริหารจัดการระบบ โดยทำการสังเกตการณ์ขบวนการเปิดบัญชี การสมัครใช้งานระบบ m-banking จนถึงการปิดบัญชี โดยอาศัยข้อมูลคดีความด้าน e-banking ที่เกิดขึ้นในประเทศไทย เป็นฐานในการวิเคราะห์ 2) ประเด็นด้านความมั่นคง (Security) จะเกี่ยวกับด้านเทคนิควิธี โดยทำการจำลองการโจมตีระบบ

m-banking เพื่อทดสอบความมั่นคงและช่องโหว่ในการใช้งานในฝั่งของผู้ใช้ รวมทั้งสำรวจผู้ให้บริการเครือข่าย และวิเคราะห์พฤติกรรมของผู้ใช้สมาร์ทโฟนที่อาจเสี่ยงต่อปัญหามัลแวร์ ซึ่งเป็นภัยคุกคามที่สำคัญบน Smartphone Application

1.2 วัตถุประสงค์

เพื่อวิเคราะห์ความปลอดภัยและความมั่นคงของระบบธนาคารผ่านโทรศัพท์มือถือ (Mobile Banking Systems) ของธนาคารพาณิชย์ไทยในกลุ่มลูกค้าส่วนบุคคล

1.3 ขอบเขตของการศึกษา

1) การศึกษาค้นคว้าอิสระนี้ มุ่งเน้นการสำรวจและวิเคราะห์ระบบ m-banking เป็นหลัก โดยไม่ได้เน้นที่ระบบ i-banking ที่มีการศึกษาจำนวนมากแล้ว โดยระบบ i-banking จะถูกกล่าวถึงเพื่อใช้ในการวิเคราะห์เปรียบเทียบกับระบบ m-banking เท่านั้น

2) กรณีศึกษาของระบบธนาคารผ่านโทรศัพท์มือถือ (Mobile Banking Systems) ของธนาคารพาณิชย์ในประเทศไทย โดยเลือกกลุ่มตัวอย่างของธนาคารจำนวน 6 ธนาคาร ดังนี้ (1) K-Mobile Banking PLUS ของธนาคารกสิกรไทย (2) KTB netbank ของธนาคารกรุงไทย (3) SCB Easy Net ของธนาคารไทยพาณิชย์ (4) TMB Touch ของธนาคารทหารไทย (5) Bualuang mbanking ของธนาคารกรุงเทพ (6) Krungsri Mobile ของธนาคารกรุงศรีอยุธยา เพื่อใช้เป็นกรณีศึกษาในครั้งนี้ โดยเลือกจากธนาคารที่ก่อตั้งในประเทศไทยที่มีระยะเวลายาวนานที่มีคนนิยมใช้มากที่สุด และเทียบกับข้อมูลเชิงสถิติของทีมงาน Topten Thailand [9] ซึ่งได้ทำการสำรวจธนาคารที่มีคนไทยใช้มากที่สุด

3) การวิเคราะห์ด้านความปลอดภัยระบบ (Safety) จะเป็นการวิเคราะห์ประเด็นด้านการจัดการ โดยทำการสังเกตการณ์ ขบวนการเปิดบัญชี การสมัครใช้งานระบบ m-banking จนถึงการปิดบัญชี โดยอาศัยข้อมูลคดีความทางด้าน e-banking ที่เกิดขึ้นในประเทศไทย เป็นฐานในการวิเคราะห์ รวมทั้งสำรวจผู้ให้บริการเครือข่าย

4) การวิเคราะห์ด้านความมั่นคง (Security) จะวิเคราะห์ในประเด็นด้านเทคนิค โดยทำการจำลองการโจมตีระบบ m-banking เพื่อทดสอบความมั่นคงและช่องโหว่ในการใช้งานในฝั่งผู้ใช้ โดยงานวิจัยนี้จะเลือกใช้เทคนิควิธีที่แฮกเกอร์นิยมใช้เจาะระบบมากที่สุด คือการโจมตีด้วยเทคนิควิธี SSL Sniff, SSL Strip รวมทั้งวิเคราะห์พฤติกรรมของผู้ใช้สมาร์ทโฟน เพื่อศึกษาพฤติกรรมที่ส่งผลต่อปัญหามัลแวร์ โดยประชากรคือ กลุ่มคนที่อาจเป็นลูกค้าของระบบ m-banking ซึ่งในงานวิจัยนี้ นิยามไว้เป็นกลุ่มผู้ใช้งานแอปพลิเคชันบนโทรศัพท์มือถือ ซึ่งจะมีความสามารถในการใช้ระบบ m-banking ได้ต่อไป และมีอายุ 15 ปีขึ้นไป ซึ่งเป็นอายุที่สามารถสมัครเปิดบัญชีธนาคารได้ การสุ่มตัวอย่าง ใช้วิธีการสุ่มอย่างง่าย โดยการใช้แบบสอบถามที่กรอกผ่านระบบออนไลน์ โดยได้มีผู้ตอบแบบสอบถามและมีคุณสมบัติใช้ได้ ทั้งหมด 481 คน

1.4 ความสำคัญของการศึกษา

1) เป็นแนวทางในการปรับปรุงและแก้ไขปัญหาระบบธนาคารผ่านโทรศัพท์มือถือ (m-banking) ในด้านความปลอดภัย (Safety) และความมั่นคง (Security) ของธนาคารพาณิชย์ในประเทศไทย

2) ผลที่ได้จากการวิเคราะห์จะเป็นประโยชน์ต่อหน่วยงานที่เกี่ยวข้อง ในการออกกฎระเบียบหรือนโยบายเกี่ยวกับการใช้งานของระบบ m-banking ต่อไปในอนาคต

1.5 นิยามศัพท์เฉพาะ

1) Mobile Banking (m-banking) หมายถึง การให้บริการทำธุรกรรมการเงินผ่านแอปพลิเคชัน บนอุปกรณ์สมาร์ทโฟน โดยทำธุรกรรมเกี่ยวกับการโอนเงิน เติมเงิน จ่ายเงิน เช็คยอดเงิน เป็นต้น

2) Internet Banking (i-banking) หมายถึง การให้บริการทำธุรกรรมทางการเงินผ่านเว็บเบราว์เซอร์ บนอุปกรณ์คอมพิวเตอร์ โดยทำธุรกรรมเกี่ยวกับการการโอนเงิน เติมเงิน จ่ายเงิน เช็คยอดเงิน เป็นต้น

3) ธนาคารพาณิชย์ในประเทศไทย หมายถึง ธนาคารที่ให้บริการเกี่ยวกับระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย โดยเลือกกรณีศึกษาเป็นระบบ m-banking ของ 6 ธนาคาร

4) ความมั่นคง (Security) หมายถึง การศึกษาความความมั่นคงของระบบธนาคารผ่านโทรศัพท์มือถือ ของธนาคารพาณิชย์ไทยในกลุ่มลูกค้าส่วนบุคคล

5) ความปลอดภัย (Safety) หมายถึง การศึกษาความปลอดภัยของระบบธนาคารผ่านโทรศัพท์มือถือ ของธนาคารพาณิชย์ไทยในกลุ่มลูกค้าส่วนบุคคล

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

เนื้อหาในบทนี้จะกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้องในการสำรวจและวิเคราะห์ความความปลอดภัยและความมั่นคงสำหรับระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย โดยมีรายละเอียดดังนี้

2.1 Mobile Banking vs. Internet Banking

Mobile Banking (m-banking) คือ การทำธุรกรรมบนโทรศัพท์มือถือ โดยใช้งานผ่านแอปพลิเคชัน [10] มีฟีเจอร์ต่างๆ ที่ใช้งานง่าย พกพาสะดวก ใช้งานได้ทุกที่และซอฟต์แวร์ของแอปพลิเคชันจะบังคับใช้โพรโทคอล HTTPS และเทคนิควิธีด้านความมั่นคงหลายอย่าง ซึ่งทำให้ระบบมีความมั่นคงมากขึ้น

Internet Banking (i-banking) คือ การทำธุรกรรมบนคอมพิวเตอร์หรืออุปกรณ์ โดยใช้งานผ่านเบราว์เซอร์ เพื่อเข้าถึง Web Application ที่ธนาคารพัฒนาขึ้นให้บริการ โดยในด้านความปลอดภัยมั่นคงของเบราว์เซอร์อาจจะไม่บังคับใช้ HTTPS (Hypertext Transfer Protocol Secure) เมื่อโดนโจมตี ผู้ใช้ต้องกรอกผ่าน URL เป็น https:// และสังเกตรูปกุญแจสีเขียว และต้องจำชื่อ URL ของธนาคาร ซึ่งหากกรอกข้อมูลผิดหรือไม่สังเกตอาจถูก Phishing หรือถูกแทรกกลางการสื่อสารไปสู่เว็บไซต์ปลอมได้

โดยทั่วไปธนาคารจะให้บริการระบบออนไลน์ (e-banking) ทั้ง 2 แบบคือระบบ i-banking และระบบ m-banking การพัฒนาระบบ m-banking จะรองรับการใช้งานบนสมาร์ทโฟนผ่านทางแอปพลิเคชัน ซึ่งสามารถทำงานได้รวดเร็วผ่านระบบ GPRS, EDGE, 3G, 4G หรือ Wi-Fi นอกจากนั้นยังมีการเข้ารหัส HTTPS เพื่อเพิ่มความปลอดภัยให้กับผู้ใช้บริการมากขึ้น และสมาร์ทโฟนยังมีระบบ Triple Lock Security [11] ซึ่งมีความมั่นคงกว่าระบบ i-banking โดยการตรวจสอบหลายชั้น ทั้งรหัสผ่าน รหัส OTP และเครื่องโทรศัพท์ รวมถึงเบอร์โทรศัพท์ผ่านเครือข่ายของผู้ให้บริการเครือข่าย

2.2 Safety vs. Security

ความหมายตามศัพท์บัญญัติราชบัณฑิตยสถาน [12] ของคำว่า Safety หมายถึง ความปลอดภัย ส่วน Security หมายถึง ความมั่นคง

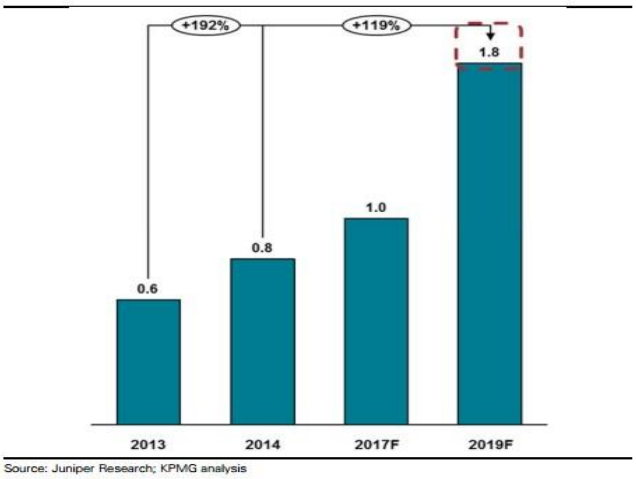
ความปลอดภัย (Safety) [8] หมายถึง กระบวนการบริหารจัดการเพื่อความปลอดภัยของระบบสารสนเทศ เช่น การออกกฎหมาย พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือกฎระเบียบที่ควบคุมการใช้งานระบบสารสนเทศต่างๆ รวมไปถึงการมีจรรยาบรรณชั้นความลับของข้อมูล ต่างก็เป็นเรื่องของการบริหารจัดการที่จะทำให้ระบบมีความปลอดภัยมากยิ่งขึ้น

ความมั่นคง (Security) หมายถึง เรื่องของเทคนิควิธีที่ทำให้ระบบคอมพิวเตอร์ปลอดภัย เช่น เทคนิคการเข้ารหัสและถอดรหัส เทคนิคการยืนยันตัวตนด้วยการลงลายมือชื่อดิจิทัล หรืออื่นๆ ที่เกี่ยวข้องกับเทคนิควิธี

Schmeh [8] ได้กล่าวว่า ความปลอดภัยและความมั่นคงมีความสำคัญเท่าเทียมกัน โดยจะขาดส่วนใดส่วนหนึ่งไม่ได้ ทั้งสองส่วนจะต้องได้รับการสนับสนุนให้ดีควบคู่กันไป ดังนั้นในการศึกษาค้นคว้าอิสระนี้จะทำการวิเคราะห์ระบบ m-banking ทั้งในด้านของความปลอดภัยและความมั่นคง

2.3 แนวโน้มของระบบธนาคารผ่านโทรศัพท์มือถือ

การใช้งานระบบธนาคารผ่านโทรศัพท์มือถือหรือ m-banking เป็นที่นิยมมากขึ้น ตามการขยายตัวของตลาดสมาร์ทโฟน ซึ่งทาง Juniper Research [13] คาดว่าจำนวนผู้ใช้งานระบบ m-banking จากปี ค.ศ. 2014 จะเพิ่มขึ้นถึง 1.8 พันล้านคน ภายในสิ้นปี ค.ศ. 2019 ดังรูปที่ 2.1 ในส่วนของประเทศไทยมีอัตราการเติบโตค่อนข้างสูงถึงร้อยละ 81.4 [14] โดยการทำธุรกรรมการชำระเงินผ่านระบบ m-banking มีการขยายตัวสูงขึ้นทั้งปริมาณและมูลค่าซึ่งสอดคล้องกับพฤติกรรมของผู้ใช้บริการที่ใช้อินเทอร์เน็ตและโทรศัพท์เคลื่อนที่ [15] อีกทั้งการพัฒนาฟังก์ชันต่างๆ ของโทรศัพท์เคลื่อนที่และเครือข่ายอินเทอร์เน็ตให้มีประสิทธิภาพมากขึ้น

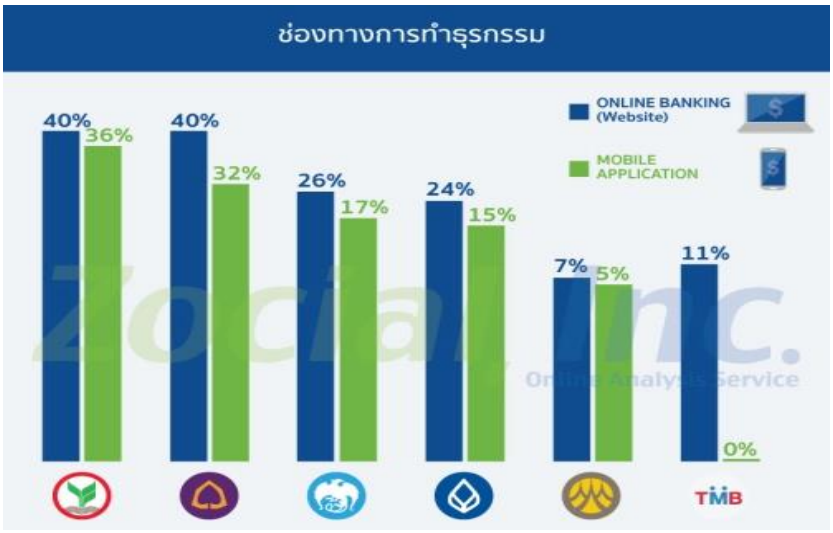


รูปที่ 2.1 Global mobile banking users
ที่มา : [13]

2.4 จำนวนผู้ใช้งานระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย

จากข้อมูลของธนาคารแห่งประเทศไทย (Use of Mobile Banking and Internet Banking) เมื่อเดือนธันวาคม ค.ศ. 2012 [16] ได้ระบุว่ามีบัญชีธนาคารในประเทศไทยจำนวน 6,645,161 บัญชีที่ใช้งานระบบ i-banking นอกจากนี้ยังเห็นจำนวนผู้ใช้บริการ m-banking เพิ่มขึ้นเป็น 864,312 บัญชี ซึ่งเพิ่มขึ้นมาจากจำนวน 688,178 บัญชีเมื่อเดือนมกราคม ค.ศ. 2012 จะเห็นได้ว่าธนาคารต่างๆ เริ่มพัฒนาระบบ Mobile Application มากขึ้นสามารถใช้งานได้งาน สะดวก รวดเร็วและมีความปลอดภัย

มั่นคงสูงขึ้นเพื่อตอบสนองความต้องการของลูกค้า นอกจากนั้นยังมีข้อมูลจากสถิติของ Zocial [17] ได้ทำการวิเคราะห์ข้อมูลเชิงลึกจากกลุ่มตัวอย่างทั้งหมด 1,050 คน ซึ่งสรุปจำนวนผู้ใช้บริการระบบธนาคารออนไลน์ผ่านเว็บไซต์และผ่านแอปพลิเคชัน ดังรูปที่ 2.2 พบว่าส่วนใหญ่ผู้ใช้บริการธุรกรรมการเงินแบบออนไลน์ โดยจะใช้ผ่านทางเว็บไซต์มากกว่าผ่านทางแอปพลิเคชันบนมือถือ จะเห็นได้ว่ามีผู้นิยมการใช้บริการระบบ m-banking มีอัตราการเพิ่มขึ้นเรื่อยๆ อย่างต่อเนื่อง การค้นคว้านี้จึงสนใจจะทำการสำรวจและวิเคราะห์ความปลอดภัยและความมั่นคงสำหรับระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย เพื่อหาช่องโหว่ของระบบ m-banking และเสนอแนวทางป้องกันและแก้ไขปัญหาต่างๆ ที่เกิดขึ้น

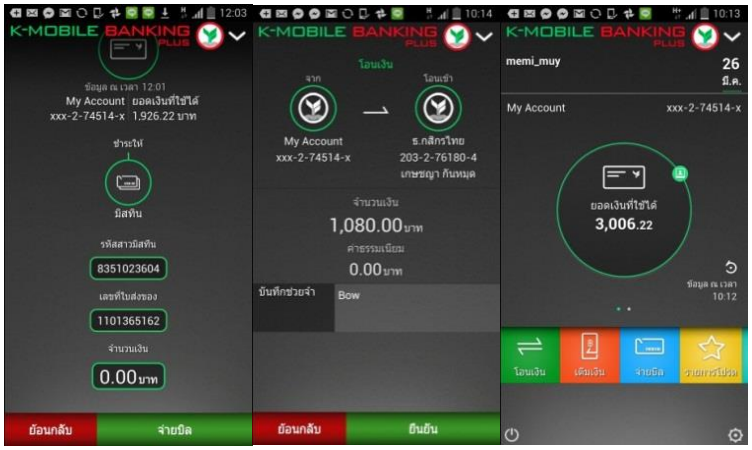


รูปที่ 2.2 สถิติเกี่ยวกับช่องทางการทำธุรกรรมทางออนไลน์ของธนาคารในประเทศไทย
ที่มา : [17]

2.5 ความเป็นมาของการทำธุรกรรมการเงินผ่านโทรศัพท์มือถือ

2.5.1 K-Mobile Banking ATM SIM: ธนาคารกสิกรไทย จำกัด (มหาชน)

การทำธุรกรรมการเงินผ่านโทรศัพท์มือถือ ถือกำเนิดครั้งแรกในปี พ.ศ. 2543 [18] โดยการร่วมมือกันระหว่างธนาคารกสิกรไทย และ DTAC พัฒนาการให้บริการธุรกรรมทางการเงินผ่านโทรศัพท์มือถือผ่านระบบ SMS เป็นสื่อกลาง เปิดให้บริการเฉพาะถามยอดบัญชีและโอนเงินระหว่างบัญชีของผู้ใช้บริการ จากแนวความคิดของเอทีเอ็มซิมที่มีความปลอดภัยสูง จึงทำให้ลูกค้าสนใจใช้บริการมากขึ้น ต่อมาในปี พ.ศ. 2551 มีการพัฒนาเทคโนโลยีระบบ m-banking ซึ่งคาดว่าจะเป็นที่นิยมในอนาคต จะเห็นได้ว่าการทำธุรกรรมทางการเงินผ่านสมาร์ทโฟนสามารถตอบโจทย์ที่ลูกค้าต้องการได้ ปัจจุบันธนาคารกสิกรไทยจึงได้พัฒนาระบบ m-banking ชื่อว่า K-Mobile Banking PLUS สามารถใช้งานได้ง่าย มีหน้าจอที่สวยงาม โดยมีจุดเด่นคือความปลอดภัยสูงสุดด้วยการเข้ารหัสความปลอดภัยจากซิมและไม่อนุญาตให้เชื่อมต่ออินเทอร์เน็ตผ่านเทคโนโลยี Wi-Fi ดังรูปที่ 2.3



รูปที่ 2.3 K-Mobile Banking PLUS

2.5.2 KTB Online Mobile: ธนาคารกรุงไทย จำกัด (มหาชน)

ธนาคารกรุงไทย จำกัด (มหาชน) [19] ได้เริ่มให้บริการการทำธุรกรรมการเงินผ่านโทรศัพท์มือถือตัวแรก ในกลางปี ค.ศ. 2008 คือ KTB Pocket Banking สำหรับมือถือ Java Phone หรือ J2ME ซึ่งผู้ใช้จะต้องทำการดาวน์โหลดแอปพลิเคชันมาติดตั้งลงบนมือถือ ซึ่งแอปพลิเคชันจะมีความรวดเร็วในการทำงาน และมีความปลอดภัยการใช้งานสูง จากนั้นในปี ค.ศ. 2009 ทางธนาคารได้เพิ่มช่องทางในการบริการโดยการพัฒนา KTB Online@Mobile ซึ่งรูปแบบการบริการจะใช้การทำงานผ่านเบราว์เซอร์บนมือถือจึงไม่ต้องยุ่งยากเรื่องการติดตั้ง แต่ผู้ใช้งานจะประสบปัญหาเรื่องความล่าช้าในการทำงาน หรือการไม่รองรับการทำงานของ SSL ที่เบราว์เซอร์ผ่านโทรศัพท์มือถือของผู้ใช้ และต่อมาทางธนาคารกรุงไทยได้พัฒนา KTB Online@Mobile ซึ่งเป็นเวอร์ชันที่รองรับการทำงานสำหรับผู้ใช้ i-Phone ปัจจุบันธนาคารกรุงไทย ได้พัฒนาแอปพลิเคชันเพื่อรองรับการใช้งานของสมาร์ทโฟนชื่อว่า KTB netbank ดังรูปที่ 2.4

รูปที่ 2.4 KTB netbank

2.5.3 SCB Mobile Banking: ธนาคารไทยพาณิชย์ จำกัด (มหาชน)

SCB Mobile Banking [20] สามารถใช้งานได้ง่าย ไม่ต้องเปลี่ยนซิมใหม่ สามารถใช้ได้กับทุกระบบ สามารถทำธุรกรรมได้ทันทีโดยไม่ต้องไปที่ธนาคาร สามารถใช้งานผ่านแอปพลิเคชันเพียงกรอก ชื่อผู้ใช้และรหัสผ่านเพื่อเข้ารหัสใช้งาน (End Clip Data) ธนาคารไทยพาณิชย์ จึงเลือกใช้วิธีการรักษาความปลอดภัยของข้อมูลเหมือนการให้บริการผ่านอินเทอร์เน็ตและใช้ GPRS, 3G, 4G และ Wi-Fi เป็นตัวเชื่อมต่อข้อมูลไปยังระบบของธนาคาร การทำธุรกรรมการเงินผ่านโทรศัพท์มือถือของธนาคารไทยพาณิชย์สามารถใช้งานได้ง่ายและสะดวกรวดเร็ว การดีไซน์รูปแบบหน้าตา เน้นเรียบง่าย แสดงฟีเจอร์ที่ตอบสนองการใช้งานที่จำเป็นเพื่อให้ผู้ใช้งานสะดวกและรวดเร็วในการใช้งานมากที่สุด ดังรูปที่ 2.5

รูปที่ 2.5 SCB Easy

2.5.4 TMB M-Banking: ธนาคารทหารไทย จำกัด (มหาชน)

TMB M-Banking [21] เป็นการทำธุรกรรมการเงินผ่านโทรศัพท์มือถือ เพื่อตอบสนองทุกไลฟ์สไตล์ของคนรุ่นใหม่ที่ไม่มีเวลาไปธนาคาร การเข้ามาทำตลาดของธนาคารทหารไทย เป็นช่องทางที่ช่วยสร้างภาพลักษณ์ให้กับธนาคารและเป็นการขยายฐานลูกค้าธนาคารไปยังกลุ่มคนทำงาน ซึ่งเป็นกลุ่มที่น่าจะใช้บริการนี้มากที่สุด ธนาคารทหารไทย จึงได้พัฒนาแอปพลิเคชัน TMB Touch เพื่อตอบสนองความต้องการของลูกค้า ซึ่งจะทำให้การทำธุรกรรมทางการเงินเป็นเรื่องง่าย พร้อมมีระบบรักษาความปลอดภัยที่สูงขึ้น เพื่อให้ลูกค้ามั่นใจในการใช้บริการทุกที่ทุกเวลาดังรูปที่ 2.6

รูปที่ 2.6 TMB Touch

2.5.5 Bualuang M-Banking: ธนาคารกรุงเทพ จำกัด (มหาชน)

ธนาคารกรุงเทพ [22] ได้มีการพัฒนาระบบการทำธุรกรรมการเงินผ่านโทรศัพท์มือถือสามารถใช้งานพื้นฐานได้และมีความมั่งคงความปลอดภัยสูง ธนาคารกรุงเทพเป็นยุคที่บุกเบิกเรื่องการพัฒนาระบบ i-banking ด้านความปลอดภัยในการใช้บริการบัวหลวงไอแบงก์กิ้ง ซึ่งจะมีความปลอดภัยในการใช้งาน โดยส่วนใหญ่เป็นการใช้งานบนคอมพิวเตอร์แบบตั้งโต๊ะ แต่ในปัจจุบันนำมาประยุกต์ใช้กับ Smartphone Application โดยมีระบบความปลอดภัยต่างๆ เช่น OTP, Mobile PIN เป็นต้น ซึ่งทำให้มีความปลอดภัยต่อการเข้าใช้งานมากขึ้น ดังรูปที่ 2.7

รูปที่ 2.7 Bualuang mbanking

2.5.6 Krungsri M-Banking: ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)

การทำธุรกรรมผ่านช่องทางอิเล็กทรอนิกส์มีการเติบโตมากขึ้น ธนาคารกรุงศรีอยุธยา [23] จึงพัฒนา Mobile Application ในการทำธุรกรรมบนสมาร์ทโฟน โดยการสร้างนวัตกรรมทางการเงินใหม่ๆ รวมถึงการสร้างความมั่นใจในการทำธุรกรรมผ่านช่องทางอิเล็กทรอนิกส์ ให้มีแนวโน้มการเติบโต

ที่เพิ่มสูงขึ้นอย่างต่อเนื่อง ธนาคารจึงได้ขยายบริการนี้ให้ลูกค้าใหม่ๆ ได้มีการใช้งานบนสมาร์ทโฟนหรือแท็ปเล็ต และยังคงระบบรักษาความปลอดภัยสูงสุด ดังรูปที่ 2.8

รูปที่ 2.8 Krungsri Mobile Application

ดังนั้นการทำธุรกรรมการเงินผ่านโทรศัพท์มือถือ ถือเป็นบริการที่เอื้อประโยชน์ทั้งผู้ให้บริการและผู้ใช้ เพราะสิ่งที่ลูกค้าได้รับคือ สามารถใช้บริการได้ทันทีแบบ Real-Time ซึ่งจะประหยัดค่าใช้จ่ายของการเดินทางไป-กลับ และลดค่าธรรมเนียมลงมาเทียบเท่ากับตู้ ATM ดีกว่าการเสียเวลาในเดินทางไปที่สาขาของธนาคาร หรือไปที่ตู้ ATM ซึ่งสามารถทำรายการโอนเงินหรือใช้เป็นช่องทางชำระเงินค่าสินค้าและบริการได้อย่างปลอดภัย อีกทั้งในส่วนของธนาคารและผู้ให้บริการโทรศัพท์มือถือต่างเห็นความสำคัญของการทำธุรกรรมการเงินผ่านโทรศัพท์มือถือเนื่องจากสาขาของธนาคารและตู้ ATM มีขั้นตอนการทำธุรกรรมหลายขั้นตอน จึงพัฒนาระบบ m-banking เพื่อเป็นช่องทางการใช้บริการของลูกค้าให้สามารถเข้าถึงบริการได้ง่ายยิ่งขึ้น การศึกษาค้นคว้าอิสระนี้จึงสนใจที่จะนำธนาคารทั้ง 6 ธนาคารเป็นกรณีศึกษา เพื่อวิเคราะห์ในด้านความปลอดภัยและความมั่นคงของการใช้บริการระบบธนาคารผ่านโทรศัพท์มือถือ

2.6 ระบบปฏิบัติการบนสมาร์ทโฟน

สมาร์ทโฟนเป็น Mobile Device ที่ได้รับความนิยมจากผู้ใช้งานมากที่สุดและคาดว่าในอนาคตจะมีการเติบโตเพิ่มขึ้นเรื่อยๆ เพราะมีระบบปฏิบัติการที่เป็น System Software ที่สามารถรองรับการใช้แอปพลิเคชันบนสมาร์ทโฟนและตอบสนองความต้องการของผู้ใช้งานในยุคไอทีได้ระบบปฏิบัติที่มีผู้นิยมใช้มากที่สุดคือ ระบบปฏิบัติการ iPhone OS และระบบปฏิบัติการ Android ซึ่งจะใช้ทดสอบในด้านความมั่นคงของระบบ m-banking ระบบปฏิบัติการ iPhone OS พัฒนาโดยบริษัท Apple เพื่อรองรับการทำงานของแอปพลิเคชันต่างๆ ของ iPhone [24] ซึ่งระบบ iOS สามารถเชื่อมต่อไปยัง Apps Store สำหรับการเข้าถึงแอปพลิเคชันที่สามารถใช้งานได้บนระบบปฏิบัติการ iOS หรือที่เรียกกันว่า iOS Application (iOS Apps) ในปัจจุบันได้มีการพัฒนา iOS Apps สำหรับใช้งานและอำนวยความสะดวกแก่ผู้ใช้ระบบ iOS อีกมากมาย ระบบปฏิบัติการ Android พัฒนาโดยบริษัท Google เป็นระบบปฏิบัติการล่าสุดที่ได้รับความนิยม รองรับการเชื่อมต่ออินเทอร์เน็ตแบบเรียลไทม์

เพื่อใช้บริการจากกูเกิ้ล จุดเด่นของระบบปฏิบัติการ Android เป็นแบบ Open Source ซึ่งทำให้มีการพัฒนาไปอย่างรวดเร็วและยังพบว่ามีระบบปฏิบัติการยังมีช่องโหว่ที่แฮกเกอร์สามารถขโมยข้อมูลได้

ตารางที่ 2.1 ส่วนแบ่งการตลาดของสมาร์ทโฟนทั่วโลก
ที่มา : [25]

Top Five Worldwide Tablet Vendors - Preliminary Results for the Second Quarter of 2015 (Shipments in millions)

Vendor	2Q15 Unit Shipments	2Q15 Market Share	2Q14 Unit Shipments	2Q14 Market Share	Year-Over-Year Growth
1. Apple	10.9	24.5%	13.3	27.7%	-17.9%
2. Samsung	7.6	17.0%	8.6	18.0%	-12.0%
3. Lenovo	2.5	5.7%	2.4	4.9%	6.8%
4. Huawei*	1.6	3.7%	0.8	1.7%	103.6%
4. LG Electronics*	1.6	3.6%	0.5	1.0%	246.4%
Others	20.4	45.6%	22.4	46.7%	-9.3%
Total	**44.7**	**100.0%**	**48.0**	**100.0%**	**-7.0%**

จากตารางที่ 2.1 ผลสำรวจล่าสุดของบริษัทพัฒนาและสำรวจข้อมูลทางไอที (IDC) เผยผลสำรวจส่วนแบ่งการตลาดของสมาร์ทโฟนทั่วโลกในไตรมาสที่ 2 ของ ค.ศ. 2015 พบว่าบริษัท Apple ยังครองแชมป์มีส่วนแบ่งทางการตลาดมากที่สุด ถึงแม้ยอดขายจะลดลงก็ตาม รองลงมาเป็นบริษัท Sumsung โดยการศึกษาค้นคว้าอิสระนี้ได้เลือกอุปกรณ์สมาร์ทโฟนของทั้ง 2 บริษัท ซึ่งเป็นสมาร์ทโฟนที่มีผู้นิยมใช้มากที่สุดเป็นเครื่องมือในการทดสอบระบบ m-banking ในด้านความมั่นคง

2.7 เทคโนโลยีที่เกี่ยวข้องในการใช้งานระบบ m-banking

โดยในการเชื่อมต่ออินเทอร์เน็ตของผู้ใช้งานสมาร์ทโฟนนั้น สามารถเชื่อมต่อผ่านเทคโนโลยีไร้สาย ปัจจุบันส่วนใหญ่ใช้เทคโนโลยี 3G [26] ในการส่งข้อมูลโดยใช้ชื่อว่า WCDMA (Wideband Code Division Multiple Access) เป็นเทคโนโลยี UMTS (Universal Mobile Telecommunication Systems) ซึ่งมีความเร็วค่อยข้างต่ำ สามารถรับส่งข้อมูลได้สูงสุดที่ความเร็ว 384 Kbps ต่อมาได้มีการพัฒนาต่อยอดขึ้นมาเป็น HSPA (High-Speed Packet Access) หรือ H ซึ่งทำให้มีความเร็วมากขึ้นอยู่ที่ประมาณ 2-7.2 Mbps จากนั้นก็ได้มีการพัฒนา HSPA เป็น HSPA+ หรือ H+ ซึ่งทำให้มีความเร็วอยู่ที่ 21-42 Mbps โดยการพัฒนา 3G ทำให้มีการใช้บริการมัลติมีเดียมากขึ้น มีการสื่อสารแบบเรียลทามมากขึ้น เพราะมีการรับส่งข้อมูลที่รวดเร็ว ต่อมาได้มีการพัฒนาขึ้นมาเป็น 4G [27] ใช้มาตรฐาน LTE (Long Term Evolution) โดยจะมีความเร็วมากกว่า 3G มีความสามารถในการส่งถ่ายข้อมูลและมัลติมีเดีย

สตรีมมิ่งที่ความเร็ว 100 Mbps และมีความเร็วสูงสุดถึง 1 Gbps ทำให้ตอบสนองการใช้งานผ่านอินเทอร์เน็ตไร้สายได้ดีขึ้น รับส่งข้อมูลได้รวดเร็ว จึงถูกนำมาใช้อย่างแพร่หลาย ทำให้สามารถใช้งานบนมาตรฐานเดียวกันทั่วโลก ในประเทศไทยมีผู้ให้บริการเครือข่ายหลายค่ายนำเทคโนโลยี 4G มาใช้ซึ่งเทคโนโลยีเหล่านี้ได้เข้ามาแทนที่ GPRS (General Packet Radio Service) และ EDGE (Enhanced Data rates for Global Evolution) ซึ่งในปัจจุบันไม่ค่อยนิยมใช้ เพราะมีความเร็วในการรับส่งข้อมูลต่ำและไม่สนับสนุนระบบโทรศัพท์ในปัจจุบัน นอกจากการเชื่อมต่ออินเทอร์เน็ตความเร็วสูงจากเทคโนโลยี 3G และ 4G แล้วยังสามารถเชื่อมต่อเทคโนโลยีแบบไร้สายผ่านระบบ LAN (Local Area Network) ทำให้สามารถเชื่อมต่ออินเตอร์เน็ตด้วยความเร็วสูงได้ผ่านทางโทรศัพท์มือถือ โดยใช้ Wi-Fi (Wireless Fidelity) ปัจจุบันมีการใช้งานเพิ่มมากขึ้น มีทั้งจุดให้บริการฟรีและเสียค่าบริการ เกือบทุกสถานที่ ทำให้มีผู้คนนิยมใช้งานมากขึ้น ซึ่ง Wi-Fi [28] มีมาตรฐานกลางในการควบคุมการทำงาน ซึ่งที่นิยมใช้มี 2 มาตรฐาน ได้แก่ 802.11g, 802.11n และมีมาตรฐานใหม่คือ 802.11ac ที่ถูกพัฒนาขึ้นมาโดยเพิ่มประสิทธิภาพในการใช้งาน ทำให้มีความเร็วเพิ่มขึ้น สามารถส่งได้ในระยะไกลและสามารถทะลุผ่านสิ่งกีดขวางได้ดี

จะเห็นได้ว่าการใช้งานผ่านเทคโนโลยี 3G และ 4G มีความปลอดภัยสูงกว่าเทคโนโลยี Wi-Fi เพราะมีข่าวที่เกิดขึ้นในปัจจุบัน โดยมีผู้ไม่หวังดีแอบแฝงมากับจุดเชื่อมต่อของ Wi-Fi เพราะคุณลักษณะทางกายภาพของการใช้งานเครือข่ายไร้สายที่เป็นการเชื่อมต่อสัญญาณผ่านตัวกลางที่เป็นคลื่นวิทยุ ซึ่งไม่สามารถระบุได้ว่ามีใครบ้างที่กำลังทำอะไรกับเครือข่ายไร้สาย ซึ่งแฮกเกอร์นิยมอาศัยช่องโหว่นี้ในการดักจับข้อมูล เช่น กรณีของธนาคารกสิกรไทย ไม่อนุญาตให้ระบบ m-banking เชื่อมต่ออินเทอร์เน็ตผ่าน Wi-Fi ได้ โดยลูกค้าจะต้องเชื่อมต่อผ่าน 3G และ 4G เท่านั้น เพื่อป้องกันการโจมตีด้วยวิธีแทรกกลางการสื่อสาร ทำให้ลดช่องทางการใช้บริการของลูกค้ากลุ่มที่ใช้ Wi-Fi จุดนี้จึงเป็นประเด็นที่น่าสนใจที่จะนำมาวิเคราะห์ในด้านความมั่นคง (Security) ระบบ m-banking

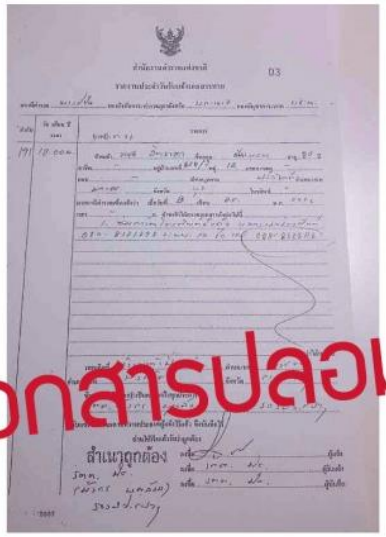
2.8 ภัยคุกคามการใช้งานระบบธนาคารบนโทรศัพท์มือถือในปัจจุบัน

2.8.1 วิเคราะห์ปัญหา Social Engineering

Social Engineering [29] คือ วิธีการโจมตีแบบวิศวกรรมสังคม หรือการใช้วิธีทางจิตวิทยาหลอกลวงเหยื่อเพื่อโจมตีระบบ สำหรับการโจมตีระบบ e-banking ได้มีการใช้เทคนิควิธีนี้ จนปรากฏเป็นคดีมากมาย ตัวอย่างเช่นคดีของคุณบุณพจน์ พราหมนก [30] เมื่อปี พ.ศ. 2557 มิจฉาชีพได้สร้างหลักฐานปลอมเพื่อขอสมัครเปิดบัญชีธนาคารที่มีชื่อเดียวกันกับเหยื่อ ปลอมเอกสารแจ้งความมือถือหายและปลอมสำเนาใบขับขี่ ดังรูปที่ 2.9 เพื่อใช้ในการขอออกซิมใหม่ แต่คุณบุณพจน์ พราหมนก ได้มีการป้องกันโดยแจ้งศูนย์บริการไว้ หากมีการแจ้งซิมหายจะต้องแจ้งรหัส 4 ตัวกับเจ้าหน้าที่ก่อน จึงจะสามารถออกซิมใหม่ได้ แต่มิจฉาชีพได้แจ้งซิมหายที่สาขาย่อยของศูนย์บริการ ซึ่งคาดว่าสาขาย่อยนั้น ยังไม่ได้รับแจ้งข้อมูลของการบอกรหัส 4 ตัว จึงออกซิมใหม่เบอร์เดิมให้มิจฉาชีพ

จากนั้นมิจฉาชีพก็ทำการเข้าระบบ i-banking โดยใส่ชื่อผู้ใช้ของคุณบุณพจน์ แล้วก็ทำเป็นแจ้งลืมรหัสผ่านเพื่อให้ธนาคารส่งหมายเลข SMS OTP มาทางโทรศัพท์มือถือ แล้วทำการเปลี่ยนรหัสผ่านใหม่และเข้าระบบ i-banking สั่งโอนเงินออกได้เหมือนกับเป็นเจ้าของตัวจริง จากปัญหาดังกล่าวพบว่าผู้ให้บริการเครือข่ายไม่มีมาตรการที่เป็นแนวทางเดียวกันในการขอออกซิมใหม่ของแต่ละ

ค่าย และแต่ละสาขา จึงมีจุดอ่อนที่เป็นช่องโหว่ทำให้มิจฉาชีพใช้วิธีการดังกล่าวในการแอบสวมรอยปลอมเอกสาร ซึ่งงานวิจัยนี้จะได้ทำการวิเคราะห์ในส่วนนี้ รวมถึงคดีอื่นๆ ที่อาศัยวิธีการโจมตีแบบวิศวกรรมสังคมเพื่อใช้ในการทดสอบด้านความปลอดภัยของระบบที่เกี่ยวข้องกับระบบ m-banking ต่อไป



รูปที่ 2.9 The Faked Document
ที่มา : [30]

ซึ่งกรณีดังกล่าวมิจฉาชีพอาศัยช่องโหว่ของกระบวนการหลายจุด และ SMS OTP ที่ธนาคารส่งมาให้กับลูกค้า ซึ่งเป็นการรักษาความปลอดภัยอีกชั้นแต่ก็ไม่ปลอดภัยเสมอไป เพราะคนร้ายสามารถหาวิธีเพื่อให้ได้มาซึ่ง SMS OTP ดังนั้นธนาคารต่างๆ ควรใช้ Hard Token ในการรับรหัสสำหรับการทำธุรกรรมบนระบบ i-banking แทนการส่งทาง SMS เหมือนกับธนาคารในต่างประเทศ ซึ่งอาจจะแก้ปัญหาช่องโหว่เหล่านี้ได้ ปัญหาดังกล่าวเกิดจากการทำงานที่บกพร่องของเจ้าหน้าที่และบริษัทผู้ให้บริการเครือข่าย ไม่มีมาตรการเกี่ยวกับการตรวจสอบเอกสารที่เป็นมาตรฐานเดียวกันและระบบการบันทึกข้อมูลของผู้ใช้บริการ ควรมีระบบออนไลน์ซึ่งสามารถเปิดดูได้ทันที ซึ่งในอนาคตในการขอออกซิมใหม่เบอร์เดิมหรือการเปลี่ยนซิมนั้นอาจจะมีระบบยืนยันตัวตนแบบแสกนนิ้วมือเพิ่ม ถึงแม้ว่าจะมีการป้องกัน 2 ชั้นจากการเข้ารหัส OTP ก็ไม่ปลอดภัยเสมอไป ดังนั้นจึงเป็นประเด็นที่น่าสนใจที่จะนำมาวิเคราะห์ในด้านความปลอดภัยของระบบ m-banking ของผู้ให้บริการเครือข่าย

2.8.2 วิเคราะห์ปัญหา SMS Spoofing

จากกรณีที่มีผู้ถูกขโมยเงินในบัญชี โดยภายหลังจากที่ตรวจพบว่า ในเครื่องของผู้เสียหายมีโปรแกรมประเภทโทรจันแอบแฝงทำหน้าที่ส่งข้อมูลความลับ รหัสต่างๆ ไปให้คนร้าย ซึ่งติดตั้งอยู่ในเครื่องโดยที่เจ้าของบัญชีไม่รู้ตัว บางรายสูญเงินหลายแสนบาท จากกรณีดังกล่าว อาจารย์ปริญญา หอมเอนก ผู้เชี่ยวชาญด้านความปลอดภัยสารสนเทศ และประธานบริษัท ACIS Professional Center [31] ได้อธิบายว่า คนร้ายใช้วิธีส่ง SMS เข้าเครื่องของเหยื่อ โดยแสดงเบอร์ผู้ส่ง เป็นเบอร์คอลเซ็นเตอร์ของธนาคาร ซึ่งแท้ที่จริงแล้ว ปัจจุบันมีโปรแกรมที่สามารถทำให้ส่ง SMS โดยระบุเบอร์ผู้ส่งเป็นเบอร์อะไรก็

ได้ โดยเฉพาะบนระบบปฏิบัติการ Android ที่มีแอปพลิเคชันเปลี่ยนเบอร์ผู้ส่งได้ด้วย จากนั้นคนร้ายก็ใช้วิธีส่ง SMS ปลอมเป็นเบอร์ธนาคาร พร้อมกับแนบ link ให้ Click เมื่อคลิกแล้ว จะทำการติดตั้งโปรแกรมประเภท โทรจันในมือถือของเหยื่อ ซึ่งตรงนี้มีจุดสังเกตสำคัญว่าไม่ใช่ URL ของธนาคาร โดเมนต้องอ่านจากข้างหลัง ซึ่งตัวอย่างนี้คือ k-cyberbank.info ซึ่งไม่เกี่ยวกับธนาคารและไม่ใช่ที่อยู่ของเว็บธนาคารและไม่มีเครื่องหมายแม่กุญแจซึ่งจะไม่ปลอดภัยหาก Login เมื่อเทียบกับ โดเมนจริงของเว็บธนาคาร ถ้าหากคลิกลิงค์ไฟล์ .APK ดังรูปที่ 2.10 เมื่อติดตั้งเสร็จโปรแกรมจะเปิดหน้าต่างให้ใส่ชื่อผู้ใช้และรหัสผ่านในระบบ i-banking ของเหยื่อ ซึ่งในขั้นตอนนี้ชื่อผู้ใช้และรหัสผ่านที่เหยื่อกรอกจะถูกส่งไปให้คนร้ายได้ซึ่งวิธีการนี้คือการ Phishing Attack และทางธนาคารจะปฏิเสธการรับผิดชอบเพราะความผิดพลาดเกิดจากผู้ใช้ ถึงแม้ว่าคนร้ายจะได้ผู้ใช้และรหัสผ่าน แต่การทำธุรกรรมทางธนาคารจะต้องใช้รหัส SMS OTP เพื่อยืนยันตัวตนอีกขั้น โปรแกรมโทรจันจะรอดักจับ SMS OTP ส่งต่อไปให้กับคนร้าย จึงทำให้เจ้าของตัวจริงที่รอ SMS OTP จากธนาคาร แต่ไม่ได้รับข้อความ ดังนั้นคนร้ายจึงสั่งโอนเงินได้เหมือนกับเป็นเจ้าของตัวจริง จากการสืบค้นทราบว่าหนึ่งในกรณีที่เกิดขึ้นมาแล้ว SMS ที่ส่งเข้ามาในเครื่องของผู้เสียหาย ถูกส่งต่อไปที่รัสเซียและมีการสั่งให้โอนเงินจากบัญชีของเหยื่อ เข้าบัญชีบุคคลหนึ่งในประเทศไทย และเงินจำนวนนี้ก็ถูกโอนต่อไปยังต่างประเทศทันที ซึ่งโทรจันลักษณะนี้ก็ยังสามารถแฝงตัวมากับแอปพลิเคชันอื่นๆ ได้อีกด้วย จึงควรดาวน์โหลดจาก Play Store, Apple App Store ก็ยังมีโอกาสเจอแอปพลิเคชันแฝงโทรจัน ที่มาคอยแอบส่งข้อมูลบนมือถือของเหยื่อไปให้คนร้ายได้เช่นกัน นอกจากจะดาวน์โหลดจากแหล่งที่น่าเชื่อถือแล้ว ยังต้องสังเกตการณ์ขอสิทธิ์และชื่อผู้พัฒนาด้วย ซึ่งจะนำไปวิเคราะห์พฤติกรรมผู้ใช้งานสมาร์ทโฟนที่ส่งผลต่อปัญหามัลแวร์

รูปที่ 2.10 เอสเอ็มเอสปลอม
ที่มา : [31]

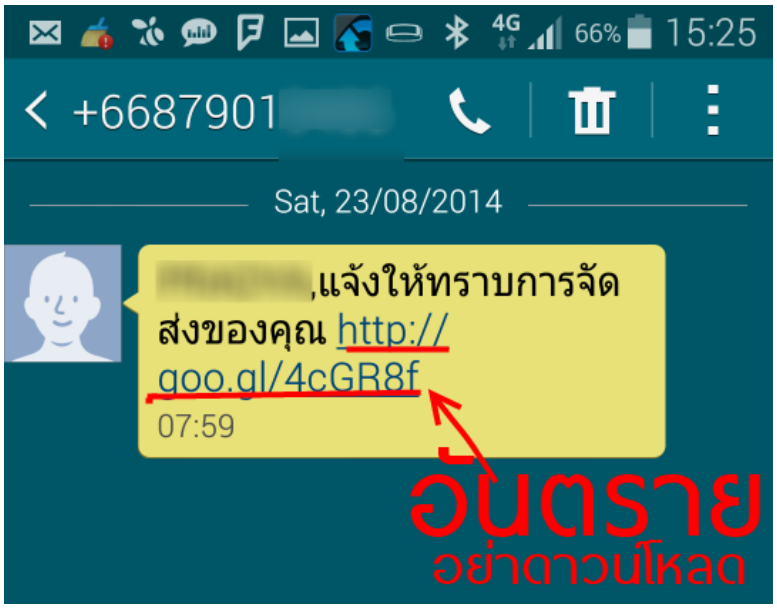
2.8.3 การโจมตีด้วย Mobile Phone Trojans

Mobile phone Trojans [7] เป็นมัลแวร์ที่ออกแบบมาเพื่อขัดขวาง SMS OTP ตัวอย่าง เช่น The ZITMO (Zeus In the mobile) Trojans ซึ่งทำงานบนระบบปฏิบัติการ Symbian โดย จะ

ร้องขอ SMS ผ่านทางเครือข่ายได้เอง ซึ่งเมื่อได้รับข้อความแล้วยังส่งต่อข้อความและลบ SMS ในเครื่องได้และต่อมาได้มีการตรวจพบมัลแวร์ตัวนี้ในระบบปฏิบัติการอื่น เช่น Window และ Android อีกด้วย

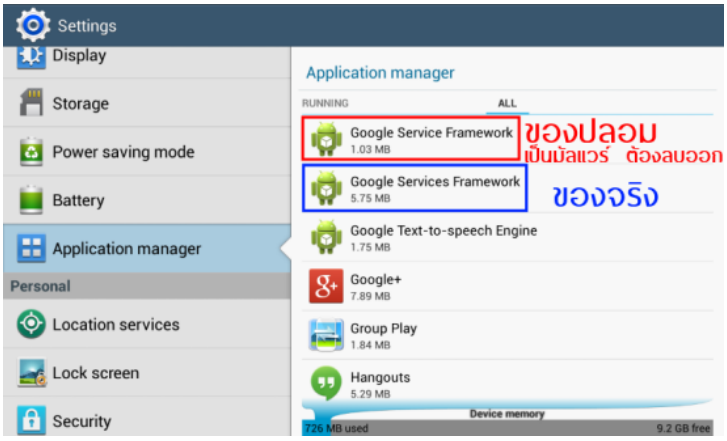
2.8.4 เตือนผู้ใช้ Android อย่าโหลดลิงค์ APK ใน SMS

Thaicert ประกาศเตือนถึงผู้ใช้ Android [32] หลังทีมงาน ได้รับข้อความลักษณะนี้คือ “ (ชื่อเรา), แจ้งให้ทราบการจัดส่งของคุณ (ลิงค์ดาวน์โหลด)” ดังรูปที่ 2.11 ในข้อความ SMS ซึ่งลิงค์นั้นเป็นลิงค์เข้าสู่การดาวน์โหลดไฟล์ APK ที่มีมัลแวร์แอบแฝง ซึ่งทางหน่วยงานด้านความปลอดภัย Thaicert ได้ให้รายละเอียดในเว็บไซต์ว่าไฟล์ลิงค์ใน SMS นั้น จากการตรวจสอบข้อมูลไฟล์ .APK ดังกล่าวโดยใช้เว็บไซต์ Virustotal พบว่าเป็นโทรจันที่มีความสามารถในการขโมยข้อมูล SMS เป็นหลัก ซึ่งมีลักษณะที่คล้ายกับมัลแวร์ที่มีเป้าหมายเพื่อโจมตีผู้ใช้งานระบบธุรกรรมออนไลน์ต่างๆ เช่น e-banking ด้วยการขโมย SMS มาใช้ในการทำธุรกรรมออนไลน์ และเมื่อมีการนำไฟล์มัลแวร์ทั้งหมดมาทำการ Decompile พบว่าซอร์สโค้ดของไฟล์มัลแวร์ แจ้ง .APK และ ไฟล์มัลแวร์ รับทราบ .APK มีการทำงานเหมือนกันทุกประการ เพียงเปลี่ยนชื่อไฟล์ให้ไม่เหมือนกันเท่านั้น โดยมัลแวร์ตัวที่ว่านี้จะอ่านรายชื่อเบอร์โทรศัพท์ อ่าน แก้ไข และรับส่งข้อความ SMS รวมถึงเชื่อมต่ออินเทอร์เน็ตโดยหลักการทำงานของไฟล์ APK ใน SMS อันตรายนี้ หากติดตั้งลงในเครื่อง แอปพลิเคชันจะลักลอบส่ง SMS ออกไปยังหมายเลขโทรศัพท์อื่นๆ ที่ถูกบันทึกอยู่ในเครื่อง เพื่อแพร่กระจายมัลแวร์ไปยังผู้ใช้รายอื่นๆ และสามารถขโมยข้อมูลหรือทำให้ผู้ที่ติดตั้งแอปพลิเคชันดังกล่าวเสียเงินค่าส่ง SMS เป็นจำนวนมากได้ นอกจากนี้ ไฟล์ .APK อันตรายใน SMS นี้ยังมีการร้องขอสิทธิ์ Device Administration ในการล็อกหน้าจอ ซึ่งอาจมีจุดประสงค์ที่ไม่ดีอื่นๆ ด้วย โดยการออกแบบครั้งนี้หวังโจมตีเหยื่อที่หลงเชื่อข้อความ SMS บนระบบปฏิบัติการ Android เพราะ ไฟล์ APK รันได้เฉพาะ Android เท่านั้น



รูปที่ 2.11 เอสเอ็มเอสที่แฝงไฟล์มัลแวร์บนระบบปฏิบัติการแอนดรอยด์
ที่มา : [32]

หากติดตั้ง APK ลงเครื่องแล้ว แอปพลิเคชันอันตรายนี้จะใช้ชื่อว่า Google Service Framework ซึ่งตั้งชื่อคล้ายคลึงกับแอปพลิเคชันจริงที่ชื่อว่า Google Services Framework ให้สังเกตของจริงต้องมี s ต่อท้าย Service ดังรูปที่ 2.12 ดังนั้นสำหรับผู้ใช้งานที่ติดตั้งแอปพลิเคชันดังกล่าว ให้รีบถอนการติดตั้งแอปพลิเคชันตามขั้นตอนปกติทั้งนี้ผู้ใช้สมาร์ทโฟนหากเจอข้อความแปลกๆ พร้อมลิงค์อย่าคลิกลิงค์เด็ดขาดและควรตรวจสอบด้วยการติดตั้งซอฟต์แวร์ Antivirus บนมือถือ เพื่อความปลอดภัยต่อข้อมูลบนสมาร์ทโฟน จากกรณีดังกล่าวจึงสนใจนำมาวิเคราะห์พฤติกรรมผู้ใช้งานสมาร์ทโฟนที่ส่งผลต่อปัญหามัลแวร์



รูปที่ 2.12 แอปพลิเคชันจริงและปลอมของ Google Services Framework
ที่มา : [32]

2.8.5 ลักษณะ SMS delay

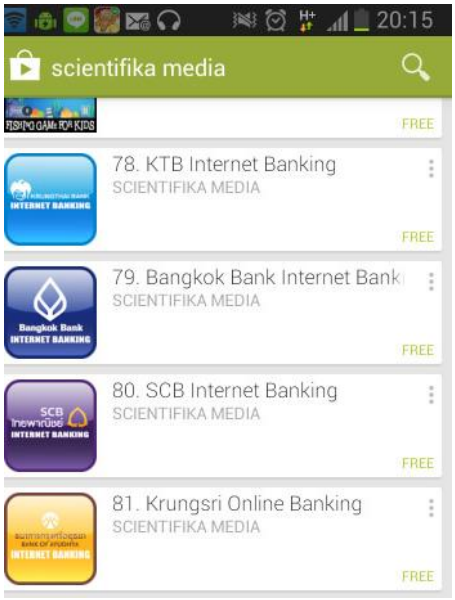
SMS delay [7] คือการที่ SMS เดินทางมาถึงโทรศัพท์ล่าช้า ตัวอย่างเช่น ในประเทศไทยได้เกิดขึ้นเมื่อวันที่ 27 ตุลาคม พ.ศ. 2558 โดยที่ผู้ให้บริการเครือข่าย True และ AIS ระบบล่มทำให้เกิด SMS Delay ซึ่งทำให้ผู้ที่ทำธุรกรรมระบบ i-banking และระบบ m-banking ของธนาคารไทยพาณิชย์และธนาคารทหารไทย ได้รับ SMS ล่าช้า ทั้งนี้อาจขึ้นอยู่กับผู้ให้บริการโทรศัพท์ หรือปัจจัยอื่นๆ ซึ่งธนาคารต่างๆ ควรให้ SMS ถึงผู้ใช้บริการภายใน 5 นาที ซึ่งถ้าข้อความไปถึงช้ากว่าเวลาที่กำหนดก็จะส่งผลต่อการทำธุรกรรม คือจะต้องดำเนินกระบวนการใหม่อีกครั้งหรือมีการดักจับขโมยข้อมูล จะเห็นว่าปัญหาดังกล่าวเกิดจากผู้ให้บริการเครือข่าย ดังนั้นผู้ใช้งานควรระมัดระวังการติดตั้งโปรแกรมที่ดาวน์โหลดมาจากแหล่งที่ไม่น่าไว้ใจและอาจหลีกเลี่ยงการทำธุรกรรมในช่วงเวลาที่มีผู้ใช้งานเครือข่ายโทรศัพท์หนาแน่นเพื่อลดปัญหาการล่าช้าในการส่งข้อมูลได้

2.8.6 วิเคราะห์ปัญหามัลแวร์

จากกรณีข่าวที่เกิดขึ้นเมื่อวันที่ 26 มีนาคม พ.ศ. 2557 [33] ธนาคารพาณิชย์ต่างๆ ได้ประกาศเตือนประชาชน ซึ่งพบว่าในขณะนี้ได้มีแอปพลิเคชันธนาคารปลอมเกลื่อนบน Play Store โดยแอปพลิเคชันดังกล่าว ไม่ได้พัฒนาจากทางธนาคาร โดยได้แจ้งไปยัง Google ให้ถอดแอปพลิเคชันปลอมออกจาก Play Store และก่อนดาวน์โหลดให้สังเกตชื่อของธนาคารผู้พัฒนา เช่น ธนาคารกรุงไทย ชื่อผู้พัฒนาคือ Krung Thai Bank PCL. ดังรูปที่ 2.13

รูปที่ 2.13 แจ้งเตือนวิธีการโหลดแอปพลิเคชันให้ปลอดภัย

ดังนั้นผู้ใช้งานควรสังเกตชื่อนักพัฒนาจะต้องเป็นชื่อธนาคารนั้นๆ ไม่ใช่ชื่อนักพัฒนารายอื่นอย่างเช่น Scientifika Media ซึ่งเป็นแอปพลิเคชันปลอม ดังรูปที่ 2.14 ดังนั้นหากพบแอปพลิเคชันที่พัฒนาโดยไม่ใช่ชื่อธนาคาร เพราะอาจนำไปสู่ภัยอันตรายบนมือถือ ซึ่งจะมีมัลแวร์แอบแฝงเพื่อขโมยข้อมูลในเครื่องสมาร์ทโฟน จากปัญหาดังกล่าวจะนำไปวิเคราะห์ในด้านการสำรวจพฤติกรรมผู้ใช้งานสมาร์ทโฟนที่ส่งผลต่อปัญหามัลแวร์



รูปที่ 2.14 Faked Mobile Banking Applications by Scientifika Media
ที่มา : [33]

จากข้อมูลดังกล่าวจึงเป็นประเด็นที่น่าสนใจที่จะใช้วิเคราะห์ด้านความปลอดภัย (Safety) ของการใช้สมาร์ทโฟนในการทำธุรกรรมผ่านระบบ m-banking โดยนำมาใช้ตรวจสอบธนาคารไทยพาณิชย์ต่างๆ ที่มีแอปพลิเคชันให้ดาวน์โหลด ว่ามีลักษณะและวิธีป้องกันด้านความปลอดภัยจากการใช้งานอย่างไรบ้าง

2.8.7 ช่องโหว่ของซิมการ์ดที่ทำให้ผู้ไม่ประสงค์ดีสามารถสำเนาซิมการ์ดได้โดยง่าย

ซิมการ์ด หรือ SIM (Subscriber Identity Module) [34] เป็นอุปกรณ์ที่นำมาใส่ในโทรศัพท์มือถือ เพื่อให้เครื่องโทรศัพท์สามารถติดต่อและใช้ในการระบุตัวตนกับผู้ให้บริการเครือข่ายโทรศัพท์ โดยซิมการ์ดนั้นจะมีหมายเลข IMSI (International Mobile Subscriber Identity) ที่จะไม่ซ้ำกันและผู้ให้บริการเครือข่ายโทรศัพท์จะนำหมายเลข IMSI นี้ไปผูกกับหมายเลขโทรศัพท์ โดยข้อมูลจะถูกเก็บที่ HLR (Home Location Register) ของผู้ใช้บริการ โดยทั่วไปซิมการ์ดจะมีระบบป้องกันการถูกสำเนา เนื่องจากซิมการ์ดสามารถใช้ในการติดต่อสื่อสารและใช้ในการระบุตัวตนกับผู้ให้บริการเครือข่ายแล้วยังสามารถการเก็บข้อมูลที่สำคัญต่างๆ เช่น ข้อมูลส่วนตัวของผู้ใช้งานรหัส PIN (Personal Identification Number) และ PUK (PIN Unlock Key) โดยรหัสที่ใช้ในการป้องกันสำเนาดังกล่าวเรียกว่า ค่า Ki ซึ่งโดยปกติแล้วไม่สามารถเข้าถึงค่านี้ได้ ซึ่ง Karsten Nohl [35] ผู้ก่อตั้ง Security Research Labs จากประเทศเยอรมัน โดยได้ค้นพบจุดอ่อนของการเข้ารหัสข้อมูลบนซิมการ์ด และจุดอ่อนของซอฟต์แวร์ที่ใช้งานร่วมกับซิมการ์ดที่มีปัญหา ซึ่งการสำเนาซิมการ์ดนั้นสามารถทำได้โดยง่าย ผู้ไม่ประสงค์ดีสามารถทำการส่ง SMS ที่มีชุดคำสั่งในการสำเนาไปยังเครื่องโทรศัพท์ปลายทาง ก็จะสามารถสำเนาซิมการ์ดได้ จากการทดลองเมื่อปี พ.ศ. 2556 ของ Karsten Nohl กับซิมการ์ดเกือบ 1,000 อัน พบว่าสามารถทำการสำเนาได้ โดยซิมการ์ดเหล่านั้นเป็นซิมการ์ดที่มีการเข้ารหัสด้วย DES (Data Encryption Standard) ซึ่งเป็นการเข้ารหัสที่ล้าสมัยและถูกแกะรหัสได้ ผลกระทบของจุดอ่อนข้างต้นคือ ผู้ไม่ประสงค์ดีสามารถทำการสำเนาซิมการ์ด และนำไปใช้ในการดำเนินการก่ออาชญากรรมทางการเงิน ใช้ในการโทรและส่งข้อความสั้นโดยแอบอ้างความเป็นเจ้าของโทรศัพท์ได้ สำหรับการป้องกันในเบื้องต้นคือ ทำการเปลี่ยนซิมการ์ดใหม่ที่ใช้เทคโนโลยีเข้ารหัสที่ทันสมัย หรือปรับปรุงรุ่นของซอฟต์แวร์ที่ใช้งานร่วมกับซิมการ์ด หรือทำการกรองและป้องกันข้อความสั้นแปลกปลอมในอุปกรณ์หรือระดับเครือข่าย

ซึ่งจากกรณีดังกล่าวทำให้ผู้ให้บริการเครือข่าย เข้มงวดกับมาตรการป้องกันและแก้ไขปัญหาซึ่งผู้ให้บริการเครือข่ายควรมีมาตรการที่เป็นแนวทางเดียวกัน มีการตรวจสอบข้อมูลเพื่อยืนยันตัวตนที่แท้จริง จากกรณีดังกล่าวผู้วิจัยจึงนำมาใช้เป็นเกณฑ์ในการวิเคราะห์ด้านความปลอดภัย (Safety) ของการออกซิมการ์ดใหม่ของผู้ให้บริการเครือข่าย

2.8.8 Masque Attack ภัยคุกคามใหม่บน iPhone และ iPad

FireEye [36] บริษัทผู้นำทางด้านการป้องกันภัยคุกคามขั้นสูงบนโลกไซเบอร์ ได้ออกมาเปิดเผยถึงช่องโหว่อันตรายใหม่ล่าสุดบน Apple iOS เรียกว่า “Masque Attack” ช่วยให้แฮกเกอร์สามารถติดตั้งแอปพลิเคชันปลอมบน iPhone และ iPad เพื่อขโมยข้อมูลอีเมล์และ SMS ได้ทันที ซึ่งรัฐบาลสหรัฐอเมริกาได้ออกมาประกาศเตือนถึงภัยคุกคามของช่องโหว่ Masque Attack เป็นช่องโหว่ที่ช่วยให้แฮกเกอร์สามารถติดตั้งมัลแวร์ในรูปของแอปพลิเคชันปลอมได้ ระบบที่ได้รับผลกระทบอุปกรณ์ Apple iOS ที่ใช้ระบบปฏิบัติการ iOS 7.1.1, 7.1.2, 8.0, 8.1 และ 8.1.1 beta ขั้นตอนการโจมตีดังกล่าวแฮกเกอร์ใช้วิธีส่ง URL ให้ติดตั้งเกมส์ “Flappy Bird” ซึ่งเป็นเวอร์ชันใหม่ของ iPhone หรือ iPad เมื่อเหยื่อกด URL ดังกล่าวนั้น มัลแวร์ในรูปของแอปพลิเคชัน “Gmail” ปลอมจะถูกดาวน์โหลดมาติดตั้งแทน ทำให้มัลแวร์สามารถปลอมตัวเองในรูปของแอปพลิเคชัน Gmail เพื่อขโมยชื่อผู้ใช้และรหัสผ่านของอีเมล์ โดยอีเมล์ทั้งหมดจะถูกอัพโหลดขึ้นเซิร์ฟเวอร์ของแฮกเกอร์โดยที่เหยื่อไม่รู้ตัวเพื่อ

ขโมยดูข้อความ SMS ของเหยื่อที่ใช้ Reset รหัสผ่านและ PIN อาจรวมไปถึงการใช้งานระบบ i-banking เพื่อความปลอดภัยควรติดตั้งแอปพลิเคชันจาก App Store เท่านั้น ห้ามกดปุ่มติดตั้งใดๆ จาก Pop-up บนหน้าเว็บไซต์ต่างๆ กรณีที่ติดตั้งแอปพลิเคชันไปแล้ว ควรลบแอปพลิเคชันนั้นทิ้งไปทันที จากกรณีดังกล่าวจะนำไปวิเคราะห์ด้านการสำรวจพฤติกรรมผู้ใช้งานสมาร์ทโฟนที่ส่งผลต่อปัญหามัลแวร์

2.8.9 เตือนภัย “Internet Banking” ปล้นวันละแสน

จากกรณีของ รศ.ยุทธพร อิสระชัย [37] ได้โพสบน facebook ของตนเองว่า “ช่วยด้วย!! ผมถูกแฮกเงิน 343,000 บาท” ในบัญชีธนาคารแห่งหนึ่ง โดยมีการโอนเงินเข้าบัญชีคนอื่นวันละ 100,000 บาท โดยที่รศ.ยุทธพร อิสระชัย เข้าไปทำธุรกรรมบนหน้าเว็บไซต์ของ SCB ครั้งล่าสุด วันที่ 16 กุมภาพันธ์ พ.ศ. 2556 ช่วงประมาณ 17.30 น. โดยเข้าไปเปลี่ยนอีเมล์เพื่อให้อีเมล์ใหม่นี้ส่งข้อมูลติดต่อถึงตนเอง และมีอีเมล์ตอบกลับมายืนยันว่าการเปลี่ยนอีเมล์สมบูรณ์แล้วซึ่งวันนั้นมียอดเงินอยู่ที่ 3 แสนกว่าบาท จนกระทั่งวันที่ 21 กุมภาพันธ์ พ.ศ. 2556 ช่วงประมาณ 16.00-17.00 น. มีโทรศัพท์มาจากศูนย์ข้อมูลของธนาคารไทยพาณิชย์ แจ้งว่ามีการทำธุรกรรมที่ผิดปกติเกิดขึ้น ทางธนาคารแจ้งให้ รศ.ยุทธพร อิสระชัย ช่วยส่งข้อมูลการธุรกรรมให้กับธนาคาร หลังจากที่ธนาคารได้ตรวจสอบปรากฏว่า รศ.ยุทธพร อิสระชัย ได้ทำธุรกรรมทั้งหมด 7 รายการ เป็นการโอนเงินไปที่ธนาคารกรุงเทพ มีชื่อและเลขเจ้าของบัญชีชื่อว่า น.ส.สนธยา ชมชื่น ซึ่งตนไม่รู้จัก ธนาคารแนะนำให้ไปแจ้งความ ทำหนังสือถึงธนาคารเพื่อปฏิเสธการทำธุรกรรม ขอให้ทางธนาคารชดเชยค่าเสียหาย รศ.ยุทธพร อิสรชัย คณบดีรัฐศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช ได้ยืนยันว่าทุกครั้งที่จะทำธุรกรรมทางการเงินบนอินเทอร์เน็ต จะเลือกใช้เฉพาะโน้ตบุ๊กส่วนตัวเท่านั้น โดยเครื่องที่ใช้ในครั้งนี้คือ “แม็คบุ๊กโปร” ซึ่งถือว่ามีระบบป้องกันการโจมตีต่างๆ ในระดับสูง และไม่มี SMS ส่งรหัส OTP มาจากธนาคารเพื่อยืนยันการโอนเงินหรือแจ้งเตือนทางอีเมล์

รูปที่ 2.15 แจ้งเตือนการส่งเอสเอ็มเอสแอบอ้างดาวน์โหลดแอปพลิเคชันของธนาคาร

ที่มา : [37]

ในช่วงเวลาเดียวกันก็มีการเตือนจากธนาคาร ดังรูปที่ 2.15 ขณะนี้มีการโจรกรรมในรูปแบบส่ง SMS โดยมีมิจฉาชีพแอบส่ง SMS ปลอมหน้าตาเหมือนเบอร์คอลเซ็นเตอร์ของธนาคาร หลอกลวงให้เหยื่อคลิกลิงค์เพื่อดาวน์โหลดหรือติดตั้งโปรแกรม ซึ่งทางธนาคารไม่มีนโยบายในการส่งลิงค์เพื่อให้ดาวน์โหลดโปรแกรมใดๆ ผ่านโทรศัพท์มือถือ หลังตรวจสอบพบว่าในมือถือของผู้เสียหาย มีโทร

จันแฝงอยู่ โดยทำหน้าที่แอบส่งซ่อผู้ใช้, รหัสผ่านและ SMS ที่ได้รับมาทำการ Redirect ส่งไปยังคนร้ายด้วย จึงทำให้เจ้าของบัญชีตัวจริงที่รอ SMS OTP จากธนาคาร แต่ไม่ได้รับข้อความ เพราะ SMS OTP ถูกคนขโมยไป ซึ่งแอปพลิเคชันปลอมเบอร์นี้พบบน Play Store และ App Store ด้วย

ในกรณีของ iOS อย่าง iPhone, iPad ต้องไม่นำเครื่องไป Jailbreak การติดตั้งแอปพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ อาจมีมัลแวร์หรือโทรจันแอบแฝงเข้ามาเพื่อขโมยข้อมูลต่างๆ ในโทรศัพท์มือถือ โดยเฉพาะชื่อผู้ใช้ , รหัสผ่านและหมายเลขบัตรเครดิต ส่วนผู้ใช้ Android แม้ว่าแอปพลิเคชันนี้จะผ่านการตรวจสอบจาก Play Store แล้วก็ยังพบแอปพลิเคชันแฝงมัลแวร์ได้ เพราะตัวระบบปฏิบัติการ Android ยังเป็น Open Source จากเหตุการณ์ดังกล่าวจึงเป็นประเด็นที่น่าสนใจที่จะนำมาวิเคราะห์พฤติกรรมผู้ใช้สมาร์ทโฟนในการทำธุรกรรมผ่านระบบ Mobile Application ว่ามีลักษณะและวิธีป้องกันด้านความปลอดภัยจากการใช้งานอย่างไร

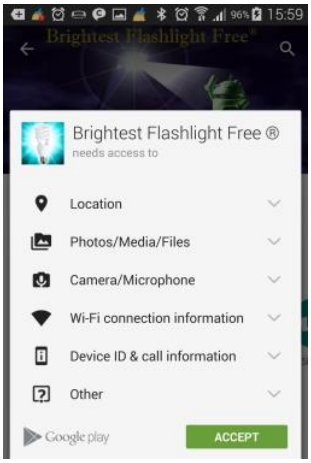
2.8.10 เตือนผู้ใช้ Apple ระวังมัลแวร์สายพันธุ์ใหม่ ระบาดบน iOS และ OS X

เมื่อวันที่ 10 พฤศจิกายน พ.ศ.2556 [38] บริษัทด้านความปลอดภัย Palo Alto Networks พบมัลแวร์สายพันธุ์ใหม่ ชื่อว่า WireLurker บนเครื่อง Mac ซึ่งสามารถเผยแพร่มัลแวร์ไปยังอุปกรณ์ iOS เช่น iPhone, iPod Touch และ iPad ผ่านทางสาย USB ที่เชื่อมกันกับเครื่อง MAC ที่ติดมัลแวร์ ซึ่งแม้เครื่อง iOS จะไม่ได้ทำการ Jailbreak ก็ติดมัลแวร์ตัวนี้ได้ โดยตัวมัลแวร์ WireLurker จะแพร่กระจายในรูปแบบแอปพลิเคชันบน App Store ชื่อ Maiyadi ซึ่งเป็น App Store ขายแอปพลิเคชันบนเครื่อง Mac สำหรับคนจีน ซึ่งมีคนดาวน์โหลดแอปพลิเคชันแฝงมัลแวร์ 356,104 ครั้ง มัลแวร์ WireLurker ต้องการขโมยข้อมูลบน iOS และ OS X ดังนั้นผู้ใช้ระบบปฏิบัติการ ต้องเตรียมรับมือภัยคุกคามจาก WireLurker จากเหตุการณ์ดังกล่าวจึงเป็นประเด็นที่น่าสนใจที่จะนำมาพฤติกรรมผู้ใช้สมาร์ทโฟนในการทำธุรกรรมผ่านระบบ Mobile Application ว่ามีลักษณะและวิธีป้องกันด้านความปลอดภัยจากการใช้งานอย่างไร

2.8.11 เตือนระวังลงแอปพลิเคชันไฟฉายบนมือถือก็โดนขโมยข้อมูล

วันที่ 6 พฤศจิกายน พ.ศ. 2557 [39] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) ได้นำเสนอข่าวจาก บริษัทด้านความมั่นคงปลอดภัย Snoopwall เกี่ยวกับแอปพลิเคชันไฟฉายยอดฮิตบน Google Play สำหรับมือถือ Android โดยแอปพลิเคชันไฟฉายยอดนิยม 10 แอปพลิเคชันขอสิทธิ์การเข้าถึงข้อมูลบนสมาร์ทโฟน ที่เกี่ยวข้องกับความเป็นส่วนตัวเกินความจำเป็น เช่น ขอสิทธิ์อ่านรายชื่อเบอร์โทรศัพท์ (Contact), พิกัด (GPS) การเข้าถึงข้อมูลไฟล์ต่างๆ บนตัวมือถือ Android ซึ่งมีความเสี่ยงที่ข้อมูลมือถือและความเป็นส่วนตัว อาจหลุด หรือถูกขโมยตกในมือของแฮกเกอร์ได้

จากรูปที่ 2.16 ก่อนที่จะติดตั้งควรดูสิทธิ์การเข้าถึงของแอปพลิเคชันไฟฉายด้วยว่าเข้าถึงข้อมูลอะไรบ้าง โดยเฉพาะการเข้าถึงการโทรเข้า โทรออก ส่งข้อความ ซึ่งถ้าเกินสิทธิ์ของแอปพลิเคชันไฟฉายแล้วก็ไม่ควรติดตั้งแอปพลิเคชันนั้น หากเผลอติดตั้งไปแล้วให้ถอนการติดตั้งออกทันที นอกจากนี้ทาง Snoopwall ก็ได้จัดทำแอปพลิเคชันไฟฉาย Privacy Flashlight ซึ่งปลอดภัยสามารถใช้ได้บน Android จากเหตุการณ์ดังกล่าวจึงเป็นประเด็นที่น่าสนใจที่จะนำมาพฤติกรรมผู้ใช้สมาร์ทโฟนในการทำธุรกรรมผ่านระบบ Mobile Application ว่ามีลักษณะและวิธีป้องกันด้านความปลอดภัยจากการใช้งานอย่างไร



รูปที่ 2.16 ตัวอย่างแอปพลิเคชันไฟฉายที่ขอสิทธิ์มากเกินไป
ที่มา : [39]

นอกจากคดีข้างต้นแล้ว การศึกษาค้นคว้าอิสระนี้ยังได้ใช้คดีอื่นๆ ที่เกี่ยวกับการทำธุรกรรมออนไลน์ โดยได้รับการอนุเคราะห์ข้อมูลจากฝ่ายคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ (DSI) เพื่อใช้ในการวิเคราะห์ปัญหา

2.9 ความมั่นคงของระบบ m-banking

2.9.1 Triple Lock Security

Triple Lock Security [40] เป็นระบบความมั่นคงปลอดภัยที่ถูกพัฒนาขึ้น เพื่อป้องกันการเข้าใช้งานจากกลุ่มบุคคลผู้ไม่หวังดี ทั้งจากการโจรกรรมข้อมูลของกลุ่มแฮกเกอร์หรือการนำเอารหัสผ่านไปใช้ในการทำธุรกรรม ซึ่งเทคโนโลยี Triple Lock Security นี้ ระบบจะมีการตรวจสอบข้อมูลทั้ง 3 ชั้น เช่น 1) ล็อคด้วยหมายเลขมือถือจากผู้ให้บริการเครือข่าย 2) ล็อคด้วย ID ของเครื่องโทรศัพท์ (IMEI) ที่ใช้งาน เมื่อเปิดการใช้งานระบบก็จะรู้ว่าเป็นเครื่องนั้นที่ใช้งานจริง จึงปลอมแปลงค่อนข้างยาก 3) ล็อครหัสผ่าน 6 หลัก ดังนั้นจึงเป็นความแตกต่างระหว่างการทำธุรกรรมบนระบบ m-banking และระบบ i-banking ที่มีระบบ Lock หลายชั้น ซึ่งการทำธุรกรรมบนระบบ i-banking ที่ผ่านเบราว์เซอร์จะใช้เพียงชื่อผู้ใช้และรหัสผ่านจึงทำให้การใช้งานผ่านแอปพลิเคชันมีความมั่นคงปลอดภัยสูงขึ้นมากกว่าเทคโนโลยี Triple Lock Security ระบบ m-banking นั้นสามารถสร้างระบบความมั่นคงได้หลายชั้นกว่านั้นก็ได้ เช่น อาจเป็น 4 หรือ 5 ชั้นก็ได้ ทั้งนี้ขึ้นอยู่กับการพัฒนา Smartphone Application ของแต่ละธนาคาร ซึ่งต่างจากการพัฒนาเว็บแอปพลิเคชันของธนาคารที่ใช้งานผ่านระบบ i-banking ที่ต้องพัฒนาโปรแกรมที่มา run อยู่บนเว็บเบราว์เซอร์ ซึ่งมีข้อจำกัดมากกว่า Smartphone Application

2.9.2 Two Factor Authentication (2FA)

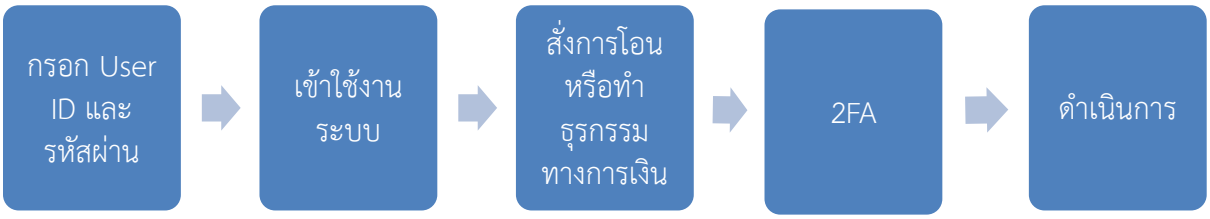
2FA (Two Factor Authentication) [41] คือการเพิ่มระบบรักษาความปลอดภัยในการใช้บริการอิเล็กทรอนิกส์แบงก์กิ้ง โดยการเพิ่มขั้นตอนที่จะต้องทำการพิสูจน์ความเป็นเจ้าของบัญชีอีก 1 ขั้นนอกเหนือไปจากการมี User ID และรหัสผ่านเข้าใช้งาน ในกรณีของธนาคารผู้ให้บริการธุรกรรมการเงินผ่านโทรศัพท์มือถือมักเลือกใช้ระบบ OTP (One Time Password) หรือรหัสผ่านแบบใช้ได้ครั้ง

เดียว เป็นมาตรการความปลอดภัย ซึ่ง OTP จะมีลักษณะเฉพาะ มีการเปลี่ยนแปลงรหัสทุกครั้งไม่ซ้ำเดิมและเมื่อถูกใช้ไปแล้ว ก็จะไม่สามารถใช้งานได้อีก เพื่อดำเนินการดังต่อไปนี้

(1) เพื่อทำการเพิ่มบัญชีคู่โอนเข้าสู่ระบบ

(2) เพื่อยืนยันการโอนสำหรับการทำธุรกรรมโอนเงิน หรือ ชำระเงิน

(3) เพื่อเปลี่ยนแปลงข้อมูลส่วนตัวเจ้าของบัญชี



รูปที่ 2.17 ลักษณะการใช้งานระบบ 2FA

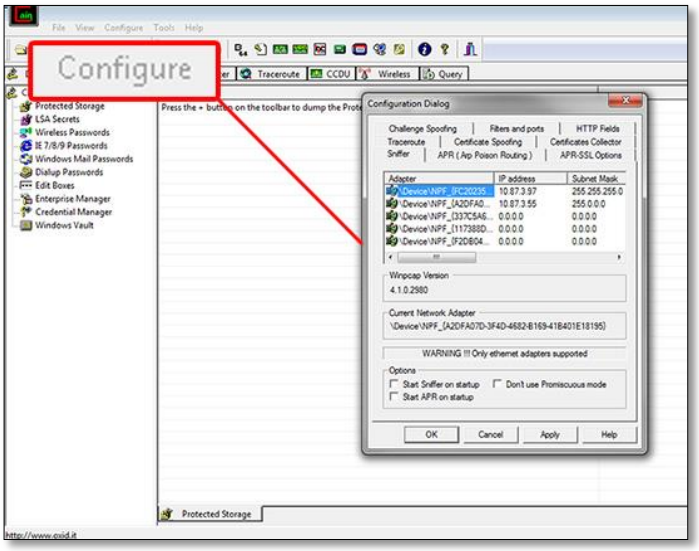
รหัส OTP จึงช่วยลดความเสี่ยงที่อาจเกิดขึ้นจากการถูกเจาะขโมยข้อมูลรหัสผ่านที่อาจกระทำได้โดยง่าย หากใช้รหัสผ่านเพียงอย่างเดียว สำหรับระบบ m-banking จะตรวจสอบ หมายเลขโทรศัพท์มือถือหรือหมายเลข IMEI ของเครื่องโทรศัพท์มือถือมาเป็นปัจจัยในการยืนยันตัวตนเพิ่มอีก ดังนั้นจึงมีโอกาสมีความมั่นคงมากขึ้น เพราะอาจเป็น Multiple Factor Authentication มากกว่า 2 ชั้น

2.10 การโจมตีแบบแทรกกลางการสื่อสาร

2.10.1 การโจมตีแบบแทรกกลางการสื่อสารด้วยเครื่องมือ Cain & Abel

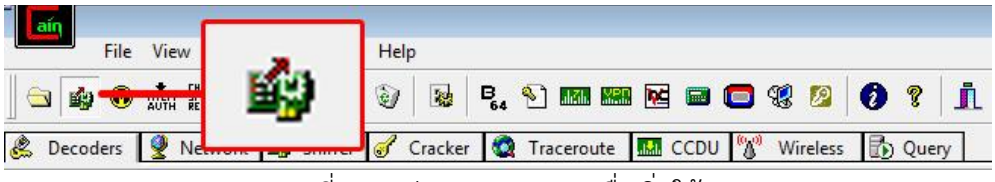
เทคนิคการโจมตีแบบแทรกกลางการสื่อสารด้วยเครื่องมือ Cain & Abel นั้น สามารถทำงานผ่านโหมด GUI (Graphic User Interface) ซึ่งมีขั้นตอนในการโจมตีดังนี้

1) เปิดโปรแกรม Cain & Abel แล้วเข้าไปกำหนดการ์ดเน็ตเวิร์ก ให้คลิกที่ Configure จากนั้นจะปรากฏหน้าต่าง Configuration Dialog ให้เลือกการ์ดที่จะใช้โจมตีในวงแลนดัง รูปที่ 2.18



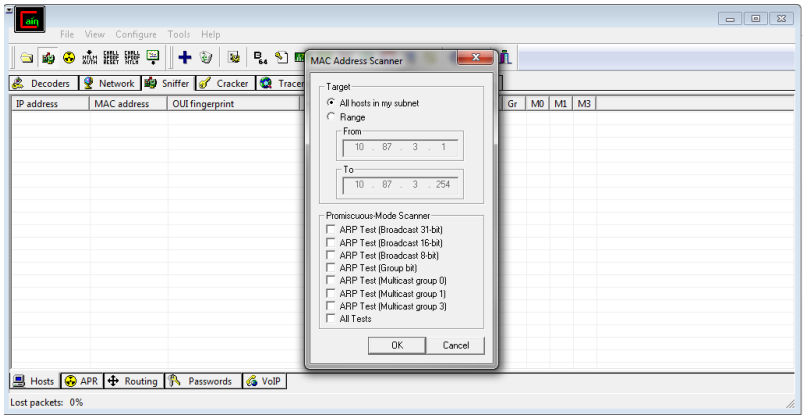
รูปที่ 2.18 การกำหนดการ์ดเครือข่าย

2) คลิกที่ปุ่ม Start/Stop เพื่อเริ่มใช้งานดัง รูปที่ 2.19



รูปที่ 2.19 ปุ่ม Start/Stop เพื่อเริ่มใช้งาน

3) ค้นหาเลขไอพีของเป้าหมายเพื่อทำการโจมตี โดยไปที่ Tap Sniffer แล้วให้ทำการคลิกขวาตรงพื้นที่วางสีขาว แล้วเลือก Scan Mac Address จะมีหน้าต่าง MAC Address Scanner ขึ้นมา จากนั้นเลือก ALL host in my subnet แล้วตอบ ok ดังรูปที่ 2.20



รูปที่ 2.20 ค้นหาเป้าหมายที่ต้องการโจมตี

4) รอสักครู่ ผลของการสแกน MAC Address จะปรากฏข้อมูล แล้วเริ่มทำการโจมตี โดยการไปคลิกที่ Tab ของ ARP ด้านล่าง แล้วเอาเมาส์ไปคลิกที่ช่องว่างพื้นที่สีขาวด้านบน 1 ครั้ง แล้วจะเห็น ไอคอนบวก หรือปุ่ม Add to list จากนั้นจะมีหน้าต่าง New ARP Poison Routing ที่ช่องด้านซ้ายเลือกไอพีของเกตเวย์ ส่วนด้านขวาให้เลือกไอพีของเครื่องเหยื่อ เสร็จแล้วจึงคลิกที่ ปุ่ม OK

5) คลิกปุ่ม Star/Stop ARP เพื่อทำการจู่โจมแบบแทรกกลางการสื่อสาร

2.10.2 การโจมตีแบบ SSL Strip

เทคนิคการโจมตีการแทรกกลางการสื่อสารด้วย Kali Linux นั้น สามารถโจมตี เป็นการดักจับข้อมูลมูลที่วิ่งบนเครือข่าย

1) ใช้คำสั่ง echo 1 >/proc/sys/net/ipv4/ip_forward

2) ใช้คำสั่ง iptables -t nat -A PREROUTING -p tcp –-destination-port 80 -j REDIRECT --to-port 888 เพื่อกำหนดให้ข้อมูลที่เข้ามายังเครื่องผู้โจมตีทาง Port หมายเลข 80 ไปยัง Port หมายเลข 888

3) ใช้คำสั่ง sslstrip –a –l 888 เพื่อโจมตีเว็บไซต์ที่ใช้งาน SSL เมื่อเครื่องของเหยื่อเข้าใช้งานเว็บไซต์แล้วตามปกติบนเว็บเบราว์เซอร์จะแสดงโพรโทคอล HTTPS แต่เมื่อถูกโจมตีด้วยวิธี SSL นี้แล้ว ผลของการโจมตีจะส่งผลให้บนเว็บเบราว์เซอร์ ถูกกำหนดให้ใช้งานโพรโทคอล HTTP แทน

4) ใช้คำสั่ง ettercap –i eth0 -T –q เพื่อแสดงข้อมูลของเครื่องเหยื่อที่สามารถดักจับได้

2.11 ดัชนีความสอดคล้อง (Index of Consistency)

ดัชนีความสอดคล้อง หรือ IOC (Index of Consistency) [42] โดยในการศึกษาค้นคว้าอิสระนี้ได้นำเครื่องมือที่ใช้ในการรวบรวมข้อมูลต้องมีความเที่ยงตรงและสมบูรณ์ ซึ่งเป็นเครื่องมือที่มีคุณภาพ โดยผ่านการตรวจสอบคุณภาพของเครื่องมือเพื่อให้มีความเที่ยงตรง ถ้าเป็นเครื่องมือที่วัดความรู้ ต้องมีความยากและอำนาจจำแนกที่ชัดเจน โดย IOC จะเป็นการตรวจสอบ 3 ส่วน ได้แก่ ความตรงเฉพาะหน้า (Face Validity), ความตรงเชิงเนื้อหา (Content Validity) และความตรงตามโครงสร้าง (Construct Validity) การตรวจสอบความครอบคลุมของเนื้อหา ซึ่งจะใช้ผู้ทรงคุณวุฒิที่มีความรู้ความเชี่ยวชาญกับเครื่องมือที่ใช้วัดเป็นผู้ทำการตรวจสอบ สำหรับงานวิจัยโดยทั่วไปจะใช้จำนวนผู้ทรงคุณวุฒิร่วมตรวจสอบคุณภาพของเครื่องมือวัดประมาณ 3 ถึง 5 คน โดยจะนำผลของผู้เชี่ยวชาญแต่ละท่านมารวมกันแล้วคำนวณหาความตรงเชิงเนื้อหา โดยคำนวณจากความสอดคล้องระหว่างประเด็นที่ต้องการวัดกับคำถามที่สร้างขึ้น วิธีการหาค่า IOC ของเครื่องมือวัด โดยผู้ศึกษาจะนำเครื่องมือที่สร้างขึ้นมาให้ผู้เชี่ยวชาญแต่ละท่านตรวจสอบและให้คะแนนรายข้อตามดุลยพินิจของผู้เชี่ยวชาญ โดยผู้เชี่ยวชาญจะต้องประเมินด้วยคะแนน 3 ระดับ คือ

ค่า + 1 คือผู้ตรวจสอบแน่ใจว่าคำถามนั้นสามารถใช้วัดค่าตัวแปรได้

ค่า 0 คือผู้ตรวจสอบไม่แน่ใจว่าคำถามนั้นสามารถใช้วัดค่าตัวแปรได้หรือไม่

ค่า -1 คือผู้ตรวจสอบแน่ใจว่าคำถามนั้นไม่สามารถใช้วัดค่าตัวแปรได้

เมื่อได้ผลคะแนนจากผู้เชี่ยวชาญครบทุกท่านแล้ว ก็จะนำข้อมูลที่ได้มาทำการคำนวณตามสูตรหาค่าดัชนีความสอดคล้อง ดังนี้

$$IOC = \frac{\sum R}{N} \qquad (2.1)$$

IOC หมายถึง ดัชนีความสอดคล้อง

R หมายถึง ค่าคะแนนรายข้อตามดุลยพินิจของผู้ตรวจสอบหรือผู้เชี่ยวชาญ

N หมายถึง จำนวนผู้ตรวจสอบหรือผู้เชี่ยวชาญ

ผลที่ได้จากการคำนวณนั้นควรมีค่าดัชนีความสอดคล้องมากกว่าหรือเท่ากับ +0.5 ขึ้นไป จึงจะถือว่าเป็นข้อคำถามที่สามารถนำไปใช้งานได้ แต่หากค่า IOC น้อยกว่า +.05 และผู้วิจัยอาจมีความจำเป็นต้องใช้ข้อคำถามนั้น อาจทำได้โดยให้ผู้วิจัยทำการพัฒนาปรับปรุงข้อคำถามนั้นให้เหมาะสมมากขึ้นตามคำแนะนำของผู้เชี่ยวชาญที่ทำการตรวจสอบ

2.12 งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้องกับระบบ e-banking ได้มีหลายงานวิจัยที่ได้ทำการศึกษาและสำรวจทั้งในประเทศและต่างประเทศ โดยศึกษาในประเด็นด้านของความปลอดภัย (Safety) ซึ่งจะเกี่ยวข้องกับการบริหารจัดการระบบ และความมั่นคง (Security) ซึ่งจะเกี่ยวข้องในด้านของเทคนิควิธีในการโจมตีระบบ โดยได้มีงานวิจัยก่อนหน้านี้จำนวนมากที่ทำการศึกษาความปลอดภัยมั่นคงของระบบ i-banking ดังนี้

ธนพล พุกเส็ง และ ศิรปัฐช์ บุญครอง [7] ได้ทำงานวิจัยมีวัตถุประสงค์เพื่อนำเสนอการรักษาความปลอดภัยการใช้งานอินเทอร์เน็ตแบงก์กิ้งธนาคารพาณิชย์ไทยสำหรับกลุ่มลูกค้าบุคคล จากการศึกษาพบว่ามีวิธีการรักษาความปลอดภัยทั้งหมด 6 ลักษณะคือ SSL ใบรับรองดิจิทัล CAPTCHA บัญชีผู้ใช้และรหัสผ่าน OTP และการพิสูจน์ทราบตัวตนด้วยสองปัจจัย โดยขอบเขตในการพิจารณานั้นเลือกจากธนาคารพาณิชย์ในประเทศไทยจำนวน 6 ธนาคาร จากงานวิจัยชิ้นนี้สรุปได้ว่าวิธีการรักษาความปลอดภัยที่แต่ละธนาคารใช้ มีเพียงธนาคารกรุงไทย ที่มีการใช้ CAPTCHA ในขั้นตอนการเข้าสู่ระบบ แต่ธนาคารอื่นๆ ใช้การพิสูจน์ตัวตนด้วยสองปัจจัย ซึ่งเป็นวิธีในการรักษาความปลอดภัยต่อการใช้บริการอินเทอร์เน็ตแบงก์กิ้งได้ดีอย่างยิ่ง ในการป้องกันปัญหาและการโจมตีที่เกิดขึ้นต่างๆ นั้น สำหรับผู้ใช้งานจะต้องมีความระมัดระวังตั้งแต่การเข้าใช้งานเว็บไซต์ ไม่ใช้งานเครือข่ายสาธารณะที่ไม่มีการรักษาความปลอดภัย รอบคอบในการใส่รหัสผ่านเข้าใช้งานระบบ ส่วนธนาคารผู้ให้บริการจะต้องนำเทคโนโลยีใหม่ๆ มาใช้ เพื่อเพิ่มความปลอดภัยให้มากยิ่งขึ้น ดังตารางที่ 2.2

ตารางที่ 2.2 ตัวอย่างปัญหา การโจมตีที่พบและแนวทางการป้องกันที่เกิดขึ้นกับการรักษาความปลอดภัยในการใช้งานอินเทอร์เน็ตแบงก์กิ้ง

ที่มา : [7]

วิธีการโจมตี	ลักษณะของโจมตีหรือปัญหา	การป้องกันปัญหาสำหรับผู้ใช้งาน	การป้องกันปัญหาสำหรับธนาคารผู้ให้บริการ
1. การโจมตี SSL			
BEAST	- คาดเดาค่า IV หรือดักจับข้อมูลที่เป็นส่วนสำคัญในการเข้ารหัส	- ตรวจสอบเว็บไซต์ที่ใช้งาน - อัพเดทเว็บบราวเซอร์สม่ำเสมอ - ใช้งานเครือข่ายที่มีการรักษาความปลอดภัย	- กำหนดให้เครื่องแม่ข่ายของธนาคารทำงานโดยใช้ โพรโทคอล HTTPS ซึ่งจะมีการเรียกใช้ SSL
SSL stripping	- โจมตีแทรกกลางการสื่อสารที่ใช้โพรโทคอล SSL แล้วบังคับให้ปลอดการใช้โพรโทคอล SSL		
2. การโจมตีใบรับรองดิจิตอล			
การปลอมแปลงใบรับรอง	- การใช้บริการเกิดความเสี่ยง ไม่สามารถตรวจสอบถึงความปลอดภัยในการใช้บริการได้	- ตรวจสอบใบรับรองของเว็บไซต์ที่ใช้งาน - อัพเดทเว็บบราวเซอร์	- ธนาคารควรมีการประยุกต์ใช้ hardware security module (HSM) เพื่อเก็บรักษากุญแจส่วนตัวให้ปลอดภัย
3. การโจมตี CAPTCHA			
โปรแกรมคอมพิวเตอร์ประสงค์ร้าย	- ก่อกวนหรือกระทำการทุจริตต่อข้อมูลผู้ใช้ระบบ	- ติดตั้งและใช้งานโปรแกรม antivirus	- ปรับปรุงรูปแบบของ CAPTCHA ให้ทันต่อเทคโนโลยีที่พัฒนาขึ้น
4. การโจมตีบัญชีผู้ใช้และรหัสผ่าน			
ฟิชชิง	- ปลอมแปลงหน้าเว็บไซต์เพื่อการขโมยข้อมูลส่วนตัวของผู้ใช้งาน	- ติดตั้งและใช้งานโปรแกรม antivirus - ตรวจสอบเว็บไซต์ว่าถูกต้องก่อนใช้งาน - เลือกใช้รหัสผ่านที่คาดเดาได้ยาก และเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ - ระวังในดาวน์โหลดและติดตั้งโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ	- มีระบบการจัดเก็บรหัสผ่านที่ปลอดภัย เช่น Salted hash
Brute force attack	- การกำหนดรหัสผ่านของผู้ใช้ที่ง่ายต่อการคาดเดาหรือโจมตีได้ง่าย		
Trojan horse	- ขโมยข้อมูลส่วนตัวของผู้ใช้งานแล้วส่งข้อมูลไปยังผู้โจมตี		
5. การโจมตี OTP			
Mobile phone Trojan	- รับส่งข้อมูล OTP โดยอัตโนมัติ รวมถึงขโมยข้อมูลในโทรศัพท์	- ระมัดระวังในการดาวน์โหลดและติดตั้งโปรแกรมในโทรศัพท์พกพา - หลีกเลี่ยงการทำธุรกรรมในช่วงเวลาที่มีผู้ใช้งานเครือข่ายหนาแน่น	- มีการสร้างและตรวจสอบรหัส OTP ว่าซ้ำกับรหัสที่เคยใช้งานมาแล้วหรือไม่ - ใช้วิธีการสร้างรหัส OTP ที่เรียกว่า time-based OTP (TOTP)
SMS delay	- ข้อความ OTP มาถึงล่าช้าทำให้การทำธุรกรรมติดขัด		
6. การโจมตีการพิสูจน์ทราบตัวตนด้วยสองปัจจัย			
การโจมตีด้วย MITM และ phishing สำหรับการใช้บัญชีผู้ใช้และรหัสผ่านร่วมกับ OTP	- สกัดกั้นการรับใบรับรองที่เครื่องผู้ใช้งาน ใช้หน้าเว็บไซต์หลอกลวงขโมยข้อมูล และขวางการสื่อสารข้อมูล OTP	- ตรวจสอบเว็บไซต์ว่าถูกต้องก่อนใช้งาน	- นำวิธีการตรวจสอบตัวตนทั้งสองทาง (mutual authentication) มาประยุกต์ใช้

Park และคณะ [3] ได้ทำการวิเคราะห์วิธีรับรองความถูกต้องสำหรับธนาคารที่ให้บริการเครือข่าย (APN) แก่สมาร์ทโฟน ซึ่งในประเทศเกาหลีได้รับการรับรองโดย พระราชบัญญัติอิเล็กทรอนิกส์ ในปี ค.ศ.1999 ซึ่งระบบนี้มีการบริหารจัดการแบบใบรับรองคีย์สาธารณะและโครงสร้างพื้นฐานของกุญแจสาธารณะที่ใช้ เช่น การเข้ารหัสคีย์ไม่สมมาตร / การถอดรหัส และยังสนับสนุนกลไกการตรวจสอบลายเซ็นดิจิตอล ซึ่งจะมีวิธีการตรวจสอบหลักฐานว่าจะรับรองหรือปฏิเสธ โดยส่วนใหญ่จะใช้ในการทำธุรกรรมออนไลน์ในประเทศเกาหลี จากการศึกษาครั้งนี้พบว่า กระบวนการวิเคราะห์ธนาคารที่ให้บริการเครือข่าย (APN) และวิธีการตรวจสอบการให้บริการของธนาคารที่ให้บริการสมาร์ทโฟนเหมาะสมที่สุด โดยใช้เกณฑ์ดังนี้ในการวิเคราะห์วิธีรับรองความถูกต้อง 1) การรักษาความปลอดภัย 2) ความสะดวกสบาย 3) ค่าใช้จ่าย จากผลการวิเคราะห์พบว่าการเข้ารหัสแบบไบโอเมตริกซ์เหมาะสมที่สุดในการรักษาความปลอดภัย การใช้รหัสผ่านทางเดียวเหมาะมากที่สุดในด้านความสะดวก และใบรับรองกุญแจสาธารณะเหมาะที่สุดในด้านของค่าใช้จ่าย เพื่อเพิ่มให้ความปลอดภัยและความสะดวกสบายของธนาคารที่ให้บริการแก่สมาร์ทโฟน

ประพจน์ ธรรมศิรารักษ์ และ สมนึก พ่วงพรพิทักษ์ [41] ได้ทำการวิเคราะห์ปัญหาและการทดสอบความมั่นคงของเทคโนโลยีรหัสผ่านแบบใช้ครั้งเดียว (OTP : One Time Password) ถือเป็นองค์ประกอบที่สำคัญสำหรับระบบการยืนยันตัวตนของธนาคารออนไลน์ ซึ่ง OTP มักจะถูกใช้ในการรักษาความมั่นคงเป็นชั้นที่สองเพื่อปกป้องระบบอย่างไรก็ตาม OTP ก็ยังมีช่องโหว่และพบปัญหาการโจมตีระบบธนาคารออนไลน์ออกมาเป็นจำนวนมาก ถึงแม้จะมีการใช้ OTP แล้วก็ตาม โดยในงานวิจัยนี้จึงได้ทำการวิเคราะห์ปัญหาของ OTP ชนิดต่างๆ ที่มีอยู่ในปัจจุบัน เพื่อแสดงให้เห็นถึงจุดแข็งจุดอ่อนของ OTP รูปแบบต่างๆ ได้แก่ Email OTP, SMS OTP, Token OTP และ Mobile OTP จากการวิเคราะห์ปัญหาของ OTP Algorithm พบว่า Time-based OTP คือรูปแบบที่ได้รับความนิยมมากที่สุด รองลงมาคือ Event-based OTP หรือ Counter-based OTP และนิยมใช้น้อยที่สุดคือแบบ Challenge-Response OTP ทั้งที่มีความมั่นคงมากที่สุด งานวิจัยดังกล่าวแสดงให้เห็นว่า OTP เป็นเครื่องมือที่สำคัญในการเพิ่มการรักษาความมั่นคงของการใช้งานระบบสารสนเทศที่สำคัญ โดยเฉพาะระบบ Online Banking ถึงแม้ว่าจะมีระบบ OTP แต่ก็ยังมีข่าวการโจรกรรมข้อมูลบนระบบ Online Banking อยู่เรื่อยๆ ในส่วนของ OTP Algorithm ที่เหมาะสมกับระบบ Online Banking คือแบบ Challenge-Response OTP เพราะมีความมั่นคงมากที่สุด จากงานวิจัยดังกล่าวผู้วิจัยจะนำมาใช้ในการวิเคราะห์ด้าน Safety ของระบบ m-banking

พัฒนรัฐ พุดหล้า และ สมนึก พ่วงพรพิทักษ์ [2] ได้ทำการวิเคราะห์ความมั่นคงและปลอดภัยของระบบอินเทอร์เน็ตแบงก์กิ้งในประเทศไทย ซึ่งจะวิเคราะห์ทั้งด้านความปลอดภัยและความมั่นคง โดยได้ทำการศึกษากับ 6 ธนาคารในประเทศไทย ซึ่งเราได้ค้นพบจุดอ่อนจำนวนมากมายทั้งในด้านความปลอดภัยและความมั่นคงงานวิจัยนี้ได้ทำการวิเคราะห์ธนาคารพาณิชย์ในประเทศไทยอยู่ 2 ประเด็น ซึ่งสามารถสรุปในแต่ละด้านได้ดังนี้ (1) ด้านมาตรการป้องกันความปลอดภัย (Safety) พบว่ายังมีช่องโหว่ที่ทำให้มิจฉาชีพเข้ามาโจรกรรมข้อมูลได้ ส่วนใหญ่จะเป็นช่องโหว่ในเรื่องของการสวมรอยเป็นเจ้าของบัญชี (2) ด้านความมั่นคงของระบบ (Security) พบว่าในการทดสอบการโจมตีแทรกกลางการสื่อสารแบบวิธี SSL Sniff และ SSL Strip ธนาคารส่วนใหญ่สามารถดักจับข้อมูลได้อย่างง่ายดาย ซึ่งในงานวิจัยนี้จะนำเสนอวิธีการใช้งานที่ปลอดภัยให้ผู้ใช้งานมีความรู้ความรอบคอบ เพื่อป้องกันการโจมตีรูปแบบ

ต่างๆ ในปัจจุบัน จากงานวิจัยดังกล่าววิเคราะห์ในส่วนระบบ i-banking ซึ่งไม่ได้ทำการวิเคราะห์ในส่วนของระบบ m-banking

Rachana [6] ได้นำเสนอการเปรียบเทียบการรักษาความมั่นคงและความปลอดภัยของธนาคารในประเทศไทยและธนาคารในประเทศกัมพูชา การศึกษาครั้งนี้ได้เลือก 3 ธนาคารทั้งในประเทศไทยและประเทศกัมพูชา ทำการวิเคราะห์จุดแข็งจุดอ่อนของการให้บริการธนาคารทางอินเทอร์เน็ต โดยการสังเกตจากการใช้งานจริง ปัญหาการโจมตีต่างๆ มาตรฐานความปลอดภัยและสัมภาษณ์จากพนักงาน พร้อมทั้งเสนอแนวทางการแก้ไขปัญหา

Subsorn และ Limwiriyakul [43] ได้นำเสนอการตรวจสอบความปลอดภัยของระบบ i-banking ใน 16 ธนาคารของประเทศออสเตรเลียโดยใช้การวิเคราะห์เปรียบเทียบจากรายการ 6 ลักษณะด้านความปลอดภัยที่สร้างขึ้นแล้วนำมาประเมินผล ซึ่งผลพบว่าธนาคารยังขาดการรักษาความปลอดภัยและส่งผลกระทบต่อการรักษาความลับของลูกค้า โดยงานวิจัยนี้ได้ทำการสำรวจความปลอดภัยของธนาคารอย่างละเอียดในแต่ละด้าน แต่ยังขาดประเด็นในเรื่องของเทคนิคการโจมตีในระบบจริงของธนาคารซึ่งเป็นอีกประเด็นปัญหาที่มีการโจมตีระบบ i-banking อย่างต่อเนื่อง

โดยงานวิจัยเหล่านี้ได้พบจุดอ่อนของระบบ i-banking ที่เป็นการโปรแกรมธนาคารผ่านเว็บเบราว์เซอร์ ว่าสามารถโจมตีด้วยวิธีการแทรกกลางการสื่อสารได้ค่อนข้างง่าย และเนื่องจากมีข้อจำกัดของ Web Programming หลายอย่างในการเสริมสร้างความมั่นคงซึ่งระบบ m-banking ที่เป็น Mobile Application น่าจะมีข้อจำกัดด้านนี้น้อยกว่า แต่ว่างานวิจัยเหล่านี้ ยังไม่ได้ศึกษาความปลอดภัยและมั่นคงของระบบ m-banking ซึ่งเป็นตัวเลือกใหม่แต่อย่างไร มีบางงานวิจัยที่ได้ทำการศึกษาเกี่ยวกับระบบ m-banking อยู่บ้างดังนี้

ACIS Research LAB [1] ได้นำเสนอเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยระบบ i-banking และ ระบบ m-banking ของธนาคารในประเทศไทยได้โดยได้กล่าวปัญหาอัตราการเพิ่มขึ้นของจำนวนเหยื่อในการถูกเจาะระบบ i-banking ในประเทศไทย โดยได้ดำเนินการให้คะแนนด้านความปลอดภัย ตามเกณฑ์ที่เลือกมา 16 ข้อ จาก 8 ระบบ 7 ธนาคาร และผลการวิจัยพบว่าระบบส่วนใหญ่ยังขาดมาตรการที่จำเป็นต่อการรับมือกับภัยคุกคามที่เกิดขึ้นในปัจจุบัน ซึ่งเกณฑ์ที่ใช้ในการวิเคราะห์ส่วนใหญ่เป็นเรื่องของความปลอดภัยซึ่งยังขาดในเรื่องของความมั่นคง ที่จะเป็นแนวทางให้บุคคลทั่วไปให้มีความระมัดระวังในการใช้งานอย่างรอบคอบ

Filiol and Iroll [4] ได้ทำการวิจัยเกี่ยวกับการรักษาความปลอดภัยของธนาคารบนมือถือและแอปพลิเคชันมือถืออื่นๆ โดยใช้เครื่องมือดังนั้นในการวิเคราะห์และรับรองแอปพลิเคชันบนโทรศัพท์มือถือ 1) Egide ใช้ในการวิเคราะห์การตรวจจับมัลแวร์ 2) Panoptes ใช้ในการวิเคราะห์ผู้ให้บริการเครือข่าย 3) Tarentula ใช้เก็บรวบรวมแอปพลิเคชันที่เป็นอันตราย โดยเปรียบเทียบการรักษาความปลอดภัยของธนาคารตะวันตกและธนาคารเอเชีย ผลจากการทดลองพบว่าธนาคารเอเชียมีความปลอดภัยสูงกว่าธนาคารตะวันตก เพราะมีวิธีการรักษาความปลอดภัยของข้อมูลโดยใช้โพรโทคอล SSL ที่ใช้สื่อสารข้อมูลระหว่างไคลเอนต์และเซิร์ฟเวอร์ การใช้โพรโทคอล HTTPS จะทำให้ไม่สามารถโจมตีแบบแทรกกลางการสื่อสารได้และการใช้งานผ่านโทรศัพท์มือถือจะมีการตรวจสอบข้อมูลผ่านหมายเลข IMEI, MAC Address, หมายเลขโทรศัพท์มือถือ จะเห็นได้ว่าการใช้งานผ่านแอปพลิเคชันของธนาคารบนโทรศัพท์มือถือจะมีความปลอดภัยกว่าการใช้งานผ่านบราว์เซอร์บนคอมพิวเตอร์ และ

ธนาคารต่างประเทศให้ความสำคัญกับการรักษาความปลอดภัยธนาคารบนโทรศัพท์มือถือและมีแนวโน้มว่าจะมีผู้คนนิยมมาใช้ธนาคารบนโทรศัพท์มือถือมากขึ้น

Islam [5] ได้ทำการสำรวจความปลอดภัยของระบบธนาคารผ่านโทรศัพท์และระบบการชำระเงินออนไลน์ ธนาคารบนระบบระบบโทรศัพท์มือถือมีความง่ายและสะดวกรวดเร็ว และมีระบบความปลอดภัยในการชำระเงิน จึงมีธนาคารจำนวนมากที่เลือกใช้ระบบ m-banking ในการให้บริการด้านการเงินเพื่อใช้เป็นกลยุทธ์ในการให้ลูกค้าใช้งานที่เพิ่มขึ้น จากงานวิจัยได้ทำการศึกษาและสำรวจในประเด็นด้านระบบความปลอดภัยของการใช้งานธนาคารผ่านโทรศัพท์มือถือ พบว่ามีช่องโหว่ที่ทำให้เกิดภัยคุกคามระบบธนาคารผ่านโทรศัพท์มือถือคือ การเข้าถึงความเป็นส่วนตัวโดยไม่ได้รับอนุญาต, ภัยจากไวรัสและมัลแวร์ของโทรศัพท์มือถือ, การดาวน์โหลดแอปพลิเคชันจากโทรศัพท์มือถือ และไวรัสจาก SMS งานวิจัยชิ้นนี้ผู้วิจัยได้ให้ความรู้เกี่ยวกับภัยคุกคามด้านความปลอดภัยและช่องโหว่ที่แฮกเกอร์ใช้ในการโจมตีเพื่อขโมยข้อมูลส่วนบุคคล เพื่อเป็นแนวทางในองค์กรต่างๆ ในการปรับปรุงและพัฒนาระบบรักษาความปลอดภัยของระบบธนาคารผ่านโทรศัพท์มือถือ เพื่อป้องกันภัยคุกคามของไวรัส มัลแวร์และภัยคุกคามต่างๆ จากงานวิจัยดังกล่าวผู้วิจัยจะใช้ในการศึกษาและวิเคราะห์พฤติกรรมของผู้ใช้สมาร์ทโฟนที่ส่งผลต่อปัญหามัลแวร์ของกลุ่มผู้ใช้งานแอปพลิเคชันบนสมาร์ทโฟน (Smartphone Application)

Masrek และคณะ [44] ได้ทำการวิจัยเกี่ยวกับความเชื่อมั่นด้านเทคโนโลยีและความพึงพอใจของระบบธนาคารผ่านโทรศัพท์มือถือ กรณีศึกษากลุ่มลูกค้าในประเทศมาเลเซีย โดยงานวิจัยนี้ได้ใช้เกณฑ์ในการศึกษา 3 เกณฑ์คือ 1) เครือข่ายของโทรศัพท์มือถือ 2) เว็บไซต์ที่ใช้งานระบบธนาคาร 3) โทรศัพท์สมาร์ทโฟน เพื่อใช้ในการสำรวจความพึงพอใจของระบบธนาคารผ่านโทรศัพท์มือถือ จากการศึกษางานวิจัยยังไม่มีการวิเคราะห์ด้านความปลอดภัยและความมั่นคงของระบบธนาคารผ่านโทรศัพท์มือถือ

Loke และคณะ [45] ได้ศึกษาการตรวจสอบความพึงพอใจของลูกค้าของธนาคารทางอินเทอร์เน็ตในประเทศมาเลเซีย ใช้สมมติฐานดังนี้ กลยุทธ์การตลาด, พนักงานและความรู้, การรักษาความปลอดภัยและความน่าเชื่อถือของเว็บไซต์ โดยใช้กลุ่มตัวอย่าง 500 คน และ แบบสอบถาม 172 แบบสอบถาม ผลการสำรวจพบว่า พนักงานและความรู้ มีความสำคัญต่อ การให้บริการธนาคารทางอินเทอร์เน็ตในประเทศมาเลเซีย

สุวรรณี ธูปจีน และคณะ [46] ได้ทำการศึกษาการตรวจจับพฤติกรรมและป้องกันมัลแวร์บนโทรศัพท์มือถือแอนดรอยด์ ซึ่งผู้วิจัยได้พบว่าการแพร่กระจายของมัลแวร์ได้มีอัตราการเพิ่มขึ้นส่งผลกระทบต่อผู้ใช้งานและความปลอดภัยของข้อมูล ดังนั้นในงานวิจัยนี้จึงได้นำเสนอวิธีการตรวจจับพฤติกรรมของมัลแวร์ โดยทำการวิเคราะห์ตัวอย่างของสายพันธุ์มัลแวร์บางสายพันธุ์ที่สามารถตรวจพบได้บนสมาร์ทโฟนแอนดรอยด์ ซึ่งผลการวิเคราะห์สรุปได้ว่ามัลแวร์บางสายพันธุ์สามารถถูกจับได้โดยโปรแกรมสแกนไวรัสหรือผู้ใช้สามารถสังเกตเห็นได้จากอาการผิดปกติของโทรศัพท์ ภัยคุกคามจากมัลแวร์บนระบบปฏิบัติการแอนดรอยด์นั้น ได้ส่งผลให้เกิดความเสียหายต่อผู้ใช้งาน ดังนั้นผู้ใช้งานควรหลีกเลี่ยงการดาวน์โหลดแอปพลิเคชันจากแหล่งที่ไม่ปลอดภัย หลีกเลี่ยงทำธุรกรรมการเงินผ่านอุปกรณ์ที่ทำการดัดแปลง (Jailbreak) ติดตั้งโปรแกรม Antivirus และอัพเดทสม่ำเสมอ เพื่อลดความเสี่ยงจากภัยคุกคามบนโทรศัพท์มือถือ ซึ่งจะใช้ในการศึกษาและวิเคราะห์พฤติกรรมของผู้ใช้สมาร์ทโฟนที่ส่งต่อปัญหามัลแวร์ของกลุ่มผู้ใช้งานแอปพลิเคชันบนสมาร์ทโฟน (Smartphone Application)

ซึ่งงานวิจัยกลุ่มนี้ ได้นำเสนองานวิจัยด้านปัญหาความมั่นคงเกี่ยวกับระบบ m-banking ซึ่งเน้นทางด้านเทคนิคเท่านั้น ยังขาดการสำรวจด้านการจัดการหรือด้านความปลอดภัยของระบบ m-banking ที่สำคัญงานเหล่านั้น ยังขาดการสังเกตการณ์จากกรณีจริง การศึกษาวิเคราะห์กรณีคดีการโจมตีระบบธนาคารที่เกิดก่อนหน้านี้ และการทดลองทดสอบการโจมตีจากฝั่งของผู้ใช้จริง ดังนั้น บทความนี้จึงทำการวิเคราะห์ระบบ m-banking ทั้งด้านความมั่นคงและความปลอดภัย และครอบคลุมประเด็นที่ขาดไปที่ได้กล่าวไว้ในขั้นต้น จากงานวิจัยก่อนหน้านี้ สามารถนำมาสรุปเป็นตารางเปรียบเทียบในแต่ละประเด็นได้ดัง ตารางที่ 2.3

ตารางที่ 2.3 เปรียบเทียบประเด็นด้านความปลอดภัยและความมั่นคงของงานวิจัยที่เกี่ยวข้อง

งานวิจัย	ด้านความปลอดภัย การบริหารจัดการ	ด้านความมั่นคง เทคนิคการโจมตี
การสำรวจการรักษาความปลอดภัยในการใช้งานอินเทอร์-เน็ตแบงค์กิ้งธนาคารพาณิชย์ไทยสำหรับลูกค้าบุคคล [7]	√	
Analysis of Authentication Methods for Smartphone Banking Service using ANP [3]		√
การวิเคราะห์ปัญหาและการทดสอบความมั่นคงของเทคโนโลยีรหัสผ่านแบบใช้ครั้งเดียว [41]		√
การวิเคราะห์ความมั่นคงและปลอดภัยของระบบอินเทอร์เน็ตแบงก์กิ้งในประเทศไทย [2]	√	√
Security and Safety Evaluation and Enhancement of Internet Banking System: A Case Study of Cambodian Public Bank Plc [6]	√	√
A comparative analysis of the security of internet banking in Australia [43]		√
รายงานผลการวิจัยมาตรการรักษาความมั่นคงปลอดภัยระบบ Internet Banking และ ระบบ Mobile Banking ของธนาคารในประเทศไทย [1]		√
(In)Security of Mobile Banking and of Other [4]		√
Security Analysis Of Mobile Two-Factor Authentication Schemes [5]	√	√
Technology Trust and Mobile Banking Satisfaction: A Case of Malaysian Consumers [44]	√	
Customer Satisfaction Towards Internet Banking Services: Case Analysis on a Malaysian Bank [45]	√	
การตรวจจับพฤติกรรมและป้องกันมัลแวร์บนโทรศัพท์มือถือแอนดรอยด์ [46]		√

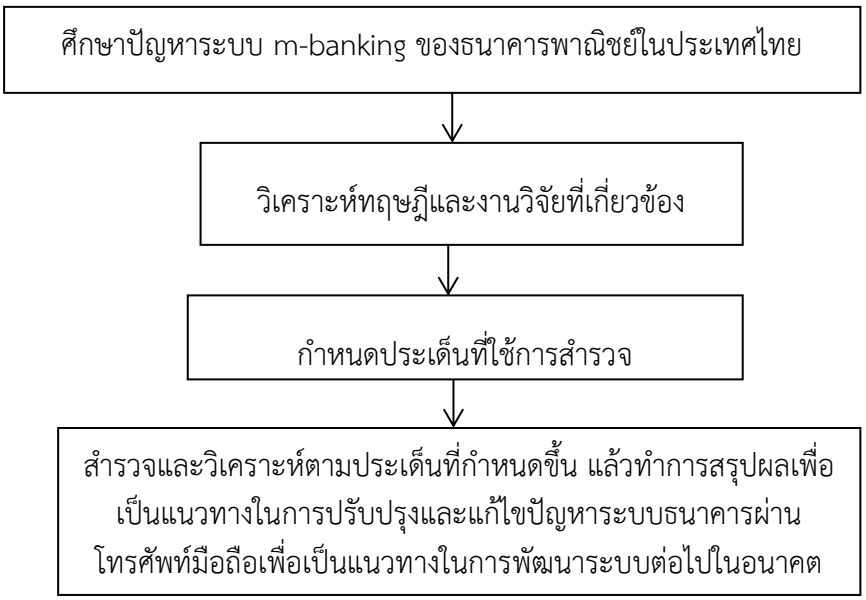
บทที่ 3

วิธีดำเนินการวิจัย

การศึกษาค้นคว้าอิสระนี้ได้เสนอการวิเคราะห์ความปลอดภัยและความมั่นคงระบบธนาคารผ่านโทรศัพท์มือถือ (m-banking) ของธนาคารพาณิชย์ในประเทศไทยในส่วนของผู้ใช้งานทั่วไป โดยเลือกกรณีศึกษาเป็นระบบ m-banking ของ 6 ธนาคาร ดังนี้ 1) K-Mobile Banking PLUS ของธนาคารกสิกรไทย 2) KTB netbank ของธนาคารกรุงไทย 3) SCB Easy Net ของธนาคารไทยพาณิชย์ 4) TMB Touch ของธนาคารทหารไทย 5) Bualuang mbanking ของธนาคารกรุงเทพ 6) Krungsri Mobile ของธนาคารกรุงศรีอยุธยา โดยเลือกจากธนาคารที่ก่อตั้งในประเทศไทยที่มีระยะเวลายาวนานที่มีคนนิยมใช้มากที่สุด [9] ในการวิเคราะห์และสำรวจ ได้ทำในช่วงวันที่ 1-31 ธันวาคม พ.ศ. 2558 โดยการแสดงผลการวิเคราะห์จะใช้ตัวอักษรภาษาอังกฤษ A - F แทนชื่อธนาคารที่เป็นกรณีศึกษา เพื่อป้องกันการเปิดเผยจุดอ่อนของธนาคารที่เป็นกรณีศึกษาแบบเฉพาะเจาะจง อันอาจเป็นการชี้ช่องทางแก่มิจฉาชีพ

ซึ่งการศึกษาค้นคว้าอิสระนี้จะวิเคราะห์ระบบ m-banking ทั้งด้านความปลอดภัยและด้านความมั่นคง รวมทั้งสำรวจผู้ให้บริการเครือข่าย และวิเคราะห์พฤติกรรมของผู้ใช้สมาร์ทโฟนที่ส่งผลต่อปัญหามัลแวร์ โดยในการทดสอบของการศึกษานี้ ได้ใช้บัญชีธนาคาร ซิมการ์ด และสมาร์ทโฟนของทีมวิจัยในการทดลอง เพื่อไม่เป็นการกระทำผิดต่อกฎหมายต่อผู้อื่น

3.1 ภาพรวมการดำเนินการศึกษา



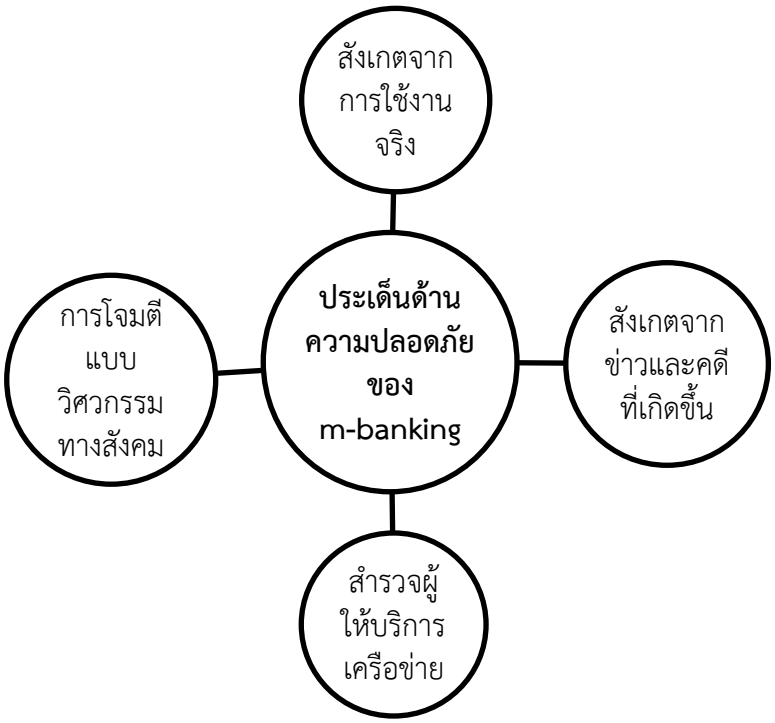
รูปที่ 3.1 ภาพรวมของการศึกษาค้นคว้าอิสระ

จาก รูปที่ 3.1 ได้แสดงถึงภาพรวมขั้นตอนการวิเคราะห์ระบบ m-banking ของธนาคารพาณิชย์ในประเทศไทย โดยได้ทำการศึกษาและวิเคราะห์ปัญหาต่างๆ ที่เกิดขึ้นในช่วง 3-4 ปีที่ผ่านมาจากข่าวและคดีที่เกิดขึ้นจริง และได้ทำการวิเคราะห์ทฤษฎีและงานวิจัยต่างๆ ที่เกี่ยวข้องเพื่อจะนำมากำหนดเป็นประเด็นในการวิเคราะห์การรักษาความมั่นคงและความปลอดภัยของการทำธุรกรรมทางการเงินผ่านโทรศัพท์มือถือ ในประเด็นต่างๆ พร้อมทั้งสรุปผลการศึกษาเพื่อนำมาเป็นแนวทางในการปรับปรุงและแก้ไขปัญหาระบบธนาคารผ่านโทรศัพท์มือถือในการพัฒนาระบบ m-banking ต่อไปในอนาคต

3.2 ด้านความปลอดภัยของ m-banking

ประเด็นที่มาใช้ในการวิเคราะห์ดังต่อไปนี้ 1) การเปิดบัญชีธนาคาร 2) การสมัครใช้งานระบบ m-banking 3) การ Login เข้าสู่ระบบ 4) การ Reset ข้อมูล 5) การเปลี่ยนเบอร์มือถือ 6) ลักษณะของ OTP 7) การเชื่อมต่ออินเทอร์เน็ต 8) มาตรการด้านความปลอดภัยอื่นๆ 9) การยกเลิกการใช้บริการระบบ m-banking 10) การปิดบัญชี

โดยจะนำประเด็นที่กำหนดไปใช้ในการสำรวจและวิเคราะห์ลักษณะการโจมตีแบบวิศวกรรมสังคม โดยใช้เทคนิคทางจิตวิทยา ที่คนร้ายมักใช้วิธีนี้เป็นส่วนใหญ่จากคดีความที่เกิดขึ้น เพราะเป็นวิธีที่ง่ายที่สุดและป้องกันได้ยาก เช่น การสร้างหลักฐานปลอมเพื่อขอเปิดบัญชีธนาคารที่มีชื่อเหมือนกันกับเหยื่อ แล้วสวมรอยขโมยเงินในบัญชี เป็นต้น ดังนั้นงานวิจัยนี้จึงได้ทำการศึกษาและวิเคราะห์เกี่ยวกับคดีต่างๆ ที่เกิดขึ้นจริงในประเทศไทย ซึ่งสรุปได้ดังรูปที่ 3.2



รูปที่ 3.2 ประเด็นที่นำมาใช้ในการวิเคราะห์ด้านความปลอดภัยของ m-banking

1) การเปิดบัญชีธนาคาร

ในขั้นตอนการสำรวจการเปิดบัญชีธนาคารใหม่นั้นต้องใช้เอกสารหลักฐานแนบในการสมัครด้วย ปัจจุบันทางธนาคารได้ให้ความสำคัญกับการเปิดบัญชีด้วยตนเองและมีการตรวจสอบเอกสารหลักฐานที่แนบมาด้วย ในขั้นตอนนี้ผู้วิจัยจึงนำมากำหนดเป็นเกณฑ์ในการวิเคราะห์ในการสำรวจด้านการตรวจสอบเอกสารหลักฐานที่ใช้ในการเปิดบัญชีธนาคาร ว่าแต่ละธนาคารเจ้าหน้าที่ได้มีการตรวจสอบเอกสารอย่างถูกต้องหรือไม่ มีช่องโหว่ให้มิจฉาชีพสามารถสวมรอยเป็นเจ้าของบัญชีโดยการปลอมแปลงเอกสารหรือจุดบกพร่องของเจ้าหน้าที่ธนาคารในการเปิดบัญชีหรือไม่ ซึ่งเกณฑ์ที่ใช้ในการสำรวจมีดังนี้

(1) บัตรประจำตัวประชาชน
(2) ใบอนุญาตขับรถและทะเบียนบ้าน
(3) บัตรข้าราชการและทะเบียนบ้าน
(4) Passport (กรณีชาวต่างชาติ)

การสำรวจลักษณะและขั้นตอนการให้บริการของเจ้าหน้าที่ธนาคาร การตรวจสอบเอกสารหลักฐานที่ใช้ในการสมัคร ที่จะเป็นช่องโหว่ให้มิจฉาชีพเข้ามาสวมรอยเป็นเจ้าของบัญชีตัวจริง ดังนั้นผู้วิจัยจึงทำการเปิดบัญชีใหม่ทั้ง 6 ธนาคาร เพื่อสังเกตการณ์การให้บริการของเจ้าหน้าที่

2) การสมัครใช้งาน m-banking

การสมัครใช้งานระบบ m-banking เป็นขั้นตอนการตรวจสอบเอกสารหลักฐานในการใช้สมัครแล้วมีการยืนยันตัวตนผู้ใช้งานด้วย โดยมิจฉาชีพมักจะปลอมตัวเป็นเจ้าของบัญชีเพื่อขโมยเงิน โดยใช้วิธีการโจมตีแบบจิตวิทยาซึ่งการโจมตีลักษณะนี้มิจฉาชีพชอบใช้ เพราะเป็นวิธีการที่ทำได้ง่าย โดยผู้วิจัยได้กำหนดเกณฑ์ในการสำรวจข้อมูลดังนี้

(1) สมัครที่ธนาคาร
(2) สมัครผ่านทางแอปพลิเคชัน
(3) สมัครที่ตู้เอทีเอ็ม

โดยผู้วิจัยได้ทำการสมัครใช้งานระบบ m-banking ทั้ง 6 ธนาคาร แล้วสังเกตขบวนการที่ธนาคารใช้ยืนยันตัวตนของแต่ละวิธีว่าช่องทางไหนมีความปลอดภัยต่างกันอย่างไร

3) การ Login เข้าสู่ระบบ

ในขั้นตอนสำรวจลักษณะการ Login ก่อนเข้าสู่ระบบ โดยใช้ชื่อผู้ใช้ รหัสผ่านและรหัส PIN เพื่อให้ผู้ใช้งานที่ใช้บริการระบบ m-banking บนสมาร์ทโฟน มั่นใจว่าระบบ m-banking ทั้ง 6 ธนาคาร มีการรักษาความปลอดภัยมากน้อยเพียงใด โดยมีการใช้ชื่อผู้ใช้ รหัสผ่านและรหัส PIN หรือไม่ในการเปิดใช้งานแอปพลิเคชัน ว่ามีจุดอ่อนใดบ้างที่อาจทำให้มิจฉาชีพสามารถสวมรอยขโมยเงินในบัญชีได้มีเกณฑ์ที่ใช้สำรวจดังนี้

(1) เข้าสู่ระบบด้วย PIN Lock

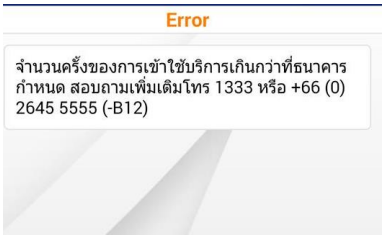
(2) Limit login PIN Lock

(3) เข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่าน

(4) Limit login ชื่อผู้ใช้และรหัสผ่าน

โดยผู้วิจัยได้ทำการทดลองและสำรวจการเข้าสู่ระบบด้วยชื่อผู้ใช้ รหัสผ่านและรหัส PIN ของแต่ละธนาคารว่ามีเงื่อนไขในลักษณะใดบ้าง ที่อาจเป็นช่องโหว่ให้มิจฉาชีพคาดเดาได้ง่ายและมีข้อดีข้อเสียอย่างไรบ้าง มีระบบป้องกันจำนวน User Login เข้าระบบ (Limit Login) ดัง รูปที่ 3.3 และ รูปที่ 3.4

รูปที่ 3.3 การใส่รหัส PIN Lock ก่อนเข้าสู่ระบบของธนาคาร



รูปที่ 3.4 การนำ Limit Login มาตรวจสอบการเข้าสู่ระบบ

โดยหัวข้อนี้ผู้วิจัยจะไปสำรวจโดยการตรวจสอบลักษณะการเข้าสู่ระบบของแต่ละธนาคาร โดยจะตรวจสอบความปลอดภัยของชื่อผู้ใช้ รหัสผ่านและรหัส PIN ว่าแต่ละธนาคารมีการกำหนดเงื่อนไขในลักษณะใดบ้าง มาใช้ตรวจสอบในการเข้าสู่ระบบว่ามีข้อดีหรือข้อเสียต่อผู้ใช้งานในด้านใดบ้าง

4) การ Reset ข้อมูล

ในขั้นตอนการสำรวจและศึกษาลักษณะเงื่อนไขการลืมชื่อผู้ใช้ รหัสผ่านและรหัส PIN ดังนี้

(1) Reset ผ่านสาขา

(2) Reset ผ่านคอลเซ็นเตอร์

(3) Reset ผ่านแอปพลิเคชัน

(4) Reset ผ่านตู้เอทีเอ็ม

โดยหัวข้อนี้ผู้วิจัยจะไปสำรวจลักษณะการชื่อผู้ใช้ รหัสผ่านและรหัส PIN ของแต่ละธนาคาร โดยจะตรวจสอบความปลอดภัยในแต่ละช่องทางของธนาคารว่าในแต่ละช่องทางมีข้อดีข้อเสียอย่างไร

รูปที่ 3.5 ลักษณะการ Reset Password

5) การเปลี่ยนเบอร์มือถือ

จากการสำรวจการเปลี่ยนเบอร์มือถือรับ OTP จากข่าวและคดีที่เกิดขึ้นในบทก่อนหน้านี้ พบว่ามิจฉาชีพได้อาศัยช่องโหว่นี้ในการสวมรอยขโมยเงินในบัญชี ดังนั้น OTP จึงมีความสำคัญในการยืนยันตัวตนในการทำธุรกรรมเป็นอย่างมาก เพราะฉะนั้นการจะเปลี่ยนข้อมูลในส่วนนี้จึงเป็นส่วนที่สำคัญ ซึ่งเกณฑ์ที่จะนำมาใช้ในการสำรวจในเรื่องของการเปลี่ยนเบอร์มือถือรับ OTP มีข้อมูลดังนี้

(1) Reset ผ่านสาขา

(2) Reset ผ่านคอลเซ็นเตอร์

(3) Reset ผ่านแอปพลิเคชัน

(4) Reset ผ่านตู้เอทีเอ็ม

โดยหัวข้อนี้ผู้วิจัยได้สำรวจตรวจสอบเมื่อต้องการเปลี่ยนเบอร์มือถือรับ OTP ของแต่ละธนาคารว่าแต่ละช่องทางมีข้อดีข้อเสียอย่างไร ตรวจสอบและวิเคราะห์ว่ามีช่องโหว่ที่สามารถถูกโจมตีมากที่สุดวิธีการที่มิจฉาชีพจะสวมรอยเปลี่ยน OTP เป็นเบอร์ของตัวเอง

6) ลักษณะของ OTP

จากการสำรวจลักษณะของ OTP จะเป็นการยืนยันตัวตนอีกชั้นเพื่อให้ผู้ใช้งานมั่นใจความปลอดภัยในการทำธุรกรรมต่างๆ ซึ่งเกณฑ์ที่จะใช้ในการสำรวจมีดังนี้

(1) ระยะเวลาของ OTP

(2) มี OTP ในการแจ้งการโอนเงิน

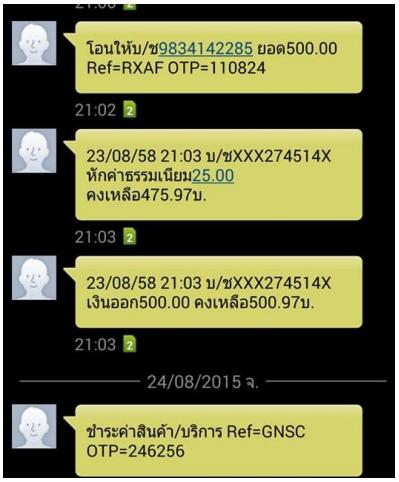
(3) มี OTP เมื่อเพิ่มบัญชีใหม่

(4) มี OTP แจ้งเปลี่ยนเบอร์มือถือ

(5) มี OTP แจ้งการชำระเงิน

(6) Limit OTP

โดยหัวข้อนี้ผู้วิจัยจะสำรวจตรวจสอบลักษณะ OTP ของในแต่ละธนาคารว่าการใช้งาน OTP ที่เพิ่มความปลอดภัยอีกชั้นหนึ่งนั้น มีช่องโหว่ที่จะสามารถโจมตีได้หรือไม่ ทั้งในเรื่องของระยะเวลาที่อาจจะเร็วไปหรือช้าไปมีข้อดีหรือข้อเสียอย่างไรบ้าง มี OTP ทุกครั้งที่ทำธุรกรรมหรือไม่ หรือในกรณีที่เคยทำธุรกรรมกับบัญชีเดิมต้องใส่ OTP อีกหรือไม่ เป็นต้น



รูปที่ 3.6 ลักษณะยืนยันการโอนเงินด้วยรหัส OTP

7) ลักษณะการเชื่อมต่ออินเทอร์เน็ต

ปัจจุบันแนวโน้มการใช้งานระบบ m-banking มีปริมาณเพิ่มขึ้น ซึ่งในแต่ละธนาคารได้มีการพัฒนาแอปพลิเคชันรองรับสำหรับการใช้งานระบบ m-banking โดยรองรับการใช้งานในหลายแพลตฟอร์ม โดยเกณฑ์ที่จะนำมาใช้ในการสำรวจมีข้อมูลดังต่อไปนี้

(1) เชื่อมต่อผ่านเทคโนโลยี 3G และ 4G

(2) เชื่อมต่อผ่านเทคโนโลยี Wi-Fi

โดยหัวข้อนี้ผู้วิจัยจะวิเคราะห์ตรวจสอบลักษณะการเชื่อมต่ออินเทอร์เน็ตผ่านเทคโนโลยีดังกล่าวในการใช้งานระบบ m-banking ว่ามีมาตรการป้องกันความปลอดภัยอย่างไร

8) มาตรการด้านความปลอดภัยอื่นๆ

ธนาคารมีมาตรการรักษาความปลอดภัยที่แตกต่างกันไปในการให้บริการ ซึ่งจากการสำรวจและวิเคราะห์สามารถนำข้อมูลมาใช้ในการสำรวจดังนี้

(1) มีการแจ้งเตือนการ Login
(2) สามารถตั้งค่าความปลอดภัยได้
(3) มีระบบ Auto Log Off
(4) รหัสลับทำธุรกรรม
(5) การแจ้งเตือนทำธุรกรรม

โดยหัวข้อนี้ผู้วิจัยจะสำรวจตรวจสอบลักษณะการใช้มาตรการความปลอดภัยอื่นๆ ที่แต่ละธนาคารมีไว้บริการ การใช้งานแต่ละครั้งมีการแจ้งเตือนผ่านอีเมล์หรือ SMS เมื่อเข้าสู่ระบบหรือไม่ เพื่อจะได้รู้ว่ามีคนอื่นแอบเข้าใช้งานหรือโดนมิจฉาชีพกำลังเข้าสู่ระบบอยู่หรือไม่ เพื่อจะได้หาทางแก้ไขป้องกันได้ทันเวลา แต่ละธนาคารมีการประกาศแจ้งเตือนภัยคุกคามต่างๆ ในปัจจุบันหรือไม่

9) การยกเลิกใช้บริการระบบ m-banking

ในการยกเลิกการใช้งานระบบ m-banking มีเกณฑ์ที่จะใช้ในการสำรวจมีข้อมูลดังต่อไปนี้

(1) ยกเลิกผ่านสาขา
(2) ยกเลิกผ่านคอลเซ็นเตอร์
(3) ยกเลิกผ่านแอปพลิเคชัน
(4) ยกเลิกผ่านตู้เอทีเอ็ม

โดยหัวข้อนี้ผู้วิจัยจะสำรวจเมื่อต้องการยกเลิกการใช้งานระบบ m-banking ของในแต่ละธนาคารว่าแต่ละช่องทางมีข้อดีข้อเสียอย่างไร

10) การปิดบัญชี

ในการปิดบัญชีของธนาคาร มีเกณฑ์ที่จะใช้ในการสำรวจมีข้อมูลดังต่อไปนี้

(1) ปิดบัญชีที่ธนาคารสาขาที่เปิดบัญชี
(2) ปิดบัญชีที่ธนาคารต่างสาขา
(3) บัตรประชาชนและสมุดบัญชี
(4) บัตรประชาชนและใบแจ้งความ

โดยหัวข้อนี้ผู้วิจัยจะสำรวจเมื่อต้องการปิดบัญชีในของในแต่ละธนาคารว่าแต่ละช่องทางมีข้อดีข้อเสียอย่างไรบ้าง การแสดงผลการทดสอบการรักษาความมั่นคงและปลอดภัยของระบบ m-banking

การแสดงผลการสำรวจและวิเคราะห์ความมั่นคงและความปลอดภัยของระบบ m-banking ของธนาคารพาณิชย์ในประเทศไทย จะแสดงผลในรูปแบบของตารางและมีการกำหนดเครื่องหมายแสดงผลการทดสอบอย่างชัดเจน โดยจะแสดงผลในการทดสอบใน 2 ด้านคือ ด้านความปลอดภัยของระบบ (Safety) และด้านความมั่นคงของระบบ (Security) โดยมีรายละเอียดดังต่อไปนี้

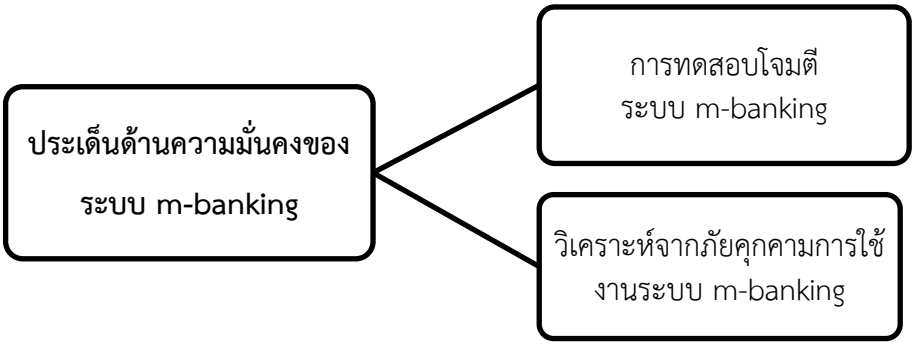
การแสดงผลการทดสอบด้านความปลอดภัยจะกำหนดให้เครื่องหมาย √ หมายถึง มีมาตรการป้องกันความปลอดภัย ดัง ตารางที่ 3.1

ตารางที่ 3.1 ตัวอย่างตารางที่ใช้ในการแสดงผลด้านความปลอดภัยของ m-banking

ประเด็นที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	ธนาคาร A	ธนาคาร B	ธนาคาร C	ธนาคาร D	ธนาคาร E	ธนาคาร F
เงื่อนไขการสำรวจ	√	√	√	√	√	√

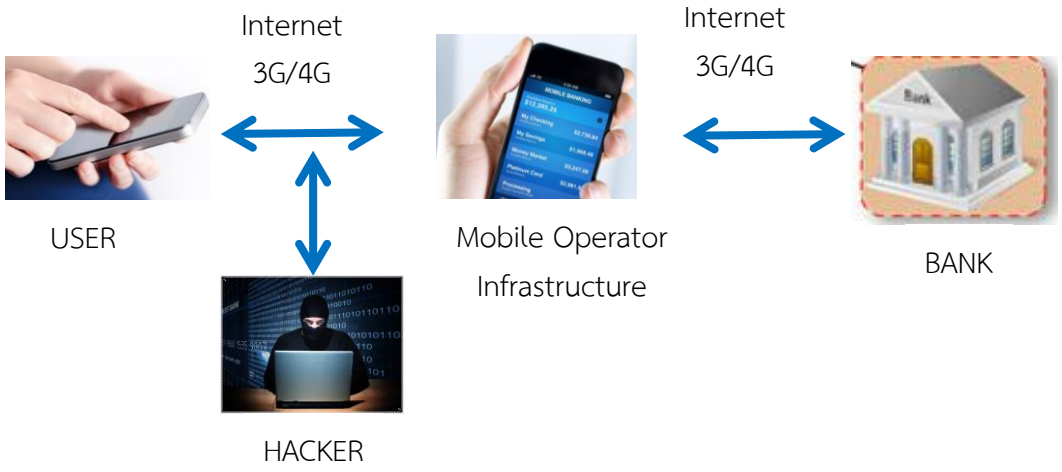
3.3 ด้านความมั่นคงของ m-banking

โดยประเด็นที่นำมาวิเคราะห์ด้านความมั่นคงผู้วิจัยได้ศึกษามาจากภัยคุกคามของระบบ m-banking ซึ่งมีหลากหลายเทคนิคในการโจมตี แต่ในงานวิจัยนี้จะเลือกเทคนิควิธีที่แฮกเกอร์นิยมใช้เจาะระบบมากที่สุด ในช่วง 3-4 ปีที่ผ่านมาดัง รูปที่ 3.7



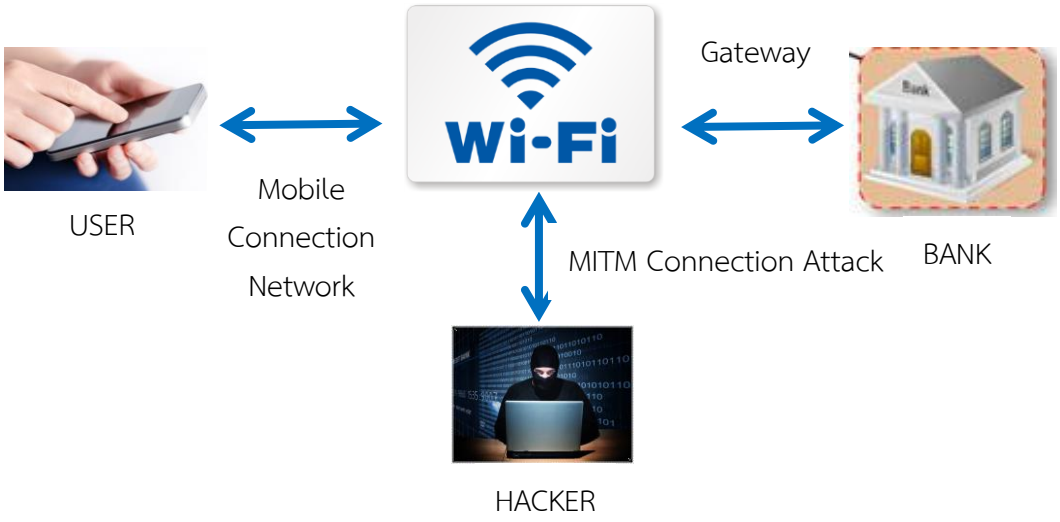
รูปที่ 3.7 ประเด็นที่จะใช้ในการวิเคราะห์ด้านความมั่นคงของ m-banking

1) วิเคราะห์สถานการณ์จำลองการโจมตีระบบ m-banking



รูปที่ 3.8 วิเคราะห์โครงสร้างการโจมตีระบบ m-banking ผ่าน 3G และ 4G

จากรูปที่ 3.8 การทดสอบโดยใช้งานแอปพลิเคชันของธนาคาร บนระบบปฏิบัติการ iOS และ Android พบว่ามีการรับส่งข้อมูลผ่านโพรโทคอล HTTPS เพราะส่งข้อมูลได้รวดเร็ว ซึ่งการรับส่งบนเครือข่าย 3G และ 4G ยังมีความเสี่ยงไม่มากนัก ทำให้มีความปลอดภัยสูง เนื่องจากเทคนิคการดักจับข้อมูลบนเครือข่าย 3G และ 4G นั้นไม่สามารถทำได้โดยง่ายเพราะเทคโนโลยี 3G มีมาตรฐานความปลอดภัยโดยใช้ KASUMI Block Cipher อัลกอริทึม UEA1/UIA1 [47] ซึ่งพบว่ายังมีจุดอ่อนอยู่แต่ไม่สามารถถอดรหัสข้อมูลได้ ในส่วนของเทคโนโลยี 4G จะมีมาตรฐานความปลอดภัยที่สูงกว่า โดยใช้ SNOW 3G Stream Cipher อัลกอริทึม UEA2/UIA2 ซึ่งมีการเข้ารหัสแบบ Symmetric – Key โดยจะตรวจสอบในส่วนของโทรศัพท์และการเข้ารหัสข้อมูลที่ส่งผ่านการเชื่อมต่อเครือข่าย 3G และ 4G ดังนั้นจึงมีความปลอดภัยสูงจากการดักจับข้อมูลของแฮกเกอร์ การดักจับข้อมูลจะทำได้ยาก แต่ก็ยังคงมีความเสี่ยงในส่วนของที่ผู้ให้บริการเครือข่ายโทรศัพท์ สามารถตรวจสอบการใช้งานของ User ได้ จากการศึกษาการทำธุรกรรมทางการเงินระบบธนาคารผ่านโทรศัพท์มือถือพบว่าการบริการ K – Mobile Banking ของธนาคารกสิกรไทย ให้ใช้การเชื่อมต่อเครือข่ายผ่านเทคโนโลยี 3G และ 4G เท่านั้น ไม่อนุญาตให้ทำการเชื่อมต่อผ่าน Wi-Fi เพื่อป้องกันการดักจับข้อมูลจากแฮกเกอร์เพราะมีความปลอดภัยสูง



รูปที่ 3.9 วิเคราะห์สถานการณ์จำลองการโจมตีระบบ m-banking ผ่าน Wi-Fi

จากรูปที่ 3.9 จะเห็นได้ว่าแฮกเกอร์สามารถโจมตีเครือข่าย LAN/Wi-Fi เพื่อเปลี่ยนเส้นทางการส่งข้อมูลโดยข้อมูลจะไหลผ่านเครื่องคอมพิวเตอร์ของแฮกเกอร์ ซึ่งในเทคนิคการขโมยข้อมูลที่เชื่อมต่อกันด้วยโพรโทคอล HTTPS นั้น แฮกเกอร์จะใช้เทคนิคการโจมตีด้วยวิธีแทรกกลางการสื่อสารและถอดรหัสลับข้อมูลได้ ซึ่งการเชื่อมต่อผ่าน Wi-Fi นั้น มีความเสี่ยงต่อการขโมยชื่อผู้ใช้และรหัสผ่านทำให้ไม่ปลอดภัยต่อการทำธุรกรรมทางการเงิน โดยผู้วิจัยจะทำการทดสอบโจมตีระบบ m-banking เพื่อหาวิธีการป้องกันและแก้ไขปัญหา

2) เครื่องมือที่ใช้ในการทดสอบระบบ

การศึกษาค้นคว้าอิสระนี้ได้ทำการทดสอบความมั่นคงของระบบ m-banking ทั้งหมด 6 ธนาคารโดยได้เลือกใช้เครื่องมือต่างๆ ซึ่งประกอบด้วยโปรแกรมที่ใช้เพื่อวัตถุประสงค์ในการแทรกกลางการสื่อสาร 2 โปรแกรมคือโปรแกรมที่ใช้ในการดักจับข้อมูลและโปรแกรมที่ใช้ในการโจมตี SSL ด้วยวิธีการ SSL Stripping Attack ซึ่งประกอบไปด้วยโปรแกรม Cain & Abel 4.9.5.6, Nmap 8.0, Kali Linux 3.12-Kali1-686-pae #1 SMP Debian 3.12.6-2kali1, Wireshark 1.12.8 โดยมีรายละเอียดการพิจารณาดังนี้

(1) Cain & Abel เป็นโปรแกรมที่สามารถรันได้ทั้งบน Windows NT/2000/XP และ Windows 7 มีความสามารถในการโจมตีแบบแทรกกลางการสื่อสารบนเว็บไซต์ที่มี HTTP และ HTTPS สามารถทำการถอดรหัสผ่านได้หลากหลายรูปแบบ เช่น ทำการดักข้อมูลรหัสผ่านจากเครือข่ายการแคร็กรหัสผ่านโดยใช้ Dictionary การแคร็กรหัสผ่านแบบ Brute-Force และการแคร็กรหัสผ่านแบบ Cryptanalysis Attacks นอกจากนี้ยังสามารถทำการบันทึกการสนทนาแบบ VoIP ทำการถอดรหัส Scrambled Passwords ทำการแสดงรหัสผ่านใน Password boxes ทำการค้นหารหัสผ่านต่างๆ ที่เก็บอยู่ในแคชได้อีกด้วย จากความสามารถที่หลากหลายและใช้งานง่าย จึงเป็นที่นิยมในกลุ่มของนักทดสอบระบบได้เป็นอย่างดี

(2) Kali Linux เป็นระบบปฏิบัติการที่ถูกสร้างมาเพื่อใช้ในการทดสอบการเจาะระบบเพื่อตรวจสอบหาความปลอดภัยของระบบต่างๆ โดยระบบปฏิบัติการ Kali Linux นี้ได้เตรียมเครื่องมือที่หลากหลายเอาไว้ให้ใช้ทดสอบระบบ ซึ่งงานวิจัยนี้ได้นำระบบปฏิบัติการ Kali Linux พร้อมเหล่าเครื่องมือดังต่อไปนี้มาเพื่อทดสอบ SSL Stripping Attack

(3) ARP Spoof ใช้ในการแทรกกลางการสื่อสาร

(4) Nmap ใช้สำหรับในการดักจับข้อมูลที่ถูกส่งระหว่างเครื่องไคลเอนต์และเซิร์ฟเวอร์ในขณะที่ถูกจู่โจมด้วยการถอด SSL

(5) Wireshark ชื่อเดิม Ethereal เป็นโปรแกรมจำพวก Packet Sniffer ประกอบไปด้วยส่วนของ Packet Capture และ Packet Analyzer โดยทำหน้าที่ในการวิเคราะห์ระบบ Network โดย Wireshark นั้นสามารถทำงานได้ทั้งระบบปฏิบัติการ Linux, Window และ OSX สามารถทำการวิเคราะห์ข้อมูลบนเครือข่ายได้หลากหลายรูปแบบ Wireshark นั้นเป็นซอฟต์แวร์แบบ Open Source หรือ Freeware สามารถใช้งานได้ฟรี

3) ระบบปฏิบัติการของโทรศัพท์สมาร์ทโฟน

การศึกษานี้จะทำการทดสอบการโจมตีบนแพลตฟอร์มของ iOS และ Android โดยจะทำการเลือกการทดสอบกับระบบปฏิบัติการที่มีผู้นิยมใช้มากที่สุดของประเทศไทยในปัจจุบัน 2 ระบบปฏิบัติการดังนี้

(1) iOS เป็นระบบปฏิบัติการที่ถูกพัฒนาโดยบริษัท Apple อุปกรณ์สื่อสารภายใต้ยี่ห้อ Apple ที่มีผู้นิยมใช้มากที่สุด งานวิจัยนี้ได้เลือกเวอร์ชันที่ใหม่ที่สุดมาทดสอบ คือเวอร์ชัน 8.4 โดยเลือกทำการทดสอบบนเครื่อง iPhone 5S ของระบบปฏิบัติการ iOS

(2) Android เป็นระบบปฏิบัติการที่ถูกพัฒนาโดยบริษัท Google ซึ่งเป็นระบบปฏิบัติการแบบ Open Source ซึ่งเป็นระบบปฏิบัติการแบบเปิดที่มีผู้ใช้งานมากที่สุด ซึ่งใน

งานวิจัยนี้ได้เลือกใช้รุ่นล่าสุดในการทดสอบคือเวอร์ชัน 4.4.2 โดยเลือกทดสอบบนเครื่อง Sumsung galaxy S4 ของระบบปฏิบัติการ Android

3.4 ด้านความปลอดภัยของผู้ให้บริการ Mobile Sim

จากข่าวคดีความ เรื่องการขอออกซิมโทรศัพท์มือถือใหม่ จนนำไปสู่การจู่โจมระบบธนาคาร ดังที่ได้กล่าวมาก่อนหน้านี้ งานวิจัยนี้จึงได้ทำการทดสอบ ผู้ให้บริการเครือข่ายโทรศัพท์มือถือ 3 ราย คือ TRUE, DTAC, AIS ในขั้นตอนการขอออกซิมใหม่ การขอเปลี่ยนซิม เพื่อหาจุดอ่อนและช่องโหว่ของเจ้าหน้าที่ ซึ่งทำให้มิจฉาชีพอาจแอบสวมรอย ดังที่เป็นข่าว [48] โดยทีมวิจัยได้ทดลองใช้เบอร์โทรศัพท์ของตนในการทดลอง เพื่อหลีกเลี่ยงการกระทำผิดกฎหมาย การแสดงผลการสำรวจผู้ให้บริการเครือข่าย ดัง ตารางที่ 3.2

ตารางที่ 3.2 ผลการสำรวจผู้ให้บริการ Mobile Sim

ประเด็นที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	TRUE	DTAC	AIS
เงื่อนไขการสำรวจ	√	√	√

3.5 ด้านการวิเคราะห์พฤติกรรมของผู้ใช้ Smartphone

มัลแวร์เป็นภัยคุกคามสำคัญสำหรับ Mobile Application และระบบ m-banking ดังที่ได้กล่าวไว้ในหลายงานวิจัยก่อนหน้านี้ [1, 46] ดังนั้นการศึกษาค้นคว้านี้ จึงได้ออกแบบสอบถาม เพื่อสำรวจพฤติกรรมของผู้ใช้งานสมาร์ทโฟน เพื่อศึกษาพฤติกรรมที่ส่งผลต่อปัญหามัลแวร์

1) ประชากร

ประชากรคือ กลุ่มคนที่อาจเป็นลูกค้าของ ระบบ m-banking ซึ่งในการศึกษาค้นคว้านี้ นิยามไว้เป็นกลุ่มผู้ใช้งานแอปพลิเคชันบนโทรศัพท์มือถือ ซึ่งจะมีความสามารถในการใช้ระบบ m-banking ได้ต่อไป และมีอายุ 15 ปีขึ้นไป ซึ่งเป็นอายุที่สามารถสมัครเปิดบัญชีธนาคารได้ การสุ่มตัวอย่าง ใช้วิธีการสุ่มอย่างง่าย โดยการใช้แบบสอบถามที่กรอกผ่านระบบออนไลน์ โดยได้มีผู้ตอบแบบสอบถามและมีคุณสมบัติใช้ได้ ทั้งหมด 481 คน

2) เครื่องมือในการวิจัย

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลเพื่อการวิจัยเชิงสำรวจครั้งนี้ เป็นการใช้แบบสอบถามทั้งปลายปิด ที่ผ่านการตรวจสอบความเที่ยงตรงของเนื้อหาและภาษาที่ใช้ (IOC) จากผู้เชี่ยวชาญด้านระบบเครือข่ายคอมพิวเตอร์ซึ่งมีทั้งหมด 3 ท่าน คือ (1) ผู้อำนวยการฝ่ายเครือข่ายของธนาคารแห่งหนึ่ง (2) พนักงานสอบสวนชำนาญการฝ่ายคดีเทคโนโลยีสารสนเทศ (DSI) (3) ผู้เชี่ยวชาญ

(1) แบบสอบถามมีทั้งหมด 1 ส่วนดังนี้

ตอนที่ 1 คำถามเกี่ยวกับลักษณะพฤติกรรมของผู้ใช้งานสมาร์ทโฟน

(2) ขั้นตอนการสร้างมือ

ขั้นตอนการสร้างแบบสอบถามเพื่อใช้ในการวิเคราะห์พฤติกรรมของผู้ใช้งานสมาร์ทโฟนมีขั้นตอนการดำเนินการ ดังนี้

(2.1) กำหนดวัตถุประสงค์ และเป้าหมายของสอบถาม

(2.2) ทำการร่างแบบสอบถาม

(3) นำไปให้ผู้เชี่ยวชาญตรวจสอบความเที่ยงตรงตามเนื้อหา (Content Validity) คือ การที่คำถามในแบบสอบถาม มีความครอบคลุมวัตถุประสงค์หรือพฤติกรรมที่ต้องการวัดหรือไม่ ค่าสถิติที่ใช้ในการหาคุณภาพ คือ ค่าความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์หรือเนื้อหา (Index of item Object Congruence: IOC) หรือดัชนีความเหมาะสม [42] โดยให้ผู้เชี่ยวชาญประเมินเนื้อหาของคำถามเป็นรายข้อ โดยคำนวณตามสูตรการหาค่าความเชื่อมั่น โดยได้ค่า IOC ของแต่ละข้ออยู่ระหว่าง 0.6-1.00

$$\mathrm{IOC} = \frac{\sum \mathrm{R}}{\mathrm{N}} \qquad (3.1)$$

เมื่อ IOC คือ ความสอดคล้องระหว่างวัตถุประสงค์กับแบบทดสอบ

∑R คือ ผลรวมจากการพิจารณาจากผู้เชี่ยวชาญ

N คือ จำนวนผู้เชี่ยวชาญ

(4) ทำการปรับปรุงความเหมาะสม การใช้ถ้อยคำและนำไปใช้จริง

3) การสร้างเครื่องมือเพื่อใช้ในการศึกษา

ขั้นตอนนี้เป็นการสร้างแบบสอบถาม เพื่อทำการสอบถาม โดยมีกลุ่มตัวอย่างคือ กลุ่มผู้ใช้งานสมาร์ทโฟน ซึ่งได้นำเสนอวิธีวิเคราะห์หาค่า IOC ซึ่งเป็นเครื่องมือในการศึกษาและวิเคราะห์ลักษณะพฤติกรรมของผู้ใช้งานสมาร์ทโฟน เป็นแบบสอบถามที่ผู้วิจัยสร้างขึ้นและสามารถตรวจสอบคุณภาพของเครื่องมือในเรื่องความตรงตามหัวข้อการวิจัยโดยให้ผู้เชี่ยวชาญตรวจสอบข้อคำถามที่ปรากฏในเครื่องมือแล้วนำมาหาค่า IOC ซึ่งเป็นการหาความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ มีค่าอยู่ระหว่าง 1 ถึง -1 ข้อคำถามที่มีความตรงตามเนื้อหาจะมีค่า IOC เข้าใกล้ 1.00 ถ้าข้อใดมีค่า IOC ต่ำกว่า 0.5 ควรจะปรับปรุง ซึ่งข้อคิดเห็นของผู้เชี่ยวชาญในการศึกษาค้นคว้าในครั้งนี้ ซึ่งถือได้ว่าแบบสอบถามเพื่อใช้ในการศึกษาของผู้วิจัยที่พัฒนาขึ้นนั้น มีความตรงของเนื้อหาและสามารถนำไปใช้สอบถามได้อย่างมีประสิทธิภาพ

4) การเก็บรวบรวมข้อมูล

ในการสำรวจผู้วิจัยจะแจกแบบสอบถามให้กลุ่มตัวอย่าง โดยผู้วิจัยจะทำการเก็บข้อมูลเฉพาะกลุ่มผู้ใช้งานสมาร์ทโฟน ระยะเวลาในการเก็บตัวอย่างประมาณ 8 สัปดาห์ เมื่อได้ข้อมูลครบถ้วนแล้ว จะตรวจสอบความถูกต้องของแบบสอบถามเพื่อทำการวิเคราะห์

3.6 ข้อจรรยาบรรณในการวิจัย

ด้วยข้อจรรยาบรรณ การศึกษาค้นคว้านี้เป็นการสำรวจเพื่อประเมินหาความเสี่ยงที่เกิดขึ้นจากช่องโหว่ที่ค้นพบ (Vulnerability Assessment) ในระบบ m-banking ของธนาคารพาณิชย์ในประเทศไทยไม่ได้เป็นการทดสอบการเจาะระบบ (Penetration Testing) เข้าไปในของระบบภายในของผู้ให้บริการแต่อย่างใด แต่จะเป็นการสำรวจและวิเคราะห์หาช่องโหว่และปัญหาในการใช้งานระบบในส่วนต่างๆ ที่ธนาคารให้บริการแก่ผู้ใช้งานทั่วไปเท่านั้นและสำรวจวิเคราะห์หาช่องโหว่ของผู้ให้บริการเครือข่ายโทรศัพท์มือถือ โดยทีมวิจัยได้ใช้สมุดบัญชี เบอร์โทรศัพท์ และอุปกรณ์สมาร์ทโฟนของตนในการทดลอง เพื่อหลีกเลี่ยงการกระทำผิดกฎหมาย

บทที่ 4

ผลการดำเนินงาน

การศึกษาค้นคว้าอิสระนี้ได้เสนอการวิเคราะห์ความปลอดภัยและความมั่นคงระบบธนาคารผ่านโทรศัพท์มือถือ (m-banking) ของธนาคารพาณิชย์ในประเทศไทยในส่วนของผู้ใช้งานทั่วไป โดยเลือกกรณีศึกษาเป็นระบบ m-banking ของ 6 ธนาคาร ดังนี้ 1) K-Mobile Banking PLUS ของธนาคารกสิกรไทย 2) KTB netbank ของธนาคารกรุงไทย 3) SCB Easy Net ของธนาคารไทยพาณิชย์ 4) TMB Touch ของธนาคารทหารไทย 5) Bualuang mbanking ของธนาคารกรุงเทพ 6) Krungsri Mobile ของธนาคารกรุงศรีอยุธยา โดยเลือกจากธนาคารที่ก่อตั้งในประเทศไทยที่มีระยะเวลายาวนานที่มีคนนิยมใช้มากที่สุด [9] ในการวิเคราะห์และสำรวจ ได้ทำในช่วงวันที่ 1-31 ธันวาคม พ.ศ. 2558 โดยการแสดงผลการวิเคราะห์จะใช้ตัวอักษรภาษาอังกฤษ A-F แทนชื่อธนาคารที่เป็นกรณีศึกษา เพื่อป้องกันการเปิดเผยจุดอ่อนของธนาคารที่เป็นกรณีศึกษาแบบเฉพาะเจาะจง อันอาจเป็นการชี้ช่องทางแก่มิจฉาชีพ

ซึ่งการศึกษานี้จะวิเคราะห์ระบบ m-banking ทั้งด้านความปลอดภัยและด้านความมั่นคง รวมทั้งสำรวจผู้ให้บริการเครือข่าย และวิเคราะห์พฤติกรรมของผู้ใช้สมาร์ทโฟนที่อาจส่งผลต่อปัญหามัลแวร์ โดยในการทดสอบของการศึกษานี้ ได้ใช้สมุดบัญชีธนาคาร ซิมการ์ด และสมาร์ทโฟนของทีมวิจัยในการทดลอง เพื่อไม่เป็นการกระทำผิดต่อกฎหมายต่อผู้อื่น

4.1 ผลด้านความปลอดภัยระบบ m-banking

ผลจากการสำรวจและการวิเคราะห์ด้านความปลอดภัยของระบบ m-banking ซึ่งสามารถสรุปผลได้ดังต่อไปนี้

4.1.1 การเปิดบัญชีธนาคาร

จากการสำรวจลักษณะของการเปิดบัญชีธนาคาร โดยทำการสำรวจขั้นตอนการเปิดบัญชีธนาคารและทำการเปิดบัญชีธนาคารของตนเองพร้อมทั้งนำเอกสารและหลักฐานต่างๆ เพื่อใช้ในการสมัครเปิดบัญชีธนาคาร และทำการสังเกตการณ์เปิดบัญชี ขบวนการตรวจสอบเอกสารและหลักฐานต่างๆ ของเจ้าหน้าที่ธนาคาร ทั้ง 6 ธนาคาร ซึ่งสามารถสรุปผลการสำรวจข้อมูลได้ดังนี้

ตารางที่ 4.1 ผลการสำรวจการเปิดบัญชีธนาคาร

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	**ธนาคาร A**	**ธนาคาร B**	**ธนาคาร C**	**ธนาคาร D**	**ธนาคาร E**	**ธนาคาร F**
1. ลักษณะการเปิดบัญชีธนาคาร						
1.1 บัตรประจำตัวประชาชน	√	√	√	√	√	√
1.2 ใบอนุญาตขับรถและทะเบียนบ้าน	√			√	√	√

ตารางที่ 4.1 ผลการสำรวจการเปิดบัญชีธนาคาร (ต่อ)

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	ธนาคาร A	ธนาคาร B	ธนาคาร C	ธนาคาร D	ธนาคาร E	ธนาคาร F
1.3 บัตรข้าราชการและทะเบียนบ้าน	√	√	√	√	√	√
1.4 Passport (กรณีชาวต่างชาติ)	√	√	√	√	√	√

จากตารางที่ 4.1 พบว่าลักษณะของการเปิดบัญชีธนาคารแต่ละธนาคารจะมีการตรวจสอบเอกสารและหลักฐานต่างๆ ในการสมัครอย่างละเอียด ซึ่งผู้ที่มาสมัครเปิดบัญชีธนาคารนั้นจะต้องมาดำเนินการด้วยตนเองพร้อมทั้งนำหลักฐานตัวจริงมาด้วย เพื่อป้องกันการมิจฉาชีพสวมรอยเปิดบัญชีธนาคาร ส่วนเจ้าหน้าที่ธนาคารที่ทำการเปิดบัญชีให้ลูกค้านั้น จะต้องมีการอนุญาตผ่านระบบจากผู้ที่รับผิดชอบก่อนทำการเปิดบัญชีให้แก่ลูกค้า เพื่อป้องกันการทุจริตของพนักงานธนาคารด้วย เนื่องจากมีการรับจ้างเปิดบัญชีซึ่งผิดกฎหมาย ธนาคารต่างๆจึงต้องมีนโยบายการป้องกันการทุจริตทั้งในส่วนของลูกค้าและเจ้าหน้าที่ธนาคาร ซึ่งกระบวนการในการสมัครของแต่ละธนาคารมีลักษณะดังต่อไปนี้

ธนาคาร A จากการสำรวจธนาคารทั้ง 3 สาขาพบว่า สาขาที่หนึ่งและสาขาที่สองในการเปิดบัญชีธนาคารต้องใช้บัตรประชาชนตัวจริง กรณีไม่มีบัตรประชาชนตัวจริงสามารถใช้ใบอนุญาตขับรถแทนได้พร้อมทั้งนำทะเบียนบ้านตัวจริงมาด้วยและสามารถใช้บัตรข้าราชการแทนได้พร้อมทั้งนำทะเบียนบ้านตัวจริงมาด้วย ส่วนสาขาที่สามจะต้องใช้บัตรประชาชนตัวจริงเท่านั้น กรณีชาวต่างชาติจะต้องยื่น Passport จะเห็นได้ว่าจากการสำรวจธนาคารทั้ง 3 สาขา พบว่าลักษณะการให้บริการจะแตกต่างกันและไม่เป็นรูปแบบเดียวกัน

ธนาคาร B จากการสำรวจธนาคารทั้ง 3 สาขาพบว่า สาขาที่หนึ่งในการเปิดบัญชีธนาคารต้องใช้บัตรประชาชนตัวจริงเท่านั้น สาขาที่สองและสาขาที่สามพบว่าในการเปิดบัญชีธนาคารต้องใช้บัตรประชาชนตัวจริง กรณีไม่มีบัตรประชาชนตัวจริงสามารถใช้บัตรข้าราชการได้จะต้องนำทะเบียนบ้านตัวจริงแนบมาด้วย กรณีชาวต่างชาติจะต้องยื่น Passport จะเห็นได้ว่าจากการสำรวจธนาคารทั้ง 3 สาขา พบว่าลักษณะการให้บริการจะแตกต่างกันและไม่เป็นรูปแบบเดียวกัน

ธนาคาร C จากการสำรวจธนาคารทั้ง 3 สาขาพบว่า สาขาที่หนึ่งและสาขาที่สองในการเปิดบัญชีธนาคารต้องใช้บัตรประชาชนตัวจริงเท่านั้น และสาขาที่สามพบว่าในการเปิดบัญชีธนาคารต้องใช้บัตรประชาชนตัวจริง กรณีไม่มีบัตรประชาชนตัวจริงสามารถใช้บัตรข้าราชการได้จะต้องนำทะเบียนบ้านตัวจริงแนบมาด้วย กรณีชาวต่างชาติจะต้องยื่น Passport จะเห็นได้ว่าจากการสำรวจธนาคารทั้ง 3 สาขา พบว่าลักษณะการให้บริการจะแตกต่างกันและไม่เป็นรูปแบบเดียวกัน

ธนาคาร D จากการสำรวจธนาคารทั้ง 3 สาขาพบว่า สาขาที่หนึ่งและสาขาที่สองในการเปิดบัญชีธนาคารต้องใช้บัตรประชาชนตัวจริงเท่านั้น กรณีไม่มีบัตรประชาชนตัวจริงสามารถใช้ใบอนุญาตขับรถและบัตรข้าราชการได้จะต้องนำทะเบียนบ้านตัวจริงหรือสำเนาทะเบียนบ้านแนบมาด้วย และสาขาที่สามพบว่าในการเปิดบัญชีธนาคารต้องใช้บัตรประชาชนตัวจริง กรณีไม่มีสามารถใช้ใบอนุญาตขับรถแทนได้ กรณีชาวต่างชาติจะต้องยื่น Passport จะเห็นได้ว่าจากการสำรวจธนาคารทั้ง 3 สาขา พบว่าลักษณะการให้บริการจะแตกต่างกันและไม่เป็นรูปแบบเดียวกัน

ธนาคาร E จากการสำรวจธนาคารทั้ง 3 สาขาพบว่า สาขาที่หนึ่งต้องใช้บัตรประชาชนตัวจริงเท่านั้น สาขาที่สองและสาขาที่สามพบว่า ต้องใช้บัตรประชาชนตัวจริง กรณีไม่มีบัตรประชาชนตัวจริงสามารถใช้ใบอนุญาตขับรถและบัตรข้าราชการได้จะต้องนำทะเบียนบ้านตัวจริงแนบมาด้วย กรณีชาวต่างชาติจะต้องยื่น Passport จะเห็นได้ว่าจากการสำรวจธนาคารทั้ง 3 สาขา พบว่าลักษณะการให้บริการจะแตกต่างกันและไม่เป็นรูปแบบเดียวกัน

ธนาคาร F จากการสำรวจธนาคารทั้ง 3 สาขาพบว่า สาขาที่หนึ่งและสาขาที่สองในการเปิดบัญชีธนาคารต้องใช้บัตรประชาชนตัวจริง กรณีไม่มีบัตรประชาชนตัวจริงสามารถใช้ใบอนุญาตขับรถแทนได้ บัตรข้าราชการจะต้องนำสำเนาทะเบียนบ้านมาด้วย ส่วนสาขาที่สามจะต้องใช้บัตรประชาชนตัวจริง หากไม่มีสามารถใช้บัตรอนุญาตขับรถแทนได้ กรณีชาวต่างชาติจะต้องยื่น Passport จะเห็นได้ว่าจากการสำรวจธนาคารทั้ง 3 สาขา พบว่าลักษณะการให้บริการจะแตกต่างกันและไม่เป็นรูปแบบเดียวกัน

จากการวิเคราะห์พบว่าในการเปิดบัญชีทุกธนาคารจะต้องใช้บัตรประชาชนในการยืนยันตัวตน มี 2 ธนาคารที่ไม่อนุญาตให้ใช้ใบอนุญาตขับรถและทะเบียนบ้าน และทุกธนาคารจะอนุญาตให้ใช้บัตรข้าราชการแต่ต้องยื่นควบคู่กับสำเนาทะเบียนบ้าน จะเห็นได้ทุกธนาคารจะให้ความสำคัญในการตรวจสอบหลักฐานที่ใช้ในการสมัคร แต่การให้บริการของแต่ละธนาคารไม่เป็นรูปแบบเดียวกัน ขาดมาตรฐานในการตรวจสอบการให้บริการของเจ้าหน้าที่ เนื่องจากมีข่าวที่เกิดขึ้นดังที่กล่าวมาแล้ว [30] โดยมิจฉาชีพอาศัยช่องโหว่ในการตรวจสอบเอกสารของเจ้าหน้าที่เข้าสวมรอยเปิดบัญชีธนาคาร โดยการใช้หลักฐานปลอม ซึ่งมีงานวิจัยในต่างประเทศ [6] พบว่ามีวิธีการที่รัดกุมกว่า โดยพนักงานจะต้องผ่านการฝึกอบรมการตรวจเอกสารก่อน ดังนั้นธนาคารควรมีมาตรการที่เป็นแนวทางเดียวกันและเพิ่มวิธีการยืนยันตัวตนที่เฉพาะเจาะจง เช่น การแสกนลายนิ้วมือ

4.1.2 การสมัครใช้งานระบบ m-banking

จากการสำรวจลักษณะการสมัครใช้งานระบบ m-banking ของธนาคารทั้ง 6 ธนาคาร พบว่าสามารถสมัครที่ธนาคาร สมัครผ่านแอปพลิเคชัน และสมัครผ่านตู้เอทีเอ็ม ซึ่งสามารถสรุปผลการสำรวจข้อมูลได้ดังนี้

ตารางที่ 4.2 ผลการสำรวจการสมัครใช้งานระบบ m-banking

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	**ธนาคาร A**	**ธนาคาร B**	**ธนาคาร C**	**ธนาคาร D**	**ธนาคาร E**	**ธนาคาร F**
2. การสมัครใช้งาน m-banking						
2.1 สมัครที่ธนาคาร	√	√	√	√	√	√
2.2 สมัครผ่านแอปพลิเคชัน				√		√
- แอปพลิเคชันและตู้เอทีเอ็ม	√	√	√		√	
- รหัส OTP		√	√		√	

ตารางที่ 4.2 ผลการสำรวจการสมัครใช้งานระบบ m-banking (ต่อ)

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	ธนาคาร A	ธนาคาร B	ธนาคาร C	ธนาคาร D	ธนาคาร E	ธนาคาร F
2.3 สมัครผ่านตู้เอทีเอ็ม	√	√	√	√	√	
- ยืนยันผ่านตู้เอทีเอ็ม	√					
- ยืนยันผ่านแอปพลิเคชัน		√	√		√	
2.4 แจ้งผลการสมัคร						
- E-mail		√	√	√	√	
- SMS	√		√			√

จากตารางที่ 4.2 พบว่าในการสมัครใช้งาน m-banking ทั้งหมด 6 ธนาคาร มี 6 ธนาคารที่สามารถขอสมัครใช้งานได้ที่ธนาคาร มี 6 ธนาคารที่สามารถสมัครผ่านแอปพลิเคชัน และมี 5 ธนาคารที่สามารถสมัครใช้งานผ่านตู้เอทีเอ็มได้ ซึ่งมีรายละเอียดดังไปนี้

ธนาคาร A สามารถสมัครได้ 3 ช่องทาง คือสมัครผ่านธนาคาร โดยเขียนแบบฟอร์มการสมัครกับเจ้าหน้าที่ธนาคาร พร้อมทั้งยื่นสมุดบัญชีเงินฝากและบัตรประชาชนเพื่อแสดงตัวตน กรณีที่ไม่มีบัตร ATM หรือสมัครผ่านแอปพลิเคชัน กรณีที่มีบัตร ATM สามารถกรอกข้อมูลหมายเลขบัตรประชาชน หมายเลขหน้าบัตร ATM และรหัสเอทีเอ็มหรือสมัครผ่านตู้ ATM ก็จะได้รหัส 8 หลักในการยืนยันตัวตนก็สามารถสมัครได้ด้วยตนเองและต้องยืนยันตัวตนที่ตู้เอทีเอ็มก่อนจึงจะสามารถใช้งานได้ แจ้งผลการสมัครผ่านทาง SMS

ธนาคาร B สามารถสมัครได้ 3 ช่องทาง คือสมัครผ่านธนาคารโดยเขียนแบบฟอร์มการสมัครกับเจ้าหน้าที่ธนาคาร พร้อมทั้งยื่นสมุดบัญชีเงินฝากและบัตรประชาชนเพื่อแสดงตัวตน กรณีที่ไม่มีบัตร ATM เพื่อขอรหัสสมัครบริการหรือสมัครผ่านแอปพลิเคชัน กรณีที่มีบัตร ATM ในการสมัครผ่านแอปพลิเคชันจะต้องขอรหัสสมัครบริการ 6 หลัก จากตู้ ATM ระบบจะส่งรหัสสมัครบริการ โดยจะได้รับรหัส OTP 6 หลักทาง SMS เพื่อใช้ในการสมัครหรือสมัครผ่านตู้ ATM จะต้องกรอกหมายเลขมือถือ 10 หลัก และใส่รหัส 6 หลักที่ได้รับทาง SMS ก็สามารถสมัครได้ด้วยตนเอง จะต้องยืนยันความเป็นเจ้าของด้วยการใช้บัตรและรหัสบัตร ATM ควบคู่กับรหัสสมัครบริการที่ได้จากการกดขอรับรหัสสมัครบริการบนแอปพลิเคชันบนมือถือ แจ้งผลการสมัครผ่านทาง E-mail

ธนาคาร C สามารถสมัครได้ 3 ช่องทาง คือสมัครผ่านธนาคารโดยเขียนแบบฟอร์มการสมัครกับเจ้าหน้าที่ธนาคาร พร้อมทั้งยื่นสมุดบัญชีและบัตรประชาชนเพื่อแสดงตัวตน กรณีที่ไม่มีบัตร ATM หรือสมัครผ่านแอปพลิเคชัน กรณีที่มีบัตร ATM สามารถกรอกเลขหน้าบัตรเอทีเอ็ม บัตรประชาชน เบอร์โทรศัพท์ และรหัสบัตรเอทีเอ็ม ระบบจะส่ง OTP มายังเบอร์โทรศัพท์เพื่อใช้ในการยืนยันตัวตนหรือสมัครผ่านตู้ ATM ก็จะได้รหัสสมัครบริการเพื่อยืนยันตัวตนผ่านแอปพลิเคชัน ก็สามารถสมัครได้ด้วยตนเองได้ แจ้งผลการสมัครผ่านทาง E-mail และ SMS

ธนาคาร D สามารถสมัครได้ 3 ช่องทาง คือสมัครผ่านธนาคารโดยเขียนแบบฟอร์มการสมัครกับเจ้าหน้าที่ธนาคาร พร้อมทั้งยื่นสมุดบัญชีและบัตรประชาชนเพื่อแสดงตัวตน กรณีที่ไม่มีบัตร ATM หรือสมัครผ่านแอปพลิเคชัน โดยกรอกเลขหน้าบัตรเอทีเอ็ม บัตรประชาชน รหัสบัตรเอทีเอ็ม วันเดือนปีเกิด และหมายเลขบัตรประชาชน กรณีที่มีบัตร ATM หรือสมัครผ่านตู้ ATM ก็สามารถสมัครได้ด้วยตนเอง แจ้งผลการสมัครผ่านทาง E-mail

ธนาคาร E สามารถสมัครได้ 3 ช่องทาง คือสมัครผ่านธนาคารโดยเขียนแบบฟอร์มการสมัครกับเจ้าหน้าที่ธนาคาร พร้อมทั้งยื่นสมุดบัญชีและบัตรประชาชนเพื่อแสดงตัวตน เพื่อขอรหัสประจำตัวลูกค้า (User ID) โดยจะส่งไปทางอีเมล์ที่ลงทะเบียนไว้และส่งรหัสลับแรกเข้า (PIN) มาทางไปรษณีย์ตามที่อยู่ที่ลงทะเบียนไว้ กรณีที่ไม่มีบัตร ATM หรือสมัครผ่านแอปพลิเคชัน โดยจะต้องใส่รหัสลับแรกเข้า (PIN) ใส่หมายเลขเบอร์มือถือเพื่อรับ OTP ยืนยันการทำธุรกรรม ระบบจะแสดงหน้าจอยืนยันการสมัครบริการผ่านตู้เอทีเอ็ม พร้อมทั้งพิมพ์ใบบันทึกรายการ (ATM Slip) ที่ระบุ "รหัสประจำตัวลูกค้า (User ID)" ซึ่งระบบกำหนดให้สำหรับการเข้าสู่บริการคู่กับ "รหัสลับแรกเข้า (PIN)" ที่ลูกค้าเป็นผู้กำหนดเอง หลังจากนั้นก็ใส่รหัสประจำตัวลูกค้า (User ID) และรหัสลับแรกเข้า (PIN) ผ่านแอปพลิเคชัน ระบบจะให้ใส่หมายเลขบัตรประชาชน เบอร์โทรศัพท์มือถือ และจะได้รับหมายเลข OTP ยืนยันการสมัครผ่าน SMS แจ้งผลการสมัครผ่านทาง E-mail

ธนาคาร F สามารถสมัครได้ 2 ช่องทาง คือกรณีที่ไม่มีบัตร ATM จะต้องสมัครผ่านเว็บไซต์ก่อนแล้วนำหมายเลขอ้างอิงมาขอยืนยันการสมัครที่ธนาคาร โดยนำสมุดบัญชีและบัตรประชาชนมาแสดงตัวตนหรือสมัครผ่านแอปพลิเคชัน โดยกรอกเลขหน้าบัตรเอทีเอ็ม วันที่หมดอายุบัตร วันเดือนปีเกิด หมายเลขบัตรประชาชน และเลขที่สมุดคู่ฝาก กรณีที่มีบัตร ATM ก็สามารถสมัครได้ด้วยตนเอง แจ้งผลการสมัครผ่านทาง E-mail

จากการวิเคราะห์พบว่ามี 2 ธนาคารที่สามารถสมัครผ่านแอปพลิเคชันได้ และมี 5 ธนาคารที่จะต้องขอรหัสสมัครบริการจากตู้เอทีเอ็มเพื่อใช้ยืนยันในการสมัครใช้งานผ่านแอปพลิเคชัน ซึ่งการสมัครใช้งานผ่านตู้เอทีเอ็มจะเป็นมาตรการรักษาความปลอดภัยขั้นสูงของธนาคาร ที่ใช้ยืนยันตัวตนความเป็นเจ้าของบัญชีซึ่งจะต้องใช้รหัสเอทีเอ็มควบคู่กับรหัสสมัครบริการและมี 2 ธนาคารที่มีจุดเด่นต่างจากธนาคารอื่นคือธนาคาร B จะกำหนดให้ใช้ 1 บัญชีสามารถใช้งานกับ 1 เบอร์โทรศัพท์เท่านั้น และธนาคาร C หากต้องการใช้งานในเครื่องอื่น หมายเลขอื่น จะต้องทำการอนุญาตขอเพิ่มอุปกรณ์ในการเข้าใช้งาน จะต้องขออนุญาตโดยใช้รหัส OTP จากเครื่องหลักเพื่อยืนยันการเพิ่มอุปกรณ์ ซึ่งข้อจำกัดที่เพิ่มมานี้ โดยการผูกระบบ m-banking ไว้ที่เครื่องโทรศัพท์มือถือ จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะการจะเข้าใช้งาน ต้องมีการยืนยันตัวตนด้วยการเป็นเจ้าของเบอร์โทรศัพท์มือถือนั้นจริง หรือถือครองโทรศัพท์ที่ติดตั้งระบบ m-banking เท่านั้น ดังนั้นแม้ว่าแฮกเกอร์จะทราบ PIN หรือ รหัสผ่านก็ไม่สามารถเข้าใช้งานได้ จะต้องทำการขโมยโทรศัพท์มือถือ หรือเบอร์โทรศัพท์ของลูกค้าด้วย จึงจะเข้าใช้งานได้

4.1.3 ลักษณะการ Login เข้าสู่ระบบ

จากการสำรวจลักษณะการ Login เข้าสู่ระบบ สามารถสรุปผลการสำรวจข้อมูลได้ดังนี้

ตารางที่ 4.3 ผลการสำรวจลักษณะการ Login เข้าสู่ระบบ

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	ธนาคาร A	ธนาคาร B	ธนาคาร C	ธนาคาร D	ธนาคาร E	ธนาคาร F
3. ลักษณะการ Login เข้าสู่ระบบ						
3.1 เข้าสู่ระบบด้วย PIN Lock		√	√		√	
3.2 Limit Login PIN Lock		3 ครั้ง	3 ครั้ง		3 ครั้ง	
3.3 เข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่าน	√			√		√
3.4 Limit Login ชื่อผู้ใช้และรหัสผ่าน	3 ครั้ง			3 ครั้ง		3 ครั้ง

จากตารางที่ 4.3 ผลการสำรวจลักษณะการใช้รหัส PIN ชื่อผู้ใช้ และรหัสผ่าน ก่อนการเข้าสู่ระบบ m-banking ทั้งหมด 6 ธนาคารพบว่ามี 3 ธนาคารที่กำหนดให้ใช้รหัส PIN ก่อนการเข้าสู่ระบบ และมี 3 ธนาคารที่ใช้ชื่อผู้ใช้และรหัสผ่านในการเข้าสู่ระบบ และมีระบบ Limit Log-in ที่จำกัดจำนวนครั้งในการใส่ PIN และชื่อผู้ใช้ และรหัสผ่าน ซึ่งมีรายละเอียดในแต่ละธนาคารดังนี้

ธนาคาร A พบว่าจะกำหนดให้ใส่ชื่อผู้ใช้และรหัสผ่านในการเข้าสู่ระบบ โดยมีเงื่อนไขในการตั้งชื่อผู้ใช้คือต้องมีความยาว 8-20 ตัวอักษรเท่านั้น โดยไม่ได้มีเงื่อนไขที่กำหนดในการใช้อักษรเล็กใหญ่ตัวเลขหรือสัญลักษณ์พิเศษ และเงื่อนไขในการตั้งรหัสผ่านคือมีความยาว 8-20 ตัวอักษร โดยมีเงื่อนไขที่กำหนดให้เป็นตัวอักษรผสมตัวเลขเท่านั้น ธนาคาร A ยังมีจุดอ่อนในด้านความปลอดภัยในการตั้งชื่อผู้ใช้และรหัสผ่าน ธนาคาร A เนื่องจากสามารถนำชื่อผู้ใช้มาใช้เป็นส่วนหนึ่งของรหัสผ่านได้ ซึ่งตามหลักความปลอดภัยของการตั้งรหัสผ่านที่ดี ไม่ควรอนุญาตให้ใช้ข้อความที่เป็นส่วนประกอบในการตั้งชื่อผู้ใช้มาตั้งเป็นรหัสผ่านเพื่อความปลอดภัยในการเข้าสู่ระบบ และธนาคาร A มีระบบ Limit Log-in หากผู้ใช้งานทำการป้อนรหัสผ่านผิดเกิน 3 ครั้ง ระบบจะล็อคทันที จะต้องทำการ Reset ใหม่

ธนาคาร B พบว่ากำหนดให้ใส่รหัส PIN ก่อนการเข้าสู่ระบบ โดยมีเงื่อนไขในการกำหนดลักษณะอักขระในการใส่ PIN คือให้ใช้ตัวเลข 0-9 เท่านั้น และมีความยาวเป็นตัวเลขจำนวน 6 หลัก ธนาคาร B ยังมีจุดอ่อนในด้านความปลอดภัยในการตั้งชื่อผู้ใช้และรหัสผ่าน ธนาคาร A เนื่องจากสามารถนำชื่อผู้ใช้มาใช้เป็นส่วนหนึ่งของรหัสผ่านได้ ซึ่งตามหลักความปลอดภัยของการตั้งรหัสผ่านที่ดี ไม่ควรอนุญาตให้ใช้ข้อความที่เป็นส่วนประกอบในการตั้งชื่อผู้ใช้มาตั้งเป็นรหัสผ่านเพื่อความปลอดภัยในการเข้าสู่ระบบ และมีระบบ Limit Log-in ที่จำกัดจำนวนครั้งในการใส่ PIN ถ้าใส่ผิดจำนวน 3 ครั้ง ระบบจะล็อคทันที ไม่สามารถเข้าใช้งานได้ จะต้องทำการ Reset ใหม่

ธนาคาร C พบว่ากำหนดให้ใส่รหัส PIN ก่อนการเข้าสู่ระบบ โดยมีเงื่อนไขในการกำหนดลักษณะอักขระในการใส่ PIN คือให้ใช้ตัวเลข 0-9 เท่านั้น และมีความยาวเป็นตัวเลขจำนวน 6 หลัก และมีระบบ Limit Log-in ที่จำกัดจำนวนครั้งในการใส่ PIN ถ้าใส่ผิดจำนวน 3 ครั้งระบบจะล็อคทันทีไม่สามารถเข้าใช้งานได้ จะต้องทำการ Reset ใหม่

ธนาคาร D พบว่ามีการเข้าสู่ระบบจะต้องใส่ชื่อผู้ใช้และรหัสผ่าน โดยมีเงื่อนไขในการตั้งชื่อผู้ใช้คือต้องมีความยาว 6-12 ตัวอักษรเท่านั้น ประกอบไปด้วยตัวเลขและตัวอักษรภาษาอังกฤษทั้งเล็กและใหญ่ผสมกันสามารถใช้สัญลักษณ์พิเศษร่วมด้วยได้ ถ้าใส่ผิดจำนวน 3 ครั้งระบบจะล็อคทันทีไม่สามารถเข้าใช้งานได้ จะต้องทำการ Reset ใหม่

ธนาคาร E พบว่ากำหนดให้ใส่รหัส PIN ก่อนการเข้าสู่ระบบ โดยมีเงื่อนไขในการกำหนดลักษณะอักขระในการใส่ PIN คือให้ใช้ตัวเลข 0-9 เท่านั้น และมีความยาวเป็นตัวเลขจำนวน 6 หลัก และมีระบบ Limit Log-in ที่จำกัดจำนวนครั้งในการใส่ PIN ถ้าใส่ผิดจำนวน 3 ครั้งระบบจะล็อคทันทีไม่สามารถเข้าใช้งานได้ จะต้องทำการ Reset ใหม่

ธนาคาร F พบว่าจะกำหนดให้ใส่ชื่อผู้ใช้และรหัสผ่านในการเข้าสู่ระบบ มีเงื่อนไขในการตั้งชื่อผู้ใช้คือต้องมีความยาว 6-12 ตัวอักษรเท่านั้น โดยไม่ได้มีเงื่อนไขที่กำหนดในการใช้อักษรเล็กใหญ่ตัวเลขหรือสัญลักษณ์พิเศษแต่อย่างใด ธนาคาร F มีความปลอดภัยที่ดีเพราะกำหนดความยาวของรหัสผ่านที่ 8-12 ตัวอักษร เป็นตัวอักษรภาษาอังกฤษหรือตัวเลข โดยตัวอักษรตัวเล็กหรือตัวใหญ่ระบบจะถือว่าแตกต่างกัน และมีการกำหนดเงื่อนไขที่ว่า 4 ตัวของรหัสผ่านจะต้องไม่เหมือนกับ 4 ตัวของชื่อผู้ใช้ ถือว่าอยู่ในเกณฑ์ความปลอดภัยของรหัสผ่านที่ดี ถ้าใส่ผิดจำนวน 3 ครั้งระบบจะล็อคทันทีไม่สามารถเข้าใช้งานได้ จะต้องทำการ Reset ใหม่

จากการวิเคราะห์ลักษณะการเข้าสู่ระบบ m-banking ของธนาคารทั้ง 6 ธนาคาร พบว่ามี 3 ธนาคารที่เข้าสู่ระบบด้วย PIN มี 3 ธนาคารที่เข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่าน ซึ่งในการใส่ PIN ก็เหมือนการใส่รหัสบัตร ATM ในการทำธุรกรรมทางการเงิน และยากต่อการคาดเดาของมิจฉาชีพ นอกจากนั้นยังมีระบบ Limit Log-in ที่จำกัดจำนวนครั้งในการ Login หากป้อนข้อมูลผิดเกินจำนวนครั้งที่กำหนด Account จะถูกล็อคทันที ซึ่งจะเห็นว่าทั้ง 6 ธนาคารมีความปลอดภัยใกล้เคียงกัน

4.1.4 ลักษณะการ Reset ข้อมูล

จากการสำรวจลักษณะการ Reset ข้อมูลของทั้ง 6 สามารถสรุปผลการสำรวจข้อมูลได้ดังนี้

ตารางที่ 4.4 ผลการสำรวจลักษณะการ Reset ข้อมูล

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	**ธนาคาร A**	**ธนาคาร B**	**ธนาคาร C**	**ธนาคาร D**	**ธนาคาร E**	**ธนาคาร F**
4. ลักษณะการลืมชื่อผู้ใช้						
4.1 Reset ผ่านสาขา	√			√		
4.2 Reset ผ่านคอลเซ็นเตอร์				√		√
ลักษณะการลืมรหัสผ่าน						
4.3 Reset ผ่านสาขา	√			√		
4.4 Reset ผ่านคอลเซ็นเตอร์				√		
4.5 Reset ผ่านแอปพลิเคชัน	√			√		√
4.6 Reset ผ่านตู้เอทีเอ็ม	√					

ตารางที่ 4.4 ผลการสำรวจลักษณะการ Reset ข้อมูล (ต่อ)

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	ธนาคาร A	ธนาคาร B	ธนาคาร C	ธนาคาร D	ธนาคาร E	ธนาคาร F
ลักษณะการลืม PIN						
4.7 Reset ผ่านสาขา						
4.8 Reset ผ่านคอลเซ็นเตอร์			√		√	
4.9 Reset ผ่านแอปพลิเคชัน			√		√	
4.10 Reset ผ่านตู้เอทีเอ็ม		√	√			

จากตารางที่ 4.4 ในการสำรวจการลืมข้อมูลชื่อผู้ใช้ รหัสผ่านและ PIN ของทั้ง 6 ธนาคาร ซึ่งมีรายละเอียดในแต่ละธนาคารดังต่อไปนี้

ธนาคาร A ลักษณะการลืมชื่อผู้ใช้สามารถ Reset ผ่านสาขาเท่านั้น โดยนำหลักฐานบัตรประจำตัวประชาชนและสมุดบัญชีเงินฝากมายืนยันตัวตน เจ้าหน้าที่ธนาคารจะตรวจสอบข้อมูล Username ที่ลืม โดยให้เรากรอกแบบฟอร์มคำขอตามที่ธนาคารกำหนด ลักษณะการลืมรหัสผ่านสามารถ Reset ผ่านสาขา โดยนำหลักฐานบัตรประจำตัวประชาชนและสมุดบัญชีเงินฝากมายืนยันตัวตน เจ้าหน้าที่ธนาคารจะตรวจสอบข้อมูลรหัสผ่านที่ลืม โดยให้เรากรอกแบบฟอร์มคำขอตามที่ธนาคารกำหนด นอกจากนั้นสามารถ Reset ผ่านแอปพลิเคชันและ Reset ผ่านตู้เอทีเอ็มได้

ธนาคาร B ลักษณะการลืม PIN สามารถ Reset ผ่านตู้เอทีเอ็มเท่านั้น เนื่องจากเป็นข้อมูลส่วนบุคคล ธนาคารจึงให้ลูกค้าทำการ Reset ด้วยตนเอง

ธนาคาร C ลักษณะการลืม PIN สามารถ Reset ผ่านคอลเซ็นเตอร์, Reset ผ่านแอปพลิเคชันและ Reset ผ่านตู้เอทีเอ็ม ในการ Reset ผ่านคอลเซ็นเตอร์นั้นอาจจะเป็นช่องโหว่ให้มิจฉาชีพแอบสวมรอยในการปลอมตัวได้ ดังนั้นธนาคารควรใช้คำถามที่เฉพาะเจาะจงตัวบุคคลไม่เพียงสอบถามข้อมูลส่วนตัว ซึ่งข้อมูลส่วนตัวสามารถค้นหาได้

ธนาคาร D ลักษณะการลืมชื่อผู้ใช้สามารถ Reset ผ่านสาขา โดยนำหลักฐานบัตรประจำตัวประชาชนและสมุดบัญชีเงินฝากมายืนยันตัวตน เจ้าหน้าที่ธนาคารจะตรวจสอบข้อมูลชื่อผู้ใช้ที่ลืม โดยให้กรอกแบบฟอร์มคำขอตามที่ธนาคารกำหนด เจ้าหน้าที่ธนาคารจะส่งชื่อผู้ใช้มาทางอีเมล์ที่แจ้งไว้กับธนาคารและ Reset ผ่านคอลเซ็นเตอร์ เจ้าหน้าที่ธนาคารจะส่งชื่อผู้ใช้มาทางอีเมล์ที่แจ้งไว้กับธนาคาร ลักษณะการลืมรหัสผ่านสามารถ Reset ผ่านสาขา โดยนำหลักฐานบัตรประจำตัวประชาชนและสมุดบัญชีเงินฝากมายืนยันตัวตน สามารถ Reset ผ่านคอลเซ็นเตอร์ โดยธนาคาร D จะทำการยืนยันตัวตนโดยการสอบถามถึงข้อมูลเลขที่บัตรประจำตัวประชาชน เลขรหัส ATM และข้อมูลทั่วไปที่เคยใช้งานเกี่ยวกับระบบ m-banking เพื่อตรวจสอบความถูกต้อง และ Reset ผ่านแอปพลิเคชันด้วยตนเอง

ธนาคาร E การ Reset รหัส PIN ผ่านคอลเซ็นเตอร์และ Reset ผ่านแอปพลิเคชัน ซึ่งผู้ใช้งานทำการ Reset ด้วยตนเองและมีการยืนยันตัวตนโดยใช้บัตรและรหัสเอทีเอ็ม

ธนาคาร F ลักษณะการลืมชื่อผู้ใช้สามารถ Reset ผ่านคอลเซ็นเตอร์ ซึ่งอาจจะไม่มีความปลอดภัยหากมิจฉาชีพแอบสวมรอยในการปลอมตัวได้ ดังนั้นธนาคารควรใช้คำถามที่เฉพาะเจาะจงตัวบุคคลไม่เพียงสอบถามข้อมูลส่วนตัว ซึ่งข้อมูลส่วนตัวสามารถค้นหาได้ เจ้าหน้าที่จะต้องทำการยืนยันตัวตนโดยการสอบถามถึงข้อมูลเลขที่บัตรประจำตัวประชาชน เลขบัญชีธนาคาร เลขรหัส ATM และข้อมูลทั่วไปที่เคยใช้งานเกี่ยวกับระบบ m-banking เพื่อตรวจสอบความถูกต้อง และการ Reset รหัสผ่านสามารถทำผ่านแอปพลิเคชัน

จากการวิเคราะห์หากมีการลืมชื่อผู้ใช้, รหัสผ่าน , PIN จะพบว่าถ้า Reset ผ่านสาขาจะมีความปลอดภัยมากกว่าซึ่งเจ้าหน้าจะให้นำสมุดบัญชีและบัตรประชาชนยืนยันตัวตนก่อนทำรายการ แต่จะมีช่องโหว่ระหว่างการส่งข้อมูล ซึ่งธนาคาร B จะส่งข้อมูลมาให้ลูกค้าทางอีเมล์ซึ่งทำให้ถูกดักจับข้อมูลได้ และการ Reset ผ่านคอลเซ็นเตอร์อาจเป็นช่องโหว่ให้มิจฉาชีพแอบสวมรอย โดยใช้การโจมตีแบบวิศวกรรมทางสังคมได้ เจ้าหน้าที่ธนาคารควรตรวจสอบข้อมูลและใช้คำถามที่เฉพาะเจาะจงตัวบุคคลเพราะการแจ้งผ่านคอลเซ็นเตอร์ไม่สามารถตรวจสอบได้ว่าเป็นตัวจริง ดังนั้นวิธีนี้จึงอาจเป็นจุดอ่อนได้ ดังนั้นการ Reset ข้อมูลผ่านตู้เอทีเอ็มเป็นวิธีการที่ปลอดภัยที่สุดเพราะต้องใช้บัตรและรหัสเอทีเอ็ม เป็นการยืนยันตัวสองชั้น โดยการถือครองบัตร และทราบรหัสของบัตร

4.1.5 ลักษณะการเปลี่ยนเบอร์มือถือ

จากการสำรวจลักษณะการเปลี่ยนเบอร์มือถือรับ OTP สามารถสรุปข้อมูลได้ดังนี้

ตารางที่ 4.5 ผลการสำรวจลักษณะการเปลี่ยนเบอร์มือถือ

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	**ธนาคาร A**	**ธนาคาร B**	**ธนาคาร C**	**ธนาคาร D**	**ธนาคาร E**	**ธนาคาร F**
5.การเปลี่ยนเบอร์มือถือ						
5.1 Reset ผ่านสาขา			√	√	√	
5.2 Reset ผ่านคอลเซ็นเตอร์		√				
5.3 Reset ผ่านแอปพลิเคชัน	√	√				√
5.4 Reset ผ่านตู้เอทีเอ็ม		√	√			√

จากตารางที่ 4.5 พบว่าการเปลี่ยนเบอร์มือถือรับ OTP ทั้งหมด 6 ธนาคาร มี 3 ธนาคารสามารถเปลี่ยนผ่านสาขาได้ มี 1 ธนาคารสามารถเปลี่ยนผ่านคอลเซ็นเตอร์ได้ มี 3 ธนาคารสามารถเปลี่ยนผ่านแอปพลิเคชันได้ มี 3 ธนาคารที่สามารถเปลี่ยนที่ตู้เอทีเอ็มได้ ซึ่งสามารถสรุปผลและวิเคราะห์ข้อมูลดังต่อไปนี้

ธนาคาร A การขอเปลี่ยนเบอร์มือถือรับ OTP โดยขอเปลี่ยนผ่านแอปพลิเคชัน

ธนาคาร B การขอเปลี่ยนเบอร์มือถือรับ OTP โดยทำการขอเปลี่ยนผ่านคอลเซ็นเตอร์, เปลี่ยนผ่านแอปพลิเคชันและเปลี่ยนผ่านตู้เอทีเอ็ม

ธนาคาร C การขอเปลี่ยนเบอร์มือถือรับ OTP โดยขอเปลี่ยนผ่านสาขา โดยนำหลักฐานบัตรประจำตัวประชาชนและสมุดบัญชีเงินฝาก เพื่อแสดงตัวตนต่อเจ้าหน้าที่ธนาคาร แล้วกรอกแบบฟอร์มในการขอเปลี่ยนแปลงหมายเลขโทรศัพท์มือถือและเปลี่ยนผ่านตู้เอทีเอ็ม

ธนาคาร D การขอเปลี่ยนเบอร์มือถือรับ OTP โดยขอเปลี่ยนผ่านสาขาเท่านั้น โดยนำหลักฐานบัตรประจำตัวประชาชนและสมุดบัญชีเงินฝาก เพื่อแสดงตัวตนต่อเจ้าหน้าที่ธนาคาร แล้วกรอกแบบฟอร์มในการขอเปลี่ยนแปลงหมายเลขโทรศัพท์มือถือ

ธนาคาร E การขอเปลี่ยนเบอร์มือถือรับ OTP โดยขอเปลี่ยนผ่านสาขาเท่านั้น โดยนำหลักฐานบัตรประจำตัวประชาชนและสมุดบัญชีเงินฝาก เพื่อแสดงตัวตนต่อเจ้าหน้าที่ธนาคาร แล้วกรอกแบบฟอร์มในการขอเปลี่ยนแปลงหมายเลขโทรศัพท์มือถือ ธนาคารจะใช้เวลา 3-5 วันทำการ หลังจากทำรายการเรียบร้อยจะมี SMS แจ้งเตือนการเปลี่ยนแปลงหมายเลขโทรศัพท์ให้ลูกค้าทราบ

ธนาคาร F การขอเปลี่ยนเบอร์มือถือรับ OTP โดยขอเปลี่ยนผ่านแอปพลิเคชันและเปลี่ยนผ่านตู้เอทีเอ็ม

จากการวิเคราะห์พบว่ามี 1 ธนาคารที่อนุญาตให้เปลี่ยนเบอร์ผ่านคอลเซ็นเตอร์ ซึ่งธนาคารจะต้องให้ความสำคัญเกี่ยวกับการตรวจสอบหลักฐานต่างๆ และการสอบถามข้อมูลที่สามารถยืนยันตัวบุคคลที่แท้จริง เพื่อความให้ถูกต้อง เนื่องจากมีข่าวที่เกิดขึ้นดังที่กล่าวมาข้างต้น เกี่ยวกับการปลอมแปลงเอกสารเพื่อออกซิมใหม่ แล้วทำการขอแจ้งเปลี่ยนเบอร์มือถือในระบบ m-banking ซึ่งเป็นวิธีการที่มิจฉาชีพใช้ในการสวมรอยทำธุรกรรมทางการเงิน จากการวิเคราะห์ความผิดพลาดเกิดจากผู้ให้บริการเครือข่ายที่ไม่มีมาตรการตรวจสอบข้อมูล ดังนั้นควรมีมาตรการที่เป็นแนวทางเดียวกันและเพิ่มวิธีการยืนยันตัวตน นอกจากจะตรวจสอบเอกสารแล้วควรมีการยืนยันตัวตนที่เฉพาะเจาะจง เช่น การแสกนลายนิ้วมือ

4.1.6 ลักษณะของ OTP

จากการสำรวจลักษณะของ OTP ที่ใช้เป็นการยืนยันตัวตนอีกชั้นเพื่อความปลอดภัยในการทำธุรกรรมต่างๆ สามารถสรุปผลได้ดังนี้

ตารางที่ 4.6 ผลการสำรวจลักษณะของ OTP

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	**ธนาคาร A**	**ธนาคาร B**	**ธนาคาร C**	**ธนาคาร D**	**ธนาคาร E**	**ธนาคาร F**
6. ลักษณะของ OTP						
6.1 ระยะเวลา OTP/นาที	15 นาที		3 นาที	5 นาที	15 นาที	12 นาที
6.2 OTP ในการแจ้งโอนเงิน	√			√		√
6.3 OTP เมื่อเพิ่มบัญชีใหม่	√			√		√
6.4 OTP แจ้งเปลี่ยนเบอร์มือถือ	√			√		√
6.5 OTP ชำระเงิน	√			√		√
6.6 Limit OTP	3 ครั้ง		3 ครั้ง	3 ครั้ง	3 ครั้ง	3 ครั้ง

จากตารางที่ 4.6 พบว่าบางธนาคารเปิดให้มีระยะเวลาการกรอก OTP ที่นานต่างกันไป จากการทดสอบ พบว่าระบบ OTP ในประเทศไทยมี Delay น้อยมาก ดังนั้นระยะเวลาไม่เกิน 3 นาที ที่ธนาคาร C ใช้อยู่ น่าจะเหมาะสมกว่า เนื่องจากระยะเวลาที่นานเกินไป อาจเป็นช่องโหว่ให้มิจฉาชีพดักขโมยข้อมูล หากโทรศัพท์ที่ใช้รับ SMS OTP ติดมัลแวร์ ทำให้ SMS OTP ส่งไปยังเครื่องของมิจฉาชีพ และทำให้มิจฉาชีพมีเวลาไปทำธุรกรรมก่อนเจ้าของบัญชี

4.1.7 ลักษณะการเชื่อมต่ออินเทอร์เน็ต

จากการสำรวจการเชื่อมต่ออินเทอร์เน็ตของระบบ m-banking มี 2 แบบคือสามารถเชื่อมต่อผ่านเทคโนโลยี 3G และ 4G และเชื่อมต่อผ่านเทคโนโลยี Wi-Fi สรุปผลดังนี้

ตารางที่ 4.7 ผลสำรวจการเชื่อมต่ออินเทอร์เน็ตของระบบ m-banking

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	**ธนาคาร A**	**ธนาคาร B**	**ธนาคาร C**	**ธนาคาร D**	**ธนาคาร E**	**ธนาคาร F**
7. การเชื่อมต่ออินเทอร์เน็ต						
7.1 เชื่อมต่อผ่าน 3G และ 4G	√	√	√	√	√	√
7.2 เชื่อมต่อผ่าน Wi-Fi	√		√	√	√	√

จากตารางที่ 4.7 พบว่าพบว่าธนาคาร B ไม่อนุญาตให้เชื่อมต่อผ่าน Wi-Fi เพราะมีโอกาสถูกดักจับข้อมูล และแทรกกลางการสื่อสารได้ง่ายกว่า โดยอนุญาตให้เชื่อมต่อผ่าน 3G และ 4G เท่านั้น เนื่องจากเทคโนโลยี 3G มีการเข้ารหัสข้อมูลที่ส่งผ่าน ด้วยอัลกอริธึม UEA1/UIA1 Kasumi Block Cipher ส่วนเทคโนโลยี 4G [47] จะมีมาตรฐานความปลอดภัยที่สูงไปอีก โดยการเข้ารหัสด้วยอัลกอริธึม UEA2/UIA2 Snow 3G Stream Cipher ดังนั้นจึงมีความปลอดภัยสูงจากการดักจับข้อมูลของแฮกเกอร์เมื่อเทียบกับการเชื่อมต่อผ่าน Wi-Fi แต่การปิดช่องทางการเชื่อมต่อ Wi-Fi ของธนาคาร B จะทำให้ลูกค้าอาจไม่เลือกใช้ระบบ m-banking ของธนาคาร แต่อาจเปลี่ยนไปใช้บริการในระบบ i-banking ที่มีความมั่นคงน้อยกว่าแทน เพราะสามารถเชื่อมต่อผ่าน Wi-Fi ได้ นอกจากนี้จากการทดลองที่จะกล่าวในหัวเรื่องถัดไป พบว่าเมื่อระบบ m-banking ถูกออกแบบมาดี ถึงแม้จะเล่นผ่าน Wi-Fi ก็ไม่สามารถที่จะดักจับข้อมูลได้โดยง่ายเหมือนระบบ i-banking ดังนั้นการปิด Wi-Fi จึงอาจไม่ใช่ทางเลือกที่ดี

4.1.8 มาตรการความปลอดภัยอื่นๆ

จากการสำรวจมาตรการความปลอดภัยอื่นๆ ของธนาคาร ที่นำมาช่วยเพิ่มความปลอดภัยในการใช้งาน สามารถสรุปข้อมูลได้ดังนี้

ตารางที่ 4.8 ผลการสำรวจมาตรการความปลอดภัยอื่นๆ

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	ธนาคาร A	ธนาคาร B	ธนาคาร C	ธนาคาร D	ธนาคาร E	ธนาคาร F
8. ความปลอดภัยอื่นๆ						
8.1 แจ้งเตือนการ Login	√		√	√	√	√
8.2 ตั้งค่าความปลอดภัย	√	√	√	√	√	√
8.3 ระบบ Auto Log Off	5 นาที	3 นาที	5 นาที	1 นาที	1 นาที	15 นาที
8.4 รหัสลับทำธุรกรรม			√			
8.5 การแจ้งเตือนทำธุรกรรม						
- E-mail	√	√	√	√	√	√
- SMS	√					

จากตารางที่ 4.8 พบว่าธนาคาร F มีระยะเวลา Auto Log off นานเกินไป เมื่อเทียบกับธนาคารอื่นๆ ซึ่งระยะเวลาที่นานเกินไปนี้ อาจทำให้มิจฉาชีพแอบสวมรอยการทำธุรกรรมได้ และธนาคารทุกธนาคารควรมีระบบการแจ้งเตือนการเข้าใช้งานทุกครั้งโดยแจ้งผ่าน Email ซึ่งจะทำให้เจ้าของบัญชีทราบความเคลื่อนไหวและรู้ทันหากไม่ได้เข้าระบบด้วยตนเอง

4.1.9 การยกเลิกการใช้งานระบบ m-banking

จากการสำรวจการยกเลิกการใช้งานระบบ m-bankingของ 6 ธนาคาร สามารถสรุปข้อมูลได้ ดังนี้

ตารางที่ 4.9 ผลการสำรวจการยกเลิกการใช้งานระบบ m-banking

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	ธนาคาร A	ธนาคาร B	ธนาคาร C	ธนาคาร D	ธนาคาร E	ธนาคาร F
9. การยกเลิกการใช้ระบบ m-banking						
9.1 ยกเลิกผ่านสาขา	√			√	√	√
9.2 ยกเลิกผ่านคอลเซ็นเตอร์		√	√	√		
9.3 ยกเลิกผ่านแอปพลิเคชัน	√	√	√			√
9.4 ยกเลิกที่ตู้เอทีเอ็ม		√				

จากตารางที่ 4.9 พบว่าขั้นตอนการเลิกใช้บริการระบบ m-banking โดยทั่วไปยังไม่มีช่องโหว่หรือเกิดกรณีการจูโจมที่เกิดขึ้นในเรื่องนี้โดยตรง แต่เพื่อความปลอดภัย ธนาคารควรตระหนักถึงการ

ตรวจสอบการยืนยันตัวหากมีการยกเลิกการใช้งานเพราะอาจจะมีการกลั่นแกล้งเพื่อต้องการทำให้บัญชีมีปัญหา ที่เรียกว่า Denial of Services หรือมิจฉาชีพอาจทำการยกเลิกการใช้งานแล้วขอเปิดใหม่เพื่อทำการสวมรอย ซึ่งทางธนาคารควรเข้มงวดในการตรวจสอบความถูกต้องในการขอเลิกใช้บริการ โดยเฉพาะอย่างยิ่งธนาคาร B, C และ D อนุญาตให้มีการยกเลิกผ่านคอลเซ็นเตอร์ ซึ่งอาจมีโอกาสถูกโจมตีแบบวิศวกรรมสังคม โดยมิจฉาชีพได้ง่ายที่สุด หากคำถามที่ใช้ตรวจสอบยืนยันตัวตนไม่ดีพอ

4.1.10 การปิดบัญชี

จากการสำรวจการปิดบัญชี ซึ่งสามารถสรุปผลได้ดังนี้

ตารางที่ 4.10 ผลการสำรวจการปิดบัญชี

เกณฑ์ที่ใช้ในการสำรวจความปลอดภัยของระบบ (Safety)	**ธนาคาร A**	**ธนาคาร B**	**ธนาคาร C**	**ธนาคาร D**	**ธนาคาร E**	**ธนาคาร F**
10. การปิดบัญชีธนาคาร						
10.1 ปิดที่ธนาคารสาขาที่เปิดบัญชี	√	√	√	√	√	√
10.2 ปิดบัญชีที่ธนาคารต่างสาขา		√	√	√		
10.3 บัตรประชาชนและสมุดบัญชี	√	√	√	√	√	√
10.4 บัตรประชาชนและใบแจ้งความ	√				√	√

จากตารางที่ 4.10 พบว่าทุกธนาคารสามารถปิดได้ที่สาขาที่เปิดและมี 3 ธนาคารที่สามารถปิดบัญชีธนาคารต่างสาขาได้ ซึ่งถือว่ามีความปลอดภัย แต่ขึ้นอยู่กับขบวนการตรวจเอกสารหลักฐานในการยืนยันตัวตนที่แท้จริง ซึ่งพบว่าขั้นตอนนี้ โดยทั่วไปมีความปลอดภัย เพราะลูกค้าจะต้องนำบัตรประชาชนและสมุดบัญชีมาใช้ควบคู่ในการปิดบัญชี และมี 3 ธนาคาร ซึ่งจะต้องนำใบแจ้งความมาประกอบด้วยเมื่อทำสมุดบัญชีเงินฝากหาย จากการวิเคราะห์กรณีคดีความที่เกิดขึ้น ยังไม่มีประเด็นด้านการโจมตีแบบวิศวกรรมสังคม ที่เกี่ยวกับเรื่องนี้โดยตรง แต่ธนาคารควรตระหนักถึงการตรวจสอบการยืนยันตัวหากมีการมาปิดบัญชีเพราะอาจจะมีการกลั่นแกล้ง หรือทำการยกเลิกการใช้งานแล้วขอเปิดใหม่เพื่อทำการสวมรอย

4.2 ผลด้านความมั่นคงของระบบ m-banking

การวิเคราะห์ประเด็นด้านความมั่นคงจะเป็นเรื่องของเทคนิค โดยจะทำการทดสอบ ใน 2 วิธี คือ SSL Sniff และ SSL Strip ในขณะที่กำลังเข้าใช้งานระบบธนาคารผ่านโทรศัพท์มือถือ ซึ่งจะทำการดักจับข้อมูลผ่านการเชื่อมต่ออินเทอร์เน็ตทั้ง 6 ธนาคารเพื่อทดสอบและได้ผลการสำรวจ สรุปผลดังนี้

4.2.1 ผลการทดสอบการโจมตีแบบ SSL Sniff

ผลการทดสอบการโจมตีด้วยวิธีการ SSL Sniff ต่อระบบ m-banking พบว่าไม่สามารถดักจับข้อมูลได้ เนื่องจากโปรแกรมของระบบ m-banking application จะไม่ยอมรับ หากมี

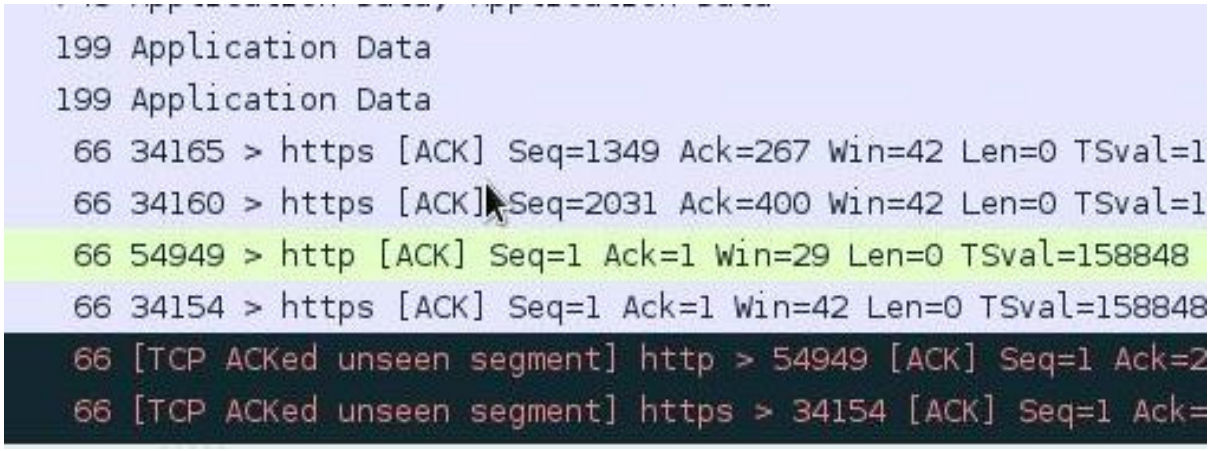
การส่งใบ Certificate ปลอม ระบบถูกออกแบบให้ไม่ทำงาน ซึ่งการเขียนโปรแกรมระดับชั้นแอปพลิเคชันจะกำหนด Certificate ที่แท้จริงจากธนาคารผู้พัฒนาตั้งแต่ขั้นพัฒนาการใช้งานจึงมีความปลอดภัยมั่นคงสูง ไม่เหมือนในระบบ i-banking ที่รายงานไว้ในงานวิจัยอื่นๆ ก่อนหน้านี้ จะให้ผู้ใช้เป็นคนตรวจสอบว่า Certificate นั้นถูกต้องหรือไม่ ซึ่งมีโอกาสถูกจู่โจมได้ หากผู้ใช้งานระบบ i-banking ไม่สังเกต โดยจากการทดลองของงานวิจัยนี้ต่อจากระบบ i-banking ก็พบว่าสามารถจะจู่โจมด้วย SSL Sniffing และดักจับข้อมูลในระบบ i-banking ได้ ดังรูปที่ 4.1 เนื่องจากเว็บเบราว์เซอร์ไม่สามารถตรวจสอบได้ว่ามีการดักจับข้อมูลจากแฮกเกอร์ หากผู้ใช้รู้เท่าไม่ถึงการณ์กดยอมรับ Certificate ปลอม หรือเข้าไปในเว็บปลอมที่แฮกเกอร์ใช้ดักจับข้อมูลก็จะถูกขโมยข้อมูลที่สำคัญไปได้โดยง่าย ดังนั้น จากการทดลองนี้จะเห็นได้ชัดเจนว่า ระบบ m-banking โดยทั่วไปมีความมั่นคงต่อการจู่โจมด้วย SSL Sniff มากกว่าระบบ i-banking

Timestamp	HTTP server	Client	Username	Password
22/01/2015 - 01:11:54	119.46.87.14	192.168.100.25	banktestA	forie
22/01/2015 - 01:13:18	115.31.152.155	192.168.100.25	banktestA	forchome
22/01/2015 - 01:14:35	119.46.87.14	192.168.100.25	banktestA	forfirefox
22/01/2015 - 01:19:58	202.12.117.134	192.168.100.25	banktestB	forie
22/01/2015 - 01:24:40	202.12.117.134	192.168.100.25	banktestB	forchome
22/01/2015 - 01:28:30	202.12.117.134	192.168.100.25	banktestB	forfirefox
22/01/2015 - 01:29:48	203.146.18.171	192.168.100.25	banktestC	forie
22/01/2015 - 01:31:05	203.146.18.171	192.168.100.25	banktestC	forchome
22/01/2015 - 01:33:33	203.146.18.171	192.168.100.25	banktestC	forfirefox
22/01/2015 - 01:36:45	110.170.151.46	192.168.100.25	banktestD	forie
22/01/2015 - 01:38:06	110.170.151.46	192.168.100.25	banktestD	forchome
22/01/2015 - 01:39:00	110.170.151.46	192.168.100.25	banktestD	forfirefox
22/01/2015 - 02:01:08	203.154.171.201	192.168.100.25	banktestF	forie
22/01/2015 - 02:01:57	203.154.171.201	192.168.100.25	banktestF	forchome
22/01/2015 - 02:02:44	203.154.171.201	192.168.100.25	banktestF	forfirefox

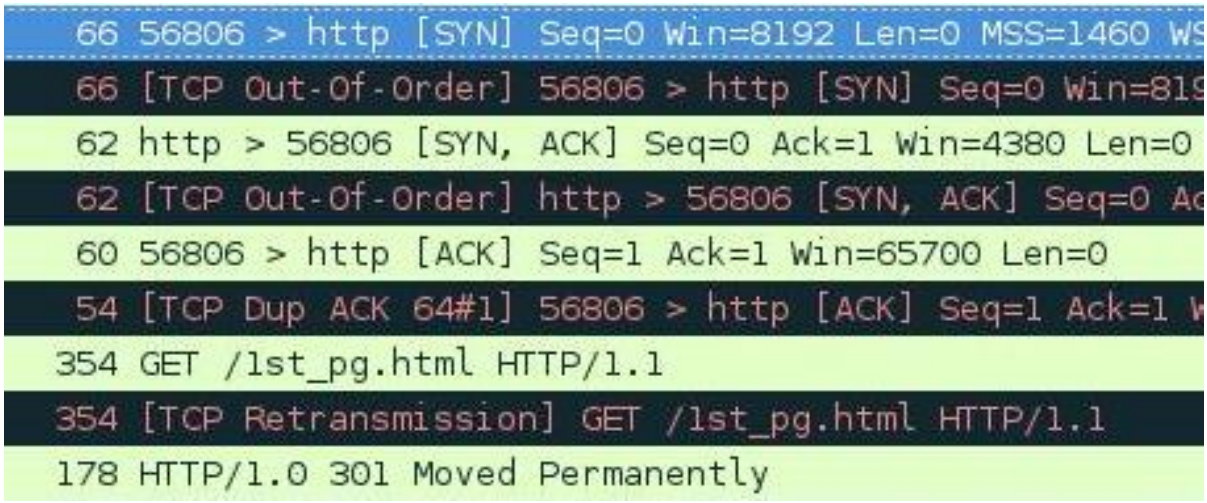
รูปที่ 4.1 ผลการดักจับข้อมูลด้วยเทคนิค SSL Sniff ผ่าน Browser

4.2.2 ผลการทดสอบการโจมตีแบบ SSL Strip

SSL Strip เป็นเทคนิควิธีที่ใช้ในการโจมตีระบบธนาคารออนไลน์ที่เป็นที่นิยมอยู่ทั่วโลกจากสถิติตั้งแต่ปี ค.ศ. 2008 จากคดีความด้านนี้ที่เกิดขึ้นในประเทศไทย พบว่า เป็นเทคนิคที่ถูกนำมาใช้มากที่สุด จากการทดลองดักจับข้อมูลด้วยเทคนิค SSL Strip ดังรูปที่ 4.2 ด้วยโปรแกรม Wireshark ซึ่งทำการดักจับ Packet ที่ Client ในขณะที่ใช้งานระบบธนาคารบนโทรศัพท์มือถือผ่านแอปพลิเคชัน พบว่าขั้นตอนการ Request มีการเรียกใช้โพรโทคอล HTTPS ทำให้ไม่สามารถโจมตีแบบ SSL Strip ได้ เพราะเริ่มต้น Session เป็น HTTPS อัตโนมัติ ไม่เหมือนกับระบบ i-banking ที่ให้ผู้ใช้เป็นผู้เริ่ม Session การสื่อสาร ซึ่งอาจเป็น HTTP แล้ว Web Server ค่อยทำการ Redirect ไปเป็น HTTPS ที่อาจโดน SSL Strip ได้



รูปที่ 4.2 ผลการดักจับข้อมูลด้วยเทคนิค SSL Strip ผ่าน Application



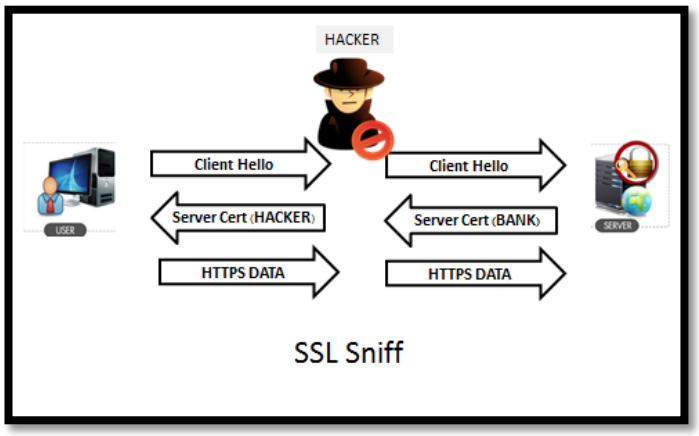
รูปที่ 4.3 ผลการดักจับข้อมูลด้วยเทคนิค SSL Strip ผ่าน Browser

จากผลการทดสอบการดักจับข้อมูลด้วยเทคนิค SSL Strip ต่อระบบ i-banking ที่ทำงานผ่านเบราว์เซอร์ดังรูปที่ 4.3 พบว่าในการต่อต้านการจู่โจมด้วยวิธีนี้ระบบ i-banking มีความมั่นคงน้อยกว่าระบบ m-banking เพราะมีโอกาสถูก Strip ได้ หากผู้ใช้ไม่พิมพ์ HTTPS แต่ Request ระบบธนาคารโดยใช้โพรโทคอล HTTP ดังนั้นจะเห็นได้ว่า การใช้งานผ่านระบบธนาคารบนโทรศัพท์มือถือจะมีความมั่นคงสูงกว่าการใช้งานผ่านอินเทอร์เน็ตแบงก์กิ้ง

จากผลการทดสอบการโจมตีด้วยวิธีแทรกกลางการสื่อสารทั้ง 2 วิธี คือ การโจมตีแบบ SSL Sniff และการโจมตีแบบ SSL Strip พบว่าไม่สามารถดักจับข้อมูลได้ เนื่องจากการทำงานบนแอปพลิเคชันจะใช้รูปแบบการสื่อสารกับเซิร์ฟเวอร์บนโพรโทคอล HTTPS ที่มีการเข้ารหัสด้วยโพรโทคอล SSL ซึ่งจะใช้ในการตรวจสอบอัลกอริธึมในการเข้ารหัสการแลกเปลี่ยน Public Key และ Session Key ก่อนทำการสื่อสารแลกเปลี่ยนข้อมูล และทำการเข้ารหัสข้อมูลด้วย Secret Key ระหว่าง Client และ

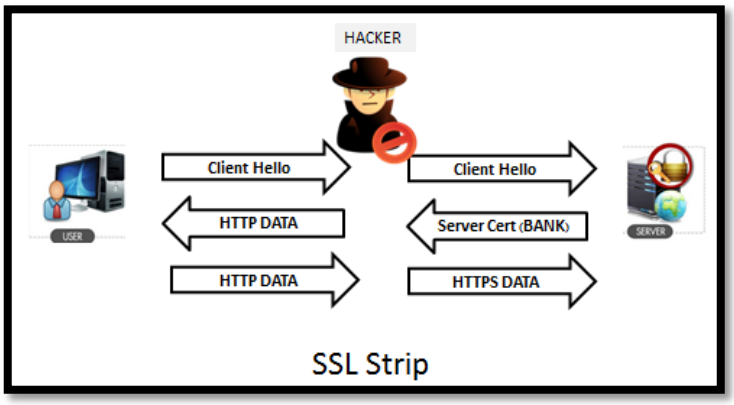
Server ซึ่งเรียกขบวนการนี้ว่า SSL Handshake ซึ่งข้อมูลที่ถูกส่งจะถูกเข้ารหัสด้วย SSL/TLS อัตโนมัติ ทำให้ข้อมูลมีความถูกต้องและเป็นความลับ เพื่อป้องกันการโจมตีด้วยวิธีแทรกกลางการสื่อสาร จะเห็นได้ว่าการสื่อสารบนโพรโทคอล HTTPS จะมีความมั่นคงสูง สามารถป้องกันการดักจับข้อมูลที่สำคัญ โดยขบวนการทั้งหมดสามารถสั่งงานผ่าน Mobile Application ที่สร้างเป็นระบบ m-banking ได้เลย โดยไม่ต้องพึ่งพาผู้ใช้งานให้สังเกต HTTPS หรือ Certificate Validity ซึ่งต่างไปจากระบบ i-banking ที่ยังต้องอาศัยการสังเกตของผู้ใช้งานเป็นด่านสุดท้ายในการป้องกันความมั่นคง ซึ่งผลการทดลองในส่วนการโจมตีระบบ i-banking นั้น สอดคล้องกับงานวิจัยก่อนหน้านี้ ที่แสดงความสำเร็จของการโจมตีระบบ i-banking ด้วยวิธี SSL Strip และ SSL Sniff เมื่อผู้ใช้ส่วนใหญ่ไม่สังเกตดีพอ

4.2.3 รูปแบบการโจมตีด้วยวิธีแทรกกลางการสื่อสาร



รูปที่ 4.4 SSL Sniff

จากรูปที่ 4.4 จะเห็นได้ว่า Client จะใช้ Certificate Hacker เข้ารหัสข้อมูล ซึ่งจะทำให้ Hacker สามารถถอดรหัสข้อมูลของ Client ได้ และเมื่อ Hacker ถอดรหัสข้อมูลของ Client ได้แล้ว ก็จะสามารถใช้ Certificate ของ Server เข้ารหัสข้อมูลจึงทำให้ Server ตรวจสอบไม่ได้ว่า Client ถูกโจมตี ถ้าเป็นการใช้งานผ่านแอปพลิเคชัน ระบบจะ Error หากพบว่ามีการใช้ Certificate ปลอม



รูปที่ 4.5 SSL Strip

จากรูปที่ 4.5 Client กับ Hacker จะสื่อสารบนโพรโทคอล HTTP ทำให้ข้อมูลของ Client ไม่ถูกเข้ารหัส ดังนั้น Hacker สามารถดักจับข้อมูลของ Client ได้ และ Hacker กับ Server สื่อสารบน HTTPS ปกติทำให้ Server ตรวจสอบไม่ได้ว่า Client ถูกโจมตี จากหลักการทำงานของ HTTPS ที่มีการกำหนดให้ระบบเว็บไซต์ทำงานบนโพรโทคอล HTTPS ที่ตำแหน่งเว็บเซิร์ฟเวอร์เท่านั้น ด้วยเหตุนี้ SSL Strip จึงอาศัยจุดอ่อนที่เว็บเบราว์เซอร์ไม่สามารถตรวจสอบและกำหนดรูปแบบการสื่อสารบนโพรโทคอล HTTPS กับเว็บเซิร์ฟเวอร์ โดยหลักการโจมตีด้วยวิธี SSL Strip เพื่อดักจับข้อมูลสำคัญของเหยื่อที่ใช้ในการสื่อสารกับเว็บเซิร์ฟเวอร์ ถ้าใช้งานผ่านแอปพลิเคชันจะบังคับเข้ารหัสด้วยโพรโทคอล SSL ซึ่งเป็นโพรโทคอลพื้นฐานในการสร้าง HTTPS จึงทำให้ลดปัญหาการโจมตีแบบแทรกกลาง

4.3 ผลด้านความปลอดภัยของผู้ให้บริการ Mobile Sim

จากการสำรวจขั้นตอนการขอออกซิมใหม่ พร้อมทั้งการนำหลักฐานต่างๆ ไปยื่นแสดงตัวตนเพื่อทำการขอซิมใหม่ พร้อมทั้งสังเกตขบวนการตรวจสอบเอกสารและหลักฐานต่างๆ ของเจ้าหน้าที่ ซึ่งสามารถสรุปผลการสำรวจข้อมูลได้ดังนี้

ตารางที่ 4.11 ผลการสำรวจผู้ให้บริการ Mobile Sim

เกณฑ์ที่ใช้ในการสำรวจการออกซิมใหม่	**TRUE**	**DTAC**	**AIS**
การออกซิมใหม่			
● บัตรประชาชน	√	√	√
● บัตรประชาชนและใบแจ้งความ		√	√
● สำเนาบัตรประชาชน	√	√	√
● ใบอนุญาตขับรถ	√	√	
● หมายเลขเบอร์โทรศัพท์	√	√	√

จากตารางที่ 4.11 พบว่าลักษณะของการออกซิมใหม่ของผู้ให้บริการมีลักษณะดังต่อไปนี้

ผู้ให้บริการ TRUE จากการสำรวจทั้ง 3 สาขา พบว่า สาขาที่หนึ่งและสองในการขอออกซิมใหม่จะต้องใช้บัตรประชาชนตัวจริงหากไม่มีสามารถใช้ใบอนุญาตขับรถแทนได้ พร้อมสำเนาบัตรประจำตัวประชาชนพร้อมทั้งใบแจ้งความกรณีซิมหาย และหมายเลขโทรศัพท์มือถือ เพื่อทำการขอออกซิมใหม่ ส่วนกรณีขอเปลี่ยนซิมใหม่จะต้องนำซิมเดิมมาด้วย เพื่อป้องกันการสวมรอยของมิจฉาชีพ หากผู้ใช้บริการไม่สามารถมาดำเนินการได้ด้วยตนเองจะต้องมีหนังสือมอบอำนาจพร้อมทั้งบัตรประจำตัวประชาชน ให้ผู้รับมอบอำนาจมาแสดงด้วย ส่วนสาขาที่สามพบว่าบอกแค่หมายเลขบัตรประชาชนและหมายเลขเบอร์โทรศัพท์มือถือก็สามารถออกซิมใหม่ได้เลย จะเห็นได้ว่าจากการสำรวจผู้ให้บริการ TRUE ทั้ง 3 สาขา พบว่าลักษณะการให้บริการจะแตกต่างกันและไม่เป็นรูปแบบเดียวกัน

ผู้ให้บริการ DTAC จากการสำรวจทั้ง 3 สาขา พบว่า สาขาที่หนึ่งและสองในการขอออกซิมใหม่จะต้องใช้บัตรประชาชนตัวจริงหากไม่มีสามารถใช้ใบอนุญาตขับรถแทนได้ พร้อมสำเนาบัตรประจำตัวประชาชนพร้อมทั้งใบแจ้งความกรณีซิมหาย และหมายเลขโทรศัพท์มือถือ เพื่อทำการขอออกซิมใหม่ ส่วนกรณีขอเปลี่ยนซิมใหม่จะต้องนำซิมเดิมมาด้วย เพื่อป้องกันการสวมรอยของมิจฉาชีพ ส่วนสาขาที่สามพบว่าสามารถใช้สำเนาบัตรประชาชนและหมายเลขเบอร์โทรศัพท์มือถือก็สามารถออกซิมใหม่ได้เลย หากผู้ใช้บริการไม่สามารถมาดำเนินการได้ด้วยตนเองจะต้องมีหนังสือมอบอำนาจพร้อมทั้งบัตรประจำตัวประชาชน ให้ผู้รับมอบอำนาจมาแสดงด้วย ซึ่งก่อนที่เจ้าหน้าที่จะทำการออกซิมใหม่ให้ทางเจ้าหน้าที่จะตรวจสอบหลักฐานและสอบถามประวัติการใช้งานของลูกค้า เพื่อป้องกันการสวมรอยของมิจฉาชีพ จะเห็นได้ว่าจากการสำรวจผู้ให้บริการ DTAC ทั้ง 3 สาขา พบว่าลักษณะการให้บริการจะแตกต่างกันและไม่เป็นรูปแบบเดียวกัน

ผู้ให้บริการ AIS จากการสำรวจทั้ง 3 สาขา พบว่า ทั้ง 3 สาขามีมาตรการในการขอออกซิมใหม่จะต้องใช้บัตรประชาชนตัวจริง พร้อมสำเนาบัตรประจำตัวประชาชนพร้อมทั้งใบแจ้งความกรณีซิมหายและหมายเลขโทรศัพท์มือถือ เพื่อทำการขอออกซิมใหม่ ส่วนกรณีขอเปลี่ยนซิมใหม่จะต้องนำซิมเดิมมาด้วย เพื่อป้องกันการสวมรอยของมิจฉาชีพ หากผู้ใช้บริการไม่สามารถมาดำเนินการได้ด้วยตนเองจะต้องมีหนังสือมอบอำนาจพร้อมทั้งบัตรประจำตัวประชาชน ให้ผู้รับมอบอำนาจมาแสดงด้วย จะเห็นได้ว่าจากการสำรวจผู้ให้บริการ AIS ทั้ง 3 สาขา พบว่าลักษณะการให้บริการในรูปแบบเดียวกัน

จากการวิเคราะห์พบว่าผู้ให้บริการทั้ง 3 ค่าย มีลักษณะการให้บริการที่แตกต่างกัน ในการออกซิมใหม่ที่ไม่เป็นมาตรฐานเดียวกัน เจ้าหน้าที่ควรตรวจสอบหลักฐานและสอบถามประวัติการใช้งานของลูกค้า เพื่อป้องกันบุคคลแอบอ้างสวมรอย แต่ในการขอออกซิมใหม่ก็ยังพบว่ามีช่องโหว่ จากงานวิจัยก่อนหน้า [6] ได้พบจุดบกพร่องของเจ้าหน้าที่ DTAC เนื่องจากใช้ซิมปลอมเปลี่ยนเป็นซิมนาโนซึ่งเป็นอีกเบอร์ โดยเจ้าหน้าที่ไม่ได้ขอตรวจสอบเอกสาร จึงทำให้ได้ซิมใหม่เบอร์ใหม่ และการศึกษาครั้งนี้ได้ค้นพบจุดอ่อนของเจ้าหน้าที่ TRUE ในการขอออกซิมใหม่กรณีซิมหายโดยเจ้าหน้าที่ไม่ได้ขอตรวจสอบหลักฐานเพียงระบุเบอร์ที่หายก็สามารถออกซิมใหม่ได้ ซึ่งข้อบกพร่องเกิดจากเจ้าหน้าที่ ที่ไม่มีมาตรฐานเดียวกัน จึงทำให้เป็นช่องโหว่เกิดขึ้น ซึ่งมีข่าวที่เกิดขึ้นจริงกรณีปลอมเอกสารเพื่อทำการสวมรอยขอออกซิมใหม่ โดยส่วนใหญ่มิจฉาชีพจะใช้การโจมตีแบบวิศวกรรมสังคม ซึ่งเป็นวิธีการที่ง่ายและทำได้จริง กรณีที่เกิดขึ้นเกิดจากเจ้าหน้าที่ ไม่รอบคอบในการตรวจสอบเอกสารและผู้ให้บริการเครือข่ายไม่มีมาตรการที่เป็นรูปแบบเดียวกัน ทำให้มิจฉาชีพอาศัยช่องโหว่ดังกล่าวในการสวมรอย ซึ่งหากคนร้ายได้เบอร์โทรศัพท์ของเหยื่อไป ก็สามารถรับ SMS OTP ในการทำธุรกรรมทางการเงินได้อย่างง่ายดาย ดังนั้นเจ้าหน้าที่จะต้องรัดกุมในการออกซิมใหม่และผู้ใช้บริการควรตรวจสอบซิมการ์ดและโทรศัพท์มือถือเพื่อป้องกันมัลแวร์ ถ้าซิมการ์ดไม่มีสัญญาณควรรีบแจ้งเจ้าหน้าที่ให้ตรวจสอบให้ทันที

4.4 ผลด้านการวิเคราะห์พฤติกรรมของผู้ใช้ Smartphone

การศึกษาค้นคว้าอิระนี้ได้ทำการสำรวจด้วยวิธีการแจกแบบสอบถาม และใช้แบบสอบถามออนไลน์ เพื่อสำรวจพฤติกรรมของกลุ่มผู้ใช้งานแอปพลิเคชันบนสมาร์ทโฟนที่มีอายุ 15 ปีขึ้นไป ซึ่งคาด

ว่ากลุ่มนี้มีโอกาสที่จะเป็นกลุ่มลูกค้าของระบบธนาคารผ่านโทรศัพท์มือถือ ใช้วิธีการสุ่มอย่างง่ายโดยใช้แบบสอบถาม มีผู้กรอกแบบสอบถาม 481 คน ผลสรุปได้ดังนี้

1) จากผลการสำรวจพบว่า มีผู้ใช้งานสมาร์ทโฟนหรือผู้ที่ใช้แท็ปเล็ตร้อยละ 98.5 ไม่ใช้ร้อยละ 1.5 โดยมีผู้ใช้สมาร์ทโฟนหรือผู้ที่ใช้แท็ปเล็ตจำนวน 474 คน และใช้ในการสำรวจในหัวข้อที่ 2) – 12)

2) จากการสำรวจพบว่ามีผู้ใช้แอปพลิเคชันบนสมาร์ทโฟนร้อยละ 97.9 ไม่ใช้ร้อยละ 2.1 เมื่อพิจารณาพบว่าคนส่วนใหญ่นิยมใช้งานแอปพลิเคชัน

3) จากผลการสำรวจพบว่าอายุผู้ใช้สมาร์ทโฟน อายุ 15-21 ปี ร้อยละ 29.3 อายุ 22-60 ปี ร้อยละ 70.5 และอายุ 60 ปีขึ้นไปร้อยละ 0.2 ซึ่งส่วนใหญ่อยู่ระหว่างอายุ 22-60 ปี ซึ่งเป็นช่วงอายุของวัยทำงาน ซึ่งกลุ่มนี้สามารถสมัครเปิดบัญชีธนาคารได้และแบ่งช่วงอายุตามกลุ่มนักเรียน/กลุ่มทำงาน/กลุ่มเกษียณอายุ

4) จากผลการสำรวจพบว่าการศึกษาระดับมัธยมปลายร้อยละ 11.5 ระดับอุดมศึกษาหรือปริญญาตรีร้อยละ 63.8 ระดับปริญญาโทร้อยละ 20.2 ระดับปริญญาเอกร้อยละ 4.5 ซึ่งระดับปริญญาตรีจะสูงกว่า คนส่วนใหญ่จะจบการศึกษาระดับอุดมศึกษาหรือปริญญาตรี

5) จากผลการสำรวจพบว่าอาชีพนักเรียน/นิสิต/นักศึกษา ร้อยละ 43.1 พนักงานบริษัทเอกชน ร้อยละ 12.1 พนักงานของรัฐ/พนักงานรัฐวิสาหกิจ ร้อยละ 33.8 ธุรกิจส่วนตัว/อาชีพอิสระ 8.5 อื่นๆ 2.5 ซึ่งส่วนใหญ่จะเป็นนักเรียน/นิสิต/นักศึกษา

6) จากการสำรวจพบว่ามีผู้ที่รู้จักการ Root หรือ Jailbreak อุปกรณ์สมาร์ทโฟน ร้อยละ 46.4 ไม่รู้จักร้อยละ 53.6

7) จากการสำรวจพบว่ามีผู้ทำการดัดแปลงอุปกรณ์ ร้อยละ 14.6 ไม่ได้ทำการดัดแปลงอุปกรณ์ร้อยละ 85.4 ซึ่งกลุ่มที่ทำการดัดแปลงอุปกรณ์ อาจเป็นกลุ่มที่เสี่ยงต่อปัญหามัลแวร์

8) จากการสำรวจพบว่ารู้จักมัลแวร์ร้อยละ 68.7 ไม่รู้จักมัลแวร์ร้อยละ 31.3

9) จากการสำรวจการติดตั้งแอปพลิเคชันที่อาจได้มาฟรี จาก File .apk หรือ File ที่มาจากเว็บไซต์บนอินเทอร์เน็ต นอกจาก App Store หรือ Play Store พบว่าไม่เคยติดตั้งร้อยละ 84.7 เคยติดตั้งร้อยละ 15.3 พบว่ากลุ่มที่เคยติดตั้งอาจจะเป็นกลุ่มที่เสี่ยงต่อปัญหามัลแวร์

10) จากการสำรวจการสังเกตการณ์ขอสิทธิ์เข้าถึงอุปกรณ์สมาร์ทโฟน ก่อนติดตั้งแอปพลิเคชันพบว่า สังเกตทุกครั้งร้อยละ 52.9 ไม่สังเกตร้อยละ 16.2 สังเกตเป็นบางครั้งร้อยละ 30.9

11) จากการสำรวจการสังเกตชื่อผู้พัฒนาแอปพลิเคชันพบว่า สังเกตร้อยละ 79.9 ไม่สังเกตร้อยละ 20.1

12) จากการสำรวจการอนุญาตให้ติดตั้งแอปพลิเคชันจากภายนอกร้อยละ 87.8 ไม่อนุญาตร้อยละ 12.2 อนุญาต

จากผลการสำรวจจะเห็นว่า มีส่วนน้อยที่อาจเป็นกลุ่มที่เสี่ยงต่อปัญหามัลแวร์คือกลุ่มที่มีการ Root หรือ Jailbreak อุปกรณ์สมาร์ทโฟน และติดตั้งแอปพลิเคชันที่อาจได้มาฟรี จาก File .apk หรือ File ที่มาจากเว็บไซต์บนอินเทอร์เน็ต และคนกลุ่มที่ใช้ Mobile Application นี้ ส่วนใหญ่สังเกตการณ์การขอสิทธิ์เข้าถึงอุปกรณ์ก่อนติดตั้งแอปพลิเคชัน สังเกตชื่อผู้พัฒนาแอปพลิเคชัน และไม่อนุญาตให้ติดตั้งแอปพลิเคชันจากภายนอก จะเห็นได้ว่าการติดตั้งแอปพลิเคชันผู้ใช้งานจะเป็นผู้กำหนดความ

ปลอดภัยและความเป็นส่วนตัว ซึ่งบางครั้งไม่ได้อ่านข้อตกลงหรือสังเกตการขอสิทธิ์ต่างๆ ทำให้ควบคุมได้ยาก จึงทำให้มีความเสี่ยงต่อการโจมตีของมัลแวร์ ซึ่งทักษะพื้นฐานของกลุ่มตัวอย่างนั้น น่าจะสามารถใช้งานระบบ m-banking ได้ปลอดภัยจากปัญหามัลแวร์

บทที่ 5

สรุปอภิปรายผล และข้อเสนอแนะ

การค้นคว้าอิสระนี้จะทำการวิเคราะห์การรักษาความปลอดภัยและความมั่นคงระบบ m-banking ของธนาคารพาณิชย์ในประเทศไทยในส่วนของผู้ใช้งานทั่วไป ทั้งนี้เพื่อเป็นประโยชน์ต่อผู้ใช้งานระบบ m-banking ตลอดจนการศึกษาข้อมูลเพื่อเป็นประโยชน์ต่อธนาคารพาณิชย์ในประเทศไทย ในการป้องกันภัยคุกคามต่างๆ จากการโจมตีด้วยมัลแวร์ การเจาะระบบของแฮกเกอร์และการโจมตีผู้ใช้สมาร์ทโฟน การศึกษานี้จะทำการสำรวจและวิเคราะห์ในส่วนของการใช้บริการระบบ m-banking ผ่านแอปพลิเคชันบนสมาร์ทโฟนเท่านั้น เพื่อเป็นแนวทางในการใช้งานที่ปลอดภัยและเป็นแนวทางในการพัฒนาระบบ m-banking ให้มีความปลอดภัยมากยิ่งขึ้น โดยมีลำดับขั้นตอนการสรุปผลที่ได้จากการศึกษาและข้อเสนอแนะดังนี้

5.1 สรุปอภิปรายผล

การค้นคว้าอิสระนี้จะทำการวิเคราะห์การรักษาความปลอดภัยและความมั่นคงระบบ m-banking ของธนาคารพาณิชย์ในประเทศไทยในส่วนของผู้ใช้งานทั่วไป โดยสามารถสรุปผลได้ดังนี้

5.1.1 ผลด้านความปลอดภัยของระบบ m-banking

ผลจากการสำรวจของการวิเคราะห์ด้านความปลอดภัยของระบบ m-banking โดยทำการสำรวจ เริ่มตั้งแต่ขบวนการสมัครเปิดบัญชีธนาคาร การสมัครใช้งานระบบ m-banking ลักษณะการใช้งานต่างๆ ไปจนถึงขบวนการยกเลิกการใช้บริการและปิดบัญชีธนาคาร ซึ่งสามารถสรุปผลตามเกณฑ์ที่สำรวจได้ดังต่อไปนี้

1) การเปิดบัญชีธนาคาร จากการวิเคราะห์พบว่าในการเปิดบัญชีทุกธนาคารจะต้องใช้บัตรประชาชนในการยืนยันตัวตน มี 2 ธนาคารที่ไม่อนุญาตให้ใช้ใบอนุญาตขับรถและทะเบียนบ้าน และทุกธนาคารจะอนุญาตให้ใช้บัตรข้าราชการแต่ต้องยื่นควบคู่กับสำเนาทะเบียนบ้าน จะเห็นได้ทุกธนาคารจะให้ความสำคัญในการตรวจสอบหลักฐานที่ใช้ในการสมัคร แต่การให้บริการของแต่ละธนาคารไม่เป็นรูปแบบเดียวกัน ขาดมาตรฐานในการตรวจสอบการให้บริการของเจ้าหน้าที่ เนื่องจากมีข่าวที่เกิดขึ้นดังที่กล่าวมาแล้ว โดยมิจฉาชีพอาศัยช่องโหว่ในการตรวจสอบเอกสารของเจ้าหน้าที่เข้าสวมรอยเปิดบัญชีธนาคาร โดยการใช้หลักฐานปลอม ซึ่งมีงานวิจัยในต่างประเทศ [6] พบว่ามีวิธีการที่รัดกุมกว่าโดยพนักงานจะต้องผ่านการฝึกอบรมการตรวจเอกสารก่อน ดังนั้นธนาคารควรมีมาตรการที่เป็นแนวทางเดียวกันและเพิ่มวิธีการยืนยันตัวตนที่เฉพาะเจาะจง เช่น การแสกนลายนิ้วมือ

2) การสมัครใช้งานระบบ m-banking จากการวิเคราะห์พบว่ามี 2 ธนาคารที่สามารถสมัครผ่านแอปพลิเคชันได้ และมี 5 ธนาคารที่จะต้องขอรหัสสมัครบริการจากตู้เอทีเอ็มเพื่อใช้ยืนยันในการสมัครใช้งานผ่านแอปพลิเคชัน ซึ่งการสมัครใช้งานผ่านตู้เอทีเอ็มจะเป็นมาตรการรักษาความปลอดภัยขั้นสูงของธนาคาร ที่ใช้ยืนยันตัวตนความเป็นเจ้าของบัญชีซึ่งจะต้องใช้รหัสเอทีเอ็มควบคู่กับรหัสสมัครบริการและมี 2 ธนาคารที่มีจุดเด่นต่างจากธนาคารอื่นคือธนาคาร B จะกำหนดให้ใช้ 1

บัญชีสามารถใช้งานกับ 1 เบอร์โทรศัพท์เท่านั้น และธนาคาร C หากต้องการใช้งานในเครื่องอื่น หมายเลขอื่น จะต้องทำการอนุญาตขอเพิ่มอุปกรณ์ในการเข้าใช้งาน จะต้องขออนุญาตโดยใช้รหัส OTP จากเครื่องหลักเพื่อยืนยันการเพิ่มอุปกรณ์ ซึ่งข้อจำกัดที่เพิ่มมานี้ โดยการผูกระบบ m-banking ไว้ที่เครื่องโทรศัพท์มือถือ จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะการจะเข้าใช้งาน ต้องมีการยืนยันตัวตนด้วยการเป็นเจ้าของเบอร์โทรศัพท์มือถือนั้นจริง หรือถือครองโทรศัพท์ที่ติดตั้งระบบ m-banking เท่านั้น ดังนั้นแม้ว่าแฮกเกอร์จะทราบ PIN หรือ รหัสผ่าน ก็ไม่สามารถเข้าใช้งานได้ จะต้องทำการขโมยโทรศัพท์มือถือ หรือเบอร์โทรศัพท์ของลูกค้าด้วย จึงจะเข้าใช้งานได้

3) การเข้าสู่ระบบ m-banking ของธนาคารทั้ง 6 ธนาคาร พบว่า มี 3 ธนาคารที่เข้าสู่ระบบด้วย PIN มี 3 ธนาคารที่เข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่าน ซึ่งในการใส่ PIN ก็เหมือนการใส่รหัสบัตร ATM ในการทำธุรกรรมทางการเงิน และยากต่อการคาดเดาของมิจฉาชีพ นอกจากนั้นยังมีระบบ Limit Log-in ที่จำกัดจำนวนครั้งในการ Login หากป้อนข้อมูลผิดเกินจำนวนครั้งที่กำหนด Account จะถูกล็อคทันที ซึ่งจะเห็นว่าทั้ง 6 ธนาคารมีความปลอดภัยใกล้เคียงกัน

4) การลืมชื่อผู้ใช้, รหัสผ่าน , PIN จะพบว่าถ้า Reset ผ่านสาขาจะมีความปลอดภัยมากกว่าซึ่งเจ้าหน้าจะให้นำสมุดบัญชีและบัตรประชาชนยืนยันตัวตนก่อนทำรายการ แต่จะมีช่องโหว่ระหว่างการส่งข้อมูล ซึ่งธนาคาร B จะส่งข้อมูลมาให้ลูกค้าทางอีเมล์ซึ่งทำให้ถูกดักจับข้อมูลได้ และการ Reset ผ่านคอลเซ็นเตอร์อาจเป็นช่องโหว่ให้มิจฉาชีพแอบสวมรอย โดยใช้การโจมตีแบบวิศวกรรมทางสังคมได้ เจ้าหน้าที่ธนาคารควรตรวจสอบข้อมูลและใช้คำถามที่เฉพาะเจาะจงตัวบุคคล เพราะการแจ้งผ่านคอลเซ็นเตอร์ไม่สามารถตรวจสอบได้ว่าเป็นตัวจริง ดังนั้นวิธีนี้จึงอาจเป็นจุดอ่อนได้ ดังนั้นการ Reset ข้อมูลผ่านตู้เอทีเอ็มเป็นวิธีการที่ปลอดภัยที่สุดเพราะต้องใช้บัตรและรหัสเอทีเอ็ม เป็นการยืนยันตัวสองชั้น โดยการถือครองบัตร และทราบรหัสของบัตร

5) การเปลี่ยนเบอร์มือถือพบว่ามี 1 ธนาคารที่อนุญาตให้เปลี่ยนเบอร์ผ่านคอลเซ็นเตอร์ ซึ่งธนาคารจะต้องให้ความสำคัญเกี่ยวกับการตรวจสอบหลักฐานต่างๆ และการสอบถามข้อมูลที่สามารถยืนยันตัวบุคคลที่แท้จริง เพื่อความให้ถูกต้อง เนื่องจากมีข่าวที่เกิดขึ้นดังที่กล่าวมาข้างต้นเกี่ยวกับการปลอมแปลงเอกสารเพื่อออกซิมใหม่ แล้วทำการขอแจ้งเปลี่ยนเบอร์มือถือในระบบ m-banking ซึ่งเป็นวิธีการที่มิจฉาชีพใช้ในการสวมรอยทำธุรกรรมทางการเงิน จากการวิเคราะห์ความผิดพลาดเกิดจากผู้ให้บริการเครือข่ายที่ไม่มีมาตรการตรวจสอบข้อมูล ดังนั้นควรมีมาตรการที่เป็นแนวทางเดียวกันและเพิ่มวิธีการยืนยันตัวตน นอกจากจะตรวจสอบเอกสารแล้วควรมีการยืนยันตัวตนที่เฉพาะเจาะจง เช่น การแสกนลายนิ้วมือ

6) ลักษณะของ OTP พบว่าบางธนาคารเปิดให้มีระยะเวลาการกรอก OTP ที่นานต่างกันไป จากการทดสอบ พบว่าระบบ OTP ในประเทศไทยมี Delay น้อยมาก ดังนั้นระยะเวลาไม่เกิน 3 นาที ที่ธนาคาร C ใช้อยู่ น่าจะเหมาะสมกว่า เนื่องจากระยะเวลาที่นานเกินไป อาจเป็นช่องโหว่ให้มิจฉาชีพดักขโมยข้อมูล หากโทรศัพท์ที่ใช้รับ SMS OTP ติดมัลแวร์ ทำให้ SMS OTP ส่งไปยังเครื่องของมิจฉาชีพและทำให้มิจฉาชีพมีเวลาไปทำธุรกรรมก่อนเจ้าของบัญชี

7) การเชื่อมต่ออินเทอร์เน็ตพบว่าธนาคาร B ไม่อนุญาตให้เชื่อมต่อผ่าน Wi-Fi เพราะมีโอกาสถูกดักจับข้อมูล และแทรกกลางการสื่อสารได้ง่ายกว่า โดยอนุญาตให้เชื่อมต่อผ่าน 3G/4G เท่านั้น เนื่องจากเทคโนโลยี 3G มีการเข้ารหัสข้อมูลที่ส่งผ่าน ด้วยอัลกอริธึม UEA1/UIA1 Kasumi

Block Cipher ส่วนเทคโนโลยี 4G [47] จะมีมาตรฐานความปลอดภัยที่สูงไปอีก โดยการเข้ารหัสด้วยอัลกอริธึม UEA2/UIA2 Snow 3G Stream Cipher ดังนั้นจึงมีความปลอดภัยสูงจากการดักจับข้อมูลของแฮกเกอร์เมื่อเทียบกับการเชื่อมต่อผ่าน Wi-Fi แต่การปิดช่องทางการเชื่อมต่อ Wi-Fi ของธนาคาร B จะทำให้ลูกค้าอาจไม่เลือกใช้ระบบ m-banking ของธนาคาร แต่อาจเปลี่ยนไปใช้บริการในระบบ i-banking ที่มีความมั่นคงน้อยกว่าแทน เพราะสามารถเชื่อมต่อผ่าน Wi-Fi ได้ นอกจากนี้จากการทดลองที่จะกล่าวในหัวเรื่องถัดไป พบว่าเมื่อระบบ m-banking ถูกออกแบบมาดี ถึงแม้จะเล่นผ่าน Wi-Fi ก็ไม่สามารถที่จะดักจับข้อมูลได้โดยง่ายเหมือนระบบ i-banking ดังนั้นการปิด Wi-Fi จึงอาจไม่ใช่ทางเลือกที่ดี

8) มาตรการด้านความปลอดภัยอื่นๆ พบว่าธนาคาร F มีระยะเวลา Auto Log off นานเกินไป เมื่อเทียบกับธนาคารอื่นๆ ซึ่งระยะเวลาที่นานเกินไปนี้ อาจทำให้มิจฉาชีพแอบสวมรอยการทำธุรกรรมได้ และ ธนาคารทุกธนาคารควรมีระบบการแจ้งเตือนการเข้าใช้งานทุกครั้งโดยแจ้งผ่านอีเมล์ ซึ่งจะทำให้เจ้าของบัญชีทราบความเคลื่อนไหวและรู้ทันหากไม่ได้เข้าระบบด้วยตนเอง

9) การเลิกใช้บริการระบบ m-banking โดยทั่วไปยังไม่มีช่องโหว่หรือเกิดกรณีการจู่โจมที่เกิดขึ้นในเรื่องนี้โดยตรง แต่เพื่อความปลอดภัย ธนาคารควรตระหนักถึงการตรวจสอบการยืนยันตัวหากมีการยกเลิกการใช้งานเพราะอาจจะมีการกลั่นแกล้งเพื่อต้องการทำให้บัญชีมีปัญหา ที่เรียกว่า Denial of Services หรือมิจฉาชีพอาจทำการยกเลิกการใช้งานแล้วขอเปิดใหม่เพื่อทำการสวมรอย ซึ่งทางธนาคารควรเข้มงวดในการตรวจสอบความถูกต้องในการขอเลิกใช้บริการ โดยเฉพาะอย่างยิ่งธนาคาร B, C และ D อนุญาตให้มีการยกเลิกผ่านคอลเซ็นเตอร์ ซึ่งอาจมีโอกาสถูกโจมตีแบบวิศวกรรมสังคม โดยมิจฉาชีพได้ง่ายที่สุด หากคำถามที่ใช้ตรวจสอบยืนยันตัวตนไม่ดีพอ

10) การขอปิดบัญชีพบว่าพบว่าทุกธนาคารสามารถปิดได้ที่สาขาที่เปิดและมี 3 ธนาคารที่สามารถปิดบัญชีธนาคารต่างสาขาได้ ซึ่งถือว่ามีความปลอดภัย แต่ขึ้นอยู่กับขบวนการตรวจเอกสารหลักฐานในการยืนยันตัวตนที่แท้จริง ซึ่งพบว่าขั้นตอนนี้ โดยทั่วไปมีความปลอดภัย เพราะลูกค้าจะต้องนำบัตรประชาชนและสมุดบัญชีมาใช้ควบคู่ในการปิดบัญชี และมี 3 ธนาคาร ซึ่งจะต้องนำใบแจ้งความมาประกอบด้วยเมื่อทำสมุดบัญชีเงินฝากหาย จากการวิเคราะห์กรณีคดีความที่เกิดขึ้น ยังไม่มีประเด็นด้านการโจมตีแบบวิศวกรรมสังคม ที่เกี่ยวกับเรื่องนี้โดยตรง แต่ธนาคารควรตระหนักถึงการตรวจสอบการยืนยันตัวหากมีการมาปิดบัญชีเพราะอาจจะมีการกลั่นแกล้ง หรือทำการยกเลิกการใช้งานแล้วขอเปิดใหม่เพื่อทำการสวมรอย

5.1.2 ผลด้านความมั่นคงระบบ m-banking

การวิเคราะห์ประเด็นด้านความมั่นคงจะเป็นเรื่องของเทคนิค โดยจะทำการทดสอบใน 2 วิธีคือ SSL Sniff และ SSL Strip ในขณะที่กำลังเข้าใช้งานระบบธนาคารผ่านโทรศัพท์มือถือ ซึ่งจะทำการดักจับข้อมูลผ่านการเชื่อมต่ออินเทอร์เน็ตทั้ง 6 ธนาคารเพื่อทดสอบและได้ผลการสำรวจ สรุปผลดังนี้

1) ผลการทดสอบการโจมตีด้วยวิธีการ SSL Sniff ต่อระบบ m-banking พบว่าไม่สามารถดักจับข้อมูลได้ เนื่องจากโปรแกรมของระบบ m-banking application จะไม่ยอมรับ หากมีการส่งใบ Certificate ปลอม ระบบถูกออกแบบให้ไม่ทำงาน ซึ่งการเขียนโปรแกรมระดับชั้นแอปพลิเคชันจะกำหนด Certificate ที่แท้จริงจากธนาคารผู้พัฒนาตั้งแต่ขั้นพัฒนาการใช้งานจึงมีความปลอดภัย

มั่นคงสูง ไม่เหมือนในระบบ i-banking ที่รายงานไว้ในงานวิจัยอื่นๆ ก่อนหน้านี้ จะให้ผู้ใช้เป็นคนตรวจสอบว่า Certificate นั้นถูกต้องหรือไม่ ซึ่งมีโอกาสถูกจู่โจมได้ หากผู้ใช้งานระบบ i-banking ไม่สังเกต โดยจากการทดลองของงานวิจัยนี้ต่อจากระบบ i-banking ก็พบว่าสามารถจะจู่โจมด้วย SSL Sniff และดักจับข้อมูลในระบบ i-banking ได้ เนื่องจากเว็บเบราว์เซอร์ไม่สามารถตรวจสอบได้ว่ามีการดักจับข้อมูลจากแฮกเกอร์ หากผู้ใช้รู้เท่าไม่ถึงการณ์กดยอมรับ Certificate ปลอมหรือเข้าไปในเว็บปลอมที่แฮกเกอร์ใช้ดักจับข้อมูลก็จะถูกขโมยข้อมูลที่สำคัญไปได้โดยง่าย ดังนั้น จากการทดลองนี้จะเห็นได้ชัดเจนว่า ระบบ m-banking โดยทั่วไปมีความมั่นคงต่อการจู่โจมด้วย SSL Sniff มากกว่าระบบ i-banking

2) ผลการทดสอบการโจมตีด้วยวิธีการทดลองดักจับข้อมูลด้วยเทคนิค SSL Strip ซึ่งทำการดักจับ Packet ที่ Client ในขณะที่ใช้งานระบบธนาคารบนโทรศัพท์มือถือผ่านแอปพลิเคชัน พบว่าขั้นตอนการ Request มีการเรียกใช้โพรโทคอล HTTPS ทำให้ไม่สามารถโจมตีแบบ SSL Strip ได้ เพราะเริ่มต้น Session เป็น HTTPS อัตโนมัติ ไม่เหมือนกับระบบ i-banking ที่ให้ผู้ใช้เป็นผู้เริ่ม Session การสื่อสาร ซึ่งอาจเป็น HTTP แล้ว Web Server ค่อยทำการ Redirect ไปเป็น HTTPS ที่อาจโดน SSL Strip ได้

5.1.3 ผลด้านความปลอดภัยของผู้ให้บริการ Mobile Sim

จากผลการวิเคราะห์พบว่าผู้ให้บริการทั้ง 3 ค่าย มีลักษณะการให้บริการที่แตกต่างกันในการออกซิมใหม่ที่ไม่เป็นมาตรฐานเดียวกัน เจ้าหน้าที่ควรตรวจสอบหลักฐานและสอบถามประวัติการใช้งานของลูกค้า เพื่อป้องกันบุคคลแอบอ้างสวมรอย แต่ในการขอออกซิมใหม่ก็ยังพบว่ามีช่องโหว่ จากงานวิจัยก่อนหน้า [6] ได้พบจุดบกพร่องของเจ้าหน้าที่ DTAC เนื่องจากใช้ซิมปลอมเปลี่ยนเป็นซิมนาโน ซึ่งเป็นอีกเบอร์ โดยเจ้าหน้าที่ไม่ได้ขอตรวจสอบเอกสาร จึงทำให้ได้ซิมใหม่เบอร์ใหม่ และการศึกษาครั้งนี้ได้ค้นพบจุดอ่อนของเจ้าหน้าที่ TRUE ในการขอออกซิมใหม่กรณีซิมหายโดยเจ้าหน้าที่ไม่ได้ขอตรวจสอบหลักฐานเพียงระบุเบอร์ที่หายก็สามารถออกซิมใหม่ได้ ซึ่งข้อบกพร่องเกิดจากเจ้าหน้าที่ ที่ไม่มีมาตรฐานเดียวกันจึงทำให้เป็นช่องโหว่เกิดขึ้น ซึ่งมีข่าวที่เกิดขึ้นจริงกรณีปลอมเอกสารเพื่อทำการสวมรอยขอออกซิมใหม่ โดยส่วนใหญ่มิจฉาชีพจะใช้การโจมตีแบบวิศวกรรมสังคม ซึ่งเป็นวิธีการที่ง่ายและทำได้จริง กรณีที่เกิดขึ้นเกิดจากเจ้าหน้าที่ ไม่รอบคอบในการตรวจสอบเอกสารและผู้ให้บริการเครือข่ายไม่มีมาตรการที่เป็นรูปแบบเดียวกัน ทำให้มิจฉาชีพอาศัยช่องโหว่ดังกล่าวในการสวมรอย ซึ่งหากคนร้ายได้เบอร์โทรศัพท์ของเหยื่อไป ก็สามารถรับ SMS OTP ในการทำธุรกรรมทางการเงินได้อย่างง่ายดาย ดังนั้นเจ้าหน้าที่จะต้องรัดกุมในการออกซิมใหม่และผู้ใช้บริการควรตรวจสอบซิมการ์ดและโทรศัพท์มือถือเพื่อป้องกันมัลแวร์ ถ้าซิมการ์ดไม่มีสัญญาณควรรีบแจ้งเจ้าหน้าที่ให้ตรวจสอบให้ทันที

5.1.4 ผลการวิเคราะห์พฤติกรรมผู้ใช้ Smartphone

จากผลการวิเคราะห์จะเห็นว่า มีส่วนน้อยที่อาจเป็นสุ่มเสี่ยงต่อปัญหามัลแวร์คือกลุ่มที่มีการ Root หรือ Jailbreak อุปกรณ์สมาร์ทโฟน และติดตั้งแอปพลิเคชันที่อาจได้มาฟรี จาก File .apk หรือ File ที่มาจากเว็บไซต์บนอินเทอร์เน็ต และคนกลุ่มที่ใช้ Mobile Application นี้ ส่วนใหญ่สังเกตการณ์การขอสิทธิ์เข้าถึงอุปกรณ์ก่อนติดตั้งแอปพลิเคชัน สังเกตชื่อผู้พัฒนาแอปพลิเคชัน และไม่อนุญาตให้ติดตั้งแอปพลิเคชันจากภายนอก จะเห็นได้ว่าการติดตั้งแอปพลิเคชันผู้ใช้งานจะเป็นผู้กำหนดความปลอดภัยและความเป็นส่วนตัว ซึ่งบางครั้งไม่ได้อ่านข้อตกลงหรือสังเกตการขอสิทธิ์ต่างๆ ทำให้

ควบคุมได้ยาก จึงทำให้มีความเสี่ยงต่อการโจมตีของมัลแวร์ ซึ่งทักษะพื้นฐานของกลุ่มตัวอย่างนั้น น่าจะสามารถใช้งานระบบ m-banking ได้ปลอดภัยจากปัญหามัลแวร์

5.2 ผลสัมฤทธิ์ที่ได้จากการศึกษา

จากการศึกษาค้นคว้าอิสระนี้ ได้ทำการสำรวจและวิเคราะห์ความปลอดภัยและความมั่นคงของระบบ m-banking อยู่ 2 ประเด็นคือด้านความปลอดภัย (Safety) และด้านความมั่นคง (Security) ซึ่งสามารถสรุปได้ดังนี้

5.2.1 ผลการศึกษาปัญหา

จากการศึกษาปัญหาการใช้งานระบบ m-banking ในปัจจุบันพบว่ายังมีปัญหาในด้านความปลอดภัยและความมั่นคง พบว่ามีข่าวที่เกิดขึ้นเกี่ยวกับการโจมตีด้านวิศวกรรมทางสังคม เพื่อสวมรอยขโมยข้อมูล การแพร่กระจายแอปพลิเคชันปลอม การโจมตี SMS OTP การโจมตีด้วยมัลแวร์ เพื่อทำการดักจับข้อมูลที่สำคัญ ซึ่งระบบ m-banking มีจำนวนผู้ใช้งานเพิ่มมากขึ้นเรื่อยๆ จึงทำให้มีความเสี่ยงต่อความปลอดภัย ซึ่งก่อนหน้านี้ยังไม่มีการศึกษาปัญหาของระบบ m-banking ที่ครอบคลุมทั้ง 2 ประเด็นคือด้านความปลอดภัยและความมั่นคง การศึกษาครั้งนี้จึงทำการวิเคราะห์ให้ครอบคลุมทั้งด้านความปลอดภัยและความมั่นคง

5.2.2 ผลการวิเคราะห์ปัญหา

จากการวิเคราะห์ความมั่นคงของระบบ m-banking ในประเทศไทย เราได้พบจุดอ่อนในด้านความปลอดภัย (Safety) ในส่วนที่เกี่ยวข้องกับการบริหารจัดการของธนาคารและความมั่นคง ช่องโหว่ด้านการตรวจสอบหลักฐานยืนยันตัวตน เนื่องจากคนร้ายใช้วิธีการโจมตีแบบวิศวกรรมสังคม ส่วนด้านความมั่นคง (Security) ที่เกี่ยวกับกับด้านเทคนิควิธีในการโจมตี พบว่าการใช้งานผ่านแอปพลิเคชันมีความปลอดภัยสูงกว่าการใช้งานระบบอินเทอร์เน็ตแบงก์กิ้ง เนื่องจากในการทดสอบระบบไม่สามารถดักจับข้อมูลได้ แต่ยังมีช่องโหว่ในด้านของมัลแวร์ ซึ่งปัญหาของมัลแวร์นั้นจุดอ่อนเกิดจากตัวบุคคล เนื่องจากไม่รอบคอบในด้านการโหลดแอปพลิเคชัน ซึ่งผลจากการทดสอบนี้สามารถใช้เป็นทิศทางและแนวทางในการปรับปรุงระบบ m-banking ต่อไปในอนาคต

5.3 ข้อเสนอแนะ

การค้นคว้าอิสระนี้ได้ทำการวิเคราะห์ธนาคารพาณิชย์ในประเทศไทยอยู่ 2 ประเด็นคือ ด้านความปลอดภัย (Safety) ในส่วนที่เกี่ยวข้องกับการบริหารจัดการและความมั่นคง (Security) ที่เป็นเรื่องทางเทคนิควิธี ในการศึกษาได้ทำการทดสอบการโจมตีด้านเทคนิคเพียง 2 วิธี ซึ่งเป็นวิธีที่คนร้ายนิยมใช้มากที่สุดในช่วงที่ผ่านมา แต่อย่างไรก็ตามการประเมินทางเทคนิคจะต้องทำอยู่เรื่อยๆ เพราะมีวิธีการจู่โจมเกิดขึ้นใหม่อยู่เสมอ ในเรื่องของความมั่นคงทางเทคนิคจึงควรทำอยู่อย่างต่อเนื่อง และวิธีใหม่ๆ โดยประเด็นที่น่าสนใจในการไปต่อยอดคือทำการทดสอบการโจมตีที่หลากหลายเทคนิควิธี เพื่อให้ครอบคลุมมากยิ่งขึ้น

เอกสารอ้างอิง

[1] Article A. รายงานผลการวิจัยมาตรการรักษาความมั่นคงปลอดภัยระบบ Internet Banking และ ระบบ Mobile Banking ของธนาคารในประเทศไทย. [สืบค้นเมื่อ 30 มีนาคม 2559]; ได้จาก: https://www.acisonline.net/?p=961&lang=th.

[2] พัฒนรัฐ พุดหล้า, สมนึก พ่วงพรพิทักษ์. การวิเคราะห์ความมั่นคงและปลอดภัยของระบบอินเทอร์เน็ตแบงก์กิ้งในประเทศไทย. The Eleventh National Conference on Computing and Information Technology 2015; กรกฎาคม 2015; Bangkok. หน้า 99-105.

[3] Park KC, Shin JW, Lee BG. Analysis of Authentication Methods for Smartphone Banking Service using ANP. KSII Transactions on Internet & Information Systems [Article] 2014; 8[6]: 2087-2103.

[4] Filiol E, Irolla P. (In)Security of Mobile Banking and of Other. Black Hat Asia; Singapore. March 2015; pp.1-22.

[5] Islam S. Security Analysis Of Mobile Two-Factor Authentication Schemes. Article: Intel Technology Journal, 2014; 18[4]:pp. 138-161.

[6] Rachana S. Security and Safety Evaluation and Enhancement of Internet Banking System: A Case Study of Cambodian Public Bank Plc. MSc Thesis: Mahasarakham University; 2015.

[7] ธนพล พุกเส็ง,ศิรปัฐช์ บุญครอง. การสำรวจการรักษาความปลอดภัยในการใช้งานอินเทอร์เน็ตแบงค์กิ้งธนาคารพาณิชย์ไทยสำหรับลูกค้าบุคคล วารสารวิทยาศาสตร์และเทคโนโลยี 2558; ปีที่ 23 ฉบับที่ 1.หน้า 141-152.

[8] Schmeh K. "Cryptography and Public Key Infrastructure on the Internet". The Atrium, Southearn Gate, Chichester: Jonh Wiley & Sons Ltd.; 2003.

[9] 10 อันดับ ธนาคารที่คนไทยใช้บริการมากที่สุด. [สืบค้นเมื่อ 10 กันยายน 2558]; ได้จาก: http://www.toptenthailand.com/topten/detail/20131121182254853.

[10] E-Banking (Electronic Banking). [สืบค้นเมื่อ 5 เมษายน 2558]; ได้จาก: http://udomchai-itm0225.blogspot.com/2009/10/e-banking.html.

[11] blognone.com. การปรับปรุงระบบไอทีครั้งใหญ่ของธนาคารกสิกรไทย. [สืบค้นเมื่อ 30 มีนาคม 2559]; ได้จาก: https://www.blognone.com/node/72423.

[12] ศัพท์บัญญัติ ราชบัณฑิตสถาน. [สืบค้นเมื่อ 12 ตุลาคม 2558]; ได้จาก: http://rirs3.royin.go.th/coinages/webcoinage.php.

[13] leveraging K. Mobile Banking 2015; Global Trends and their Impact on Banks 2015; July 2015.

[14] การชำระเงินทางอิเล็กทรอนิกส์ (e-Payment). [สืบค้นเมื่อ 20 มีนาคม 2559]; ได้จาก: https://www.etda.or.th/content/e-payment.html.

[15] Agency ETD, Organization) P. Thailand Internet User Profile 2015. [สืบค้นเมื่อ 20 มีนาคม 2559]; ได้จาก: file:///C:/Users/Administrator/Downloads/IUP_2015_interactive_290316.pdf.

[16] ธนาคารแห่งประเทศไทย. บริการทางการเงินผ่านโทรศัพท์เคลื่อนที่; 2557.

[17] เจาะลึกสถิติธนาคารไทย ที่ได้รับ Engagement บนโลกออนไลน์ Social Media มากที่สุด. [สืบค้นเมื่อ 15 มิถุนายน 2558]; ได้จาก: http://www.it24hrs.com/2014/banking-social-media-engagement/.

[18] บริการ K-Moblie Banking PLUS และ ATM SIM. [สืบค้นเมื่อ 10 กันยายน 2558]; ได้จาก: http://www.kasikornbank.com/.

[19] บริการ KTB Online@Mobile. [สืบค้นเมื่อ 10 กันยายน 2558]; ได้จาก: http://www.ktb.co.th/.

[20] บริการ SCB Mobile Banking. [สืบค้นเมื่อ 10 กันยายน 2558]; ได้จาก: http://www.scb.co.th/.

[21] บริการ TMB M - Banking. [สืบค้นเมื่อ 10 กันยายน 2558]; ได้จาก: https://www.tmbbank.com.

[22] บริการ Mobile iBanking. [สืบค้นเมื่อ 10 กันยายน 2558]; ได้จาก: www.bangkokbank.com/.

[23] กรุงศรีเผยยอดออนไลน์เติบโตแข็งแกร่ง พร้อม 3 แนวทางรุกโมบายแอพพลิเคชั่น. [สืบค้นเมื่อ 1 ตุลาคม 2558];ได้จาก: http://www.siamturakij.com/main/news.

[24] IOS Apps | Application บนระบบปฏิบัติการ IOS. [สืบค้นเมื่อ 12 ตุลาคม 2558]; ได้จาก: http://www.chaiyohosting.com/ios-apps/.

[25] Apple ยังครองอันดับ 1 ส่วนแบ่งตลาดแท็บเล็ตโลก แม้ยอดขายจะลดลง. [สืบค้นเมื่อ 4 พฤษภาคม 2558]; ได้จาก: http://www.macthai.com.

[26] 3G คืออะไร. [สืบค้นเมื่อ 15 มิถุนายน 2558]; ได้จาก: https://wordpress.com

[27] เครือข่ายมือถือ 3G, H, H+ ต่างกันอย่างไร. [สืบค้นเมื่อ 15 มิถุนายน 2558]; ได้จาก: http://www.jaymart.co.th/3g-4g-differences.asp.

[28] ระบบ Wi-Fi. [สืบค้นเมื่อ 5 พฤษภาคม 2558]; ได้จาก: http://unoom.blogspot.com/2009/09/wi-fi_13.html.

[29] วิศวกรรมสังคม. [สืบค้นเมื่อ 2 กุมภาพันธ์ 2558]; ได้จาก: http://th.wikipedia.org/wiki/.

[30] it24hrs.com. คนร้ายสวมรอยเป็นเจ้าของบัญชี Internet Banking โอนเงินออกสูญหลายแสน. [สืบค้นเมื่อ 15 กันยายน 2558];ได้จาก: http://www.it24hrs.com.

[31] it24hrs.com. ผู้ใช้มือถือต้องระวัง! ถูกจารกรรมเงินในบัญชีได้ จากการรับ SMS ! [สืบค้นเมื่อ 15 ตุลาคม 2558];ได้จาก: http://www.it24hrs.com.

[32] เตือนผู้ใช้ Android อย่าโหลดลิงค์ apk ใน sms ข้อความ “แจ้งให้ทราบ...”. [สืบค้นเมื่อ 1 สิงหาคม 2558];ได้จาก: http://www.it24hrs.com/2014/sms-apk-danger/.

[33] ระวัง แอพธนาคารปลอม ระบาดบน Play Store ของมือถือ Android. [สืบค้นเมื่อ 5 กันยายน 2558]; ได้จาก: http://www.it24hrs.com/2014/app-e-banking-fake-on-android/.

[34] ช่องโหว่ของซิมการ์ด (SIM) ที่ทำให้ผู้ไม่ประสงค์ดีสามารถสำเนาซิมการ์ดได้โดยง่าย. [สืบค้นเมื่อ 12 ตุลาคม 2558]; ได้จาก: http://www.uih.co.th/knowledge/view/604.

[35] นักวิจัย พบช่องโหว่ จากซิมการ์ด ที่อาจกระทบผู้ใช้งาน กว่าล้านซิม ทั่วโลก. [สืบค้นเมื่อ 12 พฤศจิกายน 2558]; ได้จาก: http://www.techmoblog.com.

[36] Masque Attack ภัยคุกคามใหม่บน iPhone และ iPad. [สืบค้นเมื่อ 5 กันยายน 2558]; ได้จาก: https://www.techtalkthai.com/apple-ios-masque-attack-threat/.

[37] ภัย Internet Banking รุนแรง โดนฉกเงินกว่า 3 แสน. [สืบค้นเมื่อ 10 ตุลาคม 2558];ได้จาก: http://www.it24hrs.com/2013/fake-mobile-sms-banking-hack/.

[38] ผู้ใช้ Apple ระวังมัลแวร์สายพันธุ์ใหม่! ระบาดบน iOS และ OS X.[สืบค้นเมื่อ10มิถุนายน2558]; ได้จาก: http://www.it24hrs.com/2014/wirelurker-new-osx-ios-malware-virus/.

[39] เตือนระวังลงแอพไฟฉายบนมือถือก็โดนแฮกข้อมูลคุณได้. [สืบค้นเมื่อ 26 เมษายน 2558]; ได้จาก: http://www.it24hrs.com/2014/flashlight-app-android-hack-privacy/.

[40] ความปลอดภัยในการใช้ Mobile Banking มั่นใจได้. [สืบค้นเมื่อ 10 ตุลาคม 2558]; ได้จาก: http://www.buddybe.com/index.php?lay=show&ac=article&Id=128.

[41] ประพจน์ ธรรมศิรารักษ์,สมนึก พ่วงพรพิทักษ์. การวิเคราะห์ปัญหาและการทดสอบความมั่นคงของเทคโนโลยีรหัสผ่านแบบใช้ครั้งเดียว. JSci Technol MSU 2014; หน้า 11-15.

[42] บุญชม ศรีสะอาด. การวิจัยเบื้องต้น. กรุงเทพฯ: สุวีริยาสาส์น; 2554.

[43] Subsorn P, Limwiriyakul S. A comparative analysis of the security of internet banking in Australia:a customer perspective. In: Limwiriyakul S, editor. International Cyber Resilience conference; pp. 69-83.

[44] Masrek MN, Mohamed IS, Daud NM, Omar N. Technology Trust and Mobile Banking Satisfaction: A Case of Malaysian Consumers. Procedia - Social and Behavioral Sciences 2014; 12953-58. http://www.sciencedirect.com/science/article/pii/S1877042814028298

[45] Loke SP, Noor NM, Khalid K. Customer Satisfaction Towards Internet Banking Services: Case Analysis on a Malaysian Bank. Proceedings of IEEE International Conference Colloquium on Humanities, Science and Engineering Research (CHUSER) 3-4 December 2012; 159-163.

[46] สุวรรณี ธูปจีน, ระดม เจือจันทร์, ศิรปัฐช์ บุญครอง. การตรวจจับพฤติกรรมและป้องกันมัลแวร์บนโทรศัพท์มือถือแอนดรอยด์.วารสารวิทยาศาสตร์และเทคโนโลยี. บทความวิชาการ ; 2558; หน้า 141-152.

[47] How is 4G LTE encrypted. [สืบค้นเมื่อ 1 พฤศจิกายน 2558]; ได้จาก: http://security.stackexchange.com/questions/21395/how-is-4g-lte-encrypted.

[48] Security HN. SIM Swap fraud is gaining momentum. [สืบค้นเมื่อ 10 เมษายน 2559]; ได้จาก: https://www.helpnetsecurity.com/2016/04/19/sim-swap-fraud/.

ภาคผนวก

ภาคผนวก ก

ตารางการหาค่า IOC จากความเห็นผู้เชี่ยวชาญ

คำถามข้อที่	ความเห็นผู้เชี่ยวชาญ									รวม	เฉลี่ย
	คนที่ 1			คนที่ 2			คนที่ 3				
	-1	0	1	-1	0	1	-1	0	1		
1.			✓			✓			✓	3	1
2.			✓			✓			✓	1	1
3.			✓			✓			✓	3	1
4.			✓			✓			✓	3	1
5.			✓			✓			✓	3	1
6.			✓			✓			✓	1	1
7.		✓				✓			✓	2	0.6
8.		✓				✓			✓	3	0.6
9.			✓			✓			✓	3	1
10.			✓			✓			✓	3	1
11.			✓			✓			✓	3	1
12.			✓			✓			✓	3	1

ภาคผนวก ข

แบบสอบถาม

แบบสอบถามชุดนี้จัดขึ้นเพื่อเก็บรวบรวมข้อมูลของกลุ่มผู้ใช้งานแอปพลิเคชันบนสมาร์ทโฟน

1. **คุณเป็นผู้ใช้สมาร์ทโฟนหรือผู้ที่ใช้แท็ปเล็ตหรือไม่**
   - ◉ ใช่
   - ○ ไม่ใช่
2. **ปัจจุบันคุณใช้งานแอปพลิเคชันบนสมาร์ทโฟนหรือไม่ ?**
   - ◉ เคยใช้ (กรุณาตอบแบบสอบถามข้อต่อไป)
   - ○ ไม่เคยใช้ (จบแบบสอบถาม ขอบคุณค่ะ)
3. **ปัจจุบันคุณมีอายุเท่าใด**
   - ◉ 15-21 ปี
   - ○ 22-60 ปี
   - ○ 60 ปีขึ้นไป
4. **ระดับการศึกษาสูงสุดของคุณ**
   - ○ ระดับมัธยมปลาย
   - ○ อุดมศึกษาหรือปริญญาตรี
   - ○ ปริญญาโท
   - ○ ปริญญาเอก
5. **ปัจจุบันท่านมีอาชีพใด**
   - ○ นักเรียน/นิสิต/นักศึกษา
   - ○ พนักงานบริษัทเอกชน
   - ○ พนักงานของรัฐ/พนักงานรัฐวิสาหกิจ
   - ○ ธุรกิจส่วนตัว/อาชีพอิสระ
   - ○ อื่นๆ
6. **คุณรู้จักการ Root หรือ Jailbreak อุปกรณ์สมาร์ทโฟนหรือไม่**
   - ○ รู้จัก
   - ○ ไม่รู้จัก
7. **คุณได้ทำการดัดแปลงอุปกรณ์สมาร์ทโฟนหรือไม่**
   - ○ ใช่
   - ○ ไม่ใช่

8. คุณรู้จักมัลแวร์หรือไม่

- รู้จัก
- ไม่รู้จัก

9. คุณเคยติดตั้งแอปพลิเคชันที่อาจได้มาฟรี จาก file .apk หรือ file ติดตั้ง ที่มาจากเว็บไซต์บนอินเทอร์เน็ต นอกจาก App Store หรือ Play Store หรือไม่

- เคยติดตั้ง
- ไม่เคยติดตั้ง

10. คุณได้สังเกตการณ์ขอสิทธิ์เข้าถึงอุปกรณ์สมาร์ทโฟน ก่อนติดตั้งแอปพลิเคชันหรือไม่

- สังเกตทุกครั้ง
- ไม่ได้สังเกตเลย
- สังเกตบ้างไม่สังเกตบ้าง

11. คุณสังเกตชื่อผู้พัฒนาแอปพลิเคชันก่อนติดตั้งหรือไม่

- สังเกต
- ไม่สังเกต

12. คุณอนุญาตให้ติดตั้งแอปพลิเคชันจากแหล่งที่เชื่อถือได้หรือไม่รู้จักบนสมาร์ทโฟนหรือไม่

- รูปที่ 1 ไม่อนุญาตให้ติดตั้ง
- รูปที่ 2 อนุญาตให้ติดตั้ง

รูปที่ 1 ไม่อนุญาตให้ติดตั้งกดยกเลิก

รูปที่ 2 อนุญาตให้ติดตั้งกดตกลง

ประวัติย่อผู้ศึกษา

ประวัติย่อผู้ศึกษา

ชื่อ นามสกุล	นางสาวนิภาพร แสงทวี
วัน เดือน ปีเกิด	วันที่ 8 ธันวาคม พ.ศ. 2530
จังหวัด และประเทศที่เกิด	จังหวัดมหาสารคาม ประเทศไทย
ประวัติการศึกษา	
พ.ศ. 2545	มัธยมศึกษาตอนต้น โรงเรียนผดุงนารี มหาสารคาม
พ.ศ. 2548	มัธยมศึกษาตอนปลาย โรงเรียนผดุงนารี มหาสารคาม
พ.ศ. 2552	บริหารธุรกิจบัณฑิต (บธ.บ.) สาขาวิชาคอมพิวเตอร์ธุรกิจ มหาวิทยาลัยมหาสารคาม
พ.ศ. 2554	ระดับประกาศนียบัตรบัณฑิต สาขาวิชาชีพครู คณะครุศาสตร์ มหาวิทยาลัยราชภัฏมหาสารคาม
พ.ศ. 2559	ปริญญาวิทยาศาสตรมหาบัณฑิต (วท.ม.) สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหาสารคาม
ตำแหน่งและสถานที่ทำงาน	เจ้าหน้าที่ประเมินราคาทรัพย์สิน สำนักงานธนารักษ์พื้นที่ จังหวัดมหาสารคาม
ที่อยู่ที่สามารถติดต่อได้	บ้านเลขที่ 297 หมู่ 3 TJ Villa ตำบลท่าขอนยาง อำเภอกันทรวิชัย จังหวัดมหาสารคาม 44150