# การวิเคราะห์ความปลอดภัยและความมั่นคงสำหรับระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย

# An Analysis of Safety and Security for Mobile Banking Systems in Thailand

นิภาพร แสงทวี, สมนึก พ่วงพรพิทักษ์

Nipaporn Seangtawee[1], Somnuk Puangpronpitag[2]

Received: 4 February 2016; Accepted: 10 May 2016

## บทคัดย่อ

Mobile Banking (m-banking) เป็นบริการธนาคารออนไลน์ผ่านทางแอปพลิเคชันบนสมาร์ทโฟน ซึ่งเป็นทางเลือก ที่ต่างจากระบบธนาคารผ่านเครือข่ายอินเทอร์เน็ต (i-banking) ซึ่งใช้โปรแกรมเว็บแอปพลิเคชันผ่านเบราว์เซอร์ เมื่อเทียบกับ i-banking แล้ว m-banking คาดว่าน่าจะมีความปลอดภัยและมั่นคงมากกว่า แต่ยังมีรายงานเกี่ยวกับคดีความด้านการโจมตีระบบธนาคารเพิ่มมากขึ้น ในช่วงไม่กี่ปีที่ผ่านมา ดังนั้นงานวิจัยหลายชิ้นก่อนหน้านี้ ได้วิเคราะห์ปัญหาความมั่นคงความปลอดภัยของ i-banking แต่ส่วนใหญ่ยังไม่ได้มุ่งเน้นในส่วนของ m-banking โดยมีเพียงบางส่วนที่ได้ทำการสำรวจเกี่ยวกับ m-banking แต่ส่วนใหญ่เน้นทางด้านเทคนิคหรือด้านความมั่นคง แต่ยังขาดการสำรวจด้านการจัดการหรือด้านความปลอดภัยของ 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

## Abstract

Mobile banking (m-banking) is an online banking service via a smartphone application. It is an alternative to internet banking (i-banking), which uses a web based application via a web browser. In comparison to i-banking, m-banking has been seen as safer and securer. However, several bank-hacking crimes have been reported during the last few years. So, several previous studies analyzed the i-banking security/safety issues. Yet, most of them have not yet focused on m-banking. Some of them have investigated m-banking only on the technical (security) merits but not the management (safety) side. Significantly, most of them have not yet analyzed according to the following critical points occurred crime cases, detailed observation on the real services, 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 six banks in Thailand, we have found several weaknesses of the m-banking systems. The contribution from this work can provide direction to improve the security and safety of the m-banking systems.

**Keyword**: Mobile Banking, Safety, Security, Social Engineer

---

*[1] นิสิตปริญญาโท, [2]อาจารย์, กลุ่มวิจัยความมั่นคงสารสนเทศและเครือข่ายชั้นสูง, คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม อำเภอกันทรวิชัย จังหวัดมหาสารคาม 44150*

*[1] Master's degree student, [2]Lecturer, Information Security and Advanced Network Group, Faculty of Informatics, Mahasarakham University, Kantarawichai District, Maha Sarakham 44150, Thailand.*

** Corresponding author: Somnuk Puangpronpitag, ISAN Research Group, Faculty of Informatics, Mahasarakham University, Kantarawichai District, Maha Sarakham 44150, Thailand. somnuk.p@msu.ac.th*

## บทนำ

จากเดิมการทำธุรกรรมการเงินจะต้องไปที่สาขาหรือตู้เอทีเอ็ม ซึ่งทำให้เสียเวลาในการเดินทางและการต่อคิว ธนาคารจึงเริ่มนำเทคโนโลยีมาอำนวยความสะดวกให้กับลูกค้า โดยเริ่มมีการใช้ระบบ Internet Banking (i-banking) ผ่านเว็บเบราว์เซอร์บนอุปกรณ์คอมพิวเตอร์และสมาร์ทโฟน ต่อมาเนื่องจากการใช้สมาร์ทโฟน เริ่มมีบทบาทในชีวิตประจำวันมากขึ้น เพราะเป็นอุปกรณ์ที่มีขนาดเล็กพกพาสะดวก ธนาคารต่างๆ จึงมีการพัฒนาจาก i-banking มาเป็นระบบ Mobile Banking (m-banking) หรือการทำธุรกรรมการเงินทางธนาคารผ่านโทรศัพท์มือถือ โดยใช้งานผ่าน โมบายแอปพลิเคชัน ที่มีการออกแบบให้ง่ายต่อการใช้งานและมีระบบความปลอดภัยมั่นคงที่สูงขึ้น

ระบบ m-banking ถูกพัฒนาให้มีความปลอดภัยมั่นคงมากขึ้น กว่าการใช้งานผ่านเว็บเบราว์เซอร์ เพราะระบบจะกำหนดค่าความปลอดภัยจากธนาคารที่พัฒนาแอปพลิเคชัน ซึ่งโปรแกรมที่เป็นแอปพลิเคชันบนสมาร์ทโฟน จะสามารถควบคุมกลไกความมั่นคงปลอดภัยได้ดีกว่า การเขียนโปรแกรมเพื่อรันผ่านเว็บเบราว์เซอร์ ตัวอย่างเช่น กลไกการบังคับใช้ Hypertext Transfer Protocol Secure (HTTPS), การใช้ระบบ Personal Identity Number (PIN) Code, การใช้ระบบ One Time Password (OTP) เป็นต้น ซึ่งสามารถช่วยลดความผิดพลาดของผู้ใช้จากการกรอก URL ผ่านเว็บเบราว์เซอร์ ทำให้ลดปัญหาการ Phishing Attack[5] อีกทั้งมีการเติบโตของเครือข่ายการให้บริการอินเทอร์เน็ตผ่านโทรศัพท์เคลื่อนที่ได้ขยายจาก 3G ไปสู่ 4G ทำให้มีความเร็วในการรับส่งข้อมูลรวดเร็วขึ้นและระบบเหล่านี้ ยังมีการเข้ารหัสที่สามารถป้องกันการโจมตีด้วยวิธีแทรกกลางการสื่อสาร Man In The Middle (MITM) Attack ได้ดีกว่าการใช้ Wi-Fi อีกด้วย

จากงานวิจัยก่อนหน้านี้[1-6] ได้มีการศึกษาปัญหาและทดสอบความปลอดภัยมั่นคงของระบบ i-banking พบว่ายังมีปัญหาคือ อาจถูกดักจับชื่อผู้ใช้และรหัสผ่านได้ โดยการโจมตีด้วยวิธีแทรกกลางการสื่อสาร และการจู่โจม HTTPS[5] ด้วยเทคนิควิธี เช่น SSL Sniff และ SSL Strip จากปัญหาดังกล่าวได้ส่งผลเสียต่อการทำธุรกรรมบนเว็บเบราว์เซอร์ผ่านระบบ i-banking

นอกจากนี้ ยังมีงานวิจัยก่อนหน้านี้จำนวนหนึ่ง ที่ได้ทำการศึกษาความมั่นคงของระบบ m-banking ที่น่าจะมีความปลอดภัยมากกว่าระบบ i-banking แต่งานวิจัยเหล่านี้ส่วนใหญ่ยังเป็นการศึกษาเฉพาะด้านความมั่นคง ซึ่งเน้นด้านเทคนิควิธีแต่ยังไม่ได้ครอบคลุมถึงการวิจัยด้านความปลอดภัย ทั้งนี้ Schmeh[7] ได้ชี้ให้เห็นว่าความปลอดภัย ซึ่งเป็นด้านการบริหารจัดการ มีความสำคัญไม่น้อยกว่าด้านเทคนิควิธี ซึ่งเป็นด้านความมั่นคงและต้องมีการดูแลควบคู่กันไป

ดังนั้นในงานวิจัยนี้ จึงได้เสนอวิเคราะห์ทั้งด้านความปลอดภัยและความมั่นคงของระบบ m-banking ในกลุ่มลูกค้าบุคคล โดยใช้ธนาคารพาณิชย์ในประเทศไทย 6 แห่ง เป็นกรณีศึกษา โดยทำการสำรวจทั้งสองประเด็น คือ 1) ประเด็นด้านความปลอดภัย (Safety) คือการบริหารจัดการระบบ โดยทำการสังเกตการณ์ขบวนการเปิดบัญชี การสมัครใช้งานระบบ m-banking จนถึงการปิดบัญชี โดยอาศัยข้อมูลคดีความด้าน e-banking ที่เกิดขึ้นในประเทศไทย เป็นฐานในการวิเคราะห์ 2) ประเด็นด้านความมั่นคง (Security) จะเกี่ยวกับด้านเทคนิควิธี โดยทำการจำลองการโจมตีระบบ m-banking เพื่อทดสอบความมั่นคงและช่องโหว่ในการใช้งาน ในฝั่งของผู้ใช้ รวมทั้งสำรวจผู้ให้บริการเครือข่าย และวิเคราะห์พฤติกรรมของผู้ใช้สมาร์ทโฟนที่อาจเสี่ยงต่อปัญหามัลแวร์ ซึ่งเป็นภัยคุกคามที่สำคัญบนสมาร์ทโฟนแอปพลิเคชัน

## ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

### 1. แนวโน้มของระบบธนาคารผ่านโทรศัพท์มือถือ

การใช้งานระบบธนาคารผ่านโทรศัพท์มือถือเป็นที่นิยมมากขึ้นเรื่อยๆ ตามการขยายตัวของตลาดสมาร์ทโฟน ซึ่งทาง Juniper Research[8] คาดว่าจำนวนผู้ใช้งานระบบ m-banking จากปี ค.ศ. 2014 จะเพิ่มขึ้นถึง 1.8 พันล้านคน ภายในสิ้นปี ค.ศ. 2019 ดังแสดงใน (Figure 1) ในส่วนของประเทศไทยมีอัตราการเติบโตค่อนข้างสูงถึงร้อยละ 81.4[9] โดยการทำธุรกรรมการชำระเงินผ่านบริการของระบบ m-banking ได้มีการขยายตัวสูงขึ้นทั้งปริมาณและมูลค่าซึ่งสอดคล้องกับพฤติกรรมของผู้ใช้บริการที่ใช้อินเทอร์เน็ตและโทรศัพท์เคลื่อนที่[10] อีกทั้งการพัฒนาฟังก์ชันต่างๆ ของโทรศัพท์เคลื่อนที่และเครือข่ายอินเทอร์เน็ตให้มีประสิทธิภาพมากขึ้น

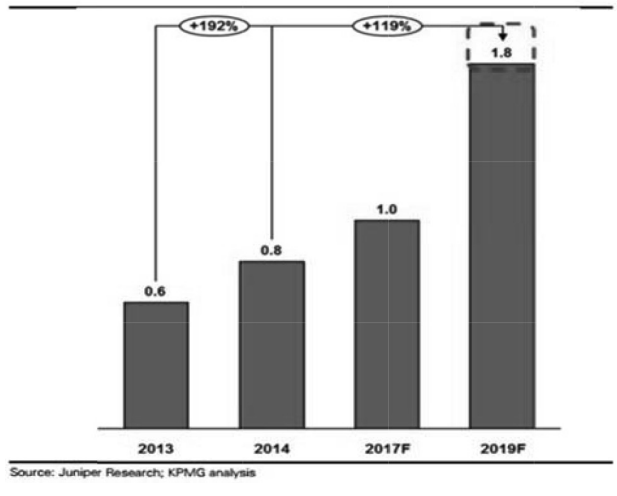


**Figure 1** Global mobile banking users[8]

**2. Mobile Banking vs. Internet Banking**

Mobile Banking คือการทำธุรกรรมผ่านโทรศัพท์มือถือ โดยใช้งานผ่านแอปพลิเคชัน มีฟีเจอร์ต่าง ๆ ที่ใช้งานง่าย พกพาสะดวก ใช้งานได้ทุกที่และซอฟต์แวร์ของแอปพลิเคชันจะบังคับใช้โพรโทคอล HTTPS และเทคนิควิธีด้านความมั่นคงหลายอย่าง ซึ่งทำให้ระบบมีความมั่นคงมากขึ้น

Internet Banking คือ การทำธุรกรรมบนคอมพิวเตอร์หรืออุปกรณ์ โดยใช้งานผ่านเบราว์เซอร์ เพื่อเข้าถึงเว็บแอปพลิเคชันที่ธนาคารพัฒนาขึ้นให้ใช้บริการ โดยในด้านความปลอดภัยมั่นคง ของเบราว์เซอร์อาจจะไม่บังคับใช้ HTTPS เมื่อโดนโจมตีผู้ใช้ต้องกรอกผ่าน URL เป็น https:// และสังเกตรูปกุญแจสีเขียว และต้องจำชื่อ URL ของธนาคาร ซึ่งหากกรอกข้อมูลผิดหรือไม่สังเกตอาจถูกโจมตีหรือถูกแทรกกลางการสื่อสารไปสู่เว็บไซต์ปลอมได้

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

**3. ความปลอดภัย vs. ความมั่นคง**

ความปลอดภัย (Safety) หมายถึงกระบวนการบริหารจัดการเพื่อความปลอดภัยของระบบสารสนเทศ เช่น การออกกฎหมาย พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[12] หรือกฎระเบียบที่ควบคุมการใช้งานระบบสารสนเทศต่าง ๆ รวมไปถึงการมีจรรยาบรรณ ชั้นความลับของข้อมูล ต่างก็เป็นเรื่องของการบริหารจัดการที่จะทำให้ระบบมีความปลอดภัยมากยิ่งขึ้น

ความมั่นคง (Security) หมายถึง เรื่องของเทคนิควิธีที่ทำให้ระบบคอมพิวเตอร์ปลอดภัย เช่น เทคนิคการเข้ารหัสและถอดรหัส เทคนิคการยืนยันตัวตนด้วยการลงลายมือชื่อดิจิทัล หรืออื่นๆ ที่เกี่ยวข้องกับเทคนิควิธี

Schmeh[7] ได้กล่าวว่า ความปลอดภัยและความมั่นคงมีความสำคัญเท่าเทียมกัน โดยจะขาดส่วนใดส่วนหนึ่งไม่ได้ ทั้งสองส่วนจะต้องได้รับการสนับสนุนให้ดีควบคู่กันไป ดังนั้นในงานวิจัยนี้จะทำการวิเคราะห์ระบบ m-banking ทั้งในด้านของความปลอดภัยและความมั่นคง

**4. ภัยคุกคามการใช้งานระบบธนาคารออนไลน์**

**1) ปัญหาการโจมตีแบบวิศวกรรมสังคม**

วิธีการโจมตีแบบวิศวกรรมสังคม (Social Engineering) หรือการใช้วิธีทางจิตวิทยาหลอกลวงเหยื่อเพื่อโจมตีระบบ สำหรับการโจมตีระบบ e-banking ได้มีการใช้เทคนิควิธีนี้ จนปรากฏเป็นคดีมากมาย ตัวอย่างเช่นคดีของคุณบุณพจน์ พราหมนก[13] เมื่อปี พ.ศ.2557 มิจฉาชีพได้สร้างหลักฐานปลอมเพื่อขอสมัครเปิดบัญชีธนาคารที่มีชื่อเดียวกันกับเหยื่อ ปลอมเอกสารแจ้งความมือถือหายและปลอมสำเนาใบขับขี่[13] ดัง (Figure 2) เพื่อใช้ในการขอออกซิมใหม่ แต่คุณบุณพจน์ พราหมนก ได้มีการป้องกันโดยแจ้งศูนย์บริการไว้หากมีการแจ้งซิมหายจะต้องแจ้งรหัส 4 ตัวกับเจ้าหน้าที่ก่อนจึงจะสามารถออกซิมใหม่ได้ แต่มิจฉาชีพได้แจ้งซิมหายที่สาขาย่อยของศูนย์บริการ ซึ่งคาดว่าสาขาย่อยนั้น ยังไม่ได้รับแจ้งข้อมูลของการบอกรหัส 4 ตัว จึงออกซิมใหม่เบอร์เดิมให้มิจฉาชีพ

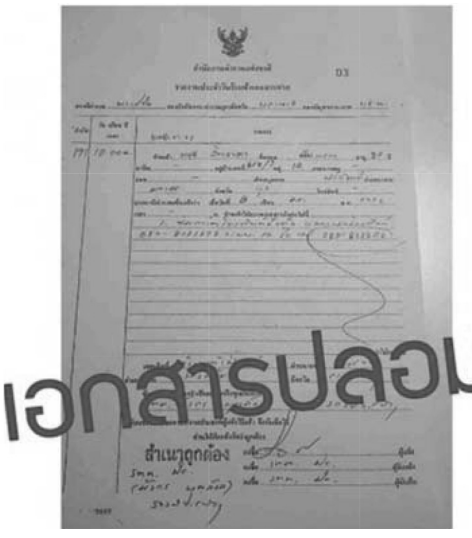


**Figure 2** the faked document[13]

จากนั้นมิจฉาชีพก็ทำการเข้าระบบ i-banking โดยใส่ชื่อผู้ใช้ของคุณบุณพจน์ แล้วก็ทำเป็นแจ้งลืม รหัสผ่านเพื่อให้ธนาคารส่งหมายเลข SMS OTP มาทางโทรศัพท์มือถือ แล้วทำการเปลี่ยนรหัสผ่านใหม่และเข้าระบบ i-banking สั่งโอนเงินออกได้เหมือนกับเป็นเจ้าของตัวจริง จากปัญหาดังกล่าวพบว่าผู้ให้บริการเครือข่ายไม่มีมาตรการที่เป็นแนวทางเดียวกันในการขอออกซิมใหม่ของแต่ละค่าย และแต่ละสาขา จึงมีจุดอ่อนที่เป็นช่องโหว่ทำให้มิจฉาชีพใช้วิธีการดังกล่าวในการแอบสวมรอยปลอมเอกสาร ซึ่งงานวิจัยนี้จะได้ทำการวิเคราะห์ในส่วนนี้ รวมถึงคดีอื่นๆ ที่อาศัยวิธีการโจมตีแบบวิศวกรรมสังคมเพื่อใช้ในการทดสอบด้านความปลอดภัยของระบบที่เกี่ยวข้องกับระบบ m-banking ต่อไป

**2) วิเคราะห์ปัญหา SMS Spoofing**

ในปัจจุบันพบว่ามีการโจรกรรมในรูปแบบส่ง SMS โดยมีมิจฉาชีพแอบส่ง SMS ปลอมหน้าตาเหมือนเบอร์คอลเซ็นเตอร์ของธนาคารหลอกลวงให้เหยื่อคลิกลิงค์เพื่อดาวน์โหลดหรือติดตั้งโปรแกรม จากการตรวจสอบพบว่าในมือถือของผู้เสียหาย มีโทรจันแฝงอยู่ โดยทำหน้าที่แอบส่งชื่อผู้ใช้ รหัสผ่านและ SMS ส่งไปยังคนร้าย จึงทำให้เจ้าของบัญชีตัวจริงที่รอ SMS OTP จากธนาคาร แต่ไม่ได้รับข้อความเพราะ SMS OTP นั้น ถูกมิจฉาชีพขโมยไป ซึ่งแอปพลิเคชันปลอมเบอร์นี้พบบน Play Store และ App Store จากปัญหาดังกล่าวจะเห็นได้ว่า ถึงจะมีการป้องกันความปลอดภัย 2 ชั้น หรือ Two Factor Authentication (2FA) ก็ยังไม่ปลอดภัยจากมิจฉาชีพ

**3) วิเคราะห์ปัญหามัลแวร์**

จากกรณีข่าวที่เกิดขึ้นเมื่อวันที่ 26 มีนาคม พ.ศ. 2557[14] ธนาคารพาณิชย์หลายแห่ง ได้ประกาศเตือนประชาชน ว่ามีแอปพลิเคชันธนาคารปลอมเกลื่อนบน Play Store โดยแอปพลิเคชันดังกล่าว ไม่ได้พัฒนาจากทางธนาคาร โดยได้แจ้งไปยังกูเกิ้ล ให้ถอดแอปพลิเคชันปลอมออกจาก Play Store และก่อนดาวน์โหลดให้สังเกตชื่อของธนาคารผู้พัฒนา เช่น ธนาคารกรุงไทย จำกัด (มหาชน) ชื่อผู้พัฒนาคือ Krung Thai Bank PCL. ซึ่งผู้ใช้งานต้องสังเกตชื่อนักพัฒนาจะต้องเป็นชื่อธนาคารนั้นๆ ไม่ใช่ชื่อนักพัฒนารายอื่นอย่างเช่น Scientifika Media ซึ่งเป็นแอปพลิเคชันปลอม โดยมีมัลแวร์แอบแฝงเพื่อขโมยข้อมูลในสมาร์ทโฟน จากปัญหาดังกล่าวงานวิจัยนี้จะนำไปวิเคราะห์ในด้านการสำรวจพฤติกรรมผู้ใช้งานสมาร์ทโฟนที่ส่งผลต่อปัญหามัลแวร์ ว่าเข้าใจปัญหาและทราบแนวทางในการป้องกันตนเองจากมัลแวร์หรือไม่

นอกจากคดีข้างต้นแล้ว งานวิจัยนี้ยังได้ใช้คดีอื่นๆ ที่เกี่ยวกับการทำธุรกรรมออนไลน์ โดยได้รับการอนุเคราะห์ข้อมูลจากฝ่ายคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ (DSI) เพื่อใช้ในการวิเคราะห์ปัญหา

## 5. ความมั่นคงของระบบ m-banking

1) Triple Lock Security

Triple Lock Security[6] เป็นระบบความมั่นคงปลอดภัยที่ถูกพัฒนาขึ้น เพื่อป้องกันการเข้าใช้งานจากกลุ่มบุคคลผู้ไม่หวังดี ทั้งจากการโจรกรรมข้อมูลของกลุ่มแฮกเกอร์หรือการนำเอารหัสผ่านไปใช้ในการทำธุรกรรม ซึ่งเทคโนโลยี Triple Lock Security นี้ ระบบจะมีการตรวจสอบข้อมูลทั้ง 3 ชั้น เช่น 1) ล็อกด้วยหมายเลขมือถือจากผู้ให้บริการเครือข่าย 2) ล็อกด้วย ID ของเครื่องโทรศัพท์ที่ใช้งาน เมื่อเปิดการใช้งานระบบก็จะรู้ว่าเป็นเครื่องนั้นที่ใช้งานจริง จึงปลอมแปลงค่อนข้างยาก 3) ล็อกรหัสผ่าน 6 หลัก ดังนั้นจึงเป็นความแตกต่างระหว่างการทำธุรกรรมบนระบบ m-banking และระบบ i-banking ที่มีระบบล็อกหลายชั้น ซึ่งการทำธุรกรรมบนระบบ i-banking ที่ผ่านเบราว์เซอร์ จะใช้เพียงชื่อผู้ใช้และรหัสผ่านจึงทำให้การใช้งานผ่านแอปพลิเคชันมีความมั่นคงปลอดภัยสูงขึ้นมากกว่า เทคโนโลยี Triple Lock Security ระบบ m-banking นั้นสามารถสร้างระบบความมั่นคง ได้หลายชั้นกว่านั้นก็ได้ เช่น อาจเป็น 4 หรือ 5 ชั้นก็ได้ ทั้งนี้ขึ้นอยู่กับการพัฒนา สมาร์ทโฟนแอปพลิเคชัน ของแต่ละธนาคาร ซึ่งต่างจากการพัฒนาเว็บแอปพลิเคชัน ของธนาคารที่ใช้งานผ่านระบบ i-banking ที่ต้องพัฒนาโปรแกรมที่มารัน อยู่บนเว็บเบราว์เซอร์ ซึ่งมีข้อจำกัดบนสมาร์ทโฟนแอปพลิเคชัน

2) Two Factor Authentication (2FA)

2FA คือการเพิ่มระบบรักษาความปลอดภัยในการใช้บริการอิเล็กทรอนิกส์แบงก์กิ้ง โดยการเพิ่มขั้นตอนที่จะต้องทำการพิสูจน์ความเป็นเจ้าของบัญชีอีก 1 ขั้นนอกเหนือไปจากการมีชื่อผู้ใช้งานและรหัสผ่านเข้าใช้งาน ในกรณีของธนาคารผู้ให้บริการธุรกรรมการเงินผ่านโทรศัพท์มือถือมักเลือกใช้ระบบ OTP เป็นมาตรการความปลอดภัย ซึ่ง OTP จะมีลักษณะเฉพาะ มีการเปลี่ยนแปลงรหัสทุกครั้งไม่ซ้ำเดิมและเมื่อถูกใช้ไปแล้ว ก็จะไม่สามารถใช้งานได้อีก จึงช่วยลดความเสี่ยงที่อาจเกิดขึ้น จากการถูกเจาะขโมยข้อมูลรหัสผ่าน ที่อาจกระทำได้โดยง่าย หากใช้รหัสผ่านเพียงอย่างเดียว สำหรับระบบ m-banking จะตรวจสอบหมายเลขโทรศัพท์มือถือและหมายเลข IMEI ของเครื่องโทรศัพท์มือถือมาเป็นปัจจัยในการยืนยันตัวตนเพิ่มอีก ดังนั้นจึงมีโอกาส มีความมั่นคงมากขึ้น เพราะเป็น Multiple Factor Authentication มากกว่า 2 ชั้น

## 6. งานวิจัยที่เกี่ยวข้อง

ได้มีงานวิจัยก่อนหน้านี้จำนวนมากที่ทำการศึกษาความปลอดภัยมั่นคงของระบบ i-banking เช่น ธนพล พุกเส็ง และศิรปัฐช์ บุญคลอง[6] ได้นำเสนอการรักษาความปลอดภัยการใช้งานระบบ i-banking ธนาคารพาณิชย์ไทยสำหรับกลุ่มลูกค้าบุคคล Park และคณะ[1] ได้ทำการวิเคราะห์วิธีรับรองความถูกต้องสำหรับธนาคารที่ให้บริการเครือข่ายแก่สมาร์ทโฟนในประเทศเกาหลี พัฒนรัฐ พุดหล้าและสมนึก พ่วงพรพิทักษ์[5] ได้ทำการวิเคราะห์ความมั่นคงและปลอดภัยของระบบอินเทอร์เน็ตแบงก์กิ้งในประเทศไทย Rachana[4] ได้นำเสนอการเปรียบเทียบการรักษาความมั่นคงและความปลอดภัยของธนาคารในประเทศไทย และธนาคารในประเทศกัมพูชา Subsorn และคณะ[15] ได้ตรวจสอบความปลอดภัยของระบบ i-banking ใน 16 ธนาคารของประเทศออสเตรเลีย โดยงานวิจัยเหล่านี้ได้พบจุดอ่อนของระบบ i-banking ที่เป็นการใช้โปรแกรมธนาคารผ่านเว็บเบราว์เซอร์

ว่าสามารถโจมตีด้วยวิธีการแทรกกลางการสื่อสารได้ค่อนข้างง่าย และเนื่องจากมีข้อจำกัดของ เว็บโปรแกรมมิ่ง หลายอย่างในการเสริมสร้างความมั่นคงซึ่งระบบ m-banking ที่เป็นโมบายแอปพลิเคชันน่าจะมีข้อจำกัดด้านนี้น้อยกว่า แต่งานวิจัยเหล่านี้ยังไม่ได้ศึกษาความปลอดภัยและมั่นคงของระบบ m-banking ซึ่งเป็นตัวเลือกใหม่แต่อย่างไร

มีบางงานวิจัยที่ได้ทำการศึกษาเกี่ยวกับระบบ m-banking อยู่บ้าง เช่น ACIS Research LAB[16] ได้วิเคราะห์ความมั่นคงของธนาคารในประเทศไทยทั้งระบบ i-banking และระบบ m-banking สุวรรณี ธูปจีนและคณะ[17] ได้เสนอวิธีการตรวจจับพฤติกรรมของมัลแวร์ โดยทำการวิเคราะห์ตัวอย่างของสายพันธุ์มัลแวร์บางสายพันธุ์ที่สามารถตรวจพบได้บนสมาร์ทโฟนแอนดรอยด์ Islam[3] ได้สำรวจความมั่นคงของระบบ m-banking และระบบการชำระเงินออนไลน์ Filiol และ Iroll[2] ได้ทำการวิจัยเกี่ยวกับการรักษาความมั่นคงระบบ m-banking และแอปพลิเคชันมือถืออื่นๆ โดยเปรียบเทียบการรักษาความมั่นคงของธนาคารตะวันตกและธนาคารเอเชีย พบว่าธนาคารเอเชียมีความปลอดภัยสูงกว่าธนาคารตะวันตก ซึ่งมีวิธีการรักษาความปลอดภัยของข้อมูลโดยใช้โพรโทคอล SSL ที่ใช้สื่อสารข้อมูลระหว่างไคลเอนต์และเซิร์ฟเวอร์ การใช้โพรโทคอล HTTPS จะทำให้ไม่สามารถโจมตีแบบแทรกกลางการสื่อสารได้และการใช้งานผ่านโทรศัพท์มือถือจะมีการตรวจสอบข้อมูลผ่านหมายเลข IMEI, MAC Address, หมายเลขโทรศัพท์มือถือ จะเห็นได้ว่าการใช้งานผ่านแอปพลิเคชันของธนาคารบนโทรศัพท์มือถือจะมีความปลอดภัยกว่าการใช้งานผ่านบราว์เซอร์บนคอมพิวเตอร์ Jiraporn และคณะ[18] ได้ศึกษาปัจจัยที่มีผลต่อการยอมรับของระบบ m-banking ในเขตกรุงเทพมหานครและเปรียบเทียบกับประเทศอื่นๆ โดยทำแบบสอบถามเพื่อสำรวจผลกระทบของปัจจัยต่างๆ เพื่อรวบรวมปัจจัยที่มีผลต่อการยอมรับ ระบบ m-banking เพื่อเป็นแนวทางให้ธนาคารดึงดูดลูกค้ามากขึ้นและเพื่อเปรียบเทียบความแตกต่างระบบ m-banking จากต่างประเทศ พบว่าปัจจัยบวกที่มีอิทธิพลต่อความตั้งใจที่จะใช้ระบบ m-banking มากกว่าปัจจัยลบ Baraka และคณะ[19] ได้นำเสนอแบบจำลองการรักษาความปลอดภัยมั่นคงของระบบ m-banking ในสหสาธารณรัฐแทนซาเนีย โดยได้เสนอการเข้ารหัส SMS ระหว่างไคลเอนต์และเซิร์ฟเวอร์เพื่อตรวจสอบความถูกต้องของข้อมูล เพื่อให้มีความปลอดภัยมากขึ้นกว่าการรับ SMS จากเบอร์โทรศัพท์โดยตรง ซึ่งงานวิจัยกลุ่มนี้ ได้นำเสนองานวิจัยด้านปัญหาความมั่นคงเกี่ยวกับระบบ m-banking ซึ่งเน้นทางด้านเทคนิคเท่านั้น ยังขาดการสำรวจด้านการจัดการ หรือด้านความปลอดภัยของระบบ m-banking ที่สำคัญงานเหล่านั้นยังขาดการสังเกตการณ์จากกรณีจริง การศึกษาวิเคราะห์กรณีคดีการโจมตีระบบธนาคารที่เกิดก่อนหน้านี้ และการทดลองทดสอบการโจมตีจากฝั่งของผู้ใช้จริง

ดังนั้นบทความนี้จึงทำการวิเคราะห์ระบบ m-banking ทั้งด้านความมั่นคงและความปลอดภัย และครอบคลุมประเด็นที่ขาดไปที่ได้กล่าวไว้ในขั้นต้น

## วิธีดำเนินการวิจัย

งานวิจัยนี้ได้เสนอการวิเคราะห์ความปลอดภัยและความมั่นคงระบบธนาคารผ่านโทรศัพท์มือถือของธนาคารพาณิชย์ในประเทศไทยในส่วนของผู้ใช้งานทั่วไป 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 โดยเลือกจากธนาคารที่ก่อตั้งในประเทศไทยที่มีระยะเวลายาวนานที่มีคนนิยมใช้มากที่สุดในการวิเคราะห์และสำรวจ ได้ทำในช่วงวันที่ 1-31 ธันวาคม พ.ศ. 2558 โดยการแสดงผลการวิเคราะห์จะใช้ตัวอักษรภาษาอังกฤษ A - F แทนชื่อธนาคารที่เป็นกรณีศึกษา โดยไม่ได้เรียงจากอันดับที่ 1-6 เพื่อป้องกันการเปิดเผยจุดอ่อนของธนาคารที่เป็นกรณีศึกษาแบบเฉพาะเจาะจง อาจเป็นการชี้ช่องทางแก่มิจฉาชีพ

ซึ่งงานวิจัยนี้จะวิเคราะห์ระบบ m-banking ทั้งด้านความปลอดภัยและด้านความมั่นคง รวมทั้งสำรวจผู้ให้บริการเครือข่าย และวิเคราะห์พฤติกรรมของผู้ใช้สมาร์ทโฟนที่อาจเสี่ยงต่อปัญหามัลแวร์ โดยในการทดสอบของงานวิจัยนี้ ได้ใช้บัญชีธนาคาร ซิมการ์ด และอุปกรณ์สมาร์ทโฟนของทีมวิจัยในการทดลอง เพื่อไม่เป็นการกระทำผิดต่อกฎหมายต่อผู้อื่น โดยรายละเอียดต่างๆ แบ่งเป็นด้านดังนี้

**1) ด้านความปลอดภัยของระบบ m-banking**

มีประเด็นที่มาใช้ในการวิเคราะห์ดังต่อไปนี้ 1) การเปิดบัญชีธนาคาร 2) การสมัครใช้งานระบบ m-banking 3) การล็อกอินเข้าสู่ระบบ 4) การรีเซตข้อมูล 5) การเปลี่ยนเบอร์มือถือ 6) ลักษณะของ OTP 7) การเชื่อมต่ออินเทอร์เน็ต 8) มาตรการด้านความปลอดภัยอื่นๆ 9) การยกเลิกการใช้บริการระบบ m-banking 10) การปิดบัญชี

โดยจะนำประเด็นที่กำหนดไปใช้ในการสำรวจและวิเคราะห์ลักษณะการโจมตีแบบวิศวกรรมสังคม ที่คนร้ายมักใช้เป็นส่วนใหญ่จากคดีความที่เคยเกิดขึ้น เช่น การสร้างหลักฐานปลอมเพื่อขอเปิดบัญชีธนาคารที่มีชื่อเหมือนกันกับ

เหยื่อ แล้วทำการสวมรอยขโมยเงินในบัญชี เป็นต้น ดังนั้นงานวิจัยนี้จึงได้ทำการศึกษาและวิเคราะห์เกี่ยวกับคดีต่างๆ ที่เกิดขึ้นจริงในประเทศไทย แล้วทำการทดลองเปิดบัญชีและสังเกตการณ์สมัครใช้งานจริงเพื่อนำมาวิเคราะห์ในด้านความปลอดภัย

**2) ด้านความมั่นคงของระบบ m-banking**

ประเด็นที่นำมาวิเคราะห์ด้านความมั่นคงผู้วิจัยได้ศึกษามาจากภัยคุกคามระบบ m-banking ซึ่งมีหลากหลายเทคนิคในการโจมตี แต่ในงานวิจัยนี้จะเลือกเทคนิควิธีที่แฮกเกอร์นิยมใช้เจาะระบบมากที่สุด ในช่วง 3 - 4 ปีที่ผ่านมา โดยได้ทำการทดสอบมาตรการความมั่นคงของระบบ ด้วยโปรแกรมที่ใช้เพื่อวัตถุประสงค์ในการโจมตีแบบแทรกกลางการสื่อสาร ในการดักจับข้อมูล โดยจะทำการทดสอบการโจมตีบนแพลตฟอร์มของ iOS และแอนดรอยด์โดยเครื่องมือที่เกี่ยวข้องมีดังนี้

1) เครื่องผู้จู่โจม (Attacker) : Intel(R) Core(TM) i7-4702MQ CPU@2.20GHz

2) ซอฟต์แวร์ ที่ใช้ในการจู่โจมและดักจับข้อมูล
- Cain & Abel v4.9.56
- Kali Linux v1.1.0a
- Wireshark v1.12.4

**3) ด้านความปลอดภัยของผู้ให้บริการโมบายซิม**

จากข่าวคดีความ เรื่องการขอออกซิมโทรศัพท์มือถือใหม่ จนนำไปสู่การจู่โจมระบบธนาคาร ดังที่ได้กล่าวมาก่อนหน้านี้ งานวิจัยนี้จึงได้ทำการทดสอบ ผู้ให้บริการเครือข่ายโทรศัพท์มือถือ 3 ราย คือ TRUE, DTAC, AIS ในขั้นตอนการขอออกซิมใหม่ การขอเปลี่ยนซิม เพื่อหาจุดอ่อนและช่องโหว่ของเจ้าหน้าที่ ซึ่งทำให้มิจฉาชีพอาจแอบสวมรอย ดังที่เป็นข่าว[20] โดยทีมวิจัยได้ทดลองใช้เบอร์โทรศัพท์ของตนในการทดลอง เพื่อหลีกเลี่ยงการกระทำผิดกฎหมาย

**4) ด้านการวิเคราะห์พฤติกรรมผู้ใช้สมาร์ทโฟน**

มัลแวร์เป็นภัยคุกคามสำคัญสำหรับโมบายแอปพลิเคชัน และระบบ m-banking ดังที่ได้กล่าวไว้ในหลายงานวิจัยก่อนหน้านี้[16,17] ดังนั้นงานวิจัยนี้ จึงได้ออกแบบสอบถามเพื่อสำรวจพฤติกรรมของผู้ใช้งานสมาร์ทโฟน เพื่อศึกษาพฤติกรรมกับความเสี่ยงต่อภัยมัลแวร์ โดยประชากรคือ กลุ่มคนที่อาจเป็นลูกค้าของ ระบบ m-banking ซึ่งในงานวิจัยนี้นิยามไว้เป็นกลุ่มผู้ใช้งานแอปพลิเคชันบนโทรศัพท์มือถือ ซึ่งจะมีความสามารถในการใช้ระบบ m-banking ได้ต่อไป และมีอายุ 15 ปีขึ้นไป ซึ่งเป็นอายุที่สามารถสมัครเปิดบัญชีธนาคารได้ การสุ่มตัวอย่าง ใช้วิธีการสุ่มอย่างง่าย โดยการใช้แบบสอบถามที่กรอกผ่านระบบออนไลน์ โดยได้มีผู้ตอบแบบสอบถามและมีคุณสมบัติใช้ได้ ทั้งหมด 481 คน

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลเพื่อการวิจัยเชิงสำรวจครั้งนี้ เป็นการใช้แบบสอบถามปลายปิด ที่ผ่านการตรวจสอบความเที่ยงตรงของเนื้อหาและภาษาที่ใช้ Index of item Object Congruence (IOC) จากผู้เชี่ยวชาญด้านระบบเครือข่ายคอมพิวเตอร์ซึ่งมีทั้งหมด 3 ท่าน คือผู้อำนวยการฝ่ายเครือข่ายของธนาคารแห่งหนึ่ง พนักงานสอบสวนชำนาญการฝ่ายคดีเทคโนโลยีสารสนเทศและผู้เชี่ยวชาญ

## ผลการดำเนินงาน

**1) ผลด้านความปลอดภัยระบบ m-banking**

**Table 1** Documents for opening a bank account

| Criteria for Safety Analysis | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1. Opening bank account | | | | | | |
| 1.1 Citizen identity card | / | / | / | / | / | / |
| 1.2 Driving license & House record document | / | | | / | / | / |
| 1.3 Civil service ID & House record document | / | / | / | / | / | / |
| 1.4 Passport (in the case of foreigners) | / | / | / | / | / | / |

จาก (Table 1) พบว่าในการเปิดบัญชีทุกธนาคารจะต้องใช้บัตรประชาชนในการยืนยันตัวตน มี 2 ธนาคารที่ไม่อนุญาตให้ใช้ใบอนุญาตขับรถและทะเบียนบ้าน และทุกธนาคารจะอนุญาตให้ใช้บัตรข้าราชการแต่ต้องยื่นควบคู่กับสำเนาทะเบียนบ้าน จะเห็นได้ทุกธนาคารจะให้ความสำคัญ ในการตรวจสอบหลักฐานที่ใช้ในการสมัคร แต่การให้บริการของแต่ละธนาคารไม่เป็นรูปแบบเดียวกัน ขาดมาตรฐานในการตรวจสอบการให้บริการของเจ้าหน้าที่ เนื่องจากมีข่าวที่เกิดขึ้นดังที่กล่าวมาแล้ว[13] โดยมิจฉาชีพอาศัยช่องโหว่ในการตรวจสอบเอกสาร ของเจ้าหน้าที่เข้าสวมรอยเปิดบัญชีธนาคาร โดยการใช้หลักฐานปลอม ซึ่งมีงานวิจัยในต่างประเทศ[4] พบว่ามีวิธีการที่รัดกุมกว่า โดยพนักงานจะต้องผ่านการฝึกอบรมการตรวจเอกสารก่อน ดังนั้นธนาคารควรมีมาตรการที่เป็นแนวทางเดียวกัน และเพิ่มวิธีการยืนยันตัวตนที่เฉพาะเจาะจง เช่น การแสกนลายนิ้วมือ

**Table 2** How to apply for m-banking

| Criteria for Safety Analysis | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 2. Applying for mobile banking | | | | | | |
| 2.1 applying at a bank branch | / | / | / | / | / | / |
| 2.2 applying via a smartphone application | | | | / | | / |
| 2.3 applying via an ATM machine | / | / | / | / | / | |

จาก (Table 2) พบว่ามี 2 ธนาคารที่สามารถสมัครผ่านแอปพลิเคชันได้ และมี 5 ธนาคารที่จะต้องขอรหัสสมัครบริการจากตู้ ATM เพื่อใช้ยืนยันในการสมัครใช้งานผ่านแอปพลิเคชัน ซึ่งการสมัครใช้งานผ่านตู้ ATM จะเป็นมาตรการรักษาความปลอดภัยขั้นสูงของธนาคาร ที่ใช้ยืนยันตัวตนความเป็นเจ้าของบัญชี แต่ละธนาคารมีวิธีที่แตกต่างกัน พบว่า ธนาคาร A จะต้องขอรหัสยืนยันจากตู้ ATM ก่อนติดตั้งและมีการยืนยันตัวตนผ่าน VDO Call เพื่อป้องกันการสวมรอย ธนาคาร D กรอกข้อมูลบัตร ATM ก็สมัครได้ไม่มีการยืนยันจากตู้ ATM ธนาคาร E จะต้องขอรหัสยืนยันจากตู้ ATM ก่อนติดตั้ง ธนาคาร F กรอกข้อมูลบัตร ATM ก็สมัครได้ไม่มีการยืนยันจากตู้ ATM แต่จะใช้คู่กับเลขที่สมุดบัญชี จะเห็นได้ว่าธนาคาร A, D, E, F ไม่ได้ผูกติดกับเบอร์โทรศัพท์แต่หากสมัครด้วยตนเองจะต้องใช้คู่กับบัตร ATM และสมุดบัญชี ซึ่งมี 2 ธนาคารที่มีจุดเด่นต่างจากธนาคารอื่นที่ผูกติดกับเบอร์โทรศัพท์คือ ธนาคาร B จะกำหนดให้ใช้ 1 บัญชีสามารถใช้งานกับ 1 เบอร์โทรศัพท์เท่านั้น และธนาคาร C หากต้องการใช้งานในเครื่องอื่น หมายเลขอื่น จะต้องทำการอนุญาตขอเพิ่มอุปกรณ์ในการเข้าใช้งาน จะต้องขออนุญาตโดยใช้รหัส OTP จากเครื่องหลักเพื่อยืนยันการเพิ่มอุปกรณ์ ซึ่งข้อจำกัดที่เพิ่มมานี้ โดยการผูกระบบ m-banking ไว้ที่เครื่องโทรศัพท์มือถือจะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะการจะเข้าใช้งานต้องมีการยืนยันตัวตนด้วยการเป็นเจ้าของเบอร์โทรศัพท์มือถือนั้นจริง หรือถือครองโทรศัพท์ที่ติดตั้งระบบ m-banking เท่านั้น ดังนั้นแม้ว่า แฮกเกอร์จะทราบรหัส PIN หรือ รหัสผ่าน ก็ไม่สามารถเข้าใช้งานได้ จะต้องทำการขโมยโทรศัพท์มือถือหรือเบอร์โทรศัพท์ของลูกค้าด้วย จึงจะเข้าใช้งานได้ ดังนั้นในการสมัครใช้งานของระบบ m-banking จะเห็นได้ว่ามีความปลอดภัยมากกว่าระบบ i-banking เพราะมีการใช้อุปกรณ์สมาร์ทโฟนในการติดตั้ง พร้อมทั้งต้องยืนยันการสมัครผ่านระบบ OTP อีกด้วย

**Table 3** Login features

| Criteria for Safety Analysis | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 3. Login Features | | | | | | |
| 3.1 Access to the system by using a PIN lock | | / | / | | / | |
| 3.2 Limit login of the PIN Lock | | 3 | 3 | | 3 | |
| 3.3 Access to the system by using username & password | / | | | / | | / |
| 3.4 Limit login of the username & password | 3 | | | 3 | | 3 |

จาก (Table 3) มี 3 ธนาคารที่เข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่าน และมี 3 ธนาคารที่เข้าสู่ระบบด้วย PIN ซึ่งในการใส่รหัส PIN ก็เหมือนการใส่รหัสบัตร ATM ในการทำธุรกรรมทางการเงิน ซึ่งแตกต่างจากระบบ i-banking ที่ไม่สามารถเข้าสู่ระบบด้วย PIN ได้จะใช้เพียงชื่อผู้ใช้และรหัสผ่านเท่านั้น ดังนั้นจึงยากต่อการคาดเดาของมิจฉาชีพ นอกจากนั้นยังมีระบบที่จำกัดจำนวนครั้งในการล็อกอิน หากป้อนข้อมูลผิดเกินจำนวนครั้งที่กำหนด ชื่อผู้ใช้จะถูกล็อกทันที ซึ่งจะเห็นว่าการเข้าสู่ระบบด้วย PIN มีความปลอดภัยสูงกว่าเพราะถ้ามิจฉาชีพมีชื่อผู้ใช้และรหัสผ่าน ก็สามารถเข้าไปทำธุรกรรมผ่านระบบ i-banking ได้

**Table 4** Resetting Username/Password or PIN

| Criteria for Safety Analysis | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 4. Resetting Username/Password or PIN | | | | | | |
| Resetting username if forget | | | | | | |
| 4.1 Reset at a bank branch | / | | | / | | |
| 4.2 Reset via a call center | | | | / | | / |
| Resetting password if forget | | | | | | |
| 4.3 Reset at a bank branch | / | | | / | | |
| 4.4 Reset via a call center | | | | / | | |
| 4.5 Reset via a smartphone application | / | | | / | | / |
| 4.6 Reset at an ATM machine | / | | | | | |
| Resetting PIN if forget | | | | | | |
| 4.7 Reset via a call center | | | / | | / | |
| 4.8 Reset via a smartphone application | | | / | | / | |
| 4.9 Reset at an ATM machine | | / | / | | | |

จาก (Table 4) มี 3 ธนาคารที่รีเซตชื่อผู้ใช้และรหัสผ่าน คือ ธนาคาร A หากมีการลืมชื่อผู้ใช้และรหัสผ่าน จะไม่สามารถรีเซตผ่านคอลเซ็นเตอร์ได้ เพื่อป้องการแอบสวมรอย ธนาคาร D สามารถรีเซตผ่านคอลเซ็นเตอร์ได้ และคำถามที่ใช้ยืนยันเฉพาะเจาะจงตัวบุคคล มีการส่งข้อมูลทางอีเมล์ ซึ่งอาจถูกดักจับข้อมูลได้ ธนาคาร F สามารถรีเซตชื่อผู้ใช้ผ่านคอลเซ็นเตอร์ได้ แต่การรีเซตรหัสผ่าน จะต้องดำเนินการผ่านแอปพลิเคชัน จะเห็นได้ว่าจะมีการรีเซตที่แตกต่างกัน และมีการป้องกันการแอบสวมรอยจากบุคคลอื่น และเจ้าหน้าที่ และมี 3 ธนาคารที่รีเซตรหัส PIN ธนาคาร B รีเซตผ่านผ่านตู้ ATM เท่านั้น ธนาคาร C รีเซตผ่านคอลเซ็นเตอร์ แล้วส่งข้อมูลทาง SMS เพื่อทำการรีเซตผ่านแอปพลิเคชันด้วยตนเอง และรีเซตผ่านตู้ ATM ส่งข้อมูลการรีเซตผ่านทาง SMS ธนาคาร E รีเซตผ่านคอลเซ็นเตอร์และผ่านแอปพลิเคชัน จะเห็นได้ว่าแต่ละธนาคารมีวิธีการป้องกันความปลอดภัยที่แตกต่างกัน และในการรีเซตข้อมูลจะต้องใช้ควบคู่กับบัตร ATM และเบอร์โทรศัพท์ ในการรีเซต

ซึ่งในการรีเซตผ่านสาขาเจ้าหน้าจะให้นำสมุดบัญชีและบัตรประชาชนยืนยันตัวตนก่อนทำรายการ แต่ต้องระวังการแอบอ้างสวมรอยโดยใช้เอกสารปลอม และมีช่องโหว่ระหว่างการส่งข้อมูล ซึ่งธนาคาร B จะส่งข้อมูลมาให้ลูกค้าทางอีเมล์ซึ่งทำให้ถูกดักจับข้อมูลได้ และการรีเซตผ่านคอลเซ็นเตอร์อาจเป็นช่องโหว่ให้มิจฉาชีพแอบสวมรอย โดยใช้การโจมตีแบบวิศวกรรมทางสังคมได้ เจ้าหน้าที่ธนาคารควรตรวจสอบข้อมูลและใช้คำถามที่เฉพาะเจาะจงตัวบุคคล เพราะการแจ้งผ่านคอลเซ็นเตอร์ ไม่สามารถตรวจสอบได้ว่าเป็นตัวจริง ดังนั้นวิธีนี้ จึงอาจเป็นจุดอ่อนได้ ดังนั้นการรีเซตข้อมูลผ่านตู้ ATM เป็นวิธีการที่ปลอดภัยที่สุด เพราะต้องใช้บัตรและรหัส ATM เป็นการยืนยันตัวสองชั้น โดยการถือครองบัตร และทราบรหัสของบัตร ซึ่งระบบ m- banking จะมีความปลอดภัยสูงกว่าเพราะสามารถรีเซตรหัสได้เองผ่านแอปพลิเคชันพร้อมยืนยันด้วยรหัสบัตร ATM และใช้อุปกรณ์สมาร์ทโฟนด้วย ดังนั้นจึงมีความปลอดภัยสูงกว่าระบบ i-banking

ลักษณะการเปลี่ยนเบอร์โทรศัพท์พบว่าธนาคาร A จะสามารถเปลี่ยนผ่านแอปพลิเคชันเท่านั้น จะต้องยืนยันตัวตนอีกชั้นผ่าน SMS OTP ธนาคาร B จะสามารถเปลี่ยนผ่านคอลเซ็นเตอร์ แอปพลิเคชันและตู้ ATM แต่จะเป็นลักษณะการยกเลิกเบอร์เดิมและสมัครใหม่ เพราะ 1 แอปพลิเคชันจะสามารถใช้ได้เพียง 1 เบอร์เท่านั้น ทุกช่องทางจะต้องยืนยันตัวตนอีกชั้นผ่านตู้ ATM เพื่อรับ SMS OTP ยืนยันการสมัคร ธนาคาร C จะสามารถเปลี่ยนผ่านสาขา แอปพลิเคชันและตู้ ATM ทุกช่องทางจะต้องมีการยืนยันตัวตนอีกชั้นผ่าน SMS OTP ธนาคาร D, E จะสามารถเปลี่ยนผ่านสาขาเท่านั้น ธนาคาร F จะสามารถเปลี่ยนผ่านแอปพลิเคชันเท่านั้น มีการยืนยันตัวตนอีกชั้นผ่าน SMS OTP พบว่าการเปลี่ยนเบอร์โทรศัพท์ผ่านคอลเซ็นเตอร์ แอปพลิเคชัน และตู้ ATM จะต้องยืนยันตัวตนผ่าน SMS OTP อีกครั้งในการยืนยันตัวตน เพื่อความปลอดภัยจากการสวมรอยของมิจฉาชีพ และในการเปลี่ยนที่สาขาธนาคารจะต้องให้ความสำคัญเกี่ยวกับการตรวจสอบหลักฐานต่าง ๆ และการสอบถามข้อมูลที่สามารถยืนยันตัวบุคคลที่แท้จริง เพื่อความถูกต้อง เนื่องจากมีข่าวที่เกิดขึ้น[13] ดังที่กล่าวมาข้างต้น เกี่ยวกับการปลอมแปลงเอกสารเพื่อออกซิมใหม่ แล้วทำการขอแจ้งเปลี่ยนเบอร์มือถือในระบบ m-banking ซึ่งเป็นวิธีการที่มิจฉาชีพใช้ในการสวมรอยทำธุรกรรมทางการเงิน จากการวิเคราะห์ความผิดพลาดเกิดจากผู้ให้บริการเครือข่ายที่ไม่มีมาตรการตรวจสอบข้อมูล ดังนั้นควรมีมาตรการที่เป็นแนวทางเดียวกันและเพิ่มวิธีการยืนยันตัวตน นอกจากจะตรวจสอบเอกสารแล้วควรมีการยืนยันตัวตนที่เฉพาะเจาะจง เช่น การแสกนลายนิ้วมือ

**Table 5** OTP features

| Criteria for Safety Analysis | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 5. OTP features | | | | | | |
| OTP life time (in minute) | 15 | | 3 | 15 | 15 | 12 |
| 5.1 using OTP when transferring money | / | | | / | | / |
| 5.2 using OTP when adding a receiver bank account | / | | | / | | / |
| 5.3 using OTP when changing the mobile phone number | / | | | / | | / |
| 5.4 using OTP when paying money for any services | / | | | / | | / |
| 5.5 The maximum number of passing wrong OTPs | 3 | | 3 | 3 | 3 | 3 |

จาก Table 5 พบว่าบางธนาคารเปิดให้มีระยะเวลาการกรอกรหัส OTP ที่นานต่างกันไป จากการทดสอบพบว่าระบบ OTP ในประเทศไทยมีการส่งล่าช้าน้อยมาก ดังนั้นระยะเวลาไม่เกิน 3 นาที ที่ธนาคาร C ใช้อยู่ น่าจะเหมาะสมกว่า เนื่องจากระยะเวลาที่นานเกินไป อาจเป็นช่องโหว่ให้มิจฉาชีพดักขโมยข้อมูล หากโทรศัพท์ที่ใช้รับ SMS OTP ติดมัลแวร์ ทำให้ SMS OTP ส่งไปยังเครื่องของมิจฉาชีพและทำให้มิจฉาชีพมีเวลาไปทำธุรกรรมก่อนเจ้าของบัญชี ดังนั้นเครื่องที่ใช้รับ SMS OTP จะต้องมีความปลอดภัย มีการแสกนไวรัสและตรวจสอบความปลอดภัยเสมอ

ลักษณะการเชื่อมต่ออินเทอร์เน็ตพบว่าธนาคาร B ไม่อนุญาตให้เชื่อมต่อผ่าน Wi-Fi เพราะมีโอกาสถูกดักจับข้อมูล และแทรกกลางการสื่อสารได้ง่ายกว่า โดยอนุญาตให้เชื่อมต่อผ่าน 3G/4G เท่านั้น เนื่องจากเทคโนโลยี 3G[21] มีการเข้ารหัสข้อมูลที่ส่งผ่าน ด้วยอัลกอริธึม UEA1/UIA1 Kasumi Block Cipher ส่วนเทคโนโลยี 4G[22] จะมีมาตรฐานความปลอดภัยที่สูงไปอีก โดยการเข้ารหัสด้วยอัลกอริธึม UEA2/UIA2 Snow 3G Stream Cipher ดังนั้นจึงมีความปลอดภัยสูงจากการดักจับข้อมูลของแฮกเกอร์ เมื่อเทียบกับการเชื่อมต่อผ่าน 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

**Table 6** Other safety issues

| Criteria for Safety Analysis | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 6. Other Safety issues | | | | | | |
| 6.1 Login notification | / | | / | / | / | / |
| 6.2 Safety setting | / | / | / | / | / | / |
| 6.3 Auto Log Off | 5 | 3 | 5 | 1 | 1 | 15 |
| 6.4 Transaction secret code | | | / | | | |
| 6.5 Activity notification | | | | | | |
| - E-mail notification | / | / | / | / | / | / |
| - SMS notification | / | | | | | |

จาก (Table 6) พบว่าธนาคาร F มีระยะเวลาการล็อกระบบอัตโนมัตินานเกินไป เมื่อเทียบกับธนาคารอื่นๆ ซึ่งระยะเวลาที่นานเกินไปนี้ อาจทำให้มิจฉาชีพแอบสวมรอยการทำธุรกรรมได้

**Table 7** Cancelling m-banking

| Criteria for Safety Analysis | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 7. Cancelling m-banking | | | | | | |
| 7.1 cancel at a bank branch | / | | | / | / | / |
| 7.2 cancel via a call center | | / | / | / | | |
| 7.3 cancel via a smartphone application | / | / | / | | | / |
| 7.4 cancel at an ATM machine cancel at a bank branch | | / | | | | |

จาก (Table 7) ขั้นตอนการเลิกใช้บริการระบบ m-banking โดยทั่วไปยังไม่มีช่องโหว่หรือเกิดกรณีการจู่โจมที่เกิดขึ้นในเรื่องนี้โดยตรง เพื่อความปลอดภัย ธนาคารควรตระหนักถึงการตรวจสอบการยืนยันตัว หากมีการยกเลิกการใช้งานเพราะอาจจะมีการกลั่นแกล้งเพื่อต้องการทำให้บัญชีมีปัญหาหรือมิจฉาชีพอาจทำการยกเลิกการใช้งานแล้วขอเปิดใหม่เพื่อทำการสวมรอย ซึ่งทางธนาคารควรเข้มงวดในการตรวจสอบความถูกต้อง ในการขอเลิกใช้บริการ โดยเฉพาะอย่างยิ่งธนาคาร B, C และ D อนุญาตให้มีการยกเลิกผ่านคอลเซ็นเตอร์ ซึ่งอาจมีโอกาสถูกโจมตีแบบวิศวกรรมสังคม โดยมิจฉาชีพได้ง่ายที่สุด หากคำถามที่ใช้ตรวจสอบยืนยันตัวตนไม่ดีพอ

**Table 8** Closing bank account

| Criteria for Safety Analysis | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 8. Closing the bank account | | | | | | |
| 8.1 closing at an account-opening bank branch | / | / | / | / | / | / |
| 8.2 closing at any other bank branchs | | / | / | / | | |
| 8.3 closing by using the citizen ID & the bank book | / | / | / | / | / | / |
| 8.4 closing by using the citizen ID & police document (if the book bank was lost) | / | | | | / | / |

จาก (Table 8) พบว่าการขอปิดบัญชีได้ที่ธนาคารต่างสาขา และทุกธนาคารให้ทำที่ธนาคารเท่านั้น ซึ่งถือว่ามีความปลอดภัย แต่ขึ้นอยู่กับขบวนการตรวจเอกสารหลักฐานในการยืนยันตัวตนที่แท้จริง ซึ่งพบว่าขั้นตอนนี้โดยทั่วไปมีความปลอดภัย เพราะลูกค้าจะต้องนำบัตรประชาชนและสมุดบัญชีมาใช้ควบคู่ในการปิดบัญชี และมี 3 ธนาคาร ซึ่งจะต้องนำใบแจ้งความมาประกอบด้วยเมื่อทำสมุดบัญชีเงินฝากหาย จากการวิเคราะห์กรณีคดีความที่เกิดขึ้นยังไม่มีประเด็นด้านการโจมตีแบบวิศวกรรมสังคม ที่เกี่ยวกับเรื่องนี้โดยตรง แต่ธนาคารควรตระหนักถึงการตรวจสอบการยืนยันตัวหากมีการมาปิดบัญชีเพราะอาจจะมีการกลั่นแกล้งหรือทำการยกเลิกการใช้งานแล้วขอเปิดใหม่ เพื่อทำการสวมรอย

**2) ผลด้านความมั่นคงของระบบ m-banking**

การวิเคราะห์ประเด็นด้านความมั่นคงจะเป็นเรื่องของเทคนิค โดยจะทำการทดสอบ ใน 2 วิธีคือ SSL Sniff และ SSL Strip ในขณะที่กำลังเข้าใช้งานระบบธนาคารผ่านโทรศัพท์มือถือ ซึ่งจะทำการดักจับข้อมูลผ่านการเชื่อมต่อ

อินเทอร์เน็ตทั้ง 6 ธนาคารเพื่อทดสอบและได้ผลการสำรวจสรุปผลดังนี้

2.1) ผลการโจมตีแบบ SSL Sniff

ผลการทดสอบการโจมตีด้วยวิธีการ SSL Sniff ต่อระบบ m-banking พบว่าไม่สามารถดักจับข้อมูลได้ เนื่องจากโปรแกรมของระบบ m-banking แอปพลิเคชัน จะไม่ยอมรับ หากมีการส่งใบรับรอง (Certificate) ปลอม ระบบถูกออกแบบให้ไม่ทำงาน ซึ่งการเขียนโปรแกรมระดับชั้นแอปพลิเคชันจะกำหนดใบรับรองที่แท้จริง จากธนาคารผู้พัฒนาตั้งแต่ขั้นพัฒนาการใช้งาน จึงมีความปลอดภัยมั่นคงสูง ไม่เหมือนในระบบ i-banking ที่รายงานไว้ในงานวิจัยอื่นๆ ก่อนหน้านี้ จะให้ผู้ใช้เป็นคนตรวจสอบว่า ใบรับรองนั้นถูกต้องหรือไม่ ซึ่งมีโอกาสถูกจู่โจมได้ หากผู้ใช้งานระบบ i-banking ไม่สังเกต โดยจากการทดลองของงานวิจัยนี้ต่อจากระบบ i-banking ซึ่งพบว่ามี 1 ธนาคารที่ไม่สามารถดักจับข้อมูลได้เนื่องจากข้อมูลมีการเข้ารหัสไว้ และมี 5 ธนาคารพบว่าสามารถจะจู่โจมด้วย SSL Sniffing และดักจับข้อมูลในระบบ i-banking ได้ ดังแสดงใน (Figure 3) เนื่องจากเว็บเบราว์เซอร์ไม่สามารถตรวจสอบได้ว่ามีการดักจับข้อมูลจากแฮกเกอร์ หากผู้ใช้รู้เท่าไม่ถึงการณ์กดยอมรับใบรับรองปลอมหรือเข้าไปในเว็บปลอมที่แฮกเกอร์ใช้ดักจับข้อมูลก็จะถูกขโมยข้อมูลที่สำคัญไปได้โดยง่าย ดังนั้นจากการทดลองนี้จะเห็นได้ชัดเจนว่า ระบบ m-banking โดยทั่วไปมีความมั่นคงต่อการจู่โจมด้วย SSL Sniffing มากกว่าระบบ i-banking

| | | | |
|---|---|---|---|
| 119.46.87.14 | 192.168.100.25 | banktestA | forie |
| 115.31.152.155 | 192.168.100.25 | banktestA | forchome |
| 119.46.87.14 | 192.168.100.25 | banktestA | forfirefox |
| 202.12.117.134 | 192.168.100.25 | banktestB | forie |
| 202.12.117.134 | 192.168.100.25 | banktestB | forchome |
| 202.12.117.134 | 192.168.100.25 | banktestB | forfirefox |
| 203.146.18.171 | 192.168.100.25 | banktestC | forie |
| 203.146.18.171 | 192.168.100.25 | banktestC | forchome |
| 203.146.18.171 | 192.168.100.25 | banktestC | forfirefox |

**Figure 3** SSL Sniffing i-banking can eavesdrop user-names & passwords

2.2) ผลการโจมตีแบบ SSL Strip

SSL Strip เป็นเทคนิควิธีที่ใช้ในการโจมตีระบบธนาคารออนไลน์ที่เป็นที่นิยมอยู่ทั่วโลก จากสถิติตั้งแต่ปี ค.ศ. 2008 จากคดีความด้านนี้ที่เกิดขึ้นในประเทศไทย พบว่าเป็นเทคนิคที่ถูกนำมาใช้มากที่สุด จากการทดลองดักจับข้อมูลด้วยเทคนิค SSL Strip ดังแสดงใน (Figure 4) ด้วยโปรแกรม Wireshark ซึ่งทำการดักจับแพ็กเก็ตที่ไคลเอนต์ ในขณะที่ใช้งานระบบธนาคารบนโทรศัพท์มือถือผ่านแอปพลิเคชัน พบว่าขั้นตอนการร้องขอมีการเรียกใช้โพรโทคอล HTTPS ทำให้ไม่สามารถโจมตีแบบ SSL Strip ได้ เพราะเริ่มต้นเป็น HTTPS อัตโนมัติ ไม่เหมือนกับระบบ i-banking ที่ให้ผู้ใช้เป็นผู้เริ่มการสื่อสาร ซึ่งอาจเป็น HTTP แล้วเว็บเซิร์ฟเวอร์ค่อยทำการ Redirect ไปเป็น HTTPS ที่อาจโดน SSL Strip ได้

```
199 Application Data
199 Application Data
 66 34165 > https [ACK] Seq=1349 Ack=267 Win=42 Len=0 TSval=1
 66 34160 > https [ACK] Seq=2031 Ack=400 Win=42 Len=0 TSval=1
 66 54949 > http [ACK] Seq=1 Ack=1 Win=29 Len=0 TSval=158848
 66 34154 > https [ACK] Seq=1 Ack=1 Win=42 Len=0 TSval=158848
 66 [TCP ACKed unseen segment] http > 54949 [ACK] Seq=1 Ack=2
 66 [TCP ACKed unseen segment] https > 34154 [ACK] Seq=1 Ack=
```

**Figure 4** SSL Stripping on m-banking failure due to https initialization

```
 66 56806 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS
 66 [TCP Out-Of-Order] 56806 > http [SYN] Seq=0 Win=819
 62 http > 56806 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0
 62 [TCP Out-Of-Order] http > 56806 [SYN, ACK] Seq=0 Ac
 60 56806 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
 54 [TCP Dup ACK 64#1] 56806 > http [ACK] Seq=1 Ack=1 W
354 GET /1st_pg.html HTTP/1.1
354 [TCP Retransmission] GET /1st_pg.html HTTP/1.1
178 HTTP/1.0 301 Moved Permanently
```

**Figure 5** The success of SSL Stripping on i-banking

จากผลการทดสอบการดักจับข้อมูลด้วยเทคนิค SSL Strip ต่อระบบ i-banking ที่ทำงานผ่านเบราว์เซอร์ดังแสดงใน (Figure 5) พบว่าในการต่อต้านการจู่โจมด้วยวิธีนี้ระบบ i-banking มีความมั่นคงน้อยกว่าระบบ m-banking เพราะมีโอกาสถูกโจมตีได้ หากผู้ใช้ไม่พิมพ์ HTTPS แต่การร้องขอระบบธนาคารโดยใช้โพรโทคอล HTTP ดังนั้นจะเห็นได้ว่า การใช้งานผ่านระบบ m-banking จะมีความมั่นคงสูงกว่าการใช้งานผ่านระบบ i-banking

จากผลการทดสอบการโจมตีด้วยวิธีแทรกกลางการสื่อสารทั้ง 2 วิธี คือ การโจมตีแบบ SSL Sniff และการโจมตีแบบ SSL Strip พบว่าไม่สามารถดักจับข้อมูลได้ เนื่องจากการทำงานบนแอปพลิเคชันจะใช้รูปแบบการสื่อสารกับเซิร์ฟเวอร์บนโพรโทคอล HTTPS ที่มีการเข้ารหัสด้วยโพรโทคอล SSL ซึ่งจะใช้ในการตรวจสอบอัลกอริธึมในการเข้ารหัส การแลกเปลี่ยน Public Key และ Session Key ก่อนทำการสื่อสารแลกเปลี่ยนข้อมูล และทำการเข้ารหัสข้อมูลด้วย Secret Key ระหว่าง ไคลเอนต์และเซิร์ฟเวอร์ซึ่งเรียกขบวนการนี้ว่า SSL Handshake ซึ่งข้อมูลที่ถูกส่งจะถูกเข้ารหัสด้วย SSL/

TLS อัตโนมัติ ทำให้ข้อมูลมีความถูกต้องและเป็นความลับ เพื่อป้องกันการโจมตีด้วยวิธีแทรกกลางการสื่อสาร จะเห็นได้ว่าการสื่อสารบนโพรโทคอล HTTPS จะมีความมั่นคงสูง สามารถป้องกันการดักจับข้อมูลที่สำคัญ โดยขบวนการทั้งหมดสามารถสั่งงานผ่านโมบายแอปพลิเคชัน ที่สร้างเป็นระบบ m-banking ได้เลย โดยไม่ต้องพึ่งพาผู้ใช้งานให้สังเกต HTTPS ซึ่งต่างไปจากระบบ i-banking ที่ยังต้องอาศัยการสังเกตของผู้ใช้งานเป็นขั้นตอนสุดท้าย ในการป้องกันความมั่นคง ซึ่งผลการทดลองในส่วนการโจมตีระบบ i-banking นั้น สอดคล้องกับงานวิจัยก่อนหน้านี้ ที่แสดงความสำเร็จของการโจมตีระบบ i-banking ด้วยวิธี SSL Strip และ SSL Sniff เมื่อผู้ใช้ส่วนใหญ่ไม่สังเกตดีพอ

2.3) รูปแบบการโจมตีด้วยวิธีแทรกกลางการสื่อสาร

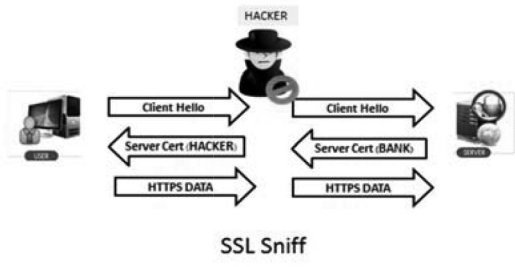


**Figure 6** SSL Sniff

จาก (Figure 6) จะเห็นได้ว่าไคลเอนต์จะใช้ ใบรับรองของแฮกเกอร์เข้ารหัสข้อมูล ซึ่งจะทำให้แฮกเกอร์สามารถถอดรหัสข้อมูลของไคลเอนต์ได้ และเมื่อแฮกเกอร์ถอดรหัสข้อมูลของไคลเอนต์ได้แล้ว ก็จะสามารถใช้ใบรับรองของเซิร์ฟเวอร์เข้ารหัสข้อมูลจึงทำให้เซิร์ฟเวอร์ตรวจสอบไม่ได้ว่าไคลเอนต์ถูกโจมตี ถ้าเป็นการใช้งานผ่านแอปพลิเคชันระบบจะ Error หากพบว่ามีการใช้ใบรับรองปลอม

จาก (Figure 7) ไคลเอนต์กับแฮกเกอร์จะสื่อสารบนโพรโทคอล HTTP ทำให้ข้อมูลของไคลเอนต์ไม่ถูกเข้ารหัส ดังนั้นแฮกเกอร์สามารถดักจับข้อมูลของไคลเอนต์ได้ และแฮกเกอร์กับเซิร์ฟเวอร์สื่อสารบน HTTPS ปกติทำให้เซิร์ฟเวอร์ตรวจสอบไม่ได้ว่าไคลเอนต์ถูกโจมตี จากหลักการทำงานของ HTTPS ที่มีการกำหนดให้ระบบเว็บไซต์ทำงานบนโพรโทคอล HTTPS ที่ตำแหน่งเว็บเซิร์ฟเวอร์เท่านั้น ด้วยเหตุนี้ SSL Strip จึงอาศัยจุดอ่อนที่เว็บเบราว์เซอร์ไม่สามารถตรวจสอบและกำหนดรูปแบบการสื่อสารบนโพรโทคอล HTTPS กับเว็บเซิร์ฟเวอร์ โดยหลักการโจมตีด้วยวิธี SSL Strip เพื่อดักจับข้อมูลสำคัญของเหยื่อที่ใช้ในการสื่อสารกับเว็บเซิร์ฟเวอร์ ถ้าใช้งานผ่านแอปพลิเคชันจะบังคับเข้ารหัสด้วยโพรโทคอล SSL ซึ่งเป็นโพรโทคอลพื้นฐานในการสร้าง HTTPS ดังนั้นจึงทำให้ลดปัญหาการโจมตีด้วยวิธีแทรกกลางการสื่อสาร

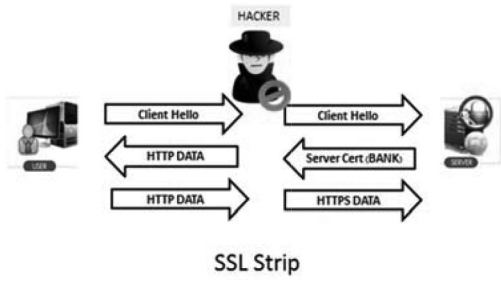


**Figure 7** SSL Strip

**3) ผลการสำรวจผู้ให้บริการโทรศัพท์มือถือ**

พบว่าผู้ให้บริการทั้ง 3 ค่ายมีการให้บริการที่แตกต่างกัน ในการออกซิมใหม่ที่ไม่เป็นมาตรฐานเดียวกัน เจ้าหน้าที่ควรตรวจสอบหลักฐานและสอบถามประวัติการใช้งานของลูกค้า เพื่อป้องกันบุคคลแอบอ้างสวมรอย แต่ในการขอออกซิมใหม่ก็ยังพบว่ามีช่องโหว่ จากงานวิจัยก่อนหน้าของ Rachana[4] ได้พบจุดบกพร่องของเจ้าหน้าที่ DTAC เนื่องจากใช้ซิมปลอมเปลี่ยนเป็นซิมนาโนซึ่งเป็นอีกเบอร์ โดยเจ้าหน้าที่ไม่ได้ขอตรวจสอบเอกสาร จึงทำให้ได้ซิมใหม่เบอร์ใหม่ และการศึกษาครั้งนี้ได้ค้นพบจุดอ่อนของเจ้าหน้าที่เครือข่าย TRUE ในการขอออกซิมใหม่กรณีซิมหายโดยเจ้าหน้าที่ไม่ได้ขอตรวจสอบหลักฐานเพียงระบุเบอร์ที่หายก็สามารถออกซิมใหม่ได้ ซึ่งข้อบกพร่องเกิดจากเจ้าหน้าที่ ที่ไม่มีมาตรฐานเดียวกันจึงทำให้เป็นช่องโหว่เกิดขึ้น ซึ่งมีข่าวที่เกิดขึ้นจริงกรณีปลอมเอกสารเพื่อทำการสวมรอยขอออกซิมใหม่ โดยส่วนใหญ่มิจฉาชีพจะใช้การโจมตีแบบวิศวกรรมสังคม ซึ่งเป็นวิธีการที่ง่ายและทำได้จริง กรณีที่เกิดขึ้นเกิดจากเจ้าหน้าที่ ไม่รอบคอบในการตรวจสอบเอกสารและผู้ให้บริการเครือข่ายไม่มีมาตรการที่เป็นรูปแบบเดียวกัน ทำให้มิจฉาชีพอาศัยช่องโหว่ดังกล่าวในการสวมรอย ซึ่งหากคนร้ายได้เบอร์โทรศัพท์ของเหยื่อไป ก็สามารถรับ SMS OTP ในการทำธุรกรรมทางการเงินได้อย่างง่ายดาย ดังนั้นเจ้าหน้าที่จะต้องรัดกุมในการออกซิมใหม่และผู้ใช้บริการควรตรวจสอบซิมการ์ดและโทรศัพท์มือถือเพื่อป้องกันมัลแวร์ ถ้าซิมการ์ดไม่มีสัญญาณควรรีบแจ้งเจ้าหน้าที่ให้ตรวจสอบให้ทันที

**4) ผลการวิเคราะห์พฤติกรรมผู้ใช้สมาร์ทโฟนที่ส่งผลต่อมัลแวร์**

งานวิจัยนี้ ได้ทำการสำรวจด้วยวิธีการแจกแบบสอบถาม และใช้แบบสอบถามออนไลน์ เพื่อสำรวจพฤติกรรมของกลุ่มผู้ใช้งานแอปพลิเคชันบนสมาร์ทโฟนที่มีอายุ 15 ปีขึ้นไป ซึ่งคาดว่ากลุ่มนี้มีโอกาสที่จะเป็นกลุ่มลูกค้าของระบบธนาคารผ่านโทรศัพท์มือถือ ใช้วิธีการสุ่มอย่างง่าย

โดยใช้แบบสอบถาม มีผู้กรอกแบบสอบถาม 481 คน ผลสรุปได้ดังนี้

1. ผู้ใช้งานสมาร์ทโฟนหรือผู้ที่ใช้แท็ปเล็ต
   - ใช้ ร้อยละ 98.5
   - ไม่ใช้ ร้อยละ 1.5

โดยมีผู้ใช้สมาร์ทโฟนหรือผู้ที่ใช้แท็ปเล็ตจำนวน 474 คน จากร้อยละ 98.5 ซึ่งสามารถตอบคำถามในข้อ 11 - 2

2. ผู้ใช้งานแอปพลิเคชันบนสมาร์ทโฟนจาก 474 คนคิดเป็นร้อยละ
   - ใช้ ร้อยละ 97.9
   - ไม่ใช้ ร้อยละ 2.1

โดยมีผู้ที่ไม่ใช้แอปพลิเคชันแต่มีความรู้ด้านแอปพลิเคชันจึงได้ทำแบบสอบถามตามหัวข้อต่อไปนี้

3. อายุ
   - อายุ 21-15 ปี ร้อยละ 29.3
   - อายุ 60-22 ปี ร้อยละ 70.5
   - อายุ 60 ปีขึ้นไป ร้อยละ 0.2

โดยอายุ 15 ปีขึ้นไปสามารถสมัครเปิดบัญชีธนาคารได้

4. อาชีพ
   - นักเรียน/นิสิต/นักศึกษา ร้อยละ 43.1
   - พนักงานบริษัทเอกชน ร้อยละ 12.1
   - พนักงานของรัฐ/พนักงานรัฐวิสาหกิจ ร้อยละ 33.8
   - ธุรกิจส่วนตัว/อาชีพอิสระ ร้อยละ 8.5
   - อื่นๆ ร้อยละ 2.5

5. รู้จักมัลแวร์หรือไม่
   - รู้จักมัลแวร์ ร้อยละ 68.7
   - ไม่รู้จักมัลแวร์ ร้อยละ 31.3

6. การติดตั้งแอปพลิเคชันที่อาจได้มาฟรีจากไฟล์.apk หรือจากเว็บไซต์บนอินเทอร์เน็ต นอกจาก App Store หรือ Play Store
   - เคยติดตั้ง ร้อยละ 15.3
   - ไม่เคยติดตั้ง ร้อยละ 84.7

7. การสังเกตการณ์ขอสิทธิ์เข้าถึงอุปกรณ์สมาร์ทโฟน ก่อนติดตั้งแอปพลิเคชัน
   - สังเกตทุกครั้ง ร้อยละ 52.9
   - ไม่สังเกต ร้อยละ 16.2
   - สังเกตเป็นบางครั้ง ร้อยละ 30.9

8. การสังเกตชื่อผู้พัฒนาแอปพลิเคชัน
   - สังเกต ร้อยละ 79.9
   - ไม่สังเกต ร้อยละ 20.1

9. รู้จักการรูทหรือเจลเบรคอุปกรณ์สมาร์ทโฟน
   - รู้จัก ร้อยละ 46.4
   - ไม่รู้จัก ร้อยละ 53.6

10. ทำการดัดแปลงอุปกรณ์
    - ดัดแปลงอุปกรณ์ ร้อยละ 14.6
    - ไม่ได้ดัดแปลงอุปกรณ์ ร้อยละ 85.4

11. การสำรวจการอนุญาตให้ติดตั้งแอปพลิเคชันจากภายนอก
    - ไม่อนุญาต ร้อยละ 87.8
    - อนุญาต ร้อยละ 12.2

โดยมีบางคนซึ่งอนุญาตให้ติดตั้งแอปพลิเคชันจากแหล่งภายนอกและหลังจากติดตั้งเรียบร้อยก็ปิดไม่อนุญาต

จากผลการสำรวจจะเห็นว่า มีส่วนน้อยที่อาจเป็นสุ่มเสี่ยงต่อปัญหามัลแวร์คือกลุ่มที่มีการดัดแปลงอุปกรณ์สมาร์ทโฟนและติดตั้งแอปพลิเคชันที่อาจได้มาฟรีจากไฟล์ .apk หรือไฟล์ที่มาจากเว็บไซต์บนอินเทอร์เน็ต และคนกลุ่มที่ใช้โมบายแอปพลิเคชันนี้ ส่วนใหญ่สังเกตการณ์การขอสิทธิ์เข้าถึงอุปกรณ์ก่อนติดตั้งแอปพลิเคชัน สังเกตชื่อผู้พัฒนาแอปพลิเคชัน และไม่อนุญาตให้ติดตั้งแอปพลิเคชันจากภายนอก จะเห็นได้ว่าการติดตั้งแอปพลิเคชันผู้ใช้งานจะเป็นผู้กำหนดความปลอดภัยและความเป็นส่วนตัว ซึ่งบางครั้งไม่ได้อ่านข้อตกลงหรือสังเกตการขอสิทธิ์ต่างๆ ทำให้ควบคุมได้ยาก จึงทำให้มีความเสี่ยงต่อการโจมตีของมัลแวร์ ซึ่งทักษะพื้นฐานของกลุ่มตัวอย่างนั้นซึ่งน่าจะสามารถใช้งานระบบ m-banking ได้ปลอดภัยจากปัญหามัลแวร์

## วิจารณ์และสรุปผล

งานวิจัยนี้ได้ทำการวิเคราะห์ธนาคารพาณิชย์ในประเทศไทยอยู่ 2 ประเด็น ซึ่งสามารถสรุปในแต่ละด้านได้ดังนี้ (1) ด้านมาตรการป้องกันความปลอดภัย พบว่ายังมีช่องโหว่ที่ทำให้มิจฉาชีพเข้ามาโจรกรรมข้อมูลได้ ส่วนใหญ่จะเป็นช่องโหว่ในเรื่องของการสวมรอยเป็นเจ้าของบัญชี ซึ่งทางธนาคารต้องทบทวนวิธีการในการตรวจเอกสารยืนยันตัวตน และพบปัญหาการปลอมแปลงเอกสารในการออกซิมใหม่ หรือขอเปลี่ยนซิมใหม่ ซึ่งทำให้ได้ SMS OTP ของระบบ e-banking ทั้ง i-banking และ m-banking ซึ่งก่อให้เกิดปัญหาอื่นๆ ตามมาได้มากมาย ทั้งนี้จุดอ่อนที่พบนี้จะแก้ไขได้ ต้องให้ทางผู้ให้บริการโทรศัพท์มือถือกำหนดข้อปฏิบัติให้กับทุกสาขาของตนเองให้มีขบวนการตรวจเอกสารในการยืนยันตัวตนให้รัดกุมยิ่งขึ้น เมื่อขอออกซิมการ์ดใหม่ หรือขอเปลี่ยนซิมการ์ดและเป็นข้อสังเกตสำหรับผู้ใช้งานระบบ e-banking ว่าหากโทรศัพท์มือถือของตนเกิดไม่มีสัญญาณและเป็นเบอร์โทรศัพท์ที่ผูกระบบ SMS OTP ของระบบ m-banking หรือระบบ i-banking ไว้ต้องอย่านิ่งนอนใจ ให้เร่งติดต่อศูนย์เพื่อตรวจสอบโดยไวที่สุด เพราะเป็นไปได้ว่าอาจถูกโจรกรรม SMS

OTP ดังที่งานวิจัยนี้ได้ทดสอบและเป็นคดี (2) ด้านความมั่นคงของระบบ พบว่าในการทดสอบการโจมตีแทรกกลางการสื่อสาร ธนาคารไม่สามารถดักจับข้อมูลได้ พบว่าระบบ m-banking มีความมั่นคงกว่าระบบ i-banking มาก นอกจากนี้ ในส่วนของพฤติกรรมผู้ใช้ ต่อปัญหามัลแวร์พบว่าปัญหาจะเกิดจากผู้ใช้ โดยที่อนุญาตให้ติดตั้งแอปพลิเคชันจากแหล่งภายนอก และไม่เข้าใจในข้อตกลง จึงทำให้มีความเสี่ยงต่อการโจมตีมัลแวร์ ซึ่งในการศึกษาครั้งนี้พบว่าผู้ที่ใช้โมบายแอปพลิเคชันอยู่แล้วส่วนใหญ่มีพฤติกรรมการใช้ ที่ปลอดภัยจากมัลแวร์ แต่ยังมีบางส่วนที่ยังมีพฤติกรรมการใช้สมาร์ทโฟนที่อาจเปิดช่องโหว่ให้มัลแวร์โจมตีได้ ซึ่งควรจะต้องมีการให้ความรู้แก่ผู้ใช้กลุ่มนี้ ในการใช้ระบบ m-banking ให้ปลอดภัยต่อไป และในอนาคตอาจทำการศึกษาเพิ่มเติมในส่วนของการสังเกตชื่อผู้พัฒนาแอปพลิเคชันที่เป็นรูปธรรมมากขึ้น ซึ่งเป็นขอบเขตนอกเหนือจากงานวิจัยนี้ จากงานวิจัยนี้จะเห็นได้ว่าระบบ m-banking มีความปลอดภัยมั่นคงสูงกว่าระบบ i-banking มากในภาพรวม

## กิตติกรรมประกาศ

ขอขอบคุณฝ่ายคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ (DSI) กระทรวงยุติธรรม สำหรับข้อมูลคดีด้านเทคโนโลยีสารสนเทศเกี่ยวกับธนาคารที่เกิดขึ้นในประเทศไทยในรอบหลายปีที่ผ่านมา และขอขอบคุณผู้อำนวยการฝ่ายเครือข่ายและ IT Security ของธนาคารแห่งหนึ่ง ที่ได้ให้ข้อมูลในเชิงลึกเพื่อประกอบการวิจัยครั้งนี้

## เอกสารอ้างอิง

[1] 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.

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

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

[4] 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.

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

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

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

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

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

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

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

[12] ธนาคารแห่งประเทศไทย. นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์. ราชกิจจานุเบกษา, 2552.

[13] it24hrs.com. คนร้ายสวมรอยเป็นเจ้าของบัญชี Internet Banking โอนเงินออก สูญหลายแสน. [สืบค้นเมื่อ 24 กรกฎาคม 2557]; ได้จาก/4102/moc.srh42ti.www//:ptth:/2-drac-mis-wen-egnahc-gniknab-pto-kcah.

[14] ระวัง แอพธนาคารปลอม ระบาดบน Play Store ของมือถือ Android.[สืบค้นเมื่อ 5 กันยายน 2558]; ได้จาก//:ptth : -no-ekaf-gniknab-e-ppa/4102/moc.srh42ti.www/diordna.

[15] 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.

[16] Article A. รายงานผลการวิจัยมาตรการรักษาความมั่นคงปลอดภัยระบบ Internet Banking และ ระบบ Mobile

Banking ของธนาคารในประเทศไทย. [สืบค้นเมื่อ 30 มีนาคม 2559]; ได้จาก: https://www.acisonline.net/?p=961&lang=th.

[17] สุวรรณี ธูปจีน, ระดม เจือจันทร์, ศิรปัฐช์ บุญครอง. การตรวจจับพฤติกรรมและป้องกันมัลแวร์บนโทรศัพท์มือถือแอนดรอยด์.วารสารวิทยาศาสตร์และเทคโนโลยี. บทความวิชาการ (Scholarly Article); 2558; หน้า 141-152.

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

[19] Baraka W. Nyamtiga, Anael Sam, Loserian S. Laizer. Enhanced Security Model for Mobile Banking Systems in Tanzania. International Journal of Technology Enhancements and Emerging Engineering Research; Vol 1, Issue 4, 2013.

[20] Jiraporn Sripalawat, Mathupayas Thongmak, Atcharawan Ngramyarn. M-Banking in Metropolitan Bangkok and a Comparison with other Countries. Journal of Computer Information Systems; Vol 51, Issue 3, 2011.

[21] 3G คืออะไร. [สืบค้นเมื่อ 15 มิถุนายน 2558]; ได้จาก: https://lovelovelover77.wordpress.com.

[22] How is 4G LTE encrypted. [สืบค้นเมื่อ 1 พฤศจิกายน 2558]; ได้จาก: http://security.stackexchange.com/questions/21395/how-is4-g-lte-encrypted.