การสำรวจการรักษาความปลอดภัยในการใช้งานอินเทอร์เน็ตแบงค์กิ้งธนาคารพาณิชย์ไทยสำหรับลูกค้าบุคคล

A Survey of Internet Banking Security of Thailand's Commercial Banks: Personal Customer Perspective

ธนพล พุกเส็ง* และศิรปัฐช์ บุญครอง

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ถนนประชาราษฎร์ 1 แขวงวงศ์สว่าง เขตบางซื่อ กรุงเทพมหานคร 10800

Thanaphon Phukseng* and Sirapat Boonkrong

Faculty of Information Technology, King Mongkut's University of Technology North Bangkok,

Pracharat 1 Road, Wongsawang, Bangsue, Bangkok 10800

บทคัดย่อ

อินเทอร์เน็ตแบงค์กิ้งเป็นบริการธุรกรรมทางการเงินที่ธนาคารพาณิชย์ไทยได้นำมาใช้เพื่ออำนวยความสะดวกต่อลูกค้าของธนาคาร โดยเฉพาะกลุ่มลูกค้าบุคคลที่มีอยู่เป็นจำนวนมาก แต่บริการดังกล่าวก็มีความเสี่ยงต่อความปลอดภัยในการใช้บริการ เช่น การปลอมแปลงเว็บไซต์ธนาคารเพื่อขโมยข้อมูลส่วนบุคคล หรือการโจมตีการพิสูจน์ตัวตนบุคคลที่เข้าใช้ระบบ ดังนั้นบทความนี้จึงมีวัตถุประสงค์เพื่อนำเสนอการรักษาความปลอดภัยในการใช้งานอินเทอร์เน็ตแบงค์กิ้งธนาคารพาณิชย์ไทยสำหรับกลุ่มลูกค้าบุคคล โดยศึกษาจากธนาคารพาณิชย์ไทย ได้แก่ ธนาคารกรุงเทพ จำกัด (มหาชน) ธนาคารกรุงไทย จำกัด (มหาชน) ธนาคารกรุงศรีอยุธยาจำกัด (มหาชน) ธนาคารกสิกรไทย จำกัด (มหาชน) ธนาคารทหารไทย จำกัด (มหาชน) และธนาคารไทยพาณิชย์ จำกัด (มหาชน) จากการศึกษาพบว่ามีวิธีการรักษาความปลอดภัยทั้งหมด 6 ลักษณะ คือ SSL ใบรับรองดิจิตอล CAPTCHA บัญชีผู้ใช้และรหัสผ่าน OTP และการพิสูจน์ทราบตัวตนด้วยสองปัจจัย ซึ่งในบทความนี้ได้กล่าวถึงหลักการในการทำงาน ลักษณะของการคุกคามที่เกิดขึ้น วิธีการป้องกันและแก้ปัญหาของแต่ละวิธีการรักษาความปลอดภัย รวมถึงแนวทางในการปฏิบัติตนของผู้ใช้งานเพื่อป้องกันภัยในการใช้งานอินเทอร์เน็ตแบงค์กิ้ง

คำสำคัญ : อินเทอร์เน็ตแบงค์กิ้ง; SSL; ใบรับรองดิจิตอล; CAPTCHA; บัญชีผู้ใช้และรหัสผ่าน; OTP; การพิสูจน์ทราบตัวตนด้วยสองปัจจัย

Abstract

Internet banking is financial transaction management system that commercial banks in Thailand have employed to facilitate the majority of their customers especially personal

***ผู้รับผิดชอบบทความ :** thanaphon134@yahoo.com

customer. However, the service can be insecure from threats such as phishing or authentication attack. The objective of this paper is to present the security methods of Thailand's internet banking for personal customer perspective. This paper investigates how the Thai commercial banks deal with internet banking threat problems. The banks studied include Bangkok Bank Public Company Limited, Krung Thai Bank Public Company Limited, Bank of Ayudhya Public Company Limited, Kasikorn Bank Public Company Limited, TMB Bank Public Company Limited, and Siam Commercial Bank Public Company Limited. The studies reveal that six methods for internet banking security currently used are SSL, Digital Certificate, CAPTCHA, Username and Password, OTP and Two-Factor Authentication. The paper also discusses how each threat occurs, how each method works, how each method prevents and solves the individual threat as well as the guidance for internet banking users.

Keywords: internet banking; SSL; digital certificate; CAPTCHA; username and password; OTP; two-factor authentication

1. บทนำ

การทำธุรกรรมทางการเงินกับธนาคารเป็นสิ่งจำเป็นที่ทุกคนต้องใช้บริการ ทั้งบริการพื้นฐาน ได้แก่ การฝาก โอน ถอน และชำระค่าบริการ เป็นต้น สำหรับธนาคารพาณิชย์ในประเทศไทยนั้น จากข้อมูลของธนาคารแห่งประเทศไทยในปี พ.ศ. 2556 มีจำนวนทั้งหมด 14 แห่ง ทั้งที่เป็นธนาคารที่ก่อตั้งในประเทศไทย และธนาคารที่ลงทุนจากต่างประเทศ ซึ่งในปัจจุบันธนาคารพาณิชย์ไทยในทุก ๆ ธนาคารนั้น ได้จัดบริการธุรกรรมทางการเงินผ่านทางระบบอินเทอร์เน็ต เพื่ออำนวยความสะดวกให้กับลูกค้า ทั้งนี้กลุ่มลูกค้าที่ใช้บริการมีทั้งลูกค้าบุคคลและลูกค้าธุรกิจ โดยสำหรับกลุ่มลูกค้าบุคคลจะมีสัดส่วนจำนวนใช้งานมากที่สุด [1] แต่ทั้งนี้บริการทางอินเทอร์เน็ตนั้นก็จะต้องเสี่ยงกับความปลอดภัยในการใช้บริการ ดังนั้นจะเป็นการดีถ้าหากผู้ใช้บริการโดยเฉพาะกลุ่มลูกค้าบุคคลจะได้รู้ถึงวิธีการรักษาความปลอดภัยในการใช้งานบริการธุรกรรมทางอินเทอร์เน็ตของธนาคาร ที่เรียกว่าอินเทอร์เน็ตแบงกิ้ง (internet banking, I-banking)

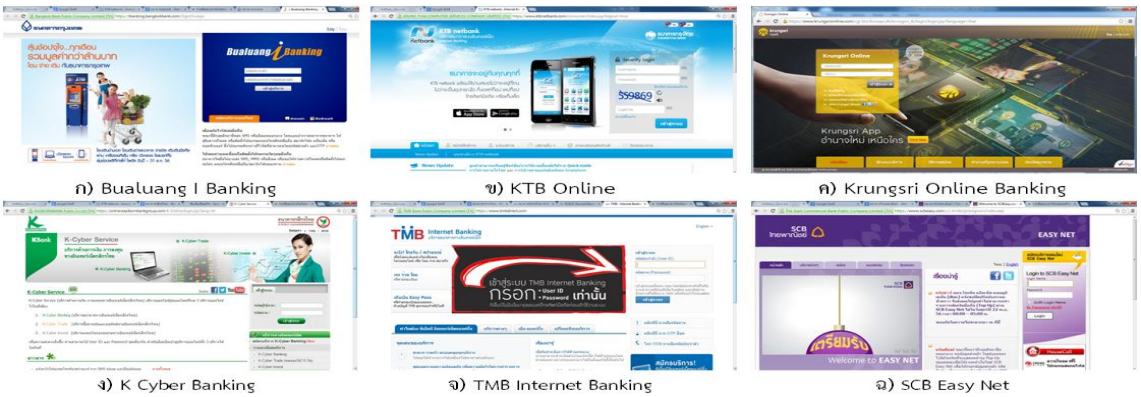
ดังนั้นวัตถุประสงค์ของบทความนี้มุ่งเน้นที่นำเสนอถึงวิธีการรักษาความปลอดภัยที่ธนาคารได้จัดเตรียมไว้เพื่อการเข้าใช้บริการอินเทอร์เน็ตแบงกิ้งของกลุ่มลูกค้าบุคคล โดยกล่าวถึงวิธีการรักษาความปลอดภัย ปัญหาหรือภัยคุกคามที่ได้เคยเกิดขึ้น วิธีการในการป้องกันแก้ปัญหา ตลอดจนแนวทางในการปฏิบัติตัวเพื่อป้องกันภัยคุกคามจากการใช้งานอินเทอร์เน็ตแบงค์กิ้ง ทั้งนี้สำหรับขอบเขตในการพิจารณานั้นจากธนาคารพาณิชย์ในประเทศไทย 14 แห่ง จะเลือกเฉพาะธนาคารพาณิชย์ที่มีการก่อตั้งในประเทศไทยและมีการดำเนินกิจการเป็นระยะเวลายาวนาน เพื่อเป็นกรณีประกอบการศึกษา ซึ่งมี 6 ธนาคาร [2] ได้แก่ ธนาคารกรุงเทพ จำกัด (มหาชน) ธนาคารกรุงไทย จำกัด (มหาชน) ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) ธนาคารกสิกรไทย จำกัด (มหาชน) ธนาคารทหารไทย จำกัด (มหาชน) และธนาคารไทยพาณิชย์ จำกัด (มหาชน)

โครงสร้างบทความประกอบด้วย ส่วนที่ 2 ความหมายของอินเทอร์เน็ตแบงค์กิ้ง ส่วนที่ 3 คุณประโยชน์ของบริการอินเทอร์เน็ตแบงค์กิ้งต่อกลุ่ม

ลูกค้าบุคคล และประเภทของการให้บริการ ส่วนที่ 4 การรักษาความปลอดภัยที่ใช้ในอินเทอร์เน็ตแบงค์กิ้งของธนาคารพาณิชย์ไทยสำหรับกลุ่มลูกค้าบุคคล ส่วนที่ 5 แนวทางในการป้องกันภัยในการใช้งานอินเทอร์เน็ตแบงค์กิ้งสำหรับลูกค้าบุคคล และสุดท้ายส่วนที่ 6 สรุปการนำเสนอ

2. ความหมายของอินเทอร์เน็ตแบงค์กิ้ง

อินเทอร์เน็ตแบงค์กิ้งเป็นกิจกรรมส่วนหนึ่งของธุรกรรมอิเล็กทรอนิกส์ (electronic business) ซึ่งหมายถึงกระบวนการดำเนินธุรกิจโดยอาศัยเทคโนโลยีอิเล็กทรอนิกส์ [3] สำหรับความหมายของอินเทอร์เน็ตแบงค์กิ้งคือการทำธุรกรรมต่าง ๆ กับธนาคารโดยผ่านทางเครือข่ายอินเทอร์เน็ต ได้แก่ การฝากเงิน ถอนเงิน โอนเงินสอบถามยอดเงิน เป็นต้น [1] โดยอินเทอร์เน็ตแบงค์กิ้งนั้นอาจเรียกโดยใช้ชื่ออื่นได้อีก ได้แก่ ออนไลน์แบงค์กิ้ง (online banking) อิเล็กทรอนิกส์แบงค์กิ้ง (electronic banking) หรือไซเบอร์แบงค์กิ้ง (cyber banking) เป็นต้น ทั้งนี้เมื่อแต่ละธนาคารได้พัฒนาระบบอินเทอร์เน็ตแบงค์กิ้งของตนเองแล้ว ก็มีการใช้ชื่อบริการที่แตกต่างกัน ดังนี้ “Bualuang I Banking” ของธนาคารกรุงเทพ จำกัด (มหาชน) “KTB Online” ของธนาคารกรุงไทย จำกัด (มหาชน) “Krungsri Online Banking” ของธนาคารกรุงศรีอยุธยาจำกัด (มหาชน) “K Cyber Banking” ของธนาคารกสิกรไทย จำกัด (มหาชน) “TMB Internet Banking” ของธนาคารทหารไทย จำกัด (มหาชน) และ “SCB Easy Net”ของธนาคารไทยพาณิชย์ จำกัด (มหาชน) ดังตัวอย่างรูปที่ 1



ก) Bualuang I Banking ข) KTB Online ค) Krungsri Online Banking

ง) K Cyber Banking จ) TMB Internet Banking ฉ) SCB Easy Net

รูปที่ 1 หน้าเว็บไซต์อินเทอร์เน็ตแบงค์กิ้ง

3. คุณประโยชน์ของบริการอินเทอร์เน็ตแบงค์กิ้งต่อกลุ่มลูกค้าบุคคลและประเภทของการให้บริการ

เมื่อพิจารณากลุ่มลูกค้าของธนาคารแล้ว โดยส่วนใหญ่ธนาคารจะมีการแบ่งกลุ่มลูกค้าออกเป็นประเภทหลัก ๆ ได้แก่ กลุ่มลูกค้าบุคคลหมายถึงบุคคลทั่วไปที่เป็นผู้ใช้บริการของธนาคาร ซึ่งบางธนาคารอาจมีการแยกเป็นกลุ่มย่อย เช่น ธนาคารกรุงไทย จำกัด (มหาชน) ยังแยกเป็นลูกค้าข้าราชการ และพนักงานรัฐวิสาหกิจ และอีกกลุ่มคือลูกค้าธุรกิจ ซึ่งหลาย ๆ ธนาคารมีการแบ่งกลุ่มย่อย เช่น ลูกค้าธุรกิจ SME ลูกค้าธุรกิจขนาดใหญ่ หรือลูกค้าธุรกิจภาครัฐ ซึ่งในแต่ละกลุ่มลูกค้านั้น ธนาคารก็ได้จัดช่องทางบริการทาง

อินเทอร์เน็ตไว้ให้โดยเฉพาะ และสำหรับกลุ่มลูกค้าบุคคลซึ่งมีจำนวนมาก ในทุกธนาคารได้จัดให้มีช่องทางบริการอินเทอร์เน็ตไว้ให้ โดยคุณประโยชน์ของบริการอินเทอร์เน็ตแบงค์กิ้งที่มีต่อกลุ่มลูกค้าบุคคล [4] คือ (1) ได้รับความสะดวกในการใช้บริการผ่านอินเทอร์เน็ต สามารถทำธุรกรรมได้ทุกที่ทุกเวลาที่เชื่อมต่ออินเทอร์เน็ตได้ (2) มีความรวดเร็วและทำรายการด้วยตนเองได้เป็นเวลานาน (3) สามารถตรวจสอบความถูกต้องหลังทำรายการได้ (4) ประหยัดค่าใช้จ่ายในการเดินทางและค่าธรรมเนียมทำธุรกรรม (5) สามารถสมัครและเรียนรู้การใช้งานได้โดยง่าย

สำหรับประเภทของบริการอินเทอร์เน็ตแบงค์กิ้งของธนาคารพาณิชย์ไทยในกลุ่มลูกค้าบุคคลนั้น จากการศึกษาพบว่ามีบริการที่คล้ายคลึงกัน ได้แก่ การจัดการข้อมูลบัญชี การโอนเงิน และการชำระค่าสินค้าและบริการ ส่วนที่แตกต่างกันตามแต่ละธนาคาร เช่น การจัดการหน่วยลงทุน การจัดการบัตรเครดิตและบริการเสริมอื่น ๆ

4. การรักษาความปลอดภัยที่ใช้ในอินเทอร์เน็ตแบงค์กิ้งของธนาคารพาณิชย์ไทยสำหรับกลุ่มลูกค้าบุคคล

การใช้บริการอินเทอร์เน็ตแบงค์กิ้งของลูกค้าจะเกี่ยวพันกับการเงินแทบทั้งสิ้น ดังนั้นลูกค้าจะต้องมีความไว้ใจในความปลอดภัยของบริการอินเทอร์เน็ตแบงค์กิ้ง ซึ่งปัจจัยในด้านความปลอดภัยนั้นเป็นสิ่งที่ส่งผลต่อการเลือกใช้บริการอินเทอร์เน็ตแบงค์กิ้งเป็นอย่างยิ่ง [3-5] ซึ่งภาพรวมการรักษาความปลอดภัยของอินเทอร์เน็ตแบงค์กิ้งในระดับโลกนั้น มีคล้ายคลึงกัน อาทิ การรักษาความปลอดภัยในความเป็นส่วนตัวของลูกค้า การตรวจสอบยืนยันตัวตนของทั้งเว็บไซต์ธนาคารและลูกค้า [6] และสำหรับบทความนี้จะได้นำเสนอการรักษาความปลอดภัยในการใช้อินเทอร์เน็ตแบงค์กิ้งสำหรับธนาคารพาณิชย์ไทยในกลุ่มลูกค้าบุคคล โดยจะได้กล่าวถึงวิธีการในการรักษาความปลอดภัย รวมถึงปัญหาการโจมตีและวิธีการป้องกันแก้ไขปัญหา โดยมีรายละเอียดต่อไปนี้

4.1 วิธีการในการรักษาความปลอดภัย

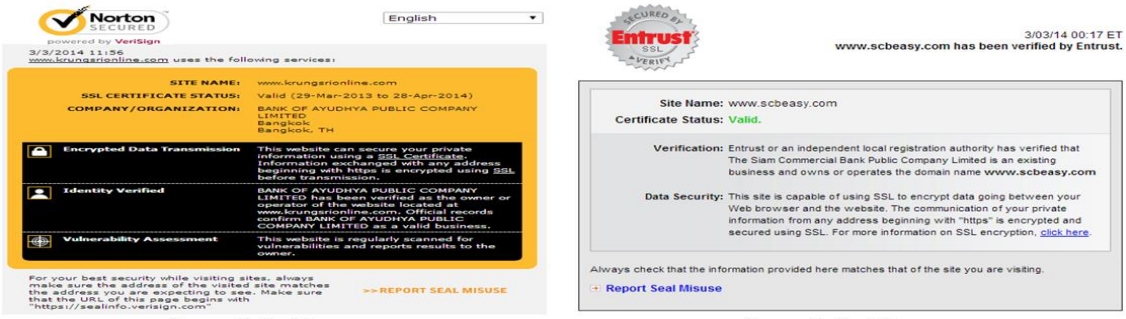
จากการสำรวจพบว่าวิธีการในการรักษาความปลอดภัยของอินเทอร์เน็ตแบงค์กิ้งธนาคารพาณิชย์ไทยนั้น สามารถจำแนกได้เป็น 6 ลักษณะ ดังนี้

4.1.1 SSL (secure socket layer) เป็นข้อตกลงในการสื่อสารหรือโพรโทคอลที่พัฒนาโดย Netscape เพื่อใช้ในการพิสูจน์ตัวตนระหว่างฝั่งผู้ให้บริการ (server) และผู้ใช้บริการ (client) และการเข้ารหัสข้อมูลในการสื่อสาร ซึ่งหน่วยงาน IETF (Internet Engineering Task Force) ได้อาศัยพื้นฐานของโพรโทคอล SSL พัฒนาเป็นโพรโทคอล TLS (transport layer security) เพื่อเป็นมาตรฐานในการสื่อสารอินเทอร์เน็ต [7] โดยโพรโทคอล SSL จะทำงานในชั้นทรานสปอร์ทเลเยอร์ (transport layer) ตามโมเดลของ OSI ดังนั้นจึงรองรับการทำงานของโพรโทคอลอื่นในชั้นแอพลิเคชันเลเยอร์ (application layer) ได้ เช่น HTTP (hyper text transfer protocol) สำหรับขั้นตอนหลักที่สำคัญของโพรโทคอล SSL มีดังนี้ [8] ขั้นแรก การพิสูจน์ทราบตัวจริงของผู้ให้บริการ โดยอาศัยใบรับรองดิจิตอล (digital certificate) ของผู้ให้บริการ ซึ่งจะได้อธิบายในหัวข้อถัดไป ขั้นที่สอง การพิสูจน์ทราบตัวจริงของผู้ใช้บริการ ซึ่งจะทำหรือไม่ก็ได้ และขั้นสุดท้าย การเข้ารหัสและถอดรหัสข้อมูลที่ต้องการติดต่อสื่อสาร ด้วยกุญแจแบบสมมาตร (symmetric key encryption)

ทั้งนี้อินเทอร์เน็ตแบงค์กิ้งนั้นจะดำเนินการผ่านเว็บบราวเซอร์ ซึ่งมีโพรโทคอลในการสื่อสารคือ HTTP แต่เพื่อเพิ่มความปลอดภัยจึงได้เพิ่มโพรโทคอล SSL เข้าไป โดยเรียกว่า HTTPS (HTTP

over SSL) สำหรับข้อสังเกตว่าเว็บบราวเซอร์นั้นใช้โพรโทคอลดังกล่าวหรือไม่ ให้ดูจากช่อง address (URL) จะต้องมี https:// นำหน้าชื่อเว็บไซต์ สำหรับการทำงานของโพรโทคอล HTTPS นั้นมีพื้นฐานการทำงานเช่นเดียวกับโพรโทคอล SSL สำหรับวิธีการเข้ารหัสและขนาดของกุญแจในแต่ละธนาคารนั้นอาจมีความแตกต่างกัน โดยจากการศึกษาพบว่าธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) และธนาคารทหารไทย จำกัด (มหาชน) ใช้กุญแจขนาด 256 บิต ส่วนที่เหลือนั้นใช้กุญแจรหัสขนาด 128 บิต ซึ่งเมื่อเทียบขนาดของกุญแจที่ใช้แล้ว เทคโนโลยีการรหัสที่ใช้กุญแจที่มีขนาดมากกว่าจะมีความปลอดภัยที่สูงกว่าเนื่องจากการคาดเดาจะมีโอกาสทำได้ยากกว่า [8]

4.1.2 ใบรับรองดิจิตอล (digital certificate) คือเอกสารทางอิเล็กทรอนิกส์ที่ใช้ในการยืนยันรับรองบุคคลหรือเว็บไซต์ว่าเป็นจริงตามที่กล่าวอ้าง โดยในการสร้างใบรับรองดิจิตอลนั้นจำเป็นที่ต้องใช้บริการจากหน่วยงานผู้ออกใบรับรองที่เรียกว่า CA (certificate authority) ซึ่งใบรับรองดิจิตอลนั้นมีความสัมพันธ์กับกระบวนการ SSL เนื่องจากจะต้องใช้ใบรับรองดิจิตอลเป็นส่วนสำคัญในการพิสูจน์ทราบตัวตน และสำหรับธนาคารเองก็จะต้องขอใบรับรองดิจิตอลให้กับอินเทอร์เน็ตแบงค์กิ้งด้วย เนื่องจากอินเทอร์เน็ตแบงค์กิ้งก็จะต้องมีการพิสูจน์ตัวตนให้กับผู้ใช้งาน โดยจะเป็นการตรวจสอบและแสดงผลโดยเว็บบราวเซอร์ของผู้ใช้งานนั้นเอง ดังนั้นธนาคารจะต้องลงทะเบียนสร้างใบรับรองดิจิตอลกับ CA ที่เป็นที่เชื่อถือโดยเว็บบราวเซอร์ทั้งหลาย ซึ่งเว็บบราวเซอร์ ในปัจจุบัน เช่น Internet Explorer 7 ขึ้นไป จะตรวจสอบใบรับรอง อายุของใบรับรองด้วย และจากข้อมูลธนาคารที่ได้นำเสนอนั้น ธนาคารกรุงเทพ จำกัด (มหาชน) และธนาคารกรุงไทยจำกัด (มหาชน) ทำใบรับรองดิจิตอลกับ VeriSign ส่วนธนาคารที่เหลือทำใบรับรองดิจิตอลกับ Entrust ซึ่งเป็น CA ที่น่าเชื่อถือและสนับสนุนการทำงานของเว็บบราวเซอร์ ดังตัวอย่างการรับรองที่แสดงในรูปที่ 2



ก) การรับรองเว็บไซต์โดย VeriSign ข) การรับรองเว็บไซต์ โดย Entrust

รูปที่ 2 ตัวอย่างการรับรองเว็บไซต์ของ CA

รูปที่ 2 เป็นตัวอย่างการรับรองเว็บไซต์ โดย (ก) เป็นการรับรองเว็บไซต์อินเทอร์เน็ตแบงค์กิ้งของธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) โดย VeriSign ส่วน (ข) เป็นการรับรองเว็บไซต์อินเทอร์เน็ตแบงค์กิ้งของธนาคารไทยพาณิชย์ จำกัด (มหาชน) โดย Entrust

4.1.3 CAPTCHA (completely automated public turing test to tell

computers and humans apart) เป็นการทดสอบเพื่อแยกแยะว่าการทำงานที่เกิดขึ้น เป็นการกระทำโดยมนุษย์มิใช่โปรแกรมคอมพิวเตอร์ [9] สำหรับ CAPTCHA สามารถแบ่งออกเป็น 3 กลุ่มหลัก [10] คือ (1) แบบอักษรข้อความ (text based CAPTCHA) เป็นการสุ่มภาพของตัวอักขระแล้วทำให้ภาพเกิดการบิดเบี้ยว หรือเติมสิ่งรบกวนเข้าไป และให้ผู้ใช้งานพิมพ์ตามอักขระที่เห็น (2) แบบเสียง (audio-based CAPTCHA) ให้ผู้ใช้งานพิมพ์อักขระตามเสียงที่ได้ยิน หรือออกเสียงตามตัวอักขระที่มองเห็น และ (3) แบบภาพ (image-based CAPTCHA) เป็นการเลือกภาพให้ตรงตามคำสั่ง และสำหรับอินเทอร์เน็ตแบงค์กิ้งนั้น จะมีเฉพาะธนาคารกรุงไทย จำกัด (มหาชน) เท่านั้น ที่นำ CAPTCHA มาใช้ร่วมในกระบวนการเข้าสู่ระบบ โดยเป็นแบบอักษรข้อความ แต่บางธนาคารจะมีการใช้ CAPTCHA ในขั้นตอนอื่นภายหลังการเข้าสู่ระบบแล้ว เช่น ใช้ประกอบในการเปลี่ยนรหัสผ่าน

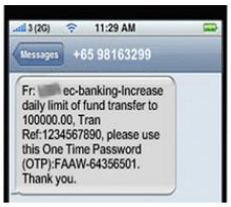
4.1.4 บัญชีผู้ใช้และรหัสผ่าน (username and password or password only) เทคนิคบัญชีผู้ใช้และรหัสผ่านนั้น เป็นวิธีการในการควบคุมการเข้าถึงข้อมูล (access control) รูปแบบหนึ่ง โดยบัญชีผู้ใช้เป็นการระบุตัวตนของผู้ใช้งาน (identification) [11] และรหัสผ่านเป็นการพิสูจน์ทราบตัวตนของผู้ใช้ว่าเป็นบุคคลจริงตามที่กล่าวอ้าง [12] ซึ่งรหัสผ่านนั้นเป็นการพิสูจน์ทราบตัวตนด้วยสิ่งที่ผู้ใช้รู้ (what you know) สำหรับทั้งบัญชีผู้ใช้และรหัสผ่านจะเป็นกลุ่มของตัวอักขระที่ถูกกำหนดโดยผู้ใช้งานและเป็นความลับเฉพาะเจ้าของเท่านั้นที่จะทราบ และเทคนิคนี้เป็นวิธีการพื้นฐานที่อินเทอร์เน็ตแบงค์กิ้งของทุกธนาคารใช้กัน ซึ่งอาจมีความแตกต่างกันในด้านข้อกำหนด เช่น ขนาดความยาวของรหัสผ่าน การบังคับให้ใช้ตัวอักษรผสมตัวเลข [6] และสำหรับการเข้าใช้งานอินเทอร์เน็ตแบงค์กิ้งในครั้งแรกนั้น ธนาคารมักจะจัดส่งบัญชีผู้ใช้และรหัสผ่านมาทางช่องทางอื่น ได้แก่ SMS หรืออีเมล์ เป็นต้น หลังจากนั้นผู้ใช้บริการก็จะสามารถเปลี่ยนบัญชีผู้ใช้และรหัสผ่านได้ในภายหลัง

4.1.5 OTP (one time password) เป็นเทคนิคการใช้รหัสผ่านโดยที่รหัสผ่านที่ได้รับมานั้นจะสามารถใช้ได้เพียงครั้งเดียว จัดเป็นรูปแบบการพิสูจน์ทราบตัวตนด้วยสิ่งที่ผู้ใช้รู้ เช่นเดียวกับการใช้บัญชีผู้ใช้และรหัสผ่าน แต่ OTP นั้นจะมีการเปลี่ยนทุกครั้งที่มีการเข้าใช้ระบบ สำหรับประเภทของ OTP นั้นสามารถแบ่งได้เป็น 4 ประเภท [13] คือ (1) SMS OTP เป็นการส่งรหัสผ่านมาทางโทรศัพท์พกพาในรูปแบบของข้อความสั้น (2) E-mail OTP เป็นการส่งรหัสผ่านมาทางอีเมล์ของผู้ใช้บริการ (3) Token OTP จะใช้อุปกรณ์เสริมในการสร้างและแสดงรหัสผ่านในการเข้าใช้ระบบ ซึ่งผู้ให้บริการจะต้องมอบอุปกรณ์นี้ไว้ให้กับผู้ใช้บริการไว้ก่อนแล้ว (4) challenge/response OTP เป็นการสร้างรหัสผ่านด้วยข้อมูล challenge ระหว่างผู้ให้บริการและผู้ใช้บริการ ซึ่งถ้าตรงกันก็สามารถเข้าสู่ระบบได้

รูปที่ 3 เป็นตัวอย่าง OTP โดย (ก) เป็น SMS OTP ส่วน (ข) เป็นตัวอย่างอุปกรณ์ Token OTP

สำหรับอินเทอร์เน็ตแบงค์กิ้งในกลุ่มลูกค้าบุคคลนั้น จากการศึกษาพบว่าในทุกธนาคารใช้ SMS OTP ซึ่งลูกค้าต้องลงทะเบียนหมายเลขโทรศัพท์ไว้กับธนาคารก่อนแล้ว โดยจะมีการใช้ OTP ประกอบในการปรับปรุงข้อมูลส่วนตัวของผู้ใช้งาน และการทำธุรกรรมทางการเงินที่สัมพันธ์กับบุคคลอื่น ได้แก่ การโอนเงินไปยังบัญชีบุคคลอื่นหรือต่างประเทศ รวมถึงการชำระค่าสินค้าหรือบริการ ซึ่งในรายละเอียดรูปแบบของข้อความใน SMS OTP นั้นก็จะแตกต่างกันไป เช่น ธนาคารกรุงไทย จำกัด (มหาชน) จะมีการแจ้ง

หมายเลขอ้างอิงมาควบคู่กับรหัสผ่าน หรือธนาคารไทยพาณิชย์ จำกัด (มหาชน) แจ้งหมายเลขบัญชีมาควบคู่กับรหัสผ่าน แต่ทั้งนี้ SMS OTP ที่ผู้ใช้งานได้รับมานั้นจะมีเวลาในการใช้งานจำกัดไว้ ถ้าหากภายในเวลาที่กำหนดไม่มีการเข้าใช้บริการก็จะต้องร้องของ SMS OTP ใหม่อีกครั้ง



ก) SMS OTP

ข) Token OTP

รูปที่ 3 ตัวอย่าง SMS OTP และ Token OTP [14]

4.1.6 การพิสูจน์ทราบตัวตนด้วยสองปัจจัย (two-factor authentication) เป็นการควบคุมการเข้าถึงระบบโดยการเพิ่มกลไกในการพิสูจน์ทราบตัวตนเป็นสองชั้น โดยอาศัยหลักเทคนิคในการรักษาความปลอดภัยที่มีอยู่เดิมแต่ต้องกระทำเป็นสองขั้น [15] ตัวอย่าง เช่น ในการถอนเงินจากตู้เอทีเอ็มนั้น ผู้ใช้งานจะต้องมีบัตรเอทีเอ็ม ซึ่งเป็นการพิสูจน์ตัวตนด้วยสิ่งที่ผู้ใช้มี (what you have) และจะต้องทราบรหัสผ่านเพื่อสำหรับกดทำธุรกรรมจากตู้เอทีเอ็ม (what you know) ซึ่งเป็นการพิสูจน์ตัวตนด้วยสิ่งที่ผู้ใช้รู้ และสำหรับการทำงานของอินเทอร์เน็ตแบงค์กิ้งนั้น ทั้ง 6 ธนาคาร ก็มีการพิสูจน์ตัวตนด้วยสองปัจจัยเช่นกัน แต่จะแยกส่วนออกจากกัน ได้แก่ ในส่วนแรกการเข้าสู่ระบบจะใช้เทคนิคบัญชีผู้ใช้และรหัสผ่านเพื่อเป็นการนำเข้าสู่อินเทอร์เน็ตแบงค์กิ้ง และหลังจากนั้นในการทำธุรกรรม เช่น การโอนเงิน หรือการชำระค่าสินค้าก็จะใช้เทคนิค OTP เพื่อตรวจสอบพิสูจน์ทราบตัวตนอีกครั้งหนึ่ง

4.2 ปัญหาการโจมตีและวิธีการป้องกันแก้ไขปัญหา

จากวิธีการรักษาความปลอดภัยที่ได้นำเสนอไปนั้น จะได้ยกตัวอย่างของปัญหาและการโจมตี ตลอดจนแนวทางในการป้องกันและแก้ปัญหาที่พบในการรักษาความปลอดภัยดังนี้

4.2.1 SSL มีโอกาสที่ถูกโจมตีได้ ดังตัวอย่างต่อไปนี้

(1) BEAST (browser exploit against SSL/TLS) เป็นการโจมตีโดยการอาศัยการคาดเดาค่า IV (initialisation vector) ที่เป็นค่าตั้งต้นที่ใช้ในการเข้ารหัส หรือการใช้โปรแกรมประสงค์ร้าย (malicious code) เพื่อดักจับข้อมูลที่เป็นส่วนสำคัญในการเข้ารหัสแบบ CBC mode ซึ่ง CBC mode นั้นจะแบ่งข้อมูลออกเป็นบล็อก โดยที่ก่อนที่จะเข้ารหัสจะนำบล็อกข้อมูลผ่านกระบวนการ Exclusive OR (XOR) กับผลลัพธ์ที่ได้จากการเข้ารหัสของบล็อกก่อนหน้า ส่วนในบล็อกแรกจะดำเนินการกับค่า IV ซึ่งวิธีการนี้ได้ใช้กันในกระบวนการ SSL โดยเป็นการดำเนินการทางฝั่งของผู้ใช้บริการ สำหรับหนทางหนึ่งในการป้องกัน คือผู้ให้บริการอาจหลีกเลี่ยงการเข้ารหัสแบบ CBC mode [16]

(2) SSL stripping attack เป็นการโจมตีการสื่อสารที่มีการติดต่อกันด้วยโพรโทคอล SSL โดยจะโจมตีแบบแทรกกลางระหว่างการสื่อสาร (MITM, man in the middle) ซึ่งผู้โจมตีจะแทรก

กลางระหว่างการสื่อสารของ ผู้ใช้บริการและผู้ให้บริการแล้ว ทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูลที่มีการสื่อสารกัน โดยที่ทั้ง 2 ฝ่าย ไม่อาจทราบได้ ซึ่งผู้โจมตีจะสามารถเห็นข้อมูลและเปลี่ยนแปลงข้อมูลได้ โดยถ้าเป็นอินเทอร์เน็ตแบงค์กิ้งซึ่งใช้โพรโทคอล HTTPS ข้อมูลที่ติดต่อกันจะถูกถอด SSL ออกและทำให้เกิดการสื่อสารด้วยโพรโทคอล HTTP ที่ไม่มีความปลอดภัย [17]

จากการโจมตีดังกล่าวได้มีการนำเสนอวิธีการแก้ปัญหาหลายวิธี เช่น วิธี HProxy [18] ซึ่งจะตรวจสอบ SSL stripping attack โดยจะติดตั้งการทำงานบน proxy ของฝั่งผู้ใช้บริการ และการเก็บประวัติการใช้งานเว็บไซต์ เพื่อตรวจสอบว่าเป็นการสื่อสารด้วยโพรโทคอล HTTPS หรือไม่ ข้อจำกัดของรูปแบบนี้คือจะทำได้เพียงการแจ้งเตือนเท่านั้น วิธี SSLight [19] โดยพัฒนาส่วนต่อขยายให้กับเว็บบราวเซอร์ ซึ่งจะมีการใช้สีในการเตือนถึงระดับความปลอดภัยของเว็บไซต์นั้นในช่องการใส่บัญชีผู้ใช้และรหัสผ่าน แต่วิธีนี้มีข้อจำกัดที่สามารถใช้ได้กับเฉพาะเว็บบราวเซอร์ Google Chrome เท่านั้น หรืออีกวิธีหนึ่งคือ HSTS (HTTP strict transport security) [20] โดยเป็นการกำหนดให้เว็บบราวเซอร์มีการตอบกลับส่วนของ HTTP header ซึ่งจะกำหนดระยะเวลาในการใช้งานโพรโทคอล HTTPS ไว้ สำหรับวิธีการนี้ก็ยังมีข้อจำกัดที่สามารถรองรับได้แค่เว็บบราวเซอร์ Google Chrome และ Firefox เท่านั้น นอกจากนั้นรายชื่อเว็บไซต์ที่ใช้งานจะต้องอยู่ใน HSTS list อีกด้วย สำหรับการโจมตี แบบ SSL stripping attack ก็ยังมีการวิจัยเพื่อหาทางป้องกันอย่างต่อเนื่อง

และนอกจากการโจมตีที่ได้ยกตัวอย่างไปนั้น ยังมีการโจมตี SSL ลักษณะอื่นอีก [21] ได้แก่ CRIME (compression ratio info-leak made easy) TIME (timing info-leak made easy) และ Lucky 13 attack เป็นต้น

ซึ่งจากตัวอย่างของการโจมตีที่ได้นำเสนอนั้นในฐานะผู้ใช้งานก็จะต้องมีความรอบคอบในการใช้งานเครือข่ายที่มีการรักษาความปลอดภัย ตรวจสอบเว็บไซต์ที่ใช้งาน รวมถึงควรอัพเดทเว็บบราวเซอร์อย่างสม่ำเสมอก็จะช่วยป้องกันปัญหาการโจมตีนี้ได้ดียิ่งขึ้น

4.2.2 ใบรับรองดิจิตอล จะพบปัญหาที่เกี่ยวกับการปลอมแปลงใบรับรองดิจิตอลหรือความไม่น่าเชื่อถือ ดังตัวอย่างที่นำเสนอต่อไปนี้

(1) ในปี ค.ศ. 2011 ตัวแทนจำหน่ายใบรับรองดิจิตอลในประเทศอิตาลีของบริษัท Comodo ได้ถูกแฮกเกอร์ “Ich Sun” โจมตี ซึ่งแฮกเกอร์ได้ใช้สิทธิ์ในการขอใบรับรองจากบริษัท Comodo และรับรองเว็บไซต์ให้มีโปรไฟล์การทำงานสูงขึ้น แต่ในไม่กี่ชั่วโมงต่อมา บริษัทได้ทราบข้อมูลการโดนโจมตี จึงได้เพิกถอนใบรับรองปลอม และแจ้งเตือนลูกค้าให้ทราบ [22]

(2) ในปีเดียวกัน บริษัท DigoNotor ผู้ให้บริการใบรับรองดิจิตอลของเนเธอแลนด์ ได้แจ้งถึงการออกใบรับรองปลอมให้กับโดเมนต่าง ๆ รวมถึง Google Yahoo และ Mozilla ซึ่งเกิดจากการถูกลอบใช้ระบบ หลังจากนั้นบริษัทต้องประกาศเพิกถอนใบรับรองต่าง ๆ แต่ก็ไม่สามารถยืนยันได้ว่าเพิกถอนได้ทั้งหมด สำหรับผลกระทบที่เกิดขึ้น เช่น ผู้ที่ดาวน์โหลดโปรแกรมที่มีการรับรองจาก Google ก็ไม่สามารถตรวจสอบการรับรองได้ว่าเป็นของจริงหรือไม่ [23]

(3) การพัฒนา Malware ที่ปลอมใบรับรองดิจิตอล โดยมีรายงานการพบ Malware เช่น Win32/FakePav มีลักษณะเป็นโปรแกรม antivirus ปลอม โดยจะปลอมใบรับรองที่มีชื่อเดียวกัน แต่แตกต่างกันที่หน่วยงานผู้ออกใบรับรอง ทำให้ส่งผลต่อชื่อเสียงของเว็บไซต์ที่มีการรับรองด้วยใบรับรองปลอม [24]

จากตัวอย่างการโจมตีจะเห็นได้ว่าถึงแม้จะมีการโจมตีใบรับรองดิจิตอลแต่ถ้าหากเว็บไซต์นั้นได้รับการรับรองจาก CA ที่น่าเชื่อถือก็จะทำให้การแก้ปัญหาสามารถเกิดได้อย่างรวดเร็วและไม่เกิดผลร้ายแรงไปในวงกว้าง รวมถึงถ้าผู้ใช้งานมีการตรวจสอบการรับรองก็จะช่วยให้มีความปลอดภัยสูงขึ้น โดยสามารถตรวจสอบด้วยตนเองโดยสังเกตสัญลักษณ์การรับรองจาก CA และเมื่อคลิกลงไปจะแสดงข้อมูลการรับรองดังในรูปที่ 2 นอกจากนั้นถ้าผู้ใช้งานอัพเดทเว็บบราวเซอร์ก็จะเป็นการปรับปรุงข้อมูลของใบรับรองเว็บไซต์ได้อีกด้วย

4.2.3 CAPTCHA สามารถโดนโจมตีจากโปรแกรมคอมพิวเตอร์ประสงค์ร้ายได้ ดังนั้นในส่วนของผู้ใช้งานก็ควรติดตั้งและใช้งานโปรแกรม antivirus เพื่อเป็นการป้องกันภัยจากโปรแกรมคอมพิวเตอร์ประสงค์ร้าย แต่เนื่องจากเทคโนโลยีที่มีการพัฒนาขึ้นมาก ลักษณะการโจมตี CAPTCHA ก็พัฒนาขึ้นเช่นกัน ดังนั้น CAPTCHA ก็จะต้องมีการปรับเปลี่ยนรูปแบบเพื่อให้ทันต่อเทคโนโลยี ซึ่งในที่นี้จะได้ยกตัวอย่างพัฒนาการรูปแบบของ CAPTCHA โดยจะมุ่งไปที่แบบอักษรข้อความ ตามตัวอย่างในรูปที่ 4 ต่อไปนี้

ก) Gimmy CAPTCHA ข) CAPTCHA based on image hiding

ค) reCAPTCHA ง) Fedora CAPTCHA

รูปที่ 4 ตัวอย่าง CAPTCHA แบบอักษรข้อความลักษณะต่าง ๆ

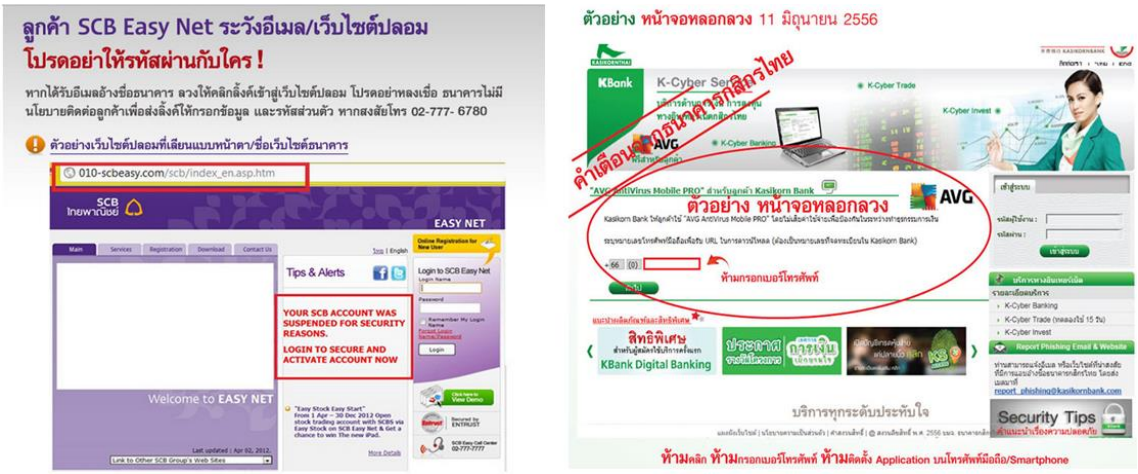
รูปที่ 4 เป็นการนำเสนอภาพตัวอย่างของ CAPTCHA ทั้งสี่ลักษณะ โดย (ก) Gimmy CAPTCHA เป็นยุคแรก ๆ ของ CAPTCHA จะมีการกำหนดข้อความไว้จำนวนหนึ่งแล้วให้ผู้ใช้งานระบุข้อความบางส่วน ซึ่งจะยากต่อการที่โปรแกรมคอมพิวเตอร์จะคำนวณ แต่ก็อาจยากเกินที่ผู้ใช้งานจะระบุข้อความให้ถูกต้องเช่นกัน [25] (ข) CAPTCHA based on image hiding เป็นการซ่อนคำในภาพที่มีการพราง ซึ่งคอมพิวเตอร์จะมองเห็นเฉพาะภาพ แต่มนุษย์จะมองเห็นเป็นข้อมูลที่ซุกซ่อนอยู่ ซึ่งลักษณะนี้จะเหมาะสมกับเว็บบราวเซอร์ Internet Explorer [25] (ค) reCAPTCHA เป็น CAPTCHA ที่มีข้อความ 2 ชุด และตกแต่งบิดภาพให้บิดเบี้ยว ผสมกับการมีเสียงการสะกดให้กับผู้มีปัญหาทางสายตา ซึ่งยังเป็นที่นิยมใช้กันโดยทั่วไป [26] และ (ง) Fedora CAPTCHA จะเป็นการแสดงตัวเลขแล้วให้ผู้ใช้ดำเนินการตามภาพ

เช่น การบวกเลขแล้วใส่ผลลัพธ์ แต่ก็ไม่เหมาะสมกับผู้มีปัญหาทางสายตา [10]

นอกจากนั้นในอนาคตจะได้มีการผสมผสาน CAPTCHA ในรูปแบบอื่นเพื่อความสามารถในการแยกการทำงานระหว่างมนุษย์กับคอมพิวเตอร์ให้มากขึ้น

4.2.4 เทคนิคบัญชีผู้ใช้และรหัสผ่านมีโอกาสถูกโจมตีได้ ตัวอย่าง เช่น [27]

(1) ฟิชชิง (phishing) เป็นการหลอกลวงปลอมแปลงอีเมล์หรือหน้าเว็บไซต์เพื่อวัตถุประสงค์ในการขโมยข้อมูลส่วนบุคคล เช่น บัญชีผู้ใช้และรหัสผ่าน สำหรับวิธีการป้องกันนั้นอาจแบ่งได้เป็น 2 วิธี [28] คือ วิธีแรกแบบบัญชี (list) โดยจะเทียบ URL กับฐานข้อมูลบัญชีดำ (black list) ซึ่งเป็นฐานข้อมูลที่มีการบันทึกรายชื่อเว็บไซต์ที่มีลักษณะของฟิชชิง แต่ทั้งนี้ฐานข้อมูลนั้นไม่ใช่ฐานข้อมูลกลางที่ใช้ร่วมกัน และวิธีที่สองแบบฮิวริสติก (heuristic) เป็นวิธีการที่อาศัยข้อมูลหลายด้านมาประกอบกัน เพื่อให้คอมพิวเตอร์คำนวณวิเคราะห์รูปแบบหรือพฤติกรรมที่เป็นการโจมตีระบบคอมพิวเตอร์ ทั้งนี้มีการเสนอวิธีคำนวณเพื่อตรวจจับฟิชชิงหลายรูปแบบ เช่น การตรวจจับฟิชชิงด้วยหลักการเรียนรู้ของเครื่องคอมพิวเตอร์ (machine learning) ซึ่งจากการทดลองพบว่าเทคนิคโครงข่ายประสาทเทียม (neural network) จะช่วยเพิ่มความสามารถในการตรวจจับได้ดีขึ้น [29] และสำหรับการปลอมอินเทอร์เน็ตแบงค์กิ้งนั้น ธนาคารก็ได้แจ้งเตือนให้ลูกค้าได้ทราบ ดังเช่นตัวอย่างในรูปที่ 5



ก) การแจ้งเตือนเว็บฟิชชิงธนาคารไทยพาณิชย์จำกัด (มหาชน) ข) การแจ้งเตือนเว็บฟิชชิงธนาคารกสิกรไทยจำกัด (มหาชน)

รูปที่ 5 ตัวอย่างการแจ้งเตือนเว็บฟิชชิงของธนาคาร

รูปที่ 5 ตัวอย่างการแจ้งเตือนการพบเว็บ ฟิชชิงของธนาคาร โดย (ก) เป็นของธนาคารไทยพาณิชย์ จำกัด (มหาชน) ส่วน (ข) เป็นของธนาคารกสิกรไทย จำกัด (มหาชน)

(2) Brute force attack หมายถึง การโจมตีผู้ใช้งานที่มีการใช้รหัสผ่านง่าย หรือคาดเดาได้ง่าย ซึ่งผู้โจมตีอาจมีการเปรียบเทียบกับพจนานุกรมรหัสผ่าน และอาจจะโจมตีจนกว่าจะได้รหัสผ่านที่ถูกต้อง

(3) การโจมตีด้วย Trojan horse [30] ในบางครั้งเครื่องคอมพิวเตอร์ของผู้ใช้งานอาจจะมีการติดตั้งโปรแกรมซึ่งมีการแฝงตัวของโปรแกรม

malware ซึ่งจะขโมยข้อมูลและส่งกลับไปยังผู้โจมตี ดังนั้นในการติดตั้งโปรแกรมใด ๆ ในเครื่องจึงต้องมีความระมัดระวังด้วย

จากที่นำเสนอจะเห็นได้ว่าเป็นปัญหาที่เกิดจากตัวของผู้ใช้งานเป็นหลัก ดังนั้นผู้ใช้งานจะต้องมีความรอบคอบในการใช้งานเว็บไซต์ การดาวน์โหลดโปรแกรม รวมถึงการกำหนดรหัสผ่าน ตลอดจนควรเปลี่ยนรหัสผ่านอยู่เป็นระยะก็จะช่วยลดความเสี่ยงได้

4.2.5 การใช้บริการ OTP โดยเฉพาะ SMS OTP ก็สามารถถูกโจมตีจากผู้ไม่ประสงค์ดีหรืออาจมีปัญหาในการใช้งานได้ ดังตัวอย่างต่อไปนี้

(1) Mobile phone Trojans [31] เป็น malware ที่ออกแบบมาเพื่อขัดขวาง SMS OTP ตัวอย่าง เช่น The ZITMO (Zeus In the mobile) Trojans ซึ่งทำงานบนระบบปฏิบัติการ Symbian โดยจะร้องขอ SMS ผ่านทางเครือข่ายได้เอง ซึ่งเมื่อได้ข้อความแล้วยังส่งต่อข้อความ และลบ SMS ในเครื่องได้ และต่อมาได้มีการตรวจพบ malware ตัวนี้ในระบบปฏิบัติการอื่น เช่น Window และ Android อีกด้วย

(2) SMS delay [32] คือการที่ SMS เดินทางมาถึงโทรศัพท์ล่าช้า ทั้งนี้อาจขึ้นอยู่กับผู้ให้บริการโทรศัพท์ หรือปัจจัยอื่น เช่น ความหนาแน่นของเครือข่ายการสื่อสาร และกำลังไฟฟ้าในแบตเตอรี่ เป็นต้น ซึ่งจากตัวอย่างของธนาคารในประเทศมาเลเซีย มีความคาดหวังว่าให้ SMS จะต้องถึงผู้ใช้บริการภายใน 5 นาที ซึ่งถ้าข้อความไปถึงช้ากว่าเวลาที่กำหนดก็จะส่งผลต่อการทำธุรกรรม คือจะต้องดำเนินกระบวนการใหม่อีกครั้ง

จากตัวอย่างการโจมตี จะเห็นว่าปัญหาที่เกิดเป็นผลมาจากการสื่อสารเป็นหลัก ดังนั้นผู้ใช้งานควรระมัดระวังการติดตั้งโปรแกรมที่ดาวน์โหลดมาจากแหล่งที่ไม่น่าไว้ใจ และอาจหลีกเลี่ยงการทำธุรกรรมในช่วงเวลาที่มีผู้ใช้งานเครือข่ายโทรศัพท์หนาแน่นเพื่อลดปัญหาการล่าช้าในการส่งข้อมูลได้

4.2.6 การใช้เทคนิคการพิสูจน์ทราบตัวตนด้วยสองปัจจัยก็อาจโดนโจมตีได้ เช่น การโจมตีด้วย MITM และ Phishing [33] โดยเริ่มจากสกัดกั้นการรับใบรับรองที่เครื่องผู้ใช้งาน แล้วจะหาบัญชีผู้ใช้และรหัสผ่านจากการฟิชชิง และเมื่อผู้ใช้งานเข้าสู่ OTP ก็จะโจมตี OTP และขวางกลางการสื่อสาร หรือ MITM ซึ่งในกรณีนี้ได้เคยเป็นปัญหากับธนาคารต่างประเทศ เช่น Swedish Internet Bank ในปี ค.ศ. 2005 และธนาคาร CitiBank ในปี ค.ศ. 2006 เป็นต้น สำหรับปัญหานี้ผู้ใช้งานเองต้องระมัดระวัง โดยควรใช้งานเครือข่ายที่มีการรักษาความปลอดภัย และตรวจสอบเว็บไซต์ที่เข้าใช้งานเพื่อป้องกันปัญหาพิชชิ่ง

และนอกจากการใช้เทคนิคการพิสูจน์ทราบตัวตนด้วยสองปัจจัยที่ใช้บัญชีผู้ใช้และรหัสผ่านร่วมกับ OTP แล้ว ก็ยังมีลักษณะอื่นอีก เช่น Biometric ได้แก่ ลายนิ้วมือ มาควบคู่กับรหัสผ่าน [34] หรือกระบวนการยืนยันที่มีมากกว่าสองปัจจัย ซึ่งจะช่วยเพิ่มความปลอดภัยให้มากขึ้น

และจากที่ได้กล่าวถึงการรักษาความปลอดภัยที่ใช้ในอินเทอร์เน็ตแบงกิ้งมาทั้งหมดนั้น ก็จะได้สรุปการนำเสนอโดยในตารางที่ 1 เป็นการเปรียบเทียบวิธีการรักษาความปลอดภัยในการใช้บริการอินเทอร์เน็ตแบงค์กิ้งสำหรับลูกค้าบุคคลของทั้ง 6 ธนาคาร และตารางที่ 2 จะเป็นการสรุปตัวอย่างปัญหา การโจมตี รวมถึงแนวการป้องกันในการรักษาความปลอดภัยทั้ง 6 วิธี ดังนี้

จากตารางที่ 1 เป็นการสรุปวิธีการรักษาความปลอดภัยที่แต่ละธนาคารใช้ ซึ่งจะมีแค่ CAPTCHA เท่านั้นที่มีเพียง ธนาคารกรุงไทยจำกัด (มหาชน) ใช้ในขั้นตอนการเข้าสู่ระบบ แต่ที่สำคัญคือการที่ทุกธนาคารเลือกใช้การพิสูจน์ทราบตัวตนด้วย

สองปัจจัย ซึ่งเป็นวิธีในการรักษาความปลอดภัยต่อการใช้บริการอินเทอร์เน็ตแบงค์กิ้งได้ดีอย่างยิ่ง และจากตารางที่ 2 จะเห็นได้ว่าจากปัญหาและการโจมตีที่เกิดขึ้นต่าง ๆ นั้น ในการป้องกันและแก้ปัญหา สำหรับผู้ใช้งานจะต้องมีความระมัดระวังตั้งแต่การเข้าใช้งานเว็บไซต์ ไม่ใช้งานเครือข่ายสาธารณะ (public network) ที่ไม่มีการรักษาความปลอดภัย อัพเดทเว็บบราวเซอร์อย่างสม่ำเสมอ รวมถึงระมัดระวังในการใส่รหัสผ่านเข้าใช้งานระบบด้วย ส่วนธนาคารผู้ให้บริการนั้นจะต้องมีการปรับปรุงนำเทคโนโลยีใหม่ ๆ มาใช้เพื่อเป็นการเพิ่มความปลอดภัยให้มากยิ่งขึ้น ซึ่งก็ได้มีงานวิจัยที่เกี่ยวข้องกับความปลอดภัยของอินเทอร์เน็ตแบงค์กิ้ง เช่น ในรายงาน [35-38] ที่สามารถนำมาใช้เป็นแนวทางประกอบการพัฒนาความปลอดภัยให้กับบริการอินเทอร์เน็ตแบงค์กิ้งของธนาคารพาณิชย์ได้

ตารางที่ 1 การเปรียบเทียบวิธีการรักษาความปลอดภัยในการใช้บริการอินเทอร์เน็ตแบงค์กิ้งธนาคารพาณิชย์ไทยสำหรับลูกค้าบุคคล

วิธีการในการรักษาความปลอดภัยในการใช้งานอินเทอร์เน็ตแบงค์กิ้ง	กลุ่มธนาคารพาณิชย์ไทยที่ศึกษา					
	ธนาคารกรุงเทพ จำกัด (มหาชน)	ธนาคารกรุงไทย จำกัด (มหาชน)	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)	ธนาคารกสิกรไทย จำกัด (มหาชน)	ธนาคารทหารไทย จำกัด(มหาชน)	ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
1. SSL						
- การใช้โพรโทคอล HTTPS	✓	✓	✓	✓	✓	✓
- ขนาดของกุญแจเข้ารหัส	128 บิต	128 บิต	256 บิต	128 บิต	256 บิต	128 บิต
2. ใบรับรองดิจิตอล						
- CA ที่เป็นผู้ออกใบรับรอง	VeriSign	VeriSign	Entrust	Entrust	Entrust	Entrust
3. CAPTCHA						
- การใช้ CAPTCHA แบบอักษรข้อความในการเข้าสู่ระบบ	-	✓	-	-	-	-
4. บัญชีผู้ใช้และรหัสผ่าน						
- การใช้บัญชีผู้ใช้และรหัสผ่านเพื่อเข้าสู่ระบบ	✓	✓	✓	✓	✓	✓
5. OTP						
- การใช้ SMS OTP ประกอบการทำธุรกรรม	✓	✓	✓	✓	✓	✓
6. การพิสูจน์ทราบตัวตนด้วยสองปัจจัย						
- การใช้บัญชีผู้ใช้และรหัสผ่านในการพิสูจน์ตัวตนในการเข้าสู่ระบบและใช้ SMS OTP ในการพิสูจน์ตัวตนในการทำธุรกรรม	✓	✓	✓	✓	✓	✓

หมายเหตุ : ✓ หมายถึง มีการดำเนินการ และ - หมายถึง ไม่มีการดำเนินการ

ตารางที่ 2 ตัวอย่างปัญหา การโจมตีที่พบ และแนวทางการป้องกันที่เกิดขึ้นกับการรักษาความปลอดภัยในใช้งานอินเทอร์เน็ตแบงค์กิ้ง

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 - เลือกใช้รหัสผ่านที่คาดเดาได้ยากและเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ - 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

5. แนวทางในการป้องกันภัยในการใช้งานอินเทอร์เน็ตแบงค์กิ้งสำหรับลูกค้าบุคคล

เพื่อให้เกิดความมั่นใจในการใช้บริการและให้ผู้ใช้งานได้มีความระมัดระวังก็จะได้นำเสนอแนวทางในการป้องกันภัยในการใช้งานอินเทอร์เน็ตแบงค์กิ้ง ซึ่งได้ประมวลรวมข้อเสนอแนะในการใช้งานที่ได้จากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) และจากข้อแนะนำในการใช้งานของแต่ละธนาคารมานำเสนอดังต่อไปนี้

(1) หลีกเลี่ยงการใช้คอมพิวเตอร์ร่วมกับผู้อื่น เช่น ในร้านอินเทอร์เน็ต เพราะอาจไม่มีระบบความปลอดภัยที่ดีพอ แต่ถ้าหากจำเป็นต้องใช้ก็ควรลบ internet temporary files และ history ออกให้หมดหลังการใช้งาน

(2) หลีกเลี่ยงการทำธุรกรรมทางการเงินด้วยอุปกรณ์ที่ผ่านการดัดแปลงระบบปฏิบัติการ (jailbreak)

(3) หลีกเลี่ยงการใช้ Wi-Fi ที่ไม่รู้จักหรือไม่มั่นใจ

(4) ติดตั้งโปรแกรม antivirus และอัพเดทสม่ำเสมอ

(5) อัพเดทเว็บบราวเซอร์ ทุกครั้งเมื่อมี version ใหม่ออกมา ซึ่งส่วนใหญ่จะครอบคลุมถึงการรักษาความปลอดภัยในรูปแบบใหม่มาให้ด้วย รวมถึงหลีกเลี่ยงการใช้เว็บบราวเซอร์ที่ไม่สามารถตรวจสอบใบรับรองดิจิตอลได้

(6) หลีกเลี่ยงการดาวน์โหลด ติดตั้งโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ หรือเปิดไฟล์แนบที่มากับอีเมล์ที่ไม่รู้ที่มา

(7) ควรพิมพ์ address (URL) เว็บไซต์ธนาคารด้วยตัวเองทุกครั้ง และไม่ควรใช้ link ที่แนบมากับอีเมล์

(8) ควรจะตรวจสอบระบบรักษาความปลอดภัยของเว็บบราวเซอร์ว่ากำลังทำงานหรือไม่ โดยดูจากไอคอนเป็นรูปกุญแจปิด ซึ่งหมายความว่าข้อมูลกำลังได้รับการเข้ารหัส

(9) ไม่ควรใช้บัญชีผู้ใช้ที่เป็น admin ของระบบปฏิบัติการ ในการทำธุรกรรม เพราะหากเกิดการติดโปรแกรมไวรัสหรือโทรจัน จะมีความเสี่ยงที่เครื่องคอมพิวเตอร์อาจเสียหาย ได้มากกว่าการใช้ บัญชีผู้ใช้ธรรมดา

(10) หลีกเลี่ยงการใช้ระบบช่วยจำบัญชีผู้ใช้และรหัสผ่าน ในเว็บบราวเซอร์

(11) หลีกเลี่ยงการใช้บัญชีผู้ใช้และรหัสผ่านของบริการอินเทอร์เน็ตแบงค์กิ้งที่เหมือนกับบัญชีผู้ใช้และรหัสผ่านของบริการผ่านอินเทอร์เน็ตอื่น ๆ เช่น บริการซื้อขายสินค้าผ่านอินเทอร์เน็ต

(12) ควรเปลี่ยนรหัสผ่าน อย่างสม่ำเสมอ และกำหนดรหัสผ่าน โดยใช้คำหรือรหัสที่คาดเดาได้ยาก ซึ่งมีข้อแนะนำในการกำหนดรหัสผ่าน ดังนี้

(12.1) เป็นคำหรือรหัสผ่านที่ไม่ปรากฏในเอกสารหรือเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

(12.2) ง่ายต่อการจดจำ เพื่อที่จะได้ไม่ต้องบันทึกไว้

(12.3) ควรจะประกอบด้วยตัวอักษร ตัวเลข และสัญลักษณ์พิเศษ

(12.4) ไม่ควรเป็นคำที่ง่ายต่อการคาดเดา เช่น ชื่อ นามสกุลตนเอง หรือสมาชิกในครอบครัว ยี่ห้อรถยนต์ หรือข้อมูลส่วนตัว เช่น หมายเลขบัตรประชาชน

(13) หากผู้ใช้บริการกรอกข้อมูลในเว็บไซต์ปลอม ให้รีบติดต่อธนาคารเพื่อเปลี่ยนรหัสผ่านหรืออายัดบัญชี

(14) หากได้รับ SMS OTP ผ่านโทรศัพท์พกพา ต้องอ่านข้อความให้ครบถ้วนว่าเป็นรายการที่ต้องการ

ทำธุรกรรมหรือไม่ หากไม่ใช่อย่าได้ใช้ SMS OTP ที่ได้รับมาโดยเด็ดขาด ให้หยุดทำธุรกรรมและติดต่อธนาคารโดยด่วน

(15) ทุกครั้งที่ทำรายการเพิ่มบัญชีบุคคลอื่น ควรจะต้องตรวจสอบ เลขที่บัญชี ซึ่งปรากฏในอีเมล์ ที่ระบบส่งไปยืนยันการเพิ่มบัญชีในครั้งนั้น เพื่อให้แน่ใจว่าเป็นหมายเลขบัญชีที่ต้องการ ก่อนที่จะโอนเงินไปยังบัญชีนั้น เนื่องจากหากมีโปรแกรมโทรจัน แอบฝังตัวอยู่บนเครื่องคอมพิวเตอร์ โปรแกรมนั้นอาจจะเปลี่ยนแปลงเลขที่บัญชีก่อนส่งข้อมูลมาให้ระบบของธนาคารโดยที่ไม่รู้ตัวได้

(16) ควรตรวจสอบความถูกต้องของการทำรายการ และตรวจสอบการเคลื่อนไหวในบัญชีอย่างสม่ำเสมอ หากพบสิ่งผิดปกติ ต้องแจ้งธนาคารทันที

(17) เมื่อพบเว็บไซต์ปลอมของธนาคารให้รีบแจ้งไปยังธนาคาร โดยเร็วที่สุด

(18) ทุกธนาคารไม่มีนโยบายที่จะสอบถามรหัสลับแรกเข้า หรือรหัสผ่านส่วนตัว ซึ่งผู้ใช้บริการจะต้องเก็บรักษาข้อมูลส่วนตัวดังกล่าวไว้เป็นความลับ

(19) เมื่อเข้าสู่ระบบแล้วไม่ควรเปิดหน้าจอคอมพิวเตอร์ค้างไว้ในกรณีที่ไม่ใช้งาน และคลิกออกจากระบบในทุกครั้งที่ต้องการออกจากบริการ และไม่เปิดหน้าจอคอมพิวเตอร์ทิ้งไว้ จนกว่าทำรายการเสร็จ

(20) แจ้งธนาคารทันทีที่ผู้ใช้บริการมีปัญหาการใช้งาน และปฏิบัติตามคำแนะนำเพิ่มเติมจากเว็บไซต์ของธนาคารเมื่อมีการแจ้งเตือนในการใช้งานทุกครั้ง

6. สรุปการนำเสนอ

อินเทอร์เน็ตแบงค์กิ้งเป็นบริการทางการเงินผ่านทางเครือข่ายอินเทอร์เน็ตที่ธนาคารพาณิชย์ได้จัดเตรียมไว้เพื่อให้บริการแก่ลูกค้าของธนาคาร ซึ่งความปลอดภัยของบริการก็เป็นปัจจัยที่ส่งผลต่อการใช้งาน ดังนั้นจึงได้นำเสนอถึงวิธีการในการรักษาความปลอดภัยของบริการอินเทอร์เน็ตแบงค์กิ้งในกลุ่มลูกค้าบุคคล สำหรับธนาคารพาณิชย์ไทย โดยได้พิจารณาข้อมูลจากธนาคารพาณิชย์ที่มีการก่อตั้งในประเทศไทยและมีการดำเนินการยาวนานจำนวน 6 แห่ง ได้แก่ ธนาคารกรุงเทพ จำกัด (มหาชน) ธนาคารกรุงไทย จำกัด (มหาชน) ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) ธนาคารกสิกรไทย จำกัด (มหาชน) ธนาคารทหารไทย จำกัด (มหาชน) และธนาคารไทยพาณิชย์ จำกัด (มหาชน) สำหรับวิธีการในการรักษาความปลอดภัยที่ธนาคารพาณิชย์ไทยได้เลือกใช้นั้น ประกอบด้วย SSL ใบรับรองดิจิตอล CAPTCHA บัญชีผู้ใช้และรหัสผ่าน OTP และการพิสูจน์ทราบตัวตนด้วยสองปัจจัย โดยได้นำเสนอถึงวิธีการทำงาน ภัยคุกคาม และการป้องกันปัญหาของแต่ละวิธี ตลอดจนแนวทางในการปฏิบัติตนเพื่อให้ใช้บริการได้อย่างปลอดภัย

7. เอกสารอ้างอิง

[1] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, E-Banking คืออะไร ?, แหล่งที่มา : http://www.etda.or.th/etda_website/mains/display/1238, 26 กุมภาพันธ์ 2557.

[2] ธนาคารแห่งประเทศไทย, รายชื่อสถาบันการเงิน, แหล่งที่มา : http://www.bot.or.th/Thai/FinancialInstitutions/WebsiteFI/Pages/instList.aspx, 15 มกราคม 2557.

[3] จิวรัส อินทร์บำรุง, 2553, ส่วนประสมทางการตลาดและทัศนคติของผู้ใช้บริการอินเตอร์เนตแบงค์กิ้ง บมจ.ธนาคารกรุงไทย ในเขตอำเภอเมืองนครปฐม จังหวัดนครปฐม, วิทยานิพนธ์ปริญญาโท, มหาวิทยาลัยศิลปากร, นครปฐม, 119 น.

[4] รัตน์ธิดา พุฒตาล, ม.ป.ป., ปัจจัยที่ส่งผลต่อการตัดสินใจใช้บริการธนาคารอินเทอร์เน็ต (E-Banking) ของผู้บริโภค : กรณีศึกษาจังหวัดพระนครศรีอยุธยา, น.483-492, การประชุมวิชาการ มหาวิทยาลัยกรุงเทพ, กรุงเทพฯ.

[5] ปัญญา สุนทรปิยะพันธ์, 2552, พฤติกรรมการใช้งานอินเทอร์เน็ตแบงกิ้งของกลุ่มนักศึกษาระดับบัณฑิตศึกษา มหาวิทยาลัยธรรมศาสตร์ ท่าพระจันทร์, วิทยานิพนธ์ปริญญาโท, มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ, 137 น.

[6] Subsorn, P. and Limwiriyaku, S., 2011, A comparative analysis of the security of internet banking in Australia: A customer perspective, pp. 70-83, Proceedings of the 2nd International Cyber Resilience Conference.

[7] สมชาย ปราการเจริญ, 2553, ความมั่นคงปลอดภัยของคอมพิวเตอร์ Computer Security, ศูนย์ผลิตตำราเรียน มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ, กรุงเทพฯ, 239 น.

[8] จตุชัย แพงจันทร์, 2553, Master in Security 2nd Ed., ไอซีดี พรีเมียร์, นนทบุรี, 579 น.

[9] มณีรัตน์ ชาติรังสรรค์ และชัชพงศ์ ตั้งมณี, 2013, Effects of Typefaces, Numbers and Sets of Characters of text-based CAPTCHA on Human Affirmative Rates, แหล่งที่มา : http://tar.thailis.or.th/bitstream/123456789/572/1/Paper%20ID_68.pdf, 18 กุมภาพันธ์ 2557.

[10] สุทธิเกียรติ มีลาภ, 2557, การสำรวจระบบแคปท์ช่า, ว.วิทยาศาสตร์และเทคโนโลยี 22: 115-129.

[11] ธวัชชัย ชมศิริ, 2553, Computer and Network Security, โปรวิชั่น, กรุงเทพฯ, 310 น.

[12] พงศพัฒน์ หังสพฤกษ์, 2551, การพิสูจน์ตัวตนผู้ใช้ ณ จุดเดียวผ่านเว็บโดยปราศจากการปรับเปลี่ยนเครื่องผู้ใช้บริการ, วิทยานิพนธ์ปริญญาโท, มหาวิทยาลัยสงขลานครินทร์, สงขลา, 96 น.

[13] ปรัชญา ไชยเมือง, สมนึก พ่วงพรพิทักษ์ และวิรัตน์ พงษ์ศิริ, 2012, An Open-source E-Learning Extension for Authentication Security Enhancement and Password Recovery Solution, แหล่งที่มา : http://tar.thailis.or.th/bitstream/123456789/506/1/_PaperID_47_Camera%20ready.pdf, 18 กุมภาพันธ์ 2557.

[14] ACIS Professional Center, รายงานผลการวิจัยมาตรการรักษาความมั่นคงปลอดภัยระบบ Internet Banking และระบบ Mobile Banking ของธนาคารในประเทศไทยโดย ACIS Research LAB–Information Security Research on Thailand's Internet Banking/Mobile Banking, แหล่งที่มา : http://www.acisonline.net/article/?p=34, 18 กุมภาพันธ์ 2557.

[15] Soare, C.A., 2012, Internet banking two-factor authentication using smartphones, JMEDS 4: 12-18.

[16] Pouw, M. and van den Haak, E., 2014, Secure Sockets Layer Health Assessment, Available Source: http://work.delaat.net/rp/2013-2014/p27/report.pdf, 17 February 2014.

[17] อภิรักษ์ ทูลธรรม และสมนึก พ่วงพรพิทักษ์,

2013, The Evaluation of the SSL Stripping Attack Problem, คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม, มหาสารคาม.

[18] Nikiforakis, N., Younan, Y. and Joosen, W., 2010, HProxy: Client-side detection of SSL stripping attack, pp. 200-218, Proceedings of the 7th international conference on Detection of intrusions, malware, and vulnerability assessment.

[19] Shin, D. and Lopes, R., 2011, An empirical study of visual security cues to prevent the SSL stripping attack, pp. 287-296, Proceedings of the 27th Annual Computer Security Applications Conference.

[20] Hodges, J., Jackson, C. and Barth, A., 2012, Http strict transport security (hsts), Available Source: http://tools.ietf.org/html/draft-ietf-websec-strict-transport-sec-04, 17 February 2014.

[21] Sarkar, P.G. and Fitzgerald, S., 2013, Attacks on SSL a comprehensive study of BEAST, CRIME, TIME, BREACH, LUCKY 13 & RC4 BIASES, iSEC Partners, San Francisco.

[22] Leavitt, N., 2011, Internet Security under Attack: The Undermining of Digital Certificates, r12tec.indd.

[23] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2554, ระวังภัยแฮ็กเกอร์ออกใบรับรองปลอมของ Google, Yahoo!, Mozilla และอื่น ๆ, แหล่งที่มา : https://www.thaicert.or.th/alerts/user/2011/al2011us001.html, 18 กุมภาพันธ์ 2557.

[24] Abravanel, D.C., 2014, Malware Deployed by Fake Digital Certificates Bypassing Endpoint Security, Available Source: https://www.seculert.com/blog/2014/01/malware-deployed-by-fake-digital-certificates-bypassing-endpoint-security.html, February 26, 2014.

[25] Men, T., Zhang, X., Huang, G. and Sun, Y., 2012, A Dynamic CAPTCHA Based on Persistence of Vision, pp. 676-679, In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 1), IEEE.

[26] สุทธิเกียรติ มีลาภ และณัฐธนนท์ หงส์วริทธิ์ธร, 2013, Geometric and Math CAPTCHA, แหล่งที่มา : http://tar.thailis.or.th/bitstream/123456789/585/1/Paper%20ID_90.pdf, 18 กุมภาพันธ์ 2557.

[27] Hanacek, P., Malinka, K. and Schafer, J., 2010, E-banking security-A comparative study, Aerospace and Electronic Systems Magazine, IEEE 25: 29-34.

[28] จักรพงษ์ หลุย และศุภกร กังพิสดาร, 2013, Phishing Web-site Detection Based on Machine Learning, แหล่งที่มา : http://tar.thailis.or.th/bitstream/123456789/599/1/Paper%20ID_104.pdf, 18 กุมภาพันธ์ 2557.

[29] Sanglerdsinlapachai, N. and Rungsawang, A., 2010, Using domain top-page similarity feature in machine learning-based web phishing detection, pp. 187-190, In Knowledge Discovery and Data Mining 2010, WKDD'10, Third International Conference.

[30] ณรงค์ชัย นิมิตบุญอนันต์, 2542, Computer Security for E-Commerce, SUM Publishing Department, กรุงเทพฯ, 259 น.

[31] Mulliner, C., Borgaonkar, R., Stewin, P. and Seifert, J.P., 2013, SMS-based one-time passwords: Attacks and defense, pp. 150-159, In Detection of Intrusions and Malware and Vulnerability Assessment.

[32] Rahman, B.A., Azlina, N., Shajaratuddur Bt Harun, K. and Bt Yusof, Y., 2013, SMS banking transaction as an alternative for information, transfer and payment at merchant shops in Malaysia, pp. 1-6, In Information Technology and e-Services (ICITeS) 2013, 3rd International Conference.

[33] Yoo, C., Kang, B.T. and Kim, H.K., 2014, Case study of the vulnerability of OTP implemented in internet banking systems of South Korea, pp. 1-15, Multimedia Tools and Applications.

[34] Go, W., Lee, K. and Kwak, J., 2012, Construction of a secure two-factor user authentication system using fingerprint information and password, J. Intel. Manuf. 23: 1-14.

[35] Adham, M., Azodi, A., Desmedt, Y. and Karaolis, I., 2013, How to attack two-factor authentication internet banking, pp. 322-328, Proceedings of the 17th International Conference on Financial Cryptography and Data Security 2013, Lecture Notes in Computer Science Volume 7859.

[36] Gupta, S., Sahni, S., Sabbu, P., Varma, S. and Gangashetty, S.V., 2012, Passblot: A Highly Scalable Graphical One Time Password System, International Journal of Network Security & Its Applications, Volume 4, Number 2.

[37] Al Fairuz, M. and Renaud, K., 2010, Multi-channel, Multi-level Authentication for More Secure eBanking, In ISSA.

[38] Blocki, J., Blum, M. and Datta, A., 2013, GOTCHA password hackers !, pp 25-34, In Proceedings of the 2013 ACM workshop on Artificial intelligence and security.