อาชญากรรมคอมพิวเตอร์ : ศึกษากรณีปัจจัยที่มีผลต่อการเกิดอาชญากรรมบนระบบ electronic banking

Cyber crime : Case Study of Factors Affecting Electronic Banking

วุฒิชัย สุชรจิต[1], ผศ.ดร.ศิริลักษณ์ เกตุฉาย[2], ผศ. (พิเศษ) พล.ต.ท. ดร.ณรงค์ กุลนิเทศ[3]
[1] นักศึกษาระดับปริญญาโท สาขานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา
Email: wuttichai.su@gmail.com
[2] อาจารย์ที่ปรึกษางานวิจัย หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยราชภัฏสวนสุนันทา
Email: sirilak.ke@ssru.ac.th
[3] ประธานหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยราชภัฏสวนสุนันทา
Email: narong.kulnides@gmail.com

บทคัดย่อ

ปัจจุบันการใช้อินเทอร์เน็ตแพร่หลายมากขึ้น เนื่องจากการพัฒนาเทคโนโลยีและอุปกรณ์ทางด้านการสื่อสาร ทำให้อุปกรณ์ประเภท คอมพิวเตอร์ สมาร์โฟน หรืออุปกรณ์อิเล็กทรอนิกส์มีราคาที่ต่ำลง ประสิทธิภาพในการทำงานสูงขึ้น ซึ่งส่งผลให้ระบบการเงินอลัสถาบันการเงินของประเทศไทยต้องมีการปรับเปลี่ยนรูปแบบการให้บริการที่นำเทคโนโลยีมาช่วยอำนวยความสะดวก นอกเหนือจากการให้บริการตามสาขาของธนาคารเหมือนในอดีต จึงทำให้เกิดการพัฒนาระบบ Electronic Banking เพื่อช่วยอำนวยความสะดวกแก่ลูกค้าของแต่ละธนาคาร ในการทำธุรกรรมได้จากคอมพิวเตอร์ สมาร์ทโฟน แท็บเล็ต หรืออุปกรณ์อื่นที่รองรับ ซึ่งลูกค้าของธนาคารสามารถทำธุรกรรมได้ด้วยตัวเองจากทุกที่ที่ต้องการ

การเกิดขึ้นของระบบใหม่ย่อมเป็นผลดีต่อสังคมหรือคนส่วนมาก แต่มีคนบางกลุ่มที่มุ่งหาผลประโยชน์จากช่องโหว่ในระบบ Electronic Banking เพื่อทำให้เกิดความเสียหายต่อลูกค้าหรือผู้ใช้บริการของธนาคาร ซึ่งการกระทำดังกล่าวถือว่าเป็น "อาชญากรรมคอมพิวเตอร์" ที่ผู้กระทำผิดใช้ความรู้เกี่ยวกับเทคโนโลยีมาก่อให้เกิดภัยคุกคามต่อการระบบ Electronic Banking ด้วยวิธีต่างๆ แต่ยังมีปัจจัยอื่นๆ ที่อาจเข้ามาทำให้เกิดอาชญากรรมคอมพิวเตอร์กับการใช้งานระบบ Electronic Banking นอกเหนือจากการกระทำของผู้กระทำผิด

คำสำคัญ: อาชญากรรมคอมพิวเตอร์, ธนาคารอิเล็กทรอนิกส์, อินเทอร์เน็ต

Abstract

Nowadays, Internet is use widely area in Thailand. Because the development of communication technology e.g. personal computer, smartphone or electronic device is low price and higher performance. So that the financial institutions in Thailand just to be transform into a new service. They can use technology to make a convenience for customer in difference service. Then they are develop "Electronic Banking System" for our customer to make transaction from anywhere, anytime by electronic device such as Personal Computer, Smartphone, Tablet.

The new system is beneficial to social of Thailand. But there are some people who looking to exploit the weakness of “Electronic Banking System”. The action is called “Cybercriminal” use the knowledge of technology to post a threat to electronic banking system. However, in social there are other factors to affecting “Electronic Banking System”.

Keyword: Cyber Crime, Electronic Banking, Internet

บทนำ

ปัจจุบันเทคโนโลยีได้เข้ามามีบทบาทในการดำเนินชีวิตของคนในสังคมมากขึ้นอย่างต่อเนื่อง โดยเฉพาะกลุ่มคนในสังคมเมือง อย่างเช่น จังหวัดกรุงเทพมหานคร ซึ่งมีผู้คนเข้ามาอยู่ศัยและทำงานกันเป็นจำนวนมาก ทำให้แหล่งเงินทุนและเทคโนโลยีจากต่างชาติเข้ามาเป็นจำนวนมาก จากการคาดการณ์ของสถาบันวิจัยประชากรศาสตร์ มหาวิทยาลัยมหิดล คาดว่า ในปี พ.ศ. 2561 จังหวัดกรุงเทพมหานครจะประชากรอาศัยรวมกันประมาณ 8.2 ล้านคน ซึ่งรวมทั้งคนไทยและคนต่างชาติที่เข้ามาอาศัยหหรือทำงานในกรุงเทพมหานครด้วย ดังนั้นคนในสังคมเมืองจึงรับเอาวัฒนธรรมและเทคโนโลยีรูปแบบใหม่ๆ ตลอดเวลา เพื่อใช้ทั้งด้านการทำงานหรือการใช้ชีวิตในรูปแบบต่างๆ รวมทั้งเทคโนโลยีการติดต่อสื่อสารที่พัฒนาไปอย่างต่อเนื่อง ทำให้เกิดโครงข่ายการติดต่อสื่อสารมากมายหลายรูปแบบ อาทิ การติดต่อสื่อสารผ่านโทรศัพท์เคลื่อนที่ การใช้สัญญาณอินเทอร์เน็ตในการรับส่งข้อมูล

ในการรับส่งข้อมูลทั้งภาพ เสียง หรือข้อมูล นอกจากคอมพิวเตอร์ที่ใช้กันอย่างแพร่หลาย ปัจจุบันได้มีการพัฒนาอุปกรณ์รับข้อมูลเหล่านี้ขึ้นมาให้มีประสิทธิภาพมากขึ้น ขนาดและราคาลดลง เพื่อให้ตอนสนองต่อความต้องการของผู้ใช้งานได้มากขึ้น จนกลายเป็น “สมาร์ทโฟน” ที่สามารถใช้ติดต่อสื่อสารด้วยเสียง หรือจะใช้รับส่งข้อมูลผ่านอินเทอร์เน็ต ข้อมูลจากสำนักงานสถิติแห่งชาติ แสดงปริมาณร้อยละการใช้โทรศัพท์มือถือในปีพ.ศ. 2558 ร้อยละ 79.3 ปี พ.ศ. 2559 ร้อยละ 81.4 และในปี พ.ศ. 2560 เป็นร้อยละ 88.2 ของจำนวนประชากรทั้งประเทศ ซึ่งแสดงให้เห็นว่าในประเทศไทยมีการใช้โทรศัพท์มือถือเพิ่มมากขึ้นทุกปี อีกทั้งการพัฒนาโครงข่ายอินเทอร์เน็ตผ่านสัญญาณโทรศัพท์มือถือก็ครอบคลุมมากขึ้น ดังจะเห็นได้จากปริมาณการใช้ดาต้าผ่านโทรศัพท์เคลื่อนที่จาก 3 โอเปอร์เรเตอร์ (AIS, Dtac, Truemove-H) ปี พ.ศ. 2560 รวมกันประมาณ 3 ล้านเทราไบต์ ซึ่งเพิ่มขึ้นจากปริมาณการใช้ดาต้าของปี พ.ศ. 2557 6 เท่าตัว (หนังสือพิมพ์ฐานเศรษฐกิจ, 2560)

จากความนิยมใช้สมาร์ทโฟนที่มากขึ้น รวมทั้งประสทธิภาพของสาร์ทโฟนที่สูงขึ้นจากในอดีต จึงทำให้สมาร์ทโฟนมีฟังก์ชั่นการทำงานคล้ายกับเครื่องคอมพิวเตอร์เครื่องเล็กๆ เครื่องหนึ่ง จึงสามารถพัฒนาแอปพลิเคชันเพื่อรองรับการทำงานต่างๆ ได้มากขึ้น เพื่อช่วยอำนวยความสะดวกในการใช้งาน ซึ่งก็รวมทั้งกลุ่มธนาคารพาณิชย์และหน่วยงานภาครัฐที่เกี่ยวข้องทางด้านการเงิน อาทิเช่น ธนาคารแห่งประเทศไทย พัฒนาแอปพลิเคชันเพื่อรองรับการทำธุรกรรมทางด้านการเงินของแต่ละธนาคารบนสมาร์ทโฟน เพื่อเป็นการอำนวยความสะดวก รวดเร็วและปลอดภัย ให้กับลูกค้าของธนาคาร แต่ในอีกมุมมองการเกิดแอปพลิเคชันด้านการเงินอาจเป็นการเพิ่มช่องทางในการเกิดอาชญากรรมคอมพิวเตอร์ จึงจำเป็นต้องศึกษาสาเหตุการก่อเหตุและปัจจัยที่ส่งผลให้เกิดอาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องกับแอปพลิเคชันทางด้านการเงิน เพื่อทราบวิธีการก่อเหตุและหาแนวทางป้องกันอาชญากรรมคอมพิวเตอร์ที่จะเกิดขึ้น

Electronic Banking (e-Banking)

Electronic Banking (e-Banking) คือ การให้ข้อมูลหรือการทำธุรกรรมต่างๆ ของธนาคารที่จัดเตรียมไว้ให้กับลูกค้า เช่น การโอนเงิน การสอบถามยอดบัญชี การชำระค่าสินค้าหรือบริการ เป็นต้น ผ่านเครือข่ายอินเทอร์เน็ตหรือเชื่อมต่อผ่านเครือข่ายของโทรศัพท์เคลื่อนที่ที่ใช้สัญาณ เช่น 3G, 4G เพื่อให้ลูกค้าสามารถทำธุรกรรมได้ด้วยตนเอง ทำจากที่ใด เวลาใดก็ได้ตามที่ลูกค้าต้องการ ตามสิทธิ์ที่ได้กำหนดไว้กับเจ้าของบัญชี ซึ่งอาจมีการเรียกด้วยชื่ออื่นๆ เช่น Internet Banking (ธนาคารอินเทอร์เน็ต), Online Banking (ธนาคารออนไลน์), Cyber Banking (ธนาคารไซเบอร์) เป็นต้น ซึ่งโดยรวมแล้วมีความหมายเช่นเดียวกับคำว่า Electronic Banking โดยอาจแบ่งการเข้าใช้งานได้ดังนี้

1. คอมพิวเตอร์ส่วนบุคคล (Personal Computer) โดยใช้การเข้าถึงผ่าน Web browser ในการเข้าถึงข้อมูลบัญชีที่กำหนดไว้สำหรับแต่ละลูกค้า

2. เครื่องเบิกเงินสดอัตโนมัติ (automated teller machine, ATM) จัดเป็นอุปกรณ์คอมพิวเตอร์รูปแบบหนึ่งที่ใช้ในการสอบถามข้อมูลและยังทำธุรกรรมบางอย่างผ่านตัวเครื่องได้ เช่น การถอนเงินสด

3. สมาร์ต ดีไว (Smart Device) อุปกรณ์อิเล็กทรอนิกส์ที่สามารถเชื่อมต่อเครือข่ายอินเทอร์เน็ตเพื่อแลกเปลี่ยนข้อมูลผ่านแอปพลิเคชัน ซึ่งอาจแบ่งแยกหรือเรียกด้วยชื่ออื่นๆ เช่น สมาร์ตโฟน, แท็บเล็ต เป็นต้น

Mobile Banking เป็นการประยุกต์การให้บริการของ Electronic Banking มาพัฒนาให้สามารถใช้บนสมาร์ทโฟนหรืออุปกรณ์แท็บเล็ตได้สะดวกมากขึ้น ผ่านแอปพลิเคชันที่พัฒนาขึ้นมาโดยเฉพาะเพื่อรองรับการทำธุรกรรมของลูกค้าแต่ละรายที่สมัครใช้บริการ โดยลูกค้าสามารถทำธุรกรรมได้เองผ่านแอปพลิเคชัน เช่น การถอนเงิน การโอนเงิน การชำระค่าสินค้าหรือบริการ การตรวจสอบยอดเงินคงเหลือ เป็นต้น จากการรวบรวมข้อมูลของ ธนาคารแห่งประเทศไทย เกี่ยวกับปริมาณการทำธุรกรรมผ่าน Internet Banking และ Mobile Banking พบว่า เดือนธันวาคม พ.ศ. 2560 มีผู้ทำธุรกรรมผ่านทั้ง 2 รูปแบบ ประมาณ 170 ล้านรายการ เพิ่มขึ้นร้อยละ 77 จากเดือนธันวาคม พ.ศ. 2559 แสดงให้เห็นว่าการทำธุรกรรมผ่าน Electronic Banking ได้รับความนิยมเพิ่มขึ้น

อาชญากรรมคอมพิวเตอร์

เมื่อสังคมมีการเปลี่ยนแปลงอีกสิ่งหนึ่งมีการเปลี่ยนแปลงด้วยก็คือ การก่ออาชญากรรม ซึ่งการก่ออาชญากรรมในรูปแบบเดิมจะใช้การเข้าถึงหรือบุรุกทางกายภาพ เช่น การปล้นชิงทรัพย์ การทำร้ายร่างกาย เป็นต้น แต่เมื่อเทคโนโลยีเปลี่ยนแปลงไป ผู้ไม่ประสงค์ดีก็พัฒนาหรือศึกษารูปแบบเพื่อใช้ในการก่ออาชญากรรมโดยใช้คอมพิวเตอร์เป็นเครื่องมือเพิ่มมากขึ้น ดังนั้น อาชญากรรมคอมพิวเตอร์ จึงมีความหมายโดยสรุป คือการกระทำความผิดต่อกฎหมายของประเทศใดประเทศหนึ่ง เพื่อแสวงหาผลประโยชน์จากผู้อื่นหรือทำให้ผู้อื่นเสื่อมเสียชื่อเสียง และรวมทั้งทำให้ผู้อื่นได้รับอันตรายต่อร่างกายและจิตใจ โดยอาศัยเครือข่ายอินเทอร์เน็ตหรือเทคโนโลยีการสื่อสารสมัยใหม่ ผ่านคอมพิวเตอร์หรือสมาร์ทดีไว

อาชญากรรมคอมพิวเตอร์มีคำที่ใช้เรียกการกระทำฝ่าฝืนกฎหมายอาญาในลักษณะดังกล่าว เช่น Computer Crime, Cyber Crime, Online Crime เป็นต้น คำศัพท์เหล่านี้ล้วนมีความหมายเหมือนกัน ในภาษาไทยมีการเรียกลักษณะการกระทำดังกล่าวว่า "อาชญากรรมคอมพิวเตอร์" ซึ่งก่อให้เกิดความเสียหายทั้งทางด้านเศรษฐกิจและสังคม อาจแบ่งประเภทอาชญากรรมคอมพิวเตอร์ได้ ดังนี้

1. การขโมยข้อมูลสารสนเทศ (Information Theft) เป็นการขโมยข้อมูลส่วนบุคคล เช่น ข้อมูลบัตรเครดิต ข้อมูลบัตรประชาชน ฯ หรือข้อมูลขององค์กร เช่น ข้อมูลการขายสินค้า ข้อมูลลูกค้าของบริษัท ฯ เพื่อนำไปทำความเสียหายแก่บุคคลหรือองค์กรต่างๆ หรือเพื่อนำข้อมูลไปทำให้เกิดความได้เปรียบทางด้านการแข่งขันในธุรกิจ ซึ่งอาจเป็นการขโมยข้อมูลจากเครื่องคอมพิวเตอร์ หรือในเครือข่ายอินเตอร์ระหว่างการส่งข้อมูลไปยังปลายทาง

2. การเจาะระบบ (Hacking) การเข้าไปในระบบหรือเครือข่ายที่ตนเองไม่มีสิทธิ์หรือไม่ได้รับอนุญาติให้เข้าใช้งาน เพื่อเข้าไปคัดลอกข้อมูล ทำลายข้อมูลหรือระบบเพื่อให้เกิดความเสียหายต่อบุคคลหรือองค์กร ผู้เจาะระบบอาจดักจับข้อมูลการเข้าใช้ระบบได้จากการส่งจดหมายอิเล็กทรอนิกส์ การเข้าถึงแฟ้มหรือไฟล์ข้อมูลในระบบ

3. การใช้โปรแกรมทำความเสียหายต่อระบบ (Computer Virus) ซึ่งโปรแกรมจำพวกนี้มีหลายประเภท ซึ่งแต่ละประเภทจะมีลักษณะการทำงานและวัตถุประสงค์ที่แตกต่างกันไป เช่น

a. ไวรัสคอมพิวเตอร์ โปรแกรมที่เขียนขึ้นเพื่อตามจุดมุ่งหมายที่ต้องการ โดยส่วนมากจะเป็นลักษณะโปรแกรมที่ก่อกวนการทำงานของเครื่องคอมพิวเตอร์หรือผู้ใช้งาน

b. คอมพิวเตอร์เวิร์ม โปรแกรมลักณะคล้ายไวรัส แต่ใช้การแพร่กระจายผ่านเครือข่าย โดยเวิร์มจะคัดลอกตัวเองไปยังคอมพิวเตอร์ที่ไม่มีการป้องกัน แล้วเข้าไปทำความเสียหายกับระบบหรือข้อมูลที่มีอยู่ในเครื่องคอมพิวเตอร์นั้นๆ

c. ม้าโทรจัน โปรแกรมคอมพิวเตอร์ที่พัฒนาเพื่อลักลอบการเก็บข้อมูลของเครื่องคอมพิวเตอร์นั้นๆ เช่น ชื่อและรหัสผู้ใช้งาน ข้อมูลบัตรเครดิต หมายเลขบัญชีธนาคาร เป็นต้น

4. การหลอกลวงทางอินเทอร์เน็ต (Phishing) เป็นการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลของผู้ที่หลงเชื่อ โดยอาจส่งจดหมายอิเล็กทรอนิกส์ ด้วยข้อความที่น่าเชื่อถือเพื่อหลอกให้ผู้ใช้งานส่งข้อมูลให้ หรืออาจเป็นการสร้างเว็ปไซต์ปลอมขึ้นมาโดยให้ผู้ใช้กรอกข้อมูลและดักจับไว้สำหับใช้ในการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาติ

5. การใช้จดหมายอิเล็กทรนิกส์ขยะ (Spam e-mail) ซึ่งเป็นการส่งจดหมายอิเล็กทรอนิกส์เพื่อใช้ประชาสัมพันธ์หรือโฆษณาชวนเชื่อ หรือเป็นบริการส่งจดหมายอิเล็กทรอนิกส์ที่ผู้ใช้ไม่ได้ร้องขอหรือต้องการ

ภัยคุกคามที่เกิดขึ้นกับ Electronic Banking

สิ่งที่จำเป็นอย่างยิ่งสำหรับ Electronic Banking ในการสร้างความเชื่อมั่นในกับการทำธุรกรรมผ่านอินเทอร์เน็ตหรือแอปพลิเคชัน นั่นก็คือ ความปลอดภัยของข้อมูล ซึ่งถือได้ว่าเป็นหัวใจสำคัญของการพัฒนาระบบและการใช้งานต่อไปในระยะยาว ถ้าหากไม่มีการป้องกันอาจก่อให้เกิดความเสียหายทั้งทางด้านทรัพย์สิน ชื่อเสียงของธนาคาร และแรงจูงใจในการใช้บริการ Electronic Banking ประเภทของภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่ Electronic Banking มีดังนี้

1. วิศวกรรมสังคม (Social Engineering) เป็นการศิลปะการหลอกลวงโดยกระทำการเพื่อให้ได้มาซึ่งข้อมูลที่ผู้หลอกลวงต้องการ โดยอาศัยจุดอ่อนจากความไม่รู้ ความประมาทเลินเล่อ หรือการให้ข้อมูล(เท็จ)เพื่อให้ผู้ถูกหลอกหลงเชื่อ

2. การสแกนช่องทางการเชื่อมต่อ (Port Scanning) เป็นการใช้ซอฟแวร์สแกนหา port เชื่อมต่อสำหรับอุปกรณ์ที่อยู่ในเครือข่าย เพื่อรวบรวมข้อมูลจากการใช้งานของเครื่องเป้าหมาย

3. Packet Sniffers เป็นการดักจับข้อมูลระหว่างทางที่เกิดจากเครื่องลูกข่าย เช่น เครื่องคอมพิวเตอร์ สมาร์ทโฟน แล้วส่งข้อมูลออกไปยังเครือข่ายอินเทอร์เน็ต โดยมีปลายทางคือเครื่องแม่ข่าย

4. การเจาะรหัสผ่าน (Password Cracking) เป็นเทคนิคถอดรหัสรูปแบบหนึ่งที่พยายามสุ่มรหัสผ่านเพื่อเข้าใช้งานระบบนั้นๆ

5. โปรแกรมโทรจัน (Trojan Programs) โปรแกรมที่เข้ามายังเครื่องคอมพิวเตอร์หรือสมาร์ทโฟนผ่านทางเครือข่ายอินเทอร์เน็ต แล้วฝั่งตัวอยู่ในเครื่องโดยผู้ใช้ไม่รู้ตัวและทำงานอยู่เบื่องหลัง

เมื่อนำช่องโหว่ของเทคโนโลยี ความไม่ระมัดระวังหรือความรู้เท่าไม่ถึงการณ์มาเป็นเครื่องมือในการก่ออาชญากรรม ซึ่งปัจจุบันอาชญากรรมคอมพิวเตอร์ในประเทศไทยเกิดขึ้นหลากหลายรูปแบบ ทั้งที่กระทำด้วยบุคคลเพียงคนเดียวหรือร่วมกันทำเป็นกระบวนการก็ได้ อาชญากรรมคอมพิวเตอร์ที่จัดเป็นภัยคุกคามต่อการใช้งาน Electronic Banking สามารถสรุปประเภทของพฤติกรรมของการก่ออาชญากรรมที่เกี่ยวข้องกับระบบ Electronic Banking ได้ ดังนี้

1. การขโมยข้อมูลทางอินเทอร์เน็ต ไม่ว่าจะเป็นการดักจับข้อมูลบนเครือข่ายอินเทอร์เน็ตด้วยวิธีการใช้ Spam โปรแกรมโทรจัน การหลอกลวง (Phishing) ฯ เพื่อให้ได้มาซึ่งข้อมูลของบุคคลอื่นที่ตกเป็นเหยื่อ เช่น ข้อมูลบัตรเครดิต ข้อมูลบัญชีธาคาร แล้วนำข้อมูลเหล่านั้นไปกระทำการที่เป็นการละเมิดสิทธิ์ของเจ้าของข้อมูล

2. การปลอมแปลงรูปแบบ หรือเลียนแบบซอฟแวร์ โดยปลอมแปลงรูปแบบเว็ปไซต์หรือแอพพิเคชันให้เหมือนกันของทางธนาคาร เพื่อให้เหยื่อหลงเชื่อและมอบข้อมูลบางส่วน เช่น ชื่อและรหัสสำหรับเข้าสู่ระบบของทางธนาคาร

3. การล่อลวงให้หลงเชื่อด้วยวาทะศิลป์ เป็นการให้ข้อมูลหรือข้อกล่าวอ้างเพื่อจูงใจให้คนคล้อยตามเพื่อซื้อสินค้าหรือบริการที่ไม่มีอยู่จริง หรือไม่ตรงตามคำโฆษณากล่าวอ้างไว้ โดยใช้สื่อสังคม (Social Media) ผ่านเครือข่ายอินเทอร์เน็ตในการติดต่อหรือโฆษณาเชิญชวน ซึ่งปัจจุบันมีผู้คนเข้าใช้สื่อสังคมเป็นจำนวนและกว้างขวาง

4. การแอบอ้างเป็นบุคคลเป้าหมายเพื่อทำธุรกรรม เป็นการใช้เอกสารหรือข้อมูลปลอมในการติดต่อกับทางธนาคารหรือผู้ให้บริการโทรศัพท์เคลื่อนที่ โดยแอบอ้างเป็นบุคคลดังกล่าวเพื่อให้ได้มาซื้อข้อมูลในการทำธุรกรรมผ่านระบบ Internet Banking หรือ Mobile Banking

5. การฉ้อโกงเงิน มีลักษณะคล้ายการให้โอนเงินค่าสินค้าหรือบริการไปแล้ว แต่หลังจากนั้นผู้โอนหรือผู้สั่งซื้อกลับไม่ได้สินค้าตามที่ตกลงกันไว้ พบมากในกรณีการซื้อขายออนไลน์ที่เป็นการซื้อขายแบบ C2C (Customer to Customer) ซึ่งทำให้การตรวจสอบความถูกต้องของข้อมูลสินค้าและผู้ขายทำได้ยากหรือไม่สามารถตรวจสอบได้เลย

จากรูปแบบพฤติกรรมที่เป็นภัยคุกคามต่อการใช้งาน Electronic Banking ที่พบในประเทศไทย ข้อมูลจากสำหนักยุทธศาสตร์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พบว่าในปี พ.ศ. 2559 มีการเข้าแจ้งความ 1,020 กรณี คิดเป็นสัดส่วนที่เพิ่มขึ้นร้อยละ 26.86 จากช่วงก่อนปี พ.ศ. 2556 แสดงให้เห็นว่าการเกิดภัยคุกคามต่อระบบ Electronic Banking มีการเพิ่มขึ้นอย่างต่อเนื่อง และพัฒนารูปแบบการเกิดหรือการกระทำที่ก่อให้เกิดภัยคุกคามให้มีความซับซ้อนมากขึ้นตามเทคโนโลยีที่เปลี่ยนแปลงไป

ปัจจัยที่มีผลต่อการเกิดอาชญากรรม

จากปัญหาอาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องกับระบบ electronic Banking ที่เกิดขึ้นในปัจจุบัน มีวิธีการก่ออาชญากรรมที่หลากหลายมากขึ้น ทั้งในด้านที่เกี่ยวกับเทคโนโลยีที่อาจมีช่องว่างหรือวิธีการต่างๆ ที่ยังไม่มีระบบรักษาความปลอดภัยที่ป้องกันปัญหาดังกล่าวได้ เช่น ผู้ใช้บริการ Electronic Banking ได้รับ email หรือ SMS ในการแจ้งให้ลงทะเบียนเพื่อยืนยันข้อมูล ซึ่งแท้ที่จริงแล้วเป็น email หรือ SMS ปลอมจาก

คนร้ายที่ต้องการข้อมูลของผู้ใช้บริการ จึงทำให้ผู้ใช้งาน electronic Banking หลงเชื่อและให้ข้อมูลจริงแก่คนร้ายโดยไม่ทันรู้ตัว หรืออาชญากรรมที่อาศัยการหลอกล่อด้วยคำพูดหรือเทคนิคต่างๆ เพื่อให้ผู้เสียหายโกงเงินหรือมอบข้อมูลส่วนตัวให้แก่คนร้าย ซึ่งปัญหาเหล่านี้สามารถพบเห็นได้ตลอดตามหน้าหนังสือพิมพ์หรือข่าวบนหน้าเว็บไซต์ ที่มีผู้เสียหายหลายรายเข้าแจ้งความเพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องดำเนินการหาตัวคนร้ายและทรัพย์สินที่สูญไปกลับคืนมา โดยเหตุการณ์ต่างๆ ที่เกิดขึ้นจริงนั้นสามารถสรุปเป็นปัจจัยที่มีผลต่อการเกิดอาชญากรรมบนระบบ Electronic Banking ได้ ดังนี้

1. ช่องโหว่ของการใช้งานระบบหรือเทคโนโลยี เป็นการใช้ช่องโหว่ของกระบวนการยืนยันตัวบุคคลการเข้าใช้ระบบ หรือช่องโหว่ของเทคโนโลยีเองที่ไม่สามารถป้องกันการเกิดอาชญากรรมได้

2. ความรู้/ความเข้าใจ เกี่ยวกับอุปกรณ์คอมพิวเตอร์ สมาร์ทโฟน หรืออุปกรณ์อิเล็กทรอนิกอื่นๆ รวมทั้งความเข้าใจถึงขั้นตอนการทำงานของระบบ Electronic Banking เนื่องจากจะช่วยในการตรวจสอบความถูกต้องของข้อมูลทั้งก่อน ระหว่างและหลังการทำธุรกรรมผ่านระบบ Electronic Banking

3. การรวบรวมพยานหลักฐานเพื่อฟ้องร้องดำเนินคดี จากกรณีที่เกิดการฉ้อโกงหรือการดักข้อมูลจากการทำธุรกรรมจากระบบ Electronic Banking ซึ่งมีผู้เสียหายจำนวนหนึ่งที่สามารถรวบรวมพยามหลักฐานในการถูกฉ้อโกงหรือถูกทำให้เสียหายไว้ได้ แต่ก็ยังมีกลุ่มคนอีกกลุ่มที่เมื่อถูกหลอกลวงแล้ว ไม่ทราบว่าจะต้องรวบรวมข้อมูลหรือพยามหลักฐานอย่างไร จึงทำให้สถิติที่หน่วยงานที่เกี่ยวข้องรวบรวมไว้อาจยังไม่ถูกต้องนัก

4. เจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้อง มีไม่เพียงพอต่อการทำงานหรือการสืบสวนสอบสวน ซึ่งการเกิดคดีที่เกี่ยวข้องกับระบบ Electronic Banking หรือคอมพิวเตอร์ปัจจุบันยังคงมีเพียงหน่วยงานในส่วนกลางเป็นหลัก จึงทำให้คดีความลักษณะนี้แต่เกิดตามภูมิภาคต่างๆ ของประเทศมีความลำบากในการแจ้งความดำเนินคดี

5. อาชญากรรมไร้พรหมแดน คือการก่ออาชญากรรมในประเทศไทยแต่ผู้กระทำผิดไม่จำเป็นต้องอยู่ในประเทศไทยก็ได้ เนื่องการใช้งานระบบ Electronic Banking เป็นการใช้งานผ่านเครือข่ายอินเทอร์เน็ตหรือเครือข่ายโทรศัพท์เคลื่อนที่ ทำให้หาตัวผู้กระทำความผิดได้

บทสรุป

อาชญากรรมคอมพิวเตอร์ ถือเป็นภัยคุกคามสำคัญต่อการใช้ระบบ Electronic Banking เป็นอย่างมาก เพราะนอกจากจะสร้างความเสียหายด้านทรัพย์สิน เช่น การหลอกให้โอนเงิน การเข้าสู่ระบบ Electronic Banking แล้วโอนเงินออกจากบัญชีผู้เสียหาย การหลอกขายสินค้าหรือบริการ เป็นต้น และยังสร้างความเสียหายต่อความน่าเชื่อถือของการใช้ระบบ Electronic Banking หรือความน่าเชื่อถือของธนาคาร รวมทั้งความมั่นใจของผู้ใช้บริการ Electronic Banking เนื่องจากหัวใจสำคัญของสถาบันการเงินก็คือ ความน่าเชื่อถือและความไว้วางใจของผู้ใช้บริการหรือลูกค้า แต่อาจถูกทำลายด้วยบุคคลบางกลุ่มที่มุ่งหวังประโยชน์ส่วนตัวประกอบกับมีความรู้เกี่ยวกับเทคโนโลยี ทำการใช้ช่องโหว่ของเทคโนโลยี เช่น การเจาะระบบ การดักจับข้อมูในเครือข่ายอินเทอร์เน็ต การโจมตีคอมพิวเตอร์ด้วยไวรัส, หนอน, ม้าโทรจัน การหลอกลวงผ่านจดหมายอิเล็กทรอนิกส์ (Phishing) หรือจดหมายอิเล็กทรอนิกส์ขยะ (Spam) เพื่อให้ได้มาซึ่งข้อมูลสำหรับนำไปต่ออาชญากรรมต่อไป

จากการศึกษาปัจจัยที่ส่งผลต่อการก่ออาชญากรรมคอมพิวเตอร์จากการใช้ Electronic Banking ที่กล่าวมาแล้ว สามารถนำมาประยุกต์ใช้ได้ ดังนี้

1. เพื่อให้ความรู้และป้องกันเกี่ยวกับการเกิดอาชญากรรมคอมพิวเตอร์จากการใช้ระบบ Electronic Banking

2. เพื่อแสดงให้เห็นถึงจุดแข็ง/จุดอ่อนของการก่ออาชญากรรมคอมพิวเตอร์จากการใช้ระบบ Electronic Banking สำหรับใช้ในการพัฒนาการป้องกันอาชญากรรมคอมพิวเตอร์

3. เพื่อใช้เป็นข้อมูลในการจัดกลุ่มการเกิดอาชญากรรมคอมพิวเตอร์ และหาวิธีการหรือแนวทางในการป้องกันการก่อเหตุ

ดังนั้น ผู้ใช้บริการ Electronic Banking รวมทั้งผู้ใช้งานระบบคอมพิวเตอร์ต่างๆ ควรจะให้ความสำคัญกับการเกิดอาชญากรรมคอมพิวเตอร์ให้มากขึ้น โดยไม่คาดคิดว่าเหตุการณ์ตามข่าวในปัจจุบันจะไม่เกิดขึ้นกับตัวเอง ซึ่งการเกิดอาชญากรรมคอมพิวเตอร์สามารถเกิดขึ้นได้กับทุกคนที่ใช้ระบบคอมพิวเตอร์ เพื่อเป็นการตระหนักรู้และป้องกันการเกิดอาชญากรรมคอมพิวเตอร์

รายการอ้างอิง

สำหนักยุทธศาสตร์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์(องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2560). รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2560 . สืบค้นเมื่อ มิถุนายน 2, 2561, จาก https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2017.html.

สำนักงานคณะกรรมการนโยบายวิทยาศาสตร์ เทคโนโลยีและนวัตกรรมแห่งชาติ. (2560). แนวโน้มการใช้โทรศัพท์พื้นฐาน โทรศัพท์เคลื่อนที่ และอินเทอร์เน็ตในประเทศไทย ปี 2553 – 2560. สืบค้นเมื่อ มิถุนายน 2, 2561, จาก http://stiic.sti.or.th/stat/ind-it/it-t003/.

กสทช. เผยสถิติการใช้มือถือไทย ปี 2560 ใช้เน็ตมือถือกระหน่ำ 3 ล้านเทราไบต์. (เมษายน 09, 2561). Retrieved from https://www.it24hrs.com/2018/smartphone-thailand-3g-4g-static-data/.

ธนาคารแห่งประเทศไทย. ธุรกรรมการชำระเงินผ่านบริการ Mobile banking และ Internet banking. (พฤษภาคม 31, 2561). Retrieved from http://www2.bot.or.th/statistics/ReportPage.aspx

องอาจ เทียนหิรัญ. (2546). อาชญากรรมทางคอมพิวเตอร์ : การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์. นิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

Michael Aaron Dennis. Cybercrime. Retrieved from https://www.britannica.com/topic/cybercrime

ประพัทธ์โชต งามขำ. (2548). องค์กรภาคเอกชนกับการแก้ไขปัญหาอาชญากรรมทางเศรษฐกิจ ศึกษากรณี : อาชญากรรมคอมพิวเตอร์. วิทยาลัยการยุติธรรม สำนักงานศาลยุติธรรม.

สถิติภัยคุกคาม ประจำปี พ.ศ. 2560. (มกราคม, 2561). Retrieved from https://www.thaicert.or.th/statistics/statistics.html

อาชญากรรมไซเบอร์พุ่ง เหรียญอีกด้านยุคดิจิตอล. (28 มีนาคม, 2560). Retrieved from http://www.thansettakij.com/content/136878

ประชากรของประเทศไทย พ.ศ. 2561. สารประชากรมหาวิทยาลัยมหิดล. (มกราคม, 2561). Retrieved from http://www.ipsr.mahidol.ac.th/ipsrbeta/th/Gazette.aspx

วิวัฒนาการโทรศัพท์มือถือ กว่า 20 ปี. (01 พฤศจิกายน, 2555). Retrieved from https://www.it24hrs.com/2012/mobile-evolution-20-years-ago/

E-BANKING คืออะไร?. (02 พฤศจิกายน, 2555). สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). Retrieved from https://standard.etda.or.th/?p=219

ปัญญา สุนทรปิยะพันธ์. (2552).พฤติกรรมการใช้งานอินเทอร์เน็ตแบงกิ้งของกลุ่มนักศึกษาระดับบัณฑิตศึกษา มหาวิทยาลัยธรรมศาสตร์ ท่าพระจันทร์. วิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริการเทคโนโลยี วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์.

Bismark Addai. (2015). Electronic Banking and Customer Satisfaction: Empirical Evidence from Ghana. British Journal of Economics, Management & Trade, 9(3), 1-8. Retrieved from https://www.researchgate.net/publication/282468257_Electronic_Banking_and_Customer_Satisfaction_Empirical_Evidence_from_Ghana

Lukic, Aleksandar. (2015). Benefits and Security Threats in Electronic Banking. International Journal of Managerial Studies and Research, 3(6), 44.-47. Retrieved from https://www.arcjournals.org/pdfs/ijmsr/v3-i6/7.pdf

Aghatise, J. (2006, June). Cybercrime definition. Retrieved from https://www.researchgate.net/publication/265350281_Cybercrime_definition

สุพล พรหมมาพันธุ์. (2014). อาชญากรรมคอมพิวเตอร์ : ภัยคุกคามแห่งศตวรรษที่ 21. Royal Thai Air Force Medical Gazette, 60(3), 57.-66. Retrieved from https://www.spu.ac.th/informatics/files/2015/03/3.pdf

Author, A. (Publication Year). Highlighting the Vulnerabilities of Online Banking System. Journal of Internet Banking and Commerce, Volume(Issue Retrieved from journal http://www.icommercecentral.com/open-access/highlighting-the-vulnerabilities-of-online-banking-system.php?aid=61518

สำนักงานสถิติแห่งชาติ. การสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2560. (2561). Retrieved from http://www.nso.go.th/sites/2014/DocLib13/ด้านICT/เทคโนโลยีในครัวเรือน/2560/