ทำธุรกรรมทางการเงินผ่าน Smartphone อย่างไร ให้ปลอดภัย

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ทำธุรกรรมทางการเงินผ่าน Smartphone อย่างไร ให้ปลอดภัย

เรียบเรียงและเผยแพร่โดย สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา อาคารรัฐประศาสนภักดี ชั้น ๖
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๘๕ - ๙๙
โทรสาร ๐ ๒๑๔๓ ๘๐๓๖ - ๓๗
เว็บไซต์กระทรวง : http://www.mict.go.th
เว็บไซต์สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ :
http://www.etcommission.go.th

คำนำ

หนังสือ **"ทำธุรกรรมทางการเงินผ่าน Smartphone อย่างไร ให้ปลอดภัย"** จัดทำขึ้น เพื่อเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการทำธุรกรรมทางการเงินผ่านสมาร์ตโฟน (Smartphone) ที่ปลอดภัย และสามารถรับมือกับภัยเทคโนโลยีสารสนเทศที่จะมาคุกคามได้ ส่งผลให้ประชาชนเกิดความเชื่อมั่น และมีการทำธุรกรรมทางการเงินผ่านสมาร์ตโฟนเพิ่มมากขึ้น

คณะผู้จัดทำหวังว่าหนังสือเล่มนี้จะเป็นประโยชน์สำหรับผู้อ่าน และช่วยให้ทุกท่าน สามารถทำธุรกรรมทางการเงินผ่านสมาร์ตโฟนได้อย่างปลอดภัยมากยิ่งขึ้น

คณะผู้จัดทำ
มีนาคม ๒๕๕๘

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

บทที่ ๑
สถานภาพการชำระเงินทางอิเล็กทรอนิกส์ (e - Payment) ของประเทศไทย

กรอบนโยบาย ICT 2020 กับการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (e - Transaction)

ในปัจจุบันประเทศไทยได้นำเทคโนโลยีสารสนเทศและการสื่อสารมาเป็นกลไกหลักที่สำคัญในการขับเคลื่อนเศรษฐกิจและสังคมของประเทศ โดยเฉพาะอย่างยิ่งการนำธุรกรรมทางอิเล็กทรอนิกส์มาเป็นส่วนหนึ่งในการเพิ่มปริมาณและมูลค่าทางเศรษฐกิจ ตลอดจนยกระดับคุณภาพชีวิตของประชาชน ซึ่งเป็นอีกหนึ่งบทบาทของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารที่เป็นองค์กรหลักในการบริหารจัดการเทคโนโลยีสารสนเทศและการสื่อสารของประเทศเพื่อการพัฒนาที่ยั่งยืน ทั้งนี้ ได้มีการกำหนดกรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสารในระยะ ๑๐ ปี ตั้งแต่ พ.ศ. ๒๕๕๔ - ๒๕๖๓ หรือเรียกว่า ICT 2020 โดยพัฒนามาจากแนวคิดของ IT 2010 ซึ่งตั้งอยู่บนหลักการสำคัญของการพัฒนาทั้งในเชิงปริมาณ คุณภาพ และความเป็นธรรมในสังคม การใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสารในการลดความเหลื่อมล้ำและสร้างโอกาสให้กับประชาชนในการได้รับประโยชน์จากการพัฒนาอย่างเท่าเทียม โดยมีแนวทางการดำเนินงานที่สำคัญที่มีความเกี่ยวข้องกับการส่งเสริมและสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ ได้แก่ การพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เป็นอินเทอร์เน็ต (Internet) ความเร็วสูง หรือการสื่อสารรูปแบบอื่นที่เป็นโครงข่ายความเร็วสูงให้มีความทันสมัย มีการกระจายอย่างทั่วถึง และมีความมั่นคงปลอดภัย สามารถรองรับความต้องการของทุกภาคส่วนได้อย่างมีประสิทธิภาพ เพื่อสร้างความเชื่อมั่นให้กับภาครัฐ ภาคธุรกิจและประชาชนในการติดต่อสื่อสาร ตลอดจนการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งรวมถึงการจัดให้มีกฎหมาย กฎ ระเบียบที่มีความทันสมัยและทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศ สนับสนุนการเพิ่มประสิทธิภาพและความปลอดภัยของระบบการชำระเงินทางอิเล็กทรอนิกส์ (e - Payment Gateway) เพื่อรองรับการก้าวสู่ประชาคมเศรษฐกิจอาเซียน โดยมีข้อกำหนดในการดำเนินการที่เกี่ยวกับระบบการชำระเงินหรือการโอนเงินทางอิเล็กทรอนิกส์ระหว่างประเทศด้วย

สถานภาพการชำระเงินทางอิเล็กทรอนิกส์ของประเทศไทย

ความก้าวหน้าด้านเทคโนโลยีสารสนเทศ การเปิดรับเทคโนโลยีของผู้ใช้บริการ รวมถึงความเชื่อมโยงและความซับซ้อนของระบบเศรษฐกิจ เป็นปัจจัยแวดล้อมที่มีผลต่อพัฒนาการของระบบการชำระเงินทางอิเล็กทรอนิกส์ ซึ่งการชำระเงินทางอิเล็กทรอนิกส์เป็นการโอนสิทธิการถือครองเงิน หรือการโอนสิทธิการถอนเงินหรือหักเงินจากบัญชีเงินฝากของผู้ใช้บริการที่เปิดไว้กับผู้ให้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน (ตามมาตรา ๓ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑) เพื่อให้ผู้ใช้บริการสามารถใช้งานได้โดยง่าย ไม่ยุ่งยากซับซ้อน ลดระยะเวลา ลดต้นทุน ตลอดจนลดความเสี่ยงในการดำเนินการได้ ตัวอย่างของการชำระเงินทางอิเล็กทรอนิกส์ผ่านช่องทางใหม่อันเป็นผลมาจากการพัฒนาด้านอินเทอร์เน็ตและเครื่องมือสื่อสาร เช่น ธนาคารทางอินเทอร์เน็ต (Internet Banking) ธนาคารทางโทรศัพท์เคลื่อนที่ (Mobile Banking) บริการเงินอิเล็กทรอนิกส์ (e - Money) ทำให้ผู้ใช้บริการได้รับความสะดวกรวดเร็วมากขึ้น ในปัจจุบันหน่วยงานภาครัฐ ภาคธุรกิจ และประชาชนนิยมใช้บริการการชำระเงินทางอิเล็กทรอนิกส์เพิ่มมากขึ้น ดังจะเห็นได้จากข้อมูลที่ธนาคารแห่งประเทศไทยรวบรวมไว้


ตารางที่ ๑-๑ ปริมาณการชำระเงินผ่านระบบการชำระเงินและช่องทางต่างๆ ตั้งแต่ พ.ศ. ๒๕๕๓ - ๒๕๕๗ (หน่วย : พันรายการ)

รายการ	๒๕๕๗	๒๕๕๖	๒๕๕๕	๒๕๕๔	๒๕๕๓
ปริมาณการชำระเงินทางอิเล็กทรอนิกส์ (รวมทั้งหมด)	**๒,๒๘๓,๙๔๔**	**๒,๐๒๖,๔๓๘**	**๑,๗๒๙,๓๗๔**	**๑,๓๘๐,๑๔๖**	**๑,๑๒๕,๘๘๐**
เงินอิเล็กทรอนิกส์	๗๘๗,๙๓๒	๖๖๙,๒๑๑	๕๑๒,๐๘๕	๓๔๘,๒๐๖	๒๒๑,๔๕๙
การโอนเงินภายในธนาคาร (รวมชำระค่าสินค้าบริการ)	๕๒๐,๕๘๖	๔๕๑,๒๒๘	๓๙๑,๗๐๔	๓๑๐,๑๙๗	๒๖๓,๓๙๗
การชำระเงินด้วยบัตรพลาสติก (Payment Cards)	๔๓๒,๖๕๗	๔๐๐,๔๐๕	๓๖๔,๔๕๘	๓๑๓,๑๖๗	๒๗๑,๐๒๔
การโอนเงินครั้งละหลายรายการ (Bulk Payment)	๓๓๙,๙๑๑	๓๒๘,๖๓๑	๓๑๖,๓๔๓	๒๘๑,๒๐๗	๒๕๘,๒๘๘
การโอนเงินรายย่อยข้ามธนาคาร (Online Retail Funds Transfer : ORFT)	๑๙๙,๖๓๓	๑๗๓,๙๐๙	๑๕๐,๔๔๐	๑๒๔,๘๓๒	๑๐๙,๕๕๖
การโอนเงินเพื่อลูกค้าผ่าน BAHTNET (BAHTNET - 3rd Party)	๓,๒๒๔	๓,๐๕๔	๒,๗๕๖	๒,๕๓๗	๒,๑๕๖

จากตารางที่ ๑-๑ จะเห็นว่าปริมาณการชำระเงินทางอิเล็กทรอนิกส์มีปริมาณสูงขึ้นอย่างต่อเนื่องทุกปี ตั้งแต่ พ.ศ. ๒๕๕๓ - ๒๕๕๗ โดยมีปริมาณการชำระเงินทางอิเล็กทรอนิกส์ ดังนี้

ปี ๒๕๕๓ มีปริมาณการชำระเงินทางอิเล็กทรอนิกส์ ๑,๑๒๕,๘๘๐ พันรายการ
ปี ๒๕๕๔ มีปริมาณการชำระเงินทางอิเล็กทรอนิกส์ ๑,๓๘๐,๑๔๖ พันรายการ
ปี ๒๕๕๕ มีปริมาณการชำระเงินทางอิเล็กทรอนิกส์ ๑,๗๒๙,๓๗๔ พันรายการ
ปี ๒๕๕๖ มีปริมาณการชำระเงินทางอิเล็กทรอนิกส์ ๒,๐๒๖,๔๓๘ พันรายการ
ปี ๒๕๕๗ มีปริมาณการชำระเงินทางอิเล็กทรอนิกส์ ๒,๒๘๓,๙๔๔ พันรายการ

ในปี ๒๕๕๗ พบว่ามีปริมาณการชำระเงินทางอิเล็กทรอนิกส์ผ่านระบบการชำระเงินและช่องทางต่างๆ โดยเรียงลำดับจากมากไปหาน้อยได้ดังนี้ ๑) เงินอิเล็กทรอนิกส์ ๒) การโอนเงินภายในธนาคาร (รวมชำระค่าสินค้าบริการ) ๓) การชำระเงินด้วยบัตรพลาสติก ๔) การโอนเงินครั้งละหลายรายการ ๕) การโอนเงินรายย่อยข้ามธนาคาร และ ๖) การโอนเงินเพื่อลูกค้าผ่าน BAHTNET

ตารางที่ ๑-๒ มูลค่าการชำระเงินผ่านระบบการชำระเงินและช่องทางต่างๆ ตั้งแต่ พ.ศ. ๒๕๕๓ - ๒๕๕๗ (หน่วย : พันล้านบาท)

รายการ	๒๕๕๗	๒๕๕๖	๒๕๕๕	๒๕๕๔	๒๕๕๓
มูลค่าการชำระเงินทางอิเล็กทรอนิกส์ (รวมทั้งหมด)	**๒๖๖,๖๓๙**	**๒๕๒,๔๐๔**	**๒๓๕,๐๔๔**	**๒๑๕,๑๓๑**	**๑๗๑,๙๔๘**
การโอนเงินเพื่อลูกค้าผ่าน BAHTNET	๒๑๒,๔๑๔	๒๐๑,๗๐๑	๑๙๑,๗๕๔	๑๘๒,๒๕๕	๑๔๔,๓๑๘
การโอนเงินภายในธนาคาร (รวมชำระค่าสินค้าบริการ)	๓๐,๑๓๔	๒๘,๖๕๕	๒๓,๒๗๔	๑๖,๖๔๓	๑๕,๐๐๖
การโอนเงินครั้งละหลายรายการ	๒๐,๙๗๕	๑๙,๒๓๖	๑๗,๔๙๕	๑๔,๒๒๔	๑๐,๙๗๘
การโอนเงินรายย่อยข้ามธนาคาร	๑,๕๘๗	๑,๓๙๙	๑,๒๕๐	๑,๐๑๔	๘๓๒
การชำระเงินด้วยบัตรพลาสติก	๑,๔๗๓	๑,๓๖๕	๑,๒๓๕	๙๗๐	๗๙๗
เงินอิเล็กทรอนิกส์	๕๖	๔๘	๓๖	๒๔	๑๘

จากตารางที่ ๑-๒ จะเห็นว่ามูลค่าการชำระเงินทางอิเล็กทรอนิกส์มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องทุกปี ตั้งแต่ พ.ศ. ๒๕๕๓ - ๒๕๕๗ โดยมีมูลค่าการชำระเงินทางอิเล็กทรอนิกส์ ดังนี้

ปี ๒๕๕๓ มีมูลค่าการชำระเงินทางอิเล็กทรอนิกส์ ๑๗๑,๙๔๘ พันล้านบาท
ปี ๒๕๕๔ มีมูลค่าการชำระเงินทางอิเล็กทรอนิกส์ ๒๑๕,๑๓๑ พันล้านบาท
ปี ๒๕๕๕ มีมูลค่าการชำระเงินทางอิเล็กทรอนิกส์ ๒๓๕,๐๔๔ พันล้านบาท
ปี ๒๕๕๖ มีมูลค่าการชำระเงินทางอิเล็กทรอนิกส์ ๒๕๒,๔๐๔ พันล้านบาท
ปี ๒๕๕๗ มีมูลค่าการชำระเงินทางอิเล็กทรอนิกส์ ๒๖๖,๖๓๙ พันล้านบาท

ในปี ๒๕๕๗ พบว่ามีมูลค่าการชำระเงินทางอิเล็กทรอนิกส์ผ่านระบบการชำระเงินและช่องทางต่างๆ โดยเรียงลำดับจากมากไปหาน้อยได้ดังนี้ ๑) การโอนเงินเพื่อลูกค้าผ่าน BAHTNET ๒) การโอนเงินภายในธนาคาร (รวมชำระค่าสินค้าบริการ) ๓) การโอนเงินครั้งละหลายรายการ ๔) การโอนเงินรายย่อยข้ามธนาคาร ๕) การชำระเงินด้วยบัตรพลาสติก และ ๖) เงินอิเล็กทรอนิกส์

ตารางที่ ๑-๓ ธุรกรรมการชำระเงินผ่านบริการธนาคารทางอินเทอร์เน็ตและธนาคารทางโทรศัพท์เคลื่อนที่ ตั้งแต่ พ.ศ. ๒๕๕๓ - ๒๕๕๗

รายการ	๒๕๕๗	๒๕๕๖	๒๕๕๕	๒๕๕๔	๒๕๕๓
ธุรกรรมการชำระเงินผ่านธนาคารทางอินเทอร์เน็ต					
จำนวนบัญชีลูกค้าที่ใช้บริการ	๘,๖๖๓,๔๗๐	๘,๐๓๓,๐๖๑	๖,๖๔๕,๑๖๑	๕,๖๒๖,๑๙๒	๔,๘๒๒,๙๔๗
ปริมาณรายการ (พันรายการ)	๑๘๔,๕๐๑	๑๖๑,๗๘๔	๑๒๕,๒๗๗	๘๓,๘๔๑	๖๐,๗๙๔
มูลค่ารายการ (พันล้านบาท)	๒๐,๔๒๒	๑๙,๕๔๘	๑๔,๑๑๒	๘,๗๘๐	๗,๘๙๒
ธุรกรรมการชำระเงินผ่านธนาคารทางโทรศัพท์เคลื่อนที่					
จำนวนบัญชีลูกค้าที่ใช้บริการ	๓,๓๗๒,๐๕๑	๑,๑๖๔,๗๙๖	๘๖๔,๓๑๒	๗๐๖,๔๓๙	๕๑๙,๔๕๐
ปริมาณรายการ (พันรายการ)	๑๐๙,๓๕๐	๕๗,๑๙๙	๓๖,๒๘๕	๑๙,๙๔๒	๑๕,๘๘๕
มูลค่ารายการ (พันล้านบาท)	๑,๓๖๔	๗๕๒	๔๔๐	๑๘๗	๑๑๐

จากตารางที่ ๑-๓ จะเห็นว่าการทำธุรกรรมการชำระเงินผ่านบริการธนาคารทางอินเทอร์เน็ตและธนาคารทางโทรศัพท์เคลื่อนที่เริ่มได้รับความนิยมและมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องทุกปี ตั้งแต่ พ.ศ. ๒๕๕๓ - ๒๕๕๗ ทั้งจำนวนบัญชีลูกค้าที่ใช้บริการ ปริมาณรายการที่ทำธุรกรรม และมูลค่ารายการที่ทำธุรกรรม

ตารางที่ ๑-๔ ธุรกรรมการชำระเงินผ่านบริการธนาคารทางอินเทอร์เน็ตและธนาคารทางโทรศัพท์เคลื่อนที่ ในรายไตรมาส ประจำปี ๒๕๕๗

รายการ	ไตรมาสที่ ๔/๒๕๕๗	ไตรมาสที่ ๓/๒๕๕๗	ไตรมาสที่ ๒/๒๕๕๗	ไตรมาสที่ ๑/๒๕๕๗
ธุรกรรมการชำระเงินผ่านธนาคารทางอินเทอร์เน็ต				
จำนวนบัญชีลูกค้าที่ใช้บริการ	๘,๖๖๓,๔๗๐	๘,๙๔๓,๙๕๐	๘,๖๙๙,๕๗๔	๘,๓๓๕,๔๔๖
ปริมาณรายการ (พันรายการ)	๔๙,๗๘๒	๔๗,๓๖๘	๔๓,๓๒๕	๔๔,๐๒๔
มูลค่ารายการ (พันล้านบาท)	๕,๐๖๘	๕,๐๑๕	๔,๙๙๙	๕,๓๑๑
ธุรกรรมการชำระเงินผ่านธนาคารทางโทรศัพท์เคลื่อนที่				
จำนวนบัญชีลูกค้าที่ใช้บริการ	๓,๓๗๒,๐๕๑	๓,๗๑๑,๓๘๒	๓,๑๗๘,๔๑๐	๒,๙๒๑,๓๔๑
ปริมาณรายการ (พันรายการ)	๓๕,๗๑๑	๒๙,๓๗๘	๒๔,๐๖๓	๒๐,๑๙๘
มูลค่ารายการ (พันล้านบาท)	๔๓๑	๓๕๕	๓๐๖	๒๗๓

จากตารางที่ ๑-๔ จะเห็นว่าการทำธุรกรรมการชำระเงินผ่านบริการธนาคารทางอินเทอร์เน็ตและธนาคารทางโทรศัพท์เคลื่อนที่ในรายไตรมาส ประจำปี ๒๕๕๗ มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ทั้งจำนวนบัญชีลูกค้าที่ใช้บริการ ปริมาณรายการที่ทำธุรกรรม และมูลค่ารายการที่ทำธุรกรรม

บทสรุป

จากข้อมูลดังกล่าวข้างต้นจะเห็นได้ว่าปริมาณและมูลค่าที่เกิดจากการชำระเงินทางอิเล็กทรอนิกส์ผ่านบริการธนาคารทางอินเทอร์เน็ตและธนาคารทางโทรศัพท์เคลื่อนที่นั้นเพิ่มสูงขึ้น ประกอบกับในปัจจุบันลักษณะการดำเนินชีวิตของผู้คนในเมืองและชนบทเปลี่ยนแปลงไป จากเดิมที่มีการทำธุรกรรมทางอิเล็กทรอนิกส์ผ่านเครื่องคอมพิวเตอร์ก็เปลี่ยนมาใช้สมาร์ตโฟน (Smartphone) โดยใช้สมาร์ตโฟนในการติดต่อสื่อสารและทำธุรกรรมทางอิเล็กทรอนิกส์เพิ่มมากขึ้น เช่น การชำระค่าสินค้าและบริการ การโอนเงิน

บทที่ ๒
ธนาคารทางโทรศัพท์เคลื่อนที่ (Mobile Banking)

ประเภทของโทรศัพท์เคลื่อนที่

Basic Phone

เป็นโทรศัพท์เคลื่อนที่ทั่วไปที่มักจะมีเพียงฟังก์ชันพื้นฐานในการโทรศัพท์และการรับส่งข้อความ อาจมีวิวัฒนาการในการแสดงผลแบบจอภาพสีหรือขาวดำ เช่น โทรศัพท์เคลื่อนที่ รุ่น Nokia 3310

Smart Phone

เป็นโทรศัพท์เคลื่อนที่ที่มีความสามารถเพิ่มเติม นอกเหนือจากโทรศัพท์เคลื่อนที่ทั่วไป รองรับการใช้งานในด้านต่างๆ มากมาย แม้ว่าในปัจจุบันจะไม่มีการกำหนดมาตรฐานของสมาร์ตโฟน (Smartphone) ออกมาอย่างชัดเจน แต่แนวโน้มในอนาคตของสมาร์ตโฟนยังคงมีการพัฒนาเรื่อยไป เพื่อตอบสนองความต้องการของผู้ใช้งานที่มีปริมาณสูงขึ้นอย่างต่อเนื่อง เช่น ความเร็วในการประมวลผล การออกแบบหน้าจอให้มีขนาดใหญ่ มีความละเอียดสูง และมีความคมชัด การปรับปรุงคุณภาพของกล้องถ่ายรูป การแก้ปัญหาแบตเตอรี่หมดเร็ว การออกแอปพลิเคชัน (Application) ใหม่ โดยฟีเจอร์ (Feature) หลักที่ต้องมีอยู่ในสมาร์ตโฟน มีดังนี้

ระบบปฏิบัติการ (Operating System)

โดยทั่วไปสมาร์ตโฟนแต่ละเครื่องจะขึ้นอยู่กับระบบปฏิบัติการที่ใช้งาน ซึ่งระบบปฏิบัติการจะช่วยให้ผู้ใช้งานสามารถเข้าถึงแอปพลิเคชันต่างๆ บนระบบนั้นได้ เช่น Apple iOS, Google Android, Microsoft Windows Phone, Nokia Symbian, Research in Motion (RIM) BlackBerry OS ซึ่งระบบปฏิบัติการแต่ละค่ายต่างก็มีความสามารถในการติดตั้งโปรแกรมเพิ่มเติม เพื่ออำนวยความสะดวกให้กับผู้ใช้งานมากขึ้น

แอปพลิเคชัน

โทรศัพท์เคลื่อนที่ทั่วไปจะมีแอปพลิเคชันพื้นฐานอยู่ภายในเครื่อง เช่น สมุดรายชื่อผู้ติดต่อ บันทึกการใช้งานโทรศัพท์ การรับส่งข้อความ แต่สำหรับสมาร์ตโฟนจะมีแอปพลิเคชันที่ช่วยอำนวยความสะดวกได้อย่างหลากหลายและครอบคลุมการใช้งานมากขึ้น เช่น การสร้างหรือแก้ไขเอกสาร Office การวาดเขียนลงบนหน้าจอพร้อมบันทึกเป็นรูปภาพ การใช้เป็นเนวิเกเตอร์ (Navigator) นำทางขณะขับขี่รถยนต์

การเข้าถึงเว็บไซต์ (Web Access)

สมาร์ตโฟนสามารถรองรับการเข้าถึงและการใช้งานอินเทอร์เน็ต (Internet) ที่มีการติดต่อสื่อสารได้ทั่วโลก เช่น การติดต่อสื่อสารผ่านเครือข่ายสังคมออนไลน์ การแบ่งปันข้อมูลออนไลน์ การโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต (Voice over Internet Protocol : VoIP)

QWERTY Keyboard

สมาร์ตโฟนทั่วไปจะมีคีย์บอร์ดที่จัดเรียงตัวอักษรคล้ายคลึงกับคีย์บอร์ดของเครื่องคอมพิวเตอร์ ในปัจจุบันคีย์บอร์ดของสมาร์ตโฟนส่วนใหญ่จะอยู่ในรูปแบบปุ่มสัมผัสบนหน้าจอ (Touch Screen Keyboard) แต่ยังมีสมาร์ตโฟนบางรุ่นที่ยังคงเป็นคีย์บอร์ดแบบปุ่มกด (Button Keyboard)

การส่งข้อความ (Messaging)

โทรศัพท์เคลื่อนที่ทั่วไปสามารถรับส่งได้แค่เพียงข้อความตัวอักษร แต่สิ่งที่สมาร์ตโฟนแตกต่างจากโทรศัพท์เคลื่อนที่ทั่วไปก็คือ สมาร์ตโฟนสามารถอัปเดตข้อมูลจดหมายอิเล็กทรอนิกส์หรืออีเมล (e - Mail) และตารางนัดหมายให้สอดคล้องกับข้อมูลบนเครื่องคอมพิวเตอร์ได้ในเวลาเดียวกัน

วิวัฒนาการของการทำธุรกรรมทางการเงิน

ยุคของการทำธุรกรรมทางการเงินผ่านการรับส่งข้อความ

เป็นยุคแรกที่มีการให้บริการการทำธุรกรรมผ่านโทรศัพท์เคลื่อนที่ โดยการรับส่งข้อความ (Short Message Service : SMS) เป็นตัวอักษร (Clear Text) ซึ่งไม่ได้มีการเข้ารหัสความปลอดภัยเอาไว้ ทำให้การให้บริการการทำธุรกรรมผ่านโทรศัพท์เคลื่อนที่ในยุคนี้ไม่มีความปลอดภัยเท่าที่ควร ธนาคารจึงออกนโยบายมาควบคุม โดยเปิดให้ใช้งานได้เฉพาะการเช็คยอดเงิน การเติมเงิน และการจ่ายบิลต่างๆ เท่านั้น ซึ่งธนาคารพิจารณาแล้วเห็นว่าบริการนี้มีความเสี่ยงไม่สูงมากนัก ด้วยปัจจัยที่หลากหลายทำให้การให้บริการการทำธุรกรรมทางการเงินผ่านการรับส่งข้อความในยุคแรกไม่เป็นที่แพร่หลาย แต่ก็ยังมีการพัฒนาบริการดังกล่าวเรื่อยมา

ยุคของการทำธุรกรรมทางการเงินผ่าน SIM Toolkit

เนื่องจากอินเทอร์เน็ตยังมีความเร็วไม่มากนัก ทำให้การทำธุรกรรมทางการเงินผ่านการรับส่งข้อความมีข้อจำกัด จึงมีการพัฒนา ATM SIM ขึ้น เพื่ออำนวยความสะดวกให้กับผู้ใช้งาน สามารถทำธุรกรรมต่างๆ ผ่านโทรศัพท์เคลื่อนที่ได้โดยไม่ต้องใช้อินเทอร์เน็ต โดยเป็นความร่วมมือระหว่างค่ายโทรศัพท์เคลื่อนที่กับธนาคารในการนำบริการต่างๆ บรรจุลงใน SIM เช่น การเช็คยอดเงิน การเติมเงิน การโอนเงิน การจ่ายบิลต่างๆ ซึ่งการใช้บริการการทำธุรกรรมต่างๆ ในแต่ละครั้งนั้น การส่งข้อมูลยังคงส่งคำสั่งผ่านการรับส่งข้อความเหมือนในยุคแรก แต่จะเพิ่มความปลอดภัยให้กับผู้ใช้บริการ โดยข้อความที่ส่งออกไปจะมีการเข้ารหัสเพิ่มเติม และรหัสนั้นจะถูกถอดที่เครื่องแม่ข่าย (Server) ของธนาคารที่ใช้บริการเท่านั้น หลังจากธนาคารได้รับข้อความที่ถูกเข้ารหัสแล้ว ข้อความนั้นจะถูกแปลเป็นคำสั่งการทำธุรกรรมต่างๆ ที่ผู้ใช้บริการได้ทำธุรกรรมผ่านโทรศัพท์เคลื่อนที่ ด้วยความปลอดภัยที่มีมากขึ้น ทำให้ผู้ใช้บริการเกิดความมั่นใจในการทำธุรกรรมต่างๆ และเริ่มมีผู้ใช้บริการในการทำธุรกรรมทางการเงินผ่านโทรศัพท์เคลื่อนที่เพิ่มมากขึ้นตามไปด้วย

ยุคของการทำธุรกรรมทางการเงินผ่านสมาร์ตโฟน

เป็นยุคโทรศัพท์เคลื่อนที่ที่มีสมาร์ตโฟนแพลตฟอร์ม (Platform) ต่างๆ ออกมามากมาย และมีการพัฒนาด้านความเร็วในการเชื่อมต่ออินเทอร์เน็ต เพื่อตอบสนองความต้องการของผู้ใช้งานในการเข้าใช้บริการแอปพลิเคชันต่างๆ ด้วยลักษณะการใช้ชีวิตประจำวันของคนในยุคปัจจุบันที่ใช้สมาร์ตโฟนเป็นส่วนใหญ่ ทำให้ธนาคารมีการพัฒนาบริการทางการเงินให้สามารถทำธุรกรรมต่างๆ ผ่านสมาร์ตโฟนได้ เพื่อเพิ่มความสะดวกให้กับผู้ใช้บริการ และที่สำคัญได้มีการพัฒนาเทคโนโลยีความปลอดภัย ทำให้การทำธุรกรรมทางการเงินผ่านธนาคารทางโทรศัพท์เคลื่อนที่เป็นไปอย่างรวดเร็ว และมีจำนวนผู้ใช้บริการเพิ่มมากขึ้น

ประโยชน์ของการใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่

การทำธุรกรรมทางการเงินผ่านธนาคารทางโทรศัพท์เคลื่อนที่เป็นทางเลือกใหม่ที่เพิ่มความสะดวกสบายและรวดเร็ว โดยที่ผู้ใช้บริการไม่ต้องเสียเวลาต่อคิวรอรับบริการจากธนาคารหรือตู้ ATM และไม่ต้องเสียค่าใช้จ่ายในการเดินทาง รวมทั้งผู้ใช้บริการสามารถทำรายการได้ทุกที่ ทุกเวลา ตลอด ๒๔ ชั่วโมง โดยสามารถทำธุรกรรมทางการเงินได้อย่างหลากหลาย เช่น ถามยอดบัญชี ตรวจสอบรายการเดินบัญชี โอนเงิน จ่ายบิล เช็คอัตราแลกเปลี่ยนเงิน

บริการทางการเงินที่ให้บริการผ่านธนาคารทางโทรศัพท์เคลื่อนที่

ธนาคารทางโทรศัพท์เคลื่อนที่ช่วยให้ผู้ใช้บริการสามารถทำรายการผ่านสมาร์ตโฟนได้ตลอด ๒๔ ชั่วโมง ซึ่งบริการทางการเงินที่ให้บริการผ่านธนาคารทางโทรศัพท์เคลื่อนที่ มีดังนี้

การถามยอดบัญชี (Account Balance)

สามารถตรวจสอบยอดคงเหลือของแต่ละบัญชีได้ ทั้งบัญชีออมทรัพย์ บัญชีกระแสรายวัน บัญชีฝากประจำ บัตรเครดิต และสินเชื่อ

การตรวจสอบรายการเดินบัญชี (Bank Statement)

สามารถตรวจสอบรายการเดินบัญชีของบัญชีต่างๆ และเรียกดูรายการเดินบัญชีย้อนหลังได้สูงสุดถึง ๙ เดือน

การโอนเงิน (Transfer)

- สามารถโอนเงินระหว่างบัญชี โอนเงินไปยังบุคคลอื่นได้
- สามารถโอนเงินต่างธนาคารแบบ Real - Time และแจ้งผลการโอนเงินทางข้อความไปยังปลายทางได้

การจ่ายบิล (Pay Bill)

สามารถชำระค่าสินค้าและบริการได้ เช่น ค่าไฟ ค่าบัตรเครดิต ค่าโทรศัพท์

การเช็คอัตราแลกเปลี่ยนเงิน (Exchange Rates)

สามารถเรียกดูข้อมูลอัตราดอกเบี้ยของธนาคารได้ ทั้งดอกเบี้ยเงินฝาก ดอกเบี้ยเงินกู้ และทราบผลได้ทันที

ขั้นตอนการใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่

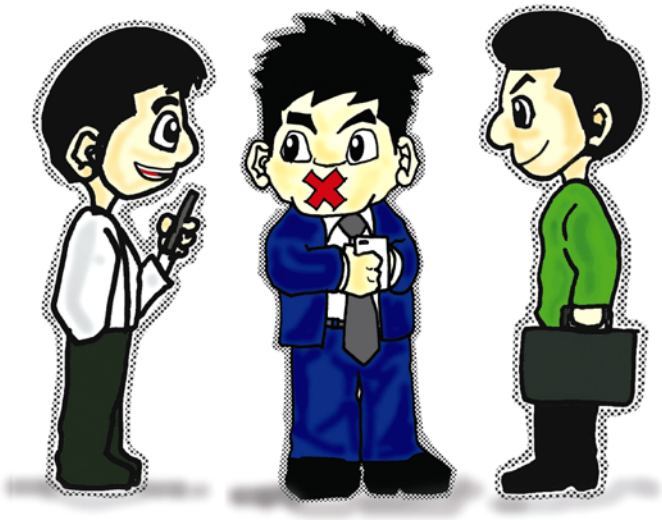
ขั้นตอนการใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่ ดังตารางที่ ๒-๑ อาจแตกต่างกันไปขึ้นอยู่กับบริการของแต่ละธนาคาร

ตารางที่ ๒-๑ ขั้นตอนการใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่

ลำดับที่	ผ่านเว็บเบราว์เซอร์ (Web Browser)	ผ่านแอปพลิเคชัน
๑	ลงทะเบียนขอใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่จากธนาคารที่เปิดให้บริการ	ลงทะเบียนขอใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่จากธนาคารที่เปิดให้บริการ
๒	ตรวจสอบและตั้งค่า GPRS/EDGE/3G บนสมาร์ตโฟนให้พร้อมสำหรับใช้งานอินเทอร์เน็ต	ตรวจสอบและตั้งค่า GPRS/EDGE/3G บนสมาร์ตโฟนให้พร้อมสำหรับใช้งานอินเทอร์เน็ต
๓	-	ทำการดาวน์โหลดและติดตั้งแอปพลิเคชันบริการธนาคารทางโทรศัพท์เคลื่อนที่ของธนาคารที่ขอใช้บริการ (เฉพาะครั้งแรก) ซึ่งวิธีการดาวน์โหลดและติดตั้งจะขึ้นอยู่กับยี่ห้อและรุ่นของสมาร์ตโฟน
๔	เปิดเข้าใช้งานบริการธนาคารทางโทรศัพท์เคลื่อนที่ของธนาคารที่ขอใช้บริการผ่านเว็บเบราว์เซอร์	เปิดเข้าใช้งานบริการธนาคารทางโทรศัพท์เคลื่อนที่ของธนาคารที่ขอใช้บริการผ่านแอปพลิเคชัน
๕	เข้าระบบบริการธนาคารทางโทรศัพท์เคลื่อนที่ของธนาคารที่ขอใช้บริการผ่านเว็บเบราว์เซอร์ โดยกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ซึ่งถูกกำหนดโดยผู้ใช้งาน	เข้าระบบบริการธนาคารทางโทรศัพท์เคลื่อนที่ของธนาคารที่ขอใช้บริการผ่านแอปพลิเคชัน โดยกรอกชื่อผู้ใช้และรหัสผ่าน ซึ่งถูกกำหนดโดยผู้ใช้งาน
๖	เข้าใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่ซึ่งจะขึ้นอยู่กับแต่ละธนาคารที่เปิดให้บริการ	เข้าใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่ซึ่งจะขึ้นอยู่กับแต่ละธนาคารที่เปิดให้บริการ
๗	ตรวจสอบรายการและยืนยันการทำรายการ	ตรวจสอบรายการและยืนยันการทำรายการ
๘	ระบบจะแสดงผลการทำรายการ	ระบบจะแสดงผลการทำรายการ
๙	เมื่อใช้งานเสร็จเรียบร้อยแล้ว ทำการออกจากระบบบริการธนาคารทางโทรศัพท์เคลื่อนที่	เมื่อใช้งานเสร็จเรียบร้อยแล้ว ทำการออกจากระบบบริการธนาคารทางโทรศัพท์เคลื่อนที่
๑๐	ทำการล้างบันทึกประวัติการใช้งาน (History Settings) บริการธนาคารทางโทรศัพท์เคลื่อนที่ในเว็บเบราว์เซอร์เพื่อลบข้อมูลบัญชีทั้งหมด	-

ข้อควรรู้เกี่ยวกับ "รหัสผ่านชั่วคราว"

ในขั้นตอนการทำรายการจะมีการยืนยันการทำธุรกรรมโดยใช้รหัสผ่านชั่วคราว ซึ่งรหัสผ่านชั่วคราวเป็นรหัสที่ธนาคารออกให้กับผู้ใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่ เพื่อยืนยันการทำธุรกรรมที่สำคัญในแต่ละครั้ง ซึ่งอาจมีชื่อเรียกแตกต่างกันไป เช่น OTP (One Time Password), TOP (Time Out Password) โดยธนาคารจะส่งรหัสผ่านชั่วคราว พร้อมแจ้งรายละเอียดการทำธุรกรรมที่ผู้ใช้บริการต้องยืนยัน ผ่านข้อความไปยังเบอร์โทรศัพท์ที่ผู้ใช้บริการแจ้งไว้กับธนาคาร โดยแต่ละธนาคารจะกำหนดระยะเวลาในการใช้รหัสผ่านชั่วคราวไว้ หากเกินกว่าระยะเวลาที่กำหนดก็จะใช้รหัสนั้นไม่ได้ บางธนาคารกำหนดให้ใช้เมื่อผู้ใช้บริการต้องการทำธุรกรรมที่สำคัญ เช่น การเพิ่มรายชื่อบัญชีเงินโอน แต่บางธนาคารกำหนดให้ใช้ทุกครั้งที่มีการโอนเงินออกจากบัญชีผู้ใช้บริการ



บทที่ ๓
ภัยเทคโนโลยีสารสนเทศที่ควรระวัง

เนื่องด้วยความเจริญก้าวหน้าทางเทคโนโลยีการสื่อสาร ส่งผลให้มีผู้พัฒนาและผลิตสมาร์ตโฟน (Smartphone) ออกมาเป็นจำนวนมาก และได้เพิ่มความสามารถของสมาร์ตโฟนในแต่ละฟังก์ชันการทำงาน เพื่ออำนวยความสะดวกให้กับผู้ใช้งานมากที่สุด เช่น สามารถเชื่อมต่อกับเครือข่ายไร้สาย (Wi-Fi) เพื่อความสะดวกในการเข้าถึงอินเทอร์เน็ต (Internet) บนสมาร์ตโฟน สามารถรับชมวิดีโอบนสมาร์ตโฟนเพื่อความบันเทิง แต่จากความสามารถและข้อดีหลายประการของสมาร์ตโฟน ยังอาจแฝงไปด้วยภัยอันตรายหรือภัยคุกคามที่ผู้ใช้งานอีกจำนวนมากอาจจะยังไม่เคยทราบ ส่งผลให้ผู้ไม่หวังดีสามารถโจมตีหรือขโมยข้อมูลต่างๆ ได้โดยง่าย ซึ่งภัยเทคโนโลยีสารสนเทศที่ควรระวัง มีดังนี้

ภัยที่มาจากการใช้งานโปรแกรมหรือแอปพลิเคชันบนสมาร์ตโฟน (Application - Based Threats)

ภัยที่มากับโปรแกรมหรือแอปพลิเคชัน (Application) ที่ติดตั้งบนสมาร์ตโฟน

โปรแกรมหรือแอปพลิเคชันจำนวนมากที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนสมาร์ตโฟนพบว่ายังไม่สามารถตรวจสอบลักษณะการทำงานในด้านความมั่นคงปลอดภัยได้ ทำให้ผู้ใช้งานไม่สามารถล่วงรู้ได้เลยว่าโปรแกรมหรือแอปพลิเคชันที่ติดตั้งไปเพื่อใช้ประโยชน์มากมายนั้น จะถูกแฝงมาด้วยปัญหาด้านความมั่นคงปลอดภัยหรือไม่ โดยภัยคุกคามที่มากับโปรแกรมหรือแอปพลิเคชันที่ติดตั้งสามารถเป็นได้มากกว่าหนึ่งประเภท ดังนี้

มัลแวร์ (Malware)

โปรแกรมที่ถูกออกแบบมาเพื่อแสดงพฤติกรรมที่เป็นอันตรายต่อข้อมูลในสมาร์ตโฟนเครื่องนั้น เช่น สั่งให้สมาร์ตโฟนส่งข้อความอันไม่พึงประสงค์ออกไปยังรายการผู้ติดต่อในสมาร์ตโฟน ขโมยข้อมูลบนสมาร์ตโฟนโดยที่ผู้ใช้งานหรือเจ้าของสมาร์ตโฟนนั้นไม่รู้ตัว ซึ่งในกรณีที่ผู้ใช้งานเก็บข้อมูลบัญชีผู้ใช้ของตนเองหรือของผู้ที่เกี่ยวข้องไว้ในสมาร์ตโฟน ก็อาจจะทำให้เกิดการเข้าโจรกรรมข้อมูลที่เกี่ยวข้องต่อไปได้

สปายแวร์ (Spyware)

โปรแกรมที่ถูกออกแบบมาเพื่อเก็บรวบรวมข้อมูลต่างๆ ของผู้ใช้งาน โดยเป้าหมายส่วนใหญ่ของสปายแวร์มักมุ่งเน้นไปยังประวัติการใช้งานโทรศัพท์ ข้อความ ที่อยู่ รายชื่อผู้ติดต่อ อีเมล (e - Mail) รวมทั้งรูปภาพ ซึ่งสปายแวร์โดยทั่วไปมักได้รับการออกแบบสำหรับเฝ้าติดตามการใช้งานของบุคคลใดบุคคลหนึ่งหรือการใช้งานที่เกี่ยวข้องกับองค์กร

การเข้าโจมตีสมาร์ตโฟนของผู้ใช้งานด้วยมัลแวร์หรือสปายแวร์ส่วนใหญ่พบว่า ใช้เทคนิคในการหลอกลวงให้ผู้ใช้งานดาวน์โหลดโปรแกรมมาติดตั้งบนสมาร์ตโฟนโดยไม่รู้ตัว เช่น ให้คลิกลิงก์ที่ดูเหมือนว่าไม่น่าจะมีความผิดปกติอะไร แต่แท้จริงแล้วนั่นคือ การสั่งให้ดาวน์โหลดและติดตั้งมัลแวร์หรือสปายแวร์ลงในสมาร์ตโฟน เมื่อมัลแวร์หรือสปายแวร์ติดตั้งโปรแกรมเสร็จแล้ว ก็จะเข้าสู่กระบวนการโจมตีในลักษณะต่างๆ ต่อไป ดังนั้น ในการดาวน์โหลดโปรแกรมหรือแอปพลิเคชันควรต้องสังเกตและระมัดระวัง หลีกเลี่ยงการดาวน์โหลดโปรแกรมหรือแอปพลิเคชันโดยไม่รู้ที่มาที่ไป เพราะมิจฉาชีพมักจะซ่อนอะไรบางอย่างไว้ในโปรแกรมหรือแอปพลิเคชันนั้น เพื่อล้วงข้อมูล

ช่องโหว่ในโปรแกรมหรือแอปพลิเคชันที่ใช้งาน

พฤติกรรมการทำงานของโปรแกรมหรือแอปพลิเคชันที่มีความผิดพลาด อาจถูกค้นพบและสามารถนำมาใช้ประโยชน์เพื่อวัตถุประสงค์ในทางที่ไม่ดี ซึ่งการค้นพบช่องโหว่ดังกล่าวมักจะส่งผลให้ผู้ค้นพบสามารถโจมตีโดยการเข้าถึงข้อมูลที่สำคัญหรือการดำเนินการอันไม่พึงประสงค์ได้ แต่อย่างไรก็ตาม ช่องโหว่ดังกล่าวมักถูกแจ้งไปยังผู้พัฒนาโปรแกรมหรือแอปพลิเคชัน เพื่ออัปเดตและแก้ไขต่อไป

ภัยที่มาจากการใช้งานเว็บไซต์บนสมาร์ตโฟน (Web - Based Threats)

เนื่องจากในปัจจุบันสมาร์ตโฟนส่วนใหญ่สามารถรองรับการใช้งานในการเชื่อมต่ออินเทอร์เน็ตได้จากเครือข่ายไร้สายทั่วไป ทำให้ผู้ใช้งานเกิดความสะดวกในการเข้าถึงเว็บไซต์ (Website) หรือบริการต่างๆ ผ่านสมาร์ตโฟน เช่น การอ่านอีเมล การใช้งานระบบธุรกรรมทางอิเล็กทรอนิกส์ (e - Transaction) การเข้าระบบที่เป็นสื่อสังคมออนไลน์ โดยภัยคุกคามที่เกิดจากการเข้าใช้งานเว็บไซต์สามารถเป็นได้มากกว่าหนึ่งประเภท ดังนี้

ฟิชชิง (Phishing)

การหลอกลวงชนิดหนึ่งโดยใช้หน้าเว็บไซต์หรือส่วนติดต่อผู้ใช้อื่นๆ ที่ออกแบบให้มีลักษณะคล้ายคลึงกับของจริง เพื่อหลอกลวงให้ผู้ใช้งานกรอกข้อมูลเข้าสู่ระบบ เช่น ผู้หลอกลวงพัฒนาหน้าเว็บไซต์ล็อกอิน (Log in) ของธนาคาร และส่งลิงก์หลอกลวงโดยแจ้งข้อมูลอันเป็นเท็จให้ผู้ใช้งานเข้าอัปเดตข้อมูลส่วนบุคคลจากลิงก์ของหน้าล็อกอินที่ทำขึ้นมา เมื่อผู้ใช้งานพยายามล็อกอินเข้าไปยังระบบ ผู้หลอกลวงดังกล่าวก็จะสามารถดักจับข้อมูลอันน่าเชื่อได้ว่าเป็นข้อมูลล็อกอินของผู้ใช้งานคนนั้น ทำให้ข้อมูลหรือบัญชีการใช้งานนั้นมีความเสี่ยงที่จะโดนขโมยข้อมูลออกไป เช่น ข้อมูลชื่อผู้ใช้ (Username) รหัสผ่าน (Password) เลขที่บัญชีธนาคาร หมายเลขบัตรเครดิต ซึ่งลิงก์ที่เป็นการฟิชชิงนี้ ส่วนใหญ่มักจะแนบไปกับอีเมลหรือเป็นลิงก์ที่มีเนื้อหาเชิญชวนต่างๆ โดยความรุนแรงของการถูกขโมยข้อมูลดังกล่าวอาจจะไม่ส่งผลกระทบในทันที ถ้าหากมีการเข้ายับยั้งได้ทัน เช่น เมื่อทราบว่าได้มีการส่งข้อมูลเข้าหน้าเว็บไซต์ฟิชชิงไปแล้วและรีบเข้าไปเปลี่ยนรหัสผ่านในหน้าเว็บไซต์ของระบบจริงทันที ก็จะไม่ส่งผลให้เกิดความเสียหายในวงกว้าง แต่หากผู้ใช้งานปล่อยให้ผู้หลอกลวงสามารถเข้าถึงบัญชีการใช้งานต่างๆ ได้ ในกรณีที่เป็นระบบที่มีความเสียหายรุนแรง เช่น ระบบธุรกรรมทางอิเล็กทรอนิกส์ ผู้หลอกลวงจะสามารถใช้เงินในบัญชีของผู้ใช้งานคนนั้นได้ทันที

ช่องโหว่ของโปรแกรมประเภทเบราว์เซอร์ (Browser)

ช่องโหว่ที่ถูกพบในโปรแกรมเบราว์เซอร์หรือโปรแกรมปลั๊กอิน (Plug in) ที่สามารถติดตั้งเพิ่มเติมได้ในเบราว์เซอร์ เช่น Flash Player, PDF Reader เพื่อวัตถุประสงค์ในทางที่ไม่ดี โดยลักษณะและวิธีการโจมตีอาจเป็นแค่เพียงการให้ผู้ใช้งานเข้าชมเว็บไซต์เท่านั้น จากนั้นก็จะทำให้ผู้ใช้งานติดมัลแวร์หรือโปรแกรมอันตรายต่างๆ ที่ผู้โจมตีใช้ในช่องโหว่ดังกล่าว

ภัยที่มาจากการใช้งานเครือข่าย (Network Threats)

ในปัจจุบันสมาร์ตโฟนมักจะสนับสนุนการใช้งานเครือข่ายไร้สาย ซึ่งมีผู้ให้บริการเป็นจำนวนมาก ทั้งที่น่าเชื่อถือและไม่สามารถตรวจสอบได้ ภัยคุกคามที่ส่งผลกระทบต่อการใช้งานบนสมาร์ตโฟน สามารถเป็นได้หลายกรณี ดังนี้

การเปลี่ยนสถานะจากผู้ใช้งานเป็นผู้โจมตีผ่านข้อบกพร่องของระบบปฏิบัติการ (Operating System) บนสมาร์ตโฟน ส่งผลให้สมาร์ตโฟนสามารถส่งต่อหรือแพร่กระจายมัลแวร์ได้โดยอัตโนมัติผ่านการทำงานบนเครือข่าย เช่น เครือข่ายไร้สาย บลูทูธ (Bluetooth)

การถูกดักจับข้อมูลบนเครือข่ายไร้สาย (Wi-Fi Sniffing) เป็นลักษณะการขโมยข้อมูลบนเครือข่ายไร้สาย ซึ่งโดยทั่วไปเป็นข้อมูลที่รับส่งกันโดยไม่ได้มีการเข้ารหัสความปลอดภัยที่เหมาะสม ทำให้มีโอกาสถูกลักลอบขโมยข้อมูลได้โดยง่าย แค่เพียงใช้เทคนิคและวิธีในการดักจับข้อมูลจากโปรแกรมประเภท Sniffer ซึ่งหาข้อมูลได้ตามเว็บไซต์ทั่วไป ในที่นี้ขอยกตัวอย่างวิธีการใช้งานโปรแกรมชื่อ Firesheep ซึ่งเป็นปลั๊กอินบนเบราว์เซอร์ Firefox ที่ใช้ในการดักจับข้อมูลในเครือข่ายเดียวกัน เป้าหมายส่วนใหญ่มักใช้กับเครือข่ายไร้สายสาธารณะและไม่ได้เชื่อมต่อบริการเว็บไซต์ที่มีการเข้ารหัส HTTPS (Hypertext Transfer Protocol Secure) โดยลักษณะการทำงานของโปรแกรมจะมีการดักจับข้อมูลแล้วกรองข้อมูลเพื่อค้นหาคุกกี้ (Cookie) ซึ่งเป็นข้อมูลที่ใช้ระบุตัวตนกับเว็บไซต์ที่เข้าใช้บริการ โดยข้อมูลคุกกี้ที่กล่าวถึงจะถูกเก็บไว้ในเบราว์เซอร์ของผู้ใช้งานหลังจากที่มีการล็อกอินเข้าสู่เว็บไซต์ จากนั้นโปรแกรมจะแสดงรายการที่ดักจับไว้ทั้งหมด ซึ่งผู้ใช้โปรแกรมสามารถคลิกที่รายการดังกล่าวเพื่อสวมรอยเป็นผู้ใช้งานคนนั้นได้

การใช้เครือข่ายไร้สายที่เปิดให้ใช้ฟรีตามสถานที่สาธารณะ เช่น ห้างสรรพสินค้า โรงแรม มิจฉาชีพอาจใช้เครือข่ายไร้สายปลอมในการขโมยข้อมูลของผู้ใช้บริการ ซึ่งมิจฉาชีพแค่เพียงใช้อุปกรณ์ในการกระจายเครือข่ายไร้สายที่ไม่มีระบบรักษาความปลอดภัย แต่มีไว้เพื่อถอดข้อมูล โดยตั้งชื่อเครือข่ายไร้สายให้เหมือนกับเครือข่ายไร้สายที่เปิดให้ใช้ฟรีตามสถานที่สาธารณะนั้น เมื่อผู้ใช้บริการเข้าใช้โดยไม่รู้ว่าเป็นเครือข่ายไร้สายปลอมและมีการทำธุรกรรมทางการเงิน มิจฉาชีพก็จะได้ข้อมูลชื่อผู้ใช้และรหัสผ่านของผู้ใช้บริการ หรืออาจได้ข้อมูลอื่นของผู้ใช้บริการไปด้วย ดังนั้น ก่อนเข้าใช้งานเครือข่ายไร้สายที่เปิดให้ใช้ฟรีตามสถานที่สาธารณะควรตรวจสอบให้แน่ใจก่อนว่าเป็นเครือข่ายไร้สายที่เชื่อถือได้หรือไม่ และควรเข้าใช้งานด้วยความระมัดระวัง

ภัยที่เกิดจากการสูญหายหรือการถูกขโมยสมาร์ตโฟน

เนื่องจากในปัจจุบันสมาร์ตโฟนเป็นอุปกรณ์ที่มีค่าสำหรับมิจฉาชีพ รวมไปถึงมีค่าสำหรับกลุ่มคนบางกลุ่มที่ต้องการได้มาซึ่งข้อมูลส่วนบุคคล ภัยคุกคามที่เกิดจากการสูญหายหรือการถูกขโมยสมาร์ตโฟนสามารถแบ่งได้เป็น ๒ ประเภท ดังนี้

การสูญหายหรือการถูกขโมยสมาร์ตโฟน

ในปัจจุบันสมาร์ตโฟนมีการพัฒนาด้านเทคโนโลยีเพื่ออำนวยความสะดวกให้ผู้ใช้งานมากขึ้น ทำให้สมาร์ตโฟนมีราคาสูง และด้วยค่านิยมทางสังคมที่ผู้ใช้งานนิยมใช้สมาร์ตโฟนที่มีราคาสูง ทำให้สมาร์ตโฟนเป็นเป้าหมายของมิจฉาชีพและมีโอกาสถูกขโมยได้โดยง่าย อีกทั้งมีตลาดที่มีความต้องการหรือรองรับการซื้อขายสมาร์ตโฟนมากมาย โดยที่ไม่มีการตรวจสอบแหล่งที่มา จึงมีความเสี่ยงสูงที่ผู้ใช้งานจะมีโอกาสถูกมิจฉาชีพขโมยสมาร์ตโฟน หรืออีกกรณีหนึ่งอาจเกิดจากผู้ใช้งานลืมสมาร์ตโฟนหรือทำตกหล่นสูญหายเอง

การถูกขโมยข้อมูลส่วนบุคคล

การถูกขโมยข้อมูลส่วนบุคคลเป็นภัยคุกคามที่สามารถเกิดขึ้นได้ตลอดเวลาและทุกสถานการณ์ ทั้งโดยความรู้เท่าไม่ถึงการณ์ของเจ้าของข้อมูล หรือเพราะโอกาสที่เปิดกว้าง จนทำให้ผู้ไม่หวังดีสบโอกาสที่จะขโมยข้อมูลส่วนบุคคล ซึ่งมักจะเกิดขึ้นจากความไม่ระมัดระวังและความไม่ตระหนักถึงความมั่นคงปลอดภัยของข้อมูลภายในสมาร์ตโฟน ทำให้ผู้ไม่หวังดีสามารถขโมยข้อมูลส่วนบุคคลไปได้ด้วยวิธีการต่างๆ เช่น การแอบมองข้อมูลการล็อกอินเข้าสู่ระบบจากสมาร์ตโฟน การนำสมาร์ตโฟนไปซ่อมที่ร้านโดยไม่ได้ทำการเคลียร์ข้อมูลการใช้งาน ข้อมูลส่วนบุคคลที่กล่าวถึงอาจไม่ใช่แค่เพียงข้อมูลส่วนตัวเท่านั้น แต่อาจเป็นข้อมูลขององค์กรด้วย เช่น เอกสารขององค์กร ข้อมูลรายชื่อผู้ติดต่องาน ข้อมูลบัญชีธนาคาร ข้อมูลอีเมลขององค์กร ซึ่งข้อมูลทั้งหมดที่กล่าวมานั้น หากข้อมูลถูกขโมยไป ความเสียหายที่เกิดขึ้นคงจะไม่สามารถประเมินมูลค่าได้

บทสรุป

จากปริมาณการใช้สมาร์ตโฟนในการทำธุรกรรมทางการเงินหรือการใช้บริการต่างๆ ในปัจจุบันที่เพิ่มสูงขึ้น ช่วยอำนวยความสะดวกให้กับผู้ใช้บริการ แต่ความสะดวกนั้นอาจแฝงไปด้วยภัยคุกคามจากการใช้งานสมาร์ตโฟน ส่งผลให้ผู้ไม่หวังดีสามารถโจมตีหรือขโมยข้อมูลต่างๆ ได้โดยง่าย ดังนั้น ผู้ใช้บริการควรใช้เทคโนโลยีอย่างรู้เท่าทัน ระมัดระวัง และตระหนักถึงความมั่นคงปลอดภัย มิฉะนั้นความสะดวกสบายอาจต้องแลกมาด้วยความเสี่ยงที่ไม่คุ้มค่าก็เป็นได้

บทที่ ๔
แนวทางการใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่ (Mobile Banking) ให้ปลอดภัย

ธนาคารในยุคใหม่ช่วยอำนวยความสะดวกสบายให้กับผู้ใช้บริการ สามารถทำธุรกรรมได้ทุกที่ ทุกเวลา แต่ผู้ใช้บริการก็ควรตระหนักถึงเรื่องความปลอดภัยด้วยทุกครั้งที่มีการทำธุรกรรม เพื่อป้องกันภัยอันตรายที่อาจแฝงตัวอยู่ในที่ต่างๆ บนโลกออนไลน์ โดยเริ่มจากการศึกษาขั้นตอนการใช้งานอย่างละเอียด เพื่อให้ทราบถึงวิธีการใช้งานที่ปลอดภัย และควรใช้งานด้วยความรอบคอบและระมัดระวังอยู่เสมอ ดังนี้

แนวทางการปฏิบัติสำหรับผู้ใช้งานสมาร์ตโฟน (Smartphone) เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย

การดูแลรักษาสมาร์ตโฟนอย่างใกล้ชิด

ผู้ใช้งานควรพึงระลึกไว้เสมอว่าความเสียหายที่เกิดขึ้นเมื่อมีการสูญหายหรือถูกขโมยสมาร์ตโฟนไปจะส่งผลกระทบทั้งในแง่ของทรัพย์สินและข้อมูลที่อยู่ในสมาร์ตโฟน ยิ่งมีการเก็บข้อมูลสำคัญไว้ในสมาร์ตโฟนมากเท่าใด ก็ยิ่งมีโอกาสก่อให้เกิดปัญหาตามมามากขึ้นเท่านั้น รวมถึงการเก็บข้อมูลที่เกี่ยวข้องกับองค์กร เช่น อีเมล (e - Mail) ซึ่งจะส่งผลกระทบต่อองค์กรโดยตรง ดังนั้น ผู้ใช้งานควรมีความรอบคอบและดูแลรักษาสมาร์ตโฟนอย่างใกล้ชิด

การตั้งค่าการล็อกสมาร์ตโฟนเมื่อไม่ใช้งาน

แม้ว่าการล็อกการใช้งานสมาร์ตโฟนจะไม่ได้เป็นการป้องกันการเข้าถึงข้อมูลที่ได้ผลร้อยเปอร์เซ็นต์ แต่ก็เป็นแนวทางเบื้องต้นในการชะลอหรือป้องกันการเข้าถึงข้อมูลสำคัญบนสมาร์ตโฟนจากผู้ไม่หวังดี ซึ่งอาจเกิดจากการถูกขโมยสมาร์ตโฟน และยังเป็นแนวทางที่ผู้ใช้งานสามารถทำได้โดยง่าย ซึ่งกระบวนการดังกล่าวสามารถทำได้โดยการตั้งค่า PIN หรือรหัสผ่าน (Password) บนสมาร์ตโฟนนั้น (วิธีการสามารถตรวจสอบได้จากเว็บไซต์ (Website) ผู้ผลิตสมาร์ตโฟน หรือสอบถามจากศูนย์บริการสมาร์ตโฟนที่ซื้อมา)

การสำรองข้อมูลจากสมาร์ตโฟนไว้ในแหล่งอื่นที่ปลอดภัย

การสำรองข้อมูลถือเป็นเรื่องสำคัญที่ต้องมีการปฏิบัติอยู่เสมอ เนื่องจากเมื่อเกิดเหตุฉุกเฉิน เช่น สมาร์ตโฟนสูญหาย สมาร์ตโฟนชำรุดหรือใช้งานไม่ได้ ปัญหาแรกที่จะตามมานอกจากการทำให้สมาร์ตโฟนกลับมาใช้งานได้ หรือหาสมาร์ตโฟนให้พบก็คือ การเข้าถึงข้อมูลบนสมาร์ตโฟน เช่น ข้อมูลผู้ติดต่อ (Contact Book) ซึ่งข้อดีของการสำรองข้อมูลก็คือ นอกจากจะมีข้อมูลที่สามารถใช้ได้เมื่อเกิดเหตุฉุกเฉินแล้ว ยังทำให้รู้ขอบเขตของข้อมูลที่สูญหายไปด้วย เช่น เก็บข้อมูลเลขที่บัญชีธนาคารและรหัสผ่านของระบบธุรกรรมทางอิเล็กทรอนิกส์ (e - Transaction) เอาไว้ ทำให้สามารถแจ้งระงับการเข้าใช้งานได้ก่อนจะเกิดความเสียหาย ซึ่งกระบวนการสำรองข้อมูลจากสมาร์ตโฟนแต่ละยี่ห้อหรือแต่ละรุ่นอาจแตกต่างกันไป (วิธีการสามารถตรวจสอบได้จากเว็บไซต์ผู้ผลิตสมาร์ตโฟน หรือสอบถามจากศูนย์บริการสมาร์ตโฟนที่ซื้อมา)

การเก็บเฉพาะข้อมูลที่จำเป็นไว้ในสมาร์ตโฟน

การเก็บข้อมูลบนสมาร์ตโฟนควรพิจารณาถึงความสำคัญและความเหมาะสมของข้อมูลที่จะจัดเก็บ ไม่ควรเก็บข้อมูลที่มีความสำคัญมาก เช่น ข้อมูลบัตรเครดิต ข้อมูลรหัสผ่านสำหรับล็อกอิน (Log in) เข้าใช้งานระบบ เนื่องจากหากสมาร์ตโฟนสูญหายหรือถูกมิจฉาชีพขโมยไป อาจทำให้เกิดความเสียหายที่รุนแรงมากกว่าเดิม แต่ในปัจจุบันผู้พัฒนาโปรแกรมบนระบบปฏิบัติการ (Operating System) สมาร์ตโฟนต่างๆ ได้พัฒนาโปรแกรมสำหรับเก็บข้อมูลส่วนบุคคลออกมามากมายและมีการรักษาความมั่นคงปลอดภัยของข้อมูล ทำให้ข้อมูลสำคัญนี้สามารถจัดเก็บบนสมาร์ตโฟนได้ เช่น ผู้พัฒนาโปรแกรมบนระบบปฏิบัติการ Symbian ได้พัฒนาโปรแกรมชื่อ Wallet ซึ่งมีวัตถุประสงค์เพื่อให้ผู้ใช้งานเก็บข้อมูลส่วนบุคคลต่างๆ ลงในสมาร์ตโฟนและมีการรักษาความมั่นคงปลอดภัยของข้อมูล โดยให้มีการล็อกอินก่อนผู้ใช้งานจะเข้าถึงข้อมูล

การปิดโหมดการเชื่อมต่อบลูทูธ (Bluetooth) หรือหลีกเลี่ยงการเชื่อมต่อบลูทูธจากแหล่งที่มาที่ไม่รู้จัก

ในปัจจุบันผู้ใช้งานมักจะมีการใช้งานการเชื่อมต่อบลูทูธบนสมาร์ตโฟนในหลายด้าน เช่น ใช้สำหรับการรับส่งไฟล์ระหว่างสมาร์ตโฟนกับเครื่องคอมพิวเตอร์ ใช้สำหรับเป็นโมเด็มเพื่อให้บริการอินเทอร์เน็ต (Internet) กับเครื่องคอมพิวเตอร์ที่เชื่อมต่อบลูทูธอยู่ ซึ่งหากเป็นการใช้งานตามปกติกับอุปกรณ์หรือบุคคลต่างๆ ที่รู้จัก และทราบถึงจุดประสงค์ในการใช้งานนั้นก็อาจไม่ก่อให้เกิดผลเสีย แต่ผลเสียจะเกิดก็ต่อเมื่อไม่ทราบว่าผู้ที่ต้องการเชื่อมต่อบลูทูธกับสมาร์ตโฟนนั้นเป็นใคร และมีจุดประสงค์ในการใช้งานอย่างไร เนื่องจากผู้ไม่หวังดีส่วนใหญ่มักจะอาศัยความรู้เท่าไม่ถึงการณ์ของผู้ใช้งานในการลักลอบใช้งานหรือดึงข้อมูลสำคัญบนสมาร์ตโฟน เช่น รูปภาพ ข้อความที่ส่งผ่านสมาร์ตโฟน (Short Message Service : SMS) ข้อดีของการใช้งานเครือข่ายบลูทูธก็คือ จะต้องได้รับการยินยอมให้มีการเชื่อมต่อบลูทูธก่อนจึงจะสามารถเชื่อมต่อได้ ซึ่งหากผู้ใช้งานมีความรู้เท่าทันผู้ไม่หวังดีก็จะทำให้การใช้งานสมาร์ตโฟนมีความมั่นคงปลอดภัยมากขึ้น โดยหากไม่มีการใช้งานก็ควรปิดโหมดการเชื่อมต่อบลูทูธไว้ เนื่องจากในบางครั้งพบว่าผู้ใช้งานไม่ได้ตั้งใจให้ยอมรับการเชื่อมต่อบลูทูธ แต่พลาดไปสัมผัสในขณะที่สมาร์ตโฟนอยู่ในกระเป๋า การปิดโหมดการเชื่อมต่อบลูทูธของสมาร์ตโฟนสามารถตรวจสอบได้จากเมนูการเชื่อมต่อ ซึ่งแต่ละยี่ห้อหรือแต่ละรุ่นอาจแตกต่างกันไป (วิธีการสามารถตรวจสอบได้จากเว็บไซต์ผู้ผลิตสมาร์ตโฟน หรือสอบถามจากศูนย์บริการสมาร์ตโฟนที่ซื้อมา)

การแจ้งผู้ให้บริการต่างๆ ที่เกี่ยวข้องเมื่อสมาร์ตโฟนสูญหาย

เมื่อพบว่าสมาร์ตโฟนสูญหายไม่ว่าจะด้วยกรณีถูกขโมยหรือทำตกหล่นที่ใดก็ตาม สิ่งแรกที่ผู้ใช้งานสมาร์ตโฟนควรทำก็คือ การแจ้งไปยังผู้ให้บริการต่างๆ เพื่อปิดบริการและป้องกันความเสียหายที่อาจจะเกิดขึ้น โดยขอบเขตการแจ้งปิดบริการตามรายการข้อมูลที่มีอยู่ในสมาร์ตโฟนนั้น เช่น แจ้งผู้ให้บริการสัญญาณโทรศัพท์ที่ใช้งานระงับสัญญาณโทรศัพท์ของตนเองชั่วคราวเพื่อป้องกันการใช้งาน ซึ่งหากมีการเก็บข้อมูลรหัสผ่านของระบบต่างๆ ไว้ในสมาร์ตโฟนก็ควรแจ้งปิดการใช้งานด้วย เช่น แจ้งปิดการใช้งานระบบธุรกรรมทางอิเล็กทรอนิกส์ชั่วคราว แจ้งผู้ดูแลระบบอีเมลขององค์กรเพื่อเปลี่ยนรหัสผ่าน

การเลือกติดตั้งโปรแกรมบนสมาร์ตโฟนเท่าที่จำเป็นและจากแหล่งที่มาที่น่าเชื่อถือ

แม้ว่าระบบปฏิบัติการบนสมาร์ตโฟนทั่วไปจะอนุญาตให้สามารถติดตั้งโปรแกรมเสริมเพื่ออำนวยความสะดวกในการใช้งานมากขึ้น แต่ก็มีความเสี่ยงที่ผู้ใช้งานจะพบกับโปรแกรมที่มีความสามารถในการขโมยข้อมูลหรือโปรแกรมอันไม่พึงประสงค์ต่างๆ ดังนั้น วิธีการป้องกันที่ดีที่สุดก็คือ ดาวน์โหลดเฉพาะโปรแกรมที่จำเป็น ดาวน์โหลดจากเว็บไซต์ของผู้พัฒนาเท่านั้น หรือจากแหล่งดาวน์โหลดที่ได้รับการควบคุมและรับรองความมั่นคงปลอดภัยจากผู้พัฒนา เช่น App Store สำหรับระบบปฏิบัติการ iOS, Android Market สำหรับระบบปฏิบัติการ Android

การควบคุมการเข้าถึงระบบต่างๆ ภายในองค์กรเมื่อมีการใช้งานผ่านสมาร์ตโฟน

องค์กรควรมีส่วนช่วยในการกำหนดขอบเขตการใช้งานหรือแนะนำแนวทางการปฏิบัติในการเข้าถึงระบบต่างๆ ภายในองค์กร เพื่อให้เกิดการรักษาความมั่นคงปลอดภัยในการใช้งานสมาร์ตโฟนอย่างเหมาะสม เช่น พัฒนาระบบการทำงานที่สามารถเข้าถึงได้จากสมาร์ตโฟนผ่านช่องทางการเข้ารหัสแบบ HTTPS (Hypertext Transfer Protocol Secure) จัดหาช่องทางการใช้งาน VPN (Virtual Private Network) เพื่อเชื่อมต่อเข้าระบบต่างๆ ภายในองค์กร

การพิจารณาลิงก์ที่อยู่บนเว็บไซต์ก่อนการคลิกทุกครั้ง

ภัยคุกคามที่เกิดขึ้นจากการใช้งานเว็บไซต์สามารถเกิดขึ้นได้ง่ายและส่งผลกระทบต่อผู้ใช้งานเป็นอย่างมาก เนื่องจากส่วนใหญ่เป็นการโจมตีโดยใช้เทคนิคทางจิตวิทยา ซึ่งไม่จำเป็นต้องใช้ความรู้ทางเทคนิคมากนัก ผู้ใช้งานส่วนใหญ่ที่ตกเป็นเหยื่อมักจะรู้ไม่เท่าทันวิธีการของผู้โจมตี ผู้โจมตีจะใช้เทคนิคต่างๆ หลอกล่อให้ผู้ใช้งานคลิกไปยังลิงก์เพื่อส่งต่อไปยังเว็บไซต์ที่มีอันตราย ดังนั้น วิธีการป้องกันที่ดีที่สุดก็คือการใช้วิจารณญาณก่อนคลิกไปยังลิงก์ต่างๆ

การอัปเดตระบบปฏิบัติการหรือโปรแกรมบนสมาร์ตโฟนให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

โดยปกติหากมีการดาวน์โหลดโปรแกรมจากผู้พัฒนาต่างๆ และโปรแกรมนั้นมีการปรับปรุงเกิดขึ้นก็จะมีการแจ้งอัปเดตโปรแกรมผ่านช่องทางต่างๆ เช่น อีเมล ผ่านระบบการแจ้งเตือนของระบบปฏิบัติการ เนื่องจากส่วนใหญ่การปรับปรุงเวอร์ชันใหม่ของโปรแกรมต่างๆ จะทำเพื่อปรับปรุงช่องโหว่หรือความผิดพลาดที่เกิดขึ้นในโปรแกรมเวอร์ชันเดิม ดังนั้น เมื่อผู้พัฒนามีการปรับปรุงเวอร์ชันของโปรแกรม ผู้ใช้งานก็ควรทำการอัปเดตโปรแกรมนั้นให้เป็นเวอร์ชันล่าสุดโดยทันที

การใช้สมาร์ตโฟนทำธุรกรรมทางอิเล็กทรอนิกส์อย่างระมัดระวัง

การใช้สมาร์ตโฟนในการทำธุรกรรมทางอิเล็กทรอนิกส์กับหน่วยงานทางการเงินที่ให้บริการผ่านเว็บไซต์ สร้างความสะดวกสบายให้กับผู้ใช้งานในการทำธุรกรรมเพิ่มมากขึ้น แต่การทำธุรกรรมทางอิเล็กทรอนิกส์ผ่านสมาร์ตโฟนควรเลือกผู้ให้บริการอินเทอร์เน็ตไร้สายที่มีความน่าเชื่อถือ ควรใช้งานในบริเวณที่ผู้ไม่หวังดีไม่สามารถแอบมองและขโมยข้อมูลส่วนบุคคลที่สำคัญ (Eavesdropping) ได้ เพราะหากผู้ใช้งานมองข้ามและเลือกใช้เครือข่ายที่ไม่น่าเชื่อถือ ก็อาจจะถูกโจรกรรมข้อมูลผ่านเครือข่ายได้

แนวทางการปฏิบัติสำหรับผู้ใช้งานสมาร์ตโฟน เพื่อให้มีความปลอดภัยในโลกออนไลน์

การป้องกันสมาร์ตโฟนให้ห่างไกลจากไวรัส (Virus) โทรจัน (Trojan) มัลแวร์ (Malware) หรือสปายแวร์ (Spyware)

- หลีกเลี่ยงการคลิกลิงก์ที่แนบมากับอีเมล เพื่อป้องกันไม่ให้คลิกเข้าสู่เว็บไซต์ปลอมที่ผู้ไม่หวังดีนั้นเตรียมไว้
- หลีกเลี่ยงการดาวน์โหลดและติดตั้งระบบปฏิบัติการหรือโปรแกรมที่ไม่มีลิขสิทธิ์ รวมทั้งข้อมูลจากเว็บไซต์ที่ไม่น่าเชื่อถือและไม่เชื่อมั่นในความปลอดภัย เพื่อป้องกันโทรจันหรือสปายแวร์ที่อาจแฝงอยู่ในโปรแกรม
- ติดตั้งซอฟต์แวร์ป้องกันไวรัส (Anti - Virus) ที่ถูกลิขสิทธิ์และเชื่อถือได้ รวมทั้งควรตรวจสอบโปรแกรมป้องกันไวรัสและทำการอัปเดตฐานข้อมูลไวรัสให้เป็นเวอร์ชันล่าสุดอยู่เสมอ เพื่อปิดช่องโหว่ที่ไวรัสหรือมัลแวร์อาจจะใช้เป็นช่องทางบุกรุกเข้าสู่ระบบ
- หากต้องการทำธุรกรรมทางการเงินให้ใช้สมาร์ตโฟนของตนเอง และระมัดระวังการเชื่อมต่อกับเครือข่ายไร้สาย (Wi-Fi) สาธารณะหรือเครือข่ายที่ไม่ปลอดภัย เช่น ร้านอินเทอร์เน็ตคาเฟ่ เพราะอาจเชื่อมต่อกับเครือข่ายไร้สายปลอมที่มิจฉาชีพสร้างขึ้นมา

การสังเกตอีเมลปลอม

- พิจารณาชื่อบัญชีอีเมล (e - Mail Address) ว่าเป็นขององค์กรหรือเจ้าหน้าที่ขององค์กรจริงหรือไม่ หากเป็นขององค์กรหรือเจ้าหน้าที่ขององค์กรจริง ชื่อบัญชีอีเมลมักต่อท้ายด้วยชื่อย่อขององค์กรนั้น เช่น xxx@mict.go.th เป็นบัญชีอีเมลของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยย่อมาจาก Ministry of Information and Communication Technology แต่ควรตรวจสอบควบคู่ไปกับลิงก์ที่แนบมากับอีเมลด้วย
- เข้าสู่เว็บไซต์ด้วยการพิมพ์ที่อยู่ (Uniform Resource Locator : URL) โดยตรงด้วยตนเองทุกครั้งที่ต้องการใช้บริการธนาคารทางโทรศัพท์เคลื่อนที่ และตรวจสอบชื่อเว็บไซต์ในช่อง Address ให้แน่ใจก่อนล็อกอิน เพื่อให้มั่นใจว่าได้เข้าสู่เว็บไซต์นั้นอย่างแท้จริง
- ตรวจสอบลิงก์ของเว็บไซต์ว่าที่อยู่ที่ให้เชื่อมโยงไปนั้นเป็นเว็บไซต์ที่ใช้บริการอยู่เป็นประจำหรือไม่ หากเป็นเว็บไซต์ระบบธนาคารทางโทรศัพท์เคลื่อนที่จะต้องมี s ต่อท้าย ซึ่ง https:// หมายถึงมีการเข้ารหัสความปลอดภัย แต่หากไม่มี s ต่อท้าย ให้สงสัยว่าเป็นอีเมลแอบอ้าง นอกจากนี้ หากเป็นการทำธุรกรรมทางการเงิน สถาบันการเงินไม่มีนโยบายในการส่งลิงก์ของเว็บไซต์ถึงผู้ใช้บริการผ่านอีเมล หากมีอีเมลแจ้งให้เชื่อมโยงเข้าสู่เว็บไซต์เพื่อทำธุรกรรมทางการเงิน ให้สงสัยว่าเป็นอีเมลแอบอ้าง

เมื่อได้รับอีเมลหลอกลวง พบเว็บไซต์ปลอม (Phishing Website) หรือได้กรอกข้อมูลไปในเว็บไซต์ปลอมแล้ว ควรติดต่อไปยังหน่วยงาน Call Center ของบริษัท ธนาคาร หรือสถาบันการเงินนั้นโดยเร็วที่สุด เพื่อทำการเปลี่ยนรหัสผ่านหรืออายัดบัญชี เนื่องจากบริษัท ธนาคาร หรือสถาบันการเงินไม่มีนโยบายส่งอีเมลที่มีลิงก์ให้คลิกเพื่อเข้าสู่ระบบต่างๆ ของธนาคาร หรือสอบถามข้อมูลส่วนบุคคลผ่านอีเมล หากต้องการเข้าสู่บริการหรือระบบต่างๆ จะต้องพิมพ์ที่อยู่เพื่อเข้าสู่เว็บไซต์ด้วยตนเอง หรือเข้าจาก Favorite/Bookmark ที่สร้างขึ้นด้วยตนเองเท่านั้น

ระมัดระวังไม่หลงเชื่อข้อความที่ได้รับในอีเมลหรือโทรศัพท์ หากมีการอ้างว่าได้ส่งหรือติดต่อมาจากบริษัท ธนาคาร หรือสถาบันการเงินใดก็ตาม ควรค้นหาเบอร์โทรศัพท์ของหน่วยงานที่ติดต่อมาหรือติดต่อไปยัง Call Center ของหน่วยงานนั้น (อย่าติดต่อไปยังเบอร์โทรศัพท์ที่มีอยู่ในอีเมลต้องสงสัยนั้น) เพื่อทำการตรวจสอบว่ามีการส่งอีเมลลักษณะดังกล่าวจริงหรือไม่ หากมีข้อสงสัยสามารถสอบถามได้ที่ศูนย์ประสานงานแก้ไขปัญหาการปล่อยสินเชื่อ (ศปส.) ธนาคารแห่งประเทศไทย เบอร์โทรศัพท์ ๐ ๒๒๘๓ ๕๙๐๐ ในวันและเวลาทำการ

ควรลบอีเมลที่สงสัยว่าจะมีไวรัสแนบมา อีเมลขยะ อีเมลลูกโซ่ หรืออีเมลล่อลวงทิ้งทันที อย่าตอบกลับอีเมลใดก็ตามที่ขอให้เปิดเผยข้อมูลส่วนบุคคล และไม่ควรรันไฟล์ที่แนบมากับอีเมลที่ส่งมาจากบุคคลที่ไม่รู้จักหรือไม่ทราบที่มาแน่ชัด ตลอดจนไฟล์ที่ส่งด้วยโปรแกรมแชต (Chat) ต่างๆ

การสังเกตเว็บไซต์ปลอม

สังเกต “สัญลักษณ์รูปกุญแจ” เพราะระบบธนาคารทางโทรศัพท์เคลื่อนที่จะต้องมีการเข้ารหัสความปลอดภัยที่หน้าเว็บไซต์ล็อกอิน โดยสัญลักษณ์รูปกุญแจจะแสดงในส่วนของเว็บเบราว์เซอร์ (Web Browser) ซึ่งตำแหน่งของสัญลักษณ์รูปกุญแจอาจแตกต่างกันไปตามประเภทของเว็บเบราว์เซอร์

สังเกต “URL” ของเว็บไซต์ระบบธนาคารทางโทรศัพท์เคลื่อนที่ว่ามีการเข้ารหัสความปลอดภัย โดยขึ้นต้นด้วย https:// หรือไม่ หากพบว่าเว็บไซต์ระบบธนาคารทางโทรศัพท์เคลื่อนที่ (หน้าล็อกอิน) ขึ้นต้นด้วย http:// (ไม่มี s ต่อท้าย) ให้สงสัยว่าเป็นเว็บไซต์ปลอม

สังเกต “ชื่อผู้ให้บริการ” ว่าจดทะเบียนภายใต้ชื่อสถาบันการเงินใด โดยสังเกตได้จากตัวอักษรที่อยู่ถัดจากสัญลักษณ์รูปกุญแจ หรือโดยการคลิกที่สัญลักษณ์รูปกุญแจก็จะเห็นชื่อสถาบันการเงินซึ่งสามารถตรวจสอบได้ว่าเป็นชื่อของสถาบันการเงินที่ใช้บริการอยู่หรือไม่

หากพบความผิดปกติของหน้าจอขณะทำรายการผ่านบริการธนาคารทางโทรศัพท์เคลื่อนที่ ให้หยุดทำรายการทันที ไม่ต้องปฏิบัติตามคำแนะนำใดทั้งสิ้น และให้ออกจากเว็บไซต์ที่น่าสงสัยทันที

การใช้รหัสผ่านชั่วคราว OTP (One Time Password) หรือ TOP (Time Out Password)

อ่านข้อความที่ได้รับแจ้งพร้อมรหัสผ่านชั่วคราวจากข้อความที่ส่งผ่านสมาร์ตโฟนว่ารหัสดังกล่าวใช้ยืนยันการทำธุรกรรมใด หากพบว่าธุรกรรมที่ต้องยืนยันไม่ตรงกับธุรกรรมที่ต้องการทำให้ออกจากระบบธนาคารทางโทรศัพท์เคลื่อนที่ และติดต่อเจ้าหน้าที่ Call Center ของธนาคารเพื่อปรึกษาวิธีการใช้งานที่ปลอดภัยต่อไป

การเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

คำแนะนำเกี่ยวกับการตั้งรหัสผ่าน

- ไม่ใช้คำที่มีอยู่ในพจนานุกรม ไม่ว่าจะเป็นพจนานุกรมภาษาใดก็ตาม รวมทั้งคำศัพท์ทางวิทยาศาสตร์ด้วย
- ไม่ใช้คำที่สะกดกลับด้าน ซึ่งเป็นคำที่มาจากพจนานุกรม เช่น flower สะกดกลับด้านเป็น rewolf
- ไม่ใช้คำที่เกี่ยวข้องกับตนเอง เช่น ที่อยู่ เบอร์โทรศัพท์ วันเกิด ชื่อเล่น ชื่อสัตว์เลี้ยง งานอดิเรก กีฬาที่ชอบ
- ไม่ใช้ตัวอักษรหรือตัวเลขที่เรียงกัน เช่น abcdef, 123456
- ไม่ใช้ตัวอักษรที่เรียงกันตามคีย์บอร์ด เช่น qwerty
- ให้ใช้ตัวอักษร ตัวเลข และตัวอักษรพิเศษร่วมกันแบบสุ่ม
- ให้ใช้ตัวอักษร ทั้งตัวพิมพ์เล็กและตัวพิมพ์ใหญ่ในภาษาอังกฤษ และให้ใช้ตัวอักษรพิเศษร่วมด้วย เช่น * @ #
- ให้ใช้รหัสผ่านที่มีความยาวอย่างน้อย ๖ ตัว ยิ่งรหัสผ่านมีความยาวมากเท่าใดก็ยิ่งมีความยากต่อการคาดเดามากขึ้นเท่านั้น
- ไม่จดรหัสผ่านเก็บไว้ ไม่ว่าจะในที่ใดก็ตาม และให้ระมัดระวังบุคคลรอบข้าง ซึ่งอาจจะแอบมองเพื่อขโมยบัญชีผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนตัวอื่นๆ ในขณะที่ผู้ใช้งานกำลังกรอกข้อมูลนั้นเข้าสู่ระบบ
- ไม่บอกรหัสผ่านกับบุคคลอื่น ไม่ว่าจะด้วยเหตุผลใดก็ตาม
- ไม่ใช้ตัวเลือกในการจำรหัสผ่านที่มีอยู่ในเว็บไซต์หรือโปรแกรมที่ใช้งาน และให้ปิดความสามารถนี้ในเว็บเบราว์เซอร์ที่ใช้งาน โดยคลิกตัวเลือกการจำรหัสผ่านออก
- ไม่ใช้รหัสผ่านเดียวกัน เพื่อเข้าใช้งานโปรแกรมต่างๆ

การป้องกันการถูกแอบอ้างเข้าใช้งานธนาคารทางโทรศัพท์เคลื่อนที่

เมื่อเสร็จการใช้งานในแต่ละครั้งควรล้างหน่วยความจำคอมพิวเตอร์ (Cache) และล้างบันทึกประวัติการใช้งาน (History Settings) ในเว็บเบราว์เซอร์ เพื่อลบข้อมูลบัญชีทั้งหมด ลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลได้ และทำการล็อกเอาต์ (Log out) ปิดเว็บเบราว์เซอร์ทั้งหมดทุกครั้ง อย่าวางสมาร์ตโฟนทิ้งไว้หากยังทำธุรกรรมทางการเงินไม่แล้วเสร็จ

ไม่ให้ข้อมูลส่วนบุคคล เช่น เลขที่บัญชีธนาคาร หมายเลขบัตรเครดิต รหัสผ่านต่างๆ กับบุคคลอื่น เพราะอาจถูกนำไปใช้แอบอ้างในการทำธุรกรรมทางการเงินได้

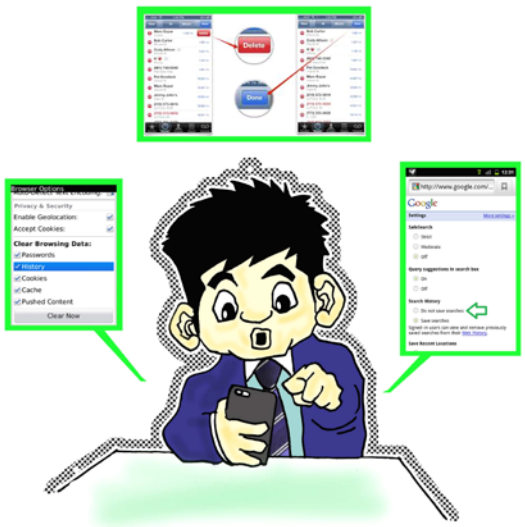
ไม่เปิดเผยข้อมูลส่วนบุคคล เช่น รหัสประจำตัว (User ID) รหัสผ่าน รหัส ATM เลขที่บัญชีธนาคาร หมายเลขบัตรเครดิต หมายเลขประจำตัวประชาชน ที่อยู่ เบอร์โทรศัพท์ วันเกิด ผ่านอีเมล หรือในระหว่างทำรายการผ่านบริการของธนาคาร เนื่องจากธนาคารไม่มีนโยบายในการดำเนินการสอบถามข้อมูลส่วนบุคคลของผู้ใช้บริการผ่านช่องทางดังกล่าว

หมั่นตรวจสอบข้อมูลความถูกต้องของการทำรายการธุรกรรมและบัญชีธนาคารทางโทรศัพท์เคลื่อนที่อย่างสม่ำเสมอ โดยไม่จำเป็นต้องรอให้ครบ ๑ เดือน และตรวจสอบยอดเงินในบัญชีของผู้ใช้บริการอย่างสม่ำเสมอ เพื่อป้องกันรายการผิดปกติที่อาจจะเกิดขึ้น รวมทั้งตรวจสอบใบแจ้งรายการใช้บัตรเครดิตทุกครั้งที่ได้รับ และตรวจสอบให้แน่ใจว่าไม่มีรายการธุรกรรมแปลกปลอม หากพบรายการที่น่าสงสัย ควรติดต่อธนาคารหรือบริษัทผู้ออกบัตรเครดิตนั้นทันที

หมั่นตรวจสอบข้อความการแจ้งเตือนต่างๆ ที่ธนาคารส่งให้ทางอีเมลและข้อความที่ส่งผ่านสมาร์ตโฟนอย่างถี่ถ้วน เพื่อให้ทราบถึงความเคลื่อนไหวในบัญชีและการทำธุรกรรมต่างๆ หากพบความผิดปกติ เช่น เลขที่บัญชีที่ปรากฏในข้อความไม่ตรงกับเลขที่บัญชีที่ต้องการลงทะเบียน ได้รับข้อความการแจ้งเตือนทางอีเมลโดยที่ไม่ได้เข้าใช้งาน ควรติดต่อธนาคารหรือสถาบันการเงินนั้นทันที

การติดตามข่าวสารกลโกงและภัยทางการเงิน

ติดตามข่าวสารกลโกงและภัยทางการเงินอย่างสม่ำเสมอ ทั้งจากเว็บไซต์ของธนาคารแห่งประเทศไทย เว็บไซต์ของสถาบันการเงินต่างๆ หรือสื่อสิ่งพิมพ์ต่างๆ เพื่อป้องกันภัยทางการเงินที่อาจจะเกิดขึ้น



บทที่ ๕
กฎหมายที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ (e - Transaction) ของประเทศไทย

ด้วยเทคโนโลยีสารสนเทศมีบทบาทสำคัญอย่างยิ่งต่อชีวิตประจำวันของประชาชน และเป็นปัจจัยสำคัญที่จะเสริมสร้างและสนับสนุนความแข็งแกร่งทางธุรกิจ อุตสาหกรรม และการค้าระหว่างประเทศ รวมทั้งเป็นเครื่องมือที่มีประสิทธิภาพในการพัฒนาสังคมและคุณภาพชีวิต การพัฒนาทรัพยากรมนุษย์ และการพัฒนาระบบสารสนเทศภาครัฐเพื่อประสิทธิภาพในการให้บริการที่ดีขึ้น ซึ่งกฎหมายที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ มีดังนี้

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

มีเจตนารมณ์เพื่อรองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เทียบเท่ากับการทำเป็นหนังสือหรือหลักฐานเป็นหนังสือ การรองรับวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ (e - Signature) ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ การรองรับผลทางกฎหมายเกี่ยวกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ และการห้ามปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์ในฐานะพยานหลักฐานทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือและมีผลทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปซึ่งเคยปฏิบัติอยู่เดิม

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

มีวัตถุประสงค์เพื่อรองรับในเรื่องตราประทับอิเล็กทรอนิกส์ และบทบัญญัติที่กำหนดให้สามารถนำเอกสารซึ่งเป็นสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์มาใช้แทนต้นฉบับหรือใช้เป็นพยานหลักฐานในศาลได้ รวมทั้งเพื่อให้มีหน่วยงานธุรการทำหน้าที่กำกับดูแลและเป็นฝ่ายเลขานุการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงสมควรจัดตั้งสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สังกัดสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารขึ้น

ประกาศภายใต้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ มีดังนี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. ๒๕๕๒

เพื่อให้การให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์มีความน่าเชื่อถือ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล โดยอ้างอิงกรอบหรือแนวทางในการทำแนวนโยบายและแนวปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่เรียกว่า Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

เพื่อให้การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์มีรูปแบบที่เหมาะสม เป็นไปตามหลักเกณฑ์และวิธีการที่กำหนด

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง การรับรองสิ่งพิมพ์ออก พ.ศ. ๒๕๕๕

เพื่อให้มีหน่วยงานรับรองสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ ให้สิ่งพิมพ์ออกสามารถใช้อ้างอิงแทนข้อมูลอิเล็กทรอนิกส์ และมีผลใช้แทนต้นฉบับได้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หน่วยงานรับรองสิ่งพิมพ์ออก พ.ศ. ๒๕๕๕

เพื่อประกาศให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) เป็นหน่วยงานรับรองสิ่งพิมพ์ออก

พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ พ.ศ. ๒๕๔๙

แม้ว่าพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ได้บัญญัติรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ให้เท่าเทียมกับธุรกรรมที่ทำบนกระดาษและการลงลายมือชื่อไว้แล้วก็ตาม แต่เนื่องจากการทำธุรกรรมบางประเภทที่เกี่ยวกับครอบครัวและมรดกยังไม่เหมาะสมที่จะให้กระทำได้ด้วยวิธีการทางอิเล็กทรอนิกส์ จึงสมควรยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ ด้วยเหตุผลที่ว่าธุรกรรมทั้งสองประเภทเป็นเรื่องที่มีความละเอียดอ่อนทางอารมณ์และความรู้สึก ซึ่งเกี่ยวข้องกับความสัมพันธ์ในครอบครัว อันเป็นสถาบันพื้นฐานของสังคมไทย

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

เนื่องจากประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศ ซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น จึงสมควรสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตน โดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์

ประกาศภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มีดังนี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล จึงมีการกำหนดแนวทางและตัวอย่างเบื้องต้นให้หน่วยงานของรัฐใช้เป็นกรอบในการจัดทำนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

เพื่อให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

เพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลของประชาชน ในกรณีที่หน่วยงานของรัฐได้ให้บริการหรือดำเนินกิจกรรมใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ และได้มีการรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลหรือข้อเท็จจริงที่ทำให้สามารถระบุตัวประชาชนได้ ไม่ว่าโดยตรงหรือโดยอ้อม จึงมีการกำหนดแนวทางและตัวอย่างเบื้องต้นให้หน่วยงานของรัฐใช้เป็นกรอบในการจัดทำนโยบายและข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์

พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

ในปัจจุบันเทคโนโลยีอิเล็กทรอนิกส์มีความก้าวหน้ามากขึ้น ซึ่งธุรกิจบริการเกี่ยวกับการชำระเงินทางอิเล็กทรอนิกส์ (e - Payment) เป็นธุรกิจที่ต้องใช้เทคโนโลยีอิเล็กทรอนิกส์ที่มีความซับซ้อนและหลากหลาย และเป็นธุรกิจที่มีมูลค่าโดยรวมทางเศรษฐกิจค่อนข้างสูงและมีการขยายตัวเพิ่มขึ้นอย่างรวดเร็ว นอกจากนี้ ผู้ให้บริการในธุรกิจการชำระเงินทางอิเล็กทรอนิกส์ในขณะนี้มิได้มีเพียงสถาบันการเงินเท่านั้น แต่ยังรวมถึงผู้ให้บริการที่มิได้มีกฎหมายใดควบคุมดูแล จึงอาจส่งผลกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ ความน่าเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์ และอาจก่อให้เกิดความเสียหายต่อสาธารณชน ประกอบกับเพื่อบูรณาการกฎหมายที่เกี่ยวข้องกับธุรกิจบริการเกี่ยวกับการชำระเงินทางอิเล็กทรอนิกส์ให้เป็นฉบับเดียวกัน อันจะช่วยก่อให้เกิดประสิทธิภาพในการควบคุมดูแลและเป็นมาตรการสำคัญประการหนึ่งในการส่งเสริมการใช้บริการการชำระเงินทางอิเล็กทรอนิกส์มากขึ้น รวมทั้งเป็นการเพิ่มศักยภาพในการแข่งขันของภาคธุรกิจหรือการให้บริการภาครัฐ

ประกาศภายใต้พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ มีดังนี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๒

เพื่อกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ให้ผู้ให้บริการถือปฏิบัติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๕

เพื่อรักษาความมั่นคงทางการเงิน และลดต้นทุนในการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ตลอดจนเพื่อประโยชน์ต่อการเข้าไปกำกับดูแลของธนาคารแห่งประเทศไทย

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์การพิจารณาลงโทษปรับทางปกครองสำหรับผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๔

เพื่อกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการพิจารณาลงโทษปรับทางปกครอง

ประกาศธนาคารแห่งประเทศไทย ที่ สรข. ๑/๒๕๕๒ เรื่อง การให้บริการเงินอิเล็กทรอนิกส์ตามบัญชี ก ที่ไม่ต้องแจ้งให้ทราบก่อนให้บริการ

เพื่อกำหนดประเภทของการให้บริการเงินอิเล็กทรอนิกส์ (e - Money) ซึ่งใช้ซื้อสินค้าหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขายหรือผู้ให้บริการเพียงรายเดียวที่ไม่ต้องแจ้งให้ทราบก่อนให้บริการ

ประกาศธนาคารแห่งประเทศไทย ที่ สรข. ๒/๒๕๕๒ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

เพื่อประโยชน์ในการควบคุมดูแลการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ ให้เกิดความมั่นคงทางการเงินและการพาณิชย์ เกิดความน่าเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์ และป้องกันไม่ให้เกิดความเสียหายต่อสาธารณชน

ประกาศธนาคารแห่งประเทศไทย ที่ สรข. ๓/๒๕๕๒ เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์

เพื่อให้มีมาตรฐานในการกำหนดนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ และใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ มีความมั่นคงปลอดภัย และสามารถให้บริการได้อย่างต่อเนื่อง

ประกาศธนาคารแห่งประเทศไทย ที่ สรข. ๔/๒๕๕๒ เรื่อง การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

เพื่อแต่งตั้งพนักงานธนาคารแห่งประเทศไทยเป็นพนักงานเจ้าหน้าที่

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

เนื่องจากในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญต่อการดำเนินการของทั้งภาครัฐและภาคเอกชน โดยมีการทำธุรกรรมทางอิเล็กทรอนิกส์กันอย่างแพร่หลาย จึงสมควรส่งเสริมให้มีการบริหารจัดการและรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้มีการยอมรับและเชื่อมั่นในข้อมูลอิเล็กทรอนิกส์มากยิ่งขึ้น

ประกาศภายใต้พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ มีดังนี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดแล้ว ให้ถือว่าเป็นวิธีการที่เชื่อถือได้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดแล้ว ให้ถือว่าเป็นวิธีการที่เชื่อถือได้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน จึงสมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว ซึ่งในพระราชบัญญัตินี้มีมาตราที่สำคัญ ดังนี้

มาตรา ๕

ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖

ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗

ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๘

ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙

ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐

ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑

ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

ประกาศภายใต้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีดังนี้

กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. ๒๕๕๑

เพื่อบัญญัติให้หนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์เป็นไปตามที่กำหนดในกฎกระทรวง

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดี อันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่มีความชัดเจนและเป็นไปอย่างมีประสิทธิภาพ

ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

เพื่อให้พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนมีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษและมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ภาคผนวก

นิยามศัพท์

ธนาคารอิเล็กทรอนิกส์ (Electronic Banking)

การประกอบธุรกิจการพาณิชย์อิเล็กทรอนิกส์เกี่ยวกับการให้บริการการทำธุรกรรมทางการเงินต่างๆ ผ่านอุปกรณ์หรือระบบอิเล็กทรอนิกส์ เช่น โทรศัพท์เคลื่อนที่ อินเทอร์เน็ต (Internet) โดยมีการให้บริการต่างๆ เช่น การฝากเงิน ถอนเงิน โอนเงิน สอบถามยอดเงิน

ธนาคารทางอินเทอร์เน็ต (Internet Banking)

การให้บริการการทำธุรกรรมทางการเงินต่างๆ ของธนาคารที่ทำได้ทุกที่ ทุกเวลา ผ่านระบบอินเทอร์เน็ต โดยอาศัยอุปกรณ์อิเล็กทรอนิกส์ต่างๆ เช่น เครื่องคอมพิวเตอร์ โทรศัพท์เคลื่อนที่ สื่ออื่นๆ ที่ช่วยให้ผู้ใช้บริการสามารถทำรายการทางการเงินในลักษณะโต้ตอบกับระบบงานของธนาคารได้เองโดยอัตโนมัติ

ธนาคารทางโทรศัพท์เคลื่อนที่ (Mobile Banking)

การทำธุรกรรมทางการเงินด้วยตนเองผ่านโทรศัพท์เคลื่อนที่ในลักษณะโต้ตอบกับระบบงานของธนาคารได้เองโดยอัตโนมัติ และสามารถใช้บริการได้ตลอดเวลาที่ต้องการ

สมาร์ตโฟน (Smartphone)

โทรศัพท์เคลื่อนที่ที่มีความสามารถเพิ่มเติมนอกเหนือจากโทรศัพท์เคลื่อนที่ทั่วไป สมาร์ตโฟนถูกมองว่าเป็นคอมพิวเตอร์พกพาที่ทำงานในลักษณะของโทรศัพท์เคลื่อนที่ โดยสามารถเชื่อมต่อความสามารถหลักของโทรศัพท์เคลื่อนที่เข้ากับแอปพลิเคชัน (Application) ของโทรศัพท์เคลื่อนที่ได้เอง ผู้ใช้งานสมาร์ตโฟนสามารถติดตั้งโปรแกรมเสริมเพื่อเพิ่มความสามารถของโทรศัพท์เคลื่อนที่ได้ด้วยตนเอง โดยรูปแบบจะขึ้นอยู่กับแพลตฟอร์ม (Platform) และระบบปฏิบัติการ (Operating System) ของโทรศัพท์เคลื่อนที่นั้น

บรรณานุกรม

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และคณะ. (ร่าง) แผนแม่บทเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทย พ.ศ. ๒๕๕๖ - ๒๕๖๐. กรุงเทพมหานคร : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ๒๕๕๖.

คณะกรรมการบริหารสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และคณะ. รายงานสถิติการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทย พ.ศ. ๒๕๕๕. กรุงเทพมหานคร : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ๒๕๕๕.

ความปลอดภัยในการใช้ Mobile Banking มั่นใจได้หรือ?. [ออนไลน์]. เข้าถึงได้จาก : http://www.buddybe.com/index.php?lay=show&ac=article&Id=128. (วันที่ค้นข้อมูล : ๒๒ มกราคม ๒๕๕๗)

ชัยชนะ มิตรพันธ์ และคณะ. บทความเผยแพร่ Cyber Security Articles 2012 โดย ThaiCERT. พิมพ์ครั้งที่ ๑. กรุงเทพมหานคร : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ๒๕๕๖.

ธนาคารทหารไทย จำกัด (มหาชน). บริการอิเล็กทรอนิกส์แบงก์กิ้ง ทีเอ็มบี M - Banking. [ออนไลน์]. เข้าถึงได้จาก : https://www.tmbbank.com/personal/e-banking/mobile-banking.php. (วันที่ค้นข้อมูล : ๑๙ กุมภาพันธ์ ๒๕๕๗)

ธนาคารสแตนดาร์ดชาร์เตอร์ด. บริการธนาคารทางโทรศัพท์เคลื่อนที่. [ออนไลน์]. เข้าถึงได้จาก : https://www.sc.com/th/ways-to-bank/mobile-banking.html. (วันที่ค้นข้อมูล : ๖ กุมภาพันธ์ ๒๕๕๗)

ธนาคารแห่งประเทศไทย. ธุรกรรมการชำระเงินผ่านบริการ Mobile banking และ Internet banking. [ออนไลน์]. เข้าถึงได้จาก : http://www2.bot.or.th/statistics/ReportPage.aspx?reportID=688&language=th. (วันที่ค้นข้อมูล : ๒๐ มีนาคม ๒๕๕๘)

ธนาคารแห่งประเทศไทย. ปริมาณการชำระเงินผ่านระบบการชำระเงินและช่องทางต่างๆ. [ออนไลน์]. เข้าถึงได้จาก : http://www2.bot.or.th/statistics/BOTWEBSTAT.aspx?reportID=681&language=TH. (วันที่ค้นข้อมูล : ๒๐ มีนาคม ๒๕๕๘)

ธนาคารแห่งประเทศไทย. มูลค่าการชำระเงินผ่านระบบการชำระเงินและช่องทางต่างๆ. [ออนไลน์]. เข้าถึงได้จาก : http://www2.bot.or.th/statistics/BOTWEBSTAT.aspx?reportID=682&language=TH. (วันที่ค้นข้อมูล : ๒๐ มีนาคม ๒๕๕๘)

บรรณานุกรม (ต่อ)

ธนาคารแห่งประเทศไทย. รอบรู้บริการทางการเงิน. [ออนไลน์]. เข้าถึงได้จาก : http://www.bot.or.th/Thai/FinancialInstitutions/PopularConner/FIservice/Pages/FinServices.aspx. (วันที่ค้นข้อมูล : ๖ กุมภาพันธ์ ๒๕๕๗)

วิกิพีเดีย สารานุกรมเสรี. ธนาคารอิเล็กทรอนิกส์. [ออนไลน์]. เข้าถึงได้จาก : http://th.wikipedia.org/wiki/ธนาคารอิเล็กทรอนิกส์. (วันที่ค้นข้อมูล : ๖ กุมภาพันธ์ ๒๕๕๗)

วิกิพีเดีย สารานุกรมเสรี. สมาร์ตโฟน. [ออนไลน์]. เข้าถึงได้จาก : http://th.wikipedia.org/wiki/สมาร์ตโฟน. (วันที่ค้นข้อมูล : ๓ กุมภาพันธ์ ๒๕๕๗)

ศศิวิมล มณีเหล็ก. ทัศนคติและความพึงพอใจในการใช้บริการ K - Mobile Banking Plus ของบุคลากรและนักศึกษา มหาวิทยาลัยเชียงใหม่. วิทยานิพนธ์เศรษฐศาสตรมหาบัณฑิต มหาวิทยาลัยเชียงใหม่, ๒๕๕๔.

ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย. ธนาคารออนไลน์ ใช้งานอย่างไรให้ปลอดภัย. [ออนไลน์]. เข้าถึงได้จาก : http://www.bot.or.th/Thai/FinancialLiteracy/Documents/ธนาคารออนไลน์ใช้อย่างไรให้ปลอดภัย.pdf. (วันที่ค้นข้อมูล : ๕ กุมภาพันธ์ ๒๕๕๗)

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. คู่มือการใช้งานเครือข่ายอินเทอร์เน็ตอย่างปลอดภัยสำหรับผู้ใช้งานทั่วไป. พิมพ์ครั้งที่ ๑. กรุงเทพมหานคร : สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, ๒๕๔๘.

ศูนย์บริหารจัดการความเสี่ยง มหาวิทยาลัยมหิดล. ระวังโจรออนไลน์ล้วงกระเป๋า. [ออนไลน์]. เข้าถึงได้จาก : http://www.op.mahidol.ac.th/orau/index.php/articles/60-Risk-Poster/165-Bandit_Online.html. (วันที่ค้นข้อมูล : ๕ กุมภาพันธ์ ๒๕๕๗)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย และคณะ. Thailand Computer Emergency Response Team Annual Report. พิมพ์ครั้งที่ ๒. กรุงเทพมหานคร : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ๒๕๕๖.

สุรางคณา วายุภาพ และคณะ. ฉลาดรู้เน็ต. พิมพ์ครั้งที่ ๒. กรุงเทพมหานคร : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ๒๕๕๕.

บรรณานุกรม (ต่อ)

สำนักกิจการระหว่างประเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอาเซียน ปี ๒๕๕๘. พิมพ์ครั้งที่ ๒. กรุงเทพมหานคร : บริษัท อัพทรูยู ครีเอทนิว จำกัด, ๒๕๕๕.

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ผู้รวบรวม. รวมกฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์และกฎหมายที่เกี่ยวข้อง. พิมพ์ครั้งที่ ๔. กรุงเทพมหานคร : บริษัท ศูนย์การพิมพ์แก่นจันทร์ จำกัด, ๒๕๕๖.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). E - Banking คืออะไร?. [ออนไลน์]. เข้าถึงได้จาก : http://www.etda.or.th/etda_website/mains/display/1238. (วันที่ค้นข้อมูล : ๖ กุมภาพันธ์ ๒๕๕๗)

สำนักนโยบายและส่งเสริมธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี ๒๕๕๖. พิมพ์ครั้งที่ ๑. กรุงเทพมหานคร : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ๒๕๕๖.

ACIS Professional Center. รายงานผลการวิจัยมาตรการรักษาความมั่นคงปลอดภัยระบบ Internet Banking และระบบ Mobile Banking ของธนาคารในประเทศไทย โดย ACIS Research LAB - Information Security Research on Thailand's Internet Banking/Mobile Banking. [ออนไลน์]. เข้าถึงได้จาก : http://www.acisonline.net/article/?p=34. (วันที่ค้นข้อมูล : ๙ กุมภาพันธ์ ๒๕๕๗)

ASTV ผู้จัดการออนไลน์. "กสทช. - DSI" ชี้ทำธุรกรรมผ่านมือถือระวังสูญเงิน! เผย 2 ช่องทางแก๊งโจรใช้ดูดเงิน - แนะวิธีไม่ตกเป็นเหยื่อ. [ออนไลน์]. เข้าถึงได้จาก : http://www.manager.co.th/Home/ViewNews.aspx?NewsID=9550000129868. (วันที่ค้นข้อมูล : ๒๗ มกราคม ๒๕๕๗)

Internet Banking. [ออนไลน์]. เข้าถึงได้จาก : http://forest25.blogspot.com/2010/08/internet-banking.html. (วันที่ค้นข้อมูล : ๖ กุมภาพันธ์ ๒๕๕๗)

Mobile Banking. [ออนไลน์]. เข้าถึงได้จาก : http://r70.wikidot.com/group5. (วันที่ค้นข้อมูล : ๒๒ มกราคม ๒๕๕๗)

SiamPhone. สมาร์ทโฟนคืออะไร? แท็บเล็ต - แฟบเล็ต ต่างกันอย่างไร?. [ออนไลน์]. เข้าถึงได้จาก : http://news.siamphone.com/news-14121.html. (วันที่ค้นข้อมูล : ๓ กุมภาพันธ์ ๒๕๕๗)

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติฯ อาคารรัฐประศาสนภักดี ชั้น ๖
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๘๕-๙๙
โทรสาร ๐ ๒๑๔๓ ๘๐๓๖-๓๗
เว็บไซต์กระทรวง : http://www.mict.go.th
เว็บไซต์สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ : http://www.etcommission.go.th