ฉลาดรู้เน็ต 3

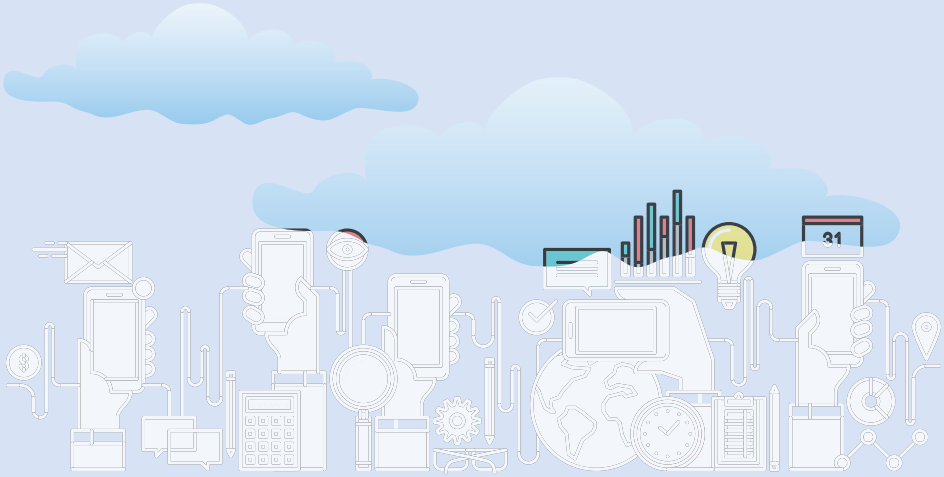
ตอน Trust on Mobile Internet

ETDA สพธอ
www.etda.or.th

ฉลาดรู้เน็ต 3

ตอน Trust on Mobile Internet

ETDA สพธอ
www.etda.or.th



หนังสือเผยแพร่เพื่อใช้ในการส่งเสริมการใช้อินเทอร์เน็ต การทำธุรกรรมออนไลน์

ฉลาดรู้เน็ต 3 ตอน Trust on Mobile Internet
เลขมาตรฐานสากลประจำหนังสือ ISBN 978-974-9765-76-0

พิมพ์ครั้งแรก : 2560

จัดพิมพ์และเผยแพร่โดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
อาคารเดอะไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระรามเก้า แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310
โทรศัพท์ 0-2123-1234
เว็บไซต์ สพธอ. : www.etda.or.th
เว็บไซต์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม : www.mdes.go.th

สุรางคณา วายุภาพ
ผอ.สพธอ.

ดร.รัฐศาสตร์ กรสูต
ผู้อำนวยการอาวุโส
สำนักพาณิชย์อิเล็กทรอนิกส์

พรรณทิมา สรรพศิรินันท์
ผู้จัดการ
งานพาณิชย์อิเล็กทรอนิกส์

ชณิกา อรัณยกานนท์
ผู้ช่วยผู้จัดการ
งานสื่อสารองค์กรและประชาสัมพันธ์

ทศพร โขมพัตร
เจ้าหน้าที่
สื่อสารองค์กรและประชาสัมพันธ์อาวุโส

ร่วมแรงกันทำ

กำหนดทิศทาง & แนะนำ	สุรางคณา วายุภาพ
กำกับดูแล	ดร.รัฐศาสตร์ กรสูต
สรรค์สร้างเนื้อหา	พรรณทิมา สรรพศิรินันท์
	ชณิกา อรัณยกานนท์
	ทศพร โขมพัตร

คำนำ

ในยุคที่ Mobile Internet เข้ามามีบทบาทกับชีวิตประจำวันของเรานับตั้งแต่ตื่นเช้าถึงเข้านอน เราต่างก็ใช้อุปกรณ์เคลื่อนที่ไม่ว่าจะเป็น สมาร์ตโฟนหรือแท็บเล็ต ในการเข้าถึงอินเทอร์เน็ตเพื่อทำกิจกรรมต่างๆ ทั้งสื่อสังคมออนไลน์ การค้นหาข้อมูล การทำธุรกรรมทางออนไลน์ รวมไปถึงการซื้อขายผ่านช่องทางออนไลน์ อย่างไรก็ตาม เมื่อสามารถทำธุรกรรมทางการเงินหรือซื้อสินค้าทางออนไลน์ได้สะดวกสบาย เพียงไม่กี่คลิก อาจทำให้ไม่ทันระมัดระวังตัว และตกเป็นเหยื่อของมิจฉาชีพหรือผู้ไม่ประสงค์ดีที่อาจสามารถเข้าถึงข้อมูลส่วนตัว หรือข้อมูลทางการเงินและนำไปสู่การสูญเสียต่างๆ ได้

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มุ่งส่งเสริมให้เกิดการใช้เทคโนโลยีดิจิทัลอย่างมั่นคงปลอดภัย จึงได้จัดทำหนังสือชุด “ฉลาดรู้เน็ต” เพื่อเป็นคู่มือในการใช้อินเทอร์เน็ตอย่างเกิดประโยชน์และมั่งคงปลอดภัย โดยหนังสือ 2 เล่ม ที่ผ่านมา นั่นคือ “ฉลาดรู้เน็ต 1 ตอน Internet of Thing” และ “ฉลาดรู้เน็ต 2 ตอน Trust on Internet” ได้ให้ความรู้ในการใช้อินเทอร์เน็ต ตลอดจนสร้างภูมิคุ้มกันให้แก่ผู้อ่านได้รู้เท่าทันภัยก่อนที่จะตกเป็นเหยื่อ เพื่อให้สามารถใช้อินเทอร์เน็ตและโซเชียลมีเดียอย่างมั่นคงปลอดภัย

หนังสือ **“ฉลาดรู้เน็ต 3”** เล่มนี้ จะเป็นการต่อยอดเนื้อหาจากเล่มที่ผ่านมา โดยส่งเสริมความรู้ ความเข้าใจในการใช้ Mobile Internet อย่างมั่นคงปลอดภัย เพื่อให้สามารถใช้งานอย่างมั่นใจและรู้เท่าทัน ไม่ตกเป็นเหยื่อของภัยที่อาจแฝงมากับผู้ไม่หวังดี เมื่อเรามีความรู้ ความเข้าใจใน Mobile Internet แล้ว ก็ย่อมใช้งานได้อย่างมั่นใจยิ่งขึ้น

สุรางคณา วายุภาพ
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
(องค์การมหาชน)

ฉลาดรู้เน็ต 3

ตอน Trust on Mobile Internet

Contents

ก้าวสู่
Mobile Internet

Mobile Internet
ช่วยให้ชีวิตมนุษย์ดีขึ้นอย่างไร
บางคนถึงกล้าพูดว่าสามารถเปลี่ยน
การสื่อสารโลกได้ทั้งใบ

1.1 อนาคตของ *Mobile Internet* ที่จะพลิกโลก

ไม่ว่าจะหันไปทางไหน พุดน้อยก็เห็นคนพกโทรศัพท์มือถืออยู่รอบตัว บางคนมีหลายเครื่อง บางคนก็มีแท็บเล็ต (Tablet) ด้วย จนแทบจะเป็นอวัยวะที่ 33 ของมนุษย์ไปแล้ว โดยเฉพาะคุณพ่อของพุดน้อย ที่หากลืมโทรศัพท์ไว้ที่บ้าน ต้องรีบขึ่งรถยนต์กลับบ้าน มาเอาโทรศัพท์ทันที

คุณพ่อของพุดน้อยบอกว่า ปัจจุบันโทรศัพท์มือถือรุ่นที่เป็นสมาร์ตโฟน (Smartphone) ราคาถูกลงมาก มีเงินสามพันบาทก็สามารถซื้อได้แล้ว ซึ่งสมาร์ตโฟนที่ว่านี้จะมีฟังก์ชันพื้นฐานก็คือ สามารถเชื่อมต่ออินเทอร์เน็ตได้ ถ่ายรูปได้ ถ่ายวิดีโอได้ มี Mobile Application (แอปพลิเคชัน) แผนที่ เล่นเกม รับส่งอีเมล เล่นเฟซบุ๊ก (Facebook) เล่นไลน์ (LINE) ได้ เรียกว่าการพกสมาร์ตโฟนเครื่องเดียว เสมือนกับพกคอมพิวเตอร์ไว้กับตัวเลย ยิ่งสมัยนี้เครือข่ายอินเทอร์เน็ตแบบ 3G/4G มีให้บริการเกือบทุกพื้นที่ของประเทศไทยแล้ว ทำให้คุณพ่อสามารถเชื่อมต่ออินเทอร์เน็ตได้ทุกที่ทุกเวลา

คุณพ่อ : คุณพ่อยังใช้สมาร์ตโฟนแทนบัตรขึ้นรถไฟฟ้า จ่ายบิลค่าน้ำ ค่าไฟ โอนเงิน จ่ายค่ากาแฟ เสมือนเป็นกระเป๋าสตางค์ของคุณพ่อ มิน่าเวลาคุณพ่อลืมโทรศัพท์ไว้ที่บ้านจึงต้องรีบกลับมาเอาไปด้วยทุกที

คุณแม่ : ด้านสมาร์ตโฟนของคุณแม่ มีเพลงมากมายที่ซื้อไว้ นอกจากนี้คุณแม่ยังใช้แอปพลิเคชันเรียนรู้วิธีการทำอาหาร และมักจะอัปโหลดรูปอาหารที่พึ่งทำเสร็จใหม่ๆ ผ่าน Facebook ติดตามสินค้าลดราคาผ่านแอปพลิเคชันดีล สั่งซื้อสินค้าผ่านแอปพลิเคชันขายสินค้า และโอนเงินชำระเงินด้วยแอปพลิเคชัน

พุดน้อย : ส่วนพุดน้อยใช้แท็บเล็ตช่วยในการเรียน ซึ่งมีแอปพลิเคชันเกี่ยวกับการศึกษามากมายทั้งแบบออนไลน์และออฟไลน์ และยังมีเกมสนุกๆ อีกมากมายให้พุดน้อยเล่นอีก ที่เว็บไซต์ของโรงเรียนก็ยังมี e-book ให้ดาวน์โหลดได้อีกด้วย ทำให้พุดน้อยไม่ต้องแบกหนังสือหนักๆ ไปโรงเรียน แต่ต้องระวังอย่าให้แบตหมดเชียวนะครับ

คุณอา : คุณอาของพุดน้อยก็ขายสินค้าโดยใช้สมาร์ตโฟนเครื่องเดียว ถ่ายรูปสินค้าโพสต์ใน Instagram ก็ขายได้แล้ว โดยลูกค้าจะติดต่อ สอบถาม และสั่งซื้อผ่าน LINE

นอกจากนี้ ครอบครัวของพุดน้อยมีการตั้งกลุ่มไลน์ (LINE) เพื่อคุยกันทั้งครอบครัว ทำให้เราใกล้ชิดกันมากขึ้น ในอีกมุมหนึ่งจะเห็นว่าเมื่อมีคนใช้สมาร์ตโฟนมากขึ้น ก็จะทำให้จำนวนผู้ใช้อินเทอร์เน็ตมากขึ้น เป็นโอกาสของพ่อค้าแม่ขายนำสินค้าเข้ามาขายออนไลน์ ผู้ซื้อสินค้าก็จะได้ประโยชน์เพราะมีสินค้าให้เลือกมากขึ้น

จะเห็นว่า Mobile Internet นั้นมีประโยชน์มากมาย ช่วยให้คนจำนวนมากเข้าถึงข้อมูล ช่วยในการทำงาน การค้าขาย การศึกษา และยังสามารถพกพาอุปกรณ์ไปใช้งานที่ไหนก็ได้ คนสามารถทำงานได้ทุกที่ เกิดการค้าขายได้ทุกเวลา และจากการเพิ่มขึ้นของอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ต ซึ่งในอนาคตสิ่งของทุกอย่างก็จะเชื่อมต่ออินเทอร์เน็ตได้ เราอาจจะได้เห็นรถที่ไม่มีคนขับ ใช้อุปกรณ์เคลื่อนที่แทนเงินสด บ้านอัจฉริยะ เมืองอัจฉริยะ ซึ่งพุดน้อยก็ยังนึกภาพไม่ออกเลยว่าจะเป็นอย่างไร

น้องพุดดิ้งชวนรู้

จากการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ที่รวบรวมโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ในปี 2559 พบว่าคน Gen Y (เกิดปี 2524-2543) เป็นกลุ่มที่มีพฤติกรรมการใช้อินเทอร์เน็ตมากที่สุดถึง 53.2 ชั่วโมง/สัปดาห์ (เฉลี่ยแล้วคน Gen Y ใช้งานอินเทอร์เน็ตเกือบ 7.6 ชั่วโมงต่อวัน) โดยอุปกรณ์ที่นิยมใช้การเข้าถึงอินเทอร์เน็ตก็คืออุปกรณ์เคลื่อนที่ เช่น สมาร์ตโฟนเฉลี่ย 6.2 ชั่วโมงต่อวัน ซึ่งกิจกรรมยอดฮิตก็คือ การใช้งานเครือข่ายสังคมออนไลน์ การดูวิดีโอผ่าน YouTube การอ่าน e-news e-book การค้นหาข้อมูล และการทำธุรกรรมทางการเงิน ตามลำดับ

สมาร์ตโฟน

85.5% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 6.2 ชั่วโมงต่อวัน

คอมพิวเตอร์ตั้งโต๊ะ

62.0% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 5.4 ชั่วโมงต่อวัน

คอมพิวเตอร์พกพา

48.7% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 4.7 ชั่วโมงต่อวัน

แท็บเล็ตคอมพิวเตอร์

30.0% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 3.5 ชั่วโมงต่อวัน

สมาร์ตทีวี

19.8% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 2.7 ชั่วโมงต่อวัน

ร้อยละของผู้ใช้อินเทอร์เน็ต เปรียบเทียบ 5 อันดับแรก
ของกิจกรรมการใช้งานผ่านอินเทอร์เน็ต ระหว่างอุปกรณ์เคลื่อนที่กับคอมพิวเตอร์

1.2 ยุคทองของ Wearable Device

นอกจากสมาร์ตโฟนแล้ว
ยังมีอุปกรณ์อื่นๆ ที่สามารถเชื่อมต่อ
กับอินเทอร์เน็ตได้อีกมากมาย
วันนี้พุดน้อยจะมาแนะนำอุปกรณ์ที่ใช้
สวมใส่เข้ากับร่างกายที่เรียกว่า
Wearable Device ให้เพื่อนๆ รู้จักกัน

นอกจากสมาร์ตโฟนที่คุณพ่อพกติดตัวแล้ว พุดน้อยยังเห็นคุณพ่อใส่สายรัดข้อมืออะไรสักอย่าง ซึ่งคุณพ่อบอกว่าเป็นอุปกรณ์ที่คอยตรวจจับว่าคุณพ่อทำกิจกรรมอะไรบ้าง เช่น นับจำนวนก้าวเดิน วัดระยะทาง วิเคราะห์การนอนหลับ เพื่อเป็นข้อมูลในการดูแลสุขภาพ ว้าว! ช่างสุดยอดอะไรเช่นนี้

Wearable Device คืออุปกรณ์สวมใส่เข้ากับร่างกาย เช่น นาฬิกา กำไลข้อมือ สายรัดข้อมือ แหวน รองเท้า แว่นตา เสื้อผ้า และอีกมากมาย ทำงานและควบคุมด้วยระบบคอมพิวเตอร์ มี Sensor เพื่อตรวจวัดค่าต่างๆ ของผู้ที่สวมใส่ ซึ่งมีทั้งแบบทำงานได้ด้วยตนเอง และแบบที่ต้องทำงานร่วมกับอุปกรณ์ เช่น สมาร์ตโฟน และแท็บเล็ต โดยเชื่อมต่อข้อมูลผ่าน Wi-Fi หรือ Bluetooth นำมาแสดงผลที่แอปพลิเคชันที่ติดตั้งไว้ในสมาร์ตโฟนและแท็บเล็ต

พูดน้อยจะยกตัวอย่าง Wearable Device ที่มีอยู่ในปัจจุบันให้เพื่อนๆ รู้จักว่ามีอะไรบ้าง

สายรัดข้อมือ Smartband

Wearable Device ที่เป็นสายรัดข้อมือจะบันทึกกิจกรรมของเพื่อนๆ ไม่ว่าจะเป็นการเดิน วิ่ง นอน ปั่นจักรยาน บันทึกเส้นทางการเคลื่อนไหวด้วย GPS คำนวณการเผาผลาญแคลอรี่ สามารถใช้งานร่วมกับสมาร์ตโฟน เช่น สั่นเตือนเมื่อมีคนโทรเข้า สั่นเมื่อปลุก ควบคุมการเล่นเพลง สามารถแชร์ข้อมูลไปยังเครือข่ายสังคมออนไลน์เพื่อแข่งกันได้ โดยซิงค์ข้อมูลร่วมกับสมาร์ตโฟน เพื่อนคนไหนที่รักสุขภาพ ก็น่าจะชอบ Smartband นะครับ

นาฬิกาอัจฉริยะ Smartwatch

ความสามารถหลักของ Smartwatch จะคล้ายๆ กับ Smartband แต่ Smartwatch จะเก่งกว่าตรงที่มีระบบปฏิบัติการในตัว สามารถทำงานได้โดยไม่ต้องเชื่อมต่อกับสมาร์ตโฟน หน้าจอมีขนาดใหญ่เท่ากับนาฬิกาใช้บอกเวลาได้ตามชื่อของมัน มีหน้าจอระบบสัมผัสหรือใช้ปุ่มควบคุม ติดตั้งแอปพลิเคชันเพิ่มเติมได้ มี Sensor ที่เยอะกว่า Smartband เช่น วัดอัตราการเต้นของหัวใจ วัดระดับความสูง วัดอุณหภูมิ วัดรังสียูวี บางรุ่นก็สามารถใส่ซิมได้ และเชื่อมต่ออินเทอร์เน็ตได้ด้วยตัวเอง

เสื้อผ้าอัจฉริยะ Smart Clothing

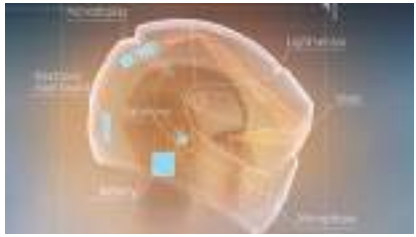
เป็นการนำ Sensor ทอเข้าไปในเสื้อผ้า แล้วนำมาประมวลผลที่ชิปขนาดเล็กที่ถอดออกได้ โดยส่งข้อมูลไปยังสมาร์ตโฟนผ่าน Bluetooth สามารถตรวจจับอัตราการเต้นของหัวใจ อัตราการหายใจ ตรวจจับการเคลื่อนไหว เหมาะสำหรับนักกีฬาหรือเพื่อนๆ ที่ต้องการออกกำลังกายอย่างจริงจัง

เทคโนโลยีนี้ยังนำมาใช้ผลิตชุดดับเพลิงที่สามารถตรวจจับความร้อนของไฟ ใช้กับอุปกรณ์ทางการแพทย์ เช่น ผ้าพันแผล โดย Sensor จะตรวจจับความแน่นของผ้าพันแผลและความถูกต้องของการพันแผล ใช้ตรวจสอบสุขภาพของผู้ป่วย และแจ้งเตือนผู้สวมใส่หรือผู้ดูแลเกี่ยวกับปัญหาของสุขภาพก่อนที่ผู้สวมใส่จะป่วย หรือขณะที่เขาหมดสติหรืออยู่ในสถานะที่ช่วยตัวเองไม่ได้

นอกจากนี้ ยังมี Wearable Device อีกมากมายที่ยังไม่ได้กล่าวถึงในที่นี้ เช่น แว่นตาอัจฉริยะ หมวกกันน็อกอัจฉริยะ เป็นต้น ซึ่งพูดน้อยคิดว่าในอนาคตทุกอย่างที่เราสวมใส่ได้ก็จะกลายเป็น Wearable Device

▶▶ แว่นตาอัจฉริยะ

▶▶ ชุดดับเพลิง



หมวกกันน็อกอัจฉริยะ

ต่อไปข้อมูลสุขภาพของเราที่ได้จาก Wearable Device จะมีประโยชน์อย่างมาก เช่น ผู้ป่วยโรคหัวใจ ถ้าใช้เครื่องมือวัดอัตราการเต้นของหัวใจหากมีสิ่งผิดปกติข้อมูลจะส่งผ่านอินเทอร์เน็ตไปให้แพทย์หรือผู้ดูแล ให้ได้รับการช่วยเหลืออย่างทันท่วงที หรือสำหรับคนทั่วไป ทางโรงพยาบาลอาจจะใช้ข้อมูลสุขภาพเราบันทึกไว้เพื่อช่วยในการวินิจฉัยโรคได้ หรือนักกีฬาก็จะสามารถส่งข้อมูลสุขภาพไปยังโค้ชได้ในขณะทำการฝึกซ้อมหรือแข่งขัน

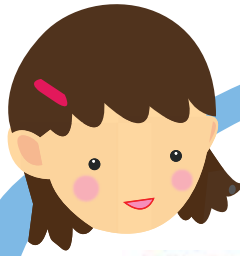
ในอนาคตอุปกรณ์เหล่านี้จะมีราคาถูกลง Sensor ต่างๆ ก็จะถูกฝังตัวไว้ในทุกสิ่งที่เราสวมใส่และเชื่อมต่อกันได้ ทำให้ Wearable Device จะมีหลากหลายรูปแบบและทุกขนาด สามารถเก็บข้อมูลสุขภาพของเราได้ทุกมิติ ซึ่งก็จะเป็นประโยชน์ถ้าข้อมูลเหล่านี้ได้รับการเข้าถึงได้เฉพาะคนที่เหมาะสม

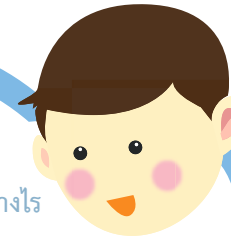
รูปภาพจาก http://www.telecomjournalthailand.com/wearable-tech/

น้องพุดดิ้งชวนรู้

Wearable Device แต่ละตัวในปัจจุบัน

Wearable Device ที่นิยมมากที่สุดในปัจจุบัน ได้แก่ **นาฬิกาอัจฉริยะ** (Smart Watch) ใช้ได้ทั้งดูเวลา วันที่ จับเวลา จนถึงขั้นแจ้งเตือน SMS จากสมาร์ตโฟนได้ **แว่นตากูเกิล** (Google Glass) แว่นตาที่เมื่อสวมใส่จะแสดงข้อมูลที่ตั้ง แผนที่ สภาพอากาศ และข้อมูลอื่นๆ ที่ดูผ่านสมาร์ตโฟนได้อีกด้วย **อุปกรณ์วัดความแอคทีฟ** (Activity Tracker) ที่จะช่วยกระตุ้นการช่วยลดน้ำหนัก เผาผลาญไขมันขณะออกกำลังกาย และสุดท้ายคือ **นาฬิกาสำหรับการวิ่ง** (Running Watch) ที่มี Sensor วัดอัตราการเต้นของหัวใจขณะวิ่ง เหมาะมากสำหรับคนรักการออกกำลังกาย





น้องพุดดิ้งชวนรู้

Wearable Device
จะเปลี่ยนไลฟ์สไตล์ของคุณได้อย่างไร

รูปภาพจาก m.thaiware.com

1.3 Mobile Application เข้าถึงง่าย ใช้สะดวก

Mobile Application คือ ซอฟต์แวร์ที่ออกแบบให้สามารถใช้งานได้บนสมาร์ตโฟนหรือแท็บเล็ตได้อย่างรวดเร็ว สะดวก ใช้งานง่าย ปัจจุบันมีโมบาย แอปพลิเคชันให้เลือกมากมาย แอปพลิเคชันเหล่านี้สามารถดาวน์โหลดและติดตั้งได้ง่ายจากอุปกรณ์นั้นเลย โดยในร้านค้าของแอปพลิเคชัน จะแบ่งแอปพลิเคชันออกเป็นหมวดหมู่ต่างๆ เช่น รูปและวิดีโอ เกม การศึกษา เด็ก ไลฟ์สไตล์ สุขภาพและฟิตเนส ความบันเทิง ท่องเที่ยว การเงิน และอื่นๆ ในแต่ละหมวดหมู่จะมีการเรียงลำดับตามความนิยม โดยแยกเป็นแอปพลิเคชันฟรีกับเสียเงินให้ด้วย เมื่อกดเข้าไปก็จะเห็นข้อมูล คำอธิบาย รวมทั้งรีวิวของผู้ที่ดาวน์โหลดไปใช้แล้ว

ร้านค้าของแอปพลิเคชัน

ในการดาวน์โหลดแอปพลิเคชัน เพื่อนๆ ต้องมีบัญชีผู้ใช้สำหรับดาวน์โหลด และหากต้องจ่ายเงินซื้อจะต้องผูกบัญชีบัตรเครดิตหรือบัตรเดบิตกับบัญชีนั้นด้วย สำหรับพุดน้อยจะให้คุณพ่อเป็นคนดาวน์โหลดแอปพลิเคชันให้ครับ

ตัวอย่างข้อมูล คำอธิบาย และรีวิวสินค้าในแอปพลิเคชัน

ประเภทของแอปพลิเคชัน นอกจากแอปพลิเคชันฟรีและไม่ฟรีแล้ว ยังมีแอปพลิเคชันอีกประเภทที่เรียกว่า in-app purchases ซึ่งสามารถดาวน์โหลดได้ฟรีโดยไม่ต้องเสียเงินซื้อ แต่หากอยากเพิ่มความสามารถของแอปพลิเคชันก็ต้องจ่ายเงินซื้อภายในแอปพลิเคชัน ยกตัวอย่างเช่น แอปพลิเคชันที่มีแถบโฆษณา อาจบอกว่าให้จ่ายเงินเพื่อแลกกับการไม่แสดงโฆษณา แอปพลิเคชันกล้องที่ต้องจ่ายเงินซื้อ Filter เพิ่มเติมหากต้องการ ในเกมมีการขายสิ่งของเพื่อเพิ่มความสามารถให้กับตัวละคร ทำให้ประหยัดเวลาเล่น เป็นต้น

เพื่อนๆ ต้องระวังไม่ไปเผลอกดซื้อของในเกมโดยไม่จำเป็นนะครับ เพราะอาจทำให้คุณพ่อคุณแม่ของเราต้องเสียเงินโดยใช่เหตุ แต่บางครั้งพุดน้อยก็เผลอกดซื้อของในเกมโดยไม่ได้ตั้งใจเหมือนกัน โดนคุณพ่อดุไปหลายที คุณพ่อเลยตั้งค่าบัญชีใหม่ให้ไม่สามารถใช้งานการซื้อในแอปพลิเคชัน (in-app purchases) ได้อัตโนมัติ ทำให้พุดน้อยไม่ต้องกลัวที่จะกดผิดอีกแล้ว ดีใจจัง

การซื้อสินค้าในแอปพลิเคชัน

สำหรับเพื่อนๆ ที่ดาวน์โหลดแอปพลิเคชันได้เอง ต้องระวังในเรื่องของแอปพลิเคชันปลอมด้วยนะครับ เพราะบางครั้งก็มีพวกหัวใสทำแอปพลิเคชันเลียนแบบของจริงขึ้นมา ทำให้ต้องเสียเงินฟรี หรือบางครั้งทำแอปพลิเคชันเลียนแบบธนาคารเพื่อขโมยบัญชีของเรา ดังนั้น ก่อนดาวน์โหลดแอปพลิเคชันพุดน้อยอยากให้เพื่อนดูว่าใครเป็นผู้พัฒนาแอปพลิเคชัน อ่านรีวิวก่อนดาวน์โหลด แต่ถ้ายังไม่แน่ใจก็ให้ถามผู้รู้หรือผู้ปกครองก่อนนะครับ

สิ่งที่ต้องระวังอีกอย่างหนึ่งก็คือ แอปพลิเคชันส่วนใหญ่ใช้การเชื่อมต่อข้อมูลกับอินเทอร์เน็ต ซึ่งเพื่อนๆ ต้องระวังในเรื่องของค่าใช้จ่าย เช่น ค่าอินเทอร์เน็ตและค่าซื้อแอปพลิเคชัน ที่จะเกิดขึ้นเมื่อมีการใช้งานแอปพลิเคชัน ซึ่งพุดน้อยจะพูดถึงในบทถัดไปครับ

แต่ละคนจะมีการใช้ชีวิตไม่เหมือนกัน ในแต่ละช่วงเวลาก็จะใช้แอปพลิเคชันแตกต่างกันไป เช่น ระหว่างวันทำงานคุณพ่อของพุดน้อยมักจะใช้แอปพลิเคชันที่เกี่ยวกับการทำงาน เช่น ดูหุ้น พยากรณ์อากาศ บันทึกเสียง จดบันทึก ปฏิทิน สิ่งที่ต้องทำ เป็นต้น ส่วนคุณแม่ที่เป็นแม่บ้านก็จะใช้แอปพลิเคชันสำหรับดูทีวี ดูละครย้อนหลัง ดูวิดีโอสอนทำกับข้าว บันทึกค่าใช้จ่าย ตกแต่งภาพ ช้อปปิ้งออนไลน์ เป็นต้น

หากเป็นวันหยุดหรือนอกเวลาทำงาน ตอนที่คุณพ่อออกไปข้างนอก คุณพ่อก็จะใช้แอปพลิเคชันแผนที่เพื่อนำทาง ดูสภาพการจราจร เพื่อหาเส้นทางที่ดีที่สุด หรือหากจะไปรับประทานอาหารนอกบ้านก็สามารถใช้แอปพลิเคชันเพื่อหาร้านอาหารอร่อยๆ ที่อยู่ใกล้ได้

ส่วนพุดน้อยก็ชอบแอปพลิเคชัน เกี่ยวกับการสอนภาษา เล่นเกม ดูการ์ตูน อ่านอีบุ๊ก (e-book) ซึ่งแต่ละคนก็จะใช้แอปพลิเคชันแตกต่างกันไปครับ

จะเห็นได้ว่าสมาร์ตโฟนมีแอปพลิเคชันให้ใช้มากมายซึ่งช่วยอำนวยความสะดวกในชีวิตประจำวัน นอกจากจะใช้ในการติดต่อสื่อสารแล้ว ยังใช้ได้ทั้งการทำงาน บันเทิง การเงิน การศึกษา ออกกำลังกาย สุขภาพ และอื่นๆ อีกมากมาย ซึ่งถ้าเพื่อนๆ รู้จักการนำมาใช้ให้เป็นประโยชน์ก็จะช่วยประหยัดเวลา เพิ่มประสิทธิภาพการทำงาน ช่วยดูแลสุขภาพ ช่วยให้สามารถค้นคว้าข้อมูลได้ง่ายขึ้น

น้องพุดดิ้งชวนรู้

จำนวนแอปพลิเคชันใน iTunes App Store มีจำนวนมากกว่า 1,500 ล้านแอปพลิเคชัน และจำนวนครั้งที่ดาวน์โหลดแอปพลิเคชันใน App Store ของ Apple มากกว่า 1 ล้านล้านครั้ง

จำนวนแอปพลิเคชันใน Google Play Store มีจำนวนมากกว่า 1,600 ล้านแอปพลิเคชัน

จำนวนแอปพลิเคชันใน Windows Phone Store มีจำนวนมากกว่า 340 ล้านแอปพลิเคชัน

มีแอปพลิเคชันใหม่เกิดขึ้นเดือนละ 40,000 แอปพลิเคชัน

25% ของแอปพลิเคชันทั้งหมดเป็นเกม แอปพลิเคชันยอดนิยม 5 อันดับแรก คือ เกม การศึกษา ธุรกิจ ไลฟ์สไตล์ และบันเทิง ตามลำดับ

ข้อมูลจาก :

http://techcrunch.com/2015/06/08/itunes-app-store-passes-1-5m-apps-100b-downloads-30b-paid-to-developers/

http://www.statista.com/topics/1002/mobile-app-usage/

http://www.mirum.co.th/paper/

บทที่ 2

นับ 1 ถึง 3 ก็พร้อมใช้ Mobile Internet

ก่อนที่จะซื้อมือถือจะต้องรู้ว่า
เรามีพฤติกรรมการใช้งานอย่างไร
เพื่อที่จะได้เลือกที่เหมาะกับตัวเอง
และใช้งานอย่างคุ้มค่ามากที่สุด

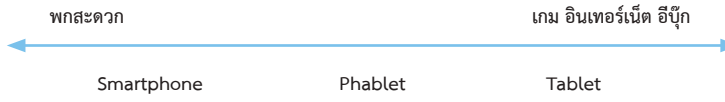
2.1 นับ 1...เลือก Device ที่เหมาะกับตัวเอง

เดี๋ยวนี้ Mobile Device มีให้เลือกมากมาย หลายรุ่น หลายแบบ หลายราคา แล้วแบบไหนล่ะที่ตรงกับการใช้งานของเรามากที่สุด พูดน้อยมีข้อคิดเล็กๆ น้อยๆ ในการเลือกซื้อสมาร์ตโฟนให้เหมาะสมกับเราเองครับ

1. ขนาดของหน้าจอ (Screen Size)

ขนาดของหน้าจอเป็นตัวเลือกแรกๆ ของการเลือกซื้อเลยนะครับ เพราะเป็นการแบ่งประเภทของ Mobile Device ด้วย โดยสมาร์ตโฟนจะมีขนาดหน้าจอไม่เกิน 5 นิ้ว ส่วนแท็บเล็ตจะมีขนาดหน้าจอตั้งแต่ 7 นิ้วขึ้นไป และยังมี Device อีกประเภทหนึ่งที่กำลังเป็นที่นิยมอยู่ในขณะนี้เรียกว่า แฟบเล็ต (Phablet) จะมีขนาดตั้งแต่ 5-7 นิ้วครับ

การเลือกซื้อ Mobile Device ประเภทไหนให้ดูที่พฤติกรรมของเรา เช่น ถ้าต้องการความสะดวกในการพกพา สมาร์ตโฟนจะเป็นตัวเลือกที่ดีที่สุด ถ้าต้องการอ่านอีบุ๊ก ท่องอินเทอร์เน็ต เล่นเกมเป็นส่วนใหญ่ แท็บเล็ตจะเป็นตัวเลือกที่ดีที่สุด แต่ถ้าต้องการแบบ All in one ก็เลือกใช้แฟบเล็ต



2. ระบบปฏิบัติการ (Operating System)

เมื่อเราเลือกขนาดของ Mobile Device ได้แล้ว ตัวเลือกอันดับถัดมาก็คือระบบปฏิบัติการ (OS) ซึ่งปัจจุบันมีให้เลือก 3 ระบบ คือ iOS ของ Apple, Android จากค่าย Google และ Windows Phone ของ Microsoft ซึ่งจะมีข้อดีข้อจำกัดแตกต่างกันไป พุดน้อยจะสรุปให้ฟังดังนี้ครับ

- iOS เป็น OS ของ Apple ที่มากับ iPhone เป็นต้นแบบของ Mobile OS ในปัจจุบัน มีการใช้งานที่ง่าย ไม่ซับซ้อน มีแอปพลิเคชันให้เลือกมากมาย OS เป็นระบบปิดซึ่งจำกัดให้ Apple พัฒนาได้เพียงผู้เดียว ไม่เปิดเผยโค้ดให้ผู้ผลิตยี่ห้ออื่นนำไปพัฒนาต่อ จึงสามารถใช้ OS ได้เฉพาะผลิตภัณฑ์ของ Apple เช่น iPhone กับ iPad เท่านั้น ผู้ใช้ไม่สามารถปรับแต่งอะไรได้มาก
- Android เป็น OS ของ Google เป็นระบบเปิด อนุญาตให้ผู้ผลิตสมาร์ตโฟนสามารถนำโค้ดโปรแกรมไปพัฒนาต่อได้ ทำให้มียี่ห้อและขนาดให้เลือกมากมาย ผู้ใช้สามารถปรับแต่งการใช้งานได้มากกว่า มีอิสระในการลงแอปพลิเคชันได้หลายทาง ทั้งจาก Google Play Store หรือจากไฟล์ .apk แต่ต้องระวังเรื่องไวรัสและมัลแวร์จากการติดตั้งไฟล์ที่ไม่ผ่าน Google Play Store กันด้วยนะครับ
- Windows Phone เป็น OS ของ Microsoft มีจุดเด่นคือสามารถใช้งานเอกสาร Microsoft Office ได้ดีกว่า ส่วน OS เป็นระบบปิดเช่นเดียวกับ iOS แต่ก็มียี่ห้อให้เลือกมากกว่า

พุดน้อยจะยกตัวอย่างให้ดูนะครับ ถ้าเราต้องการ Device ที่ใช้งานง่าย และมีงบประมาณพอสมควรก็อาจเลือก Device จากค่าย Apple แต่ถ้าต้องการ Device ที่ราคาย่อมเยาและมีหลายยี่ห้อให้เลือกก็ลองดู Device ที่เป็น Android หรือถ้าเน้นเรื่องการใช้งานเอกสารก็ใช้ Windows Phone เป็นต้น เพื่อนๆ จะลองดูตารางตัวอย่างเปรียบเทียบในตัวอย่างข้างล่างก็ได้นะครับ

	iOS	Android	Windows Phone
เจ้าของระบบปฏิบัติการ	Apple	Google	Microsoft
ระบบเปิด/ปิด	ปิด	เปิด	ปิด
การปรับแต่ง	ไม่ได้	ได้	ได้
App Store	App Store	Google Play Store	Windows Phone
อุปกรณ์/ยี่ห้อ	iPhone, iPad, iPod Touch	Samsung, LG, Huawei, Lenovo, Oppo, ASUS ฯลฯ	Microsoft, Nokia, HTC
มีหลายรุ่นให้เลือก	น้อยมาก	มาก	น้อย
การจัดการไฟล์	ยาก	ง่าย	ง่าย
โปรแกรมเอกสาร	Page, Number, Keynote	Google Docs, Sheet, Slide	Microsoft Office
ที่เก็บข้อมูล	iCloud	Google Drive	One Drive

ข้างต้นนี้เป็นเพียงตัวอย่างง่ายๆ นะครับ ในความเป็นจริงแล้วอาจมีปัจจัยอีกมากมายที่พุดน้อยไม่ได้กล่าวไว้ในที่นี้ ทั้งนี้ขึ้นอยู่กับผู้ใช้งานว่าถนัดใช้ OS แบบไหนมากที่สุด

3. หน่วยประมวลผลกลาง (Central Processor Unit)

หน่วยประมวลผลกลางหรือเรียกย่อๆ ว่า CPU เปรียบได้กับสมองของคนเรา ซึ่งมักจะมีตัวเลขอยู่สองแบบคือ

1) ความเร็ว CPU หน่วยเป็น GHz ตัวเลขไหนมากกว่าก็จะเร็วกว่า

2) จำนวนแกนสมองหรือ Core จำนวนแกนมากกว่ายิ่งดี

4. หน่วยความจำ (Internal Storage)

หน่วยความจำ มี 2 ประเภทคือ

1) RAM คือ หน่วยความจำหลักที่ใช้ประมวลผลโปรแกรม ยิ่งมีเยอะยิ่งเร็ว

2) Internal Storage คือ หน่วยความจำที่ใช้เก็บข้อมูลในเครื่อง

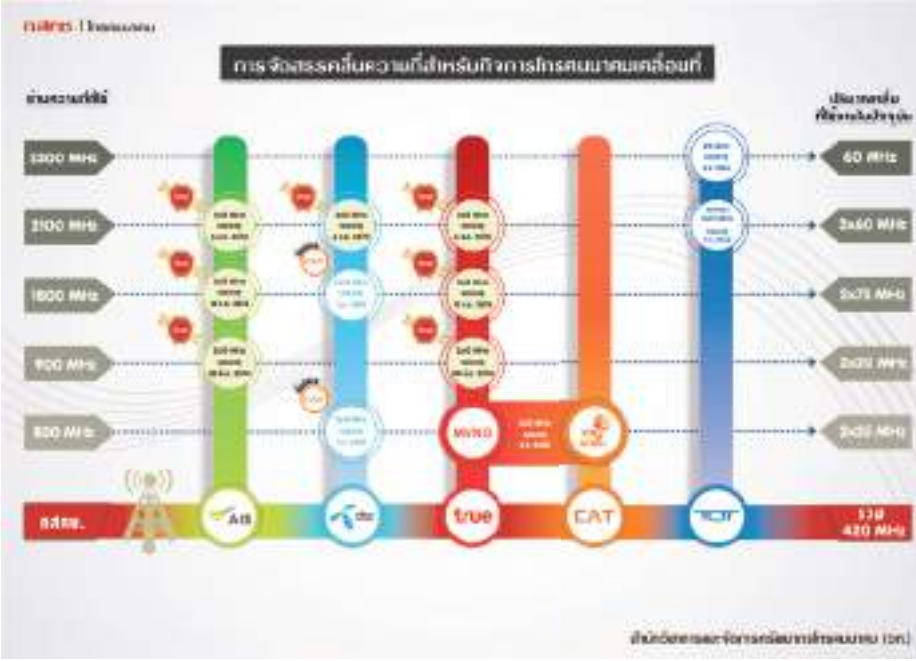
เริ่มต้นควรมี RAM อย่างน้อย 1 GB ส่วนหน่วยความจำภายใน แล้วแต่พฤติกรรมของผู้ใช้ โดยคำนวณจากพื้นที่ที่เหลือจากการลง OS แล้ว เช่น หน่วยความจำภายใน 8 GB อาจจะเหลือพื้นที่ใช้จริงเพียง 4 GB สมมติว่าแอปพลิเคชันหนึ่งแอปพลิเคชันมีขนาด 200 MB ก็จะเหลือพื้นที่ให้ลงแอปพลิเคชันเพียง 20 แอปพลิเคชันเท่านั้น ซึ่งถ้าเราใช้แอปพลิเคชันไม่เยอะก็จะเหลือพื้นที่ไว้เก็บข้อมูลอย่างอื่นอีก เช่น รูปถ่าย วิดีโอ เพลง ซึ่งหากลงแอปพลิเคชันไปแล้วเหลือพื้นที่ประมาณ 3 GB ถ้าจะลงเกมทั่วไปที่มีขนาดไฟล์ไม่ใหญ่นัก (ประมาณ 200 MB) จะลงได้อีกประมาณ 5-10 เกม แต่ถ้าเป็นเกมที่ใหญ่ขนาด 1 GB ก็คงลงได้แค่ 1-2 เกมเท่านั้น เพราะต้องเก็บพื้นที่เอาไว้ถ่ายรูป ถ่ายวิดีโอ ดาวน์โหลดหนัง หรือเพลงอีก จากตัวอย่างที่พุดน้อยกล่าวมานั้น 8 GB อาจจะไม่เพียงพอ ถ้าดูจากพฤติกรรมที่กล่าวมา อาจจะต้องเลือกหน่วยความจำตั้งแต่ 16 GB ขึ้นไปครับ ขึ้นอยู่กับการใช้งานของแต่ละคนด้วย อย่างพุดน้อยไม่ค่อยติดตั้งแอปพลิเคชัน ไม่ค่อยได้ถ่ายรูป เลยใช้หน่วยความจำแค่ 8 GB ก็พอครับ

5. กล้อง (Camera)

กล้องกลายเป็นคุณสมบัติพื้นฐานของ Mobile Device ไปซะแล้ว ซึ่งเดี๋ยวนี้จะมีทั้งกล้องหน้า (Front) เอาไว้ถ่ายเซลฟี่ และกล้องหลัง (Rare) โดยที่ความละเอียดของกล้องจะแตกต่างกันออกไป ถ้าเราชอบถ่ายรูปเป็นชีวิตจิตใจ สิ่งนี้เป็นสิ่งหนึ่งที่ต้องพิจารณาก่อนเลย ความละเอียดของกล้องจะมีหน่วยเป็นเมกะพิกเซล (MP) โดยความละเอียดกล้องหน้าและหลังจะไม่เท่ากัน กล้องหน้าคือกล้องที่อยู่ฝั่งเดียวกับหน้าจอจะมีความละเอียดน้อยกว่ากล้องหลัง เช่น 13MP/2MP หมายความว่า กล้องหน้ามีความละเอียด 2 ล้านพิกเซล กล้องหลังมีความละเอียด 13 ล้านพิกเซล ยิ่งกล้องมีความละเอียดสูง ภาพก็จะคมชัดกว่าและขนาดของรูปก็จะใหญ่กว่าครับ

6. คลื่นความถี่

สำหรับคนที่ซื้อแท็บเล็ตจะสามารถเลือกรุ่นที่ใช้อินเทอร์เน็ตผ่าน Wi-Fi อย่างเดียวก็ได้ ซึ่งราคาจะถูกกว่าเครื่องที่ใส่ซิมการ์ดของโทรศัพท์ แต่ถ้าจะซื้อแท็บเล็ตรุ่นที่ต้องใส่ซิมการ์ดหรือสมาร์ตโฟน จะต้องทราบว่า Mobile Device ของเราใช้งานได้กับคลื่นความถี่ไหนบ้าง จะได้เลือกใช้บริการให้ถูกค่ายด้วยครับ ซึ่งหากเราใช้เครื่องไม่ตรงกับความถี่ ประสิทธิภาพก็อาจจะลดลง โดยเพื่อนๆ สามารถดูได้จากที่กล่อง หรือเว็บไซต์ของผู้ผลิตก็ได้ครับ



เป็นที่ทราบกันดีว่า Mobile Device มีให้เลือกมากมายหลายรุ่นแต่ที่สำคัญเพื่อนๆ จะต้องเลือกให้เหมาะกับลักษณะการใช้งานของตนเอง ซึ่งจะทำให้เกิดความคุ้มค่าในการใช้งาน ยกตัวอย่าง

คุณพ่อ ต้องการใช้ Mobile Device ที่พกสะดวกแต่ก็ไม่เล็กจนทำงานไม่ได้ คุณพ่อพุดน้อยเลยเลือกสมาร์ตโฟนขนาด 5.7 นิ้วหรือที่เรียกว่าแฟบเล็ต และเลือกใช้ Android OS เพราะคุณพ่อชอบใช้บริการของ Google และใช้หน่วยความจำขนาด 32 GB เพื่อจะได้ไม่มีปัญหาเรื่องการจัดเก็บข้อมูล

คุณแม่ เป็นแม่บ้าน ไม่ต้องออกไปไหนก็เลยเลือกซื้อแท็บเล็ตแบบไม่มีซิมการ์ด โดยเชื่อมต่ออินเทอร์เน็ตผ่าน Wi-Fi ในบ้าน ใช้ดูหนัง ฟังเพลง ดูวิดีโอสอนทำอาหาร เข้าเว็บไซต์ไม่ค่อยดาวน์โหลดหรือลงแอปพลิเคชันไม่ค่อยถ่ายรูป และไม่ค่อยชอบปรับแต่งอะไรมาก จึงเลือกใช้ iPad Wi-Fi ขนาด 16 GB

พุดน้อย ชอบเล่นเกม และใช้แอปพลิเคชันเพื่อการศึกษา แต่ก็ไม่ได้ออกไปข้างนอกบ่อย ก็เลยใช้แท็บเล็ต Wi-Fi เหมือนกับคุณแม่ แต่ขนาดจะเล็กกว่าและหน่วยความจำมากกว่า

พุดดิ้ง เน้น Chat กับถ่ายรูปโพสต์ลงโซเชียล ใช้สมาร์ตโฟนขนาดพอดีมือ หน่วยความจำ 16 GB กล้องหน้าชัดๆ

น้องพุดดิ้งชวนรู้

ความแตกต่างระหว่างคลื่น 1800 MHz กับ 900 MHz

รูปจาก http://news.mthai.com/hot-news/infographics/469248.html

Package Internet
มีมากมาย จะมีวิธีเลือกอย่างไร
ให้เหมาะสมกับการใช้งาน
ของเราเอง

2.2 นับ 2...Package Internet ที่คุ้มค่า

ก่อนที่จะเลือก Package Internet ให้เราคำนวณปริมาณข้อมูลที่เราจะใช้ก่อน โดยสามารถดูจากรูป

ในแต่ละค่ายก็จะมีโปรแกรมช่วยคำนวณการใช้งานอินเทอร์เน็ต เพื่อช่วยให้เราเลือกแพ็กเกจได้เหมาะสม เช่น หากเราใช้งานอินเทอร์เน็ตทั่วไป ท่องเว็บไซต์ รับ/ส่งอีเมล ใช้งานโซเชียลเน็ตเวิร์ก ข้อมูล 500 MB ก็อาจเพียงพอกับการใช้งาน แต่ถ้าเราชอบดาวน์โหลดเพลงหรือวิดีโอ แชร์/ดูวิดีโอในโซเชียลเน็ตเวิร์ก ดู YouTube ด้วย อาจต้องใช้ข้อมูลตั้งแต่ 3 GB ขึ้นไป ซึ่งแตกต่างกันไปตามอุปกรณ์ที่ใช้

- AIS http://www.ais.co.th/4g/data-calculator/
- TRUE http://www.truemove-h.com/calculator.aspx
- DTAC https://www.dtac.co.th/postpaid/services/internet-calculator.html

ซึ่งแพ็กเกจก็มีให้เลือกหลายแบบ ทั้งแบบรายเดือน (Postpaid) และแบบเติมเงิน (Prepaid)

โปรแกรมคำนวณข้อมูลการใช้งาน

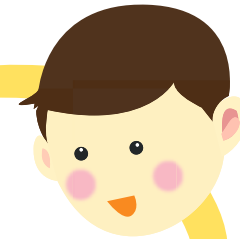
1. แบบรายเดือน ใช้ก่อนจ่ายทีหลัง

ผู้ให้บริการเครือข่ายมักจะคิดค่าอินเทอร์เน็ตเป็นค่าบริการแบบเหมาจ่ายไว้ เช่น ใช้บริการอินเทอร์เน็ต 3G/4G ความเร็วสูงสุดได้ที่ 6 GB ถ้าใช้เกินจากนี้แล้ว ความเร็วของอินเทอร์เน็ตก็จะเหลือเพียง 384 Kbps ถ้าต้องการความเร็วที่เพิ่มขึ้นก็สามารถซื้อแพ็กเกจเสริมได้ตามจำนวนข้อมูลที่ใช้ เช่น แพ็กเกจเสริมอินเทอร์เน็ต 3G/4G ความเร็วสูงสุด 1 GB ราคา 150 บาท ใช้ได้ 30 วัน

2. แบบเติมเงิน จ่ายก่อนใช้

การคิดค่าบริการมักจะคิดเป็น MB ซึ่งค่าบริการต่อ MB จะค่อนข้างสูง แต่ก็มีแพ็กเกจเสริมให้คนเล่นอินเทอร์เน็ตด้วยครับ เช่น สมัครแพ็กเกจหลัก โทร 0.50 บาท/นาที SMS 2 บาท/ครั้ง อินเทอร์เน็ต 1 บาท/MB ถ้าเติมเงิน 100 บาท แล้วเผลอไปใช้อินเทอร์เน็ตรับส่งข้อมูลแค่ 100 MB เงินก็หมดแล้ว พุดน้อยแนะนำให้ซื้อแพ็กเกจเสริมด้วย เช่น แพ็กเกจอินเทอร์เน็ตไม่อั้นความเร็ว 384 Kbps 30 วัน เพิ่มจากแพ็กเกจหลัก ซึ่งอาจจะจ่ายเพิ่มแค่ 100 บาท แต่ใช้อินเทอร์เน็ตแบบไม่จำกัดในเวลา 30 วัน

จากตัวอย่าง คุณพ่อพุดน้อยก็เลือกแพ็กเกจแบบรายเดือน โดยใช้อินเทอร์เน็ต 3G/4G ที่ความเร็วสูงสุดได้ 6 GB ครับ



น้องพุดดิ้งชวนรู้

รู้จักกับ Fair Usage Policy (FUP)

คือการจำกัดความเร็วในการใช้งานเครือข่ายโทรศัพท์มือถือในการเชื่อมต่ออินเทอร์เน็ต 3G/4G

ทำไมต้องมี Fair Usage Policy (FUP)

ผู้ให้บริการโทรศัพท์มือถือได้กำหนด Fair Usage Policy เพื่อกำหนดเงื่อนไขในการใช้งานข้อมูลผ่านเครือข่าย 3G/4G ให้สามารถใช้งานอินเทอร์เน็ตบนมือถือได้อย่างเต็มประสิทธิภาพ และใช้งานอย่างเหมาะสม หากใช้งานครบตามปริมาณการใช้งานที่กำหนดแล้ว ผู้ใช้งานจะได้รับ SMS เตือนว่าเราใช้แพ็กเกจความเร็วสูงสุดตามที่เครื่องรองรับครบแล้ว โดยที่ยังสามารถใช้งานอินเทอร์เน็ตต่อไปได้โดยไม่เสียค่าใช้จ่ายเพิ่มเติม แต่จะถูกปรับลดความเร็วลง ซึ่งขึ้นอยู่กับผู้ให้บริการว่าจะปรับลดเหลือความเร็วเท่าไหร่ ซึ่งส่วนใหญ่จะเหลือเพียงแค่ 384 Kbps จนกว่าจะครบรอบบิลตามแพ็กเกจ หรือซื้อแพ็กเกจอินเทอร์เน็ตเสริมเพิ่มเติม

สำหรับเพื่อนๆ ที่เดินทางไปต่างประเทศและต้องการใช้งานอินเทอร์เน็ต พุดน้อยวิธีการแนะนำอยู่สองวิธีครับ

1. ซื้อซิมการ์ดอินเทอร์เน็ตที่ประเทศปลายทาง

วิธีนี้เหมาะมากหากประเทศที่เราไปสามารถซื้อหาซิมการ์ดได้ง่าย และซิมการ์ดที่ซื้อจะต้องใช้กับโทรศัพท์เราได้ด้วย ซึ่งก่อนไปให้เพื่อนๆ ติดต่อกับผู้ให้บริการมือถือที่เพื่อนๆ ใช้งานอยู่ เพื่อสอบถามข้อมูลว่าประเทศที่จะไปนั้นใช้คลื่นความถี่อะไร จะได้รู้ว่าเครื่องที่มีอยู่สามารถนำไปใช้งานได้หรือเปล่าครับ

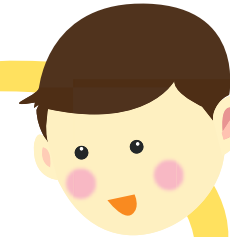
2. เช่า Pocket Wi-Fi จากประเทศไทยไปใช้ที่ประเทศปลายทาง

Pocket Wi-Fi เป็นอุปกรณ์ที่สามารถใส่ซิมการ์ดได้เหมือนกับโทรศัพท์มือถือ และสามารถกระจายสัญญาณอินเทอร์เน็ตผ่านสัญญาณ Wi-Fi ได้ ซึ่งทำให้ใช้อินเทอร์เน็ตพร้อมกันได้หลายเครื่อง โดยที่ผู้ให้บริการจะเป็นคนเตรียมเครื่องและซิมการ์ดที่เหมาะในการใช้งานของแต่ละประเทศมาให้เลย ไม่ต้องกลัวว่าจะหาซื้อซิมการ์ดที่ประเทศปลายทางไม่ได้

3. สมัครแพ็กเกจอินเทอร์เน็ตต่างประเทศ (โรมมิ่ง) ก่อนเดินทางจากผู้ให้บริการในไทย

สำหรับเพื่อนๆ ที่ต้องการรับสายโทรศัพท์จากประเทศไทย ระหว่างที่อยู่ประเทศปลายทางต้องใช้วิธีนี้ครับ เพราะจะทำให้เพื่อนๆ สามารถโทรออก/รับสายได้โดยใช้เบอร์โทรศัพท์เดิม แต่ต้องระวังเรื่องค่าใช้จ่ายนะครับ เพราะการใช้งานแบบนี้จะมีค่าใช้จ่ายในการรับสายด้วยครับ

นอกจากนี้แล้ว เพื่อนๆ จะต้องศึกษารายละเอียดของแพ็กเกจให้ดี เช่น เครือข่ายไหนของประเทศปลายทางที่อยู่ในแพ็กเกจ เพื่อจะได้ตั้งค่ามือถือให้ถูกต้อง ไม่ควรตั้งค่าการเลือกเครือข่ายของมือถือเป็นแบบอัตโนมัติ ควรตั้งค่าเครือข่ายด้วยตนเอง เพื่อป้องกันการเลือกเครือข่ายที่ไม่อยู่ในแพ็กเกจ และอาจเกิดค่าใช้จ่ายส่วนเกินได้นะครับ



น้องพุดดิ้งชวนรู้

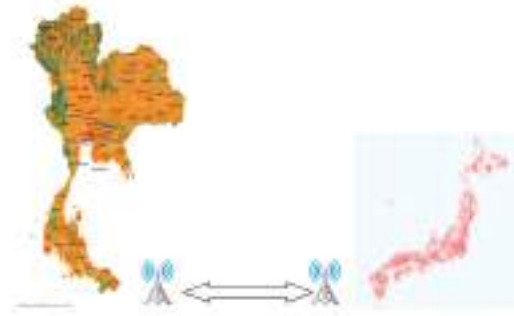
โรมมิ่ง (Roaming) คืออะไร?

โรมมิ่ง คือ บริการข้ามเครือข่าย ออกแบบมาเพื่อให้สามารถใช้สมาร์ตโฟนได้นอกพื้นที่ ซึ่งเครือข่ายที่เลือกใช้ส่งคลื่นความถี่ไปไม่ถึง โดยอาศัยเครือข่ายอื่นมาเป็นสื่อกลางในการเชื่อมต่อ แบ่งเป็น 2 แบบคือ โรมมิ่งในประเทศ (Local Roaming) และโรมมิ่งต่างประเทศ (International Roaming)

• **โรมมิ่งในประเทศ** (Local Roaming) เป็นการใช้งานโทรศัพท์ในประเทศ เกิดขึ้นเมื่อผู้ให้บริการเดียวกันมีคลื่นความถี่มากกว่าหนึ่งคลื่น หากผู้ใช้บริการออกนอกพื้นที่ให้บริการก็จะสลับไปใช้อีกคลื่นความถี่ที่สามารถให้บริการได้โดยไม่เสียค่าบริการเพิ่ม

• **โรมมิ่งต่างประเทศ** (International Roaming) เป็นการใช้งานโทรศัพท์ในต่างประเทศ โดยใช้เครือข่ายโทรศัพท์ของผู้ให้บริการต่างประเทศ ซึ่งเป็นการเชื่อมต่อเครือข่ายกันระหว่างสองประเทศ

โรมมิ่งในประเทศ



โรมมิ่งระหว่างประเทศ

เมื่อเพื่อนๆ ได้
Mobile Device
และ Package Internet ที่เหมาะสมแล้ว
คราวนี้เราจะมาเริ่มใช้
Mobile Internet กัน

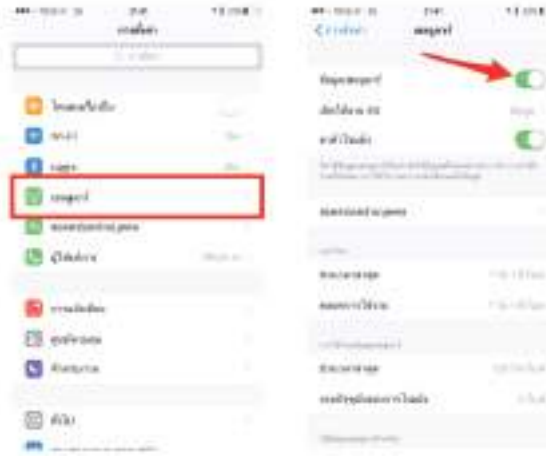
2.3 นับ 3...Mobile Internet ฉบับมือใหม่

อินเทอร์เน็ต (Internet) คือ การเชื่อมโยงอุปกรณ์คอมพิวเตอร์เข้าด้วยกันเป็นเครือข่ายขนาดใหญ่ ผู้ใช้สามารถท่องเว็บไซต์ ดูวิดีโอ เล่นโซเชียลเน็ตเวิร์ก แชต วิดีโอคอล ได้อย่างสะดวก การเชื่อมต่อก็มีทั้งแบบใช้สายและแบบไร้สาย ซึ่งคอมพิวเตอร์เหล่านั้นต้องมีอุปกรณ์รับส่งสัญญาณที่สามารถรับส่งข้อมูลที่ต้องการผ่านเครือข่ายอินเทอร์เน็ตได้

ส่วน Mobile Internet คือการใช้งานอินเทอร์เน็ตผ่าน Mobile Device ที่มีอุปกรณ์เชื่อมกับระบบอินเทอร์เน็ตได้ในตัว ไม่ว่าจะเป็นการเชื่อมต่อกับเครือข่ายโทรศัพท์มือถือ หรือเชื่อมต่อกับ Wi-Fi

การใช้งาน Mobile Internet ผ่านเครือข่ายโทรศัพท์มือถือ ผู้ใช้งานต้องตั้งค่าเปิดใช้งานข้อมูลก่อน โดยเข้าไปที่การตั้งค่าโทรศัพท์ซึ่งจะแตกต่างกันไปตามยี่ห้อและเวอร์ชันของระบบปฏิบัติการ

ตัวอย่างการตั้งค่าเปิดใช้ข้อมูลของระบบปฏิบัติการแอนดรอยด์



▸▸ ตัวอย่างการตั้งค่าเปิดใช้ข้อมูลของระบบปฏิบัติการ iOS

ปัจจุบัน Mobile Device ไม่ว่าจะเป็นสมาร์ตโฟน แท็บเล็ต แฟบเล็ต จะสามารถเชื่อมต่อ Wi-Fi ได้ โดยอุปกรณ์แต่ละชิ้นจะมีวิธีการเปิด/ปิด Wi-Fi ที่แตกต่างกัน การใช้งาน Wi-Fi นิยมใช้ภายในอาคาร ซึ่งเมื่อเปิดใช้งาน Wi-Fi ในอุปกรณ์มือถือได้แล้ว ระบบจะทำการค้นหา “สัญญาณ Wi-Fi” ที่อยู่รอบๆ อุปกรณ์นั้น เพื่อนๆ สามารถเลือกได้ว่าจะใช้งานเครือข่าย Wi-Fi อันไหน ซึ่งอาจต้องใช้รหัสผ่านในการเข้าใช้งาน

▸▸ ตัวอย่างการตั้งค่า Wi-Fi ของระบบปฏิบัติการแอนดรอยด์

เมื่อเข้าใช้งาน Wi-Fi และ Wi-Fi ที่เชื่อมต่อนั้นมีการเชื่อมโยงกับอินเทอร์เน็ต เพื่อนๆ ก็จะสามารถเล่นอินเทอร์เน็ตได้เช่นเดียวกับการใช้คอมพิวเตอร์ และสามารถใช้งานแอปพลิเคชัน ที่ต้องใช้ข้อมูลจากอินเทอร์เน็ตได้ เช่น Facebook, Twitter, LINE, Google Maps, Safari เป็นต้น

แต่ Wi-Fi ก็มีข้อจำกัด คือสามารถเชื่อมต่อได้ในระยะที่ไม่ไกลนัก เมื่อเพื่อนๆ ต้องเดินทางไปเที่ยวไกลๆ สัญญาณ Wi-Fi จะไม่สามารถส่งไปถึง และหากจะให้สัญญาณ Wi-Fi ครอบคลุมทั่วประเทศ จะต้องตั้งเสาสัญญาณเยอะมาก ไม่คุ้มต่อการลงทุน จึงได้พัฒนาการส่งข้อมูลผ่านเครือข่ายมือถือขึ้นมา ซึ่งยุคแรกๆ นั้นเป็นการส่งข้อมูลผ่านโครงข่ายโทรศัพท์มือถือระยะที่ 2 (2G) โดยเทคโนโลยีที่เป็นที่นิยมก็คือ EDGE/GPRS ซึ่งปัจจุบันประเทศไทยได้เปิดให้บริการโครงข่ายโทรศัพท์มือถือระยะที่ 3 (3G) โดยมีเครือข่ายครอบคลุมเกือบ 100% ของประเทศ ทำให้เพื่อนๆ สามารถเชื่อมต่ออินเทอร์เน็ตความเร็วสูงได้ทุกที่ทุกเวลา ด้วยอุปกรณ์ที่รองรับบริการ 3G และหากอยู่ในพื้นที่ที่มีสัญญาณ 3G อ่อนมาก ระบบค้นหาสัญญาณในอุปกรณ์นั้นจะนำเทคโนโลยี EDGE/GPRS มาแทนโดยอัตโนมัติ

ส่วนเพื่อนๆ ที่ใช้อุปกรณ์เคลื่อนที่ซึ่งสามารถเชื่อมต่อเทคโนโลยี 4G คือเครือข่ายไร้สายความเร็วสูงก็จะสามารถส่งข้อมูล ด้วยสัญญาณและความเร็วที่มีคุณภาพมากกว่าเครือข่าย 3G ได้ต่อเนื่องไม่สะดุด และรับ-ส่งข้อมูลที่มีไฟล์ขนาดใหญ่ได้รวดเร็วขึ้น

การเปิดใช้งาน 3G/4G นั้น มีค่าใช้จ่ายดังที่พูดน้อยได้กล่าวไปในหัวข้อที่แล้ว การเชื่อมต่อก็ง่ายกว่า Wi-Fi เพราะไม่ต้องใส่รหัสผ่าน โดยผู้ใช้ต้องไปที่เมนูการจัดการเครือข่ายและการเชื่อมต่อ และทำการเปิดการใช้งาน 3G (Voice & Data) ก็สามารถเชื่อมต่อได้เลย

เวลาที่คุณพ่อของพุดน้อยไปต่างจังหวัด คุณพ่อจะเปิดการแชร์อินเทอร์เน็ต (Personal Hotspot) จากสมาร์ตโฟน เพื่อใช้ทำงานกับโน้ตบุ๊กของคุณพ่อได้เลย ซึ่งคุณพ่อบอกว่าสามารถตั้งค่าได้ไม่ยาก และสามารถกำหนดรหัสผ่านเพื่อไม่ให้ใครแอบมาใช้อินเทอร์เน็ตได้ด้วย

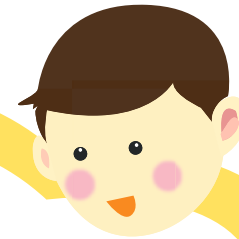
น้องพุดดิ้งชวนรู้

วิวัฒนาการของโทรศัพท์มือถือ

เรามีการแบ่งยุคของการพัฒนาโทรศัพท์มือถือเป็น Generation ต่างๆ ดังนี้

ยุคที่ 1 (1G) เป็นยุคที่มือถือรับส่งสัญญาณแบบแอนะล็อก (Analog) โดยส่งคลื่นเสียงผ่านสัญญาณวิทยุ ให้บริการเสียง (Voice) เพียงอย่างเดียว ไม่สามารถเชื่อมต่ออินเทอร์เน็ตหรือแม้แต่ส่งข้อความได้ มีปัญหาเรื่องความคมชัดของเสียงและปัญหาในด้านความปลอดภัย สามารถถูกดักฟังได้ง่าย หน้าจอโทรศัพท์แสดงเฉพาะตัวเลขเท่านั้น เครื่องโทรศัพท์มีขนาดใหญ่และมีน้ำหนักมาก

ยุคที่ 2 (2G) เป็นยุคแรกของเทคโนโลยีมือถือแบบดิจิทัล (Digital) ทำให้มีความคมชัดของสัญญาณเสียงมากขึ้น ป้องกันการดักฟังได้เนื่องจากมีการเข้ารหัสไว้ มีการส่งข้อความสั้น (Short Message Service หรือ SMS) ได้ และมีการใช้ SIM Card ที่สามารถบันทึกข้อมูลได้ หน้าจอโทรศัพท์สามารถแสดงได้ทั้งตัวอักษร ตัวเลข และรูปภาพ แต่หน้าจอยังเป็นแบบขาวดำอยู่



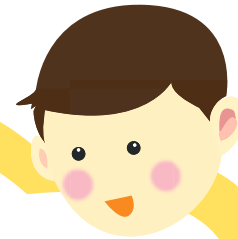
เทคโนโลยี 2G นอกจากให้บริการเสียง (Voice) แล้ว ยังสามารถส่งข้อมูล (Data) ได้ด้วย แต่มีการรับส่งข้อมูลที่ช้ามาก จึงมีการพัฒนาระบบ GPRS (General Packet Radio Service) หรือเรียกกันว่า 2.5G มีความเร็วอินเทอร์เน็ตสูงสุด 114 kbps แต่ในทางปฏิบัติความเร็วจะสูงสุดไม่เกิน 48 kbps ซึ่งถือว่าช้ามาก

ต่อมาจึงมีการพัฒนามาตรฐานเพิ่มขึ้นเรียกว่า EDGE (Enhanced Data Rates for Global Evolution) หรือเรียกว่ายุค 2.75G ความเร็วในการดาวน์โหลดข้อมูลสูงสุดอยู่ที่ 384 kbps ซึ่งเพียงพอในการรับส่งอีเมลและการเข้าใช้งานเว็บไซต์ทั่วๆ ไปได้

โทรศัพท์ในยุค 2.5-2.75G จึงเป็นยุคที่มีการส่งข้อมูลด้วยความเร็วที่มากขึ้น ทำให้เริ่มมีการให้บริการส่งข้อความ ภาพ และเสียงไปพร้อมๆ กัน (Multimedia Messaging Service หรือ MMS) ได้ โทรศัพท์เริ่มมีความสามารถหลากหลายขึ้น เริ่มมีการใช้จอสี ถ่ายรูปได้ ฟังเพลงได้ เชื่อมต่ออินเทอร์เน็ตได้

ยุคที่ 3 (3G) มีการรับส่งข้อมูลที่เร็วขึ้น โดยเริ่มต้นที่ความเร็ว 2 Mbps ทำให้สามารถเข้าดูเว็บไซต์ที่มีภาพเคลื่อนไหว ดูทีวี วิดีโอ เล่นเกมออนไลน์ได้ สามารถโทรศัพท์แบบเห็นหน้า (VDO Call) ได้ และได้มีการพัฒนาเทคโนโลยี 3.5G และ 3.9G ที่มีความเร็วในการเชื่อมต่ออินเทอร์เน็ตสูงสุดที่ 14.4 และ 42 Mbps ตามลำดับ

ยุคที่ 4 (4G) เป็นเทคโนโลยีสื่อสารไร้สายความเร็วสูงที่สามารถเชื่อมต่ออินเทอร์เน็ตด้วยความเร็วสูงสุดถึง 100 Mbps ทำให้สามารถใช้รับส่งไฟล์ขนาดใหญ่ ดูวิดีโอแบบความละเอียดสูง (High-Definition) เทคโนโลยี 4G จะเน้นให้บริการด้านข้อมูล (Data) เท่านั้น ถ้ามีการโทรหากันระบบจะเปลี่ยนไปใช้งานระบบ 3G ที่รองรับทั้ง Voice และ Data แทน ในประเทศไทยมีการใช้เทคโนโลยี 4G แบบ LTE (Long Term Evolution)



น้องพุดดิ้งชวนรู้

ข้อควรระวังการใช้ Mobile Internet

ปัจจุบันจะพบว่า Mobile Internet เข้ามามีบทบาทในชีวิตประจำวันของเรามาก โดยเฉพาะอย่างยิ่ง Social Network ที่มีทั้งคนดีและคนไม่ดี ดังนั้นจึงต้องมีวิธีการป้องกันและยึดถือปฏิบัติเพื่อให้ตนเองห่างจากภัยอันตรายต่างๆ และเพื่อความมั่นคงปลอดภัยของตนเอง ดังนี้

1. การใช้ Mobile Internet ต้องระมัดระวังในการเปิดเผยข้อมูลส่วนตัว เช่น เบอร์โทรศัพท์มือถือ วันเดือนปีเกิด อาชีพ ที่อยู่ ฯลฯ ซึ่งจะเป็นช่องทางให้มิจฉาชีพ หรือผู้ประสงค์ร้ายนำข้อมูลไปใช้ในการยืนยันตัวตนทำธุรกรรมต่างๆ ได้

2. การใช้ Mobile Internet ไม่ควรโพสต์แจ้งสถานะต่างๆ ว่าอยู่ที่ไหนหรือกำลังจะไปไหนนานเท่าไหร่ เพราะเป็นช่องทางให้มิจฉาชีพมาเยี่ยมบ้านเวลาที่คุณไม่อยู่ก็ได้ หรือผู้ไม่ประสงค์ดีมาดักทำร้ายได้จากข้อมูลของเราเอง

3. ใช้ Mobile Internet ไม่ควรรับแอดคนที่ไม่รู้จัก คุณต้องพิจารณาให้ดีก่อนรับใครเป็นเพื่อน และไม่ควรไปพบเพื่อนที่รู้จักกันในโซเชียลมีเดียโดยที่ไม่รู้จักภูมิหลัง

4. ใช้ Mobile Internet ต้องระวังภัยคุกคามทางไซเบอร์ โดยเฉพาะไวรัส สแปม โทรจัน หรือสคริปต์ต่างๆ ผ่านลิงก์ที่แนบมาในข้อความ ดังนั้นถ้าคุณไม่แน่ใจอย่าคลิกลิงก์เด็ดขาด

5. ใช้ Mobile Internet ต้องระมัดระวังในการแสดงความคิดเห็นที่นำมาสู่ความแตกแยก การโพสต์ข้อความที่ไม่เหมาะสม การโพสต์ข้อความพาดพิงถึงบุคคลที่ 3 ในทางเสียหาย เพราะถือเป็นการกระทำความผิดตามกฎหมาย

6. ใช้ Mobile Internet ต้องไม่ปักใจเชื่อสิ่งที่ได้ยิน ได้อ่านจากโซเชียลมีเดีย โดยเฉพาะข้อความที่แชร์กันต่อๆ มาหรือข่าวลืออื่นๆ

ชีวิตออนไลน์ ด้วยมือถือเครื่องเดียว

ด้วยมือถือเครื่องเดียว
พุดน้อยสามารถติดตามข่าวสาร
ความเคลื่อนไหวของเพื่อน
ได้ตลอดเวลาเลยครับ

3.1 Social Network ทุกนาทีคือกิจกรรมยอดฮิต

สมาร์ตโฟนเป็นอุปกรณ์สื่อสารที่คนนิยมใช้มากขึ้นเรื่อยๆ ราคาก็ถูกลงมากๆ สามารถเชื่อมต่ออินเทอร์เน็ตได้ตลอดเวลา มีแอปพลิเคชันที่ช่วยในการสื่อสารมากมาย ทำให้สามารถสื่อสารได้ทั้งทางเสียง ทางภาพนิ่งหรือภาพเคลื่อนไหวได้ด้วย

สมาร์ตโฟนสามารถใช้ได้ทั้งวัน เรียกว่าตั้งแต่ตื่นนอนจนเข้านอนเลยทีเดียว ใช้เป็นนาฬิกาปลุก ใช้ดูเวลาระหว่างวัน ตื่นมาก็เช็กสถานะ Facebook เช็กข้อความ LINE เช็กอีเมล อัปเดตสถานะระหว่างเดินทาง สำหรับคนที่ใช้บริการรถสาธารณะก็ใช้สมาร์ตโฟนอ่านข่าวออนไลน์ อ่าน News feed ของ Facebook หรือ LINE หรือจะดูคลิปจาก YouTube หรือฟังเพลง สำหรับคนที่ใช้รถส่วนตัวก็ใช้สมาร์ตโฟนสำหรับวางแผนก่อนเดินทาง หาเส้นทาง เช็กสภาพการจราจร

เวลาหิวก็ใช้แอปพลิเคชัน เพื่อสั่งอาหารมารับประทานได้ ซื้อสินค้าออนไลน์ โอนเงิน ชำระเงิน และอีกมากมาย เรียกได้ว่ามีสมาร์ตโฟนเครื่องเดียวก็สามารถใช้บริการออนไลน์ได้เกือบทุกอย่าง ทำให้คนยุคนี้ขาดสมาร์ตโฟนไม่ได้แล้วครับ

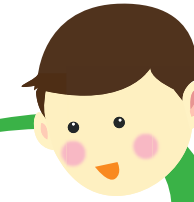
จากการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2559 ของ ETDA พบว่า กิจกรรมยอดฮิตสำหรับ Mobile Device คือ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) รองลงมาก็คือ การชมวิดีโอผ่าน YouTube และการอ่านหนังสืออิเล็กทรอนิกส์ ตามลำดับ โดยที่ Facebook เป็นเครือข่ายสังคมออนไลน์ที่มีคนใช้มากที่สุด

Facebook สังคมออนไลน์ยอดฮิต

ในปี 2559 มีผู้ใช้ Facebook ทั่วโลกถึง 1,590 ล้านคน และในประเทศไทยมีผู้ใช้งาน 38 ล้านคน ซึ่ง 90% เป็นการใช้งานผ่านโทรศัพท์มือถือ Facebook ทำให้คุณพ่อของพุดน้อยได้เจอเพื่อนเก่าๆ มากมาย ซึ่งบางคนไม่ได้เจอกันตั้งแต่เรียนจบ ทำให้คุณพ่อรู้ข่าวสารของเพื่อนๆ ได้ง่ายขึ้น เพียงแค่อ่าน News feed ของ Facebook ซึ่งเพื่อนๆ ของคุณพ่อก็จะแชร์รูปภาพ วิดีโอ เช็กอินสถานที่ที่ไปเที่ยว ไปกิน หรือทำกิจกรรมต่างๆ คุณพ่อก็จะไปกดไลค์และแสดงความคิดเห็นไว้ด้วย

- **คุณแม่**ของพุดน้อยกดไลค์เพจเกี่ยวกับการดูแลรักษาบ้าน หรือเพจอื่นๆ ที่คุณแม่สนใจเพื่อติดตามข้อมูลดีๆ จากเพจเหล่านี้ กดไลค์เพจเกี่ยวกับสินค้าหรือบริการ เพื่อดูสินค้า ติดตามโปรโมชัน และสามารถสั่งซื้อได้อีกด้วย

- **คุณพ่อ**ก็สมัครเข้าร่วมกลุ่มจักรยาน เป็นชมรมจักรยานที่คุณพ่อไปปั่นด้วยเสมอ ซึ่งในกลุ่มก็จะมีการพูดคุยแลกเปลี่ยนความรู้ นัดปั่นจักรยาน ขายจักรยานมือสอง และเรื่องต่างๆ ที่เกี่ยวกับจักรยาน แต่คุณพ่อมักจะเตือนพุดน้อยว่าอย่าแชร์ข้อมูลส่วนตัวแบบสาธารณะ เช่น ข้อมูลตำแหน่งที่อยู่ หรือภาพถ่ายภายในบ้าน เพราะหากผู้ไม่หวังดีได้ข้อมูลพวกนี้ไปอาจจะเข้ามาขโมยของที่บ้านเรา ขณะที่ไม่มีใครอยู่ก็ได้ครับ



น้องพุดดิ้งชวนรู้

ข้อคิดในการใช้ Social Network

การแชร์รูป แชร์กิจกรรม เช็กอิน อัปเดตสถานะตลอด จะเป็นข้อมูลให้มิจฉาชีพนำไปใช้ในทางที่ผิดได้

อีกอย่างหนึ่งที่คุณพ่อพูดย้ำกับพุดน้อยว่า อย่ารับแอดคนแปลกหน้าหรือแม้กระทั่งเป็นรูปคนรู้จัก เพราะปัจจุบันมีการปลอมตัวใน Facebook มากมาย สามารถเซฟรูปจากโปรไฟล์อื่นแล้วมาทำโปรไฟล์ปลอมได้ง่ายๆ ทางที่ดีควรจะถามเพื่อนให้แน่ใจก่อนว่าเป็นตัวจริงถึงจะรับแอด และยิ่งถ้าเป็นคนแปลกหน้าก็อย่าไปรับแอดเลยเพราะอาจเป็นผู้ไม่หวังดีได้

การแชร์ข้อมูลที่แชร์ต่อๆ กันมาก็เหมือนกัน ควรตรวจสอบข้อมูลด้วยว่าเป็นเรื่องจริงหรือไม่ เช่น ข้อมูลการบริจาคเงิน เพราะเดี๋ยวนี้มีการตัดต่อเลขบัญชีเพื่อให้โอนเข้าบัญชีของตนเอง

การแชร์ข้อมูลโดยใช้ Facebook ข้อมูลสามารถกระจายไปได้อย่างรวดเร็ว หากข้อมูลนั้นทำผู้อื่นเกิดความเสียหายคนที่กดไลค์ หรือแชร์อาจถูกดำเนินคดีได้ครับ

Twitter สั้นกระชับฉับไว

Twitter (ทวิตเตอร์) เป็น Social Network ขนาดเล็กที่เรียกว่า Micro Blog มีลักษณะคล้ายๆ กับ Blog ทั่วไป แต่ต่างกันที่สามารถเขียนข้อความได้เพียง 140 ตัวอักษรเท่านั้น เพราะต้นกำเนิดของทวิตเตอร์มาจากการพัฒนาการส่งข้อความสั้น (SMS) จากโทรศัพท์มือถือในปี 2549

เดี๋ยวนี้ทวิตเตอร์ก็ยังคงรักษาเอกลักษณ์เดิมไว้ คือส่งข้อความหรือเรียกว่าทวีตได้เพียง 140 ตัวอักษร และได้พัฒนาให้ส่งรูป ส่งวิดีโอได้เหมือนกับ Social Network ทั่วๆ ไป พุดน้อยสามารถเชื่อมต่อกับเพื่อนๆ ของพุดน้อยและผู้คนที่น่าสนใจ โดยการไปติดตาม (Follow) เพื่อรับข่าวสารในสิ่งที่พุดน้อยสนใจอย่างทันท่วงที และติดตามเหตุการณ์ขณะที่กำลังเกิดขึ้นในเวลาจริงจากทุกมุมมอง

เช่น ในช่วงการแข่งขันฟุตบอลโลก คุณพ่อพุดน้อยจะตามแฮชแท็ก (Hashtag) #worldcup2014 เพื่อติดตามข่าวสารเฉพาะการแข่งขันฟุตบอลโลกในปีนั้น ระหว่างการแข่งขันก็จะมีแฮชแท็กของแต่ละคู่ด้วย เช่น คู่ชิงชนะเลิศระหว่างเยอรมันกับอาร์เจนตินาก็จะใช้ #GERvARG เพื่อติดตามข่าวสารขณะที่กำลังแข่งกัน

Twitter ยังมีแฮชแท็กแนะนำให้พุดน้อยติดตามด้วย โดยจะดูจากความนิยมในการใช้แฮชแท็กในช่วงเวลานั้น เช่น ช่วงที่ละครกำลังฉายก็จะมีแฮชแท็กชื่อของละครนั้น เช่น #นาคี แฮชแท็กที่ถูกแนะนำเหล่านี้แสดงให้เห็นถึง Trends ในขณะนั้น ทำให้รู้ว่าช่วงเวลานั้นผู้คนสนใจเรื่องอะไรกันอยู่บ้าง

ประโยชน์ของ Twitter มีเยอะจนคาดไม่ถึงเลยใช่ไหมครับ จริงๆ ยังมีประโยชน์มากกว่านี้อีกซึ่งพุดน้อยคงกล่าวได้ไม่หมดครับ เพื่อนๆ คงอยากลองใช้ Twitter บ้างแล้วละสิ ลองใช้แล้วก็อย่าลืมมา Follow พุดน้อยบ้างนะครับ

น้องพุดดิ้งชวนรู้

คำแนะนำในการใช้ Twitter

- จากข้อจำกัดของ Twitter ที่สามารถทวีตได้เพียง 140 ตัวอักษรเท่านั้น ทำให้อาจมีการตีความหมายผิดไปจากความตั้งใจของผู้ทวีตได้
- การทวีตข้อความออกไปแล้ว ไม่สามารถแก้ไขข้อความนั้นได้เหมือนกับ Facebook ดังนั้นก่อนทวีตต้องคิดให้ดี
- ข้อความที่ทวีตจะมีการกระจายอย่างรวดเร็ว จึงไม่ควรทวีตสิ่งที่ไม่เป็นความจริง หรือข่าวลือที่ยังไม่ได้รับการยืนยันแน่นอน
- ไม่รีทวีตข่าวหรือข้อความที่เราไม่แน่ใจว่าเป็นความจริงหรือไม่
- ไม่แชร์ตำแหน่งไปกับทวีตโดยไม่จำเป็น

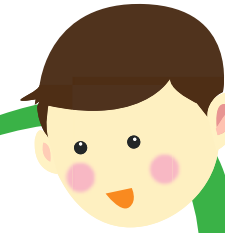
Instagram

Instagram (อินสตาแกรม) คือ แอปพลิเคชันถ่ายภาพและวิดีโอที่สามารถปรับแต่งภาพได้ตามแบบที่เพื่อนๆ ต้องการด้วยฟิลเตอร์ที่แอปพลิเคชันเตรียมไว้ให้ ซึ่งมีหลากหลายอารมณ์ ภาพหรือวิดีโอที่ถ่ายสัดส่วน 1:1 หรือเป็นสี่เหลี่ยมจัตุรัส นอกจากพุดน้อยจะโพสต์บน Instagram แล้วยังสามารถแชร์ไปยัง Facebook, Twitter, Tumblr และอื่นๆ อีกมากมายได้ในทันที หรือจะส่งตรงในรูปแบบข้อความส่วนตัวไปหาเพื่อนๆ ของพุดน้อยก็ได้

พุดน้อยสามารถค้นหาเพื่อนจาก Facebook และจากรายชื่อผู้ติดต่อในโทรศัพท์ของพุดน้อย หรือจากที่ Instagram แนะนำ และหากพุดน้อยต้องการเห็นโพสต์ของใครบนฟีดของพุดน้อย พุดน้อยก็จะแค่กดติดตามคนๆ นั้น

Instagram ก็เหมือนกับ Social Network ทั่วๆ ไป เพียงแต่การโพสต์จะต้องเป็นรูปหรือวิดีโอเท่านั้น และพุดน้อยสามารถกดไลค์หรือคอมเมนต์รูปหรือวิดีโอของคนอื่นได้ด้วย

Instagram ยังมีฟีเจอร์เรียกว่า Photo Map ที่ทำให้ภาพหรือวิดีโอของเรามีการระบุตำแหน่งในแผนที่ด้วย แค่โพสต์ภาพหรือวิดีโอก็อาจถูกสะกดรอยจากผู้ไม่หวังดีได้ คุณพ่อเลยแนะนำให้พุดน้อยไม่ระบุตำแหน่งของรูปภาพที่โพสต์



น้องพุดดิ้งชวนรู้

คำแนะนำการใช้ Social Network อย่างอุ่นใจ

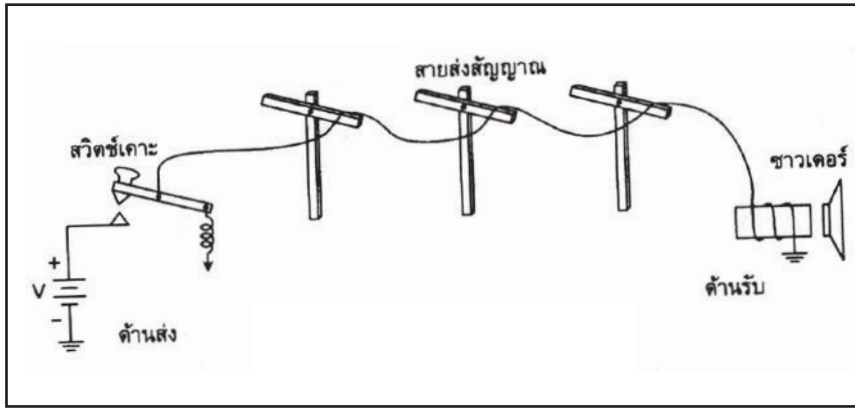
การใช้งาน Social Network เป็นการแชร์ข้อมูลส่วนตัวของเราในที่สาธารณะ ทำให้คนอื่นรู้ว่าเราเป็นใคร ทำอะไร อยู่ที่ไหน เรียนหรือทำงานอะไร มีเพื่อนเป็นใคร ชอบไปไหน ชอบกินอะไร บ้านอยู่ที่ไหน หรือรู้แม้กระทั่งเวลากลับบ้าน ซึ่งขึ้นอยู่กับว่าเพื่อนๆ แชร์ข้อมูลอะไรบ้าง ถ้ามิจฉาชีพนำข้อมูลเราไปใช้ เช่น คอยติดตามเราแอบเข้ามาขโมยของที่บ้านตอนเราไม่อยู่ หรือปลอมตัวเป็นเราเพื่อวัตถุประสงค์ไม่ดี และอีกมากมาย ดังนั้น เพื่อนๆ จำเป็นต้องสนใจเรื่องความมั่นคงปลอดภัยและป้องกันตัวเองจากภัยของโลกออนไลน์ด้วย

มีวิธีป้องกันตัวเองจากการใช้ Social Network มาแนะนำดังนี้

1. ตรวจสอบการเข้าถึงข้อมูลส่วนตัวจากแอปพลิเคชัน
2. ปิดการค้นหาแบบ Public Search เพื่อไม่ให้คนแปลกหน้าค้นหาชื่อเรา
3. Info Accessible เลือกแสดง/ซ่อนข้อมูลส่วนตัวที่จะให้เพื่อนเราเห็น
4. ปิดการระบุตำแหน่งเวลา Chat
5. อย่าเช็กอินที่บ้านของตัวเอง
6. อย่ารับแอดคนที่ไม่รู้จัก
7. ไม่กด Link แปลกๆ
8. เปลี่ยนพาสเวิร์ดทุก 3-6 เดือน

3.2 Chat ใกล้...ไกล คุยได้ ง่ายนิดเดียว

คุณพ่อพุดน้อยเล่าให้ฟังว่าสมัยก่อนโทรศัพท์ตามบ้านยังไม่ค่อย จะมี การสื่อสารทางไกลจะเป็นการเขียนจดหมาย แต่การส่งจดหมาย หากันก็ใช้เวลานานหลายวันกว่าจดหมายจะถึงมือผู้รับ หากจำเป็นต้อง ส่งข้อความด่วนจะต้องใช้บริการที่เรียกว่า โทรเลข ซึ่งเป็นการส่งข้อความ ที่เป็นรหัสมอสผ่านสายโทรเลขที่เชื่อมต่อระหว่างไปรษณีย์ เมื่อข้อความ ส่งถึงปลายทางก็จะมีการแปลรหัสให้เป็นข้อความและบุรุษไปรษณีย์ จะเป็นคนนำข้อความส่งถึงบ้านผู้รับทันที ซึ่งข้อความที่ส่งทางโทรเลข ต้องเป็นข้อความที่สำคัญและเร่งด่วนมาก เพราะคิดค่าส่งเป็นคำจึงมีราคาสูง



วงจรโทรเลข

การส่งข้อความโดยใช้เพจเจอร์

ก่อนที่โทรศัพท์เคลื่อนที่จะส่งข้อความหากันได้นั้น มีอุปกรณ์ที่ใช้รับข้อความโดยเฉพาะเรียกว่า เพจเจอร์ โดยผู้ส่งข้อความจะต้องโทรไปยังโอเปอเรเตอร์ เพื่อให้โอเปอเรเตอร์ส่งข้อความไปยังเครื่องของผู้รับ แต่เมื่อโทรศัพท์เคลื่อนที่มีระบบส่งข้อความสั้นที่เรียกว่า Short Message Service (SMS) ผู้ใช้งานสามารถส่งข้อความหากันเองได้โดยไม่ต้องผ่านโอเปอเรเตอร์ เพจเจอร์จึงเสื่อมความนิยมลงและปิดบริการไปในที่สุด

โทรศัพท์สามารถส่งข้อความหากันได้โดยตรง

ต่อมาบริษัท รีเสิร์ช อิน โมชั่น จำกัด (RIM) ผู้ผลิตโทรศัพท์เคลื่อนที่ยี่ห้อแบล็กเบอร์รี่ (BlackBerry) ได้พัฒนาโปรแกรมแชต (BlackBerry Messenger) หรือ BBM ขึ้น ซึ่งมีความแตกต่างจากการส่ง SMS ทั่วไปคือ BBM เป็นโปรแกรมที่ใช้ส่งข้อความระหว่างเครื่อง BlackBerry เท่านั้น โดยแต่ละเครื่องจะมีเลขประจำตัว Personal Identification Number (PIN) เอาไว้เป็นหมายเลขในการส่งข้อความหากัน ซึ่งนอกจากการรับส่งข้อความแล้ว ยังสามารถส่งไฟล์ภาพ อัดเสียงแล้วส่ง ส่งตำแหน่งทางภูมิศาสตร์ไปยังผู้รับได้ มีความสามารถในการแชตเป็นกลุ่มได้

เนื่องจาก BBM เป็นโปรแกรมที่ใช้ส่งข้อความระหว่างเครื่อง Black Berry เท่านั้น จึงได้มีคนพัฒนาแอปพลิเคชันที่สามารถส่งข้อความ ภาพ เสียง วิดีโอ ข้ามระบบปฏิบัติการได้ ไม่ว่าจะใช้โทรศัพท์ยี่ห้ออะไรก็ตาม เพียงแค่รู้เบอร์โทรศัพท์เพื่อนที่ใช้ WhatsApp ก็สามารถส่งข้อความหากันได้แล้ว

ในปัจจุบันแอปพลิเคชัน Chat ที่เป็นที่นิยมที่สุดของไทยก็คือ LINE มีผู้ใช้งานในประเทศไทยถึง 41 ล้านคน และทั่วโลกกว่า 560 ล้านคน ซึ่งความสามารถพื้นฐานของแอปพลิเคชัน Chat ในปัจจุบันนี้คือ การเพิ่มเพื่อนจากสมุดโทรศัพท์ การส่งข้อความรูปภาพ วิดีโอ เสียง สติกเกอร์ การโทรคุยผ่านอินเทอร์เน็ต พุดน้อยจะแนะนำแอปพลิเคชัน Chat ที่นิยมของคนไทยให้เพื่อนๆ รู้จักนะครับ

LINE ส่งข้อความฟรีทุกที่ทุกเวลา

LINE เป็นแอปพลิเคชันสำหรับส่งข้อความที่ได้รับความนิยมในการติดต่อสื่อสารของคนยุคนี้ ด้วยการใช้งานที่ง่าย ไม่ซับซ้อน ติดตั้งง่าย แค่ลงแอปพลิเคชันและใช้เบอร์โทรศัพท์ก็สามารถติดต่อกับเพื่อนที่ใช้ LINE ได้แล้ว โดยสามารถส่งข้อความและยังมีสติกเกอร์แสดงความรู้สึกน่ารักๆ มากมาย ส่งรูปวิดีโอ ข้อความเสียง มีฟังก์ชันโทรฟรีและวิดีโอคอลฟรีผ่านอินเทอร์เน็ต (แต่ต้องเสียค่าบริการอินเทอร์เน็ตนะครับ) นอกจากนี้ยังสามารถแชร์ Location ได้อีกด้วย

การสนทนาทาง LINE

นอกจากเป็นแอปพลิเคชันสำหรับสมาร์ตโฟนแล้ว LINE ยังสามารถติดตั้งได้ทั้งบนระบบปฏิบัติการ Windows และ Mac OS ซึ่งทำให้คนที่ใช้คอมพิวเตอร์ก็สามารถคุยกับคนที่ใช้สมาร์ตโฟนได้ โดยใช้ LINE ID เดียวกันกับที่สมัครไว้กับสมาร์ตโฟน

LINE ได้เพิ่มความสามารถขึ้นเรื่อยๆ โดยมีหน้าไทม์ไลน์ไว้สำหรับแชร์ข้อความ รูปภาพ วิดีโอ และสติกเกอร์ เพื่อแลกเปลี่ยนเรื่องราวต่างๆ กับเพื่อนสนิทของเรา

คุณสมบัติของ LINE ที่เป็นที่นิยมอีกอย่างหนึ่งก็คือ LINE Group ซึ่งเป็นการ Chat เป็นกลุ่ม พูดน้อยเป็นสมาชิกของกลุ่มครอบครัว ทำให้ครอบครัวเราสื่อสารกันได้ง่ายขึ้น ส่วนคุณพ่อจะใช้กลุ่มสำหรับคุยกับเพื่อนร่วมงาน คุณแม่มีกลุ่มแม่บ้าน คุณปู่ก็มีกลุ่มเพื่อนร่วมรุ่นสมัยเรียน เรียกว่าทำให้ไม่ขาดการติดต่อกันเลย

แต่บางครั้งการใช้ LINE มากเกินไป เช่น การส่งข้อความเข้าไปในกลุ่มโดยไม่จำเป็นก็อาจทำให้พลาดข้อความที่สำคัญ อีกทั้งยังเป็นการรบกวนเพื่อนๆ อีกด้วย

LINE สามารถเพิ่มเพื่อนโดยอัตโนมัติเพียงแค่เราบันทึกเบอร์เอาไว้ในสมุดผู้ติดต่อของสมาร์ตโฟน ดังนั้น หากเราตั้งค่าให้เพิ่มเพื่อนอัตโนมัติ เขาก็จะสามารถเข้ามาเห็นไทม์ไลน์เราได้ ซึ่งสำหรับเพื่อนหรือคนรู้จักคงไม่เป็นไร แต่ถ้าเป็นผู้ไม่หวังดีแล้วก็ไม่ปลอดภัยเลย ดังนั้น การแชร์อะไรก็ตามบนไทม์ไลน์จะต้องระมัดระวังเสมอนะครับ

Messenger แอปพลิเคชัน แชตจาก *Facebook*

Messenger เป็นแอปพลิเคชันที่แยกออกมาจากแอปพลิเคชันหลักของ Facebook ใช้สำหรับส่งข้อความคุยกับเพื่อนใน Facebook รวมถึงคนที่อยู่ในสมุดโทรศัพท์ของเรา โดยที่คนคนนั้นยังไม่ได้เป็นเพื่อนเราใน Facebook สามารถใช้โทรหากันผ่านอินเทอร์เน็ตได้ รองรับการสนทนาเป็นกลุ่ม มีสติกเกอร์ให้ใช้เหมือนกับ LINE สามารถบันทึกเสียงแล้วส่ง แชร์ตำแหน่งที่ตั้งได้เหมือนกับแอปพลิเคชัน Chat ทั่วไป นอกจากนี้ยังสามารถส่งภาพเคลื่อนไหวประเภท GIF ได้อีกด้วย

BeeTalk หาเพื่อนใหม่รอบๆ ตัว

BeeTalk เป็นแอปพลิเคชันที่นิยมในหมู่วัยรุ่นเมืองไทย สามารถสมัครใช้ได้เพียงมีเบอร์โทรศัพท์หรือใช้บัญชี Facebook การใช้งานตอนแรกก็จะคล้ายๆ กัน คือ ทำการค้นหาเพื่อนจากรายชื่อในโทรศัพท์ของเรา หรือจากรายชื่อเพื่อนใน Facebook จุดเด่นของ BeeTalk ก็คือสามารถหากลุ่มเพื่อนรอบๆ ตัวเราได้ตามความสนใจ เช่น เพื่อนปั่นจักรยาน เพื่อนช้อปปิ้ง หรือเพื่อนในหมู่บ้านและที่ทำงาน ด้วยฟังก์ชันคลับของ BeeTalk หรือจะเข้าไปใช้บอร์ดซึ่งมีเรื่องราวน่าสนใจมากมาย มีการแบ่งตามหมวดคล้ายกับเว็บบอร์ดบนคอมพิวเตอร์ แต่ใช้ง่ายกว่าเพราะออกแบบมาให้ใช้งานบนโทรศัพท์มือถือโดยเฉพาะ การส่งข้อความหรือแชตก็มีฟังก์ชันกระซิบ ที่ข้อความจะหายไปหลังจากเปิดอ่าน นอกจากนี้ เรายังสามารถวาดรูปและส่งสติกเกอร์ให้เพื่อนๆ ได้อีกด้วย

ถ้าพูดน้อยจะเปรียบการใช้งาน Facebook กับ BeeTalk อาจกล่าวได้ว่า Facebook เอาไว้ค้นหาเพื่อนเก่า BeeTalk เอาไว้หาเพื่อนใหม่ แต่เพื่อนๆ ต้องระมัดระวังในการคุยกับคนแปลกหน้าด้วยนะครับ อย่าพึ่งไว้ใจใครง่ายๆ ล่ะ

ดูหนัง ฟังเพลง เล่นเกม
รวมความบันเทิง
ไว้ในสมาร์ตโฟนเครื่องเดียว

3.3 Entertainment พกความบันเทิงไปได้ทุกที่

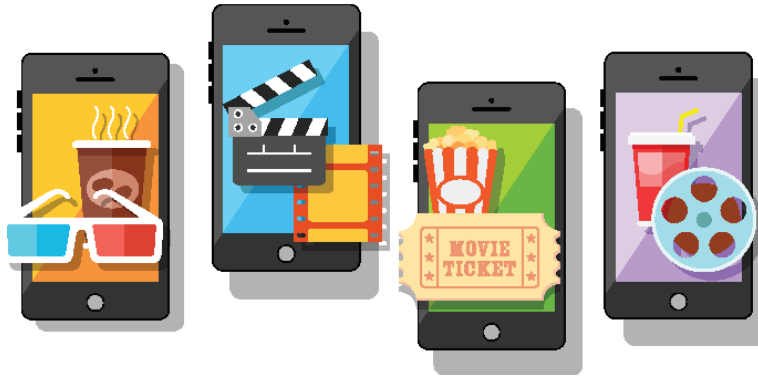
ฟังเพลง

ในประเทศไทยค่ายเพลงเกือบทุกค่ายจะมีช่อง YouTube เป็นของตนเองเพื่อเผยแพร่เพลงของศิลปิน สามารถดูและฟังได้ฟรี หากเพลงนั้นมีคนฟังและส่งต่อกันเยอะ ก็จะทำให้ศิลปินนั้นดังขึ้นมาได้ เช่น ศิลปินเกาหลีชื่อ “ไช” ที่ดังจากเพลง “กังนัมสไตล์” ด้วยเหตุนี้ คุณแม่ของพุดน้อยเลยได้ฟังเพลงใหม่ๆ เสมอ และหากชอบเพลงนั้น คุณแม่ก็จะซื้อมาฟังทีหลัง

ดูทีวีแบบสดๆ

สมาร์ตโฟนมีแอปพลิเคชันสำหรับดูทีวีมากมาย ซึ่งมีทั้งแอปพลิเคชันของช่องเอง และแอปพลิเคชันรวมช่องทีวีมีแบบดูสดได้อย่างเดียว และแบบดูย้อนหลังก็ได้ แถม YouTube มีบริการที่เรียกว่า YouTube Live ที่ทำให้ผู้ที่มีบัญชี YouTube สามารถถ่ายทอดสดรายการของตนเองได้ ทีวีหลายช่องจึงเชื่อมต่อสัญญาณสดมาออกอากาศทาง YouTube และยังสามารถเลื่อนดูย้อนหลังในขณะที่กำลังถ่ายทอดสดได้อีกด้วย คุณพ่อของพุดน้อยชอบมาก เพราะเวลาดูบอลแล้วดูจังหวะรีเพลย์ไม่ทัน คุณพ่อสามารถเลื่อนไปดูจังหวะยิงประตูกี่ครั้งก็ได้

นอกจากช่องทีวีที่มาใช้ YouTube ออกอากาศแล้ว ยังมีช่องที่ผลิตรายการออกทาง YouTube เพียงอย่างเดียว ทำให้พุดน้อยมีตัวเลือกที่จะชมรายการได้มากมาย โดยเฉพาะช่องที่เกี่ยวกับการศึกษา มีพี่ๆ ใจดีได้ทำคลิปวิดีโอสอนหนังสือเอาไว้ให้ด้วย แถมมีบทเรียนที่พุดน้อยเรียนอยู่พอดีเลย พุดน้อยเลยไม่ต้องเสียเงินไปเรียนพิเศษเพิ่มเลย



Streaming เพลงนับล้านฟังฟรีได้ทั้งออนไลน์และออฟไลน์

พุดน้อยเล่าให้คุณพ่อฟังว่า เพื่อนๆ ของพุดน้อยแนะนำว่า มีแอปพลิเคชันสำหรับฟังเพลงฟรี มีเพลงนับล้านเพลงให้เลือกฟังทั้งเพลงไทย เพลงสากล โดยสามารถเลือกฟังแบบฟรีหรือแบบเสียค่าสมาชิก ยกตัวอย่าง เช่น แอปพลิเคชัน JOOX ที่เราสามารถเลือกเพลงมาเก็บไว้ฟังในแอปพลิเคชันในขณะไม่ได้เชื่อมต่ออินเทอร์เน็ต นอกจากนี้ยังมีโหมดคาราโอเกะร้องเพลงคลอตามได้ในขณะกำลังฟังเพลง แต่คุณพ่อก็แนะนำพุดน้อยว่าเพลงทุกเพลงล้วนแล้วแต่มีลิขสิทธิ์ ต้องระมัดระวังไม่ดาวน์โหลดหรือแจกจ่าย หรือทำอะไรที่เป็นการผิดกฎหมายลิขสิทธิ์

การซื้อเพลงที่ถูกต้องตามลิขสิทธิ์

คุณพ่อบอกว่าในสมาร์ตโฟนมีแอปพลิเคชันที่ซื้อเพลงอยู่แล้ว สามารถค้นหาเพลงได้ทุกยุค ทุกแนว แต่จะต้องมีบัญชีที่ผูกกับธนาคารไว้เพื่อซื้อเพลง เมื่อซื้อแล้วเพลงจะเป็นของเราไปตลอด สามารถใช้บัญชีของเราดาวน์โหลดเพลงกี่ครั้งก็ได้ คุณภาพของเสียงเพลงก็ดี ซึ่งปัจจุบันเพลงหนึ่งเพลงมีราคาเทียบได้กับข้าวจานเดียวเท่านั้น ถ้าซื้อเป็นอัลบั้มก็จะถูกลงอีก และการซื้อเพลงยังเป็นการสนับสนุนศิลปิน สนับสนุนค่ายเพลงให้สามารถสร้างสรรค์งานให้เราได้ฟังต่อไป เพื่อนๆ ได้ยินแบบนี้แล้ว เรามาซื้อเพลงถูกลิขสิทธิ์ฟังกันดีกว่าครับ

นอกจากการซื้อเพลงมาเป็นของตัวเองแล้ว ยังมีแอปพลิเคชันสำหรับฟังเพลงเป็นรายเดือน สามารถฟังเพลงได้ไม่จำกัดโดยไม่ต้องซื้อเป็นเพลงๆ แต่ต้องเสียค่าบริการรายเดือนแทน เหมาะสำหรับคนที่อยากจะฟังเพลงเยอะๆ ปัจจุบันมีผู้ให้บริการทั้งไทยและต่างประเทศมากมายให้เลือก จนพุดน้อยเลือกไม่ถูกเลยล่ะครับ แต่สำหรับเพื่อนๆ ที่อยากลองใช้บริการ ก็ควรตรวจสอบเงื่อนไขการให้บริการให้ดีนะครับ

น้องพุดดิ้งชวนรู้

ดูหนังออนไลน์

เสริมสักนิดสำหรับเพื่อนๆ ที่อยากดูภาพยนตร์ แต่ไม่ค่อยมีเวลาว่าง เพราะต้องใช้ชีวิตไปกับการทำงานและเดินทางนอกสถานที่ พุดดิ้งมีวิธีที่คุณพ่อมักใช้เป็นประจำ คือ ใช้การดาวน์โหลดแอปพลิเคชันดูหนังออนไลน์ เช่น แอปพลิเคชัน Hollywood HDTV คลังหนังฮอลลีวูดพรีเมียมถูกลิขสิทธิ์ พร้อมทั้ง Soundtrack และพากย์ไทย มากกว่า 10,000 เรื่อง ดูได้ทันที ไม่ต้องดาวน์โหลด ไม่เสียเวลาและเปลืองเนื้อที่หน่วยความจำอุปกรณ์ คุณพ่อบอกว่าต่อไปถ้าอยากดูหนัง ก็สามารถเลือกดูจากแอปพลิเคชัน ซึ่งจะประหยัดเงินและประหยัดเวลาเดินทางไปได้อีก

จะไปไหนมาไหนก็สะดวก
ด้วยแผนที่นำทาง
ไม่ต้องกลัวหลงทางอีกต่อไป

3.4 Location Base แผนที่ย่อส่วน

เดี๋ยวนี้ไม่ค่อยเห็นใครพกแผนที่ใหญ่ๆ กันแล้ว ไม่ว่าจะเป็นคนไทยหรือนักท่องเที่ยว เพราะว่าสมาร์ตโฟนมีแอปพลิเคชันแผนที่นำทางนี่เอง เวลาคุณพ่อพาพุดน้อยไปเที่ยว ก็จะดูแผนที่จากสมาร์ตโฟนที่ยึดไว้กับกระจกรถ ทำให้พวกเราไม่หลงทาง สามารถไปถึงจุดหมายได้ถูกต้อง

สมาร์ตโฟนปัจจุบันจะมีระบบ GPS ที่สามารถระบุตำแหน่งของโทรศัพท์ได้ เมื่อนำตำแหน่งไปใช้กับแผนที่นำทางก็จะสามารถแสดงตำแหน่งของเราบนแผนที่ได้อย่างแม่นยำ คำนวณเส้นทางไปยังตำแหน่งที่ต้องการได้ มีการบอกสภาพการจราจร และตัวเลือกในการเดินทาง เช่น หลีกเลี่ยงทางหลวง ไม่ขึ้นทางพิเศษ แอปพลิเคชันก็จะคำนวณเส้นทางให้ใหม่

ตอนพุดน้อยไปต่างจังหวัด คุณพ่อมักจะใช้แอปพลิเคชัน เพื่อค้นหาร้านอาหารเด็ดๆ ที่อยู่ใกล้ๆ ที่พัก หรือระหว่างทางที่ผ่าน พุดน้อยเลยได้กินของอร่อยๆ ตลอดการเดินทางเลย บางครั้งน้ำมันรถใกล้จะหมด คุณพ่อก็ใช้แอปพลิเคชัน เพื่อหาปั๊มน้ำมันที่ใกล้ที่สุดได้อีกด้วย สามารถใช้ค้นหาโรงแรมที่พัก และอื่นๆ อีกมากมาย

ยังมีแอปพลิเคชันอีกหลายอย่างที่ใช้ประโยชน์จาก Location Base เช่น แอปพลิเคชันเรียกแท็กซี่ บางครั้งคุณพ่อไม่สามารถมารับพุดน้อยได้ คุณพ่อก็จะใช้แอปพลิเคชันเรียกแท็กซี่มารับพุดน้อยได้เลย โดยคนขับจะรู้ตำแหน่งของผู้โดยสาร คนเรียกก็จะรู้ว่าใครเป็นคนขับ คนขับสามารถโทรมาหาคนเรียกได้ และระหว่างทางสามารถดูได้ว่าตำแหน่งของรถแท็กซี่นั้นอยู่ที่ไหน คุณพ่ออุ่นใจได้เลยครับ

มีบางครั้งคุณพ่อจะไปบ้านเพื่อน แต่หาทางไปไม่ถูก เพื่อนของคุณพ่อก็ส่ง Location มาให้ทางข้อความ เมื่อคุณพ่อได้แล้วก็ใช้ Location นั้นนำทางไปยังบ้านเพื่อนได้ถูกต้อง ใน Social Network ไม่ว่าจะเป็น Facebook, Twitter หรือ LINE เพื่อนๆ สามารถใช้ฟังก์ชันที่เรียกว่า การ Check-in เพื่อบอกให้คนรู้ว่าตอนนี้เราอยู่ที่ไหน คุณพ่อบอกว่าเราไม่จำเป็นต้องเช็กอินหรืออัปเดตตลอดเวลา เพราะอาจมีผู้ไม่หวังดีคอยติดตามเรา หรือแอบมาขโมยของที่บ้านของเราตอนเราไม่อยู่ได้

ถ้าอีคอมเมิร์ซทำให้พุดน้อย
สะดวกสบาย ไม่ต้องไปซื้อของที่ร้าน
แล้วละก็ เอ็มคอมเมิร์ซยิ่งทำให้พุดน้อย
สบายขึ้นไปใหญ่ เพราะไม่ต้องเปิดคอมพิวเตอร์
ก็สามารถซื้อของได้แล้ว มีสมาร์ตโฟนเครื่องเดียว
ก็ซื้อขายสินค้าออนไลน์ได้ทุกที่ทุกเวลาจริงๆ

3.5 Shopping (Local) ซื้อสินค้าออนไลน์แค่ปลายนิ้ว

ช้อปปิ้งออนไลน์ด้วยมือถือเครื่องเดียว

ประเทศไทยมีคนซื้อขายสินค้าผ่านอินเทอร์เน็ตมากมาย นับวันก็ยิ่งจะมากขึ้นเรื่อยๆ ตามจำนวนผู้ใช้อินเทอร์เน็ต เป็นเพราะการเติบโตของผู้ใช้สมาร์ตโฟนและเครือข่าย 3G ที่ครอบคลุมเกือบทั้งประเทศ ทำให้การช้อปปิ้งผ่านโทรศัพท์มือถือเป็นที่นิยมแถมมีแอปพลิเคชันที่ช่วยในการซื้อขายอีกมากมาย แค่ถ่ายรูปแล้วโพสต์ก็สามารถขายสินค้าได้แล้ว ทำให้มีผู้ขายเพิ่มขึ้นเป็นจำนวนมาก ในขณะที่ผู้ซื้อก็สะดวก เพราะมีแอปพลิเคชันมากมายที่ช่วยในการเลือกซื้อสินค้า ซึ่งมีทั้งแอปพลิเคชันที่เป็นแหล่งรวมร้านค้าหลายๆ ร้าน เช่น Lazada, WeloveShopping, Tarad แอปพลิเคชันที่รวมคูปอง หรือดีลส่วนลดร้านค้า เช่น Priceza เป็นต้น และยังมีพ่อค้าแม่ค้าที่ขายของโดยใช้ Social Network เช่น Facebook, LINE, Instagram อีก เห็นด้วยกับพุดน้อยไหมครับว่า เพียงแค่มีสมาร์ตโฟนก็มีช่องทางที่จะช้อปปิ้งมากมายเลย

แอปพลิเคชันที่เป็นแหล่งรวมร้านค้า

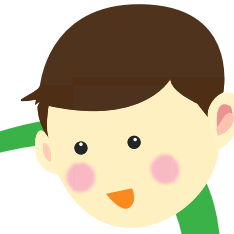
แอปพลิเคชันช้อปปิ้งเยอะจัง แล้วจะเริ่มจากแอปพลิเคชันอะไรดีนะ? พุดน้อยแนะนำให้เพื่อนเริ่มจากแอปพลิเคชันที่เป็นแหล่งรวมสินค้าก่อน จะรวมสินค้าจากผู้ขายหลายๆ ร้านแล้วมาจัดหมวดหมู่ให้ค้นหาง่าย ผู้ขายมีทั้งเป็นแบรนด์ใหญ่ๆ ขายเอง มีทั้งร้านค้าทั่วไป และบุคคลทั่วไปมาประกาศขาย มีการรับประกันสินค้าให้ด้วย การชำระเงินก็มีหลายวิธี และที่พุดน้อยชอบก็คือมีวิธีเก็บเงินปลายทางให้เลือกด้วย เช่น H&M, TopShop และ Zara เป็นต้น

แอปพลิเคชันดีลหรือคูปอง

เป็นแอปพลิเคชันที่รวมดีลต่างๆ ให้พุดน้อยได้เลือก เช่น คูปองอาหารมูลค่า 1,000 บาท แต่จ่ายเงินซื้อแค่ 499 บาท หรือเป็นสินค้าราคาพิเศษที่สามารถจัดส่งสินค้าได้เลยเหมือนซื้อสินค้าออนไลน์ทั่วไป สินค้าและบริการที่นิยมมาขายดีลมักจะเป็นสินค้าและบริการที่ขายดีตามช่วงเวลา เช่น ร้านอาหารจะขายดีช่วงสุดสัปดาห์ โรงแรมจะมีลูกค้ามากในฤดูท่องเที่ยว ดีลที่ขายก็จะมีการจำกัดช่วงเวลา เช่น ใช้ได้เฉพาะวันจันทร์ถึงวันพฤหัสบดีเท่านั้น หรือเป็นร้านค้าเปิดใหม่ ต้องการดึงลูกค้าไปใช้บริการเยอะๆ ซึ่งแอปพลิเคชันดีลจะมีฟังก์ชันค้นหาดีลที่อยู่ใกล้ๆ กับตำแหน่งที่เราอยู่ปัจจุบันได้ด้วย และหากซื้อดีล ดีลจะมีการบันทึกไว้ที่แอปพลิเคชัน และสามารถนำคูปองที่ได้ไปแสดงก่อนใช้บริการได้เลย เช่น PaiNaiDii, XetaSale และ Buzzebees เป็นต้น

ช้อปปิ้งผ่าน Social Network

เดี๋ยวนี้การขายสินค้าโดยใช้ Social Network เป็นที่นิยมมาก เพราะนอกจากจะใช้ง่ายแล้ว ยังเข้าถึงผู้คนได้เป็นจำนวนมากอีกด้วย ผู้ขายแค่ใส่รายละเอียดของสินค้า ไม่ว่าจะเป็นรูปภาพหรือวิดีโอ สำหรับเพื่อนๆ ที่จะซื้อสินค้าผ่านช่องทางนี้ ก็สามารถคุยกับคนขายได้อย่างสะดวก ทั้งทางโพสต์หรือทางข้อความ (Inbox)



น้องพุดดิ้งชวนรู้

ข้อควรระวังในการช้อปปิ้งออนโมบาย (Shopping on Mobile)

การซื้อสินค้าออนไลน์ไม่ว่าจะทางคอมพิวเตอร์หรือทางสมาร์ตโฟน ข้อจำกัดก็คือ เราไม่ได้เห็นและสัมผัสสินค้าจริงๆ เราไม่เห็นร้านค้าของผู้ขาย เราไม่รู้ว่าผู้ขายมีตัวตนจริงหรือไม่ พุดดิ้งจึงมีวิธีเช็กข้อมูลมาให้เพื่อนอ่านก่อนช้อปค่ะ

1. ควรเปรียบเทียบราคาสินค้าในท้องตลาดก่อนซื้อ โดยเฉพาะสินค้าที่ราคาถูกเกินจริง ต้องระวังให้ดีเพราะอาจจะได้สินค้าปลอม หรือของไม่มีคุณภาพได้

2. ควรจะดูข้อมูลของผู้ขาย ซึ่งบางแอปพลิเคชันจะมีคะแนนบอก และลองหาข้อมูลผู้ขายโดยใช้เบอร์โทรศัพท์ เลขที่บัญชี ชื่อร้านค้าจาก Google ก่อนว่าน่าเชื่อถือหรือไม่

3. อ่านรีวิวสินค้าและบริการว่ามีใครซื้อแล้วมีปัญหาอะไรหรือเปล่า

4. การซื้อของจากแอปพลิเคชันขายของมือสอง ไม่ควรโอนเงินชำระค่าสินค้าไม่ว่าในกรณีใด เพราะโอนแล้วอาจจะไม่ได้ของก็ได้ ควรอ่านคำแนะนำของผู้ให้บริการทุกครั้ง

5. ตรวจดูการพูดคุยระหว่างผู้ขายกับลูกค้าใน Social Network ว่ามีการให้บริการที่ดีหรือไม่

6. อ่านข้อมูลสินค้าและเงื่อนไขให้ละเอียดก่อนตัดสินใจซื้อทุกครั้ง

7. ถ้าซื้อคูปอง ก็ให้ดูวันที่สามารถใช้ได้และวันหมดอายุ เงื่อนไขข้อยกเว้น

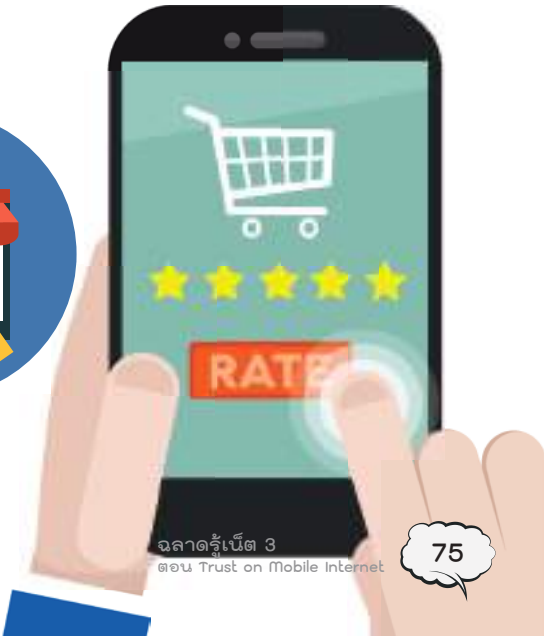
8. หากมีการรับประกัน ให้ศึกษาเงื่อนไขการรับประกันให้ละเอียด

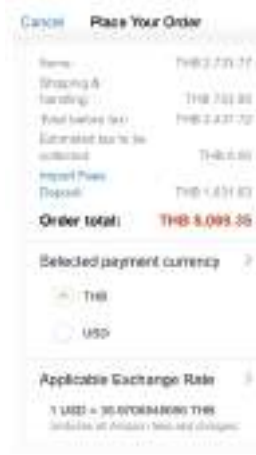
แค่สแกนก็ช้อปได้แล้ว
ด้วยแอปพลิเคชัน ของ Amazon
จะทำให้เพื่อนๆ สามารถช้อปสินค้า
จากต่างประเทศ โดยใช้อุปกรณ์เคลื่อนที่
สแกนบาร์โค้ดของสินค้า หรือรูปถ่าย หรือตัว
สินค้าจริงๆ เพื่อค้นหาสินค้า แทนการพิมพ์ได้เลย

3.6 Shopping (Global) ซื้อสินค้าต่างประเทศไม่ยาก

อีกหนึ่งความสุขของการใช้ชีวิตในยุคโซเชียลนี้ก็คือ การที่เราต้องการจะซื้อสินค้า แต่ไม่ต้องออกไปเดินช้อปสินค้าตามห้างสรรพสินค้าให้เมื่อยเท้า โดยหนึ่งในร้านค้าอีคอมเมิร์ซที่ได้รับความนิยมมากที่สุดในโลกคงหนีไม่พ้น Amazon

Amazon เว็บไซต์อีคอมเมิร์ซที่เริ่มจากการขายหนังสือ แต่ปัจจุบันได้ขายสินค้าทุกอย่าง มีสินค้าให้เลือกมากมายทุกหมวดหมู่สินค้า และมีโมบายแอปพลิเคชันให้ทั้งในสมาร์ตโฟนและแท็บเล็ต ทำให้เราสามารถใช้กล้องจากอุปกรณ์โมบายค้นหาสินค้าด้วยบาร์โค้ด รูปหรือสินค้าจริงได้ รองรับการค้นหาด้วยเสียง เวลาพูดน้อยไปที่ห้องสมุด แล้วอยากสั่งซื้อหนังสือที่อยู่ในห้องสมุด พูดน้อยเพียงแค่สแกนบาร์โค้ด หรือหน้าปกหนังสือ เพื่อค้นหาหนังสือแล้วก็สั่งซื้อได้ทันที หรือถ้ายังไม่ซื้อก็บันทึกเก็บไว้ในสิ่งที่ต้องการซื้อ (Wish List) ได้





▶▶ Feedback Rating ▶▶ การชำระเงิน

นอกจากเราจะไปซื้อสินค้าบน Amazon ได้แล้ว Amazon ยังอนุญาตให้เรานำสินค้ามาประกาศขายได้อีกด้วย ทำให้มีผู้ประกอบการรายย่อยมากมายนำสินค้ามาขายบน Amazon ซึ่งมีสินค้าทั้งของใหม่แกะกล่อง ของใช้แล้วสภาพดี หรือ Refurbished ราคาก็แตกต่างกัน บางครั้งสินค้ามีราคาที่ถูกมากๆ จนน่าสงสัย ดังนั้น การซื้อสินค้าบน Amazon จำเป็นต้องตรวจสอบข้อมูลผู้ขายโดยสังเกตจาก Feedback Rating ที่เปรียบเสมือนความพึงพอใจจากลูกค้า ซึ่งสามารถดู Feedback ย้อนได้

เมื่อได้สินค้าที่ต้องการแล้ว เราอาจคลิก Buy This Item เพื่อไปจ่ายเงินเลย หรือจะคลิก Add to Cart เพื่อช้อปสินค้าตัวอื่นต่อ

การ Checkout เพื่อชำระเงิน ให้กรอกที่อยู่และข้อมูลบัตรเครดิต เลือกวิธีการจัดส่งสินค้า เลือกสกุลเงินในการชำระเงิน พูดน้อยแนะนำให้เลือกเป็นเงินดอลลาร์ เพราะหากเลือกสกุลเงินบาทแล้ว อัตราแลกเปลี่ยนที่ Amazon ตั้งไว้จะแพงกว่าอัตราแลกเปลี่ยนปัจจุบันเพราะมีค่าธรรมเนียมของ Amazon บวกเข้าไปด้วย ส่วนการตัดบัตรเครดิตเป็นสกุลเงินดอลลาร์จะคิดอัตราแลกเปลี่ยนตามวันที่ตัดเงินจากบัตรเครดิต ซึ่งจะถูกกว่าคิดจาก Amazon

ในขั้นตอนนี้เราจะเห็นค่าใช้จ่ายทั้งหมด มูลค่าสินค้า ค่าขนส่ง ภาษี เมื่อรวมแล้วหากเรารู้สึกว่ามันแพง เราสามารถยกเลิกการสั่งซื้อได้ หรือหากเผลอกดสั่งซื้อไปแล้ว ก็สามารถยกเลิกได้ทันทีหรือภายหลัง แต่เราต้องแจ้งยกเลิกก่อนที่สินค้าจะจัดส่งนะครับ

เมื่อสั่งซื้อสินค้าเสร็จแล้วเราสามารถติดตามสถานะการจัดส่งได้จากแอปพลิเคชัน ซึ่งจะแจ้งเตือนทุกสถานะการส่งสินค้า เช่น สินค้าได้รับการบรรจุแล้ว กำลังจัดส่ง ส่งถึงผู้รับแล้ว เรียกว่าติดตามได้ทุกขั้นตอนเลย

นอกจาก Amazon ที่ทำแอปพลิเคชันแล้ว eBay เว็บไซต์ประมูลสินค้าชื่อดังของอเมริกา ก็ได้ทำแอปพลิเคชันไว้ให้เราใช้ด้วยเหมือนกัน การใช้งานก็ไม่ได้แตกต่างกันมาก มีระบบสแกนบาร์โค้ดเพื่อค้นหาสินค้า มีการแยกสินค้าไว้เป็นหมวดหมู่ ระบบการค้นหาใช้งานง่าย สินค้าใน eBay จะมีทั้งสินค้าแปลกๆ สินค้าหายาก ของเก่า ของสะสม มีระบบการขายหลายแบบ ทั้งแบบประมูลและแบบชำระเงินได้ทันที การชำระเงินก็ใช้ระบบ PayPal ซึ่งมั่นคงปลอดภัยและใช้งานง่าย มีระบบตรวจสอบและให้คะแนนผู้ขาย ทำให้เรามั่นใจในการซื้อสินค้า

eBay

AliExpress

ถ้าเพื่อนๆ อยากได้สินค้าราคาถูก ค่าส่งฟรี แถมมีเมนูภาษาไทยด้วย พุดน้อยแนะนำให้ลองใช้แอปพลิเคชัน AliExpress ซึ่งเป็นเจ้าของเดียวกับ Alibaba เว็บไซต์ค้าส่งชื่อดังจากจีน โดยที่เราสามารถซื้อของได้ทีละชิ้นไม่ต้องซื้อเยอะเหมือนกับสั่งที่ Alibaba และยังส่งฟรีอีกด้วย โดยอาจจะได้สินค้าช้าหน่อย แต่ถ้าเพื่อนๆ อยากให้ส่งไวขึ้น เราสามารถเลือกวิธีส่งแบบอื่นได้ ซึ่งจะมีการคิดค่าขนส่งเพิ่มขึ้นตามบริการที่เลือก

การชำระเงินก็มีทั้งแบบเครดิตการ์ด และระบบชำระเงินของ Alibaba ที่เรียกว่า AliPay มีระบบคุ้มครองผู้ซื้อโดยจะคืนเงินเต็มจำนวนหากเราไม่ได้รับสินค้า และคืนเงินบางส่วนหรือเต็มจำนวนหากสินค้าไม่เป็นไปตามที่ระบุไว้

หากเราไม่พอใจผู้ขาย สามารถให้ Feedback Rating กับผู้ขายคนนั้นได้

นอกจากนี้ ยังมีแอปพลิเคชันอีกมากมายที่สามารถใช้ช้อปสินค้าจากต่างประเทศบนโทรศัพท์มือถือที่ไม่ได้กล่าวถึง ไม่ว่าจะเป็นของ Alibaba, Taobao ซึ่งไม่ว่าจะซื้อของจากแอปพลิเคชันอะไร ก่อนจ่ายเงินเราจะต้องพิจารณาหลายอย่าง เช่น เรื่องคุณภาพสินค้า คะแนนของผู้ขาย ระบบการจ่ายเงิน วิธีการจัดส่ง และการรับประกันสินค้า ซึ่งจะทำให้เราลดความเสี่ยงที่จะถูกโกงหรือได้สินค้าไม่ตรงกับที่ต้องการ

น้องพุดดิ้งชวนรู้

ข้อควรระวังในการช้อปปิ้งต่างประเทศ

ในยุคสมัยนี้นักช้อปแทบทุกคนจะมีสมาร์ตโฟนติดตัว นั่นเท่ากับว่าอำนาจการซื้อสินค้าจะอยู่ในมือสองข้างไม่ไปไหน ในหัวข้อ 3.5 เราได้พูดถึงการช้อปปิ้งออนโมบายกันไปแล้ว ครั้งนี้สำหรับนักช้อปที่จะโกอินเตอร์ไปสั่งซื้อสินค้าจากต่างประเทศจะต้องมีข้อควรระวังอย่างไรกันบ้าง

1. ถ้าไม่กลัวว่าจะถูกเชิดเงินไปแบบฟรี ควรเช็กคอมเมนต์หรือแหล่งที่มาของร้านค้าในต่างประเทศเสียก่อน ซึ่งปัจจุบันนี้เทคโนโลยีก้าวไกล จะลองเช็กข้อมูลจากเว็บไซต์พันทิปว่าเพื่อนๆ ที่เป็นเคสตัวอย่างเคยช้อปสินค้าจากร้านค้านี้หรือเปล่า

2. แม้จะเป็นร้านค้าที่เชื่อถือได้ ก็อย่าปักใจเชื่อเสียทีเดียว เพราะอาจจะเคยมีประวัติในการส่งของที่ผิดพลาด เช่น สินค้าชำรุด บุบสลาย ซึ่งก่อนสั่งซื้อต้องคุยกับทางร้านให้เรียบร้อย เพราะอาจไม่รับประกันเปลี่ยนคืนได้

3. เลือกช้อปกับร้านค้าที่จดทะเบียนพาณิชย์อิเล็กทรอนิกส์ ซึ่งในแต่ละประเทศจะมีหน่วยงานคุ้มครองอยู่

4. อัปเดตโปรแกรมแอนตี้ไวรัสอยู่ตลอด เพราะขนาดการทำธุรกรรมผ่านระบบออนไลน์ภายในประเทศ เรายังต้องระมัดระวังถูกโจรกรรมข้อมูลส่วนตัว แล้วนี่กำลังไปช้อปซื้อสินค้าจากต่างประเทศเชียวจะไม่ระมัดระวังได้อย่างไร

สังคมไร้เงินสด

หลังจากที่เพื่อนๆ
รู้วิธีการเลือกซื้อสินค้าผ่าน
โมบายอินเทอร์เน็ตไปแล้ว
ถึงเวลาต้องจ่ายเงินแล้วล่ะ พุดน้อยมีวิธี
การจ่ายเงินด้วยสมาร์ตโฟนมาเล่าให้ฟังนะ
ครับ

การชำระเงินค่าสินค้าหลังจากทำรายการสั่งซื้อแล้วมีมากมายหลายวิธี ไม่ว่าจะเป็นการเก็บเงินปลายทาง การโอนเงินผ่านธนาคาร การชำระด้วยบัตรเครดิต การชำระผ่านจุดชำระเงิน นอกจากนี้ ยังมีบริการทางการเงินบนอินเทอร์เน็ต เช่น บริการธนาคารทางอินเทอร์เน็ต บริการส่งเงินผ่านอีเมล บริการกระเป๋าสตางค์อิเล็กทรอนิกส์ และอีกมากมาย

ด้วยสมาร์ตโฟนเครื่องเดียว เพื่อนๆ สามารถชำระค่าสินค้าแทนเงินสด โดยใช้ทำรายการผ่านธนาคารอินเทอร์เน็ต ชำระบิลต่างๆ เช่น ค่าน้ำ ค่าไฟ ค่าโทรศัพท์ ใช้เป็นบัตรผ่านรถไฟฟ้า เรียกว่าแทบไม่ต้องพกเงินสดเลยทีเดียว

มีแค่มือถือ
ก็เปิดบัญชีธนาคารได้แล้ว ไม่ต้องมี
เงินฝากขั้นต่ำ ไม่ต้องมีสมุดบัญชี
แถมมีดอกเบี้ยให้ด้วย

4.1 เปลี่ยนมือถือให้เป็นธนาคารดิจิทัล

เพื่อนๆ คงเคยได้ยินคำว่ากระเป๋าเงินออนไลน์ หรือกระเป๋าเงินอิเล็กทรอนิกส์ (e-Wallet) กันบ้างใช่ไหมครับ พูดน้อยจะเล่าให้ฟังว่ามันคืออะไร เจ้า e-Wallet ก็เหมือนกับกระเป๋าสตางค์ของเรานั่นแหละ เพียงแต่เมื่อเรามีเงินในกระเป๋านี้แล้ว สามารถนำไปใช้จ่ายค่าสินค้าและบริการต่างๆ ทั้งในโลกออนไลน์และออฟไลน์ได้ง่าย เปรียบเสมือนมีเงินในบัญชีธนาคาร แต่สามารถนำเงินไปใช้จ่ายได้อย่างรวดเร็วเสมือนมีเงินสดอยู่ในมือ

ในประเทศไทยมีผู้ให้บริการด้าน e-Wallet อยู่ 3 ค่ายใหญ่คือ AIS, DTAC และ Truemove โดยใช้บริการชื่อว่า AIS mPAY, Jaew Wallet, Wallet by Truemoney ตามลำดับ ซึ่งแต่ละบริการก็จะมีแอปพลิเคชันให้ดาวน์โหลดเพื่อใช้บนสมาร์ตโฟน

Jaew Wallet

Wallet by Truemoney

โดยทั่วไปแอปพลิเคชัน *e-Wallet* จะมีความสามารถดังนี้

- โอน/รับเงิน
- ชำระบิล

โอน/รับเงิน

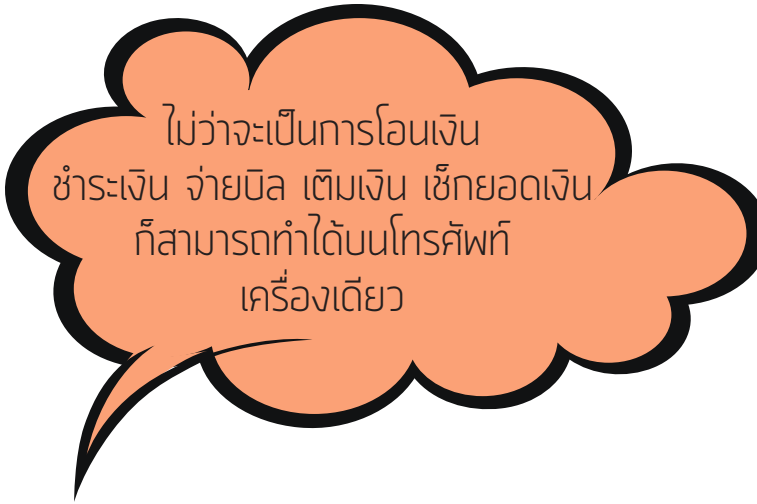
เราสามารถโอนเงินระหว่างบัญชี e-Wallet ได้เพียงทราบเบอร์มือถือของผู้รับเงิน ซึ่งสามารถโอนเงินข้ามค่ายได้ ไม่ว่าผู้รับเงินจะใช้ e-Wallet ค่ายเดียวกับเราหรือไม่ หรือหากผู้รับเงินยังไม่ได้ใช้บริการ e-Wallet เราก็สามารถโอนเงินไปยังบัญชีธนาคารของผู้รับเงินได้เช่นกัน

ชำระบิล

เราสามารถใช้ e-Wallet ชำระบิล ไม่ว่าจะเป็นบิลค่าน้ำ ค่าไฟ ค่าโทรศัพท์ ค่าสาธารณูปโภคอื่นๆ ค่าบัตรเครดิต สินเชื่อ ประกัน อินเทอร์เน็ต เคเบิลทีวี ฯลฯ ซึ่งอาจจะมีค่าธรรมเนียมในการชำระเงินแตกต่างกันไปตามค่าย แต่สิ่งที่พูดน้อยชอบมากที่สุดก็คือ ความสามารถในการสแกนบาร์โค้ดเพื่อชำระเงินได้ ทำให้การทำรายการสะดวกรวดเร็ว ไม่ต้องเสียเวลาพิมพ์รายละเอียดเวลาจ่ายบิล

แค่นี้ก็สะดวกมากมายแล้วใช่ไหมครับ แต่การเติมเงินเข้า e-Wallet หรือโอนเงินจาก e-Wallet กลับเข้าบัญชีธนาคารนั้นอาจจะต้องเสียค่าธรรมเนียม แถมยังไม่มีดอกเบี้ยเหมือนกับฝากธนาคารทั่วไป ดังนั้นพูดน้อยจะเติมเงินเท่าที่จำเป็น ไม่เหลือเงินค้างไว้เยอะครับ

แต่ถ้าเพื่อนๆ อยากใช้งาน e-Wallet ที่ได้ดอกเบี้ยด้วย ปัจจุบันนี้เริ่มมีการให้บริการ e-Wallet ของบางค่ายที่ผูกกับบัญชีธนาคารที่ร่วมโครงการ โดยจะสามารถใช้เงินในบัญชีธนาคารเป็นเงินใน e-Wallet ได้เลย และยังได้ดอกเบี้ยหากมีเงินเหลือในบัญชีอีกด้วย



4.2 แอปพลิเคชัน Mobile Banking รับกระแสดิจิทัล

ทุกธนาคารในประเทศไทยจะมีบริการธนาคารทางอินเทอร์เน็ต ที่เรียกว่า “อินเทอร์เน็ตแบงก์กิ้ง” ทำให้พุดน้อยสามารถเช็กยอดเงินฝากได้ โดยไม่ต้องไปอัปเดตสมุดบัญชีที่ธนาคาร คุณพ่อพุดน้อยก็ชอบทำรายการทางธนาคาร เช่น โอนเงินมาให้พุดน้อย ชำระค่าบัตรเครดิต เติมเงินค่าทางด่วน เติมเงินค่าโทรศัพท์ให้พุดน้อยได้ด้วยตัวเอง

การสมัครใช้บริการอินเทอร์เน็ตแบงก์กิ้งก็ง่าย สามารถสมัครออนไลน์ได้เลย หรือทางตู้เอทีเอ็ม ถ้ามีบัตรเอทีเอ็มของธนาคาร หรือจะไปที่สาขาก็ได้ ในการสมัครจะต้องเตรียมเลขบัตรประจำตัวประชาชน เลขที่บัญชีธนาคาร หรือเลขบัตรเอทีเอ็ม หรือบัตรเครดิตอย่างใดอย่างหนึ่ง อีเมลสำหรับสมัคร และเบอร์โทรศัพท์มือถือด้วยนะครับ ซึ่งขั้นตอนก็ไม่ยุ่งยาก แต่จะแตกต่างกันไปตามนโยบายของแต่ละธนาคารครับ

การใช้บริการ Mobile Banking ก็สามารถทำได้ 2 วิธี วิธีที่หนึ่งคือ การใช้บริการผ่านเว็บเบราว์เซอร์ของโทรศัพท์ที่เป็นโมบายไซต์ (Mobile Site : เว็บไซต์ที่มีการปรับขนาดให้เหมาะกับการใช้งานผ่านอุปกรณ์มือถือ) วิธีที่สอง คือ การใช้บริการผ่านแอปพลิเคชันที่ธนาคารมีไว้ให้ ซึ่งพุดน้อยจะขอแนะนำวิธีที่สอง เพราะใช้งานง่ายกว่า แถมยังมั่นคงปลอดภัยด้วย

การโหลดแอปพลิเคชัน เพื่อติดตั้งลงเครื่องก็ไม่ยากเลย เหมือนกับการติดตั้งแอปพลิเคชันทั่วไป เพียงแต่เพื่อนๆ ต้องระวังอย่าติดตั้งแอปพลิเคชันปลอมที่ไม่ได้ทำโดยธนาคารเอง แต่ทำโดยผู้ไม่หวังดี หากเพื่อนๆ นำแอปพลิเคชันเหล่านั้นมาใช้ เงินในบัญชีของเราอาจถูกขโมยได้

วิธีสังเกตแอปพลิเคชันว่าเป็นแอปพลิเคชันปลอมหรือไม่ ให้เพื่อนๆ ดูชื่อผู้พัฒนาข้างใต้ชื่อแอปพลิเคชัน ว่าเป็นชื่อธนาคารนั้นๆ หรือไม่ ถ้าไม่ใช่ก็อย่าติดตั้งนะครับ หรือจะเข้าไปที่หน้าเว็บไซต์ของธนาคารเพื่อกดลิงก์ที่ธนาคารให้ไว้เพื่อติดตั้งก็ได้

เพียงเท่านี้ เพื่อนๆ ก็จะสามารถทำรายการทางธนาคารได้อย่างสะดวก รวดเร็ว มั่นคงปลอดภัยบนโทรศัพท์มือถือ โดยไม่ต้องไปที่ธนาคารอีกต่อไป

สำหรับแอปพลิเคชัน Mobile Banking จะมีความสามารถเพิ่มเติมจากการใช้งานธนาคารออนไลน์ผ่านเว็บไซต์ ซึ่งความสามารถของแอปพลิเคชัน Mobile Banking จะแตกต่างกันไปตามแต่ละธนาคาร เช่น

- สามารถแสดงสาขาธนาคารที่ใกล้ๆ กับตำแหน่งที่เราอยู่ แสดงตำแหน่งของตู้เอทีเอ็มที่อยู่ใกล้เราได้ และมีระบบนำทางไปยังจุดหมาย
- สามารถสแกนบิลเพื่อชำระเงินค่าสินค้าได้ โดยใช้กล้องจากโทรศัพท์
- มีปุ่มหรือเมนูสำหรับโทรเข้า Call Center
- มีระบบปฏิทินแสดงการทำธุรกรรมทางอิเล็กทรอนิกส์

การใช้ Mobile Banking
มีความมั่นคงปลอดภัยหรือเปล่า
พุดน้อยเคยอ่านข่าวเกี่ยวกับปล้นเงิน
ออนไลน์อยู่หลายครั้ง
แล้วเราจะมั่นใจได้อย่างไรว่าเงินของเรา
จะไม่หาย

4.3 มั่นใจใช้ Mobile Banking

จริงๆ แล้วระบบรักษาความมั่นคงปลอดภัยของธนาคารจะมีความเข้มงวดมาก ซึ่งจะปกป้องบัญชีเราตั้งแต่การเข้าใช้งาน ถ้าเราใช้งานผ่านโปรแกรมเว็บเบราว์เซอร์ธนาคารจะใช้ระบบ Secure Socket Layer (SSL) ซึ่งจะทำการเข้ารหัสข้อมูล Username กับ Password ทำให้ผู้ไม่หวังดีแอบขโมยข้อมูลเราไปใช้ไม่ได้ สังเกตได้จากไอคอนกุญแจสีเขียวเวลาเรา Login เข้าใช้บริการ และดูได้จาก URL จะต้องเป็น https:// ซึ่งจะปกป้อง Username กับ Password ซึ่งเปรียบเสมือนกับลูกกุญแจไม่ให้ใครมาแอบก๊อปปี้ไปใช้งานได้เลย

การเข้ารหัสข้อมูลด้วย SSL

ไอคอนรูปกุญแจสีเขียว

และหากเป็นการลงแอปพลิเคชัน บางธนาคารจะมีการตรวจสอบตัวเลขเครื่องมือถือ เบอร์มือถือ และรหัสผ่าน ซึ่งต้องตรงกันกับที่สมัครเท่านั้น จึงสามารถทำธุรกรรมได้ โดยเมื่อ Login เข้าใช้บริการแล้ว อาจมี SMS และอีเมลส่งมาให้เราทุกครั้ง ซึ่งหากเราไม่ได้เป็นคน Login เราก็จะรู้ได้ทันทีว่ามีคนแอบเข้าไปทำธุรกรรมในบัญชีของเราอยู่ ซึ่งเราจะได้แจ้งธนาคารทันที

เมื่อ Login เข้ามาแล้ว ในขณะทำธุรกรรมทางธนาคารก็จะมีการเข้ารหัสข้อมูลด้วยมาตรฐาน AES 256 Bits ซึ่งเป็นมาตรฐานความมั่นคงปลอดภัยระดับโลก ทำให้ข้อมูลของเราไม่มีทางถูกโจรกรรม และหากมีการเพิ่มบัญชีบุคคลอื่น หรือมีการโอนทุกๆ Transaction จะมีการส่งรหัส One Time Password (OTP) มายังเบอร์โทรศัพท์ที่เราได้แจ้งไว้ตอนสมัครใช้บริการ ซึ่งหากเราจะเปลี่ยนเบอร์โทรศัพท์ ทางธนาคารก็จะมีขั้นตอนที่ยืนยันตัวตนว่าเป็นเราเปลี่ยนจริงๆ ซึ่งบางธนาคารต้องไปทำเรื่องเปลี่ยนที่สาขาเลย

จากข้อมูลพุดน้อยเล่าให้ฟังจะเข้าใจว่าทางธนาคารได้มีระบบรักษาความมั่นคงปลอดภัยให้กับผู้ใช้งานตั้งแต่การเข้าสู่บริการแล้ว โดยทางธนาคารได้มีระบบการป้องกันการก๊อปปี้ลูกกุญแจเพื่อป้องกันไม่ให้โจรเข้าไปทำธุรกรรมในบัญชีของเราได้ แต่หากโจรสามารถเข้าไปได้แล้ว เราก็จะทราบได้อย่างรวดเร็วจากการเตือนผ่าน SMS ว่ามีการ Login เข้ามาในบัญชีของเรา และหากจะโอนเงินออกจากบัญชีของเราก็ทำได้ยาก เพราะจะต้องใช้รหัส OTP ในการทำรายการทุกครั้ง เห็นไหมล่ะครับว่าระบบรักษาความมั่นคงปลอดภัยของธนาคารเขาเจ๋งจริงๆ

แต่พุดน้อยก็ยังสงสัยว่า เมื่อธนาคารมีระบบรักษาความมั่นคงปลอดภัยขนาดนี้แล้ว ทำไมยังมีข่าวว่ามีการขโมยเงินจากบัญชีอินเทอร์เน็ตแบงก์กิ้งอยู่ คุณพ่อบอกว่าคนร้ายสามารถขโมย Username กับ Password โดยการสร้างเว็บไซต์ธนาคารปลอม ซึ่งการกระทำแบบนี้เรียกว่า Phishing คนร้ายอาจปลอมอีเมลธนาคาร หรือ SMS ส่งข้อความมาให้เหยื่อโดยมี Link ธนาคารปลอมที่เมื่อคลิกไปแล้ว หน้าเว็บไซต์จะเหมือนกับหน้า Login ของธนาคารเลย ถ้าเรากรอก Username กับ Password ไปก็เท่ากับว่าเราส่งกุญแจให้เขาไปแล้ว เมื่อเขาเข้าไปได้ เขาก็จะไปเพิ่มบัญชีธนาคารและโอนเงินออกจากบัญชีของเรา

เพื่อนๆ สงสัยไหมครับว่า เขาจะเพิ่มบัญชีได้อย่างไร ในเมื่อการเพิ่มบัญชีต้องทราบรหัส OTP ซึ่งจะส่งมายังโทรศัพท์ของเจ้าของบัญชีเท่านั้น คุณพ่อก็เฉลยให้พุดน้อยฟังว่า นอกจากเขาจะได้กุญแจไปแล้ว เขายังมีวิธีฝังโปรแกรมไว้ที่เครื่องของเรา หรือที่เรียกว่า Malware โดยใช้วิธีส่ง SMS หรืออีเมลที่เหมือนกับว่าส่งมาจากธนาคาร ทำให้เหยื่อหลงเชื่อและติดตั้งโปรแกรม Malware ที่มือถือ โดยที่ไม่รู้ว่านั่นคือโปรแกรมดัก SMS จากธนาคารที่ส่งมายังโทรศัพท์ของเราให้ส่งไปยังโทรศัพท์ของคนร้ายแทน เมื่อเขาเข้าไปในบัญชีเราได้ และสามารถเพิ่มบัญชีของตนเองและโอนเงินได้ เงินในบัญชีของเราก็จะหายไปโดยไม่รู้ตัว

เมื่อเหยื่อติดตั้งมัลแวร์ที่โทรศัพท์ก็จะถูกขโมย Username และ Password รวมถึงรหัส OTP

ปัจจุบันบางธนาคารถึงกับป้องกันการเข้าใช้บริการ โดยผู้เข้าใช้งานต้องใช้เครื่องเดิม ซิมเบอร์เดิม และรหัสผ่าน ถึงจะเข้าใช้บริการได้ เรียกว่าต่อให้ถูกขโมยข้อมูลก็ไม่สามารถเข้าไปทำรายการได้ และก็มีการพัฒนาระบบรักษาความมั่นคงปลอดภัยที่มากขึ้นตลอดเวลา เช่น การทำแอปพลิเคชันของธนาคารที่มีระบบรักษาความมั่นคงปลอดภัยมากกว่า Mobile Banking ที่ใช้งานผ่านเว็บเบราว์เซอร์

น้องพุดดิ้งชวนรู้

พุดดิ้งมีวิธีสังเกตแอปพลิเคชันปลอมมาบอกเพื่อนๆ ดังนี้ค่ะ

• ตรวจสอบจากชื่อ Developer โดยแอปพลิเคชันที่มาจากธนาคารส่วนใหญ่จะใช้ชื่อธนาคารเป็นผู้พัฒนาแอปพลิเคชัน โดยมีรายการชื่อ Developer ดังต่อไปนี้

- ธนาคารกรุงไทย : Krung Thai Bank PCL.
- ธนาคารกรุงเทพ : Bangkok Bank PCL.
- ธนาคารไทยพาณิชย์ : Siam Commercial Bank PCL.
- ธนาคารกสิกรไทย : KASIKORNBANK PCL.
- ธนาคารกรุงศรีอยุธยา : Bank of Ayudhya Public Company Limited
- ธนาคารธนชาต : Thanachart Bank Plc.

• ให้ตรวจสอบจากจำนวนดาวน์โหลด และรีวิวของผู้ใช้งาน โดยสังเกตแอปพลิเคชันที่มียอดดาวน์โหลดต่ำหรือรีวิวของผู้ใช้งานที่แจ้งถึงความผิดปกติ

• ให้ตรวจสอบจากธนาคาร โดยอาจเข้าไปดูรายละเอียดจากเว็บไซต์ของธนาคาร หรือสอบถามจากธนาคารโดยตรง

เพียงเท่านี้เพื่อนๆ ก็จะใช้งาน Mobile Banking ได้อย่างมั่นใจแล้วนะคะ ว่าแล้วพุดดิ้งขอไปโหลดแอปพลิเคชันมาใช้สักหน่อยดีกว่า


PHISHING
ปลอมอีเมล
เว็บไซต์ปลอม
คำแนะนำ
URL
HTTPS
HELP & SUPPORT
ThaiCERT
ETDA


SCB Thailand
ใช้ Mobile Banking
App Store
Google play

พุดน้อยได้แนะนำเพื่อนๆ
เกี่ยวกับแอปพลิเคชันที่ทำให้มือถือเปลี่ยนเป็น
บัตรเงินสดอิเล็กทรอนิกส์แล้ว แต่ส่วนใหญ่จะต้องมี
การเติมเงินก่อนใช้เสมอ แต่แอปพลิเคชัน
ที่พุดน้อยจะแนะนำในหัวข้อนี้ ไม่จำเป็นต้องเติมเงิน
เพราะเป็นการจ่ายเงินด้วยวงเงินบัตรเครดิต
น่าสนใจไหมล่ะครับ

4.4 ชำระเงินแสนง่ายด้วย e-Payment

ในชีวิตประจำวันของมนุษย์ยุคปัจจุบันนั้น พุดน้อยพบว่าเรามักมีเรื่องเกี่ยวข้องกับการทำธุรกรรมและการชำระเงินอยู่ตลอด ยิ่งในสมัยนี้การชำระเงินเพื่อซื้อสินค้าและบริการต่างก็มีตัวช่วย โดยมีการนำกระบวนการชำระเงินระบบอิเล็กทรอนิกส์หรือเรียกกันว่า ระบบการชำระเงินแบบอิเล็กทรอนิกส์ (e-Payment) มาใช้ในการทำธุรกรรมต่างๆ มากขึ้น

โดย e-Payment จัดเป็นระบบการชำระเงินแบบอิเล็กทรอนิกส์ที่รัฐบาลกำลังพยายามผลักดันเพื่อให้มีระบบรองรับการชำระเงินทางอิเล็กทรอนิกส์ที่ได้มาตรฐาน เพื่อสอดคล้องกับการใช้งานเทคโนโลยีโดยเฉพาะอินเทอร์เน็ตและโทรศัพท์มือถือที่ขยายวงกว้างขึ้นตั้งแต่ในช่วงปี 2558 ที่ผ่านมา ซึ่งรายละเอียดด้านความเป็นมานั้น หากเพื่อนๆ คนใดต้องการทราบสามารถเข้าไปศึกษาได้ที่ www.epayment.go.th

สำหรับเพื่อนๆ ที่กำลังจะเป็นนักธุรกรรมรุ่นใหม่ แต่ยังไม่ทราบถึงวิธีการชำระเงินผ่าน e-Payment พุดน้อยจะขออธิบายขั้นตอนการชำระให้เข้าใจง่ายๆ ดังนี้

ขั้นตอนการชำระเงิน

1. เมื่อมีการตกลงซื้อสินค้าและบริการ เพื่อนๆ จะต้องกรอกข้อมูลบัตรเครดิตให้ละเอียด หลังจากนั้นก็ส่งข้อมูลไปยัง Acquiring Bank (ธนาคารที่ฝ่ายร้านค้าใช้บริการอยู่)

หมายเหตุ แต่ทั้งนี้ก็ไม่ต้องกลัวว่าร้านค้าจะรู้ข้อมูลดังกล่าว เนื่องจาก e-Payment จะมีระบบรักษาความมั่นคงปลอดภัยข้อมูลส่วนนี้ ซึ่งทางร้านไม่สามารถเห็นได้

2. หลังจากนั้น Acquiring Bank ทำการตรวจสอบมายังธนาคารผู้ออกบัตร ว่าบัตรเป็นของจริงและสามารถใช้ซื้อสินค้าได้อยู่หรือไม่

3. เมื่อตรวจสอบเรียบร้อยแล้ว Acquiring Bank จะทำการเรียกเก็บเงินจากธนาคารผู้ออกบัตร

4. ธนาคารผู้ออกบัตรโอนเงินไปยัง Acquiring Bank เข้าสู่บัญชีร้านค้า

5. ส่งข้อมูลการชำระกลับไปยังร้านค้า

6. ร้านค้าส่งข้อมูลการชำระกลับไปยังลูกค้า เพื่อยืนยันการสั่งซื้อ

ไม่ว่าจะเป็นบริการ e-Wallet เช่น mPAY, Jaew Wallet, Wallet by Truemoney หรือบริการ Beat Banking หรือ AIS mPAY Rabbit เราจำเป็นจะต้องมีเงินเติม หรือฝากเข้าไปยังบัญชีเหล่านี้ แต่แอปพลิเคชันที่พูดน้อยจะแนะนำ เป็นแอปพลิเคชันที่สามารถตัดเงินจากบัตรเครดิตได้ทันที เช่น แอปพลิเคชัน Mobile Credit Card และ LINE Pay

แอปพลิเคชันแรกที่พูดน้อยจะแนะนำก็คือ แอปพลิเคชัน Mobile Credit Card เป็นแอปพลิเคชันที่ทำให้โทรศัพท์เปลี่ยนเป็นบัตรเครดิตที่สามารถเพิ่มบัตรเครดิตได้ถึง 3 ใบ สามารถสแกนบิลเพื่อจ่ายบิลค่าน้ำ ค่าไฟ หรือจะเติมเงินโทรศัพท์ ซื้อการ์ดเกม ซื้อ Skype Credit, Gift Cards ของ Google Play/iTunes

การลงทะเบียนแอปพลิเคชันใช้เพียงโทรศัพท์มือถือกับบัตรเครดิตเท่านั้น เมื่อลงทะเบียนสำเร็จเราสามารถใช้วงเงินบัตรเครดิตในการช้อปปิ้งได้ทันที โดยไม่จำเป็นต้องเติมเงินก่อนใช้บริการเหมือนบัตรเงินสดอิเล็กทรอนิกส์ เราสามารถเติมเงินค่าโทรศัพท์ เกมออนไลน์ เติมเครดิต Digital Content เช่น iTunes, Google Play และ Skype Credit ได้ จ่ายบิลค่าน้ำ ค่าไฟ ได้ทันที

เริ่มต้นใช้งานได้ทันที

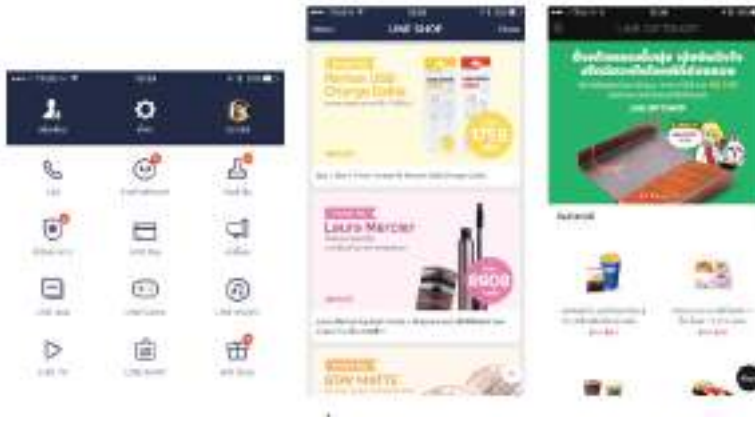
- Mobile Top Up
เติมเงินได้ไม่จำกัดค่ายทั้ง dtac happy, 1-2 call, truemove, truemove-H
- Digital Content Top Up
บริการเติมเงิน iTunes Gift Card, Google play หรือ Skype
- Utility Bill
ไม่ว่าจะค่าน้ำ ค่าไฟ ค่าโทรศัพท์ ก็สามารถจ่ายได้
- Game Card Top Up
รองรับการเติมเงินจากหลากหลายค่ายเกม
- Dtac Postpaid Bill
บริการเติมเงิน iTunes Gift Card หรือ Google play
- E-Commerce stuff
ช้อปปิ้งออนไลน์

ข้อดีของแอปพลิเคชันนี้ก็คือ การตัดเงินไม่ได้ตัดเงินสด เพราะเป็นการใช้วงเงินบัตรเครดิต แต่คนที่จะใช้แอปพลิเคชันนี้ได้ จำเป็นต้องมีบัตรเครดิตเท่านั้น และบิลที่สามารถจ่ายได้ด้วยแอปพลิเคชันนี้ก็ยังน้อยมาก เมื่อเทียบกับแอปพลิเคชัน Truemoney Wallet และ mPAY ของค่ายทรูและเอไอเอส คุณพ่อพุดน้อยจะลงแอปพลิเคชันนี้ไว้จ่ายค่าน้ำ ค่าไฟ เพราะไม่ต้องจ่ายเป็นเงินสด ส่วนบิลอื่นๆ ก็จะใช้แอปพลิเคชันของค่ายอื่นแทนครับ

แอปพลิเคชันสองที่พุดน้อยจะแนะนำก็คือ LINE ครับ แอปพลิเคชัน LINE มีบริการชำระเงินของตัวเองชื่อ “LINE Pay” โดยที่เพื่อนๆ สามารถเพิ่มบัตรเครดิตหรือบัตรเดบิตก่อน เมื่อเราใช้บัญชี LINE Pay ไปชำระเงิน เราเพียงแค่เลือกบัตรที่ต้องการให้ตัดเงินได้เลย โดยไม่ต้องใส่ข้อมูลบัตรทุกครั้งเวลาชำระเงิน ทำให้เราสามารถชำระเงินได้อย่างรวดเร็ว

LINE Pay

เราสามารถเลือกซื้อสินค้าบนร้านค้าที่อยู่ในแอปพลิเคชัน LINE เช่น LINE Shop, Gift Shop ซื้อสติกเกอร์ไลน์ ธีมไลน์ ผ่าน LINE Store (http://store.line.me) และยังมีร้านค้าออนไลน์จำนวนมากรับชำระด้วย LINE Pay



ร้านค้าที่อยู่ในแอปพลิเคชัน LINE

LINE Store

การชำระเงินด้วย LINE Pay

นอกจาก LINE Pay จะใช้ชำระเงิน โดยการตัดบัญชีบัตรเครดิต/เดบิตแล้ว แต่ถ้าเราไม่มีบัตรทั้งสองแบบ ก็ยังเติมเงินเข้า “กระเป๋าเงิน LINE Pay” เพื่อใช้ในการชำระเงินได้ แถมยังส่งเงินทางข้อความ Chat ให้กับเพื่อนได้

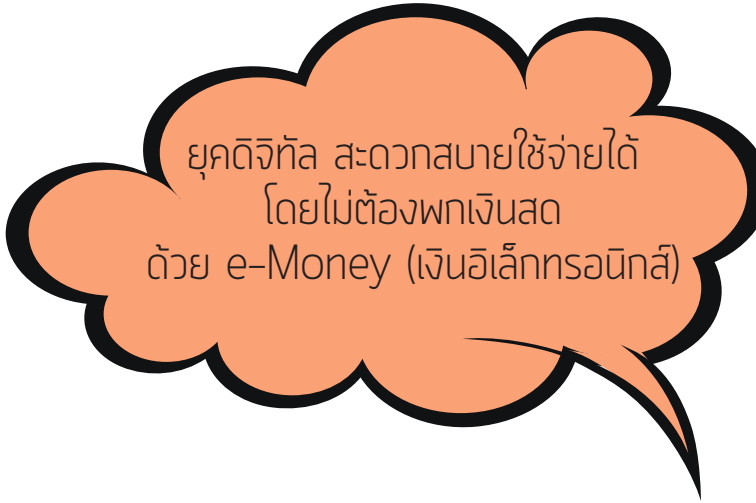
นอกจากการส่งเงินหรือโอนเงินแล้ว ผู้ใช้สามารถส่งคำขอเงินให้เพื่อนส่งเงินกลับมาได้ด้วย โดยไม่จำเป็นต้องใช้บัญชีธนาคารเลย โดยเงินที่ได้รับก็สามารถนำไปใช้จ่ายกับร้านค้าออนไลน์หรือออฟไลน์ที่รับการชำระเงินด้วย LINE Pay ได้อีกด้วย หรือหากจะถอนเงินก็สามารถโอนเงินไปยังบัญชีธนาคารได้เช่นกัน

การเลือกชำระเงินผ่าน e-Payment/Payment gateway แทนการโอนเงินผ่านบัญชีธนาคาร นอกจากสะดวกรวดเร็วแล้ว ยังเป็นอีกวิธีที่มั่นคงปลอดภัยในการช้อปปิ้งออนไลน์ เนื่องจากมีช่วงเวลาที่ผู้ให้บริการยังไม่โอนเงินไปยังผู้ขายสินค้าทันที ซึ่งหากมีปัญหาในการส่งสินค้ายังมีโอกาสที่เราจะแจ้งไปยังผู้ให้บริการ เพื่อระงับการชำระเงินไปยังผู้ขายได้ นับเป็นข้อดีที่ช่วยป้องกันการสูญเสียโดยใช่เหตุ นอกจากนี้ยังสามารถดำเนินการได้ตลอด 24 ชั่วโมง

น้องพุดดิ้งชวนรู้

เพื่อนๆ จะเห็นว่าสมัยนี้มีแอปพลิเคชันสำหรับการชำระเงินเยอะมากจนสับสน พุดดิ้งได้ทำตารางสรุปไว้ให้แล้วค่ะ

	AIS mPay	Jaew Wallet	Wallet by Truemoney	LINE Pay	Mobile Credit Card
กระเป๋าเงิน	√	√	√	√	—
Credit Card	—	—	—	√	√
Debit Card	—	—	—	√	—
Rabbit Card	√	—	—	—	—
Virtual Card	√	—	√	—	—
โอน/รับเงิน	√	√	—	—	—
โอนระหว่างค่าย	√	√	√	—	—
ส่งคำขอ	—	√	—	—	—
แชร์เงิน	—	√	—	—	—
ชำระบิล	√	√	√	—	√
Beat Banking	√	—	—	—	—



4.5 e-Money พร้อมใช้

พุดน้อยรู้สึกว่าตัวเองโชคดีจริงๆ กับการเป็นเด็กยุค Gen Z ที่มีเทคโนโลยีทันสมัยมาอำนวยความสะดวกในการใช้ชีวิตประจำวัน ยกตัวอย่าง การซื้อสินค้าและบริการต่างๆ ไม่ต้องพกเงินสดมากมายเหมือนแต่ก่อน เพราะปัจจุบันนี้ขอเพียงแค่มี e-Money ก็สามารถใช้จ่ายได้แล้ว ซึ่งในอนาคตคาดว่า จะมีผู้ให้บริการ e-Money มากขึ้นแน่นอน

e-Money (เงินอิเล็กทรอนิกส์) คือ มูลค่าเงินที่ถูกบันทึกในระบบอิเล็กทรอนิกส์ เช่น เครือข่ายโทรศัพท์มือถือ หรือเครือข่ายอินเทอร์เน็ต ซึ่งผู้ใช้บริการได้ชำระเงินล่วงหน้า (Prepaid) แก่ผู้ให้บริการ e-Money และสามารถใช้ชำระค่าสินค้าและบริการตามร้านค้าหรือหน่วยงานที่ร่วมรายการได้ทันที เช่น บัตรซื้ออาหาร บัตรเติมเงินมือถือ บัตรชมภาพยนตร์ บัตรรถโดยสาร รวมทั้งการซื้อสินค้าผ่านเว็บไซต์ ทำให้มีความสะดวกรวดเร็ว ไม่เสียเวลารอเงินทอน ไม่ต้องพกเงินสดให้ยุ่งยากอีกด้วย

ในปัจจุบันเราสามารถใช้บริการ e-Money ได้จาก 3 ช่องทาง ดังนี้

1. การซื้อหรือเติมเงินบัตร e-Money ผ่านร้านค้าที่ร่วมรายการ

2. การใช้ผ่านโทรศัพท์มือถือ โดยใช้วิธีการสมัครผ่านโทรศัพท์มือถือ โดยเมื่อซื้อสินค้าและบริการเรียบร้อยแล้ว ผู้ให้บริการจะส่ง SMS แทนใบเสร็จรับเงินและแสดงยอดเงินคงเหลือในบัญชีให้แก่ผู้ใช้บริการ

3. การใช้ผ่านเครือข่ายอินเทอร์เน็ต โดยใช้วิธีการสมัครผ่านเว็บไซต์ของผู้ให้บริการเพื่อขอเปิดบัญชี e-Money และทุกครั้งที่มีการซื้อสินค้าและบริการ ผู้ใช้บริการจะต้องทำการกรอกเลขที่บัญชีและรหัสผ่านส่วนตัว เพื่อให้ร้านค้าตรวจสอบรายการชำระเงิน โดยเมื่อตัดเงินแล้ว ผู้ให้บริการจะส่ง SMS แทนใบเสร็จรับเงินและแสดงยอดเงินคงเหลือในบัญชีให้แก่ผู้ใช้บริการ

หากเงินหมดจะทำอย่างไร

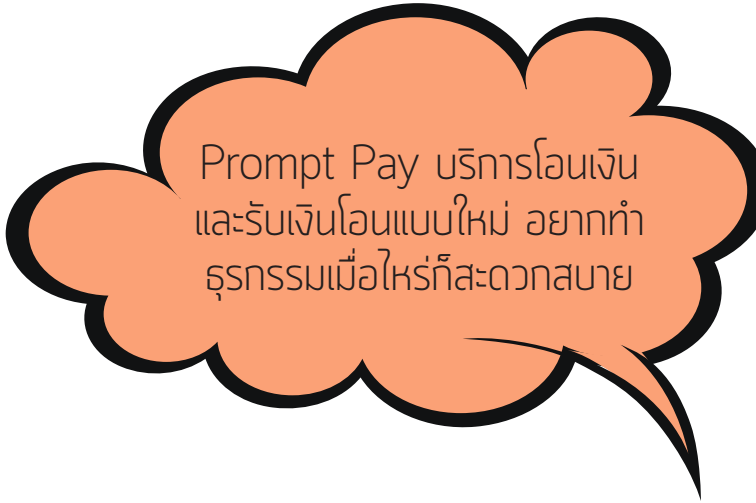
1. ผู้ใช้บริการสามารถติดต่อขอเติมเงินกับร้านค้า ตู้ ATM เว็บไซต์ของผู้ให้บริการ หรือบัญชีบัตรเครดิตของผู้ใช้บริการที่มีสัญลักษณ์เติมเงิน

2. ผู้ให้บริการเงินอิเล็กทรอนิกส์ จะทำการบันทึกมูลค่าของเงินที่เติมให้แก่ผู้ใช้บริการเติมเงิน โดยผู้ใช้บริการสามารถตรวจสอบการทำธุรกรรมการเติมเงินผ่านใบเสร็จรับเงิน ข้อความใน SMS บนโทรศัพท์มือถือ หรือทางอีเมลของผู้ใช้บริการ

น้องพุดดิ้งชวนรู้

ข้อควรระวัง การใช้ e-Money

เพื่อนๆ ต้องไม่ลืมว่า e-Money แท้จริงแล้ว คือ เงินสดที่อยู่ในรูปแบบของอุปกรณ์อิเล็กทรอนิกส์ หากเกิดกรณีทำบัตร e-Money หาย ก็ไม่ต่างจากการทำกระเป๋าเงินสดหาย โดยจำนวนเงินที่จะสูญหายนั้นจะมีมูลค่าเท่ากับเงินที่คงค้างเหลืออยู่ ดังนั้นต้องระมัดระวังกันด้วยนะครับ



4.6 พร้อมเพย์ (Prompt Pay) ปลอดภัยใช้ได้จริง

เทคโนโลยี ถ้าเรารู้จักใช้อย่างระมัดระวัง ก็จะเกิดความมั่นคงปลอดภัยกับตนเอง โดยเฉพาะในเรื่องของเงินทองที่กว่าจะหามาให้เราใช้ได้แต่ละสตางค์นั้นก็แสนยากลำบาก ยิ่งถ้าต้องพกเงินจำนวนมากแล้วเกิดทำหายไปละก็ คงเครียดตายแน่ๆ แต่ก็ยังดีที่วันนี้มีนวัตกรรมใหม่เรียกว่า Prompt Pay (พร้อมเพย์) หรือบริการโอนเงินและรับเงินโอนแบบใหม่

Prompt Pay จะทำให้ผู้ใช้บริการสะดวกมากขึ้น โดยในที่นี้จะต้องทำการผูกบัญชีเงินฝากธนาคารกับหมายเลขบัตรประจำตัวประชาชนหรือเบอร์โทรศัพท์มือถือ โดยบริการดังกล่าวดำเนินการโดยธนาคารแห่งประเทศไทยและธนาคารพาณิชย์ทุกแห่งได้ร่วมมือพัฒนาขึ้น เพื่อสนับสนุนระบบการชำระเงินแบบ Any ID ที่อำนวยความสะดวกในการโอนเงินและการจ่ายสวัสดิการของรัฐอีกด้วย ทั้งยังลดการพกพาเงินสดในการที่ต้องใช้จ่ายครั้งละมากๆ มาใช้จ่ายผ่าน e-Payment ที่สะดวกแค่เพียงคลิกผ่านปลายนิ้ว

การใช้งานบริการ Prompt Pay

เพื่อนๆ ที่สนใจจะใช้บริการ Prompt Pay สามารถเลือกช่องทางบริการที่ปัจจุบันถูกพัฒนาขึ้นมาให้ใช้ได้ ดังนี้

1. ใช้บัญชีธนาคารผูกกับบัตรประชาชน หรือผูกกับเบอร์โทรศัพท์มือถือได้สูงสุด 3 เบอร์ต่อ 1 บัญชี สรุปคือ สามารถใช้ได้สูงสุดเพียง 4 บัญชี

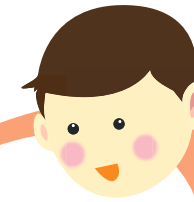
2. หากมี 2 บัญชี เราสามารถเลือกบัญชีแรกผูกกับบัตรประชาชน ซึ่งบัญชีนั้นจะมีความสำคัญในกรณีคืนเงินภาษี หรือรับเงินกับสวัสดิการภาครัฐ ส่วนบัญชีที่สองเลือกผูกกับเบอร์โทรศัพท์มือถือไว้สำหรับโอนเงิน ทำธุรกรรมทั่วไป เรียกว่าอยากทำธุรกรรมเมื่อไหร่ก็คลิกเลย

น้องพุดดิ้งชวนรู้

ประโยชน์ของบริการ Prompt Pay

อย่ามองว่า บริการ Prompt Pay มีดีแค่เป็นช่องทางสะดวกในการโอนเงินเท่านั้นนะครับ เพราะนอกจากประโยชน์ข้างต้นแล้ว การโอนเงินเข้าธนาคารเดียวกันหรือต่างธนาคารผ่านระบบ Prompt Pay ยังช่วยประหยัดค่าธรรมเนียมได้มากเลยด้วย ซึ่งปัจจุบันมี เรต ดังนี้

1. วงเงินไม่เกิน 5,000 บาท ไม่เสียค่าธรรมเนียม
2. วงเงิน 5,001-30,000 บาท คิดค่าธรรมเนียมไม่เกิน 2 บาท ต่อรายการ
3. วงเงิน 30,001-100,000 บาท คิดค่าธรรมเนียมไม่เกิน 5 บาท ต่อรายการ
4. วงเงินมากกว่า 100,000 บาทขึ้นไป คิดค่าธรรมเนียมไม่เกิน 10 บาท ต่อรายการ



น้องพุดดิ้งชวนรู้

ความปลอดภัยในการใช้งาน Prompt Pay

ระบบ Prompt Pay มีการดูแลความมั่นคงปลอดภัย แบ่งได้เป็น 3 ขั้นตอนหลักๆ คือ ขั้นตอนตั้งการลงทะเบียนที่รัดกุม ขั้นตอนการพัฒนาระบบกลาง และขั้นตอนการใช้งานของประชาชนผู้โอนเงินอย่างถูกต้อง

1. ขั้นตอนตั้งการลงทะเบียนที่รัดกุม : ธนาคารจะมีการตรวจสอบตัวตนของลูกค้าและความเป็นเจ้าของหมายเลขโทรศัพท์มือถือ นอกจากนี้ ธนาคารแห่งประเทศไทย ได้กำชับให้ธนาคารปฏิบัติตามแนวทางที่กำหนดในการรับลงทะเบียน Prompt Pay เพื่อให้การลงทะเบียนมีความมั่นคงปลอดภัย

2. ขั้นตอนการพัฒนาระบบกลาง : Prompt Pay เป็นระบบที่พัฒนาเพิ่มจากระบบโอนเงินที่ใช้อยู่ปัจจุบัน จึงมีความปลอดภัยไม่ด้อยกว่าบริการโอนเงินในปัจจุบัน เป็นระบบที่เชื่อมระหว่างธนาคารกับผู้ให้บริการระบบกลาง Prompt Pay ของประเทศ คนภายนอกไม่สามารถต่อเข้ากับระบบนี้ผ่านช่องทางอินเทอร์เน็ตทั่วไปได้ และธนาคารแห่งประเทศไทย ได้ติดตามดูแลการพัฒนาระบบด้านความมั่นคงปลอดภัยด้วย

ทั้งนี้ ผู้ให้บริการระบบกลางได้ให้บริการในระบบที่มีมาตรฐานความปลอดภัยด้านเทคโนโลยีและสารสนเทศ ตามมาตรฐาน ISO-27001 ซึ่งเป็นที่ยอมรับในระบบสากล และมีการตรวจสอบประเมินความปลอดภัยจากหน่วยงานภายนอกที่ได้รับการรับรองอีกชั้นหนึ่ง

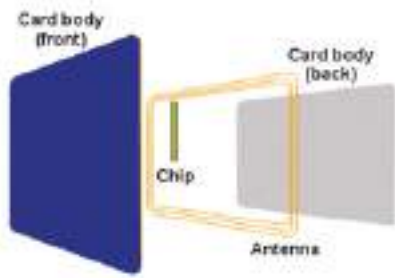
3. ขั้นตอนการใช้งานของประชาชน : นอกเหนือจากระบบกลางแล้ว Prompt Pay ได้มีการออกแบบในส่วนของกระบวนการเข้าใช้งาน กล่าวคือ ผู้ใช้บริการที่ทุกธนาคาร จะต้องมีการใส่เลขรหัสหรือ Password และมีการยืนยันรายการก่อนทำการโอนทุกครั้ง ซึ่งจะทำให้ผู้ใช้บริการสามารถทำธุรกรรมได้อย่างมั่นคงปลอดภัย

ไม่ว่าจะดูหนัง ซื้อของกิน ของใช้
ขึ้นรถไฟฟ้า ก็ใช้โทรศัพท์แทน
เงินสดได้ด้วยเทคโนโลยี NFC

4.7 รู้จัก NFC เทคโนโลยีเปลี่ยนมือถือเป็นกระเป๋าสตางค์

บัตรเงินสดอิเล็กทรอนิกส์

ปัจจุบันเราจะพกเงินสดกันน้อยลง และหันมาชำระเงินด้วยบัตรเงินสดอิเล็กทรอนิกส์มากขึ้น เพราะสะดวกในการพกพา รวดเร็ว ไม่ต้องรอเงินทอนหรือกลัวว่าจะไม่มีเงินทอน เราจะพบเห็นบัตรเหล่านี้ในรูปแบบของบัตรซื้ออาหารในศูนย์อาหาร บัตรรถไฟฟ้า บัตรเติมเงินมือถือ บัตรชมภาพยนตร์ และบัตรอื่นๆ ซึ่งผู้ใช้บริการได้ชำระเงินล่วงหน้าให้กับผู้ให้บริการเงินอิเล็กทรอนิกส์หรือเรียกว่า การเติมเงิน และผู้ใช้บริการสามารถนำไปใช้ชำระค่าสินค้าค่าบริการแทนการชำระด้วยเงินสดตามร้านค้าที่รับชำระได้



บัตรเงินสดอิเล็กทรอนิกส์ที่เราใช้อยู่มีหลายแบบ ถ้าเป็นแบบที่ใช้ในศูนย์อาหารมักจะเป็นบัตรแถบแม่เหล็ก เวลาใช้ต้องนำบัตรไปรูดกับหัวอ่านเพื่ออ่านข้อมูลเงินในบัตรและตัดเงินในบัตร ถ้าบัตรที่ใช้เป็นตั๋วรถไฟฟ้าจะต้องแตะกับเครื่องอ่านเท่านั้น เพื่อความสะดวกรวดเร็ว โดยตัวบัตรจะมีการฝังชิปและขดลวดสายอากาศไว้ภายใน ทำให้สามารถติดต่อกับเครื่องอ่านบัตรที่รับส่งสัญญาณผ่านคลื่นวิทยุได้ในระยะที่กำหนด และทำการบันทึกจำนวนเงินเอาไว้ในชิป ซึ่งบัตรแบบนี้จะเรียกว่าสมาร์ตการ์ดแบบไร้สัมผัส (Contactless Smart Card)

นอกจากเราจะเห็นการใช้งานสมาร์ตการ์ดแบบไร้สัมผัสเป็นตั๋วรถไฟฟ้าแล้ว ยังมีบัตรที่ใช้ซื้อของในร้านสะดวกซื้อ เช่น บัตรเซเว่นการ์ดของ 7-11 ซึ่งนอกจากใช้แทนเงินสดแล้ว ยังสามารถสะสมแต้มได้อีกด้วย และก็มีบัตรที่สามารถใช้ขึ้นรถไฟฟ้าและซื้อสินค้าในร้านค้าปลีก ใช้ในร้านอาหารและเครื่องดื่ม ใช้ซื้อตั๋วหนัง และอื่นๆ ได้ภายในบัตรใบเดียว เรียกว่า บัตรแรบบิท ซึ่งก็มีการสะสมแต้มด้วยเหมือนกัน แต่ต้องเช็กด้วยนะครับว่าใช้บริการได้ที่ไหนบ้าง

ร้านค้าที่รับชำระด้วยบัตรแรบบิท

NFC เปลี่ยนมือถือเป็นกระเป๋าสตางค์

NFC คืออะไร

NFC ย่อมาจาก Near Field Communication (การสื่อสารระยะใกล้) เป็นเทคโนโลยี RFID : Radio Frequency Identification แบบหนึ่งที่ช่วยให้อุปกรณ์สองเครื่อง “สื่อสาร” กันแบบไร้สายได้ในระยะใกล้ประมาณ 4-10 เซนติเมตร มีรูปแบบการใช้งาน 3 แบบ ได้แก่

1. NFC Card Emulation Mode ทำงานเสมือนเป็นบัตร Contactless Smart Card เพื่อใช้ในการทำธุรกรรม โดยนำมือถือไปแตะหรือนำไปใกล้กับเครื่องอ่าน

2. Peer-to-Peer Mode ในโหมดนี้อนุญาตให้มีการจับคู่และการเชื่อมต่ออย่างรวดเร็วแบบไร้สายกับอุปกรณ์ที่เปิดใช้งาน NFC อื่นๆ โดยไม่จำเป็นต้องป้อนรหัสผ่านและมีการยืนยันเพียงแค่นำอุปกรณ์ทั้งสอง “แตะ” หรือนำมาใกล้กันเท่านั้น ก็สามารถส่งรูปถ่ายหรือข้อมูลอื่นๆ ถึงกันได้ เช่น การจับคู่มือถือกับลำโพง หรือจับคู่มือถือกับเครื่องพิมพ์ เป็นต้น

3. Reader/Writer Mode ในโหมดนี้อุปกรณ์ NFC สามารถทำตัวเสมือนเป็นเครื่องอ่านเขียนแท็ก NFC ที่ติดอยู่ในสมาร์ตโปสเตอร์ นามบัตร หรือจุดให้บริการข้อมูล โดยสามารถกำหนดเงื่อนไขได้ เช่น 100 คนแรกที่อ่านโฆษณาที่จุดบริการจะได้คูปองส่วนลดพิเศษ ซึ่งจำนวนที่ลดลงไปเรื่อยๆ ก็คือการเขียนข้อมูลไปยังแท็ก NFC นั่นเอง ซึ่งการใช้ Barcode, QR Code หรือ RFID Tag ไม่สามารถทำได้

วันก่อนพุดน้อยเห็นคุณพ่อใช้โทรศัพท์จ่ายเงินแทนบัตรเงินสด ใช้แตะผ่านประตูสถานีรถไฟฟ้าแทนบัตรรถไฟฟ้า คุณพ่อบอกว่าคุณพ่อเพิ่งไปเปลี่ยนซิมการ์ดเป็น Rabbit SIM ซึ่งเป็นซิมที่รองรับเทคโนโลยี NFC (Near Field Communication) ในโทรศัพท์มือถือ ทำให้มือถือของคุณพ่อกลายเป็นกระเป๋าสตางค์สามารถชำระเงินแบบอิเล็กทรอนิกส์ เพียงนำโทรศัพท์มือถือแตะที่เครื่องอ่าน ณ จุดชำระเงินได้เหมือนบัตรแรบบิทเลย แถมยังสามารถเติมเงินโดยใช้ mPAY App ด้วยนะ เรียกว่าไม่ต้องไปต่อคิวเติมเงินให้เสียเวลา นอกจากนี้ ยังสามารถดูประวัติการใช้งานผ่านแอปพลิเคชันได้เลยด้วย

AIS mPAY Rabbit

สำหรับเพื่อนๆ ที่จะใช้มือถือแทนกระเป๋าสตางค์ ต้องตรวจสอบก่อนนะครับว่ามือถือของเราสามารถใช้งาน AIS mPAY Rabbit ได้หรือยัง โดยเข้าไปเช็กที่ http://www.ais.co.th/mpay/aismpayrabbit/handset.html ถ้าใช้งานได้ก็ให้ไปเปลี่ยนซิมที่ศูนย์บริการ ซึ่งอาจจะมีค่าใช้จ่ายในการเปลี่ยนซิม ก่อนใช้ก็ต้องเติมเงินเข้าบัตรด้วยนะครับ แต่อย่าเติมเงินมากไปล่ะ เพราะถ้าโทรศัพท์หาย เงินก็อาจถูกนำไปใช้ด้วย ถึงแม้ว่าสามารถโทรอายัดได้ แต่ก็อาจจะไม่ทัน นอกจากนี้ หากเพื่อนๆ ที่ใช้บริการรถไฟฟ้า ต้องระวังอย่าให้แบตเตอรี่มือถือหมดระหว่างทาง เพราะจะไม่สามารถใช้มือถือในการแตะเพื่อออกจากสถานีได้เนื่องจาก NFC จะถูกปิดไปด้วย

น้องพุดดิ้งชวนรู้

ในสหรัฐอเมริกา การใช้โทรศัพท์มือถือแตะจ่ายแทนเงินสดมีมานานแล้วในปี 2554 ทาง Google ได้เปิดการใช้งาน Google Wallet โดยมีโมบายแอปพลิเคชันที่เก็บข้อมูลบัตรเครดิต บัตรสะสมแต้ม บัตรของขวัญ และคูปอง เพียงแค่นำมือถือไปแตะที่เครื่องอ่านและกด Pin ที่มือถือก็สามารถจ่ายเงินได้ โดยก่อนจ่ายเราสามารถเลือกบัตรที่จะตัดเงินได้ และหากเรามีคูปองส่วนลด คูปองจะถูกนำมาใช้แบบอัตโนมัติ

ในปี 2557 Apple ได้เปิดตัวระบบจ่ายเงินที่เหมือนกับ Google Wallet แต่มีข้อดีกว่าตรงที่เราไม่ต้องใส่ Pin Code ตอนจ่ายเงิน เพราะ Apple ใช้ระบบ Touch ID ในการยืนยันตัวตน เพียงแค่นำโทรศัพท์ไปแตะที่เครื่องอ่าน NFC ของร้านและเอานิ้วแตะที่ Touch ID หรือปุ่ม Home ของเครื่อง ก็สามารถชำระเงินได้อย่างมั่นคงปลอดภัยและรวดเร็ว

ความมั่นคงปลอดภัยในการใช้ NFC

การใช้งานมือถือแทนเงินสดด้วยเทคโนโลยี NFC นั้นมีความมั่นคงปลอดภัยไหมนะ เนื่องจากเป็นการเก็บข้อมูลทางการเงินไว้ที่โทรศัพท์ หากมีใครที่สามารถขโมยข้อมูลนี้ไป ก็สามารถขโมยเงินเราไปใช้ได้นะสิ ซึ่งการขโมยข้อมูลสามารถทำได้โดยการใช้โทรศัพท์ที่ติดตั้งแอปพลิเคชันสำหรับดูดข้อมูลจากมือถือเราและส่งต่อไปยังมือถืออีกเครื่องหนึ่ง ทำให้มือถือเครื่องที่ได้รับข้อมูลสามารถนำเงินที่อยู่ในมือถือของเราไปใช้ซื้อสินค้าได้

นอกจากนี้ ยังมีการทำเครื่องอ่าน NFC ปลอม หรือติดตั้งอุปกรณ์เพิ่มเติมที่เครื่องอ่าน NFC เพื่อทำสำเนาข้อมูลทางการเงินของเราแล้วนำไปใช้ได้อีกด้วย

บทที่ 5

รู้เท่าทันมิจฉาชีพในมือถือ

เคยได้ยินประโยค
ที่ว่า “โลกนี้เริ่มอยู่ยากขึ้นทุกวัน” ไหมครับ
ไม่ทราบว่าใครเป็นเจ้าของประโยค แต่วัยรุ่นอย่าง
พุดน้อยอยากจะอุทานเป็นศัพท์วัยรุ่นว่า “ฟังแล้วขนลุก”
แต่กระนั้นในกรณีนี้ของการใช้ชีวิตในโลก Social Media
แล้วละก็ มิจฉาชีพที่แฝงเข้ามาในช่องทางต่างๆ จะไม่สามารถ
ทำอันตรายกับเราได้เลย หากเรารู้ถึงกลลวงและวิธีป้องกัน
ไวรัสที่บรรดามิจฉาชีพจะส่งผ่านเข้ามาทางสมาร์ตโฟน
ของเรา ซึ่งเพื่อนๆ สามารถศึกษาและปฏิบัติได้ตามวิธี
ต่อไปนี้

เดี๋ยวนี้มีการหลอกลวงทางโทรศัพท์ที่เรียกว่า **“แก๊งคอลเซ็นเตอร์”** โดยมิจฉาชีพจะใช้โทรศัพท์ หรือบริการเสียงผ่านอินเทอร์เน็ต (Voice Over Internet Protocol หรือ VoIP) แอบอ้างเป็นเจ้าหน้าที่สถาบันการเงิน หรือพนักงานในหน่วยงานของรัฐ ฯลฯ เพื่อหลอกลวงขอข้อมูลสำคัญหรือให้เหยื่อโอนเงินไปให้โดยมีหลากหลายวิธี ดังนี้

- ถูกรางวัลใหญ่จากการชิงโชค แต่ต้องไปโอนเงินค่าธรรมเนียมหรือค่าภาษีก่อน ถึงจะได้รับรางวัล
- คืนเงินค่าภาษี อ้างว่าเป็นเจ้าหน้าที่กรมสรรพากร เพื่อให้เหยื่อไปกด ATM ตามคำสั่งเพื่อรับเงินคืนภาษี แต่กลับกลายเป็นการโอนเงินให้คนร้ายไปแทน
- เงินประกันชีวิต อ้างว่าเป็นเจ้าหน้าที่จากบริษัทประกันชีวิต ผู้เสียชีวิตได้ทำประกันชีวิตไว้แต่ขาดส่งจำนวนหนึ่ง หลอกให้เหยื่อที่เป็นญาติโอนเงินจำนวนนี้เพื่อที่จะได้รับเงินประกันก้อนใหญ่
- บัญชีถูกอายัด อ้างว่าเป็นเจ้าหน้าที่จากสถาบันการเงิน แล้วแจ้งว่าบัญชีของเหยื่อถูกอายัดโดยธนาคารแห่งประเทศไทย ขอให้ยืนยันข้อมูลส่วนตัว เมื่อได้ข้อมูลของเหยื่อก็จะนำไปทำธุรกรรมทางการเงินในนามของเหยื่อ หรือหลอกให้เหยื่อไปยกเลิกรายการที่ตู้ ATM โดยทำตามวิธีของมิจฉาชีพ

นอกจากวิธีที่พุดน้อยเล่าให้ฟัง ก็ยังมีวิธีอื่นๆ อีกมากมาย โดย “แก๊งคอลเซ็นเตอร์” จะเป็นผู้ที่มีจิตวิทยาสูง ทำงานกันเป็นทีม ดังนั้น เพื่อนๆ ควรจะศึกษา ติดตามข้อมูลอย่างสม่ำเสมอ เพื่อที่จะไม่ตกเป็นเหยื่อนะครับ และหากสงสัยว่ากำลังถูกหลอก พุดน้อยแนะนำให้อย่าหลงเชื่อโดยง่าย ให้ลองโทรศัพท์ไปยังหน่วยงานที่ถูกแอบอ้างเพื่อตรวจสอบข้อมูลให้แน่ใจก่อน จะได้ไม่ถูกหลอกครับ

การใช้บริการโทรศัพท์มือถือ นอกจากจะต้องระวังภัยจาก **“แก๊งคอลเซ็นเตอร์”** ก็ยังมีภัยร้ายจากมิจฉาชีพ ด้วยกลร้ายรูปแบบอื่นๆ เช่น ภัยร้ายจากการปล่อยมัลแวร์ โปรแกรมประสงค์ร้ายที่จ้องโจมตีระบบ รวมไปถึงการขโมยข้อมูลในมือถือของคุณ ที่ต้องคอยระมัดระวังไม่แพ้กัน ซึ่งพุดน้อยจะกล่าวในหัวข้อถัดไปครับ

5.1 มือถือก็ติดไวรัสได้

เพื่อนๆ อาจจะคิดว่ามือถือไม่ติดไวรัส ซึ่งความจริงมือถือทั่วไปก็ไม่น่าติดไวรัสได้ แต่ถ้าเพื่อนๆ ใช้มือถือที่เป็นสมาร์ตโฟน ที่มีความสามารถเหมือนกับคอมพิวเตอร์ สามารถติดตั้งโปรแกรมหรือแอปพลิเคชันได้ ก็มีความเสี่ยงที่จะติดไวรัสได้เหมือนกันครับ

ไวรัสที่แพร่ระบาดในสมาร์ตโฟนมักเกิดจากการที่เราติดตั้งแอปพลิเคชันจากแหล่งที่ไม่รู้จัก ติดตั้งแอปพลิเคชันจาก SMS ที่ส่งมาในโทรศัพท์ การติดตั้งแอปพลิเคชันเถื่อน แอปพลิเคชันปลอม การไปปรับแต่งระบบปฏิบัติการของเครื่อง หรือการนำสมาร์ตโฟนไปเชื่อมต่อกับคอมพิวเตอร์ที่ไม่น่าไว้วางใจ

เมื่อไวรัสได้ทำการติดตั้งตัวเองบนสมาร์ตโฟนของเราแล้ว จะสามารถทำความเสียหายให้กับเราหลายรูปแบบ

1. ขโมยข้อมูลส่วนตัว เช่น Username หรือ Password ของบัญชีธนาคาร บัญชีอีเมล บัญชีโซเชียลเน็ตเวิร์ก ข้อมูลรายชื่อผู้ติดต่อ เบอร์โทรศัพท์ ฯลฯ

2. ลบข้อมูลในสมาร์ตโฟนของเรา เช่น รูปภาพ วิดีโอ อีเมล

3. ลักลอบใช้ SMS โปรแกรมแชต อีเมล ส่งข้อความสแปมไปยังเพื่อนๆ ของเราให้ติดตั้งไวรัสตัวนี้ต่อ

4. ดักรหัส OTP จากธนาคารที่ใช้ในการทำธุรกรรมทางอิเล็กทรอนิกส์

5. ก่อกวนระบบ ทำให้แบตเตอรี่หมดไว ทำให้เครื่องช้า ใช้งานไม่ได้

ซึ่งหากผู้ที่ปล่อยไวรัสได้ข้อมูลของเราไป อาจนำไปโอนเงินจากบัญชีของเราได้ ขโมยบัญชีอีเมล บัญชีโซเชียลเน็ตเวิร์ก เพื่อหลอกให้เพื่อนเราโอนเงินให้

เราสามารถป้องกันไวรัสเบื้องต้นได้โดย

1. ติดตั้งแอปพลิเคชันระบบรักษาความมั่นคงปลอดภัยที่สามารถสแกนไวรัสได้

2. แต่ต้องไม่ติดตั้งแอปพลิเคชันที่ส่งมาทาง SMS แอปพลิเคชันแชต หรือทางอีเมล

3. หลีกเลี่ยงการติดตั้งแอปพลิเคชันจากผู้ให้บริการรายอื่นๆ ที่ไม่น่าเชื่อถือ

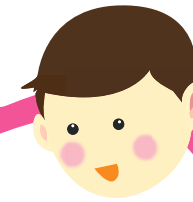
4. ติดตั้งแอปพลิเคชัน จากผู้ให้บริการที่ไว้วางใจได้เท่านั้น เช่น ระบบปฏิบัติการแอนดรอยด์ ก็ติดตั้งจาก Google Play ถ้าเป็น iOS ก็ติดตั้งจาก App Store

5. อ่านสิทธิ์การเข้าถึงข้อมูลต่างๆ ของแอปพลิเคชันที่ติดตั้ง หากมีการเรียกร้องสิทธิ์ที่น่าสงสัยก็ไม่ควรโหลด

6. อ่านรีวิวของแอปพลิเคชันก่อนโหลดมาใช้งาน

7. ดูผู้พัฒนาว่าน่าเชื่อถือหรือไม่

8. อัปเดตระบบปฏิบัติการให้เป็นรุ่นล่าสุดเสมอ



น้องพุดดิ้งชวนรู้

มัลแวร์ (Malware : Malicious Software) เป็นโปรแกรมที่มีวัตถุประสงค์ร้ายต่อระบบคอมพิวเตอร์ถูกสร้างขึ้นมาเพื่อขัดขวางการทำงานหรือเข้าแทรกซึมขโมยข้อมูลของผู้ใช้และส่งกลับไปให้แฮกเกอร์ที่สร้างมัลแวร์นั้น ซึ่งในปัจจุบันมีมือถือติดมัลแวร์เยอะมาก

ข้อสังเกตมือถือติดมัลแวร์

1. แบตเตอรี่มือถือหมดเร็วผิดปกติ อาจเกิดจากมัลแวร์ที่ทำงานอยู่เบื้องหลังและใช้งานแบตเตอรี่ตลอดเวลาก็ได้

2. สายหลุดบ่อย เพราะระหว่างที่เพื่อนๆ คุยโทรศัพท์อยู่ มัลแวร์อาจกำลังทำงานอยู่เพื่อดักฟังหรือดักข้อมูลต่างๆ ระหว่างการโทรก็ได้

3. ตรวจสอบ SMS ในมือถือของเพื่อนๆ ว่ามีการส่งจากเครื่องโดยเราไม่ได้ส่งหรือเปล่า หรือหากไม่พบก็ให้ตรวจจากค่าบริการโทรศัพท์มือถือว่ามีค่าใช้จ่ายไหนผิดปกติไหม

4. ตรวจสอบข้อมูลการใช้อินเทอร์เน็ตว่ามีการใช้งานเยอะขึ้นผิดปกติหรือเปล่า เพราะมัลแวร์บางตัวมีการขโมยข้อมูลในมือถือของเรา และอัปโหลดข้อมูลผ่านทางอินเทอร์เน็ตไปยัง Server ของแฮกเกอร์ผู้สร้างมัลแวร์นั้น

5. มือถือทำงานช้าลง เนื่องจากมัลแวร์ไปแย่งการใช้งาน CPU เพื่อนๆ ตรวจสอบได้โดยการดูว่าใน RAM มีการทำงานอะไรอยู่บ้าง ลองลบให้หมด และหากเครื่องยังช้าอยู่แสดงว่าเราโดนมัลแวร์เข้าแล้ว

หากมือถือติดมัลแวร์ควรทำอย่างไร?

1. เปลี่ยนรหัสผ่านโมบายแบงก์กิ้ง อีเมล โซเชียลเน็ตเวิร์กต่างๆ เพื่อป้องกันการนำไปใช้

2. ลบแอปพลิเคชันที่น่าสงสัย หรือเพิ่งดาวน์โหลดทิ้ง ถ้าเพื่อนๆ สงสัยว่าแอปพลิเคชันที่ดาวน์โหลดมานั้นทำให้เกิดอาการขั้นต้น

3. ลองติดตั้งแอปพลิเคชันกำจัดไวรัส เช่น Kaspersky Antivirus & Security ซึ่งจะช่วยเตือนและลบสิ่งที่น่าสงสัยให้ได้อัตโนมัติ

4. หากอาการของเครื่องยังไม่ดีขึ้น ทำการล้างเครื่องใหม่ซึ่งอาจเป็นทางเลือกสุดท้ายที่จำเป็นก็ได้

วันนี้มีอีเมลมาหาพุดน้อยว่า
"คุณเป็นผู้โชคดีถูกลอตเตอรี่รางวัลใหญ่"
ตื่นเต้นจัง แต่ว่า พุดน้อยไม่เคยซื้อลอตเตอรี่
แล้วจะถูกรางวัลได้อย่างไรนะ?

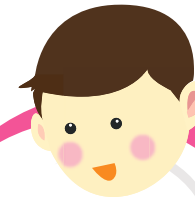
5.2 อีเมลลวงโลกระวังให้ดี

มีการหลอกลวงทางอินเทอร์เน็ต เรียกว่า Scam เป็นการหลอกให้เราคิดว่าจะได้เงินก้อนโต เช่น หลอกว่าเป็นผู้โชคดีถูกรางวัล หลอกว่าจะส่งสิ่งของที่มีมูลค่าสูงมาให้ หลอกว่าจะได้เงินฟรีๆ ด้วยเหตุผลต่างๆ หลอกให้ร่วมทำธุรกิจที่มีผลตอบแทนสูง เรียกว่าทำให้เราโลภก่อน โดยคนร้ายจะส่งอีเมลเป็นจำนวนมาก ไปหาเหยื่อกลุ่มใหญ่ ภายในอีเมลจะมีเนื้อหาเชิญชวนโน้มน้าว ทำให้เหยื่อเชื่อมั่นว่าจะได้รับเงินจำนวนมาก และยอมโอนเงินค่าธรรมเนียม ค่ามัดจำสินค้า หรือเงินลงทุนไปให้คนร้าย โดยหวังว่าจะได้เงินก้อนโตคืนภายหลัง

อีเมลที่คนร้ายส่งไปมีจำนวนมาก ถ้ามีคนเชื่อไม่กี่เปอร์เซ็นต์ก็เพียงพอแล้ว เมื่อเหยื่อติดกับดักและติดต่อกลับมา คนร้ายหรือเรียกว่า Scammer ก็จะโน้มน้าวให้เหยื่อหลงเชื่อ เกิดความโลภ และโอนเงินไปให้คนร้าย

ในประเทศไทยมีผู้เสียหายที่ถูกหลอกว่าได้รับรางวัลจากต่างประเทศเป็นจำนวนเงินนับพันล้านบาท ซึ่งพอติดต่อกลับไป ทางคนร้ายได้บอกให้เหยื่อเดินทางไปรับรางวัลที่ประเทศนั้น แต่เหยื่อไม่สามารถไปได้ ซึ่งแท้จริงแล้วเป็นอุบายของคนร้ายเพื่อหลอกให้เหยื่อตายใจ และต่อมาก็อีเมลมาบอกเหยื่อว่าไม่ต้องเดินทางไปก็ได้ แต่ให้เหยื่อส่งเงินค่าธรรมเนียมการจ่ายเงินรางวัลมาก่อน แล้วจะส่งเงินรางวัลมาให้ด้วยวิธีโอนทางบัญชีเงินฝาก เมื่อเหยื่อหลงเชื่อและได้โอนเงินไปให้คนร้าย รวมทั้งหมดประมาณ 6 ล้านบาท แต่หลังจากโอนเสร็จแล้วก็ไม่ได้รับการติดต่อกลับมาอีกเลย ซึ่งเงินที่โอนไปนั้นเป็นเงินส่วนตัว เงินที่ได้จากการจำนองบ้าน และเงินกู้นอกระบบ ซึ่งเหยื่อไม่มีโอกาสได้เงินที่โอนไปให้คนร้ายคืนแน่นอน

น่าตกใจมากใช่ไหมครับ ไม่น่าเชื่อว่าจะมีคนหลงเชื่ออีเมลแบบนี้ แต่เนื่องจากมีการส่งเป็นจำนวนมาก และอาศัยความโลภของคน ทำให้ยังมีคนที่ถูกหลอกอยู่ครับ



น้องพุดดิ้งชวนรู้

วิธีการป้องกันให้พ้นภัยจาก Email Scam

1. ไม่ควรเปิดอีเมลจากผู้ส่งที่ไม่รู้จักหรือไม่น่าไว้ใจ
2. ถ้าได้รับอีเมลประเภทถูกรางวัลใหญ่ ชวนให้ลงทุน ได้เงินมาง่ายๆ ให้สงสัยไว้ก่อนว่าเป็นการหลอกลวง
3. ไม่ตอบกลับอีเมลแปลกๆ ที่เราไม่รู้จัก
4. พึงระลึกไว้เสมอว่า ในโลกออนไลน์ทุกอย่างสามารถปลอมได้หมด เช่น ชื่อผู้ส่ง ปลอมเป็นคนอื่น ใช้ชื่อหรือรูปคนอื่นในการติดต่อ ดังนั้น ไม่ควรไว้ใจใครง่ายๆ
5. ศึกษารูปแบบของการหลอกลวงทางอีเมลแบบต่างๆ กรณีศึกษาที่มีผู้นำมาเผยแพร่ทางสื่อต่างๆ เพื่อป้องกันการตกเป็นเหยื่อ

5.3 การปลอมแปลงหน้าเว็บไซต์ (Phishing)

Phishing คือ การหลอกลวงทางอินเทอร์เน็ตโดยใช้อีเมลหรือเว็บไซต์ปลอม เพื่อให้ได้ข้อมูลสำคัญ เช่น การส่งอีเมลปลอมที่อ้างว่ามาจากธนาคาร โดยส่งข้อความเพื่อขอให้ท่าน “อัปเดต” หรือ “ยืนยัน” ข้อมูล เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนตัวต่างๆ อาทิ หมายเลขบัตรเครดิต รหัสประจำตัว (User Name) รหัสผ่าน (Password) หมายเลขบัตรประจำตัว ซึ่งผู้ไม่ประสงค์ดีก็จะได้ข้อมูลสำคัญเหล่านั้นไปทันที หรือบางครั้งอาจใช้ช่วงเหตุการณ์สำคัญ โดยปลอมอีเมลจากธนาคารเพื่อขอรับบริจาคในการช่วยเหลือภัยพิบัติต่างๆ เป็นต้น

การทำ *Phishing* เพื่อขโมยข้อมูลส่วนตัว

ผู้ที่ทำ Phishing จะส่งอีเมลหรือข้อความที่อ้างว่ามาจากองค์กรต่างๆ ที่เหยื่อติดต่อด้วย เช่น บริษัทให้บริการอินเทอร์เน็ตหรือธนาคาร โดยส่งข้อความเพื่อให้เหยื่อกลัวเพื่อ “อัปเดต” หรือ “ยืนยัน” ข้อมูลบัญชีก่อนที่จะมีผลเสียหายกับเหยื่อ โดยอีเมลที่เหยื่อได้รับจะดูสมจริงมาก มีการใส่ Hyperlink ที่อีเมล ให้เหมือนกับ URL ขององค์กรนั้นจริงๆ แต่ถ้านำเมาส์ไปชี้ที่ Link ก็จะพบว่าไม่ใช่ URL จริง แต่เป็น Link ที่ส่งไปยังเว็บไซต์ปลอมหรือหน้าต่างที่สร้างขึ้น

ตัวอย่างอีเมลปลอม

เมื่อเหยื่อเข้าสู่เว็บไซต์ปลอมเหล่านี้ จะถูกล่อลวงให้กรอกข้อมูลส่วนตัว ซึ่งจะถูกส่งไปยังผู้สร้างเว็บไซต์ปลอม เพื่อนำข้อมูลของเหยื่อไปใช้ เช่น ซื้อสินค้า ขโมยบัญชีอีเมล บัญชีธนาคารทางอินเทอร์เน็ต หรืออื่นๆ

ป้องกันตนเองจาก *Phishing* ที่หลอกขโมยข้อมูลส่วนตัวได้อย่างไร

1. ระวังอีเมลที่ขอให้กรอกข้อมูลส่วนบุคคล โดยเฉพาะอีเมลที่มาจากสถาบันการเงิน ผู้ส่งอีเมลลวงมักจะขอให้เรากรอกข้อมูล เช่น รหัสประจำตัว (Username) รหัสผ่าน (Password) หมายเลขบัตรเครดิต ซึ่งข้อความที่ได้รับส่วนใหญ่จะเป็นข้อความที่ทำให้เรากลัว และต้องรีบปฏิบัติตาม เพราะอาจเกิดความเสียหาย ในความเป็นจริงทางสถาบันการเงินจะไม่มีนโยบายขอข้อมูลประเภทนี้ของลูกค้าทางอีเมลโดยเด็ดขาด

2. ไม่ควรคลิกลิงก์ในอีเมลเพื่อเข้าไปยังหน้าเว็บไซต์ เพราะลิงก์ที่เห็นในอีเมลอาจเป็นลิงก์ที่นำไปยังเว็บไซต์ปลอม เราควรเข้าสู่เว็บไซต์โดยตรงโดยการพิมพ์ URL ใหม่

3. หากเว็บไซต์ที่ท่านจะให้ข้อมูลสำคัญต้องขึ้นต้นด้วย https เสมอ หากเป็นแค่ http ก็ไม่ควรให้ข้อมูล

4. รายงานอีเมลที่น่าสงสัยว่าเป็นสแปม หรือลบทิ้งเพื่อป้องกันการเปิดซ้ำและเผลอไปคลิกลิงก์

การทำ *Phishing* เพื่อหลอกให้โอนเงินชำระค่าสินค้า

นอกจากการปลอมอีเมลเป็นสถาบันการเงินเพื่อขโมยข้อมูลทางการเงินแล้ว ยังมีการทำ Phishing เพื่อหลอกให้คู่ค้าโอนชำระเงินค่าสินค้าไปยังบัญชีธนาคารของคนร้าย โดยผู้เสียหายส่วนใหญ่เป็นธุรกิจสั่งสินค้านำเข้าจากต่างประเทศ ซึ่งติดต่อกันทางอีเมล โดยมีวิธีการชำระค่าสินค้าด้วยวิธีการโอนเงินผ่านทางบัญชีธนาคาร

คนร้ายจะสวมรอยเป็นคู่ค้าจากต่างประเทศ โดยปลอมแปลงอีเมลให้คล้ายกับอีเมลของผู้ที่ติดต่ออยู่เดิม ซึ่งอีเมลอาจจะต่างกันที่การสะกดคำ ถ้าผู้รับไม่สังเกตให้ดีก็จะไม่รู้ ถ้ามีการตอบกลับด้วยปุ่ม Reply ก็จะไม่มีทางรู้เลยว่ากำลังคุยผิดคนอยู่

เมื่อคนร้ายปลอมเป็นคู่ค้าทั้งสองฝ่ายและเป็นตัวกลางตอบกลับอีเมลโดยที่ทั้งสองฝ่ายไม่รู้ตัว และเมื่อถึงเวลาจะชำระเงินก็จะแจ้งเปลี่ยนบัญชีธนาคารเป็นของคนร้าย โดยใช้อุบายต่างๆ เช่น การให้ส่วนลดในการชำระเงินผ่านบัญชีใหม่ การปรับเพิ่มค่าธรรมเนียมของธนาคารเดิม เป็นต้น

การทำ Phishing กรณีแบบนี้ มีผู้เสียหายเคยโอนเงินไปให้คนร้ายอยู่หลายคดี มูลค่าความเสียหายนับล้านบาท

วิธีการป้องกันตนเองจากการทำ *Phishing* เพื่อหลอกให้โอนเงินผิดบัญชี

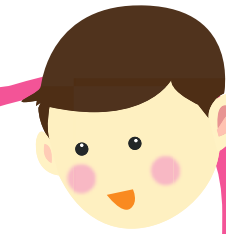
1. ไม่ควรใช้ปุ่ม Reply เพื่อตอบอีเมล ควรพิมพ์ คัดลอก หรือเลือกจาก Contact เท่านั้น

2. หากมีการแจ้งเปลี่ยนแปลงหมายเลขบัญชีธนาคาร ควรโทรไปสอบถามเพื่อยืนยันความถูกต้อง หรือมีการยืนยันเป็นลายลักษณ์อักษรหรือยืนยันโดยตรวจสอบย้อนกลับ

3. ตรวจสอบบัญชีอีเมลของเราอย่างสม่ำเสมอ หากมีความผิดปกติ เช่น อีเมลที่คู่ค้าส่งมามีคนเปิดอ่านก่อนที่เราจะอ่าน หรือหายไป หรือมีการใช้อีเมลจากเครื่องที่ไม่รู้จัก ให้รีบเปลี่ยนพาสเวิร์ดอีเมลทันที

4. ตั้งคำถามกันลืมของอีเมลให้รัดกุม และใช้การยืนยันตัวตนผ่านมือถือ

5. เปลี่ยนพาสเวิร์ดอีเมลอย่างน้อยเดือนละครั้ง



น้องพุดดิ้งชวนรู้

จุดสังเกตอีเมลปลอม

1. ชื่อผู้ส่ง มิจฉาชีพมักแอบอ้างโดยปลอมแปลงชื่อผู้ส่งให้เป็นชื่อขององค์กร จึงควรตรวจสอบชื่อบัญชีอีเมลควบคู่

2. ชื่อบัญชีอีเมล มักจะไม่ใช่ขององค์กรที่ถูกอ้างอิง ซึ่งโดยส่วนมากหากเป็นชื่อบัญชีอีเมลของสถาบันการเงินจริงๆ มักลงท้ายด้วยตัวย่อขององค์กรนั้นๆ เช่น xxx@bot.or.th ซึ่งมาจาก Bank of Thailand

3. URL ตรวจสอบว่าเป็น URL ของสถาบันการเงินนั้นจริงๆ โดยดูว่าขึ้นต้นด้วย https:// หรือไม่ และควรสะกดถูกต้องทุกตัวอักษร

จุดสังเกตเว็บไซต์ปลอม

1. สัญลักษณ์รูปกุญแจ แสดงการเข้ารหัสปลอดภัย จะแสดงในหน้าเว็บไซต์ที่ลงชื่อเข้าใช้ระบบ

2. ชื่อผู้ให้บริการ จะแสดงชื่อสถาบันการเงินที่จดทะเบียนใช้เว็บไซต์นั้นๆ

3. URL จะต้องขึ้นต้นด้วย https:// เพราะ “s” แสดงถึงการเข้ารหัสความปลอดภัยในการเข้าสู่ระบบ

ข้อมูลจากกลโกงธนาคารออนไลน์ : http://www.1213.or.th/th/finfrauds/OnlineFraud/Pages/OnlineFraud.aspx

แม้ว่าระบบปฏิบัติการ iOS
เป็นระบบที่มีความปลอดภัยสูง แต่ก็ไม่ได้
หมายความว่าผู้ใช้ระบบปฏิบัติการ iOS
จะปลอดภัยจากมัลแวร์นะครับ เพราะล่าสุดมีการค้นพบ
มัลแวร์ตัวใหม่ที่สามารถโจมตีอุปกรณ์ที่ใช้งาน
ระบบปฏิบัติการ iOS ได้

5.4 ภัยบน iOS

iOS (ไอโอเอส) เป็นชื่อเรียกระบบปฏิบัติการบนอุปกรณ์พกพาที่พัฒนาโดยบริษัท Apple ใช้กับ iPhone, iPad และ iPod Touch เท่านั้น บริษัท Apple ไม่อนุญาตให้นำ iOS ไปติดตั้งบนอุปกรณ์พกพาที่ผลิตโดยบริษัทอื่น เหมือนกับระบบปฏิบัติการ Android ของ Google และระบบปฏิบัติการ Windows Phone ของ Microsoft

อุปกรณ์ของ Apple ที่ติดตั้งระบบปฏิบัติการ iOS

ระบบปฏิบัติการ iOS ได้ออกแบบให้มีความมั่นคงปลอดภัยมาก โดยมีมาตรการดังนี้

1. ผู้ใช้ไม่สามารถติดตั้งแอปพลิเคชันจากแหล่งภายนอกได้ ต้องดาวน์โหลดจาก App Store เท่านั้น

2. กระบวนการตรวจสอบแอปพลิเคชันที่จะส่งขึ้น App Store นั้นเป็นการตรวจสอบโดยมนุษย์ ซึ่งมีการตรวจสอบทั้งคุณภาพของแอปพลิเคชันและความมั่นคงปลอดภัยในการใช้งาน ดังนั้นจึงมีโอกาสน้อยที่แอปพลิเคชันที่เป็นอันตรายจะหลุดขึ้นมาอยู่บน App Store

3. iOS ความเข้มงวดในการจำกัดสิทธิ์การเข้าถึงข้อมูลสำคัญของผู้ใช้แอปพลิเคชัน เช่น เปิดใช้งานกล้องถ่ายรูป อัดเสียง ดูภาพที่ถ่าย ดูข้อมูลปฏิทิน ดูตำแหน่ง GPS ซึ่งจำเป็นต้องได้รับการอนุญาตจากผู้ใช้ก่อนเสมอ โดยจะมีหน้าต่างแจ้งเตือนการขออนุญาตแสดงขึ้นมาในครั้งแรกที่ผู้ใช้เรียกใช้งานความสามารถนั้นๆ

4. แอปพลิเคชันที่ติดตั้งอยู่ในเครื่องจะไม่สามารถเข้าถึงข้อมูลของแอปพลิเคชันอื่นๆ ได้ นอกจากผู้ใช้จะเป็นคนกำหนดข้อมูลที่ต้องการแชร์ระหว่างแอปพลิเคชันต่างๆ เอง

5. ระบบการจัดการแอปพลิเคชันของ iOS แอปพลิเคชันที่มีการทำงานอยู่เบื้องหลัง (ไม่ถูกเรียกขึ้นมาแสดงผล) จะถูกจำกัดความสามารถในการทำงาน ไม่สามารถใช้ทรัพยากรของระบบได้มากเท่า Android เช่น แอปพลิเคชันของ iOS ที่รันอยู่เบื้องหลัง จะสามารถรับข้อความแจ้งเตือนเพื่อมาแสดงผลได้เท่านั้น ไม่สามารถอัดเสียงหรือประมวลผลงานอื่นที่ทำค้างอยู่ได้

มาตรการทั้ง 5 ข้อนี้ทำให้การใช้งานระบบปฏิบัติการ iOS แบบผู้ใช้ทั่วไปมีความปลอดภัยมาก ยกเว้นว่าจะมีการผิดพลาดของกระบวนการบางอย่าง เช่น การตรวจสอบแอปพลิเคชันด้วยคนก่อนส่งขึ้น App Store ไม่รัดกุมพอ ก็อาจมีแอปพลิเคชันที่เป็นมัลแวร์หลุดออกมาให้ดาวน์โหลดได้ ซึ่งก็เคยเกิดขึ้นมาแล้ว

มัลแวร์ใน iOS ตัวแรกสุดค้นพบเมื่อปี พ.ศ. 2552 เป็นมัลแวร์ที่มีการแอบส่งต่อผ่าน SMS ของผู้ใช้ไปยังบุคคลอื่น หลังจากนั้นก็เริ่มมีการค้นพบมัลแวร์ใน iOS อยู่เรื่อยๆ โดยมีทั้งแบบที่เป็น Spyware หรือมัลแวร์ขโมยข้อมูลธนาคารออนไลน์ แต่เกือบทั้งหมดสามารถติดได้เฉพาะเครื่องที่มีการปรับแต่งระบบปฏิบัติการเพื่อลงแอปพลิเคชันจากแหล่งอื่น หรือเรียกว่าการเจลเบรคเท่านั้น

ในปี พ.ศ. 2554 นักวิจัยชื่อ Charlie Miller ได้ทดลองส่งแอปพลิเคชันขึ้น App Store โดยลักษณะภายนอกเป็นแอปพลิเคชันธรรมดา แต่ตั้งค่าไว้ว่าเมื่อผู้ใช้ติดตั้งแอปพลิเคชันนี้ลงในเครื่องแล้วจะสามารถดาวน์โหลดโค้ดของมัลแวร์มาทำงานบนแอปพลิเคชันตัวนี้ ซึ่งจะผ่านการตรวจสอบจาก Apple และหลุดขึ้นมาอยู่บน App Store ได้ ทำให้เห็นช่องโหว่ของ iOS ในขณะนั้น

- ผู้ใช้งาน iOS ต้องติดตั้งแอปพลิเคชันผ่าน App Store เท่านั้น
- การขอสิทธิ์ในการเข้าถึงข้อมูลสำคัญจากผู้ใช้

มีเพียง 2 ครั้งเท่านั้นที่มัลแวร์ใน iOS (ตัวที่ไม่ใช่นักวิจัยทำ) สามารถหลุดขึ้นไปอยู่ใน App Store และสร้างความเสียหายให้กับผู้ใช้ หลังจากที่ค้นพบก็จะมีการลบออกจาก App Store ด้วยเวลาอันรวดเร็ว

นอกจากมัลแวร์ 2 ตัวข้างต้นแล้ว มัลแวร์เกือบทั้งหมดที่พบใน iOS จะติดได้จากเครื่องที่ถูกเจลเบรคเท่านั้น ดังนั้น ถ้าเพื่อนๆ ไม่ไปเจลเบรคเครื่อง โอกาสที่จะติดมัลแวร์ก็เป็นไปได้น้อยมาก

ต่อมาใน พ.ศ. 2556 มีทีมนักวิจัยจาก Georgia Tech ได้ใช้เทคนิคใหม่ที่ทำให้สามารถส่งแอปพลิเคชันที่เป็นมัลแวร์ขึ้นไปอยู่บน App Store ได้อีกครั้ง เหตุการณ์เหล่านี้ก็เป็นเครื่องพิสูจน์ที่ดีว่า ถึงแม้จะใช้คนตรวจแล้วก็ตาม แต่ก็ไม่อาจไว้ใจเรื่องความปลอดภัยได้ 100% อยู่ดี

iPhone iPad iPod ติดมัลแวร์ภายใน 1 นาที

โดยปกติแล้วระบบปฏิบัติการ iOS จะไม่อนุญาตให้ผู้ใช้ติดตั้งแอปพลิเคชันจากแหล่งอื่นที่ไม่ใช่ App Store แต่ Apple ก็ได้เปิดช่องทางให้ผู้พัฒนาแอปพลิเคชันหรือองค์กรต่างๆ สามารถแจกจ่ายหรือติดตั้งแอปพลิเคชันที่พัฒนาขึ้นมาเองลงในอุปกรณ์ของตัวเองได้โดยไม่ผ่านช่องทาง App Store ซึ่งโดยส่วนใหญ่จะเป็นแอปพลิเคชันที่พัฒนาขึ้นมาสำหรับทดสอบหรือเพื่อใช้งานเฉพาะภายในองค์กรเป็นหลัก

การจะทำแบบนี้ได้ ผู้พัฒนาจะต้องแจ้งหมายเลขประจำเครื่อง (UDID) ให้กับ Apple และสร้าง Provisioning Profiles ขึ้นมาในอุปกรณ์ iOS นั้น เมื่อทำตามขั้นตอนทั้งสองอย่างแล้วจะสามารถติดตั้งแอปพลิเคชัน โดยไม่ผ่าน App Store ได้ ซึ่งทำให้เกิดความเสี่ยงในการติดมัลแวร์ แต่ก็เกิดขึ้นในวงแคบเท่านั้น

แต่จากช่องโหว่นี้เองก็มีผู้พัฒนาเครื่องชาร์จไฟที่สามารถทำให้อุปกรณ์ iOS ของเราสร้าง Provisioning Profiles ขึ้นมาเองและติดตั้งมัลแวร์เข้าสู่เครื่องอัตโนมัติภายในเวลาไม่ถึง 1 นาที โดยที่เราไม่มีทางรู้ตัวเลย

วิธีการตรวจสอบเพียงแค่เราเข้าไปที่แอปพลิเคชัน Settings ->General -> Profiles ซึ่งคนทั่วไปมักจะไม่ได้เข้ามาตรวจสอบ

แต่ปัญหานี้ได้ถูกแก้ไขแล้วใน iOS เวอร์ชัน 7 โดยมีข้อความเตือนการเชื่อมต่อทุกครั้ง เพื่อป้องกันการเชื่อมต่อที่ไม่ได้รับอนุญาต แต่บางครั้งเจ้าของเครื่องก็เผลอกด Trust ได้โดยไม่ได้ตั้งใจ

ฉะนั้นการป้องกันที่น่าจะมีประสิทธิภาพมากที่สุดก็คือ หลีกเลี่ยงการเชื่อมต่อกับอุปกรณ์ที่ไม่รู้จัก หรือเชื่อมต่อเฉพาะอุปกรณ์ที่เป็นของตนเองเท่านั้น เท่านี้ก็น่าจะช่วยให้การใช้งานอุปกรณ์ iOS ของเรามีความปลอดภัยมากขึ้นได้แล้ว

ข้อความเตือนเมื่อนำเครื่องไปเชื่อมต่อกับเครื่องคอมพิวเตอร์

มัลแวร์ WireLurker

WireLurker เป็นมัลแวร์ติดในเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Mac OS X หรือ Windows ก่อน และเมื่อผู้ใช้นำอุปกรณ์ iOS มาเชื่อมต่อกับเครื่องคอมพิวเตอร์เครื่องนั้นผ่านสาย USB มัลแวร์จะแอบติดตั้งแอปพลิเคชันอันตรายไว้ที่อุปกรณ์ iOS ของเรา แม้ว่าเครื่องของเราจะไม่ผ่านการเจลเบรคก็ตาม

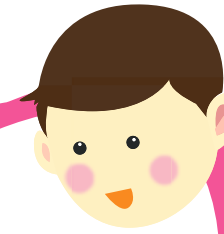
อันตรายของมัลแวร์ WireLurker คือ ความสามารถที่จะเข้าถึงข้อมูลทุกอย่างบนอุปกรณ์เคลื่อนที่ระบบ iOS ได้ เช่น ข้อมูล Address Book หรือ iMessage ความสามารถติดตั้งแอปพลิเคชันอันตรายลงไปทับแอปพลิเคชันเดิมในเครื่องได้

ทางศูนย์วิจัยของ Kaspersky พบว่ามัลแวร์ WireLurker แพร่ระบาดในประเทศจีน แคนาดา ไต้หวัน หรือฮ่องกง แต่ยังไม่พบในประเทศไทย ถึงแม้ว่ามัลแวร์ตัวนี้ยังไม่มีรายงานค้นพบว่าระบาดในบ้านเรา แต่เพื่อนๆ สบายใจได้ เพราะมัลแวร์ตัวนี้จะมากับแอปพลิเคชันเถื่อนของเครื่อง Mac ที่ปล่อยให้ดาวน์โหลดที่เว็บไซต์จีนเท่านั้น ถ้าเพื่อนๆ ใช้โปรแกรมอย่างถูกต้องก็ไม่มีทางติดมัลแวร์ตัวนี้แน่นอน ยิ่งไปกว่านั้นทาง Apple ก็ได้ทำการบล็อกแอปพลิเคชันที่ปล่อยมัลแวร์ตัวนี้ทางเว็บไซต์ดังกล่าวแล้ว และผู้ที่พัฒนาก็ถูกจับกุมตัวไปแล้ว

ถึงแม้ว่ามัลแวร์ WireLurker จะไม่แพร่ระบาดแล้ว ก็ยังวางใจไม่ได้ เพราะอาจมีนักพัฒนารายอื่นพัฒนามัลแวร์ที่คล้ายๆ กับ WireLurker มาเผยแพร่อีกก็ได้ พุดน้อยจึงมีวิธีป้องกันตนเองจากภัยคุกคามของมัลแวร์แบบ WireLurker มาบอกเพื่อนๆ ดังนี้

1. ควรดาวน์โหลดโปรแกรมหรือแอปพลิเคชันที่ถูกลิขสิทธิ์เท่านั้น
2. ควรชาร์จอุปกรณ์มือถือผ่านปลั๊กไฟโดยตรง เพื่อป้องกันมัลแวร์ติดผ่านทางสาย USB
3. ติดตั้งโปรแกรมป้องกันไวรัสในระบบปฏิบัติการ Mac OS X และ Windows
4. ควรสแกนเพื่อตรวจหามัลแวร์ในคอมพิวเตอร์ของผู้ใช้งานสม่ำเสมอ
5. ไม่ดาวน์โหลดโปรแกรมออนไลน์จากเว็บไซต์ที่ไม่น่าเชื่อถือ
6. อัปเดตระบบปฏิบัติการ Mac OS X และ Windows ให้เป็นเวอร์ชันล่าสุดเสมอ
7. ไม่ติดตั้งโปรแกรมหรือแอปพลิเคชันที่ไม่แน่ใจ

จากภัยที่พุดน้อยยกตัวอย่างมาทำให้เรารู้ว่า ไม่มีระบบปฏิบัติการใดปลอดภัยจากมัลแวร์ 100% ดังนั้นเพื่อนๆ จำเป็นต้องระมัดระวังและศึกษาหาความรู้อย่างสม่ำเสมอนะครับ



น้องพุดดิ้งชวนรู้

การเจลเบรค (Jailbreak) เครื่องคืออะไร?

โดยปกติแล้วผู้ใช้ระบบปฏิบัติการ iOS จะติดตั้งแอปพลิเคชันได้จาก App Store ซึ่งเป็นร้านจำหน่ายแอปพลิเคชันของ Apple ได้เพียงที่เดียวเท่านั้น ซึ่งแอปพลิเคชันทั้งหมดใน App Store ได้ผ่านการตรวจสอบของ Apple แล้ว

การเจลเบรคคือ การปรับแต่งระบบปฏิบัติการ iOS ของ Apple ทำให้สามารถติดตั้งแอปพลิเคชันที่ไม่ได้ผ่านการตรวจสอบของ Apple หรือเรียกว่า แอปพลิเคชันเถื่อนได้ โดยผ่านร้านจำหน่ายแอปพลิเคชัน เช่น Cydia หรือ Icy ซึ่งขึ้นอยู่กับเครื่องมือในการเจลเบรค

▶▶ Cydia Store สำหรับติดตั้งแอปพลิเคชันเถื่อน

▶▶ ตัวอย่าง Provisioning Profiles ที่มีการติดตั้งอยู่ในอุปกรณ์ iOS สามารถดูได้จากเมนู General -> Profiles

Provisioning Profiles คืออะไร?

โดยปกติแล้ว Provisioning Profiles นั้นจะใช้กับอุปกรณ์ iOS ที่อนุญาตให้มีการลงทะเบียน เป็นอุปกรณ์สำหรับใช้ในการพัฒนา หมายถึงอุปกรณ์ iOS ใดก็ตามที่ติดตั้ง Provisioning Profiles เท่ากับว่าสามารถติดตั้งแอปพลิเคชันที่พัฒนาขึ้นเองได้ทันที มักจะถูกนำมาใช้งานกับนักพัฒนาแอปพลิเคชันเป็นส่วนใหญ่

Android เป็นระบบปฏิบัติการ
บนสมาร์ตโฟนที่มีคนใช้มากที่สุดในโลก จึงมี
ผู้พัฒนา Malware เป็นจำนวนมาก
ทั้งในรูปแบบของ .apk และใน Google Play Store
ดังนั้นเพื่อนๆ ที่ใช้ Android
จะต้องระวังในการติดตั้งแอปพลิเคชันด้วยนะ

5.5 ภัยบน Android

Android (แอนดรอยด์) เป็นชื่อเรียกระบบปฏิบัติการบนอุปกรณ์พกพา เริ่มพัฒนาโดยบริษัทแอนดรอยด์ซึ่งภายหลังบริษัท Google ได้ซื้อกิจการไปพัฒนาต่อ Android เป็นระบบปฏิบัติการแบบโอเพนซอร์ซ (Open Source) ทำให้นักพัฒนาสามารถแก้ไข ดัดแปลงโค้ดแอนดรอยด์ได้อย่างอิสระ ไม่มีค่าลิขสิทธิ์ในการนำไปใช้ ทำให้บริษัทผู้ผลิตอุปกรณ์พกพาอื่นๆ สามารถนำ Android ไปปรับแต่งและติดตั้งในอุปกรณ์พกพาของตนเองได้

ก่อนที่จะมารู้จักกับภัยบน Android พุดน้อยจะอธิบายถึงวิธีการติดตั้งแอปพลิเคชันในระบบปฏิบัติการให้เพื่อนๆ เข้าใจกันก่อนนะครับ

การติดตั้งแอปพลิเคชันในระบบปฏิบัติการ Android

การติดตั้งโปรแกรมในระบบปฏิบัติการ Android สามารถทำได้ 2 ทาง คือ ติดตั้งจาก Google Play และดาวน์โหลดไฟล์ .apk มาติดตั้งเอง ซึ่งแต่ละแบบมีวิธีการดังนี้

ติดตั้งจาก Google Play

Google Play คือ ศูนย์รวมโปรแกรมของระบบปฏิบัติการ Android ที่ Google เปิดให้ผู้ใช้สามารถเข้ามาค้นหาและดาวน์โหลดโปรแกรมที่มาจากผู้พัฒนาภายนอกได้ผ่านทางเว็บไซต์ https://play.google.com หรือเข้าจากแอปพลิเคชัน Google Play ในโทรศัพท์มือถือ หากผู้ใช้ต้องการติดตั้งโปรแกรมใดๆ ก็สามารถติดตั้งฟรีหรือซื้อตามราคาที่ระบุไว้ โดยคลิกไปที่ราคาที่อยู่ใต้ชื่อของโปรแกรมนั้นๆ หลังจากเลือกอุปกรณ์ที่ต้องการติดตั้งโปรแกรมแล้ว หากผู้ใช้เชื่อมต่ออุปกรณ์ดังกล่าวเข้ากับอินเทอร์เน็ต โปรแกรมที่เลือกก็จะมีการดาวน์โหลดและติดตั้งลงในอุปกรณ์ดังกล่าวให้โดยอัตโนมัติ ตัวอย่างหน้าจอเว็บไซต์ Google Play เป็นดังรูป

Google Play

ติดตั้งจากไฟล์ .apk

ไฟล์ .apk เป็นไฟล์ที่ใช้สำหรับติดตั้งโปรแกรมของระบบปฏิบัติการ Android ซึ่งผู้ใช้อาจดาวน์โหลดมาจากเว็บไซต์ของผู้พัฒนาโปรแกรมเอง หรือดาวน์โหลดมาจากเว็บไซต์ที่แจกโปรแกรมซึ่งอาจละเมิดลิขสิทธิ์ โดยปกติแล้วระบบปฏิบัติการ Android จะรองรับการติดตั้งโปรแกรมอื่นๆ ที่ไม่ได้อยู่ใน Google Play ได้ โดยผู้ใช้ต้องมากำหนดค่าจากเมนู Setting เลือก Applications แล้วเลือก Unknown Sources เพื่อยอมรับการติดตั้งโปรแกรมที่ไม่รู้แหล่งที่มา ดังรูป

การกำหนดค่าให้อุปกรณ์สามารถติดตั้งแอปพลิเคชันจากแหล่งอื่นๆ ได้

การติดตั้งแอปพลิเคชัน จากไฟล์ที่มีนามสกุล .apk

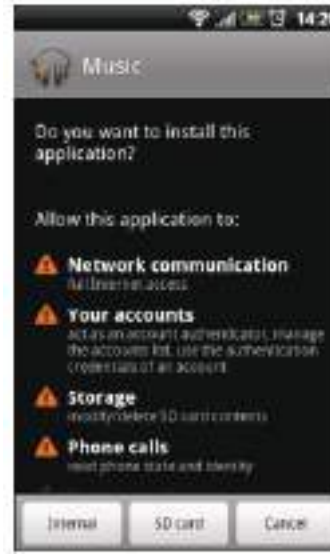
ผู้ใช้สามารถใช้โปรแกรมประเภท File Manager เพื่อเปิดหาโปรแกรม .apk ที่อยู่ใน SD Card ทำการติดตั้งโปรแกรมจากไฟล์ .apk ที่ดาวน์โหลดมาได้

แต่ไม่ว่าจะเป็นการติดตั้งแอปพลิเคชันจาก Google Play หรือจากไฟล์ .apk จะมีการแสดงหน้าจอ Permission เพื่อให้ผู้ใช้ตรวจสอบและยอมรับสิทธิ์การเข้าถึงของโปรแกรมที่จะติดตั้ง

Permission ใน Android คืออะไร

ระบบปฏิบัติการ Android นั้นออกแบบมาให้มีความมั่นคงปลอดภัยตั้งแต่แรก โปรแกรมทุกตัวในระบบจะสามารถเข้าถึงได้แค่คุณสมบัติพื้นฐานของระบบ เช่น ส่วนติดต่อกับผู้ใช้การแสดงผลทางหน้าจอ เป็นต้น หากผู้พัฒนาต้องการให้โปรแกรมของตนมีการเรียกใช้คุณสมบัติพิเศษเพิ่มเติมจากระบบปฏิบัติการ เช่น อ่านข้อมูลบัญชีผู้ใช้ หรือเขียนข้อมูลใน SD Card ก็จำเป็นต้องเพิ่มส่วนที่เป็นการขอใช้สิทธิ์ (Permission) ดังกล่าวในโปรแกรมของตนด้วย

รายการสิทธิ์ทั้งหมดที่โปรแกรมต้องการใช้งานนั้นจะปรากฏตั้งแต่แรกตอนผู้ใช้ติดตั้งโปรแกรม ดังรูป เพื่อให้ผู้ใช้ได้รับทราบและพิจารณาการทำงานของโปรแกรมก่อนทำการติดตั้ง



การขอสิทธิ์ในการเข้าถึง (คุณสมบัติพื้นฐานของอุปกรณ์พกพา จากแอปพลิเคชันที่กำลังติดตั้ง)

ผู้ใช้ควรดูว่าแอปพลิเคชันที่จะติดตั้งนี้ขอสิทธิ์อะไรบ้าง สามารถเข้าถึงส่วนไหนได้บ้าง เป็นการป้องกันตัวเองจากแอปพลิเคชันที่ไม่พึงประสงค์ ยกตัวอย่างเช่น ขอ Permission Full Internet Access เพื่อขออนุญาตให้แอปพลิเคชันเชื่อมต่อกับอินเทอร์เน็ตได้ ขอ Permission Read Contact Data คือ การอนุญาตให้แอปพลิเคชันอ่านหรือสร้างรายชื่อผู้ติดต่อในสมุดโทรศัพท์ได้ และยังมีอีกหลาย Permission ที่ผู้ใช้ต้องระวัง

จะเห็นได้ว่า Permission บางอย่างอาจถูกผู้ไม่หวังดีนำไปใช้ในทางที่ผิดได้ เช่น สร้าง Malware เพื่อแอบอ่านข้อมูลรายชื่อผู้ติดต่อของผู้ใช้ แอบถ่ายรูปผู้ใช้ รวมถึงแอบส่งข้อมูลของผู้ใช้งานผ่านอินเทอร์เน็ตกลับไปให้ผู้พัฒนา Malware เป็นต้น Malware ที่ถูกสร้างมาเพื่อขโมยข้อมูลอาจมาในรูปของโปรแกรมธรรมดา เช่น เครื่องคิดเลข แต่มีความต้องการ Permission ที่ไม่น่าจะเกี่ยวข้องกับการทำงานของโปรแกรม เช่น เข้าถึงข้อมูลรายชื่อผู้ติดต่อ เข้าถึงกล้องถ่ายรูป หรือเชื่อมต่อกับอินเทอร์เน็ต เป็นต้น ดังนั้น ก่อนทำการติดตั้งโปรแกรมทุกครั้งควรตรวจสอบให้แน่ใจว่าโปรแกรมนั้นไม่ได้มีการขอใช้สิทธิ์เกินความจำเป็น

Settings -> Applications -> Manage Applications -> Permission

หากผู้ใช้ต้องการตรวจสอบว่าโปรแกรมที่ติดตั้งไปแล้วนั้น มีการขอ Permission อะไรบ้าง สามารถทำได้ด้วยการเข้าไปที่เมนู Settings เลือก Applications แล้วเลือก Manage Applications จากนั้นจะปรากฏรายชื่อโปรแกรมที่ติดตั้งในระบบ ซึ่งสามารถเลือกดูรายละเอียด Permission ของแต่ละโปรแกรมได้

หากโปรแกรมที่ได้ติดตั้งไปแล้วแจ้งให้ทำการ Update แบบ Manual Update หมายความว่า ทางผู้พัฒนามีการปรับเปลี่ยน Permission บางอย่างจากเวอร์ชันก่อนหน้า ก่อนทำการติดตั้งโปรแกรมเวอร์ชันใหม่ควรตรวจสอบ Permission เพื่อความแน่ใจอีกครั้งหนึ่ง

ภัยจากการติดตั้งแอปพลิเคชัน บน Android

หลังจากที่เพื่อนๆ ได้ทำความเข้าใจในการติดตั้งแอปพลิเคชันบน Android แล้ว พุดน้อยจะยกตัวอย่างการโจรกรรมข้อมูลจากแอปพลิเคชันให้เพื่อนๆ ได้รู้และระวังตัวครับ

การปลอม SMS (Phishing SMS) จากธนาคารให้ติดตั้งแอปพลิเคชัน

ข้อมูลจาก ThaiCERT เมื่อวันที่ 8 มีนาคม 2556 ได้เตือนว่ามีการส่ง SMS โดยปลอมเบอร์โทรศัพท์ผู้ส่งว่ามาจากธนาคาร และมี Link ให้ดาวน์โหลดแอปพลิเคชัน (.apk) เมื่อผู้ใช้กดติดตั้งแอปพลิเคชัน แอปพลิเคชันจะขอ Permission ในการเขียนข้อมูลลงใน External Storage (เช่น SD Card) และรับส่ง SMS

เมื่อติดตั้งเสร็จแล้วเปิดแอปพลิเคชันเข้าไปจะพบหน้าจอให้ใส่รหัสผ่านสำหรับเข้าใช้งานบัญชีธนาคารออนไลน์ ดังรูป ซึ่งหากกรอกข้อมูลไปผู้ใช้อาจถูกขโมยข้อมูลรหัสผ่านได้ เพราะจากการตรวจสอบของ ThaiCERT พบว่าแอปพลิเคชันมีฟังก์ชันในการส่ง SMS ไปยังหมายเลขโทรศัพท์ที่อยู่ในประเทศรัสเซีย ผู้ซึ่งอาจนำไปสู่การขโมยเงินจากธนาคารในภายหลังได้

แอปพลิเคชันธนาคารปลอมใน Google Play Store

ข้อมูลจาก ThaiCERT เมื่อวันที่ 27 มีนาคม 2557 ได้เตือนว่ามีการพบแอปพลิเคชันธนาคารปลอมอยู่ใน Google Play Store โดยแอปพลิเคชันเหล่านี้พัฒนาโดย SCIENTIFIKA MEDIA

เมื่อเรียกใช้งานแอปพลิเคชันปลอม จะพบหน้าจอให้ใส่รหัสผ่านสำหรับเข้าใช้งานบัญชีธนาคารออนไลน์ ซึ่งเป็น Link ของธนาคารจริงๆ และมีโฆษณาอยู่ด้านล่างแอปพลิเคชัน

จากการตรวจสอบ Permission ที่แอปพลิเคชันร้องขอ พบว่าทั้ง 5 แอปพลิเคชันต้องการสิทธิ์ในการเชื่อมต่ออินเทอร์เน็ตและแสดงผล Ads เท่านั้น ซึ่งไม่มีการส่งข้อมูลหรือการขโมยข้อมูล วัตถุประสงค์ของผู้พัฒนาแอปพลิเคชันน่าจะเป็นการหารายได้จากการโฆษณาที่แสดงด้านล่างแอปพลิเคชันเท่านั้น

อย่างไรก็ตาม การใช้งานแอปพลิเคชันลักษณะนี้ในการทำธุรกรรมออนไลน์ถือว่ามีความเสี่ยง เนื่องจากผู้ใช้ไม่สามารถทราบได้ว่าแอปพลิเคชันที่ใช้งานอยู่นั้นมีการขโมยข้อมูลหรือไม่ หรือในอนาคตแอปพลิเคชันที่ในขณะนี้ไม่มีพฤติกรรมประสงค์ร้าย จะมีการอัปเดตตัวเองเพื่อให้มีความสามารถอื่นๆ ที่เป็นอันตรายเพิ่มขึ้นหรือไม่ ผู้ใช้งานจึงควรทำธุรกรรมออนไลน์ผ่านทางแอปพลิเคชันที่เป็นทางการของธนาคารเท่านั้น

แอปพลิเคชัน iMessage Chat อาจขโมยข้อมูลสำคัญ

ข้อมูลจาก ThaiCERT เมื่อวันที่ 24 กันยายน 2556 ได้เตือนเกี่ยวกับแอปพลิเคชัน iMessage Chat ที่ให้ดาวน์โหลดใน Google Play Store ซึ่งสามารถทำให้มือถือ Android คุยกับแอปพลิเคชัน iMessage ของไอโฟนได้ ซึ่งการใช้งานจะต้องใช้ Apple ID ในการใช้งาน

ThaiCERT ได้ตรวจสอบแอปพลิเคชันดังกล่าวแล้วพบว่า ไม่ได้ถูกพัฒนาขึ้นโดย Apple จึงได้ทดลองติดตั้งแอปพลิเคชันดังกล่าวลงในเครื่อง Galaxy Nexus ที่ใช้ Android 4.3 แล้วทดลองส่งข้อความไปยังเครื่อง iPad ที่ใช้ iOS 7.0 ผลการทดสอบพบว่าทั้ง 2 เครื่องสามารถส่งข้อความสนทนากันได้จริง

แอปพลิเคชันดังกล่าวนี้ร้องขอ Permission ที่น่าสงสัย ดังนี้ :

- ตรวจสอบสถานะและเชื่อมต่อกับระบบเครือข่าย
- ตรวจสอบสถานะการใช้งานโทรศัพท์
- แก้ไขหรือลบข้อมูลที่อยู่ใน SD Card
- ติดตั้ง Shortcut เพิ่มเติมในระบบ
- เข้าถึงข้อมูลในส่วนที่มีการสงวนสิทธิ์ (Protected Storage)
- เปิดใช้งานกล้อง ถ่ายภาพ บันทึกเสียง
- อ่านข้อมูลรายชื่อผู้ติดต่อและข้อมูลบันทึกการโทรล่าสุด

การอนุญาตให้แอปพลิเคชันเข้าถึงข้อมูลเหล่านี้ อาจถูกขโมยข้อมูลส่วนตัวได้ เช่น ขโมย Apple ID หรืออาจถูกดักข้อมูลการสนทนาใน iMessage นอกจากนี้ยังอาจถูกขโมยข้อมูลสำคัญ เช่น รายชื่อผู้ติดต่อ ภาพถ่าย วิดีโอคลิป ไฟล์ที่อยู่ใน SD Card หรือข้อมูลสำคัญอื่นๆ ที่อยู่ในเครื่องได้

แม้ว่าเมื่อวันที่ 25 กันยายน 2556 ทาง Google Play Store ได้ถอนแอปพลิเคชัน iMessage Chat ออกจากการให้บริการดาวน์โหลดแล้ว แต่ก็ยังมี .apk ให้ผู้ใช้ดาวน์โหลด ซึ่งเพื่อนๆ ไม่ควรติดตั้งแอปพลิเคชันที่มีความเสี่ยงเช่นนี้นะครับ

จากตัวอย่างที่พูดน้อยกล่าวมาทั้งหมด ไม่ว่าจะเป็นแอปพลิเคชันที่อยู่ใน Google Play Store หรือแอปพลิเคชันที่ติดตั้งโดยตรงจาก .apk ล้วนแล้วแต่มีความเสี่ยงในการถูกโจรกรรมข้อมูลทั้งนั้นครับ แต่แอปพลิเคชันที่อยู่ใน Google Play Store จะมีความปลอดภัยมากกว่า เพราะทาง Google ได้กรองมาแล้วขั้นหนึ่ง แต่ผู้ใช้ก็ต้องระวังอยู่ดี โดยผู้ใช้อาจตรวจสอบแอปพลิเคชันที่น่าสงสัยได้โดยวิธีการดังต่อไปนี้

1. ตรวจสอบจากจำนวนดาวน์โหลด และรีวิวของผู้ใช้งาน โดยสังเกตแอปพลิเคชันที่มียอดดาวน์โหลดที่ต่ำหรือรีวิวของผู้ใช้งานที่แจ้งถึงความผิดปกติ

2. ตรวจสอบการร้องขอสิทธิ์ (Permission) ของแอปพลิเคชันว่ามีความเหมาะสมหรือไม่ เช่น แอปพลิเคชันที่มีการขอสิทธิ์ในการส่ง SMS และ Internet Access ควรพิจารณาว่ามีการร้องขอสิทธิ์ดังกล่าวเพื่อจุดประสงค์ใด

3. ตรวจสอบจากชื่อ Developer หากเป็นแอปพลิเคชันของธนาคารผู้พัฒนาจะต้องเป็นชื่อของธนาคารนั้นๆ

4. ไม่ควรติดตั้งแอปพลิเคชัน .apk ที่ถูกส่งผ่าน SMS หรือโปรแกรมแชต หรืออีเมล หรือผ่านเว็บไซต์ที่ให้ดาวน์โหลด .apk

ช้อปปิ้งออนไลน์ มีดี มีร้าย
"เช็กข้อมูลผู้ขายให้ละเอียด"
ท่องจำให้ขึ้นใจ

5.6 Online Shopping
ช้อปง่าย สบายใจ แต่ต้องรู้จักระวังตัว

ปัจจุบันคนไทยนิยมซื้อสินค้าผ่านช่องทางออนไลน์กันมากขึ้น เรียกว่าใน 1 ปี มีเงินหมุนอยู่ในระบบจำนวนมาก ประเทศไทยมีมูลค่าอีคอมเมิร์ซทั้งสิ้น 2,245,147.02 ล้านบาท จากผลสำรวจมูลค่าพาณิชย์อิเล็กทรอนิกส์ไทยปี 2558 โดย ETDA ซึ่งมูลค่าสูงนี้ถือเป็นเรื่องดีกับเศรษฐกิจของประเทศไทย แต่สำหรับนักช้อปทั้งหลาย พุดน้อยก็อยากจะให้ข้อสังเกตในการช้อปอย่างระมัดระวังตัว ซึ่งจะช่วยสร้างความมั่นคงปลอดภัยให้กับทุกคนเอง โดยสามารถปฏิบัติได้ ดังนี้

6 ข้อสังเกต ซื้อสินค้าผ่านช่องทางออนไลน์ให้มั่นใจ

1. อย่าเห็นแก่ของถูก รู้ว่าเขาหลอก อย่าให้เขาหลอก : เวลาค้นหาสินค้าในช่องทางออนไลน์ หากเจอสินค้าที่ราคาต่ำกว่าท้องตลาดมากเสียจนผิดสังเกต เพื่อนๆ ต้องรู้จักตรวจสอบข้อมูลผู้ขายให้ละเอียดเสียก่อน เช่น ชื่อจริง นามสกุลจริง เลขบัญชีธนาคาร ฯลฯ สามารถค้นหาได้ผ่านเว็บเสิร์ชเอนจิน เพราะบางทีอาจพบข้อมูลดีๆ มีผู้ซื้อรายอื่นๆ มาบ่นว่าถูกโกงจากผู้ขายรายนี้ก็เป็นได้ ดังนั้นอย่าคิดแต่ต้องการจะได้ของถูกเพราะแท้ที่จริงแล้วอาจเป็นกลอุบายของผู้ร้าย เพื่อโน้มน้าวให้เราอยากซื้อสินค้า

2. ของถูกใช่ว่าจะดีเสมอไป : บางครั้งการได้สินค้าราคาถูกมาไว้ในครอบครองเพื่อนหลายคนอาจจะรู้สึกภูมิใจในความสามารถในด้านการหาของถูกของตนเอง แต่หารู้ไม่ว่า สินค้าที่เราเห็นเพียงแค่รูปภาพหรือข้อความสั้นๆ ผ่านช่องทางออนไลน์ พอส่งมาถึงมือเรา อาจจะเป็นของที่มีตำหนิหรือชำรุดบุบสลาย หรืออาจเป็นของปลอมก็เป็นได้ เพราะฉะนั้น ควรที่จะสอบถามถึงรายละเอียดของสินค้าจากผู้ขายให้ละเอียดว่าสินค้าเป็นอย่างไร อยู่ในสภาพกี่เปอร์เซ็นต์ เพื่อใช้เป็นหลักฐานยืนยันในภายหลัง

3. หัดซื้อทีละน้อย แต่มั่นคงปลอดภัย : ข้อนี้ พุดน้อยเตือนไว้สำหรับเพื่อนๆ ที่เป็นนักช้อปมือใหม่ อยากให้ลองสั่งซื้อสินค้าในราคาที่ไม่แพง และจำนวนที่ไม่มากนักกับผู้ขายออนไลน์ก่อน และเมื่อซื้อสินค้ากันไปจนมั่นใจ จึงค่อยๆ ขยับขึ้นไปซื้อสินค้าที่มีราคาสูงขึ้น เพราะหากเป็นผู้ร้ายแฝงตัวมาเป็นพ่อค้าออนไลน์ คนเหล่านี้จะมีความต้องการให้เราสั่งสินค้าจำนวนมากและแสนแพง เพื่อกินอร่อยเรียบในทีเดียว

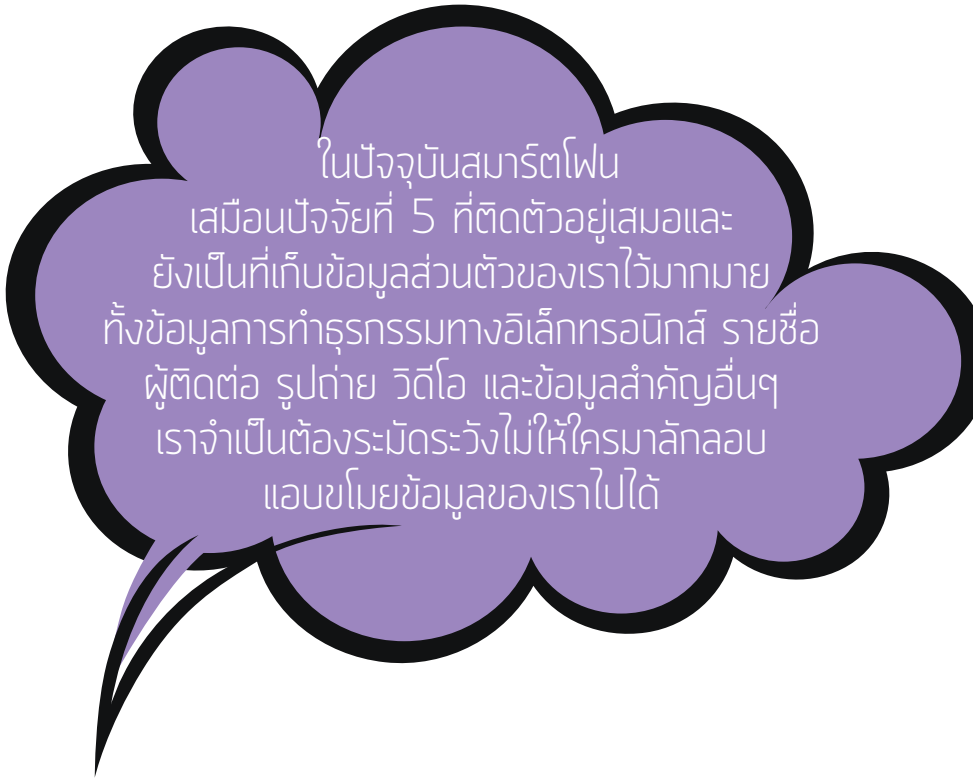
4. เช็กความเคลื่อนไหว อย่าเชื่อในสิ่งที่เห็นด้วยตาเสมอไป : โลกออนไลน์นั้นก็มีทั้งคนดีและคนไม่ดี ไม่ต่างจากโลกจริงเท่าใดนัก แต่โลกออนไลน์จะต้องเพิ่มความระวังมากกว่านิด ตรงที่ผู้ขายสินค้าบางคนอาจมีได้มากกว่า 1 ตัวตน หรือ 1 Account ดังนั้น การจะเป็นนักช้อปออนไลน์ที่มีสกิลขั้นเทพ จะต้องรู้จักขอ Account จริงๆ ที่เราสามารถเห็นพฤติกรรมความเคลื่อนไหว มีการอัปเดตเป็นประจำ มีการเปลี่ยนแปลงโปรโมชันและกลุ่มเพื่อนหมุนเวียนกันมาพูดคุยซื้อสินค้าอยู่ตลอด

5. เป็นเว็บไซต์จดทะเบียนการค้า : หากจะเอาให้ชัวร์ขึ้นไปอีก เราก็ควรซื้อสินค้าจากเว็บไซต์หรือผู้ขายที่มีการจดทะเบียนกับกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ซึ่งสามารถตรวจสอบได้ที่ http://www.dbd.go.th/edirectory

6. จ่ายแบบบัตรเครดิต หรือชำระผ่านระบบชำระเงินออนไลน์ เพิ่มความเซฟตี้ มีความมั่นคงปลอดภัย : เพื่อนๆ หลายคน มักใช้วิธีจ่ายเงินให้ร้านค้าออนไลน์ด้วยการโอนเงิน ซึ่งหากมีปัญหาในการซื้อขาย ส่วนใหญ่มักจะไม่ได้รับเงินคืน การชำระด้วยบัตรเครดิตหรือผ่านระบบชำระเงินออนไลน์ที่ร้านค้านั้นรองรับ หากมีปัญหาเรายังสามารถแจ้งระงับสตางค์ที่กำลังจะเสียไปได้

บทที่ 6

ความเป็นส่วนตัว ที่อยู่ในมือคุณ



สมาร์ตโฟนไม่ได้เป็นเพียงแค่เครื่องมือในการติดต่อสื่อสารที่ใช้โทรศัพท์หรือส่งข้อความเท่านั้น ยังเป็นทั้งกล้องถ่ายรูป กล้องถ่ายวิดีโอ เครื่องมือเข้าใช้งานอินเทอร์เน็ต รวมถึงเป็นกระเป๋าสตางค์ เป็นธนาคารออนไลน์อีกด้วย ซึ่งหากมีใครหยิบโทรศัพท์เราไป และเข้าใช้งานแอปพลิเคชันต่างๆ เช่น อีเมล หรือโพสต์ข้อความในโซเชียลเน็ตเวิร์กในชื่อของเราได้ และอาจถูกขโมยบัญชีผู้ใช้งานไม่ว่าจะเป็นอีเมล โซเชียลเน็ตเวิร์ก หรือแม้แต่เข้าถึงบัญชีอินเทอร์เน็ตแบงก์กิ้ง

สมาร์ตโฟนเป็นอุปกรณ์ส่วนตัว ดังนั้น เราควรตั้งรหัสล็อกหน้าจอ เพื่อไม่ให้ใครสามารถใช้งานโทรศัพท์ของเราได้โดยที่เราไม่อนุญาตและหากจะต้องส่งโทรศัพท์ซ่อมหรือขายต่อ เราต้องลบข้อมูลและการตั้งค่าทั้งหมดก่อนเสมอ เราควรศึกษาการใช้งานโหมดสูญหายเพื่อตั้งค่าการใช้งานกรณีเครื่องหาย ซึ่งเราจะสามารถล็อกเครื่องได้ สามารถที่จะสั่งให้ลบข้อมูลในมือถือทางคอมพิวเตอร์ได้ ควรบันทึกหมายเลข IMEI 15 หลักไว้ เพื่อใช้สำหรับแจ้งความและติดตามการใช้งานของมือถือ

การตั้งรหัสล็อกหน้าจอ

การใช้งานโหมดสูญหาย
เพื่อติดตามตำแหน่งโทรศัพท์

ในโลกออนไลน์ผู้ใช้งานอินเทอร์เน็ต จะสามารถถูกติดตาม (Tracking) ได้ตลอดเวลา ไม่ว่าจะเป็นตำแหน่งที่ใช้งาน พฤติกรรมการท่องเว็บไซต์ และอื่นๆ

6.1 ใช้อินเทอร์เน็ตบนมือถือให้เป็นส่วนตัว

ในโลกของความเป็นจริงข้อมูลส่วนต่างๆ ของเราจะไม่เปิดเผยได้ง่าย เช่น ข้อมูลอายุ ที่อยู่ สถานะครอบครัว แต่ในโลกออนไลน์ เราถูกติดตามอยู่ตลอดเวลา ทั้งจากผู้ให้บริการเว็บไซต์ เพื่อนในโซเชียลเน็ตเวิร์ก ซึ่งหากเราไม่ระวังอาจเป็นเหยื่อให้กับผู้ไม่หวังดีได้ ดังนั้น เราจำเป็นต้องรู้จักตั้งค่าความเป็นส่วนตัวเมื่อเราใช้งานโมบายอินเทอร์เน็ต

ปิดการแสดงตำแหน่ง

แอปพลิเคชันหลายตัวจำเป็นต้องใช้ข้อมูลพิกัดตำแหน่งที่เราอยู่ เช่น แอปพลิเคชันแผนที่จะต้องรู้ตำแหน่งของเราเพื่อบอกเส้นทาง แอปพลิเคชันคูปองจะขอตำแหน่งของเราเพื่อใช้หาร้านค้าที่มีข้อเสนอใกล้ๆ กับตำแหน่งของเรา ซึ่งเป็นประโยชน์กับเรา

แต่บางครั้งถ้าเราไม่ต้องการเปิดเผยที่อยู่ของเราให้คนอื่นทราบ เราจำเป็นต้องปิดการแสดงตำแหน่งสำหรับแอปพลิเคชันเหล่านั้น เช่น แอปพลิเคชันแชตจะแสดงตำแหน่งของเราขณะแชต ทำให้คนที่แชตกับเรารู้ว่าเราอยู่ที่ไหน แอปพลิเคชันโซเชียลเน็ตเวิร์กจะแสดงตำแหน่งที่อยู่ของเราขณะที่โพสต์โดยเราไม่ต้องเช็กอิน ซึ่งอาจทำให้คนอื่นสามารถติดตามเราได้

การปิดการแสดงตำแหน่งสามารถทำได้ โดยไปที่ การตั้งค่า -> ความเป็นส่วนตัว ->การเข้าถึงตำแหน่ง แล้วเลือกเปิด/ปิดการเข้าถึงตำแหน่งในแต่ละแอปพลิเคชันได้

การปิดการแสดงตำแหน่ง

การตั้งค่าความเป็นส่วนตัว

การใช้ Browser ให้เป็นส่วนตัว

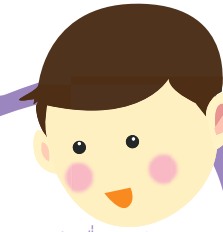
สำหรับการใช้งาน Browser เพื่อเยี่ยมชมเว็บไซต์ เจ้าของเว็บไซต์สามารถติดตามสะกดรอย เก็บสถิติ เก็บพฤติกรรมการท่องเว็บไซต์ของเรา ซึ่งจะทำให้เว็บไซต์เหล่านั้นสามารถนำเสนอโฆษณาเฉพาะบุคคล จากประวัติการท่องเว็บไซต์ของเราได้

เราสามารถตั้งค่าให้ไม่สามารถติดตามได้ โดยไปที่ การตั้งค่า -> ความเป็นส่วนตัว -> ไม่ต้องติดตาม (Do Not Track) ซึ่งจะเป็นการระบุว่าคุณไม่ต้องการให้มีการติดตามการเรียกดูของเรา แต่ก็ขึ้นอยู่กับนโยบายด้านความเป็นส่วนตัวของแต่ละเว็บไซต์ว่าจะดำเนินการตามที่เราร้องขอหรือไม่

ความเป็นส่วนตัวในโซเชียลเน็ตเวิร์ก

การใช้งานโซเชียลเน็ตเวิร์กเราจำเป็นต้องตั้งค่าความเป็นส่วนตัว เพื่อไม่ให้ข้อมูล หรือกิจกรรมที่เราแชร์เผยแพร่ไปยังคนที่ไม่พึงประสงค์ ดังนั้น เราควรตั้งค่าให้เพื่อนเท่านั้นที่เห็นกิจกรรมของเรา และหลีกเลี่ยงการตั้งค่าสิ่งที่เราทำให้เป็นสาธารณะ หรือคนทั่วไปเห็นได้ เราควรตั้งค่าให้ซ่อนข้อมูลส่วนตัว เช่น วันเกิด เบอร์โทรศัพท์ ที่อยู่ ข้อมูลครอบครัว ให้ดูได้เฉพาะเราเท่านั้น เพราะมิจฉาชีพอาจนำข้อมูลเหล่านี้ปลอมไปทำธุรกรรมทางการเงิน หรือนำไปหลอกลวงผู้อื่นได้

นอกจากการตั้งค่าแล้ว เราต้องระวังเรื่องการโพสต์ด้วย เราไม่ควรโพสต์แชร์สถานที่ โดยเฉพาะตำแหน่งของบ้าน เพราะเราอาจถูกสะกดรอยจากผู้ไม่หวังดีได้ เราไม่ควรแสดงข้อมูลส่วนตัวที่เป็นความลับ เช่น บัตรประจำตัวประชาชน บัตรเครดิตลงในโซเชียลเน็ตเวิร์ก ไม่ว่าจะอยู่ในรูปแบบข้อความ หรือรูปภาพ เพราะแฮกเกอร์และผู้ไม่หวังดีสามารถแฝงตัวมากับกลุ่มเพื่อนที่เราอนุญาตให้เข้าชมได้



น้องพุดดิ้งชวนรู้

ทำอย่างไรเมื่อโทรศัพท์มือถือหาย

1. โทรติดต่อไปยังผู้ให้บริการโทรศัพท์มือถือที่ตนเองใช้บริการอยู่ เพื่อระงับการใช้งานหมายเลขของเรา

2. หากมีการตั้งค่าเปิดการใช้งานการค้นหาโทรศัพท์มือถือ ให้ไปที่เว็บไซต์หรือแอปพลิเคชันสำหรับค้นหาโทรศัพท์มือถือตามระบบปฏิบัติการที่เราใช้งานอยู่ โดยเว็บไซต์สามารถแสดงตำแหน่งปัจจุบันของเครื่องหากเครื่องออนไลน์อยู่ หรือตำแหน่งสุดท้ายหากมีการปิดเครื่อง ซึ่งเราสามารถสั่งล็อกเครื่องหรือลบข้อมูลในเครื่องได้อีกด้วย

3. ไปทำเรื่องแจ้งความที่สถานีตำรวจ แจ้งหมายเลข IMEI แล้วให้ทางผู้ให้บริการโทรศัพท์มือถือดำเนินการตรวจสอบหมายเลข IMEI ที่หายไปว่ามีการโทรออกโดยใช้มือถือหมายเลข IMEI ที่หายหรือไม่ ซึ่งทันทีที่หาเจอโอเปอเรเตอร์ที่พบ IMEI นี้จะรายงานให้เราทราบได้

วิธีการเช็กหมายเลข IMEI ของโทรศัพท์มือถือ

หมายเลข IMEI คือ รหัสประจำตัวเครื่องโทรศัพท์ เราสามารถเช็กหมายเลข IMEI ได้ด้วยการกดแป้น *#06# จะมีตัวเลข 15 หลักปรากฏขึ้นมา วิธีการเช็กหมายเลข IMEI มีอีกหลายวิธี ดังนี้

1. อยู่ที่ถาดใส่ซิมหรือช่องใส่แบตเตอรี่หรือด้านหลังเครื่อง หรือตำแหน่งอื่นๆ แล้วแต่รุ่น/ยี่ห้อของโทรศัพท์

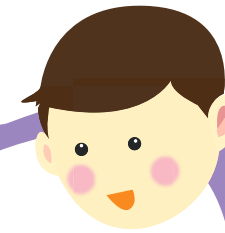
2. ดูที่การตั้งค่าโทรศัพท์

- **iOS** ไปที่ Settings > General > About
- **Android** ไปที่ Settings > About Device > Status > IMEI
- **Windows** ไปที่ Settings > About

3. เช็กที่เว็บไซต์ www.google.com/settings/dashboard สำหรับระบบปฏิบัติการ Android จากนั้น Login ด้วยบัญชี Google แล้วเลือกในส่วน Android จะเห็นเลข IMEI เครื่องที่คุณใช้

4. สำหรับ iOS สามารถใช้ iTunes บนคอมพิวเตอร์ โดยไปที่การตั้งค่าบน PC ให้ไปที่แก้ไข -> การตั้งค่า จากนั้นคลิกแท็บอุปกรณ์ และวางเมาส์ค้างไว้เหนือข้อมูลสำรองของอุปกรณ์ iOS เพื่อดูหมายเลขประจำเครื่อง

5. ดูจากหมายเลขข้างกล่องโทรศัพท์มือถือ หรือใบเสร็จรับเงิน



การตั้งค่าเปิดใช้งานการค้นหาโทรศัพท์มือถือ

เมื่อซื้อโทรศัพท์มือถือใหม่ นอกจากที่จะต้องจดหมายเลข IMEI ไว้แล้ว เรายังต้องตั้งค่าโทรศัพท์ตามแต่ละระบบปฏิบัติการต่างๆ ดังนี้

1. **iOS** ไปที่ Settings > iCloud > Find My iPhone เพื่อเปิดใช้งาน Find My iPhone และ Send Last Location

2. **Android** ไปที่ System Setting > Security > Device Administrators เพื่อเปิดใช้งาน Android Device Manager

3. **Windows** ไปที่ Setting > Find My Phone เพื่อเปิดการใช้งาน Find My Phone

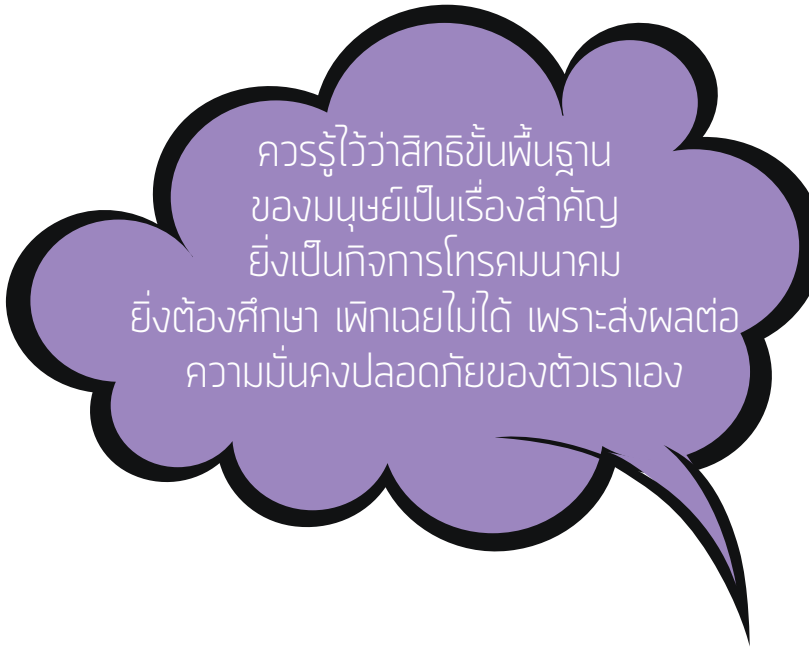
การใช้งานเว็บไซต์แอปพลิเคชันค้นหาโทรศัพท์มือถือ

1. ไปที่เว็บไซต์หรือแอปพลิเคชันของแต่ละระบบปฏิบัติการ

- **iOS** ให้ไปที่ www.icloud.com/#find หรือแอปพลิเคชัน Find My iPhone
- **Android** ให้ไปที่ www.google.com/android/devicemanager หรือแอปพลิเคชัน Google Device Manager
- **Windows** ให้ไปที่ WindowsPhone.com หรือ account.microsoft.com/devices

2. เราจะเห็นตำแหน่งล่าสุดของโทรศัพท์ของเราบนแผนที่

3. เราสามารถสั่งให้เครื่องส่งเสียงหรือล็อกเครื่อง หรือลบข้อมูลจากเครื่องได้



6.2 สิทธิขั้นพื้นฐานของผู้บริโภคในกิจการโทรคมนาคม 39 ประการ

สำนักงาน กสทช. ได้กำหนดสิทธิขั้นพื้นฐานของผู้บริโภคในกิจการโทรคมนาคมไว้ 39 ประการ เพื่อป้องกันการถูกเอาเปรียบจากผู้ให้บริการโทรศัพท์มือถือไว้ดังนี้

1. ผู้บริโภคต้องได้รับข้อมูลรายละเอียดของบริการและเงื่อนไขอย่างชัดเจนเพื่อการตัดสินใจเลือกและตกลงทำสัญญา

2. บริษัทต้องทำสำเนาสัญญามอบให้ผู้บริโภค

3. ห้ามบริษัทเลือกปฏิบัติ แบ่งแยก หรือกีดกันผู้บริโภครายหนึ่งรายใด

4. บริษัทต้องเรียกเก็บค่าบริการในอัตราเท่ากันสำหรับบริการลักษณะเดียวกันหรือประเภทเดียวกัน

5. บริษัทไม่มีสิทธิ์เปลี่ยนโปรโมชันก่อนหมดเวลาและโดยผู้บริโภคไม่ยินยอม

6. บริษัทจะขอข้อมูลส่วนบุคคลเกินจำเป็นไม่ได้

7. บริษัทไม่มีสิทธิ์นำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้ประโยชน์ และไม่มีสิทธิ์เปิดเผยข้อมูลการใช้บริการแก่ผู้อื่น

8. หลังยกเลิกสัญญาแล้ว บริษัทต้องเก็บข้อมูลส่วนบุคคลของผู้บริโภคไว้ 3 เดือน ยกเว้นมีเหตุจำเป็น ให้เก็บไม่เกิน 2 ปี หรือตามที่กฎหมายกำหนด

9. ผู้บริโภคมีสิทธิ์ขอดู ขอสำเนา แก้ไข ระงับการเปิดเผย หรือห้ามการประมวลผลข้อมูลส่วนบุคคลของตนเองได้

10. ผู้บริโภคมีสิทธิ์ขอทราบข้อมูลการใช้บริการของตนเองได้

11. บริษัทต้องจัดให้มีมาตรการป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

12. บริษัทต้องจัดให้มีระบบป้องกันการดักฟัง ตรวจ กักสัญญาณ หรือเปิดเผยข้อมูลที่สื่อสารกัน หรือทำให้ความหมายของข้อมูลเปลี่ยนแปลงไป

13. ผู้บริโภคต้องได้รับบริการที่มีคุณภาพตามที่บริษัทโฆษณาได้แจ้งไว้ มิเช่นนั้นบริษัทต้องเยียวยาความเสียหายอย่างเป็นธรรม

14. ห้ามบริษัทเก็บค่าบริการในช่วงที่เกิดเหตุขัดข้องเว้นแต่เหตุนั้นเกิดจากผู้บริโภค

15. ห้ามบริษัทเรียกเก็บค่าใช้จ่ายอื่นใดนอกจากที่กำหนดในสัญญา และห้ามเรียกเก็บเงินในลักษณะการวางเงินประกัน

16. ห้ามบริษัทเรียกเก็บค่าบริการล่วงหน้า เว้นแต่ได้รับอนุญาตจาก กสทช.

17. ห้ามกำหนดระยะเวลาใช้งานของเงินเติมล่วงหน้า (Prepaid) เว้นแต่ได้รับอนุญาตจาก กสทช.

18. เมื่อผู้บริโภคแจ้งว่ามีการคิดค่าบริการผิดพลาด บริษัทต้องพิสูจน์ความถูกต้องและแจ้งข้อมูลกลับโดยเร็ว หากเกิน 60 วันจะไม่มีสิทธิ์เรียกเก็บเงินจากจำนวนที่ถูกโต้แย้ง

19. หากมีการคิดค่าบริการผิดจริงบริษัทต้องคืนเงินส่วนต่างให้ผู้บริโภคภายใน 30 วัน หากเกินกำหนดต้องเสียดอกเบี้ยด้วย

20. ผู้บริโภคมีสิทธิ์แจ้งระงับการใช้บริการชั่วคราวได้ฟรีโดยแจ้งบริษัทล่วงหน้า 3 วัน และเมื่อครบกำหนดแล้วบริษัทต้องเปิดบริการโดยไม่คิดค่าใช้จ่าย

21. หากผู้บริโภคระงับบริการเกินกว่าระยะเวลาขั้นสูงที่บริษัทกำหนด บริษัทมีสิทธิ์ยกเลิกบริการโดยแจ้งเป็นหนังสือให้ทราบล่วงหน้าอย่างน้อย 30 วัน

22. ห้ามบริษัทระงับบริการเมื่อผู้บริโภคค้างชำระค่าบริการน้อยกว่า 2 รอบการเรียกเก็บ

23. กรณีถูกระงับบริการผู้บริโภคมีสิทธิ์ขอเปิดใช้บริการใหม่โดยไม่เสียค่าใช้จ่าย

24. ผู้บริโภคมีสิทธิ์ยกเลิกสัญญาเมื่อไหร่ก็ได้ด้วยการแจ้งเป็นหนังสือไปยังบริษัทล่วงหน้าอย่างน้อย 5 วันทำการ

25. กรณีบริษัททำผิดสัญญาบริการ ผู้บริโภคมีสิทธิ์บอกเลิกสัญญาทันที

26. ห้ามบริษัทเรียกค่าปรับจากการยกเลิกสัญญาของผู้บริโภค แม้ในกรณีที่มีการขายอุปกรณ์พ่วงบริการและทำสัญญาแบบกำหนดระยะเวลาขั้นต่ำไว้ แต่ผู้บริโภคต้องคืนหรือจ่ายค่าเครื่องอุปกรณ์นั้นให้บริษัทในราคาไม่เกินราคาตลาด

27. เมื่อสัญญาเลิกกันบริษัทต้องคืนเงินที่ค้างชำระหรือเงินคงเหลือจากการชำระล่วงหน้าให้ผู้บริโภค

28. ผู้บริโภคมีสิทธิ์เปลี่ยนเครือข่ายผู้ให้บริการโทรศัพท์มือถือโดยยังคงใช้เลขหมายเดิม

29. เมื่อใช้โทรศัพท์มือถือโทรไปยังเลขหมายเครือข่ายเดียวกัน การเรียกสายสำเร็จต้องมากกว่า 90% และอัตราสายหลุดต้องไม่เกิน 2%

30. เมื่อใช้โทรศัพท์มือถือโทรไปยังเลขหมายต่างเครือข่ายกัน การเรียกสายสำเร็จต้องมากกว่า 85%

31. ผู้บริโภคสามารถแจ้งยกเลิก SMS ที่มีการส่งผ่านทางเครือข่ายผู้ให้บริการได้ที่ Call Center ของผู้ให้บริการ

32. เมื่อโทรหา Call Center ต้องรอสายไม่เกิน 60 วินาที

33. หลังสมัครใช้บริการโทรศัพท์บ้านต้องใช้บริการได้ภายใน 10 วันทำการ

34. หลังแจ้งซ่อมแซมโทรศัพท์บ้านและโทรศัพท์สาธารณะ ต้องมีการดำเนินการภายใน 24 ชั่วโมง

35. ต้องมีการจัดโทรศัพท์สาธารณะให้บริการอย่างน้อย 2 เลขหมายต่อหมู่บ้าน 6,000 แห่งทั่วประเทศ

36. ต้องมีการจัดโทรศัพท์สาธารณะและโทรศัพท์พื้นฐานให้บริการในสถานศึกษา ศาสนสถาน สถานพยาบาล และหน่วยงานที่ทำงานเพื่อสังคม 4,000 แห่ง

37. หากจัดตั้งสถานีวิทยุคมนาคม (เสาสัญญาณฯ) บริษัทต้องทำความเข้าใจกับประชาชนในพื้นที่ก่อน

38. บริษัทต้องติดตั้งป้ายเครื่องหมายการค้า เบอร์ติดต่อ รวมถึงป้ายเตือนในบริเวณที่ตั้งเสาสัญญาณฯ

39. ผู้บริโภคสามารถร้องเรียนปัญหาการใช้บริการไปยังผู้ให้บริการและหน่วยงานกำกับดูแลได้

ที่มา : มือถือในมือเด็ก ฉบับการ์ตูน

http://tcp.nbtc.go.th/website/home/ebook/556

น้องพุดดิ้งชวนรู้

การร้องเรียนหากถูกละเมิดสิทธิ์

สามารถร้องเรียนกับทาง กสทช. ได้ทางอีเมล tcp.service@nbtc.go.th หรือ tcp.service@hotmail.com หรือโทร 1200 กด 1 (โทรฟรี) และสามารถดูรายละเอียดเพิ่มเติมได้ที่ http://tcp.nbtc.go.th

ภาคผนวก

คำศัพท์น่ารู้

1. **Application (แอปพลิเคชัน) :** โปรแกรมประยุกต์ที่ได้รับการออกแบบให้ทำงานกับสมาร์ตโฟนหรือแท็บเล็ต ซึ่งมีโปรแกรมให้เลือกหลายๆ ประเภท เช่น ประเภทสร้างความบันเทิง การศึกษา สุขภาพ ถ่ายภาพ ฯลฯ
2. **App Store (แอปสโตร์) :** คือร้านขายแอปพลิเคชัน สร้างขึ้นมาเพื่อให้เราสามารถซื้อหรือดาวน์โหลดและติดตั้งแอปพลิเคชันลงในโทรศัพท์มือถือของเราได้ มีทั้งแบบฟรีและจ่ายเงินซื้อ โดยแต่ละระบบปฏิบัติการจะมีร้านค้าแอปพลิเคชันของตนเอง โดย iOS จะเรียกว่า “App Store” ส่วน Android จะเรียกว่า “Play Store” และ Windows เรียกว่า “Windows Store”
3. **Blog (บล็อก) :** เป็นคำรวมมาจากคำว่า เว็บล็อก (weblog) เป็นรูปแบบเว็บไซต์ประเภทหนึ่ง จะเขียนขึ้นในลำดับที่เรียงตามเวลาในการเขียน โดยแสดงข้อมูลที่เขียนล่าสุดไว้แรกสุด บล็อกโดยปกติจะประกอบด้วย ข้อความ ภาพ ลิงก์ ซึ่งบางครั้งจะรวมสื่อต่างๆ ไม่ว่าจะเป็นเพลง หรือวิดีโอในหลายรูปแบบได้ จุดที่แตกต่างของบล็อกกับเว็บไซต์โดยปกติคือ บล็อกจะเปิดให้ผู้เข้ามาอ่านข้อมูล สามารถแสดงความคิดเห็นต่อท้ายข้อความที่เจ้าของบล็อกเป็นคนเขียน ทำให้ผู้เขียนสามารถได้ผลตอบกลับโดยทันที คำว่า “บล็อก” ยังใช้เป็นคำกริยาได้หมายถึง การเขียนบล็อก และนอกจากนี้ผู้ที่เขียนบล็อกเป็นอาชีพก็จะเรียกว่า “บล็อกเกอร์”
4. **Contact smart card (คอนแทค สมาร์ตการ์ด) :** สมาร์ตการ์ดแบบสัมผัสเป็นบัตรที่มีการฝังชิปใต้หน้าสัมผัสที่เป็นแผ่นโลหะสีทองขนาดเล็ก มีเส้นผ่านศูนย์กลางประมาณครึ่งนิ้วที่ด้านหน้าของบัตร ตอนใช้งานต้องสอดบัตรเข้าในเครื่องอ่านให้หน้าสัมผัสของบัตรได้แตะกับหน้าสัมผัสภายในเครื่องอ่านบัตร ส่วนใหญ่จะเป็นกับบัตรเครดิตหรือบัตรเอทีเอ็ม ปัจจุบันประเทศไทยได้ใช้สมาร์ตการ์ดชนิดนี้ทำบัตรประจำตัวประชาชนหรือซิมการ์ดของโทรศัพท์มือถือ

5. **Contactless smart card (คอนแทคเลส สมาร์ตการ์ด) :** สมาร์ตการ์ดแบบไร้สัมผัส เป็นบัตรที่มีการฝังชิปและขดลวดสายอากาศเอาไว้ภายในอาจมองด้วยตาเปล่าไม่เห็น สามารถติดต่อกับเครื่องอ่านบัตรที่รับส่งสัญญาณผ่านคลื่นวิทยุได้ในระยะที่กำหนด ซึ่งอาจเป็นระยะที่ใกล้ชิด (Proximity Card) หรือระยะที่ใกล้เคียง (Vicinity Card) แล้วแต่มาตรฐานของบัตร โดยไม่จำเป็นต้องให้บัตรสัมผัสกับเครื่องอ่านดังกล่าว ส่วนใหญ่จะใช้กับบัตรเก็บเงินทางด่วน บัตรโดยสารของรถไฟฟ้าบีทีเอส และรถไฟฟ้าใต้ดิน และบัตรชำระเงินย่อย เช่น บัตร Smart Purse เป็นต้น

6. **CPU (ซีพียู) :** คือหน่วยประมวลผลกลาง เป็นสมองกลของสมาร์ตโฟน แท็บเล็ต และแฟบเล็ต ซีพียูมีหลายประเภท ทั้งแบบ Single Core, Dual Core, Quad Core ซึ่งเป็นจำนวนแกนสมองเปรียบเสมือนมีคนทำงานเพิ่มตามจำนวน Core ที่เพิ่มขึ้นมา ยิ่งจำนวนของแกนสมองมีมากเท่าไหร่ ยิ่งส่งผลให้การประมวลของสมาร์ตโฟนมีประสิทธิภาพมากขึ้นเท่านั้น นอกจากนี้ ความเร็วของ CPU ก็ยังเป็นตัวแปรสำคัญในการประมวลผล ยิ่งมีความเร็วมากเท่าไหร่ การประมวลผลของ CPU ก็ยิ่งตอบสนองการทำงานได้เร็วขึ้นเท่านั้น

7. **Fair Usage Policy (แฟร์ ยูเสจ โพลิซี) :** กฎเกณฑ์การใช้งานอินเทอร์เน็ตผ่านเครือข่ายโทรศัพท์เคลื่อนที่ กฎเกณฑ์นี้กำหนดขึ้นโดยผู้ให้บริการ เพื่อให้ผู้ใช้บริการมีโอกาสเข้าใช้งานอินเทอร์เน็ตผ่านเครือข่ายโทรศัพท์เคลื่อนที่ได้อย่างยุติธรรมและเท่าเทียมกัน

8. **GPS (จีพีเอส) :** ย่อมาจาก Global Positioning System คือระบบบอกตำแหน่งบนพื้นผิวโลก โดยอาศัยการคำนวณจากความถี่สัญญาณนาฬิกาที่ส่งมาจากดาวเทียมที่โคจรอยู่รอบโลกซึ่งมีตำแหน่งที่แน่นอน ทำให้ระบบนี้สามารถบอกตำแหน่ง ณ จุดที่สามารถรับสัญญาณได้ทั่วโลก โดยเครื่องรับสัญญาณจีพีเอสรุ่นใหม่ๆ จะสามารถคำนวณความเร็วและทิศทางนำมาใช้ร่วมกับโปรแกรมแผนที่ เพื่อใช้ในการนำทางได้

9. **Hashtag (แฮชแท็ก) :** คือคำที่ขึ้นต้นด้วยเครื่องหมาย “#” เพื่อใช้ในการจัดกลุ่มสิ่งที่เราโพสต์ เพื่อให้ผู้ใช้งานสื่อสังคมออนไลน์สามารถติดตามความสนใจเรื่องใดเรื่องหนึ่ง

10. **Location Based Service (โลเคชั่น เบส เซอร์วิส) :** เป็นการบริการบอกตำแหน่งทางภูมิศาสตร์ โดยใช้อุปกรณ์พกพา เช่น โทรศัพท์มือถือ แท็บเล็ต สมาร์ตโฟน หรืออุปกรณ์อื่นๆ สัญญาณเครือข่ายของผู้ให้บริการต่างๆ การให้บริการตำแหน่งที่อยู่นั้นต้องอาศัยอุปกรณ์เฉพาะในการเชื่อมต่อกับดาวเทียม เช่น เครื่องรับสัญญาณ GPS

11. **Mobile Banking (โมบายแบงก์กิ้ง) :** เป็นการพัฒนารูปแบบการให้บริการต่างๆ ของ Online Banking โดยออกแบบมาให้ใช้งานได้ง่ายๆ ผ่านอินเทอร์เน็ตเบราว์เซอร์บนมือถือหรือแอปพลิเคชันของแต่ละธนาคาร
12. **NFC (เอ็นเอฟซี) :** ย่อมาจาก Near Field Communication เป็นเทคโนโลยีการสื่อสารไร้สายผ่านคลื่นวิทยุที่ความถี่ 13.56 MHz ใช้ส่งข้อมูลได้ในระยะไม่เกิน 10 ซม. มีความเร็วในการรับส่งข้อมูลได้สูงสุด 424 kbit/s สามารถจับคู่อุปกรณ์ได้อย่างรวดเร็วและใช้พลังงานต่ำ จากข้อดีดังกล่าว NFC จึงมีการนำมาใช้ในการรับส่งข้อมูลปริมาณเล็กน้อยภายในระยะเวลาสั้นๆ ดังนั้น อุปกรณ์ที่สามารถใช้งาน NFC ได้สะดวกจึงเป็นอุปกรณ์พกพา เช่น โทรศัพท์มือถือหรือแท็บเล็ต ซึ่งสามารถใช้งานได้โดยการนำไปแตะหรือสัมผัสกับเครื่องอ่าน NFC หรืออุปกรณ์ที่มีความสามารถ NFC เหมือนกัน ตัวอย่างการใช้งาน NFC เช่น การจ่ายเงินผ่านโทรศัพท์มือถือ (Mobile Payment) การใช้แทนบัตรโดยสาร การใช้แทนบัตรเข้าตัวอาคาร การใช้ยืนยันตัวตนในการเชื่อมต่อ Bluetooth / Wi-Fi หรือการรับส่งข้อมูลที่มีขนาดไม่ใหญ่มาก เช่น รูปถ่าย เป็นต้น
13. **One Time Password : OTP (วัน ไทม์ พาสเวิร์ด : โอทีพี) :** คือรหัสผ่านที่ใช้ครั้งเดียวที่ส่งทาง SMS ให้ผู้ที่ทำธุรกรรมออนไลน์เพื่อการตรวจสอบและยืนยันตัวตน
14. **Phishing (ฟิชชิง) :** เป็นรูปแบบการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือ ข้อมูลส่วนบุคคลอื่นๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายด้านอื่นๆ โดยเฉพาะด้านการเงิน โดยคำว่า Phishing เป็นคำพ้องเสียงจากคำว่า Fishing ซึ่งหมายถึง การตกปลา โดยเปรียบเหมือนการใช้เหยื่อล่อในการตกปลานั่นเอง โดยวิธีการมักจะหลอกหลวงด้วยการปลอมอีเมล หรือปลอมหน้าเว็บไซต์ที่ทำให้หลงเชื่อ และกรอกข้อมูลในการล็อกอินเข้าระบบ ผู้ไม่หวังดีก็จะได้ชื่อผู้ใช้และรหัสผ่านไปทันที

15. **RAM (แรม) :** เป็นหน่วยความจำชั่วคราวในสมาร์ตโฟน มีหน้าที่พักข้อมูลสำหรับการคำนวณของเครื่องและเป็นพื้นที่ในการรันแอปพลิเคชันต่างๆ สมาร์ตโฟนที่มี RAM มาก เครื่องก็จะทำงานได้รวดเร็วและราบรื่น หากมี RAM น้อยก็อาจทำให้เครื่องเกิดอาการกระตุกได้ RAM จะมีการจองการใช้งานให้กับแอปพลิเคชันต่างๆ ที่เราเปิดขึ้นมา ซึ่งหากเปิดหลายๆ แอปพลิเคชันพร้อมกัน จะทำให้หน่วยความจำเหลือน้อยลงและเครื่องจะช้าหรือหยุดทำงานได้

16. **ROM (รอม) :** เป็นหน่วยความจำในสมาร์ตโฟนทำหน้าที่เสมือนฮาร์ดดิสก์ในคอมพิวเตอร์ เป็นพื้นที่ที่ใช้เก็บระบบปฏิบัติการ แอปพลิเคชัน และไฟล์ต่างๆ เช่น รูปถ่าย วิดีโอ เพลง เป็นต้น

17. **Secure Sockets Layer : SSL (ซีเคียว ซ็อกเก็ต เลเยอร์ : เอสเอสแอล) :** เป็นเทคโนโลยีที่พัฒนาขึ้นมาใช้จัดการกับภัยคุกคามทางอินเทอร์เน็ต ด้วยความสามารถในการเข้ารหัสลับข้อมูล (Encrypt) ก่อนที่จะส่งผ่านเครือข่ายไปถึงผู้รับปลายทาง เว็บไซต์ที่ใช้โพรโทคอล HTTPS จะเป็นเว็บไซต์ที่เข้ารหัสข้อมูลก่อนส่ง หากมีผู้ไม่หวังดีดักรับข้อมูลก็จะไม่สามารถเข้าใจข้อมูลนั้นได้ ซึ่งการที่จะใช้งานโพรโทคอล HTTPS ได้นั้น เครื่องให้บริการเว็บไซต์จะต้องทำการติดตั้งใบรับรองความปลอดภัยทางอิเล็กทรอนิกส์ (Certificate) เสียก่อน ซึ่งใบรับรองความปลอดภัยทางอิเล็กทรอนิกส์สามารถทำขึ้นเองหรือซื้อจากผู้ให้บริการรับรองที่น่าเชื่อถือ (Trusted certificate authority) ก็ได้ เพียงแต่ใบรับรองที่ทำขึ้นเองนั้น ป้องกันเว็บเบราว์เซอร์จะแจ้งเตือนความผิดปกติ เนื่องจากไม่มีผู้รับรองความน่าเชื่อถือ ทั้งนี้ใบรับรองจะเป็นตัวบ่งบอกความถูกต้องของข้อมูลที่เกี่ยวข้องกับเว็บไซต์นั้น เช่น การยืนยันความเป็นเจ้าของเว็บไซต์ ความสมบูรณ์ของการเข้ารหัสลับข้อมูล ช่วยเพิ่มความมั่นใจให้กับผู้ใช้งานขณะที่มีการรับ-ส่งข้อมูล

18. **Smart Card (สมาร์ตการ์ด) :** เป็นบัตรพลาสติกชนิดหนึ่ง มีขนาดเท่ากับบัตรเครดิตหรือบัตรเอทีเอ็ม แต่ต่างกันตรงที่มีการฝังชิปไว้ที่บนบัตรด้วย ซึ่งในตัวชิปนี้สามารถบันทึกข้อมูลทางอิเล็กทรอนิกส์ได้ และมีวิธีการรักษาความปลอดภัยเป็นอย่างดี

19. **Smartphone (สมาร์ตโฟน) :** คือโทรศัพท์มือถือที่มีความสามารถในการเชื่อมต่ออินเทอร์เน็ตและสามารถดาวน์โหลดแอปพลิเคชันติดตั้งเพิ่มเติมที่เครื่องได้ เสมือนกับคอมพิวเตอร์ขนาดเล็กที่เราสามารถพกพาไปไหนมาไหน เพื่อติดต่อข้อมูลและสื่อสารตลอดจนทำงานได้สะดวกในทุกที่ที่เราต้องการ

20. **Tablet (แท็บเล็ต) :** คืออุปกรณ์คอมพิวเตอร์ที่มีหน้าจอระบบสัมผัสขนาดใหญ่ ตั้งแต่ 7 นิ้วขึ้นไป พกพาได้สะดวก สามารถใช้งานหน้าจอผ่านการสัมผัส มีแอปพลิเคชันมากมายให้เลือกใช้ ข้อดีของแท็บเล็ตคือมีหน้าจอที่กว้าง ทำให้มีพื้นที่การใช้งานเยอะ มีน้ำหนักเบา พกพาได้สะดวกกว่าโน้ตบุ๊กหรือคอมพิวเตอร์ สามารถจดบันทึกหรือใช้เป็นอุปกรณ์เพื่อการศึกษาได้เป็นอย่างดี

21. **Phablet (แฟบเล็ต) :** เป็นคำที่เกิดจากคำ 2 คำคือ คำว่า Phone และ Tablet ที่เป็นการผสมผสานกันระหว่างโทรศัพท์มือถือและแท็บเล็ต โดยคำนิยามที่ดูจะใกล้เคียงที่สุดเวลานี้คือ “มือถือลูกผสมกับแท็บเล็ต” โดยโทรศัพท์มือถือประเภทนี้มีจุดเด่นคือมีหน้าจอขนาดใหญ่และใช้เป็นโทรศัพท์ได้อีกด้วย

22. **Voice over IP : VoIP (วอยซ์ โอเวอร์ ไอพี : วีโอไอพี) :** เป็นการสื่อสารทางเสียงผ่านโครงข่ายอินเทอร์เน็ต หรือโครงข่ายอื่นๆ ที่ใช้อินเทอร์เน็ตโพรโทคอล สัญญาณเสียงจะมีการตัดแบ่งเป็นแพ็กเกจวิ่งผ่านไปบนโครงข่ายที่ใช้สำหรับการสื่อสารข้อมูลทั่วไป แทนการใช้วงจรเฉพาะตามวิธีการสื่อสารในระบบโทรศัพท์แบบดั้งเดิม เปรียบได้กับการให้รถยนต์วิ่งแทรกกันได้ตามช่องว่างที่มีอยู่ของถนน แทนการให้รถยนต์คันเดียวจองถนนวิ่งแบบผูกขาด ข้อดีของวอยซ์ โอเวอร์ ไอพี ก็คือการสามารถใช้โครงข่ายได้อย่างมีประสิทธิภาพ ทำให้สามารถให้บริการได้ในอัตราค่าบริการที่ถูกลงมา

หน้าที่ของผู้ให้บริการที่เกี่ยวข้องกับโทรศัพท์มือถือ

เพื่อประโยชน์แก่ผู้ใช้บริการที่เกี่ยวข้องกับโทรศัพท์มือถือ สำนักรับเรื่องร้องเรียนและคุ้มครองผู้บริโภคในกิจการโทรคมนาคม (รท.) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ได้ระบุสิทธิในการร้องเรียน กรณี “การร้องเรียนต่อผู้ให้บริการโดยตรง” 5 ประการ ดังนี้

1. กรณีที่ผู้บริโภคได้รับความเสียหายยื่นเรื่องร้องเรียนต่อผู้ให้บริการ ผู้ให้บริการต้องออกหนังสือแจ้งการรับเรื่องร้องเรียน พร้อมแจ้งสิทธิให้ผู้ร้องเรียนทราบภายใน 7 วัน
2. ถ้าผู้ให้บริการตรวจเรื่องร้องเรียน ปรากฏว่าเรื่องร้องเรียนไม่มีมูล ผู้ให้บริการต้องทำหนังสือแจ้งให้กับผู้ร้องเรียนทราบภายใน 14 วัน พร้อมแสดงเหตุผลที่ไม่รับพิจารณาเรื่องร้องเรียน และแจ้งสิทธิในการร้องเรียนต่อ กสทช. และหน่วยงานอื่น โดยระบุสถานที่ติดต่อและเลขหมายโทรศัพท์ของหน่วยงานนั้นๆ ให้ทราบโดยชัดเจน
3. แต่หากผู้ร้องเรียนยังคงเห็นว่าเรื่องร้องเรียนมีมูล เป็นสาระ หรือสมเหตุสมผล ผู้ร้องเรียนสามารถส่งเรื่องให้ กสทช. พิจารณา และ รท. จะเป็นผู้แจ้งผลการพิจารณาให้ผู้ร้องเรียนและผู้ให้บริการทราบภายใน 14 วัน และถ้าผลปรากฏว่าเรื่องร้องเรียนมีมูล ให้ผู้ให้บริการดำเนินการแก้ไขต่อไป
4. ผู้ให้บริการต้องแก้ไขข้อร้องเรียนให้แล้วเสร็จภายใน 30 วัน ยกเว้นแต่มีเหตุสุดวิสัยไม่อาจดำเนินการให้แล้วเสร็จ จะต้องแจ้งความคืบหน้าและกำหนดเวลาที่คาดจะดำเนินการให้แล้วเสร็จทุก 10 วัน
5. กรณีผลการเจรจาระหว่างผู้ให้บริการและผู้ร้องเรียนไม่ได้ข้อยุติ ไม่ว่าทั้งหมดหรือบางส่วน ผู้ให้บริการต้องเสนอรายงานกระบวนการแก้ไขปัญหาเรื่องร้องเรียน บันทึกการเจรจา รายละเอียด พยาน หลักฐานทั้งหมดให้ รท. ทราบภายใน 3 วัน นับจากวันที่การเจรจาตกลงเสร็จสิ้น เพื่อนำเข้าสู่กระบวนการพิจารณาเรื่องร้องเรียนและระงับข้อพิพาทโดย กสทช. ต่อไป

ท่องโลกออนไลน์ พบปัญหาเมื่อใดติดต่อได้ที่นี่

หน่วยงาน	เว็บไซต์	ติดต่อ	ภารกิจ
ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ ETDA (เอ็ตด้า)	www.1212occ.com	**โทรศัพท์** 1212 **อีเมล** 1212@mict.go.th **โทรสาร** 0-2127-5789 **แอปพลิเคชัน** 1212 OCC **เว็บไซต์** www.1212occ.com	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มอบหมายให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ดำเนินการศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ 1212 Online Complaint Center หรือ 1212 OCC เพื่อเป็นศูนย์กลางการรับเรื่องร้องเรียนปัญหาที่เกิดจากการซื้อขายทางออนไลน์ การกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมถึงการกระทำความผิดทางเทคโนโลยีสารสนเทศ ภัยคุกคามทางไซเบอร์ตลอดจนปัญหาทางออนไลน์อื่นๆ ที่เกี่ยวข้อง
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ภายใต้ ETDA กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	www.thaicert.or.th	**โทรศัพท์** 0-2123-1212 **อีเมล** แจ้งเหตุภัยคุกคาม report@thaicert.or.th	รับแจ้งเหตุภัยคุกคาม รวมทั้งประสานงานระหว่างหน่วยงานทั้งในและต่างประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
สำนักงานคณะกรรมการคุ้มครองผู้บริโภค	www.ocpb.go.th	**สายด่วน** 1166 **อีเมล** consumer@ocpb.go.th **เว็บไซต์** http://complain.ocpb.go.th/	มีบทบาทหน้าที่ในการบังคับใช้กฎหมายให้เกิดประโยชน์สูงสุดต่อผู้บริโภค โดยคุ้มครองผู้บริโภคในด้านโฆษณา ด้านฉลาก และด้านสัญญา

หน่วยงาน	เว็บไซต์	ติดต่อ	ภารกิจ
สำนักงานคณะกรรมการอาหารและยา	www.fda.moph.go.th	**สายด่วน** 1556 **โทรศัพท์** 0-2590-1556 **อีเมล** 1556@fda.moph.go.th	มีบทบาทหน้าที่ในการบังคับใช้กฎหมายว่าด้วยผลิตภัณฑ์สุขภาพ ซึ่งมีขอบเขตการรับเรื่องร้องเรียนและดำเนินการให้คำปรึกษาตลอดจนแก้ไขปัญหาในเรื่องดังต่อไปนี้ • มีความบกพร่องของผลิตภัณฑ์สุขภาพที่เห็นได้ชัดเจน เช่น ไม่มีคุณภาพตามมาตรฐานที่กฎหมายกำหนด • มีการโฆษณาโอ้อวด หลอกลวงหรือทำให้เข้าใจผิดในสาระสำคัญของผลิตภัณฑ์สุขภาพนั้น • เป็นผลิตภัณฑ์สุขภาพที่ไม่ได้รับอนุญาต ปลอม ไม่ได้มาตรฐานเรื่องคุณภาพหรืออาจไม่ปลอดภัยต่อผู้บริโภคในทุกกรณี
กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือ บก.ปอท.	www.tcsd.in.th/	**โทรศัพท์** 0-2142-2555-60 **เว็บไซต์** http://www.tcsd.in.th/แจ้งเหตุเบาะแส	มีขอบเขตการรับเรื่องร้องเรียนและดำเนินการให้คำปรึกษา ตลอดจนแก้ไขปัญหาในด้านการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมไปถึงการหลอกลวง หรือฉ้อโกงทางอินเทอร์เน็ตหรือสื่อสังคมออนไลน์และเรื่องอื่นๆ ที่เกี่ยวข้อง
ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย	www.1213.or.th	**สายด่วน** 1213 **อีเมล** fcc@bot.or.th	เป็นศูนย์กลางในการดำเนินงานด้านการคุ้มครองผู้ใช้บริการทางการเงิน เพื่อลดความเสี่ยงและความเสียหายที่อาจจะเกิดขึ้นจากการใช้บริการ รวมทั้งให้รู้เท่าทันการหลอกลวงทางการเงินจากกลุ่มมิจฉาชีพ เพื่อไม่ให้ตกเป็นเหยื่อภัยทางการเงินในรูปแบบต่างๆ

ฉลาดรู้เน็ต 3

ตอน Trust on Mobile Internet

เราปั้นหนังสือเล่มนี้เพื่อคุณ :

- ○ เต้าแก่ยุคไอที
- ○ นักช้อปออนไลน์
- ✓ ครอบครัวไซเบอร์

จัดพิมพ์และเผยแพร่โดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
อาคารเดอะไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระรามเก้า แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310
โทรศัพท์ 0-2123-1234
เว็บไซต์ สพธอ. : www.etda.or.th
เว็บไซต์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม : www.mdes.go.th

ISBN 978-974-9765-76-0
9 789749 765760 >