กสทช.

คู่มือแนวทางปฏิบัติการรักษาความปลอดภัยบนโลกไซเบอร์ภาคประชาชน

คู่มือ Cyber Security สำหรับประชาชน

บิลช็อค! พลาดซื้อไอเท็ม แอพโดยไม่รู้ตัว

Chat, Comment, Share ก็ผิดกฎหมายได้

ข้อมูลลับอยู่ในเครื่องที่หายหรือเปลี่ยนมือ

ปลอมข้อมูลส่วนตัว หรือข้อมูลการเงิน

ขโมยใช้อีเมล์หรือ Facebook ของเรา

หลอกลวงเรื่องช้อปปิ้งออนไลน์

เจาะระบบโดย Hacker

Cyber Security สำหรับประชาชน

กสทช. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานคณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

87 ถนนพหลโยธิน ซอย 8
แขวงสามเสนใน เขตพญาไท กรุงเทพฯ 10400
โทรศัพท์ 0 2271 0151, 0 2670 8888
และ Call Center 1200 (โทรฟรี)
เว็บไซต์ : http://www.nbtc.go.th

คู่มือ Cyber Security สำหรับประชาชน

คู่มือแนวทางปฏิบัติการรักษาความปลอดภัยบนโลกไซเบอร์ภาคประชาชน

เลขมาตรฐานสากลประจำหนังสือ : 978-616-204-530-1

ผู้จัดทำ : บริษัท โปรวิชั่น จำกัด

พิมพ์ที่ : บริษัท วีพริ้นท์ (1991) จำกัด

พิมพ์ครั้งที่ 1 : พฤศจิกายน 2557

จำนวนพิมพ์ : 3,000 เล่ม

ห้าม
จำหน่าย

รายชื่อคณะอนุกรรมการ
ความมั่นคงเครือข่ายภายในกิจการโทรคมนาคม
และกิจการวิทยุโทรคมนาคม

รายชื่อ	ตำแหน่ง
พันเอก ดร. เศรษฐพงศ์ มะลิสุวรรณ	ที่ปรึกษาอนุกรรมการ
ดร. สุทธิพล ทวีชัยการ	ที่ปรึกษาอนุกรรมการ
รองศาสตราจารย์ ประเสริฐ ศีลพิพัฒน์	ที่ปรึกษาอนุกรรมการ
นายประวิทย์ ลี่สถาพรวงศา	ที่ปรึกษาอนุกรรมการ
พลเอก สุกิจ ขมะสุนทร	ที่ปรึกษาอนุกรรมการ
พลเอก ภูดิท วีระศักดิ์	ประธานอนุกรรมการ
พลอากาศตรี ดร. ธนพันธุ์ หร่ายเจริญ	อนุกรรมการ
รองศาสตราจารย์ ดร. ธนิศ ภู่ศิริ	อนุกรรมการ
นายนัทธี พุคยาภรณ์	อนุกรรมการ
นายฉัตรพงศ์ ฉัตราคม	อนุกรรมการ
นางอรนิตย์ บุนนาค	อนุกรรมการ
นายปริญญา หอมอเนก	อนุกรรมการ
นางสุรางคณา วายุภาพ	อนุกรรมการ
ดร. ฐิติพงศ์ นันทาภิวัฒน์	อนุกรรมการและเลขานุการ
ผู้แทนสำนักบริหารความถี่วิทยุ	ผู้ช่วยเลขานุการ
ผู้แทนสำนักขับเคลื่อนภารกิจพิเศษ	ผู้ช่วยเลขานุการ

คำนำ

ด้วยในปัจจุบันเทคโนโลยีการสื่อสารมีความก้าวหน้าอย่างมาก และได้เข้ามาเป็นส่วนหนึ่งของชีวิตประจำวันของประชาชนทุกเพศทุกวัยอย่างไม่อาจหลีกเลี่ยงได้ โดยการสื่อสารไม่ว่าจะเป็นภาพ วิดีโอ เสียง และสื่อมัลติมีเดียต่างๆ สามารถรับส่งผ่านเครือข่ายโทรคมนาคมได้อย่างรวดเร็วภายในเสี้ยววินาที ส่งผลให้การติดต่อสื่อสารเรื่องงานหรือธุรกรรมต่างๆ ดำเนินไปได้อย่างรวดเร็วกว่าในอดีตอย่างเห็นได้ชัด แต่ถึงกระนั้นก็ตาม แม้เทคโนโลยีจะมีคุณอนันต์แต่ก็มีโทษมหันต์เช่นเดียวกัน หากผู้ใช้รู้ไม่เท่าถึงอันตรายที่อาจเกิดจากการใช้อุปกรณ์มือถือหรือพกพานั้นๆ

ด้วยเหตุนี้ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ โดย คณะอนุกรรมการความมั่นคงเครือข่ายและข้อมูลในกิจการโทรคมนาคมและกิจการวิทยุคมนาคม จึงเล็งเห็นความสำคัญในเรื่องดังกล่าว และได้จัดทำหนังสือเล่มนี้ขึ้น เพื่อให้ประชาชนได้ตระหนักถึงการใช้เทคโนโลยีการสื่อสารอย่างชาญฉลาด รู้ทันกลโกงต่างๆ เพื่อให้เกิดความปลอดภัยในชีวิต และทรัพย์สิน โดยการใช้คำอธิบายและภาพประกอบที่ผู้อ่านไม่จำเป็นต้องมีพื้นฐานทางเทคนิค ก็สามารถอ่านและเข้าใจได้โดยง่าย หวังว่าหนังสือเล่มนี้จะเป็นประโยชน์แก่เยาวชนและประชาชนทั่วไป

พันเอก

(เศรษฐพงศ์ มะลิสุวรรณ)

รองประธานกรรมการ

กิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

ประธานกรรมการกิจโทรคมนาคม

หนังสือเล่มนี้จะช่วยคุณได้อย่างไร?

ปัจจุบันเรามีโทรศัพท์สมาร์ทโฟนหรือแท็บเล็ตที่เชื่อมต่ออินเทอร์เน็ตได้กันแทบทุกคนแล้ว แถมในอนาคตอันใกล้ยังอาจจะมีอุปกรณ์อื่นๆ ที่ต่ออินเทอร์เน็ตได้เพิ่มอีกคนละหลายๆ ชิ้น ไม่ว่าจะเป็นของติดตัวเช่น นาฬิกา กำไลข้อมือ แว่นตา ฯลฯ ไปจนถึงของใช้ใหญ่ๆ เช่นรถยนต์ เครื่องใช้ไฟฟ้า หรือระบบควบคุมอุปกรณ์ต่างๆ ในบ้าน จนเรียกกันว่าเป็น "อินเทอร์เน็ตของสรรพสิ่ง" (Internet of Things) ไปแล้ว

การเชื่อมต่ออินเทอร์เน็ต หรือที่เรียกว่าการ "ออนไลน์" (Online) หรือการเข้าสู่โลก "ไซเบอร์" (Cyber) นั้นมีประโยชน์และสร้างความสะดวกอย่างมหาศาลทั้งในชีวิตประจำวัน การทำงาน การสันทนาการหรือบันเทิงต่างๆ เพราะทำให้เราสามารถติดต่อกับผู้คนหรือใช้บริการสารพัดอย่างได้โดยไม่ต้องเดินทางไปพบกันจริงๆ และทำได้ตลอด 24 ชั่วโมงด้วย แต่ในทางกลับกันก็เป็นช่องทางให้อันตรายต่างๆ ที่เรานึกไม่ถึง เข้ามาถึงตัวเราหรืออุปกรณ์ต่างๆ รอบตัวเราได้ตลอดเวลา โดยที่เราไม่รู้เห็นหรือไม่ทันระวังตัวเลยเช่นกัน

ทางแก้ปัญหานี้คงไม่ใช่การเลิกออนไลน์ไปเลย แต่ต้องรู้จักและเข้าใจวิธีใช้อุปกรณ์ต่างๆ ที่ต่ออินเทอร์เน็ตอย่างถูกต้อง ปลอดภัย รู้หลักการและเทคนิค รวมถึงข้อควรระวังหรือวิธีแก้ไขเมื่อเกิดปัญหาขึ้น ซึ่งไม่ใช่เรื่องที่ไกลตัวหรือ "มีปัญหาแล้วค่อยหาคนถาม" อีกต่อไป แต่ต้องเตรียมพร้อมรับมือตั้งแต่เริ่มเข้าใช้งานเลย ไม่เช่นนั้นกว่าจะรู้ตัวก็อาจสายไป จนตกเป็นเหยื่อของการโจมตีหรือภัยอันตรายต่างๆ ได้ เพราะภัยออนไลน์ในปัจจุบันเพิ่มความซับซ้อนขึ้นมาก ขั้นตอนหรือมาตรการในการป้องกันตัวก็เลยต้องมีมากขึ้นตามไปด้วย ซึ่งในหนังสือ Cyber Security เล่มนี้ก็มีทั้งหลักการหรือข้อแนะนำ และขั้นตอนที่ทำตามได้จริงบนอุปกรณ์ต่างๆ ไว้ให้แล้ว

อย่างไรก็ตาม อุปกรณ์แต่ละรุ่นหรือยี่ห้อต่างๆ จะแตกต่างกันและเปลี่ยนแปลงตลอดเวลา ทำให้ในหนังสือไม่สามารถเขียนอธิบายให้ครอบคลุมทุกอุปกรณ์ ทั้งในปัจจุบันและที่จะมีมาใหม่ๆ ต่อไปในอนาคตได้ แต่ก็ได้เลือกยกตัวอย่างเอาระบบที่มีผู้ใช้จำนวนมาก เช่นระบบ iOS ของ Apple และ Android ของ Google ซึ่งน่าจะใช้ได้กับผู้อ่านส่วนใหญ่ โดยได้อธิบายทั้ง "หลักการ" ที่น่าจะเหมือนเดิม และ "ขั้นตอน" ที่อาจเปลี่ยนได้ในอนาคต ดังนั้นหากพบปัญหาในลักษณะคล้ายกัน ก็ขอให้พยายามจับประเด็นของหลักการให้ได้ก่อน แล้วดูว่าขั้นตอนที่อธิบายนั้นทำตามได้เลยหรือจะต้องปรับใช้อย่างไรบ้าง ซึ่งถึงแม้จะไม่เหมือน 100% แต่ก็น่าจะได้แนวทางที่จะนำไปปรับใช้กับกรณีของคุณได้ในระดับหนึ่ง

หวังว่าหนังสือนี้คงมีส่วนช่วยให้ทุกคนตระหนักถึงความเสี่ยงของภัยคุกคามต่างๆ ในปัจจุบัน และปรับตัวเข้าสู่โลกออนไลน์อย่างอยู่รอดปลอดภัยได้ตามสมควร

คณะอนุกรรมการความมั่นคงเครือข่ายและข้อมูล
ในกิจการโทรคมนาคมและกิจการวิทยุคมนาคม

สารบัญ

บทที่ 03

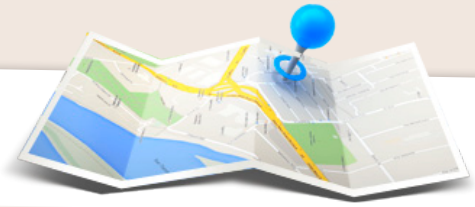
ระวังอันตรายเรื่องข้อมูลส่วนตัว





สารบัญ

สารบัญ



บทที่ 04 ระวังอันตรายเรื่องข้อมูลตำแหน่งที่อยู่

บทที่ 05 ระวังอันตรายจากการหลอกลวงรูปแบบต่างๆ

บทที่ 06

ระวัง! แอพพลิเคชั่นอันตราย

สารบัญ

บทที่ 09

ระวังผลกระทบทางสังคมและวัฒนธรรม

CHAPTER 1

เทคโนโลยีกับปัญหาความปลอดภัย

ด้วยเทคโนโลยีของอุปกรณ์พกพาในปัจจุบันที่รองรับการใช้งานได้สารพัดรูปแบบ ทั้งส่งอีเมล์ ถ่ายภาพ ดูหนัง ฟังเพลง อ่านอีบุ๊ค เล่นเกม แชท เล่น Facebook ท่องเว็บ เช็ค-โอนเงิน ฯลฯ นอกจากนี้ยังเชื่อมต่ออินเทอร์เน็ตได้ทุกที่ทุกเวลาจนแทบจะเรียกได้ว่าเป็นปัจจัยที่ 5 ไปแล้ว แถมยังเก็บข้อมูลส่วนตัวไว้มากมาย รวมทั้งส่งข้อมูลในเครื่องขึ้นไปเก็บสำรองบนเน็ตให้อัตโนมัติด้วย จึงต้องระวังอย่างยิ่งที่จะไม่ให้เครื่องหาย ควรตั้งรหัสผ่านในการปลดล็อคก่อนเข้าใช้เครื่อง และระวังตัวจากภัยออนไลน์ทั้งหลาย เช่น การขโมยข้อมูลที่ฝากไว้บนเน็ตด้วย ในบทนี้เราจะมาดูกันว่ามีปัญหาด้านไหนที่ต้องระมัดระวังกันบ้าง :)

เทคโนโลยีในอนาคต


Wearable : Google Glass ของ Google

เทคโนโลยีของเครือข่ายและการรับส่งข้อมูลดิจิตอลในปัจจุบันพัฒนาไปอย่างรวดเร็วมาก เช่น จาก 3G ไปเป็น 4G และ 5G ในอนาคตพร้อมความเร็วที่เพิ่มขึ้นจากเดิมอีก 10 และ 100 เท่า ตามลำดับ รวมถึงอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์เกี่ยวข้อง ทั้งความสามารถของตัวตรวจวัดหรือ sensor ทั้งหลาย ทั้งที่ใส่ติดตัว (wearable) ติดบ้าน ติดรถยนต์ ที่ทำให้เกิดข้อมูลดิบในเรื่องต่างๆ ทั้งภาพ เสียง วิดีโอ หรือค่าที่วัดได้แบบอื่นๆ เช่น ตำแหน่งที่อยู่ การเคลื่อนที่ อุณหภูมิ ฯลฯ นอกจากนี้ด้วยความเร็วในการประมวลผลข้อมูล ความซับซ้อนของซอฟต์แวร์และการทำงานผ่านเครือข่ายร่วมกับระบบ cloud ที่ทำให้งานยากๆ สามารถทำได้บนอุปกรณ์พกพาต่างๆ ไม่ว่าจะถ่ายภาพ ตัดต่อวิดีโอ ค้นหาข้อมูล ระบุตำแหน่งบนแผนที่จาก GPS ค้นหาเพลงจากเสียงที่ได้ยิน นำทางระหว่างการขับรถ แปลข้อความในภาพเป็นตัวอักษร (OCR) ค้นหาหรือจำแนกหน้าตาของคนในรูปถ่าย แปลภาษาเขียนหรือภาษาพูดอัตโนมัติ ฯลฯ


GPS ในรถยนต์ เช่น Sygic


ตัวอย่างแอพ Savant ควบคุมอุปกรณ์เครื่องใช้ในบ้าน

ทั้งหมดนี้ทำให้เกิดความสะดวกในการใช้ชีวิตและการทำงานมากขึ้นกว่าแต่ก่อน ขณะเดียวกันก็สร้างปัญหาใหม่ที่ไม่เคยมีใครคาดคิดไว้ตามมาอีกหลายอย่าง เช่น

- ข้อมูลดิบปริมาณมากขึ้น เช่นระดับหลายกิกะไบต์ต่อวัน โอกาสที่ข้อมูลจะผิดพลาด รั่วไหล หรือถูกบิดเบือนรบกวน ก็มีมากขึ้นด้วย
- เครือข่ายเร็วขึ้น ข้อมูลที่ตกอยู่ในความเสี่ยงก็มีปริมาณมากขึ้น กว่าจะรู้ว่าถูกขโมยข้อมูลก็รั่วไปหมดแล้ว เป็นต้น
- ข้อมูลส่วนตัวมากขึ้น ก็ต้องใช้ความพยายามควบคุมปิดกั้นข้อมูลมากขึ้น เพื่อรักษาความเป็นส่วนตัวเอาไว้
- เกิดค่าใช้จ่ายต่อเดือนค่อนข้างมากในการเชื่อมต่ออินเทอร์เน็ตความเร็วสูง ผ่านช่องทางต่างๆ ทั้ง mobile, Wi-Fi และ ADSL เพราะมีหลายอุปกรณ์
- อื่นๆอีกมากมาย

ข้อเสนอแนะในการป้องกันและแก้ไขปัญหาเหล่านี้ เริ่มตรงที่เราต้องเข้าใจว่าการพัฒนาเหล่านี้เป็นเรื่องธรรมดาที่หลีกเลี่ยงไม่ได้ และคนที่จะอยู่รอดได้ในสังคมยุคนี้จำต้องมีทักษะทางเทคโนโลยีใหม่ๆ อีกหลายอย่าง ซึ่งทำให้ชีวิตไม่เหมือนแบบเดิมๆ ที่คนรุ่นก่อนเคยใช้มา ขณะเดียวกันงานและชีวิตในรูปแบบเดิมๆ จะค่อยหายไป แทนที่ด้วยสังคมที่โลกออนไลน์และออฟไลน์ทับซ้อนกันอยู่ การใช้ชีวิตในโลกแบบนี้ต้องมีสติอยู่ตลอดเวลาว่าอะไรควรหรือไม่ควรทำ และอะไรที่ควรลงมือทำทันทีโดยไม่ผลัดวันประกันพรุ่งต่อไปอีก

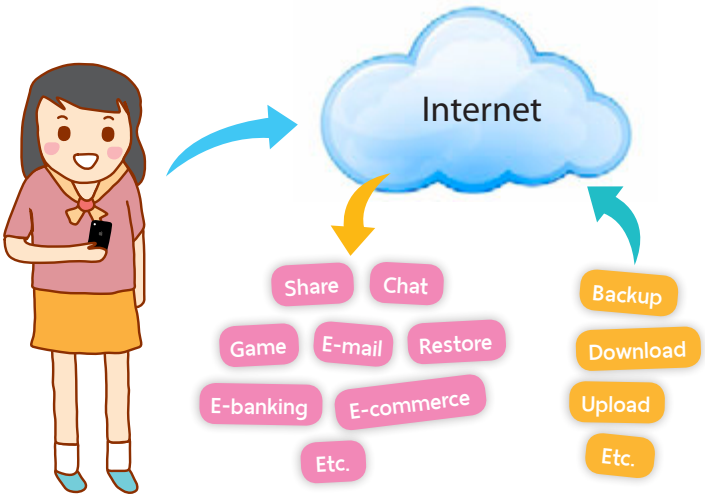
อุปกรณ์ออนไลน์กับความปลอดภัย

อุปกรณ์พกพานั้นมีความเสี่ยงด้านความปลอดภัยมากมาย อย่างแรกคือ หายได้ง่ายเนื่องจากพกพาไปไหนมาไหนด้วยตลอด จึงต้องระวังให้ดี เพราะภายในอุปกรณ์ก็จะเต็มไปด้วยข้อมูลส่วนตัวมากมาย นอกจากนี้ยังควรตั้งรหัสผ่านให้กรอกก่อนเข้าเครื่องไว้ด้วย

พกพาสะดวกก็ต้องระวังเครื่องหาย
ถ่ายภาพก็ระวังไม่ให้ไปละเมิดสิทธิ์ผู้อื่น
ออนไลน์ก็ให้ระวังการดักจับข้อมูล

กล้องในอุปกรณ์พกพาก็มีกันแทบทุกรุ่น ทำให้ถ่ายง่าย พบเห็นอะไรก็ถ่ายไว้ไม่ว่าจะเป็นภาพนิ่งหรือวิดีโอ จากนั้นก็นำมาแชร์บนโลกออนไลน์ได้ง่ายดาย บางภาพหรือบางคลิปอาจไปละเมิดสิทธิ์ของผู้อื่น ซึ่งอาจถูกฟ้องได้ง่ายๆ เช่นกัน

ถ้าอุปกรณ์นั้นต่อเน็ตได้ก็จะต้องระวังภัยออนไลน์ ทั้งไวรัส สแปม แฮกเกอร์ การหลอกลวง ข้อมูลเท็จต่างๆ ที่ปะปนอยู่ ฯลฯ อีกทั้งการระบุตำแหน่งที่อยู่ที่ทำให้สามารถติดตามตัวได้ง่ายขึ้น



เดี๋ยวนี้ใครๆ ก็ใช้เน็ตได้จากทุกที่ทุกเวลา บางแอพหรือบางบริการก็จะรับส่งข้อมูลอยู่เป็นระยะทำให้ข้อมูลต่างๆ ไหลเข้าและออกจากอุปกรณ์ของเราตลอดเวลา ถึงแม้ขณะที่เราเสียบชาร์จไว้เฉยๆ (เช่น การแบ็คอัพรูปและข้อมูลจากในเครื่อง การอัพเดทซอฟต์แวร์ออนไลน์อัตโนมัติ) อันตรายจึงมาถึงเราได้ตลอด 24 ชม. ที่เชื่อมต่ออินเทอร์เน็ต

ช่วงเวลากลางคืน เป็นเวลาที่แฮกเกอร์มักใช้ในการนำข้อมูลที่ดักจับได้มาลองของ เพราะเป็นเวลาที่เจ้าของหลับใหล แฮกเกอร์สามารถลองล็อกอินเว็บหรือบริการต่างๆ ด้วยข้อมูลที่ดักจับมาได้เพื่อกระทำการบางอย่าง กว่าเจ้าของจะรู้ตัวก็อาจถูกแฮกหรือขโมยอะไรไปแล้วก็ได้

ผู้ใช้ควรป้องกันตัวเองด้วยระบบรักษาความปลอดภัยที่บริการต่างๆมีให้ใช้ ควรจะตั้งค่าให้ครบเพื่อให้ระบบคอยแจ้งเราในกรณีต่างๆ เช่น ให้ส่งข้อความเตือนเมื่อมีการล็อกอินแอคเคาท์ด้วยอุปกรณ์เครื่องใหม่, ให้ส่งรหัส OTP มาที่โทรศัพท์เพื่อนำไปกรอกยืนยันก่อนใช้บริการต่างๆ เป็นต้น ซึ่งเราจะรู้ได้ทันทีว่ามีใครมาทำอะไรกับแอคเคาท์ ทำให้ป้องกันตัวได้ทันท่วงทีไม่ตกเป็นเหยื่อของเหล่าแฮกเกอร์

เมื่อเรื่องส่วนตัวไม่เป็นความลับ

ทัศนคติของคนยุคนี้เปลี่ยนไปจากเรื่องส่วนตัวต้องเก็บ กลายเป็นมีดีต้องแชร์ผ่านช่องทางออนไลน์ต่างๆ เพื่อให้เพื่อนและคนใกล้ชิดได้รับรู้ ซึ่งอาจรวมถึงคนทั้งโลกที่จะเห็นเรื่องส่วนตัวที่คุณแชร์ออกไป อีกทั้งการคลิก LIKE ก็เป็นข้อมูลให้ผู้อื่นรู้ว่าคุณชอบหรือสนใจอะไร ทำให้ข้อมูลเฉพาะตัวถูกเอาไปใช้ได้ง่ายขึ้น ทั้งจากนักการตลาด หน่วยงานราชการ และผู้ไม่หวังดี

เปิดเผยเรื่องส่วนตัวให้น้อย ก็จะปลอดภัยมากขึ้น

การเปิดเผยเรื่องส่วนตัวต่างๆ ก็ควรทำด้วยความรอบคอบ บางเรื่องที่ดูเล็กน้อยไม่น่ามีปัญหาก็อาจส่งผลเสียได้ เช่น การเช็คอินตำแหน่งที่อยู่ บอกข้อมูลส่วนตัว ชื่อ นามสกุล บ้านอยู่ไหน ทำงานอะไร วันเกิดวันที่เท่าไหร่ มีพี่น้องกี่คน เพื่อนสนิทเป็นใคร เบอร์โทรศัพท์อะไร กำลังจะไปไหน ไปกับใคร มีใครอยู่บ้านมั้ย ระบบกันขโมยหรือกล้องวงจรปิดเสีย รถจอดหน้าบ้านในซอยเปลี่ยว กลับดึกเป็นประจำ ใช้ของมีค่า ฯลฯ เหล่านี้เป็นข้อมูลเล็กๆ น้อยๆ บางคนก็โพสต์บอกสถานะส่วนตัวเสียอย่างกับเป็นเซเลป อาจคิดว่าอยากแชร์เปิดเผยแล้วไม่น่าจะมีอันตราย แต่พอข้อมูลหลายๆ อย่างมารวมกัน ปะติดปะต่อจนอาจกลายเป็นโอกาสที่ผู้ไม่หวังดีจะนำข้อมูลเหล่านี้ไปใช้ประโยชน์ได้ อย่างเช่น เอาไปแอบอ้างเป็นตัวเราหลอกผู้อื่นให้โอนเงินให้, รู้ว่ามีของมีค่าอาจแอบมาดักจี้ในซอยเปลี่ยว, บอกหมดเลยรถจอดหน้าบ้านไม่มียามก็เสร็จโจร, รู้ว่าไม่มีใครอยู่บ้านหลายวันก็ย่องมาขโมยของ, ระบบกันขโมยเสียใช่มั้ย ย่องมายกเค้าซะเลย เป็นต้น

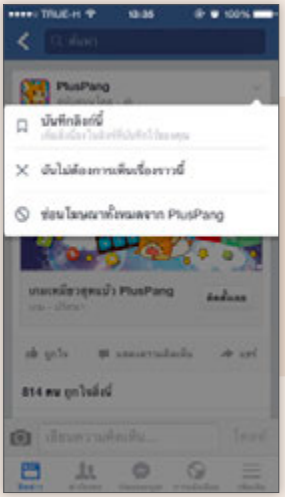
รูปภาพที่โพสต์ขึ้นไปบนอินเทอร์เน็ตก็มีการแอบเอาไปใช้กันบ่อยครั้ง บางรายถูกนำภาพที่อัพโหลดไว้บนอัลบั้มออนไลน์ไปใช้แอบอ้างเป็นคนอื่น แอบอ้างว่าคนนั้นเป็นเจ้าของภาพ นำไปตัดต่อเป็นภาพลามกอนาจาร บ้างก็ถูกนำไปเป็นภาพประกอบโฆษณาบนเว็บลามกหรือขายบริการก็มี

ท่องเว็บก็โดนเก็บข้อมูลไม่รู้ตัว

ขณะท่องเว็บหรือใช้ Social Network ต่างๆ มักจะแสดงโฆษณาสินค้าของเว็บหรือเพจ Facebook ที่เคยเปิดเข้าไปดู นั่นเป็นผลมาจากการตลาดแบบ “retargeting marketing” ซึ่งเป็นการเน้นย้ำสินค้าที่แต่ละคนสนใจอีกครั้ง เพื่อชักชวนให้เกิดการซื้อหรือเน้นย้ำไม่ให้ลืม เช่น ระหว่างเล่น Facebook ได้คลิกเข้าไปดูเพจขายสินค้าเกี่ยวกับอุปกรณ์ตกแต่งบ้าน หลังจากปิดหน้าเพจนั้นไปแล้วมาเล่น Facebook ตามปกติ คุณจะเห็นโฆษณาอุปกรณ์ตกแต่งบ้านจากเพจนั้นขึ้นมาแสดงให้เห็นซ้ำอีก

นั่นเป็นเพราะ Facebook ได้เก็บข้อมูลการเข้าชมเพจและเว็บของคุณไว้ จากนั้นก็จะนำข้อมูลมาประมวลผลแล้วนำเสนอโฆษณาที่ตรงกับความสนใจของคุณที่สุดขึ้นมา เพื่อเตือนและกระตุ้นให้เกิดการกลับไปที่เพจนั้นซ้ำอีก ทำให้เกิดการซื้อสินค้าในที่สุด

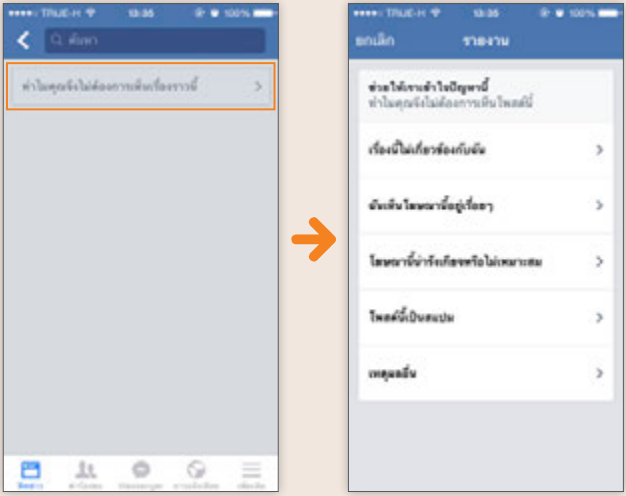
หลายเว็บจะเก็บข้อมูลการเข้าชมเว็บของคุณว่าสนใจเกี่ยวกับอะไร แล้วนำเสนอเนื้อหาหรือโฆษณาให้โดนใจตามมาในภายหลัง



วิธีปิดโฆษณาที่ไม่ต้องการ บน Facebook

เมื่อเห็นโฆษณาขณะใช้ Facebook คุณสามารถปิดการแสดงโฆษณาที่ไม่ต้องการได้ โดยแตะกรอบโฆษณา แตะที่ ▾ แล้วเลือก **ฉันไม่ต้องการเห็นเรื่องราวนี้** เพื่อปิดโฆษณานี้ หรือเลือก **ซ่อนโฆษณาทั้งหมดจาก...** จะยกเลิกการแสดงโฆษณาของแอพหรือหน้านั้นไปเลย

ในที่นี้เลือก **ฉันไม่ต้องการเห็นเรื่องราวนี้** Facebook จะซ่อนโฆษณาและถามเหตุผล ให้แตะที่ **ทำไมคุณจึงไม่ต้องการเห็นเรื่องราวนี้** แล้วเลือกเหตุผลของคุณ



Twitter ก็มีการเก็บข้อมูลเพื่อแสดงโฆษณาที่ตรงกับความสนใจแบบนี้เช่นกัน โดยไปปิดได้ (ดูหน้า 61)

การเก็บข้อมูลบน Cloud ปลอดภัยหรือเชื่อถือได้แค่ไหน?

จากแนวโน้มที่อินเทอร์เน็ตสามารถรับส่งข้อมูลได้ด้วยความเร็วที่สูงขึ้น ทำให้เกิดความนิยมจัดเก็บข้อมูลไว้บนบริการออนไลน์ในรูปแบบของ cloud มากขึ้น ซึ่งก็จะรวมไปถึงบริการที่คล้ายกันแต่มีมาก่อน เช่น บริการอีเมล์ฟรีทั้งหลาย ดังจะเห็นได้จากบริการของเว็บต่างๆ เช่น Dropbox, GMail/Google Drive, Hotmail/OneDrive (Microsoft) และอื่นๆ ซึ่งล้วนอำนวยความสะดวกกับผู้ใช้ที่สามารถเรียกข้อมูลจากดิสก์หรืออีเมล์ได้จากทุกที่ในโลก ทุกเวลาที่ต้องการ เพียงแต่ต้องสามารถต่อเน็ตได้ด้วยความเร็วสูงพอเท่านั้น โดยสามารถเรียกดูข้อมูลได้จากทุกอุปกรณ์ที่รองรับ (ต่างกับการบันทึกไฟล์ไว้ในเครื่องที่จะเรียกดูได้เฉพาะเครื่องนั้น)

การเก็บข้อมูลไว้บนบริการ Cloud นั้น ถ้าจะอธิบายให้เห็นภาพ ก็เปรียบได้กับการนำข้อมูลไปใส่ไว้ในก้อนเมฆ

ซึ่งก้อนเมฆแต่ละก้อนก็เปรียบได้กับกล่องเก็บข้อมูลของแต่ละคน ไม่ว่าอยู่ที่ไหนหรือใช้อุปกรณ์ใดก็จะมองเห็นก้อนเมฆติดตามไปด้วยตลอด ทำให้สามารถดึงข้อมูลของตัวเองที่เก็บไว้บนก้อนเมฆลงมาใช้งานได้ทุกที่ทุกเวลา

คำถามที่ตามมาคือการเก็บข้อมูลในลักษณะดังกล่าว ทั้งที่เป็นอีเมล์และไฟล์ มีความปลอดภัยแค่ไหน ในประเด็นต่างๆ เช่น

- **ความเชื่อถือได้ของข้อมูล** ว่าจะไม่มีการเสียหาย สูญหาย ซึ่งน่าจะอยู่ในระดับดี เพราะระบบของผู้ให้บริการแต่ละรายมักมีการกระจายข้อมูลไปเก็บซ้ำซ้อนกันหลายที่ มีการทำสำเนาสำรองอย่างรัดกุม หากระบบมีปัญหาก็อาจเพียงเข้าถึงไม่ได้ชั่วคราว แต่สามารถแก้ไขให้กลับมาเป็นปกติได้ในเวลาไม่นาน

- **ความเป็นส่วนตัว** ข้อนี้ต้องอาศัยความเชื่อใจว่าผู้ให้บริการจะไม่ถือโอกาสเข้ามาดูข้อมูลในอีเมล์หรือไฟล์ของผู้ใช้ (บางราย เช่น Google บอกไว้ก่อนว่าจะใช้โปรแกรมอัตโนมัติอ่านอีเมล์ของลูกค้าเพื่อไปดึงโฆษณาที่เกี่ยวข้องกับเนื้อหาในอีเมล์มาแสดง แต่รับรองว่าจะไม่มีการให้คนจริงเปิดอ่าน เพื่อคุ้มครองความเป็นส่วนตัวของผู้ใช้)

- **ความปลอดภัย** หากเป็นข้อมูลที่มีความสำคัญ หรือเป็นความลับของหน่วยงานหรือองค์กร บริษัท หรือหน่วยงานราชการเหล่านั้นอาจวางนโยบายให้ใช้อีเมล์ขององค์กรเองแทนที่จะยอมเสี่ยงกับบริการฟรี (แต่ก็มักมีปัญหาในการบริหารจัดการในเชิงเทคนิคที่ไม่สามารถทำได้ดีหรือคุ้มค่าการลงทุนเท่ากับมืออาชีพที่ให้บริการคนทั้งโลกได้) หรือหากเป็นข้อมูลส่วนตัว ความลับ ภาพหลุด ฯลฯ ก็ต้องระวังว่าอาจถูกขโมยข้อมูลออกไปจากบริการ Cloud ได้ ดังเช่นที่เคยเกิดกรณีภาพเปลือยของดาราดังถูกขโมยจากที่เก็บบน Cloud มาแล้ว

CHAPTER 2

การใช้อินเทอร์เน็ตผ่านสมาร์ทโฟนหรือแท็บเล็ตให้ปลอดภัย

ด้วยความสามารถของสมาร์ทโฟนและแท็บเล็ต ที่สามารถรองรับการใช้งานของผู้ใช้ได้หลากหลาย ไม่ว่าจะดูหนัง, ฟังเพลง, เล่นเกม, ถ่ายหรือแต่งภาพ, จดบันทึก, คิดเลข, แชท LINE, เข้า Facebook, อ่านเว็บ, ค้นหาข้อมูลใน Google, รับส่งอีเมล์ หรือจะลงแอพต่างๆ เพิ่มเพื่อใช้งานได้สารพัดรูปแบบ ทำให้เกิดสังคมก้มหน้าไปทั่วโลก ด้วยลักษณะการใช้งานที่แต่ละคนต่างก้มหน้าก้มตา “จิ้ม” หน้าจอมือถือหรือแท็บเล็ตกันอย่างเอาเป็นเอาตาย และถ้าใครใช้ “เน็ตซิม” ด้วยละก็ ไม่ว่าจะอยู่ที่ไหน ก็เข้าใช้อินเทอร์เน็ตได้ตลอดเวลา ในบทนี้เราจะมาเข้าใจกลไกการใช้อินเทอร์เน็ตผ่านอุปกรณ์เหล่านี้ และข้อควรระวังต่างๆ

ใช้อินเทอร์เน็ตผ่าน “เน็ตซิม” ต่างกับ Wi-Fi อย่างไร

การใช้งานบางอย่างในสมาร์ทโฟนและแท็บเล็ตจะต้องเชื่อมต่ออินเทอร์เน็ตขณะใช้งานด้วย ไม่ว่าจะเป็นการดู YouTube, เล่นเกมออนไลน์, ท่องเว็บ, ค้นหาข้อมูล, เล่น LINE, เข้าใช้ Facebook, รับส่งอีเมล์ หรืออื่นๆ ซึ่งการเชื่อมต่ออินเทอร์เน็ตจากมือถือหรือแท็บเล็ตก็จะทำได้ 2 วิธีคือ

- **ต่อผ่านผู้ให้บริการบนมือถือ** หรือเรียกว่า “เน็ตซิม” ใช้ได้ทุกที่เหมือนโทรศัพท์มือถือ โดยเสียค่าบริการตามแพ็กเกจ ซึ่งความเร็วในการใช้งานจะมีหลายระดับ ตั้งแต่ GPRS/EDGE/3G/4G (LTE) ตามลำดับ จากความเร็วต่ำสุด (GPRS : 40 kbps) ไปยังสูงสุด (4G : 100 Mbps-1024 Mbps) ซึ่ง 4G นี้ ปัจจุบัน (2014) จะใช้ได้เฉพาะในบางพื้นที่เท่านั้น
- **ต่อผ่าน Wi-Fi** เช่น ตามบ้าน สถานศึกษา แหล่งชุมชน ที่ทำงาน บางที่ก็ให้เข้าใช้งานได้ฟรี (อาจต้องใส่รหัสผ่านหรือลงทะเบียนก่อนเข้าใช้งาน) หรืออาจเป็น Wi-Fi จากการแชร์จากอุปกรณ์หนึ่งที่ใช้เน็ตซิมไปยังอุปกรณ์อื่นๆ อีกทีก็ได้ ซึ่งความเร็วของ Wi-Fi จะแตกต่างกันไป

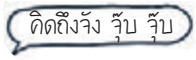
ความเร็วเน็ตซิมกับข้อมูลแบบต่างๆ

สมัยก่อนเน็ตซิมมีแต่ระบบ 2G/Edge เร็วแค่ประมาณ 0.3 เมกะบิตต่อวินาที (Mbps) จะเปิดเว็บ เช็คเมล์ทีก็รอกันนาน โหลดรูป อัพไฟล์ ยิ่งไม่ต้องพูดถึงตอนนี้เรามีเน็ตซิมแบบ 3G เร็วขึ้นเป็นประมาณ 3 เมกะบิตต่อวินาที (Mbps) เร็วกว่าเดิม 10 เท่าเข้าเว็บ ส่งอีเมล์ แชร์รูป เช็คสเตตัส Facebook ได้เหมือนเน็ตบ้าน ดูหนังก็พอได้ ถ่ายวิดีโอแล้วแชร์ก็พอไหว ต่อไปเราเริ่มจะมีเน็ตซิมแบบ 4G เร็วขึ้นอีกเป็น 10 เมกะบิตต่อวินาที (Mbps) หรือกว่านั้น เร็วกว่า 3G อีกอย่างน้อย 3 เท่า ถ่ายวิดีโอแล้วอัพโหลดได้สบาย ดูหนังยิ่งลื่นไหล

แต่เราอาจจะลืมไปว่า ข้อมูลแต่ละแบบนั้นมันมีขนาดผิดกันมากมายนับร้อยเท่า เช่นตัวอย่างต่อไปนี้

▲ หนึ่งภาพแทนได้พันคำ แต่ก็ต้องส่งข้อมูลเพิ่มพันเท่า ยิ่งถ้าเป็นเสียงหรือวิดีโอยิ่งต้องส่งให้ทันตามเวลาด้วย

- **ข้อมูลที่เป็นข้อความ** หรือตัวหนังสือล้วนๆ (Text) เป็นอะไรที่เบาสบาย รับส่งง่ายที่สุด การส่งข้อความผ่านอีเมล์ LINE หรือแอพอื่นๆ บนมือถือถึงใช้เวลาน้อยมาก ส่งปุ๊บถึงปั๊บทันใจ



ภาษาเทคนิค ขนาดไม่ถึง 1 กิโลไบต์

- **ข้อมูลที่เป็นภาพ** โดยเฉพาะภาพถ่าย (Photo) นั้นมีขนาดใหญ่มาก ภาษิตโบราณบอกว่า “หนึ่งภาพแทนได้พันคำ” แต่ข้อมูลของภาพถ่ายโดยทั่วไปนั้น ถึงแม้จะมีการบีบข้อมูลให้เล็กลงแล้วก็ตาม ข้อมูลภาพก็ยังอาจใหญ่กว่าข้อความเป็นพันเท่า (หรือบางทีก็เป็นหมื่นหรือแสนเท่า) ด้วยเช่นกัน ดังนั้นการส่งภาพผ่านระบบ 3G ก็เลยไม่ได้รู้สึกว่าเร็วมากนัก

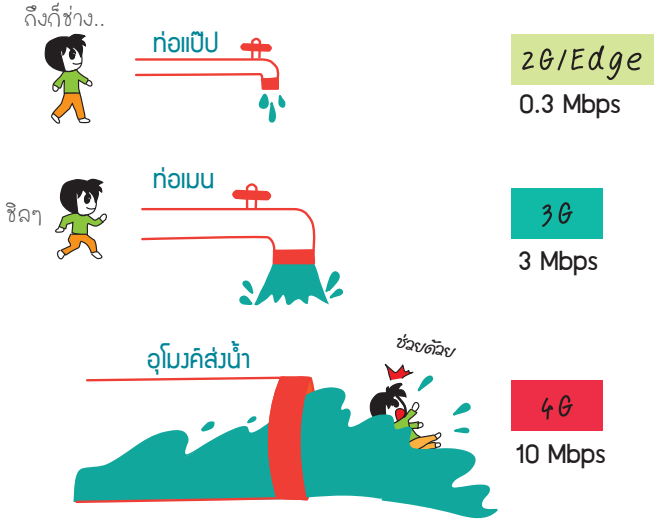
ภาษาเทคนิค ขนาดประมาณ 100 หรือ 1,000 กิโลไบต์ คือ 1 เมกะไบต์

- **ข้อมูลที่เป็นเสียง** เสียงมีขนาดพอๆ กับข้อมูลภาพ แต่ถ้าเป็นการส่งเสียงคุยโต้ตอบกัน เช่น แอพที่โทรฟรีผ่านเน็ต ไม่ว่าจะเป็น LINE, Skype, FaceTime หรืออื่นๆ จะมีเงื่อนไขเพิ่มตรงที่ต้องส่งข้อมูลให้ทันเวลา ไม่งั้นเสียงจะเพี้ยนหรือขาดๆ หายๆ

ภาษาเทคนิค เสียงในคุณภาพระดับที่ “พอฟังได้” จะมีขนาดข้อมูลที่ส่งประมาณ 50 กิโลไบต์ต่อวินาที ที่ต้องมี “ต่อวินาที” ด้วยแปลว่าต้องส่งให้ทันใน 1 วินาทีด้วย ไม่งั้นเสียงพูดจะยืดยานและเพี้ยน ยิ่งถ้าเป็นเสียงเพลงที่จะฟังให้เพราะหรือเป็นเสียงระบบสเตอริโอแยกซ้าย-ขวา อาจต้องเพิ่มข้อมูลที่รับส่งขึ้นไปถึง 100 -200 กิโลไบต์ต่อวินาที

- **ข้อมูลที่เป็นภาพเคลื่อนไหว (วิดีโอ)** วิดีโอที่เราดูทั่วไปนั้นถ้าจะไม่ให้กระตุกจะต้องประกอบด้วยภาพย่อยๆ ประมาณ 20-30 ภาพต่อวินาที ซึ่งเวลาส่งจะต้องบีบข้อมูลอย่างมากและยอมให้ภาพไม่คมชัดเท่าภาพนิ่ง (จะเห็นได้ว่าภาพที่ถ่ายด้วยการจับหน้าจอวิดีโอจะเบลอกว่าภาพถ่ายจริงๆ) แถมยังต้องมีเสียงด้วย ดังนั้นวิดีโอจึงกินกำลังของเครื่องและเครือข่ายมากกว่าภาพนิ่งไปอีก 20-30 เท่า

ภาษาเทคนิค วิดีโอในคุณภาพระดับที่ “ดูดี” ทั้งภาพและเสียงรวมกันจะมีขนาดประมาณ 1,000 กิโลไบต์ หรือ 1 เมกะไบต์ต่อวินาทีขึ้นไป



▲ เครือข่ายเน็ตซิมความเร็วสูง ก็เหมือนท่อน้ำที่มีขนาดใหญ่ น้ำ (ข้อมูล) ก็ไหลผ่านได้เร็วกว่าท่อเล็ก)

ดังนั้นก่อนจะบ่นว่า “เน็ตช้า” ให้ดูว่าเรากำลังรับหรือส่งข้อมูลอะไรอยู่เสียก่อน ถ้าใช้งานแค่จิ้มๆ ไม่ได้ดูหนังฟังเพลงหรือส่งรูปใหญ่ๆ ให้ใครเลย ค่อยบ่นดังๆ ออกมา ;-)

ใช้เน็ตซิมอย่างไรไม่ให้หมดโควต้า

จากหัวข้อก่อน เราได้เห็นปริมาณข้อมูลที่ต้องรับส่งสำหรับข้อมูลแต่ละประเภทแล้ว ซึ่งจะทำให้เราเข้าใจได้ว่าทำไมถึงต้องมีโควต้าที่จำกัดการใช้งานในแต่ละเดือนขึ้นมา เพราะ

- **บางคนใช้เน็ตน้อย** รับส่งข้อความเป็นหลัก มีรูปภาพบ้าง เช่นอีเมล์ แอพพวก Social เช่น Facebook, LINE
- **บางคนใช้เน็ตเยอะ** ดูหนังฟังเพลงบ่อยๆ ดู YouTube ฟังวิทยุออนไลน์ ฯลฯ ซึ่งรับส่งข้อมูลมากกว่าพวกแรกเป็นสิบเท่าร้อยเท่า

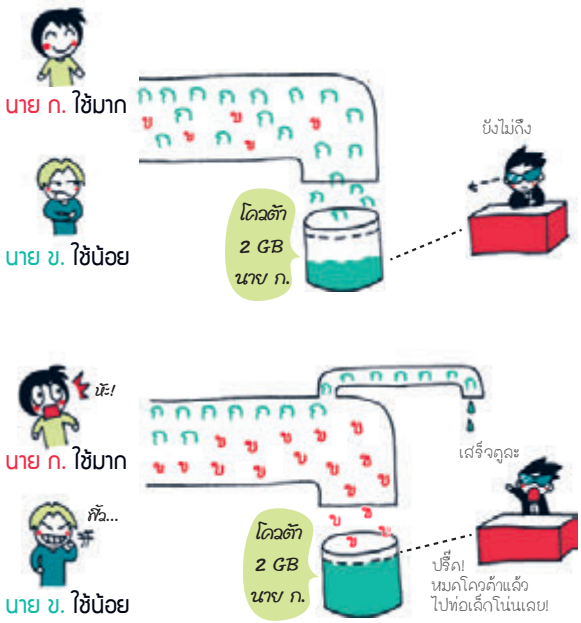
แต่สองคนนี้จ่ายค่าบริการรายเดือนเท่ากัน ซึ่งไม่แฟร์ !?!

เพราะคนที่ใช้เยอะจะเป็นภาระหรือโหลดระบบเครือข่ายมาก ทำให้คนที่ใช้น้อยพลอยใช้ไม่ออกไปด้วย

ระบบโควต้าหรือ FAIR USE POLICY (FUP) จึงเกิดขึ้น เพื่อ “จำกัดคนที่ใช้เน็ตมาก ไม่ให้มากเกินไปจนไปรบกวนผู้ใช้อื่นๆ” เพราะอย่าลืมว่านอกจากเน็ตผ่านซิมแล้ว อุปกรณ์ทุกเครื่องไม่ว่าจะเป็นสมาร์ทโฟนหรือแท็บเล็ตยังสามารถเลี่ยงไปใช้เน็ตบ้าน ที่ทำงาน ที่โรงเรียน หรือ Wi-Fi ตามที่ต่างๆ ได้ ไม่จำเป็นต้องเอางานหนักๆ มาโหลดเครือข่ายของเน็ตซิมถ้าขณะนั้นอยู่ประจำที่ ไม่ได้อยู่ระหว่างเดินทางไปมา และ Wi-Fi นี้ก็มักจะเร็วกว่าเน็ตซิมหลายเท่า นอกจากนี้ทั้ง Wi-Fi และเน็ตบ้านยังไม่มีโควต้าจำกัดว่ารับส่งข้อมูลได้แค่ไหนอีกด้วย

วิธีการของระบบโควต้านี้ก็คือ จำกัดปริมาณข้อมูลที่รับส่งว่า เดือนหนึ่งๆ จะใช้ได้**ตามความเร็วเต็มที่ของแพ็กเกจที่ซื้อ**นั้นไม่เกินเท่าไหร่ เช่น กำหนดโควต้าไว้ 2 กิกะไบต์ (ประมาณ 2,000 เมกะไบต์ คิดง่ายๆ ว่าเทียบเท่าการถ่ายรูปจากกล้องมือถือแล้วส่งต่อประมาณสองพันรูป หรือดูหนังที่ความละเอียดระดับ DVD ได้ประมาณสามสี่ชั่วโมง) ก็แปลว่า ถ้ายังรับส่งข้อมูลไม่เกินที่กำหนดจะได้ความเร็วเต็มที่ แต่ถ้ารับส่งเกินนั้นไม่ใช่ว่าเน็ตตัดเลย แต่จะถูกจำกัดสิทธิ์การใช้ที่เกินโควต้า โดยลดความเร็วลงเหลือเท่าระบบ 2G หรือ Edge ที่ช้ากว่ากันเป็นสิบเท่าแทน ทีนี้เดือนถัดๆ ไปก็จะต้องวางแผนการใช้เน็ตอย่างเหมาะสมกว่านี้ รวมทั้งทำให้เหลือที่หรือเวลาว่างของเครือข่ายให้คนอื่นใช้บ้างด้วย

ภาษาเทคนิค เช่น ปกติใช้ 3G ก็อาจได้ความเร็ว 2-3 หรือ 4 เมกะบิตต่อวินาที พอติดโควต้าก็จะลดลงสิบเท่าคือเหลือ 0.3 เมกะบิตต่อวินาทีเท่านั้น



▲ ระบบโควต้าหรือ Fair Use Policy (FUP) เพื่อให้คนที่ใช้มากและใช้น้อยสามารถใช้งานร่วมกันได้อย่างเป็นธรรมเท่าเทียมกัน เพราะจ่ายเท่ากัน

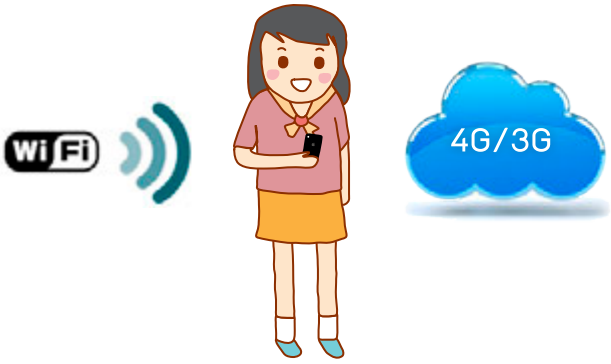
ต่อเน็ตแบบไหน เมื่อไหร่ดี

ถ้าไม่ได้ใช้เน็ตซิมก็จะใช้อินเทอร์เน็ตได้เมื่อบริเวณนั้นมี Wi-Fi ให้เข้าใช้งานเท่านั้น ซึ่งส่วนใหญ่ก็มักจะล็อคไว้จะต้องใส่รหัสผ่านก่อนเข้าใช้ เมื่อเปิดใช้ Wi-Fi สมาร์ทโฟนหรือแท็บเล็ตก็จะตรวจหาสัญญาณในบริเวณนั้นแล้วเชื่อมต่อให้เข้าไปใช้ได้ทันที (ครั้งแรกอาจต้องใส่รหัสผ่านก่อน ซึ่งเจ้าของระบบ Wi-Fi มักมีป้ายบอกไว้ เช่น ในร้านกาแฟ) ถ้าเป็น Wi-Fi ที่ไม่ต้องใส่รหัสผ่านให้ระวังอาจเป็น Wi-Fi ที่มิจฉาชีพเปิดไว้ล่อเหยื่อเพื่อการดักจับข้อมูล (ดูหน้า 187)

หลังจากที่เข้าใช้ในครั้งแรกได้แล้ว ครั้งต่อไปถ้าเปิดใช้ Wi-Fi ในอุปกรณ์ไว้ก็จะเข้าใช้ Wi-Fi ที่เคยใช้งานนั้นให้อัตโนมัติ แม้ว่าคุณจะใช้ “เน็ตซิม” อยู่แล้วก็ตาม เพื่อลดปริมาณการใช้อินเทอร์เน็ตจาก “เน็ตซิม” ที่จำกัดปริมาณข้อมูลที่ใช้ได้ในแต่ละเดือน นอกจากนี้การใช้ Wi-Fi แทนยังประหยัดแบตกว่าอีกด้วย

มี Wi-Fi ก็ใช้ก่อน ประหยัดเน็ตซิมไว้ ออกนอกสถานที่ค่อยใช้

เมื่ออยู่ในที่ๆไม่มี Wi-Fi ให้ใช้งาน อุปกรณ์จะสลับไปใช้เน็ตซิมโดยอัตโนมัติ (ต้องเปิดใช้งานคำสั่ง Cellular Data ของอุปกรณ์นั้นๆ เอาไว้ด้วย) หรือถ้าคุณไม่ต้องการใช้บริการเน็ตผ่านผู้ให้บริการมือถือก็ควรไปปิดการใช้งาน Cellular Data เพื่อป้องกันการใช้เน็ตอัตโนมัติโดยที่เราไม่รู้ตัว (บางแอพหรือ service ในโทรศัพท์จะใช้งานอินเทอร์เน็ตอยู่เบื้องหลัง -ดูหน้า 34) ซึ่งถ้าเป็นกรณีที่ไม่ได้สมัครแพ็กเกจเน็ตของผู้ให้บริการไว้ก็จะเสียค่าบริการในอัตราที่แพงกว่าปกติ

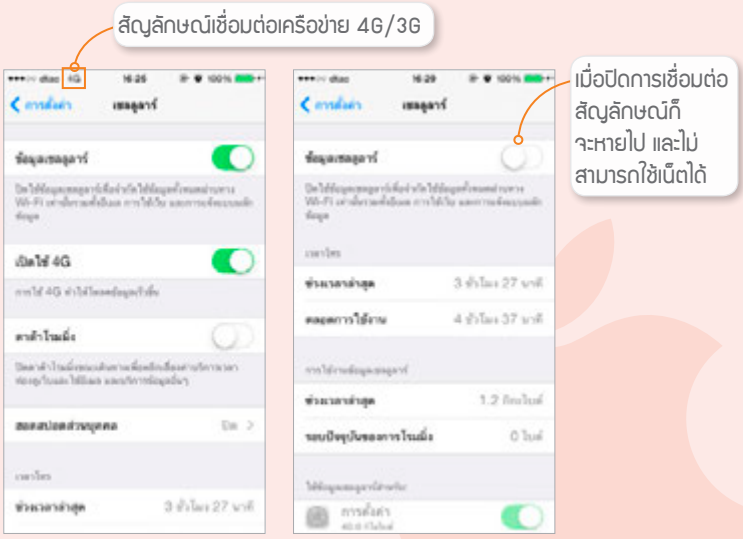


เปิด-ปิดเน็ตบนอุปกรณ์ได้อย่างไร

ถ้าใช้เน็ตซิมแพ็กเกจแบบจำกัดชั่วโมงหรือปริมาณข้อมูล ก็จำเป็นจะต้องคอยเปิด-ปิดการทำงานของอินเทอร์เน็ตเองเพื่อป้องกันไม่ให้อุปกรณ์เรียกใช้อินเทอร์เน็ตโดยที่คุณไม่รู้ตัว โดยวิธีเปิด-ปิดเน็ตในอุปกรณ์จะทำได้ดังนี้

iOS ไปที่ **การตั้งค่า** ▸ **เซลลูลาร์** (**Settings** ▸ **Cellular**) ให้แตะปุ่มเปิดใช้งานที่ **ข้อมูลเซลลูลาร์** (**Cellular Data**) เพื่อเชื่อมต่อเน็ตผ่านเครือข่าย จะแสดงสัญลักษณ์ เช่น **E**, **3G** หรือ **4G** บนแถบสถานะด้วย จากนั้นให้แตะปุ่มเปิดใช้งานที่ **เปิดใช้ 4G** (**Enable 4G**) หรือ **เปิดใช้ 3G** (**Enable 3G**) (แล้วแต่เครื่องที่ใช้งานว่ารองรับ 4G หรือไม่) เพื่อเชื่อมต่อเน็ตผ่าน 4G/3G จะแสดงสัญลักษณ์ 4G/3G บนแถบสถานะ

- เมื่อต้องการปิดการเชื่อมต่อเน็ตซิม ให้แตะปุ่มปิดใช้งาน ข้อมูลเซลลูลาร์ (Cellular Data) ตามรูปขวา สัญลักษณ์ **E** หรือ **4G/3G** ก็จะหายไป



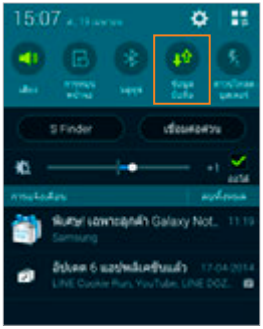
Android

Android แตะไอคอน **การตั้งค่า** ▸ **เครือข่ายเพิ่มเติม** ▸ **เครือข่ายมือถือ** (Settings ▸ More networks ▸ Mobile networks) แล้ว ✔ เลือก **ข้อมูลมือถือ** (Mobile data)

หรืออีกวิธีหนึ่งให้แตะที่แถบสถานะด้านบนแล้วลากลงล่าง จากนั้นแตะปุ่ม **ข้อมูลมือถือ** (Mobile data) ให้เป็นสีเขียวเพื่อเปิดการต่ออินเทอร์เน็ตผ่าน 4G/3G/EDGE/GPRS

ที่แถบสถานะจะเห็นสัญลักษณ์ 3G เชื่อมต่ออินเทอร์เน็ตความเร็วสูงด้วย 3G หรือ H+ เชื่อมต่อแบบ HSPDA (3.5 Mbps) และ H+ คือ HSPDA+ (7 Mbps) หรือ E เชื่อมต่อด้วย EDGE และลูกศรจะเปลี่ยนสีตามการทำงานขณะที่รับส่งข้อมูล

เมื่อต้องการปิดการเชื่อมต่อ ให้ยกเลิกที่ **ข้อมูลมือถือ** (Mobile data) หรือแตะที่แถบสถานะด้านบนแล้วลากลงล่าง จากนั้นแตะปุ่ม **ข้อมูลมือถือ** (Mobile data) ให้เป็นสีเทา



ใช้เน็ตตลอดเวลาแม้ไม่ได้ใช้งานเครื่อง

อุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS และ Android นั้นจะมีแอพและบริการของระบบที่ทำงานอยู่ตลอดเวลาแม้ว่าคุณจะปิดหน้าจอไว้ ซึ่งบางเวลาก็อาจต้องการเชื่อมต่อกับอินเทอร์เน็ตเพื่อทำงานบางอย่าง โดยจะทำงานอยู่เบื้องหลังตลอดเวลาถึงแม้ว่าจะไม่ได้เปิดใช้แอพ เช่น การอัพเดทแอพอัตโนมัติ, การแจ้งเตือนต่างๆ (notification), ดึงอีเมล์ใหม่ เป็นต้น ถ้าอุปกรณ์นั้นต่ออินเทอร์เน็ต แอพและบริการต่างๆ ก็จะรับส่งข้อมูลจากอินเทอร์เน็ตอยู่ตลอด เพื่อให้คุณไม่พลาดข้อมูลสำคัญ ซึ่งการทำงานตลอดเวลานี้อาจทำให้เปลืองแบตเตอรี่และเปลืองเน็ต ซึ่งคุณสามารถปิดการทำงานนี้ได้ทั้งใน iOS และ Android ดังนี้

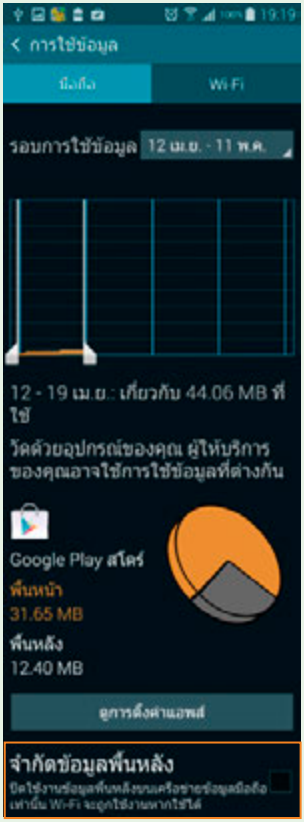
iOS เป็นการอนุญาตให้แอพต่างๆ ที่ทำงานอยู่เบื้องหลังสามารถดึงข้อมูลมาอัพเดทได้ตลอดเวลาที่เชื่อมต่อ Wi-Fi หรือ 4G/3G รวมถึงการดึงข้อมูลแสดงพิกัดตำแหน่งที่อยู่ โดยเลือกปิดบางแอพที่ไม่จำเป็นได้ ซึ่งจะช่วยประหยัดแบตเตอรี่และทำให้เครื่องหน่วงน้อยลงได้ด้วย โดยไปที่ **การตั้งค่า ▸ ทั่วไป ▸ ดึงข้อมูลใหม่อยู่เบื้องหลัง** (Settings ▸ General ▸ Background App Refresh)

เปิดให้แอพที่เลือกดึงข้อมูลผ่านอินเทอร์เน็ตได้ หรือปิดไม่ให้แอพที่ทำงานเบื้องหลังใดๆ ดึงข้อมูลผ่านอินเทอร์เน็ตได้

เปิด/ปิดการดึงข้อมูลผ่านอินเทอร์เน็ตในขณะที่ทำงานอยู่เบื้องหลังของแต่ละแอพ

Android

Android สามารถตั้งค่าการใช้อินเทอร์เน็ตอยู่เบื้องหลังได้ โดยให้ทำงานเฉพาะตอนที่เชื่อมต่อแบบ Wi-Fi เท่านั้น เพื่อประหยัดปริมาณการใช้แพ็กเกจอินเทอร์เน็ตในมือถือ

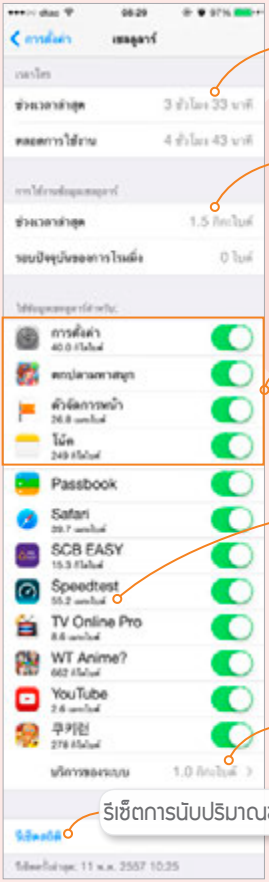


แตะไอคอน **การตั้งค่า** ▸ **การใช้ข้อมูล** (Settings ▸ Data usage) เลื่อนหน้าจอลงไปด้านล่างแล้วแตะเลือกแอพที่ต้องการปิดการใช้อินเทอร์เน็ต Mobile ขณะทำงานอยู่เบื้องหลัง แตะ ☑ เลือก **จำกัดข้อมูลพื้นหลัง** (Restrict background data) แล้วแตะ **ตกลง** (OK)

เช็คได้ว่าใช้เน็ตไปมากแค่ไหนแล้ว

เมื่อเปิดอินเทอร์เน็ตบนมือถือ คุณสามารถตั้งค่าการเชื่อมต่ออินเทอร์เน็ตผ่านเครือข่ายผู้ให้บริการเพิ่มเติมได้อีก รวมทั้งเช็คได้ว่าใช้เน็ตไปมากแค่ไหนแล้ว ดังนี้

iOS



ดูเวลาทั้งหมดที่ใช้สนทนาไป

ดูปริมาณการรับส่งข้อมูล สำหรับใช้ตรวจสอบปริมาณการใช้เน็ต กรณีที่ไม่ได้ใช้แพ็กเกจ Unlimited

เปิด/ปิดแอพที่จะยอมให้ใช้อินเทอร์เน็ตจากเครือข่ายมือถือได้ ถ้าปิดไว้แอพนั้นจะใช้อินเทอร์เน็ตจาก Wi-Fi อย่างเดียว

แสดงปริมาณการใช้อินเทอร์เน็ตของแอพและบริการต่างๆ แตะปุ่มเปิดปิดการใช้อินเทอร์เน็ตของแต่ละแอพและบริการได้

ดูปริมาณข้อมูลที่ใช้โดยบริการของระบบ

รีเซ็ตการนับปริมาณข้อมูลใหม่

Android

Android แตะไอคอน **การตั้งค่า** ▸ **การใช้ข้อมูล** (Settings ▸ Data usage) แล้วแตะ ☑ **ข้อมูลมือถือ** (Mobile data) และแตะ ☑ **ตั้งค่าขีดจำกัดข้อมูลมือถือ** (Set mobile data limit) จะแสดงกราฟปริมาณการใช้ข้อมูล 4G/3G/EDGE/GPRS ดังรูป

Android

จำกัดปริมาณการใช้อินเทอร์เน็ตในเน็ตซิม

ใน Android จะสามารถจำกัดปริมาณการใช้อินเทอร์เน็ตในเน็ตซิมได้ โดยจะแจ้งเตือนเมื่อใช้อินเทอร์เน็ตจนใกล้ถึงปริมาณที่ตั้งไว้ โดยจะมีวิธีจำกัดปริมาณการใช้อินเทอร์เน็ตในเน็ตซิมดังนี้

1 แตะ ☑ เลือก **ตั้งค่าขีดจำกัดข้อมูลมือถือ** (Set mobile data limit) แสดงข้อความการกำหนดขอบเขตการใช้ข้อมูล แล้วแตะ **ตกลง** (OK)

2 ตั้งวันที่ระหว่างรอบบิลให้แตะที่ **รอบการใช้ข้อมูล** (Data usage cycle) เลือกวันที่เริ่มรอบบิลของแต่ละเดือน

3 แตะ ▬ แล้วลากกำหนดระดับการใช้งานสูงสุด เช่น 2 GB

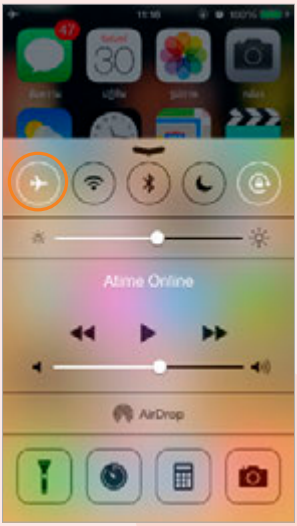
4 แตะ ▬ แล้วลากกำหนดระดับการแจ้งเตือนล่วงหน้าก่อนถึงกำหนด เช่น 1.5 GB เป็นต้น

ปิดสัญญาณวิทยุเวลาขึ้นเครื่องบิน

iOS และ Android มีโหมดการใช้งานที่เรียกว่า Airplane Mode (โหมดเครื่องบินใน iOS หรือโหมดการบินใน Android) ซึ่งจะปิดระบบส่งสัญญาณวิทยุทั้งหมด ไม่ว่าจะเป็นสัญญาณโทรศัพท์, Wi-Fi และ Bluetooth เพื่อหลีกเลี่ยงการไปรบกวนระบบสื่อสารของเครื่องบิน รวมทั้งเครื่องมือทางการแพทย์ในโรงพยาบาลด้วย แต่เรายังสามารถใช้งานเพื่อดูหนัง ฟังเพลง หรือการใช้งานอื่นๆ ที่ไม่เกี่ยวข้องกับการส่งสัญญาณวิทยุได้บนเครื่องบินและในโรงพยาบาลโดยที่ไม่ต้องปิดเครื่อง

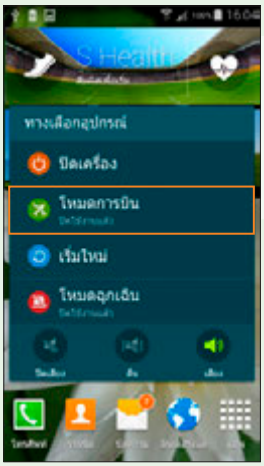
iOS

iOS แตะ **การตั้งค่า** (**Settings**) แตะปุ่มเปิดใช้งานที่ **โหมดเครื่องบิน** (**Airplane Mode**) หรือแตะขอบจอด้านล่างแล้วแตะลากขึ้นเพื่อเปิด Control Center ขึ้นมา แล้วแตะ  เปิดใช้โหมดเครื่องบิน หรือแตะซ้ำเพื่อปิดโหมดเครื่องบินเมื่อลงจากเครื่องแล้ว



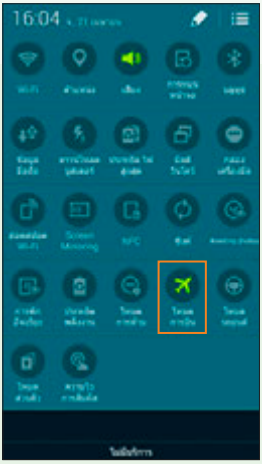
Android

Android จะเปิด-ปิดโหมดการบินได้หลายวิธีดังนี้

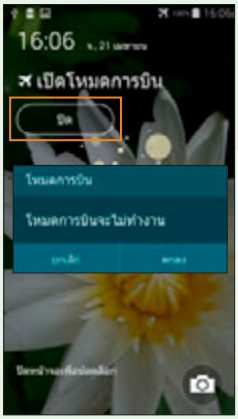


วิธีที่ 1 กดปุ่ม **Power** ค้างไว้ จนปรากฏคำสั่งขึ้นมา แตะ **โหมดการบิน** (Airplane mode) แล้วแตะ **ตกลง** (OK) ก็จะเข้าสู่โหมดการบิน โดยจะแสดงสัญลักษณ์ ✈ บนแถบสถานะ

วิธีที่ 2 แตะลากแถบสถานะที่ขอบจอด้านบนลงมา แตะ ⚙ แล้วแตะที่ **โหมดการบิน** (Airplane mode)จะมีสถานะเป็นสีเขียว (เปิด) หากต้องการยกเลิกโหมดนี้ให้แตะซ้ำอีกครั้งเป็นสีเทา (ปิด)



วิธีที่ 3 ไปที่ **การตั้งค่า** (Settings) แตะ **โหมดการบิน** (Airplane mode) จากนั้นแตะเปิดใช้งาน ▮ ที่ **โหมดการบิน** (Airplane mode) แล้วแตะ **ตกลง** (OK)



กลับไปใช้โหมดปกติ ให้ปิดการทำงานที่ **การตั้งค่า** (Settings) หรือกดปุ่ม **Power** ค้างไว้ แตะ **โหมดการบิน** (Airplane mode) แล้วแตะ **ปิด** (OFF) หรือปิดในหน้า Lock screen โดยแตะปุ่ม **ปิด** (OFF) แล้วแตะ **ตกลง** (OK)

นำมือถือไปใช้ในต่างประเทศได้อย่างไร?

เวลานำมือถือติดตัวเดินทางไปต่างประเทศจะมีการเชื่อมต่อเน็ตผ่านผู้ให้บริการของประเทศนั้นๆ ที่เรียกว่า Data Roaming ซึ่งปกติคิดค่าบริการแพงมหาโหด ดังนั้นจึงควรปิดการใช้งาน Data Roaming นี้เอาไว้ (ถ้าเผลอเปิดทิ้งไว้แล้วเกิดกรณีที่เข้าใช้อินเทอร์เน็ตโดยไม่ได้ตั้งใจอาจทำให้เสียค่าบริการหลักหมื่น แสน หรือล้านบาทได้!) แต่ถ้าคุณต้องการใช้เน็ตที่ต่างประเทศด้วยก็สามารถแจ้งเปิดใช้บริการ Data Roaming ผ่านค่ายมือถือของไทยไว้ก่อนได้ ซึ่งจะมีราคาถูกกว่ามาก แนะนำให้สมัครแพ็กเกจ Data Roaming แบบไม่จำกัดหรือ Unlimit ของผู้ให้บริการเดิมที่ใช้อยู่ ซึ่งจะเสียแต่ค่าบริการรายวันตามราคาแพ็กเกจที่ใช้ประมาณวันละ 3-4 ร้อยบาทเท่านั้น

ใช้อินเทอร์เน็ตในต่างประเทศด้วยอุปกรณ์ iOS

เปิดใช้ Data Roaming

เมื่อสมัครแพ็กเกจกับผู้ให้บริการไว้แล้ว ตอนเปิดใช้ให้ไปที่ **การตั้งค่า** ▸ **เซลลูลาร์** (Settings ▸ Cellular) เปิดใช้งานที่ **ข้อมูลเซลลูลาร์** (Cellular Data) และ **ดาต้าโรมมิ่ง** (Data Roaming)

หลังจากเปิดใช้ Data Roaming แล้ว ให้เข้าไปเลือกเครือข่ายผู้ให้บริการในประเทศนั้นๆ (**ระวัง!!** *ต้องเลือกให้ตรงกับที่ผู้ให้บริการแจ้งไว้ด้วย ถ้าเลือกผิดอาจเสียค่าบริการมหาศาลได้*) ให้ไปที่ **การตั้งค่า** ▸ **ผู้ให้บริการ** (Settings ▸ Carrier) ปิดใช้งานที่ **อัตโนมัติ** (Automatic) จากนั้นเลือกเครือข่ายผู้ให้บริการในประเทศนั้นด้วยตัวเอง *อย่าลืมปล่อยเป็นอัตโนมัติเด็ดขาด!* (ดูวิธีในหัวข้อถัดไป)

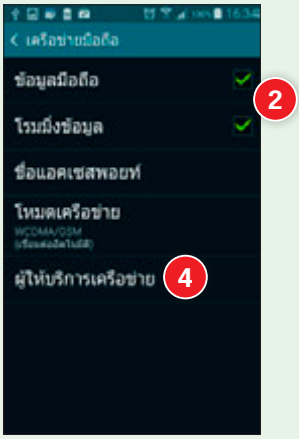
ปิด Data Roaming

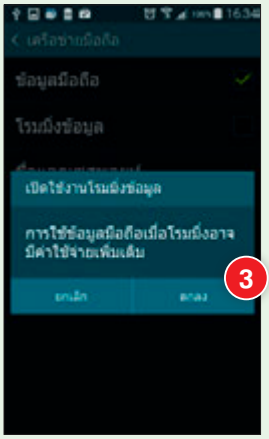
เมื่อไม่ใช้งานแล้วให้แตะปุ่มปิดที่ **ดาต้าโรมมิ่ง** (Data Roaming)

Android

ใช้อินเทอร์เน็ตในต่างประเทศด้วยอุปกรณ์ Android

เปิดใช้ Data Roaming





1 ไปที่ **การตั้งค่า** ▸ **เครือข่ายเพิ่มเติม** ▸ **เครือข่ายมือถือ** (Settings ▸ More networks ▸ Mobile networks)

2 แตะ ☑ เลือกทั้ง **ข้อมูลมือถือ** (Mobile data) และ **โรมมิ่งข้อมูล** (Data roaming) (ถ้าไม่ได้ซื้อแพ็กเกจ Data roaming ให้ยกเลิกทั้งสองข้อ!)

3 แจ้งเตือนว่าการโรมมิ่งจะเสียค่าใช้จ่ายเพิ่มจากปกติ ให้แตะปุ่ม **ตกลง** (OK)

4 แตะ **ผู้ให้บริการเครือข่าย** (Network operators) จะค้นหารายชื่อสักครู่ใหญ่ๆ แล้วเลือกชื่อ Operator ให้ตรงกับแพ็กเกจที่ซื้อไว้ (*ห้ามเลือกผิด*) และห้ามเลือก เลือกโดยอัตโนมัติ (Select automatically) เด็ดขาด (ดูหน้าถัดไป)

ปิด Data Roaming

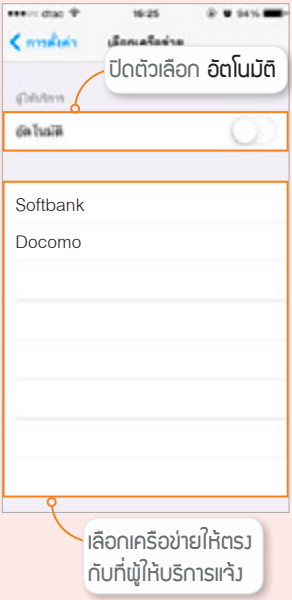
เมื่อไม่ใช้งานแล้วให้ยกเลิกการทำงานที่ **โรมมิ่งข้อมูล** (Data roaming)

ระวังการเลือกผู้ให้บริการในต่างประเทศ

เมื่อเดินทางต่างประเทศและเปิดเครื่องไว้ ถ้าเปิดการเลือกเครือข่ายอัตโนมัติเอาไว้ อุปกรณ์จะค้นหาแล้วเลือกเครือข่ายที่ดีที่สุดในขณะนั้นให้ทันที และเมื่อคุณอยู่ในบริเวณที่มีสัญญาณอ่อน โทรศัพท์มือถือก็จะเลือกเครือข่ายใหม่ที่สัญญาณแรงกว่าให้โดยอัตโนมัติ ซึ่งอาจไม่ตรงกับเครือข่ายที่อยู่ในแพ็กเกจใช้งาน ทำให้เสียค่าบริการแพงกว่าปกติ คุณจึงต้องปิดการค้นหาและเลือกเครือข่ายอัตโนมัติ แล้วเลือกเครือข่ายตามเงื่อนไขของแพ็กเกจด้วยตนเอง ซึ่งในเครื่อง iOS กับ Android จะมีขั้นตอนการเลือกผู้ให้บริการดังนี้

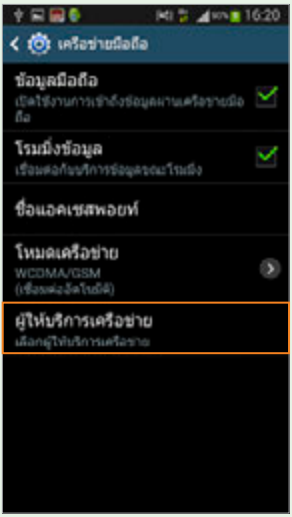
iOS

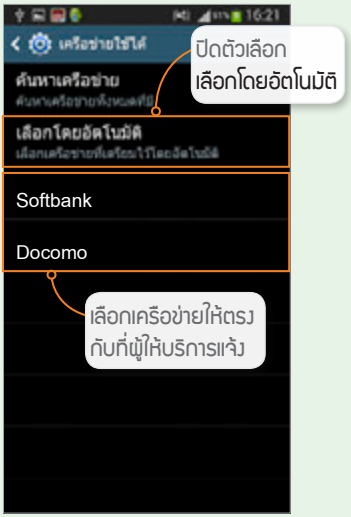
iOS การเลือกเครือข่ายผู้ให้บริการในประเทศนั้นๆ ต้องเลือกให้ตรงกับที่ผู้ให้บริการแจ้งไว้ด้วย ให้ไปที่ **การตั้งค่า** ▸ **ผู้ให้บริการ** (**Settings** ▸ **Carrier**) ปิดใช้งานที่ **อัตโนมัติ** (**Automatic**) จากนั้นเลือกเครือข่ายผู้ให้บริการในประเทศนั้นด้วยตัวเอง อย่าลืมปิดเด็ดขาด!



Android

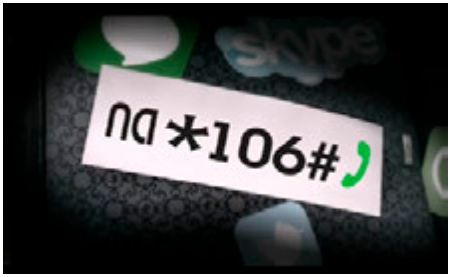
หลังจากเปิด Data Roaming โดยไปที่ **การตั้งค่า** ▸ **เครือข่ายเพิ่มเติม** ▸ **เครือข่ายมือถือ** (**Settings** ▸ **More networks** ▸ **Mobile networks**) แล้วให้แตะ **ผู้ให้บริการเครือข่าย** (**Network operators**) จะค้นหารายชื่อสักครู่ใหญ่ๆ แล้วเลือกชื่อผู้ให้บริการให้ตรงกับแพ็กเกจที่ซื้อไว้ *ห้ามเลือกผิดและห้ามเลือก เลือกโดยอัตโนมัติ (Select automatically) เด็ดขาด*





- หากไม่ได้เปิดใช้แพ็กเกจ Data Roaming ไปจากเมืองไทย คุณอาจซื้อซิมการ์ดที่ต่างประเทศใช้ชั่วคราว ซึ่งอาจจำกัดจำนวนนาทีในการโทรต่างประเทศ โทรในประเทศนั้นๆ และอาจรวมหรือไม่รวมบริการรับส่งข้อมูลก็ได้ (บางประเทศต้องสมัครเพิ่มและเติมเงินเข้าไปเอง ขึ้นกับซิมนั้นๆ ว่ามีเงื่อนไขอย่างไร) ต้องตรวจสอบจากผู้ให้บริการของซิมนั้นๆ อีกที
- ในกรณีที่ต้องการความเร็วระดับ 4G การเปิด Data Roaming บางประเทศมักไม่รองรับ อาจต้องไปซื้อซิมของประเทศนั้นๆ หรือเช่าอุปกรณ์ Wi-Fi Router รุ่นที่รองรับ 4G ในประเทศนั้นๆ แทน

ปิดเน็ตก่อนไปต่างประเทศแบบใช้ได้ทุกเครื่อง



หลายคนที่นำโทรศัพท์ไปใช้งานในต่างประเทศแม้ไม่ได้ใช้เน็ตแต่ไม่ได้ไปปิด กลับมาก็มีการเรียกเก็บค่าบริการ (เนื่องจากมีแอพที่ทำงานอยู่เบื้องหลังอาจใช้เน็ตโดยที่คุณไม่รู้ตัว) บางคนเปิดแพ็กเกจใช้เน็ตในต่างประเทศแล้วแต่เลือกผู้ให้บริการผิดราย ก็อาจโดนเรียกเก็บค่าบริการมหาศาลได้ ถ้าไม่มั่นใจหรือไม่ต้องใช้ก็แนะนำให้สั่งปิดเองเสมอ

กด *106# แล้วกดโทรออก

นอกจากนี้แม้ว่าไปแค่บริเวณเขตชายแดนของไทยก็อาจมีการสลับไปใช้เครือข่ายของประเทศเพื่อนบ้านโดยอัตโนมัติได้ ด้วยเหตุนี้ทำให้มีการร้องเรียนจากผู้ใช้บริการหลายราย ทาง กสทช. จึงได้กำหนดหมายเลข ***106# แล้วกดโทรออก** ให้ผู้ใช้สามารถปิดการใช้เน็ตบนมือถือผ่านผู้ให้บริการในต่างประเทศได้ทั้ง AIS, DTAC และ TRUE ได้โดยไม่เสียค่าใช้จ่าย ซึ่งจะส่งข้อความยืนยันการปิดบริการและวิธีเปิดใช้เมื่อกลับมาถึงไทยให้ทราบด้วย

หรืออีกวิธีหนึ่ง ให้ปิดเน็ต Data Roaming ที่ผู้ให้บริการโดยตรง ป้องกันการใช้เน็ตในต่างประเทศโดยไม่ตั้งใจ โดยโทรแจ้ง call center ของแต่ละค่าย หรือกดรหัสดังนี้

DTAC : ปิด *124*3# เปิด *124*4#

AIS : ปิด *129*1# เปิด *129*2# ตรวจสอบ *129#

TRUE : ปิด/เปิด *9399 **หรือ** 1331

CHAPTER 3

ระวังอันตราย เรื่องข้อมูลส่วนตัว

ปัจจุบันเป็นเรื่องสะดวกสบายที่จะชำระเงิน โอน ซื้อของ ผ่านอินเทอร์เน็ต สามารถทำได้โดยไม่ต้องออกจากบ้านไปที่ธนาคารหรือตู้ ATM เพียงแค่ต้องกรอกข้อมูลทางการเงินต่างๆ หรือล็อกอินด้วยชื่อและรหัสผ่านที่สมัครใช้งาน Internet Banking กับแต่ละธนาคารเอาไว้เพื่อเข้าไปทำธุรกรรม ซึ่งก็เคยมีกรณีหน้าเว็บปลอม หลอกให้กรอกชื่อและรหัสผ่านแล้วขโมยไปใช้งาน จึงควรใช้ความระมัดระวังและต้องสังเกตความผิดปกติบนหน้าเว็บอยู่เสมอก่อนที่จะกรอกข้อมูลส่วนตัวใดๆ

การโพสต์ข้อมูลส่วนตัวว่าตอนนี้อยู่ที่ไหน กำลังทำอะไร อยู่กับใคร ฯลฯ บน Social Network ต่างๆ นั้น อย่าลืมว่าถึงอย่างไรเว็บออนไลน์เหล่านี้ก็ไม่ใช่พื้นที่ส่วนตัว อาจเป็นการเปิดช่องให้มิจฉาชีพหรือผู้ประสงค์ร้ายเข้ามาหาประโยชน์จากข้อมูลที่คุณเป็นผู้ป่าวประกาศบอกผู้คนทั้งโลกได้เป็นอย่างดี ก่อนโพสต์อะไรก็ควรคิดให้มากๆ เพื่อป้องกันอันตรายที่อาจเกิดขึ้นได้

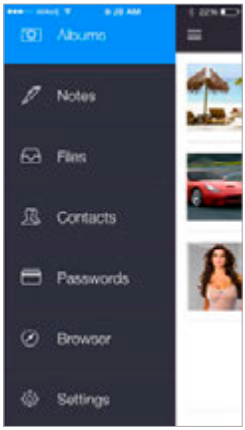
ข้อมูล ส่วนตัวควรเป็นความลับ

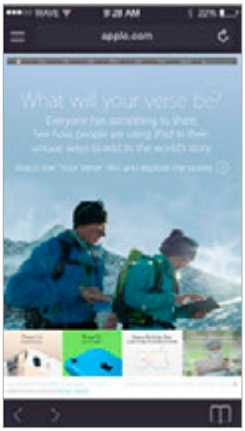
การกรอกข้อมูลส่วนตัว ไม่ว่าจะเป็น รูปภาพ ภาพถ่ายบัตรประชาชน เลขประจำตัวประชาชน วันเดือนปีเกิด หมายเลขโทรศัพท์ ที่อยู่ เลขที่บัญชี เลขบัตรเครดิต หรืออื่นๆ ในเว็บให้บริการด้านต่างๆ และสื่อสังคมออนไลน์ เช่น Facebook, Twitter จะต้องใช้ความระมัดระวังเป็นอย่างมาก เว็บนั้นจะต้องมีความน่าเชื่อถือว่าจะไม่นำข้อมูลของคุณไปเปิดเผย หรือนำไปใช้ในทางที่ไม่เหมาะสม ถ้าไม่แน่ใจอาจลองค้นหาข้อมูลของเว็บนั้นจาก Google ว่ามีความเสี่ยงหรือมีชื่อเสียงเสียๆ หายๆ เกี่ยวกับการนำข้อมูลผู้ใช้ไปเปิดเผยหรือไม่ เพื่อป้องกันไม่ให้มีปัญหาในภายหลัง

นอกจากนี้การถ่ายภาพเอกสารสำคัญต่างๆ อย่างเช่น บัตรประชาชน บัตรเครดิต หรือภาพส่วนตัวลับเฉพาะอื่นๆ รวมถึงการจดชื่อผู้ใช้และรหัสผ่านสำหรับเข้าใช้บริการต่างๆ ไว้ในเครื่องก็อาจเป็นอันตราย ถ้าเครื่องหายหรือวางทิ้งไว้ไม่ได้ใส่รหัสล็อค ใครๆ ก็สามารถเปิดดูแล้วขโมยรูปนั้นไปได้เลย นอกจากนี้ถ้ามีการเปิดให้อัพโหลดรูปภาพไปเก็บไว้บนบริการ Cloud ทั้งระบบ iOS ของ Apple และระบบ Android ของ Google หรือแม้แต่ Facebook ถ้าเปิดให้อัพโหลดรูปอัตโนมัติไว้ก็จะแชร์ไปยังอุปกรณ์ต่างๆ ที่ล็อกอินด้วยแอคเคาท์เดียวกันนั้นไว้ได้ด้วยโดยอัตโนมัติ ซึ่งบางทีเราอาจจำไม่ได้ว่าเคยไปใช้เครื่องไหนค้างไว้บ้าง ล็อกอินแล้วได้ล็อกเอาท์ออกมาหรือยัง จึงควรระวังไว้ให้มาก

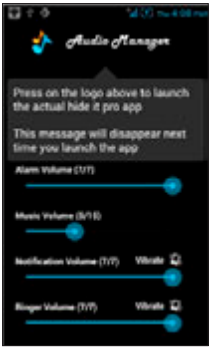
ซ่อนข้อมูลในเครื่อง

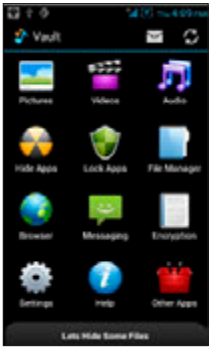
ใน iOS และ Android จะมีแอพที่ช่วยซ่อนข้อมูลลับของคุณไม่ให้ใครเห็นได้ถ้าไม่รู้รหัสผ่าน เช่น ใน iOS จะมีแอพ **Fake Calculator** หรือ **Private Calculator** เมื่อเปิดเข้าใช้แอพก็จะมีหน้าตาและทำงานเหมือนกับเครื่องคิดเลขทั่วไป แต่เมื่อใส่ตัวเลขตรงกับรหัสผ่านก็จะเข้าใช้แอพในโหมดลับได้ โดยจะซ่อนได้ทั้งรูปภาพ, คลิปวิดีโอ, รายชื่อ Contact, ข้อความ, รหัสผ่าน, ไฟล์ต่างๆ บางแอพยังสามารถใช้เปิดเว็บด้วยบุ๊คมาร์คลับที่ไม่อยากให้ใครเห็นได้ด้วย





สำหรับ Android ของเครื่อง Samsung จะมีโหมดส่วนตัว (Private mode) สำหรับเก็บข้อมูลลับอยู่แล้ว โดยให้มาพร้อมกับระบบปฏิบัติการเวอร์ชั่น 4.4.2 แต่ถ้าใช้ Android รุ่นอื่นก็สามารถหาแอพช่วยซ่อนข้อมูลอื่นๆ มาใช้งานได้ เช่น แอพ **Hide It Pro** ซึ่งจะทำตัวเป็นแอพ Audio Manager ใช้ดูหนังฟังเพลงบังหน้า เบื้องหลังจะช่วยซ่อนไฟล์ลับ ทั้งรูปภาพ วิดีโอ ข้อความ ไอคอนแอพ และอื่นๆ โดยจะต้องแตะค้างที่ชื่อ Audio Manager เพื่อเข้าใช้โหมดลับ

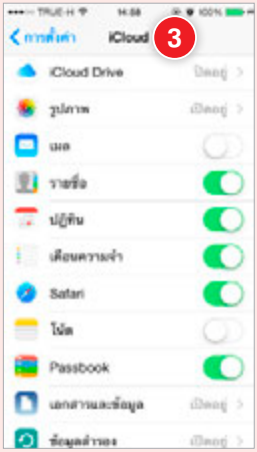




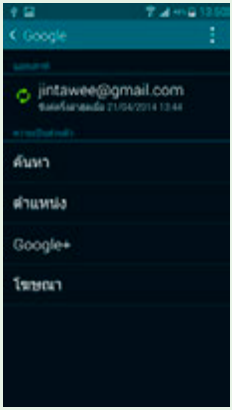
ระวังข้อมูลอัพขึ้น Cloud ไม่รู้ตัว

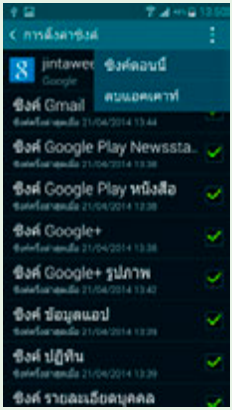
iOS ใน iOS จะมี iCloud ซึ่งเป็นบริการซิงค์ข้อมูลต่างๆ ไปเก็บไว้บน Cloud ให้สามารถดึงมาใช้ในเครื่องอื่นหรือเครื่องที่ซื้อใหม่ได้สะดวก ไม่ว่าจะเป็นรายชื่อในเครื่อง, ปฏิทินนัดหมาย, รายการแจ้งเตือน, บุ๊คมาร์คในแอพ Safari, ข้อความใน Notes, รูปภาพที่ถ่ายด้วย iPhone หรือ iPad ซึ่งเครื่องจะคอยซิงค์ข้อมูลที่แก้ไขในเครื่องขึ้นไปอัพเดทข้อมูลบน Cloud ให้ตรงกันอยู่เสมอ โดยสามารถไปเปิด-ปิดแต่ละรายการได้ดังนี้

1. แตะไอคอน **การตั้งค่า** (Settings) ▸ **iCloud**
2. พิมพ์แอคเคาท์และรหัสผ่านที่สมัครไว้ลงไป เสร็จแล้วแตะปุ่ม **ลงชื่อเข้า** (Sign In) ถ้าล็อกอินไว้แล้วให้ข้ามไป
3. แตะปุ่มเปิด-ปิดตัวเลือกต่างๆ เพื่อซิงค์หรือยกเลิกการซิงค์ข้อมูลนั้นกับ iCloud ได้ตามต้องการ ไม่ว่าจะเป็นรายชื่อ Contact ในเครื่อง, รายการนัดหมาย, โน้ตที่จดบันทึก, บุ๊คมาร์คในแอพ Safari, รูปภาพหรือวิดีโอที่ถ่ายด้วยกล้องหรือจับภาพหน้าจอ เป็นต้น



Android สำหรับ Android ข้อมูลจะซิงค์กับแอคเคาท์ Google โดยให้เข้าไปที่ **การตั้งค่า** ▸ **แอคเคาท์** (Settings ▸ Accounts) แตะ Google account เข้าไปเปิด-ปิดการซิงค์ข้อมูลต่างๆ เช่น ปฏิทิน, สมุดโทรศัพท์, Gmail ฯลฯ





ความลับไม่มีในโลก (อินเทอร์เน็ต)

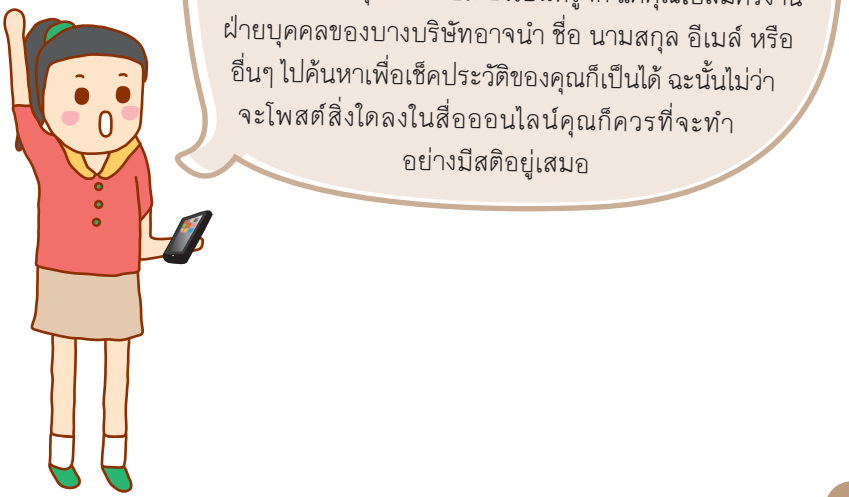
เมื่อปี 2012 มีข่าวในระดับโลกเกี่ยวกับการที่นาย Edward Snowden เจ้าหน้าที่หน่วยงาน NSA ของสหรัฐฯ ออกมาเปิดโปงถึงโครงการ PRISM ของ NSA ที่มีการดักฟังข้อมูลบนอินเทอร์เน็ตจากทั่วโลก ด้วยเหตุผลด้านความมั่นคงของชาติ แต่โดยไม่ชอบด้วยกฎหมาย จนทำให้เจ้าตัวถูกคาดโทษว่าเป็นผู้ทรยศและถึงกับต้องขอลี้ภัยไปอยู่รัสเซีย และยังทำให้มีคนอื่นๆ พากันเปิดโปงโครงการต่างๆ ที่ทำโดยหน่วยงานของรัฐในลักษณะที่กว้างขวางและคล้ายคลึงกันอย่างที่ไม่เคยมีใครกล้าพูดมาก่อน ตามกันมาเป็นแถว

ในปี 2014 มีข่าวใหญ่เรื่องภาพลับเฉพาะของดาราดังจำนวนมากถูกขโมยไปจากที่อัพโหลดไปเก็บไว้บนบริการ Cloud ของสมาร์ทโฟนยี่ห้อหนึ่ง เหตุการณ์ทั้งหมดนี้เป็นเครื่องพิสูจน์และเตือนใจผู้ใช้เน็ตทั่วโลกเป็นอย่างดีว่า

- ข้อมูลทั้งหลายทุกรูปแบบที่รับส่งกันผ่านอินเทอร์เน็ตนั้น อาจถูกดักจับระหว่างทางหรือขโมยจากที่เก็บบน Cloud ได้เสมอ ไม่ว่าจะโดยมิจฉาชีพ หน่วยงานของรัฐ ทั้งในหรือต่างประเทศ คู่แข่งทางการค้า ฝ่ายตรงข้ามหรือคู่แข่ง ทั้งทางการเมืองหรือธุรกิจ ฯลฯ เพียงแต่ข้อมูลเหล่านั้นจะมีสาระควรแก่การสนใจ หรือให้ประโยชน์คุ้มกับความพยายามที่ขโมยเอาไปหรือไม่ หากจะให้ข้อมูลนั้นๆ ปลอดภัยอย่างแท้จริงก็ต้องป้องกันไม่ให้ไปอยู่บนอินเทอร์เน็ตเลยตั้งแต่ต้น
- การรับส่งข้อมูลที่เป็นความลับหรือมีผลกระทบกับผู้มีส่วนได้เสียอย่างมาก และเสี่ยงต่อการรั่วไหล เช่น ที่เกี่ยวกับการเงิน สุขภาพ เรื่องส่วนตัวหรือน่าเสื่อมเสียชื่อเสียง สูตรลับทางการค้า ฯลฯ ควรมีการเข้ารหัสเพื่อปกป้องความปลอดภัยของข้อมูลเสมอ อย่างน้อยก็ใช้บราวเซอร์ที่ทำงานด้วยโปรโตคอล https: ก็ยังดี (ดูหน้า 85) อย่าหลงวางใจว่าไม่มีใครรู้ใครเห็นเป็นอันขาด

เปิดเผยเรื่องส่วนตัวแค่ไหนให้พอดี

สำหรับนักการเมือง ศิลปิน/ดารา นักข่าวสื่อสารมวลชน คนดัง ผู้มีชื่อเสียงด้านต่างๆ อาจต้องเปิดเผยตัวตนผ่านทาง Social Media เช่น Facebook, Instagram (IG) หรืออื่นๆ มากหน่อย เนื่องจากมีคนคอยติดตามดูความเคลื่อนไหว ทำให้มีความจำเป็นที่จะต้องโพสต์เรื่องส่วนตัวในบางครั้งคราวไปจนถึงบ่อยๆ เพื่อประชาสัมพันธ์ไปในตัว แต่สำหรับบุคคลทั่วไปอย่างเราๆ นั้นไม่มีความจำเป็นใดๆ ที่จะต้องนำเรื่องส่วนตัวมาเผยแพร่นอกจากต้องการให้เพื่อนทราบ แต่นอกจากเพื่อนแล้วคนทั้งโลกยังสามารถเห็นสิ่งที่คุณนำเสนอนั้นเช่นกัน ถ้าไม่ต้องการให้คนนอกเห็นตอนโพสต์นั้นคุณต้องไม่เลือกเป็น *สาธารณะ*หรือ *Public* ให้เลือกแสดงเฉพาะเพื่อนก็พอ (ดูตัวอย่างหน้า 58)

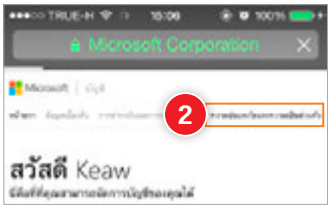


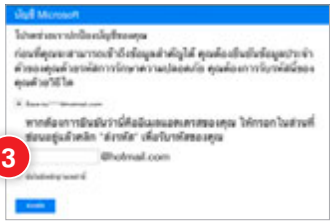
ยกเลิกการใช้งานแอคเคาท์ต่างๆ ที่ไม่ใช้

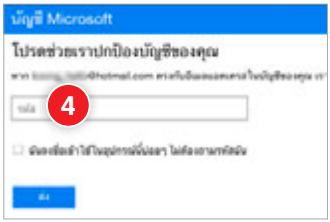
แอคเคาท์บริการต่างๆ ไม่ว่าจะเป็น Facebook, Twitter หรืออีเมล์ต่างๆ เมื่อไม่ใช้แล้วก็ควรจะลบทิ้งเพื่อรักษาความเป็นส่วนตัว ซึ่งลบแล้วจะเอาคืนไม่ได้ ในที่นี้จะยกตัวอย่างการยกเลิกใช้งานแอคเคาท์ Hotmail, Gmail และ Facebook ดังนี้ (ระวัง! ก่อนยกเลิกต้องแน่ใจว่าไม่ใช้จริงๆ และไม่มีบริการออนไลน์ใดๆ ผูกหรืออ้างอิงกับอีเมล์เหล่านี้แล้ว ไม่เช่นนั้นภายหลังอาจมีคนไปใช้สมัครชื่อแอคเคาท์นี้แทน และสวมรอยเป็นคุณ เช่น ไปรีเซ็ตรหัสผ่านต่างๆ โดยอ้างว่าจำไม่ได้ ให้ส่งลิงค์มาที่อีเมล์เหล่านี้ได้)

ยกเลิกแอคเคาท์ Hotmail

เนื่องจากแอคเคาท์ Hotmail (รวมถึงแอคเคาท์อื่นๆ ของไมโครซอฟท์) นั้นมีการผูกกับบริการต่างๆ ไว้ด้วย เมื่อยกเลิกแอคเคาท์แล้วอาจส่งผลกระทบต่อแอพและบริการอื่นๆ ที่ใช้งานอยู่ หลังจากยกเลิกจะให้เวลา 60 วันเผื่อคุณเปลี่ยนใจจะกลับไปใช้บริการอีกครั้งได้ โดยวิธียกเลิกแอคเคาท์จะทำได้ดังนี้







1. เปิดบราวเซอร์ที่ใช้เข้าเว็บเข้าไปที่ account.live.com แล้ว Sign in แอคเคาท์ที่จะยกเลิก
2. แตะ **ความปลอดภัยและความเป็นส่วนตัว** (Security & privacy)
3. ถ้าเปิดเว็บด้วยมือถือจะให้กรอกอีเมล์สำรองที่ตรงกับข้อมูลเดิมเพื่อส่งรหัสให้ทางอีเมล์สำรอง ถ้าเปิดเว็บด้วยคอมพิวเตอร์จะให้เลือกส่งรหัสทางเบอร์โทรศัพท์หรืออีเมล์สำรอง(แล้วแต่ข้อมูลที่เคยให้ไว้) แล้วแตะปุ่ม **ส่งรหัส** (Send code)
4. ไปตรวจสอบอีเมล์สำรองหรือเบอร์โทรศัพท์เพื่อดูรหัสที่ไมโครซอฟท์ส่งมาให้ แล้วนำมากรอก จากนั้นแตะปุ่ม **ส่ง** (Submit)

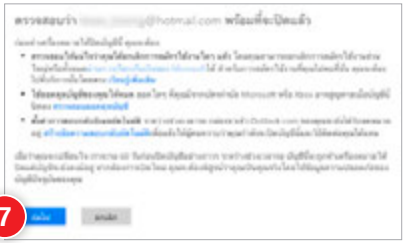
7 ตรวจสอบให้แน่ใจว่าเป็นแอคเคาท์ที่ต้องการยกเลิก แล้วคลิก Next (**ถัดไป**)

8 แตะยอมรับผลการยกเลิกแต่ละข้อและเลือกเหตุผลที่ต้องการยกเลิกแอคเคาท์

9 แตะ **ทำเครื่องหมายบัญชีเพื่อให้ปิด** (Mark account for closure)

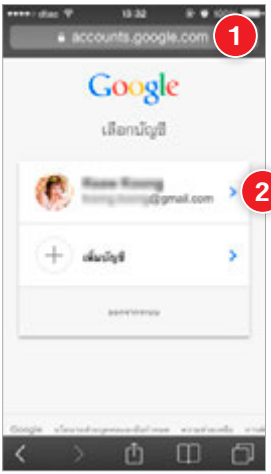
5 อาจให้ตั้งค่าการใส่รหัสรักษาความปลอดภัย ให้แตะ **ตั้งค่าในภายหลัง** (Set it up later) ข้ามไป (ถ้าไม่ขึ้นให้ข้ามไปข้อ 6 เลย

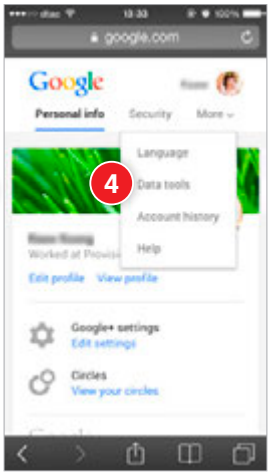
6 ที่หัวข้อ เลือกบัญชีของคุณ (Close your account) ให้แตะ **เลือกบัญชีของฉัน** (Close my account)



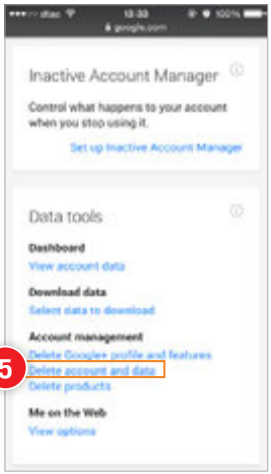
ยกเลิกแอคเคาท์ Gmail

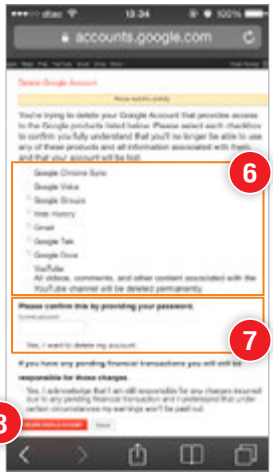
1. เปิดบราวเซอร์ที่ใช้เข้าเว็บเข้าไปที่ accounts.google.com
2. Sign in แอคเคาท์ที่จะยกเลิก (ถ้า Sign in แล้วให้เลือกแอคเคาท์ได้เลย)
3. ถ้าขึ้นให้กรอกหมายเลขโทรศัพท์เพื่อส่งรหัสยืนยันให้แตะ **ข้าม** (Skip) ข้ามไป (ถ้าไม่ขึ้นให้ข้ามไปข้อ 4 เลย)





4. แตะ More ▸ Data tools



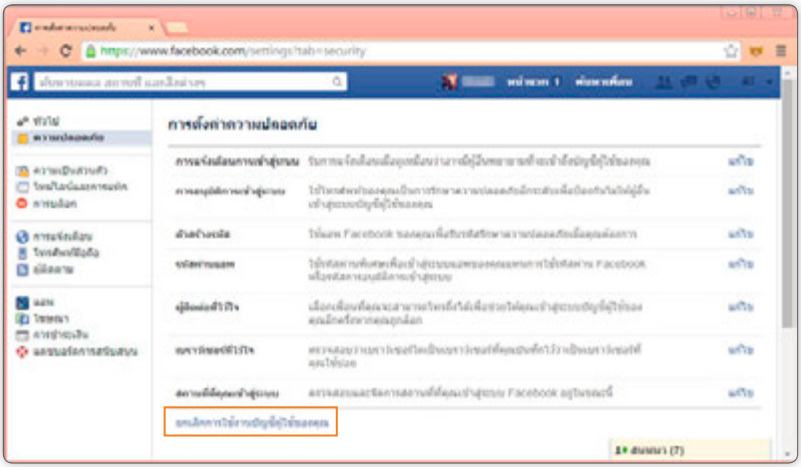


5. เลื่อนหน้าจอลงไปที่หัวข้อ Data tools แล้วแตะ **Delete account and data**
6. เลือกข้อมูลที่จะลบ
7. ใส่รหัสผ่าน และแตะเลือก **Yes, I want to delete my account**
8. แตะปุ่ม **DELETE GOOGLE ACCOUNT**

ยกเลิกแอคเคาท์ Facebook

Mobile เปิดแอพ Facebook แตะ **เพิ่มเติม** ▸ **การตั้งค่า** ▸ **ทั่วไป** แตะ **ระงับการใช้งาน** แล้วแตะเลือกเหตุผลที่ต้องการยกเลิก จากนั้นแตะปุ่ม **ระงับการใช้งาน**

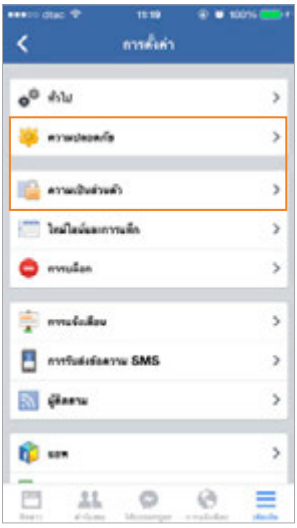
Computer ขณะเปิดใช้ Facebook ให้คลิก ▾ ที่มุมขวาบนของหน้าเว็บ เลือก **การตั้งค่า** (หรือเข้าไปที่ www.facebook.com/settings) คลิกหัวข้อ **ความปลอดภัย** แล้วคลิกที่ **ยกเลิกการใช้งานบัญชีผู้ใช้ของคุณ** จะให้ระบุเหตุผล แล้วคลิกปุ่ม **ยืนยัน**



ตั้งค่าความปลอดภัยและความเป็นส่วนตัวใน Social Network

ใน Social Network จะสามารถตั้งค่าความเป็นส่วนตัวได้ เช่น ตั้งค่าว่าใครจะเห็นโพสต์ของคุณได้บ้าง, ใครที่จะติดต่อกับคุณได้, คนอื่นสามารถค้นหาคุณเจอจากอีเมล์ได้หรือไม่ เป็นต้น ซึ่งวิธีการตั้งค่าจะต่างกันไปตามแต่ละที่ ในที่นี้จะยกตัวอย่าง 2 Social Network ที่นิยมใช้กันคือ Facebook และ Twitter ดังนี้

ตั้งค่าใน Facebook



Mobile ขณะเปิดใช้ Facebook ให้แตะ **เพิ่มเติม** ▸ **การตั้งค่า** แล้วแตะ **ความปลอดภัย** หรือ **ความเป็นส่วนตัว** แล้วตั้งค่าหรือแก้ไขค่าด้านต่างๆ ตามต้องการ เช่น กำหนดว่าใครจะเห็นโพสต์ของคุณได้บ้าง, กำหนดใครที่สามารถค้นหาคุณด้วยอีเมล์หรือเบอร์โทรได้ เป็นต้น

ความปลอดภัย

- **ข้อความการแจ้งเตือนการเข้าสู่ระบบ** เลือกให้แจ้งเตือนทาง SMS เมื่อมีการล็อกอินเข้าระบบ
- **การแจ้งเตือนการเข้าสู่ระบบทางอีเมล** เลือกให้แจ้งเตือนทางอีเมล์เมื่อมีการล็อกอิน
- **การอนุมัติการเข้าสู่ระบบเปิดอยู่** เลือกเปิดให้ใส่รหัสที่ได้รับทาง SMS เมื่อเข้าระบบจากบราวเซอร์ที่ไม่เคยเข้าใช้มาก่อน
- **ตัวตรวจสอบความถูกต้องของบุคคลที่สาม** ตั้งค่าแอพบนอุปกรณ์นี้หรืออุปกรณ์อื่นให้สร้างรหัสรักษาความปลอดภัย

- **ผู้ติดต่อที่ไว้ใจ** กำหนดบุคคลที่จะช่วยเหลือคุณเมื่อมีปัญหาในการเข้าใช้งาน
- **รหัสผ่านแอพ** กำหนดรหัสผ่านให้กรอกเมื่อเข้าใช้แอพ Facebook

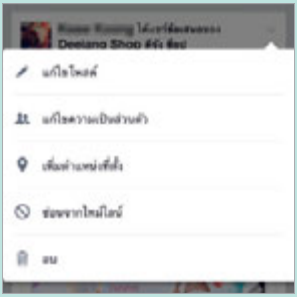
- **อุปกรณ์ที่รู้จัก** แสดงรายการอุปกรณ์ที่เคยเข้าใช้ Facebook ของเรา ซึ่งเมื่อล็อกอินจากอุปกรณ์ในรายการนี้จะไม่มีการแจ้งเตือนหรือให้ยืนยันตัวตนอีก ถ้าเห็นว่ามีอุปกรณ์ไหนที่ไม่ได้ใช้ก็แตะ ✕ ทางขวาเพื่อลบออกได้ (ถ้าไม่แน่ใจจะลบทุกอันเลยก็ไม่เป็นไร แค่ต้องล็อกอินและใส่รหัสผ่านใหม่เมื่อจะใช้อุปกรณ์นั้นอีกและสั่งให้ Facebook จำอุปกรณ์นั้นใหม่)

- **เซสชันที่ใช้งานอยู่** แสดงรายการอุปกรณ์ที่กำลังเข้าใช้ Facebook ในชื่อของเราอยู่ในพื้นที่ต่างๆ ทั่วโลก ถ้ามีอันไหนน่าสงสัยว่าจะไม่ใช่เราก็แตะ ✕ ทางขวาเพื่อลบออกเพื่อตัดการใช้งานบนอุปกรณ์นั้น (ซึ่งจะบังคับเครื่องนั้นๆ ให้ล็อกอินใหม่ ดังนั้นถ้าเจอแบบนี้ควรรีบเปลี่ยนรหัสผ่านด้วย)

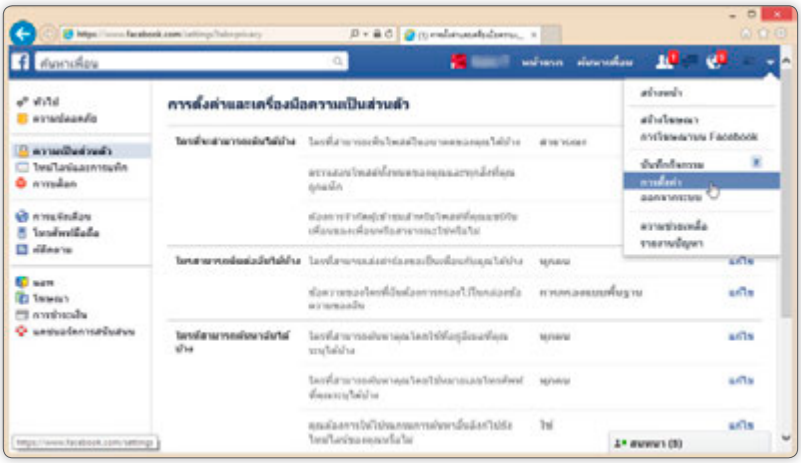
ความเป็นส่วนตัว

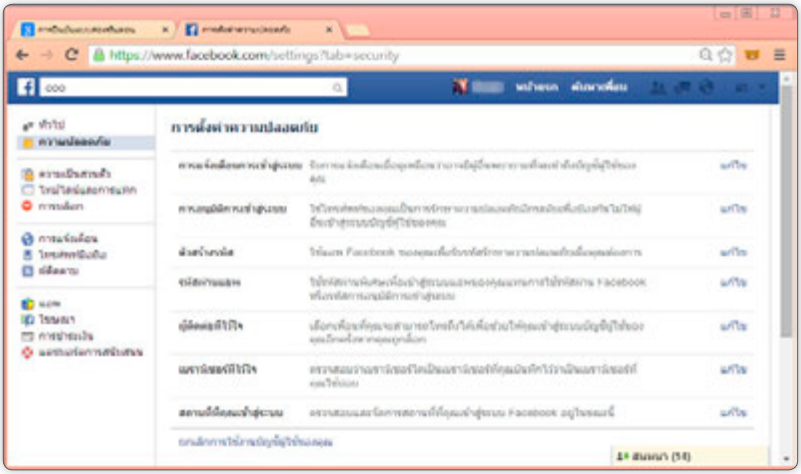
- **ใครที่สามารถเห็นโพสต์ในอนาคตของคุณได้บ้าง** ตั้งค่าหลักว่าจะให้ใครเห็นโพสต์ใหม่ของคุณบ้าง เช่น เฉพาะเพื่อน เพื่อนสนิท กลุ่มบางกลุ่ม สาธารณะ เป็นต้น โดยจะขึ้นค่าที่เลือกไว้นี้เสมอไม่ต้องมาคอยเปลี่ยนเอง (ส่วนที่โพสต์ไปแล้วก็ไปแก้ไขทีละโพสต์เองได้ -ดูกรอบด้านล่าง หรือแก้ไขทั้งหมดให้ดูหัวข้อถัดไป)
- **ต้องการจำกัดผู้เข้าชมสำหรับโพสต์ที่คุณแชร์กับเพื่อนของเพื่อนหรือสาธารณะใช่หรือไม่** ตั้งค่าจำกัดผู้ชมของโพสต์ก่อนหน้านี้ทั้งหมดให้เห็นได้เฉพาะเพื่อน
- **ใครที่สามารถส่งคำร้องขอเป็นเพื่อนกับคุณได้บ้าง** ตั้งว่าให้ใครส่งคำร้องขอเป็นเพื่อนมาถึงคุณได้บ้าง
- **ใครที่สามารถค้นหาคุณโดยใช้ที่อยู่อีเมลที่คุณระบุได้บ้าง** ให้ใครค้นหาคุณด้วยอีเมล์แอดเดรสของคุณได้บ้าง
- **ใครที่สามารถค้นหาคุณโดยใช้หมายเลขโทรศัพท์ที่คุณระบุได้บ้าง** ให้ใครค้นหาคุณด้วยเบอร์โทรศัพท์ของคุณได้บ้าง
- **คุณต้องการให้โปรแกรมการค้นหาอื่นลิงก์ไปยังไทม์ไลน์ของคุณหรือไม่** กำหนดให้โปรแกรมอื่นสามารถค้นหาโดยลิงค์มายังหน้าของคุณได้หรือไม่

หลังจากโพสต์ไปแล้วก็สามารถเปลี่ยนความเป็นส่วนตัวว่าจะให้ใครเห็นบ้างได้ โดยแตะ ที่โพสต์ แตะ **แก้ไขความเป็นส่วนตัว** แล้วเลือกกลุ่มที่จะให้เห็นโพสต์นั้น

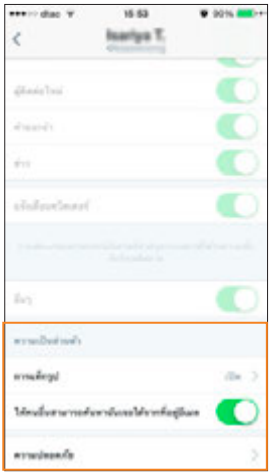


Computer ขณะเปิดใช้ Facebook ให้คลิก ▼ ที่มุมขวาบนของหน้าเว็บ เลือก **การตั้งค่า** (หรือเข้าไปที่ www.facebook.com/settings) คลิกหัวข้อ **ความปลอดภัย** หรือ **ความเป็นส่วนตัว** แล้วตั้งค่าหรือแก้ไขค่าความเป็นส่วนตัวและความปลอดภัยในด้านต่างๆ ได้เลย (แต่ละข้อจะเหมือนกับในส่วน Mobile)





ตั้งค่าความเป็นส่วนตัวใน Twitter



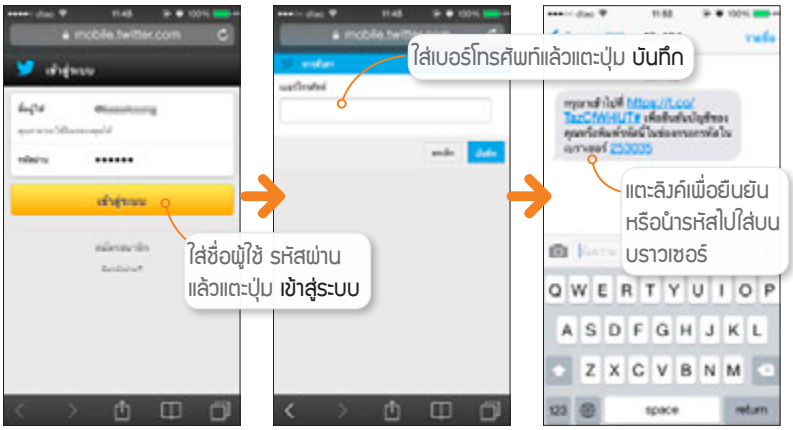
Mobile เปิดใช้งาน Twitter แตะ **ฉัน** ▸ ⚙ ▸ **ตั้งค่า** ▸ แตะชื่อแอคเคาท์ด้านบน เลื่อนหน้าจอลงไปด้านล่างแล้วตั้งค่าด้านต่างๆ

ความเป็นส่วนตัว

- **การแท็กรูป** เปิด-ปิดการแท็กรูปภาพและกำหนดให้ใครสามารถแท็กคุณได้บ้าง
- **ให้คนอื่นสามารถค้นหาฉันเจอได้จากที่อยู่อีเมล์** เปิด-ปิดการให้คนอื่นค้นหาคุณจากอีเมล์แอดเดรส

ความปลอดภัย

การตั้งค่าความปลอดภัยนี้จะให้ผูกแอคเคาท์กับเบอร์โทรศัพท์เพื่อใช้ยืนยันการเข้าระบบด้วย ให้แตะ **เพิ่มโทรศัพท์** แล้วล็อกอินเข้าระบบ แตะลิงค์ยืนยันการตั้งค่า จากนั้นให้แตะที่ **ความปลอดภัย** แล้วเปิด-ปิดตัวเลือก **ยืนยันการเข้าระบบ** ถ้าเปิดข้อนี้เอาไว้ เมื่อล็อกอินเข้าใช้งานครั้งใดก็จะต้องรอรับรหัสยืนยันทาง SMS มากรอกให้ถูกต้องทุกครั้ง



Computer เปิดเว็บ Twitter.com คลิก ⚙ เลือก **การตั้งค่า** (หรือเข้าไปที่ twitter.com/settings/account) คลิกหัวข้อ **ความปลอดภัยและความเป็นส่วนตัว** ตั้งค่าต่างๆ ดังรูป เสร็จแล้วคลิกปุ่ม **บันทึกการเปลี่ยนแปลง**

ตั้งค่าคุกกี้ และความเป็นส่วนตัว ในบราวเซอร์

การท่องเว็บบนมือถือหรือแท็บเล็ตด้วยบราวเซอร์ต่างๆ จะมีการบันทึกคุกกี้ (cookies) คือไฟล์เล็กๆ ที่เหมือนกับการทำเครื่องหมายไว้ที่บราวเซอร์และเครื่องของเรา เพื่อให้เครื่องที่เป็นเซิร์ฟเวอร์นั้นจำเราได้ รวมทั้งทำให้โปรแกรมบนเซิร์ฟเวอร์อื่นๆ สามารถดูได้ว่าเราเคยเข้าไปดูเว็บประเภทไหน สนใจอะไร ได้ด้วย ซึ่งถ้าไม่ต้องการก็สามารถปิดไม่รับคุ้กกี้ รวมถึงตั้งค่าอื่นๆ ได้ดังนี้

iOS

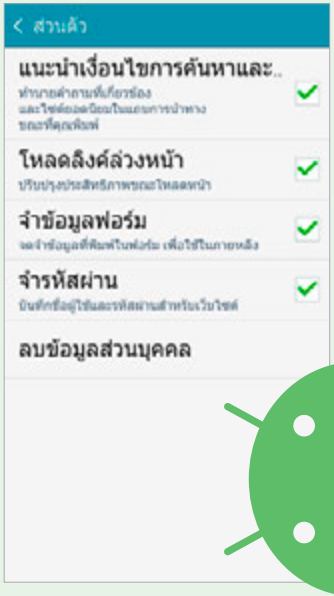
iOS (แอพ Safari) ไปที่ **การตั้งค่า** (Settings) ▸ **Safari** แล้วตั้งค่าคุกกี้ (Cookies) และความเป็นส่วนตัว (Privacy)

- **การติดตาม (Do not Track)** เปิด-ปิดการสะกดรอยจากเว็บ เช่น การติดตามสอดส่องพฤติกรรมการเข้าชมเว็บต่างๆ ของคุณ
- **กั้นคุกกี้ (Block Cookies)** ตั้งค่าการปิดกั้นคุกกี้จากการโฆษณา หรือเลือกปิดกั้นคุ้กกี้ทั้งหมด หรือไม่ปิดกั้นเลยก็ได้
- **ช่องค้นหาอัจฉริยะ (Smart Search Field)** เปิด-ปิดการจดจำและแสดงรายชื่อคำที่เราเคยค้นหามาให้เลือกล่วงหน้า

- **คำเตือนเว็บไซต์หลอกลวง (Fraudulent Website Warning)** เปิด-ปิดการเตือนเว็บไซต์เข้าข่ายหลอกลวง (ซึ่งจะเอาเว็บที่เราจะเปิดไปเช็คกับรายชื่อเว็บอันตราย ถ้าไม่อยากให้ทำข้อนี้ก็ปิดได้)

Android

Android (แอพ Internet) เปิดแอพ อินเทอร์เน็ต (Internet) แตะ ▸ **การตั้งค่า** (Settings) จากนั้นแตะ **ส่วนตัว** (Privacy) ตั้งค่าระบบรักษาความปลอดภัยต่างๆ ดังนี้



- **แนะนำเงื่อนไขการค้นหาและ URL (Suggest search terms and Web addresses)** เปิด/ปิดการแสดงชื่อเว็บหรือคำค้นหาที่ใกล้เคียงกับที่กรอกในช่อง Address
- **โหลดลิงค์ล่วงหน้า (Preload available links)** เปิด-ปิดการโหลดเว็บต่างๆ ที่มีลิงค์ไปถึงจากหน้าที่ดูอยู่ล่วงหน้า ช่วยให้เปิดเว็บได้เร็วขึ้น
- **จำข้อมูลฟอร์ม (Remember form data)** จดจำข้อมูลที่เรากรอกลงในช่องต่างๆ เพื่อนำมาใช้ในการกรอกข้อมูลครั้งถัดไป (ซึ่งจะมีการเก็บข้อมูลบางอย่าง เช่น เลขบัตรเครดิต ไว้ในเครื่องด้วย)
- **จำรหัสผ่าน (Remember passwords)** บันทึกชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานเว็บต่างๆ (ทำให้มีการเก็บข้อมูลเหล่านี้ในเครื่องด้วย ซึ่งสะดวกแต่อาจถูกขโมยข้อมูล หรือถ้ามือถือหายคนอื่นก็เข้าได้)
- **ลบข้อมูลส่วนบุคคล (Delete personal data)** เลือกลบข้อมูลทั้งหมดที่บันทึกไว้ระหว่างใช้งานบราวเซอร์

ไม่ให้จำรหัสผ่านในเครื่องสาธารณะ

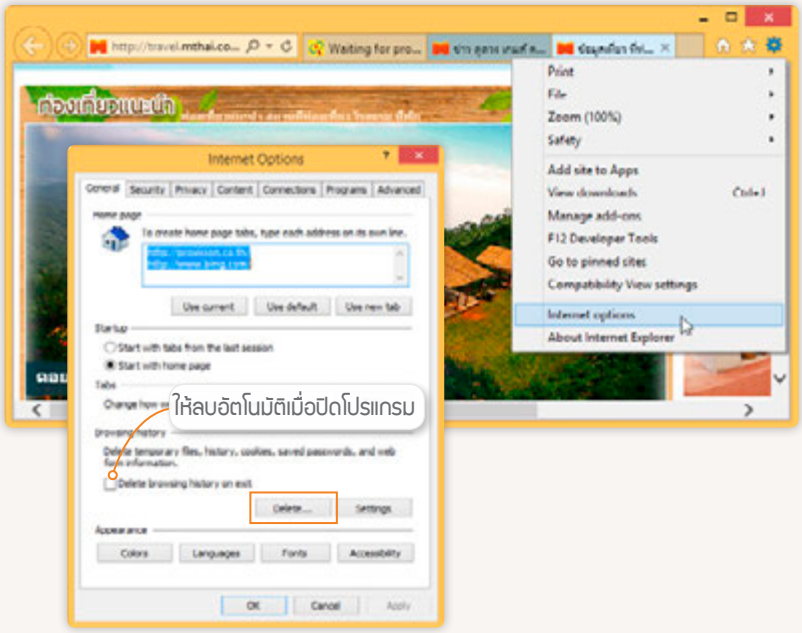
ถ้ายืมเครื่องคนอื่นใช้ หรือใช้เครื่องคอมพิวเตอร์สาธารณะ เช่น ในร้านเน็ต เมื่อล็อกอินเข้าใช้งานบริการต่างๆ ไม่ควรเลือกให้จดจำรหัสผ่านเอาไว้ ไม่เช่นนั้นคนที่ใช้เครื่องต่อจากคุณก็จะเข้าใช้หน้าที่คุณล็อกอินไว้ได้ตลอดเลย (ถึงคุณจะล็อกเอาท์ออกมาเพื่อเลิกใช้แล้วก็ตาม) จนกว่าจะมีใครไปสั่งลบข้อมูลการท่องเว็บจากบราวเซอร์นั้นๆ ล้างเครื่อง หรือคุณไปเปลี่ยนรหัสผ่านใหม่

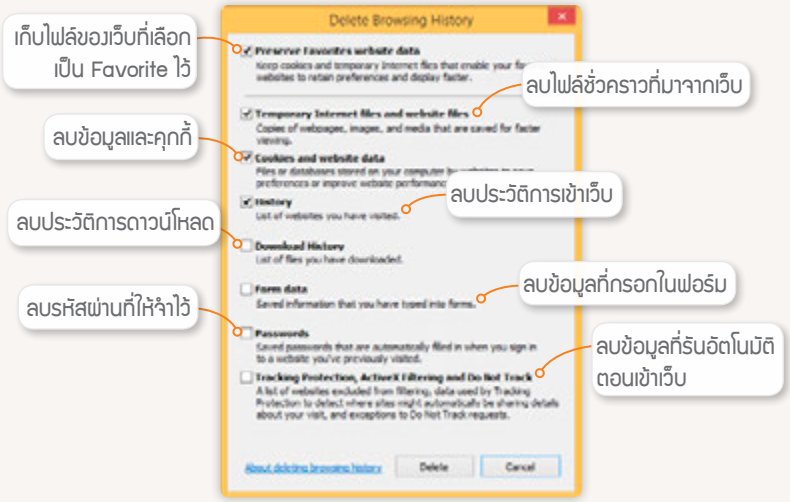
ลบข้อมูลการท่องเว็บ

ถ้าคุณไปล็อกอินไว้ที่เครื่องสาธารณะแล้วไม่แน่ใจว่าไปตั้งให้จำรหัสผ่านไว้หรือเปล่า หรือใช้งานเครื่องส่วนรวมในออฟฟิศ หรือลาออกจากงาน แล้วต้องการลบข้อมูลส่วนตัวที่เคยให้เครื่องจดจำไว้ ก็ให้ไปลบข้อมูลการท่องเว็บดังนี้

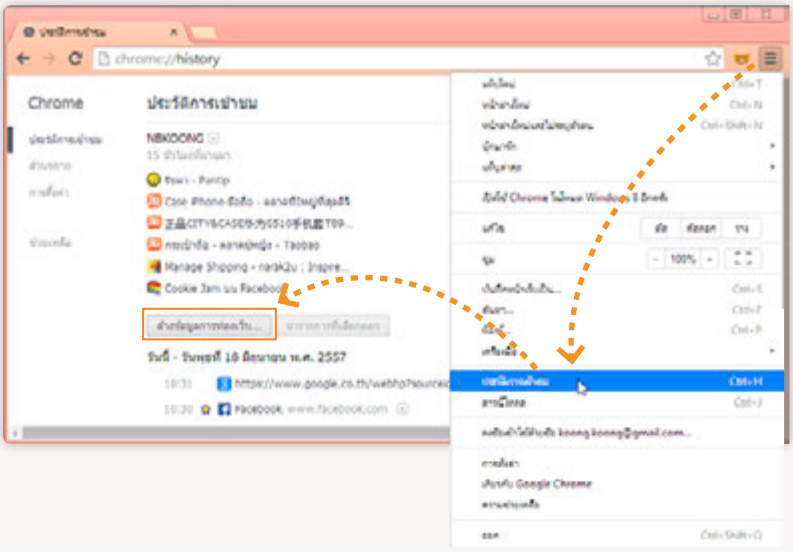
Windows

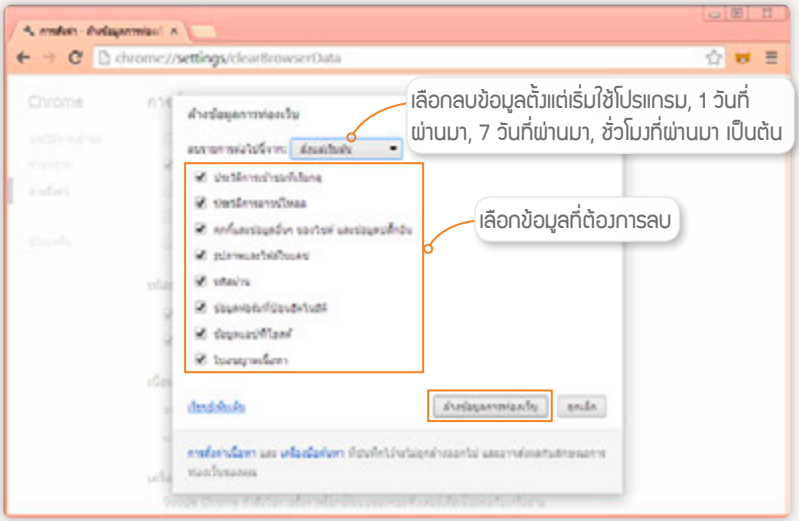
IE คลิก ⚙ ▸ **Internet options** คลิกปุ่ม **Delete** แล้วเลือกลบข้อมูลต่างๆ จากนั้นคลิกปุ่ม **Delete** เลือกลบข้อมูลที่ต้องการ แล้วคลิกปุ่ม **Delete**





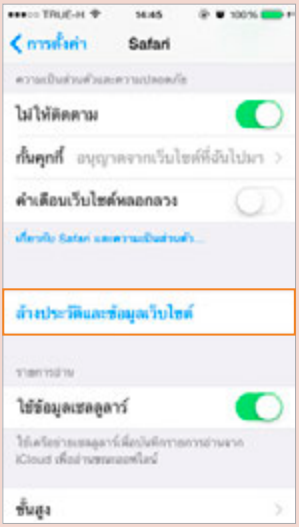
Chrome คลิก ☰ เลือก **ประวัติการเข้าชม** คลิกปุ่ม **ล้างข้อมูลการท่องเว็บ** จากนั้นให้เลือกข้อมูลที่ต้องการลบ (เลือกได้ว่าจะลบย้อนหลังไปนานแค่ไหน ดังรูปหน้าถัดไป) แล้วคลิกปุ่ม **ล้างข้อมูลการท่องเว็บ**





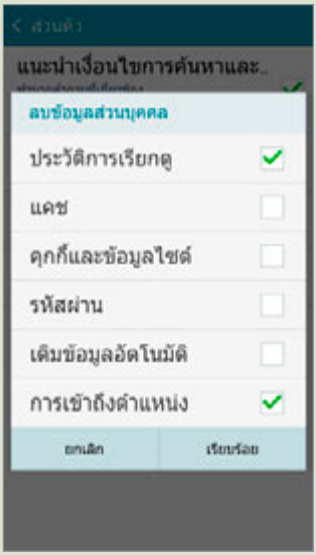
นอกจากในคอมพิวเตอร์แล้ว บราวเซอร์บนมือถือก็จำรหัสผ่านเช่นกัน ซึ่งสั่งลบได้ดังนี้

iOS (แอพ Safari) แตะไอคอน **การตั้งค่า** (Settings) ▸ **Safari** จากนั้นแตะ **ล้างประวัติและข้อมูลเว็บไซต์** (Clear History and Website Data) แล้วแตะ **ล้างประวัติและข้อมูล** (Clear History and Data) ยืนยันการลบรายชื่อเว็บไซต์ที่เคยเข้าไปเยี่ยมชม รวมถึงไฟล์คุกกี้ และข้อมูลทั้งหมด



Android

Android (แอพ Internet) ถ้าต้องการล้างข้อมูลที่เก็บไว้ระหว่างท่องเว็บ ไม่ว่าจะลบคุกกี้ รหัสผ่านที่เคยบันทึก ฯลฯ ให้แตะ ⋮ ▸ **การตั้งค่า** ▸ **ส่วนตัว** ▸ **ลบข้อมูลส่วนบุคคล** (⋮ ▸ Settings ▸ Privacy ▸ Delete personal data) เลือกรายการข้อมูลที่ต้องการลบ แล้วแตะปุ่ม **เรียบร้อย** (Done)

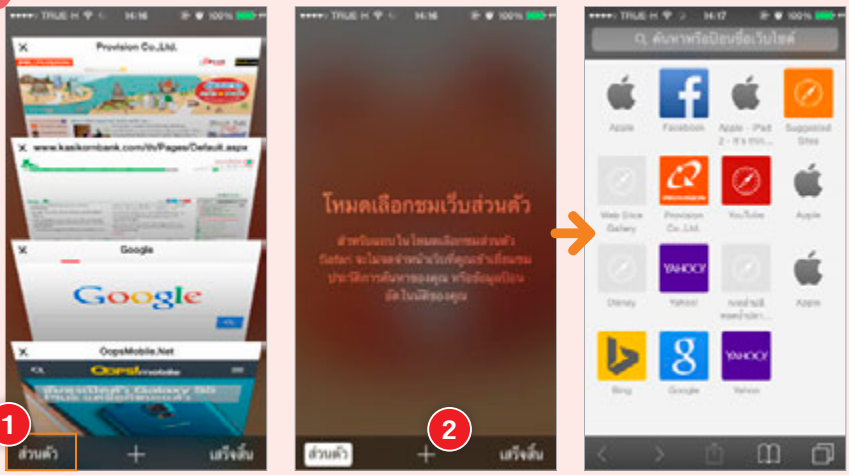


- **ประวัติการเรียกดู** (Browsing history) ลบรายการเว็บเพจที่เคยเข้าชม
- **แคช** (Cache) ลบหน่วยความจำแคช
- **คุกกี้และข้อมูลไซต์** (Cookies and site data) ลบไฟล์คุกกี้ทั้งหมด
- **รหัสผ่าน** (Passwords) ลบรหัสผ่านทั้งหมดที่เคยบันทึกไว้
- **เติมข้อมูลอัตโนมัติ** (Auto-fill data) ลบค่าการป้อนข้อมูลอัตโนมัติ
- **การเข้าถึงตำแหน่ง** (Location access) ลบข้อมูลพิกัดที่เคยเข้าถึง

ท่องเว็บแบบไร้ประวัติ

เมื่อต้องการท่องเว็บแบบส่วนตัวสุดๆ หรือไปใช้เครื่องสาธารณะหรือเครื่องคนอื่นที่ไม่ได้ใช้ประจำ แล้วไม่อยากให้มีการบันทึกชื่อเว็บที่เข้าไปดู หรือมีการเก็บประวัติของการค้นหาอะไรก็ตามที่ค้นจาก Search Engine หรือข้อมูลที่กรอกลงในแบบฟอร์มต่างๆ รวมทั้งไฟล์คุกกี้ เพื่อจะได้ไม่ต้องไปคอยลบเองแบบหัวข้อก่อน มีวิธีดังนี้

iOS



1 แตะ แล้วแตะ **ส่วนตัว** (Private)

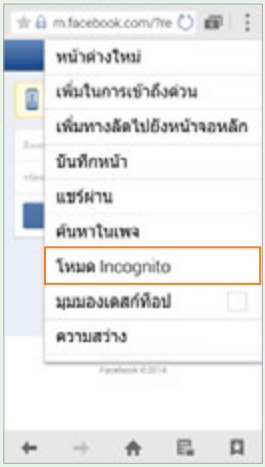
2 แตะ + สังเกตว่าหน้าต่างจะเปลี่ยนเป็นสีเทาเข้ม ให้เข้าเว็บที่ต้องการได้เลย ซึ่งจะไม่เก็บประวัติระหว่างใช้งานเอาไว้

การออกจากโหมด Private ให้แตะ แล้วแตะปุ่ม **ส่วนตัว** (Private)

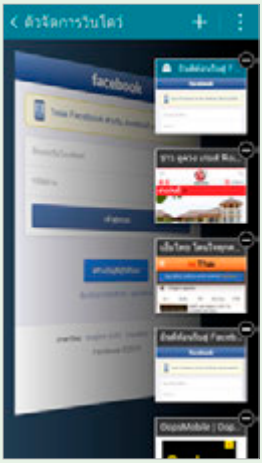
แม้ว่าจะไม่เก็บประวัติ คุกกี้ หรือข้อมูลอื่นๆ ไว้ในเครื่องที่ใช้งาน แต่ยังมีการเก็บข้อมูลที่ผู้ให้บริการหรือ ISP ตามปกติ ซึ่งสามารถตามตรวจสอบได้อยู่ดี ถ้าเป็นเรื่องผิดกฎหมายร้ายแรงขึ้นมา

Android

แตะ ⋮ ▸ **โหมด Incognito** (Incognito mode) แล้วแตะ **ตกลง** (OK) จะเปิดหน้าเว็บที่เปิดอยู่ขึ้นมาใหม่แบบไม่เก็บประวัติ หัวหน้าต่างก็จะเปลี่ยนเป็นสีดำ

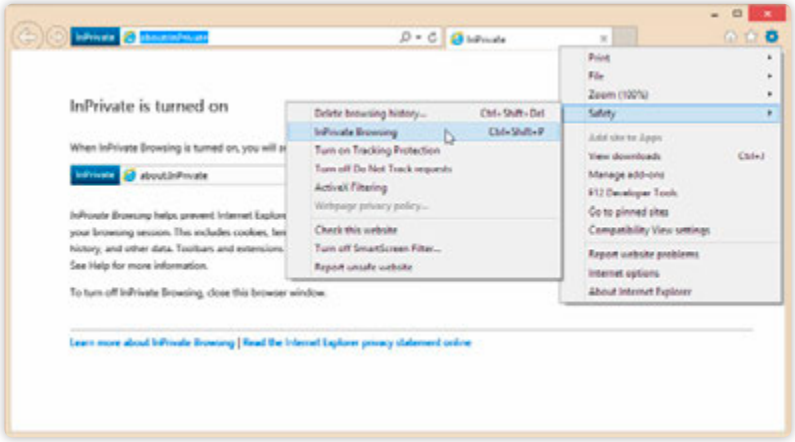


การออกจาก incognito mode ให้ปิดเฉพาะหน้าต่างที่อยู่ในโหมด Incognito ไปได้เลย

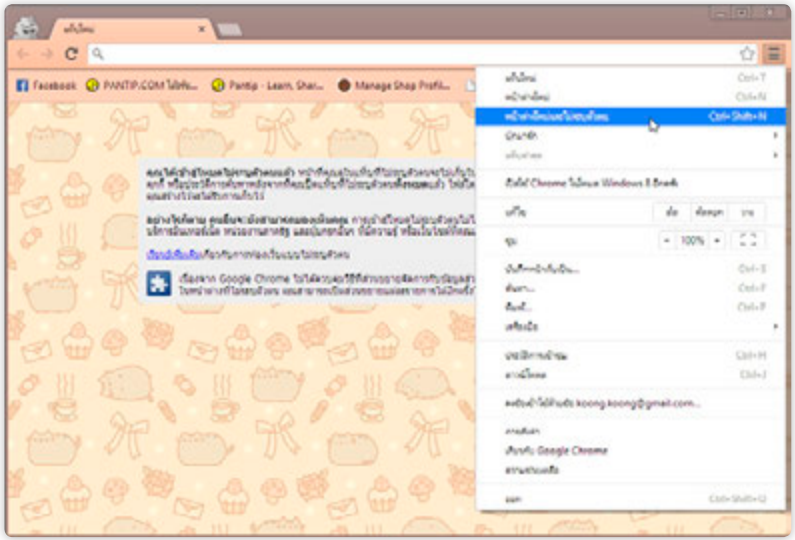


ถ้าใช้เครื่องคอมพิวเตอร์ก็เปิดใช้งานแบบไม่เก็บประวัติและข้อมูลส่วนตัวอื่นๆ ได้ โดยใน IE และ Chrome จะมีวิธีเปิดใช้โหมดไม่เก็บประวัติดังนี้

IE คลิก ⚙ เลือก **Safety** ▸ **InPrivate Browsing** หรือกดคีย์ Ctrl + Shift + P



Chrome คลิก ☰ เลือก **หน้าต่างใหม่และไม่ระบุตัวตน** (New Incognito Window) หรือกดคีย์ Ctrl + Shift + N



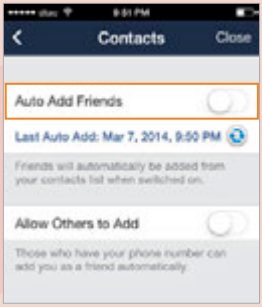
ตั้งค่าการแจ้งเตือน และความเป็นส่วนตัวใน LINE

ในการใช้งานแอพแชทอย่าง LINE ก็สามารถตั้งค่าการแจ้งเตือนต่างๆ รวมถึงความเป็นส่วนตัว เช่น ไม่ให้แจ้งเตือนจากเกม บล็อคบางรายชื่อที่ไม่รู้จัก บล็อคโฆษณา เป็นต้น ซึ่งการตั้งค่าต่างๆ จะทำได้ดังนี้

ยกเลิกการเพิ่มรายชื่ออัตโนมัติ

iOS

หากไม่ต้องการให้ LINE เพิ่มรายชื่อเพื่อนเข้ามาในรายการ Friends อัตโนมัติ ให้แตะแท็บ **More** ▸ **Settings** ▸ **Friends** ▸ **Contacts** แตะปุ่มปิดใช้งานที่คำสั่ง **Auto Add Friends**



Android

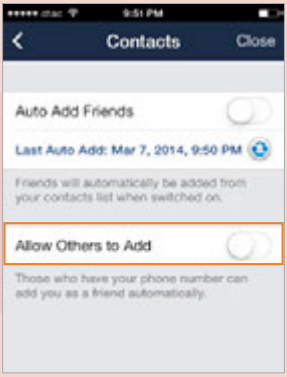
หากไม่ต้องการให้ LINE เพิ่มรายชื่อเพื่อนเข้ามาในรายการเพื่อนอัตโนมัติ ให้แตะแท็บ **อื่นๆ** ▸ **ตั้งค่า** ▸ **บริหารรายการเพื่อน** แตะยกเลิกคำสั่ง **เพิ่มเพื่อนโดยอัตโนมัติ**

ป้องกันไม่ให้คนอื่นเพิ่มชื่อเราอัตโนมัติ

ใครก็ตามที่มีเบอร์โทรศัพท์ของคุณอยู่ในเครื่อง เช่น อาจจะเป็นเพื่อนของเพื่อน ระบบ LINE จะเพิ่มชื่อของคุณเข้าไปให้อัตโนมัติ คุณสามารถป้องกันไม่ให้ถูกเพิ่มชื่อลงไปในเครื่องของเพื่อนคนอื่นได้ดังนี้

iOS

แตะแท็บ **More** ▸ **Settings** ▸ **Friends** ▸ **Contacts** แตะปุ่มปิดใช้งานที่คำสั่ง **Allow Others to Add**



Android

แตะแท็บ **อื่นๆ** ▸ **ตั้งค่า** ▸ **บริหารรายการเพื่อน** แตะยกเลิกคำสั่ง **อนุญาตให้ผู้อื่นเพิ่มเป็นเพื่อนได้**

บล็อคหรือซ่อนรายชื่อ

บล็อครายชื่อ ตัดความสัมพันธ์ของคุณกับเพื่อนไม่ให้ติดต่อถึงกันได้ โดยรายชื่อที่บล็อคไว้จะไม่สามารถส่งข้อความและโทรหาคุณได้ และในเวลาเดียวกันคุณก็ไม่สามารถส่งข้อความไปยังชื่อที่บล็อคไว้ได้เช่นกัน

เมื่อเปลี่ยนรูปโปรไฟล์, เปลี่ยนชื่อ Display, ข้อความที่ What's Up? และข้อความบน Timeline เพื่อนในรายชื่อที่ถูกบล็อคไว้จะไม่สามารถมองเห็นข้อความต่างๆ ของคุณได้

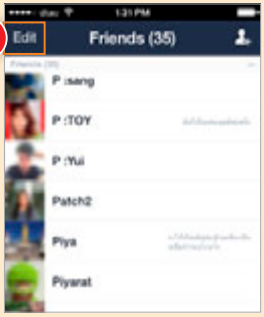
ซ่อนรายชื่อผู้ใช้อื่น ไม่ให้แสดงบนหน้า Friends แต่ชื่อที่ซ่อนไว้จะส่งข้อความและโทรถึงคุณได้ตามปกติ

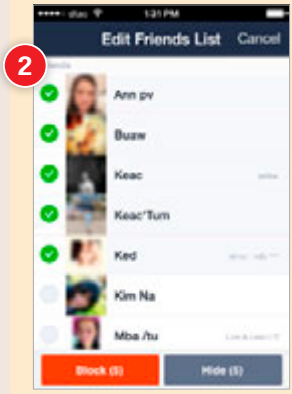
iOS & Android

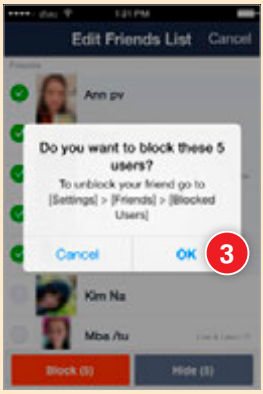
1 เปิดไปที่หน้า **เพื่อนๆ** (Friends) แตะ **แก้ไข** (Edit)

2 แตะ ✓ เลือกรายชื่อ แล้วแตะ **บล็อค** (Block) บล็อครายชื่อ หรือแตะ **ซ่อน** (Hide) ซ่อนรายชื่อ

3 แตะ **ตกลง** (OK) ยืนยันการบล็อคหรือซ่อนรายชื่อ



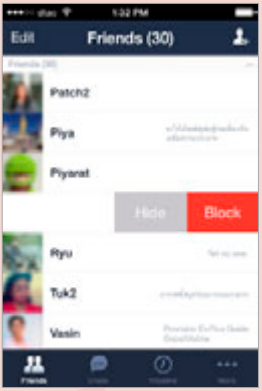




บล็อคหรือซ่อนรายชื่อทีละคน

หากเห็นว่ารายชื่อที่เพิ่มเข้ามานั้นเป็นชื่อที่คุณไม่รู้จัก ก็สามารถบล็อคได้ทันทีด้วยวิธีง่ายๆ ดังนี้

iOS



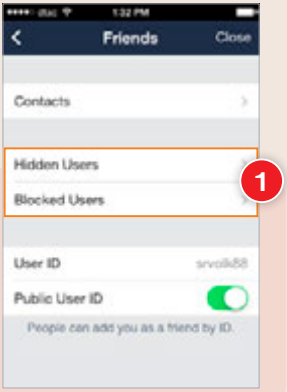
ในหน้า Friends แตะบนชื่อที่ต้องการบล็อคแล้วสไลด์ไปทางซ้าย จากนั้นแตะ Block บล็อคชื่อนี้ หรือ Hide ซ่อน

Android

ขณะที่อยู่หน้า **เพื่อน** ให้แตะบนชื่อที่ต้องการบล็อคค้างไว้จนปรากฏคำสั่ง ให้แตะ **กีดกัน** หรือแตะ **ซ่อน** ชื่อนี้ก็จะถูกบล็อคหรือซ่อนทันที

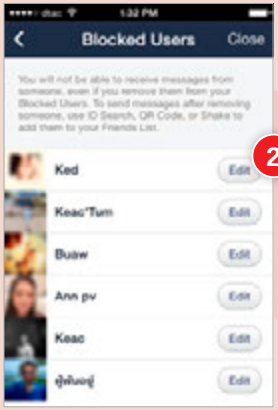
ยกเลิกการบล็อคหรือซ่อนรายชื่อ

ยกเลิกการบล็อคหรือซ่อนรายชื่อ เพื่อให้กลับมาแชทกันใหม่ได้อีกครั้ง มีวิธีดังนี้

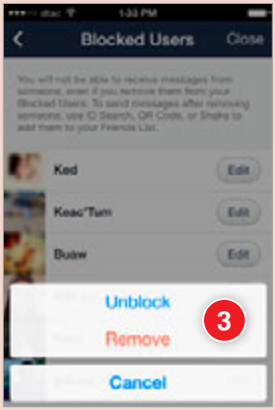


iOS

1 แตะแท็บ More ▸ Settings ▸ Friends แตะคำสั่ง Hidden Users ยกเลิกการซ่อนรายชื่อ หรือแตะคำสั่ง Blocked Users ยกเลิกการบล็อครายชื่อ



2 แตะ **Edit** ตรงรายชื่อที่จะยกเลิกการบล็อคหรือซ่อนรายชื่อ



3 แตะ **Unblock** ยกเลิกการบล็อค (หรือแตะ **Display** ยกเลิกการซ่อนรายชื่อ) หรือแตะ **Remove** เพื่อลบชื่อนั้น

Android

1 แตะแท็บ **อื่นๆ** ▸ **ตั้งค่า** ▸ **บริหารรายการเพื่อน** แตะคำสั่ง **ผู้ใช้ที่ซ่อนไว้** ยกเลิกการซ่อนรายชื่อ หรือแตะคำสั่ง **รายชื่อคนถูกกีดกัน** ยกเลิกการบล็อครายชื่อ

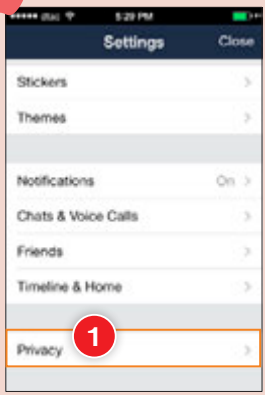
2 แตะ **แก้ไข** ตรงรายชื่อที่จะยกเลิกการบล็อคหรือซ่อนรายชื่อ

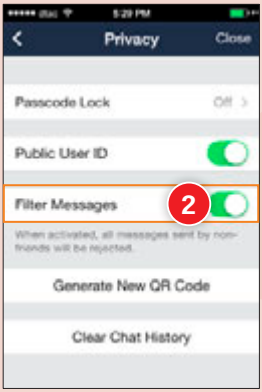
3 แตะ **ไม่กีดกัน** ยกเลิกการบล็อค (หรือแตะ **แสดง** ยกเลิกการซ่อนรายชื่อ) หากแตะ **ลบ** จะเป็นการลบชื่อนั้น

บล็อคข้อความจากบุคคลอื่น

หากคุณได้รับข้อความจากบุคคลอื่นที่ไม่ได้เป็นเพื่อนในลิสต์ คุณสามารถบล็อคข้อความจากบุคคลอื่นที่ไม่ได้เป็นเพื่อนไว้ก็ได้ มีวิธีดังนี้

iOS





1 แตะ More ▸ Settings แตะที่คำสั่ง Privacy

2 แตะเปิดใช้งานที่คำสั่ง Filter Messages ให้บล็อคข้อความจากบุคคลอื่นที่ไม่ใช่เพื่อน

Android

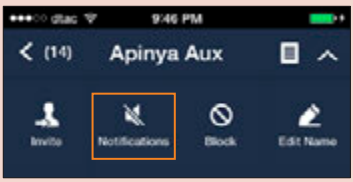
1 แตะ อื่นๆ ▸ ตั้งค่า แตะที่คำสั่ง ตั้งค่าความเป็นส่วนตัว

2 แตะ ☑ คำสั่ง ไม่ยอมรับข้อความ ให้บล็อคข้อความจากบุคคลอื่นที่ไม่ใช่เพื่อน

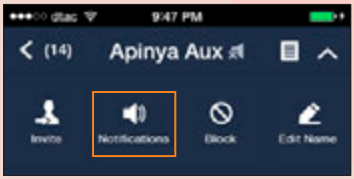
ปิดเสียงเตือนเฉพาะบางคน

ปิดเสียงไม่ให้แจ้งเตือนเมื่อได้รับข้อความ โดยจะเป็นการปิดเสียงเฉพาะการแชทกับเพื่อนคนนี้เท่านั้น

iOS



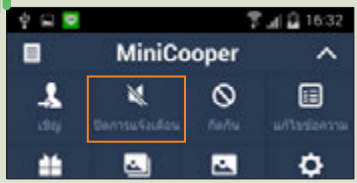
แตะปิดเสียงแจ้งเตือน



แตะเปิดเสียงแจ้งเตือน

ขณะแชทกับเพื่อนคนนี้ให้แตะ แตะ **Notifications** เมื่อเพื่อนคนนี้ส่งข้อความถึงคุณก็จะไม่มีเสียงแจ้งเตือน หากต้องการให้มีเสียงเตือนเหมือนเดิม ให้แตะ แตะ **Notifications** ก็จะเตือนตามปกติ

Android



ปิดเสียงแจ้งเตือน

เปิดเสียงแจ้งเตือน

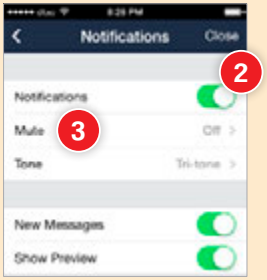
ขณะแชทกับเพื่อนคนนี้ให้แตะ แตะ **ปิดการแจ้งเตือน** เมื่อเพื่อนคนนี้ส่งข้อความถึงคุณก็จะไม่มีเสียงแจ้งเตือน หากต้องการให้มีเสียงเตือนเหมือนเดิม ให้แตะ แตะ **เปิดการแจ้งเตือน** ก็จะเตือนตามปกติ

ปิดเสียงหรือการแจ้งเตือนทั้งหมด

ถ้าไม่ต้องการให้แจ้งเตือนใดๆ เลย หรือยังต้องการให้เตือน แต่รำคาญเสียง ซึ่งถ้าปิดเสียงที่เครื่องเลยก็จะปิดเสียงเรียกเข้าไปด้วย คุณสามารถเลือกปิดเฉพาะเสียงเตือนจาก LINE ได้ดังนี้

iOS & Android

1. แตะแท็บ **อื่นๆ** ▸ **ตั้งค่า** ▸ **การแจ้งเตือน** (More ▸ Settings ▸ Notifications)
2. ปิดใช้งานที่ **การแจ้งเตือน** (Notifications)
3. แตะ **ปิดเสียง** (Mute) แล้วเลือกปิดเสียงเตือนจาก LINE ตลอดไป, ปิดแค่ 1 ชั่วโมง หรือปิดตั้งแต่ตอนนี้ไปจนถึง 8 โมงเช้าของวันรุ่งขึ้นก็ได้

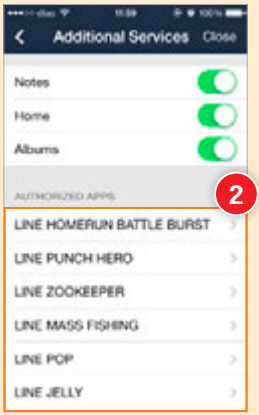


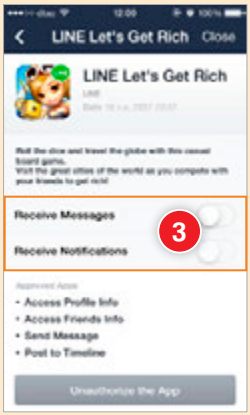
ปิดการแจ้งเตือนจากเกม

ถ้าเพื่อนส่งคำร้องขอจากเกมมามากมายจนเกินจะทน คุณสามารถปิดการรับข้อความและการแจ้งเตือนจากเกมต่างๆ ได้เองโดยไม่ต้องไปบอกเพื่อนแต่ละคนว่าไม่ต้องส่งมาอีก โดยจะต้องปิดไปทีละเกมดังนี้

iOS & Android

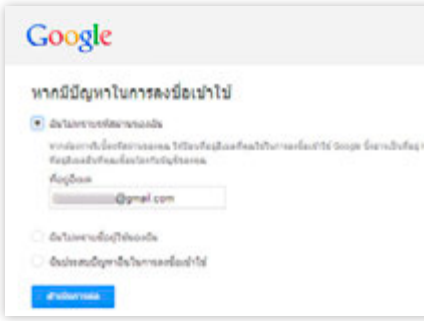
1. แตะแท็บ **อื่นๆ** ▸ **ตั้งค่า** ▸ **การแจ้งเตือน** (More ▸ Settings ▸ Notifications)
2. แตะที่ **บริการเสริม** (Additional Services) แตะชื่อเกมที่ต้องการปิด





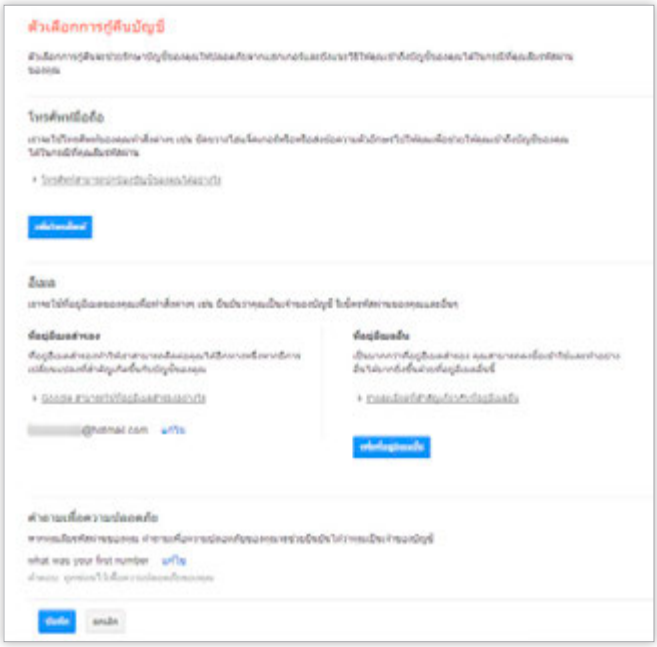
3. ปิดที่ **รับข้อความ** (Receive Messages) ไม่รับข้อความ และปิดที่ **รับการแจ้งเตือน** (Receive Notifications) ไม่รับการแจ้งเตือนจากเกมนี้

ผูกแอคเคาท์กับอีเมล์หรือเบอร์โทรไว้กู้คืนรหัสผ่านและแอคเคาท์

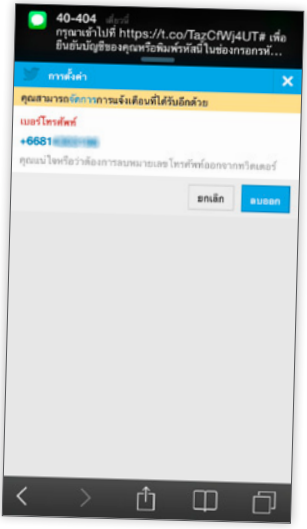


ถ้าตั้งรหัสผ่านในแต่ละเว็บไว้แตกต่างกัน อาจมีสักครั้งที่สับสนหรือลืมรหัสผ่าน ลองใส่กี่แบบก็ไม่ผ่านสักที ซึ่งแต่ละเว็บก็จะมีวิธีกู้คืนแอคเคาท์โดยการรีเซ็ตรหัสผ่านต่างกัน ส่วนใหญ่จะส่งลิงค์รีเซ็ตให้ทางอีเมล์สำรอง หรือให้ตอบคำถามที่เคยใส่ไว้ให้ถูกต้อง (เรียกว่า Security Question) บางเว็บก็จะให้ยืนยันการเป็นเจ้าของแอคเคาท์ทางเบอร์โทรศัพท์ด้วย

การจะกู้คืนนั้นจะต้องเคยตั้งค่าไว้ก่อนด้วย แนะนำว่าควรจะตั้งค่าไว้หลายๆ แบบ ยกตัวอย่างเช่น Gmail ก็จะมีทั้งกู้คืนทางเบอร์โทรศัพท์, อีเมล์สำรอง, ผูกกับอีเมล์แอดเดรสอื่น (ที่ไม่ใช่ Gmail), ตั้งคำถาม/คำตอบ ตั้งให้หมดทุกแบบที่มีให้บริการเลยยิ่งดี ซึ่งการตั้งค่านี้จะใช้ยืนยันตัวตนเมื่อถูกคนอื่นขโมยแอคเคาท์ไปได้ด้วย



การระบุข้อมูลยืนยันตัวตนนั้นบางเว็บมีให้ใส่แค่เบอร์โทรศัพท์เพื่อเป็นหลักฐานแสดงความเป็นเจ้าของ (บางเว็บเช่น Facebook ส่ง SMS เตือนได้ ส่วนของ Twitter ก็มีให้ใช้เช่นกัน -ดูหน้า 61)



ธนาคารและผู้ให้บริการบัตรเครดิตส่วนมากก็มีการผูกกับเบอร์โทรศัพท์เพื่อส่ง SMS ยืนยันเช่นกัน แต่อาจใช้เฉพาะกรณี เช่น เปิดใช้การจ่ายบัตรเครดิตออนไลน์ครั้งแรกกับเว็บใดเว็บหนึ่ง, ยืนยันการโอนเงิน หรือเพิ่มผู้รับโอนเงินรายใหม่ที่จะโอนเงินออกไปจากบัญชีของคุณได้ ซึ่งถ้าเป็นแบบนี้ถึงแฮกเกอร์ได้รหัสผ่านเข้าบริการธนาคารไปก็ทำอะไรไม่ได้ง่ายๆ เพราะการแก้ไขเบอร์โทรมักต้องเอาตัวเป็นๆ ไปแจ้งที่สาขา (แต่เปลี่ยนรหัสผ่านไว้ก่อนก็ดีนะเผื่อเค้าปลอมหลักฐานเป็นคุณไปที่สาขาขึ้นมาจริงๆ)

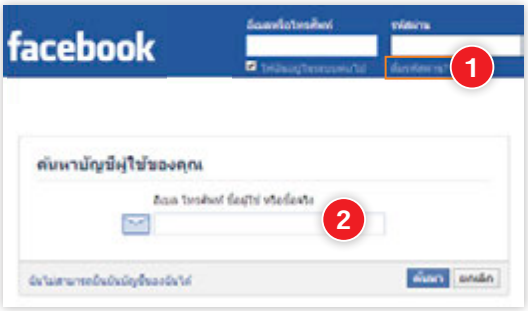
แอคเคาท์ถูกแฮกหรือขโมยไป ทำไงดี?

กู้คืนแอคเคาท์ Facebook กลับมา

ถ้าโดนขโมยหรือแฮกแอคเคาท์ Facebook ไปให้รีบเข้าไปเปลี่ยนรหัสผ่าน ถ้าไม่ทันแล้ว คุณสามารถรายงานไปยัง Facebook โดยยืนยันว่าแอคเคาท์นั้นเป็นของคุณได้ โดยควรจะต้องไปแจ้งความที่สถานีตำรวจเอาไว้ด้วย เพื่อเป็นหลักฐานหากมีใครใช้แอคเคาท์ของคุณไปทำเรื่องเสียหายขึ้นมา

กู้คืนโดยแจ้งลืมรหัสผ่าน

ถ้าล็อกอินด้วยรหัสผ่านเดิมไม่ได้แล้ว ให้แจ้งลืมรหัสผ่าน เพื่อรีเซ็ตรหัสผ่านใหม่ได้ ซึ่งจะให้ส่งลิงค์รีเซ็ตรหัสผ่านให้ทางอีเมล์สำรองที่เคยให้ข้อมูลไว้ได้ (ควรรีบทำอย่างเร่งด่วน เพราะหลังจากแฮกเกอร์เปลี่ยนรหัสผ่านแล้วมักจะมาเปลี่ยนอีเมล์สำรองด้วย เพื่อป้องกันไม่ให้เจ้าของมาเปลี่ยนรหัสผ่านได้)



1 ไปที่ Facebook.com คลิก **ลืมรหัสผ่าน?** ในส่วนล็อกอิน

2 กรอกอีเมล์สำรอง เบอร์โทรศัพท์ ชื่อผู้ใช้ หรือชื่อจริงที่เคยใส่ไว้ แล้วคลิกปุ่ม **ค้นหา**

3 คลิกเลือกหน้ารายการ **ส่งลิงก์มาให้ฉันทางอีเมลเพื่อกำหนดรหัสผ่านของฉันใหม่** *อีเมล์สำรอง*

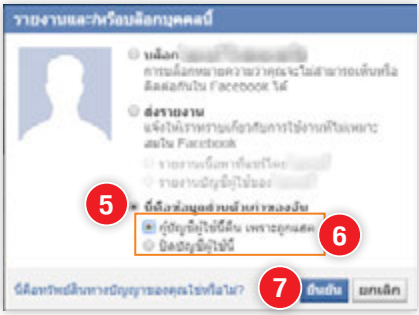
4 คลิกปุ่ม **ดำเนินการต่อ**

5 ไปตรวจสอบอีเมล์สำรอง คลิกอีเมล์ของ Facebook คลิกลิงก์รีเซ็ตรหัสผ่าน แล้วใส่รหัสผ่านใหม่ ทำตามขั้นตอนจนเสร็จ ก็จะเข้าใช้ Facebook ได้ด้วยรหัสผ่านใหม่

กู้คืนโดยรายงานให้ Facebook ทราบ

กรณีที่โดนเปลี่ยนรหัสผ่านและอีเมล์สำรองไปแล้วจะไม่สามารถกู้คืนแบบลืมรหัสผ่านได้ ให้ใช้วิธีแจ้งให้ทาง Facebook ทราบว่าโดนแฮกแอคเคาท์ไปดังนี้

1. ล็อกอิน Facebook ด้วยแอคเคาท์อื่น หรือให้เพื่อนช่วยก็ได้ แล้วเปิดหน้าแอคเคาท์ที่เคยเป็นของคุณ
2. คลิกปุ่ม **เพื่อน** เลือก **เลิกเป็นเพื่อน**



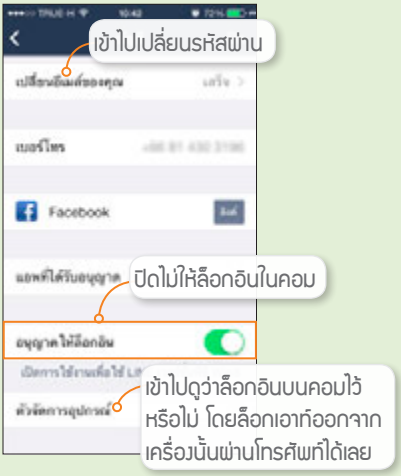
3. คลิก ··· เลือก **รายงาน/บล็อก**
4. คลิกเลือก **ส่งรายงาน** แล้วเลือก **รายงานบัญชีผู้ใช้ของ *ชื่อแอคเคาท์***
5. คลิกเลือก **นี่คือข้อมูลส่วนตัวเก่าของฉัน**
6. เลือก **กู้บัญชีผู้ใช้คืน เพราะถูกแฮค** เพื่อกู้ขอแอคเคาท์คืนมา หรือเลือก **ปิดบัญชีผู้ใช้นี้** ถ้าต้องการยกเลิกการใช้แอคเคาท์นี้ไปเลย
7. คลิกปุ่ม **ยืนยัน** แล้วทำตามขั้นตอนตรวจสอบข้อเท็จจริงของ Facebook จนเสร็จ

กู้คืนแอคเคาท์ LINE

ถ้าถูกแฮก LINE ให้เปลี่ยนรหัสผ่านทันที ถ้าล็อกอินเข้าใช้ไม่ได้ให้แตะ **ล็อกอิน ▸ คุณลืมรหัสผ่านใช่ไหม** กรอกอีเมล์ที่ลงทะเบียนไว้ จากนั้นไปเช็คอีเมล์เพื่อรีเซ็ตรหัสผ่าน (ถ้ายังล็อกอินเข้าได้ให้ไปที่ **อื่นๆ ▸ ตั้งค่า ▸ บัญชี ▸ เปลี่ยนอีเมล์ของคุณ ▸ กรุณาเปลี่ยนรหัสผ่าน**)

แนะนำให้เปลี่ยนรหัสผ่านที่อีเมล์แอคเคาท์ที่ผูกกันอยู่ด้วยเพื่อป้องกันไม่ให้แฮกเกอร์รีเซ็ตรหัสผ่านของ LINE ได้ และถ้าใช้อีเมล์นี้กับบริการของที่อื่นด้วย ก็ควรไปเปลี่ยนรหัสผ่านที่บริการเหล่านั้นป้องกันการถูกแฮกที่อื่นเพิ่มอีก

นอกจากนี้ยังควรไปปิด ไม่ใช้การล็อกอินบนคอมพิวเตอร์ (ดังรูป) เพราะแฮกเกอร์มักล็อกอินแอคเคาท์ที่แฮกได้ทางคอมพิวเตอร์

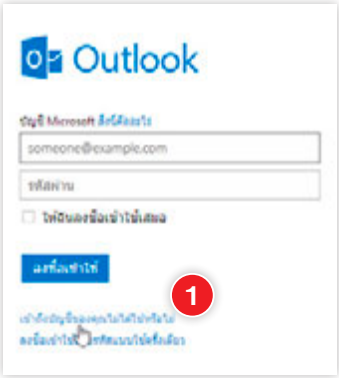


ถ้าทำตามหัวข้อนี้แล้วยังไม่สามารถแก้ไขได้ให้ไปกรอกแบบฟอร์มแจ้งปัญหาที่ https://contact.line.me ซึ่งเป็นหน้ารับแจ้งปัญหาของ LINE แล้วรอการตอบกลับ

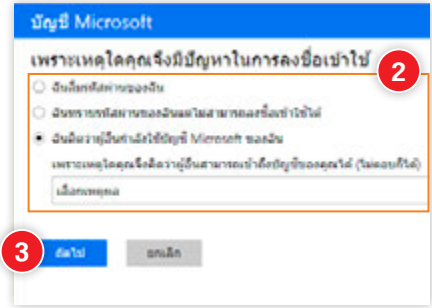
กู้คืนแอคเคาท์ Hotmail กลับมา

ถ้าโดนขโมยแอคเคาท์ Hotmail หรือแอคเคาท์อื่นๆ ของไมโครซอฟท์ เมื่อรู้ตัวให้รีบไปเปลี่ยนรหัสผ่าน (ถ้าไม่รู้ว่าโดนแฮกได้ยังไง อาจถูกดักจับรหัสผ่านด้วยโปรแกรมแปลกๆ ในเครื่อง ให้ติดตั้งโปรแกรมป้องกันไวรัสก่อน ถ้ามีอยู่แล้วให้อัพเดทข้อมูลไวรัสในโปรแกรม ป้องกันการแอบส่องรหัสผ่านซ้ำอีก) แต่ถ้าไม่สามารถเข้าไปเปลี่ยนรหัสผ่านได้ให้ทำดังนี้

1. ไปที่เว็บ outlook.com คลิกที่ **เข้าถึงบัญชีของคุณไม่ได้ใช่หรือไม่** ในหน้าล็อกอิน



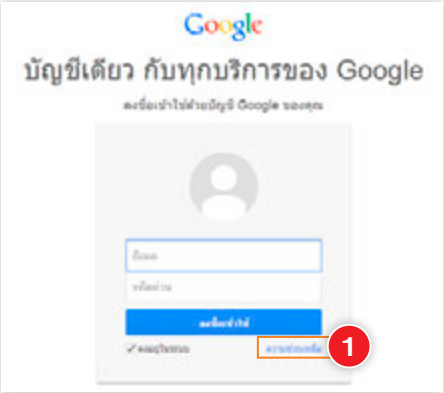
2. ให้ลองเลือก **ฉันลืมรหัสผ่านของฉัน** หรือ**ฉันทราบรหัสผ่านของฉันแต่ไม่สามารถลงชื่อเข้าใช้ได้** เพื่อรีเซ็ตรหัสผ่านดูก่อน โดยจะส่งลิงค์รีเซ็ตรหัสผ่านไปให้ทางอีเมล์สำรอง ถ้าโดนเปลี่ยนอีเมล์สำรองไปแล้วก็จะกู้คืนด้วยวิธีนี้ไม่ได้ ให้เลือก **ฉันคิดว่าผู้อื่นกำลังใช้บัญชี Microsoft ของฉัน** แล้วใส่เหตุผลว่าทำไมถึงรู้ว่าถูกแฮก (ไม่ตอบก็ได้)
3. คลิกปุ่ม **ถัดไป**
4. ทำตามขั้นตอนการกู้คืนแอคเคาท์ของไมโครซอฟท์จนเสร็จสิ้น

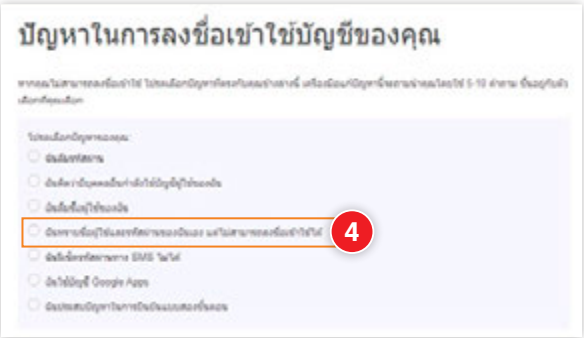


อีกวิธีหนึ่งคือ เข้าไปที่ https://account.live.com/acsr แล้วกรอกข้อมูลในหน้านั้น เพื่อส่งให้เจ้าหน้าที่ของไมโครซอฟท์ ซึ่งส่วนใหญ่จะตอบกลับภายใน 3 วัน

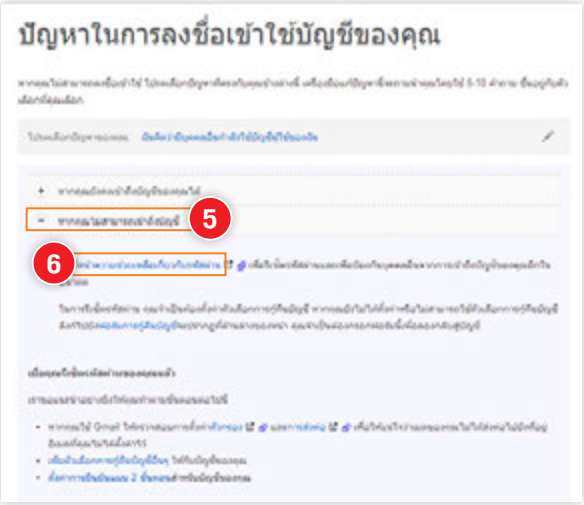
กู้คืนแอคเคาท์ Gmail กลับมา

1. ไปที่เว็บ mail.google.com คลิกที่ **ความช่วยเหลือ** ในหน้าล็อกอิน
2. คลิกเลือก **ฉันประสบปัญหาอื่นในการลงชื่อเข้าใช้** และกรอกอีเมล์แอดเดรส Gmail ที่ถูกแฮก
3. คลิกปุ่ม **ดำเนินการต่อ**



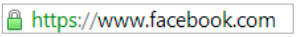


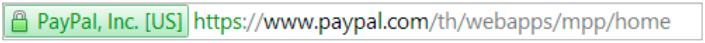
4. คลิกเลือก **ฉันทราบชื่อผู้ใช้และรหัสผ่านของฉันเอง แต่ไม่สามารถลงชื่อเข้าใช้ได้**
5. ระบบจะแนะนำวิธีแก้ไข ให้คลิก **หากคุณไม่สามารถเข้าถึงบัญชี**
6. คลิกลิงค์ **หน้าความช่วยเหลือเกี่ยวกับรหัสผ่าน** เพื่อไปรีเซ็ตรหัสผ่าน โดยจะให้กรอกฟอร์มกู้คืนแอคเคาท์ ให้ทำตามขั้นตอนของ Google จนเสร็จ



เรียกดูเว็บอย่างปลอดภัยด้วย https

ปกติเวลาเข้าเว็บเราจะใช้การรับส่งข้อมูลแบบธรรมดาที่เรียกว่า **http** (ดังที่เห็นในช่องแอดเดรสของบราวเซอร์ทั่วไป) แต่ถ้าเป็นเว็บที่ต้องการรักษาความปลอดภัยของข้อมูลที่สูงกว่าปกติ จะใช้วิธีการที่เรียกย่อๆ ว่า **https (Secured http)** ซึ่งเป็นการแลกเปลี่ยนข้อมูลในเครือข่ายด้วยการเข้ารหัสในตอนที่ส่งข้อมูลออกไป และฝ่ายที่รับข้อมูลก็จะต้องถอดรหัสก่อนจึงจะนำข้อมูลไปใช้ได้ ถ้าระหว่างทางมีใครมาดักจับข้อมูลของเรา ก็จะไม่สามารถถอดรหัสเพื่ออ่านข้อมูลนั้นได้ มักใช้กับเว็บที่จำเป็นจะต้องเข้มงวดด้านความปลอดภัย เช่น เว็บไซต์ของสถาบันการเงินหรือธนาคารต่างๆ ที่ให้บริการทำธุรกรรมออนไลน์ รวมถึงเว็บที่ต้องเข้าใช้งานโดยการล็อกอินด้วยชื่อและรหัสผ่าน เช่น เว็บให้บริการรับส่งอีเมล์, Social Network ต่างๆ ซึ่งเว็บเหล่านั้นจะมีการไปลงทะเบียนเพื่อขอรหัสพิเศษที่เรียกว่า **ใบรับรองดิจิตอล (Digital Certificate)** เพื่อยืนยันตัวตนที่เชื่อถือได้ ซึ่งใบรับรองนี้เองจะถูกนำมาใช้เข้ารหัสและถอดรหัส เมื่อทำงานแบบ https อีกทีหนึ่ง





ดูอย่างไรว่าเว็บไหนมีการเข้ารหัสแบบ https

การตรวจสอบว่าเว็บใดที่มีระบบรักษาความปลอดภัยโดยเข้ารหัสแบบ https ก็ดูได้ง่ายนิดเดียว ให้สังเกตที่แถบ Address หรือช่องใส่ที่อยู่เว็บไซต์ ถ้าเป็นเว็บที่ไม่มีการเข้ารหัสจะแสดงเป็นช่องสีขาว แต่ถ้ามีการเข้ารหัสแบบ https จะแสดงสีเขียว โดยแต่ละบราวเซอร์อาจแสดงแตกต่างกัน แต่ส่วนใหญ่ก็จะใช้สีเขียว ในที่นี้จะยกตัวอย่างบราวเซอร์ IE และ Chrome ซึ่งจะแสดงสัญลักษณ์การเข้ารหัสแตกต่างกันดังนี้

IE : เมื่อเปิดหน้าเว็บที่มีการเข้ารหัสข้อมูลจะแสดงแถบ Address เป็นสีเขียว และจะแสดงที่อยู่เว็บเป็น https ด้วย คลิกที่ เพื่อดูรายละเอียดการยืนยันตัวตนของเว็บไซต์นั้น

Chrome : เมื่อเปิดหน้าเว็บที่มีการเข้ารหัสข้อมูลจะแสดงไอคอนชื่อเว็บสีเขียว และจะแสดงที่อยู่เว็บเป็น https ด้วย คลิกที่ไอคอน จะแสดงรายละเอียดการยืนยันตัวตนของเว็บไซต์นั้น

การใช้งานบราวเซอร์ในมือถือหรือแท็บเล็ตจะมีสัญลักษณ์แม่กุญแจแสดงการเข้ารหัส https เช่นเดียวกับบราวเซอร์ในคอมพิวเตอร์ ดังรูป

การเข้าใช้งานเว็บไซต์ที่จำเป็นจะต้องกรอกข้อมูลส่วนตัวหรือล็อกอินเข้าใช้งานเป็นเรื่องที่ต้องระมัดระวัง หลายครั้งที่แฮกเกอร์มาสร้างหน้าเว็บปลอมหลอกให้กรอกข้อมูลส่วนตัวต่างๆ แล้วดักจับข้อมูลเหล่านั้นไปใช้ในทางที่ไม่เหมาะสม (ดู Phishing หน้า 150) โดยเฉพาะเว็บไซต์ของธนาคารต่างๆ ที่มีบริการทำธุรกรรมออนไลน์ ดังนั้นก่อนที่จะกรอกข้อมูลใดๆ ในหน้าเว็บคุณควรตรวจสอบว่าเว็บไซต์นั้นเข้าใช้ระบบเข้ารหัสความปลอดภัย https อยู่หรือเปล่า ซึ่งเว็บปลอมจะไม่มีใบรับรองจะใช้รูปแบบ http (ไม่มี s และไม่ขึ้นรูปกุญแจ) ส่วนเว็บจริงที่มีใบรับรองยืนยันตัวตนจะใช้รูปแบบ https เพื่อเข้ารหัสข้อมูลก่อนส่งออกไป

รู้จัก “บั๊ก” อันตราย ที่เรียกว่า Heartbleed

บั๊กเป็นสำนวนของโปรแกรมเมอร์ที่แปลว่า “ข้อผิดพลาดในโปรแกรม” ซึ่งกรณีนี้เป็นโปรแกรมของระบบที่เรียกว่า SSL (Secure Socket Layer) ซึ่งอยู่บนฝั่งเซิร์ฟเวอร์ ที่ใช้ในการเข้าเว็บแบบ https (ที่กล่าวไปแล้วในหัวข้อก่อนหน้า) เป็นการเข้ารหัสเพื่อรักษาความลับระหว่างส่งข้อมูลผ่านอินเทอร์เน็ต

บั๊ก Heartbleed ทำให้การเข้ารหัสนี้มีช่องโหว่ ทำให้แฮกเกอร์สามารถเข้ามาล้วงเอารหัสลับที่เป็น “กุญแจ” หรือ key ที่ใช้ถอดรหัสไปจากฝั่งเซิร์ฟเวอร์ได้ ถ้าถอดรหัสนี้ได้ ย่อมสามารถเข้ามาอ่านข้อมูลอื่นๆ ทั้งชื่อและรหัสผ่านของผู้ใช้ ฯลฯ เรียกว่าทำอะไรก็ได้ ซึ่งเป็นเรื่องที่น่ากลัวมาก รวมถึงอ่านข้อมูลต่างๆ เช่น ใบรับรองดิจิตอล (digital certificate) เพื่อเอาไปใช้ปลอมทำเครื่องอื่นขึ้นมาหลอกผู้ใช้ว่าเป็นเซิร์ฟเวอร์นั้นก็ได้ คือทำให้เว็บปลอมของแฮกเกอร์ขึ้น https: และรูปกุญแจได้ทั้งๆ ที่ไม่ใช่เว็บนั้นจริงๆ

อันตรายอื่นๆที่ตามออกมาอีกเรื่อยๆ

การทำงานของระบบในอุปกรณ์ต่างๆก็มีโอกาสที่จะเกิดข้อผิดพลาดหรือพบช่องโหว่กันได้ ซึ่งศัพท์เทคนิคด้านไอทีจะเรียกว่า “บั๊ก” โดยในปี 2013 ก็เพิ่งจะพบบั๊ก *Heartbleed* (ที่กล่าวถึงในหัวข้อนี้) ไม่ทันไร ในปี 2014 ก็ถึงคิวบั๊กใหม่ที่มีชื่อว่า *Shellshock* (เชลล์ช็อค) ที่เป็นช่องโหว่ที่เกิดกับระบบปฏิบัติการ Unix, Linux และ Mac OS ซึ่งเชลล์ช็อคนี้ว่ากันว่าอันตรายยิ่งกว่า Heartbleed เสียอีก เนื่องจากเป็นการเปิดช่องให้แฮกเกอร์เข้ามาควบคุมเครื่องคอมพิวเตอร์ แล้วขโมยเอาไฟล์หรือข้อมูลสำคัญต่างๆไปได้หมดเลย โดยผู้ที่เกี่ยวข้องก็กำลังพยายามหาทางอุดช่องโหว่ที่เกิดขึ้นนี้ เพื่อป้องกันอันตรายก่อนที่จะโดนโจมตีจากแฮกเกอร์

ในอนาคตก็มีโอกาสที่จะพบบั๊กหรือช่องโหว่ใหม่ๆได้อีก ดังนั้นผู้ใช้ควรติดตามข่าวให้ทันเหตุการณ์ เพื่อให้สามารถหาวิธีป้องกันหรือแก้ไขได้อย่างทันท่วงที

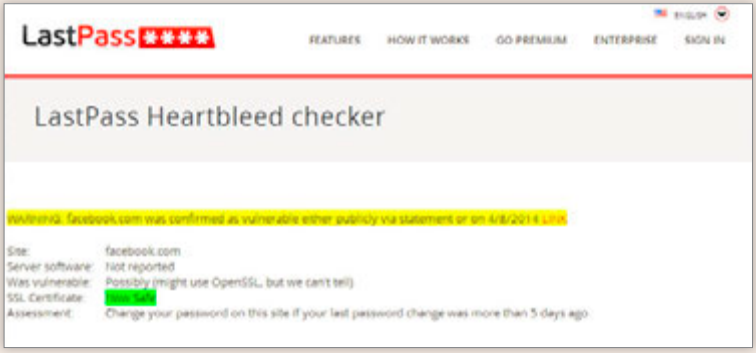
แล้วเราต้องทำยังไง?

เว็บใหญ่ๆ หลายแห่งได้แก้ไขปัญหา Heartbleed นี้ไปแล้ว แต่เราไม่มีทางรู้ว่าก่อนจะรู้ตัวนั้นเซิร์ฟเวอร์ของแต่ละเว็บโดนเจาะเอาข้อมูลไปหรือยัง ดังนั้นทุกแห่งที่ประกาศว่าได้แก้ไขข้อผิดพลาดนี้จนปลอดภัยแล้ว แปลว่า “เรารู้ปัญหาและเปลี่ยนกุญแจบ้านแล้วนะ” แต่ไม่มีใครกล้ารับรองว่า “ก่อนหน้านี้ไม่มีใครแอบเข้ามาขโมยเอาข้อมูลของเราหรือของคุณไปนะ” จึง “แนะนำให้ผู้ใช้เปลี่ยนรหัสผ่านเพื่อความมั่นใจว่าหากแฮกเกอร์ได้ชื่อและรหัสผ่านเก่าไปก็จะใช้ไม่ได้อีก”

ส่วนเว็บที่ยังไม่ได้แก้ปัญหานี้ ถ้าไม่ใช่เว็บที่เคยสมัครสมาชิกหรือกรอกข้อมูลสำคัญเอาไว้ก็ไม่เป็นไร แต่ถ้าเคยกรอกข้อมูลสำคัญหรือใช้บริการจริงจังก็แนะนำให้หลีกเลี่ยงโดยยกเลิกการใช้บริการแบบออนไลน์ไปเสียก่อนเพื่อความปลอดภัย

จะรู้ได้ไงว่าเว็บไหนแก้ข้อผิดพลาดนี้หรือยัง?

ที่เว็บใหญ่ๆ จะรวบรวมรายชื่อและสถานะไว้หลายที่ เช่น mashable.com/2014/04/09/heartbleed-bug-websites-affected, www.cnet.com/how-to/which-sites-have-patched-the-heartbleed-bug นอกจากนั้นหลายที่ก็มีบริการให้ทดสอบ เช่นที่ Lastpass.com, filippo.io โดยใส่ชื่อเว็บของคุณได้เลย เค้าจะส่งสัญญาณไปทดสอบกันเองแล้วแจ้งผลทันที



สำหรับของไทยก็ไปทดสอบได้ที่หน้าเพจของ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association – TISA) www.aciscyberlab.com/hearbleed.php

ถ้าเว็บไซต์ที่ใช้บริการอยู่ถูกเจาะระบบได้จะเสียหายอย่างไร?

สารพัดเรื่องร้ายๆ อาจเกิดได้ แล้วแต่ว่าแฮกเกอร์ที่เจาะเข้ามาจะทำอะไร มีตั้งแต่

- **ขโมยข้อมูลส่วนตัวของเรา** เช่น เรื่องส่วนตัว รูปภาพ เลขที่บัตรเครดิต รวมถึงรหัสผ่านอื่นๆ ถ้าเราเก็บไว้บนเน็ต แล้วขโมยเงินจากบัญชีธนาคารของเราไปซื้อข้าวของแพงๆ ด้วยหมายเลขบัตรเครดิตของเรา หรือขู่กรรโชกว่าจะเปิดเผยความลับ เป็นต้น
- **ขโมยอีเมล์ของเรา** หรือชื่อและรหัสผ่านของเราไปหลอกลวงคนอื่นต่อ เช่น เอาอีเมล์ของเราไปส่งขอยืมเงินจากคนอื่นที่เรารู้จักหรือมีรายชื่ออยู่ หรือเอาชื่ออีเมล์ของเราไปสมัครบริการอื่นๆ ปลอมว่าเป็นเรา แล้วไปทำเรื่องผิดกฎหมายบนอินเทอร์เน็ต เป็นต้น
- **ขโมยตัวตนของเซิร์ฟเวอร์นั้น** คือได้รหัสที่สามารถปลอมเป็นเซิร์ฟเวอร์หรือบริการนั้นๆ ไปหลอกคนอื่นต่อ เช่น สามารถปลอมเครื่องตัวเองเป็นเครื่องของแบงก์ หรือของผู้ให้บริการอีเมล์ ให้คนหลงเชื่อเข้ามากรอกชื่อและรหัสผ่านที่ถูกต้อง จากนั้นเอาไปขโมยเงินหรือปลอมตัวตนไปทำอย่างอื่นต่ออีกก็ได้
- **แฮกเกอร์บางรายขี้เกียจไปทำอะไรต่อเอง** (หรือทำไปแล้วยังไม่หนำใจ) ก็เอาข้อมูลชื่อและรหัสผ่านของผู้ใช้ที่เจาะระบบได้ไปแจกจ่ายหรือขายต่อทีละมากๆ นับร้อยนับพันชื่อ ในตลาดมืดออนไลน์ ให้ผู้ (ร้าย) อื่นซื้อไปทำเรื่องร้ายๆ ต่อในราคางามๆ
- อื่นๆ อีกสารพัด ฯลฯ

อย่าใช้รหัสผ่านเดียวกันกับทุกบริการ

ปกติเราต้องมีรหัสผ่านสำหรับเข้าใช้สารพัดบริการออนไลน์ ไม่ว่าจะเป็นชื่อล็อกอินสำหรับเข้าใช้อีเมล์ที่ Hotmail, Google, Yahoo ฯลฯ, เข้าใช้ Facebook, Twitter, Instagram, Google+, ทำธุรกรรมผ่านเน็ตอีกตั้งหลายแบงก์ ไหนจะ Dropbox, 4Shared, Apple ID, Samsung account เยอะแยะมากมายขนาดนี้จะจำยังไงไหว หลายคนคงใช้เป็นรหัสผ่านเดียวกันไปเลยจำง่ายดี **แต่ต้องระวัง!** ถ้าถูกแฮกไปสักอันก็อาจถูกแฮกที่อื่นไปด้วยได้ง่ายๆ เลย ยิ่งถ้าใช้อีเมล์ที่ผูกกับบริการต่างๆ มากมาย อย่างเช่น Google ที่ระบบชื่อผู้ใช้และรหัสผ่านเดียวใช้ได้กับทุกบริการ ถ้าถูกแฮกไปคงเป็นเรื่องใหญ่เลยทีเดียว (แต่ Google นั้นมีระบบล็อค 2 ขั้นตอนซึ่งทำให้มีความปลอดภัยในการใช้งานมากยิ่งขึ้น –ดูเพิ่มหน้า 97) ดังนั้นเพื่อความปลอดภัย แนะนำให้ตั้งรหัสผ่านสำหรับแต่ละบริการแยกจากกัน อย่าให้ซ้ำกันเป็นอันขาด

รหัสผ่านตั้งมากมายจะจดจำยังไงไหว?

สำหรับคนที่มีรหัสผ่านเยอะที่จนจำไม่ไหว หากจะตั้งไม่ซ้ำกันก็ต้องจดลงสมุดหรือหาโปรแกรมประเภท password manager มาช่วย ซึ่งบางตัวก็ช่วยเก็บชื่อผู้ใช้และรหัสผ่านเฉยๆ บางตัวก็ช่วยทั้งจำแล้วกรอกให้เลยเวลาเข้าเว็บ เช่น

- **Keeper** (ฟรีบน Windows/Mac, ปีละประมาณ 10 USD บน smartphone/tablet)
- **1Password** (Windows/mac/iOS/Android – จ่ายครั้งเดียว ประมาณ 40 USD)
- **Lastpass** (ฟรีบน Windows/Mac, ปีละ 12 USD บน smartphone/tablet)
- **KeePass** (ฟรี! Windows) หรือ KeePassX (ฟรี! Mac/Linux/Unix)
- **RoboForm** (Windows/iOS/Android/Blackberry/Symbian – จ่ายครั้งเดียว ประมาณ 30 USD)

การใช้แอพเหล่านี้ก็ต้องระวังอาจมีพวกที่ปลอมตัวเป็นบริการช่วยจำ แต่ที่จริงขโมยรหัสผ่านไปก็ได้ แต่รายชื่อที่รวบรวมมานี้เชื่อถือได้ ซึ่งบริการเหล่านี้จะให้ผู้ใช้จำรหัสผ่านหลัก หรือ Master password ตัวเดียวพอ (แต่ถ้าลืมก็จบกัน หลายที่เตือนไว้เลยว่าเค้าเข้ารหัสแบบที่เราเปิดได้คนเดียว เจ้าของบริการเองก็เปิดดูรหัสของเราไม่ได้ ดังนั้นถ้าลืม Master password ก็จบ เอาคืนไม่ได้) แต่ข้อเสียอีกอย่างคือโปรแกรมหรือบริการเหล่านี้มักจะไม่ฟรี

ตั้งรหัสผ่านอย่างไรให้ปลอดภัย?

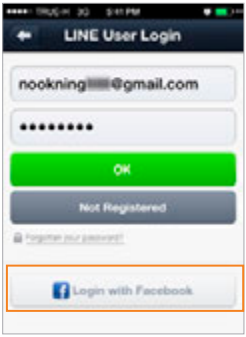
การตั้งรหัสผ่านก็ต้องคิดให้รอบคอบ โดยจะต้องไม่ง่ายจนเกินไป หลังจากตั้งไปแล้วก็ให้เปลี่ยนเป็นครั้งคราวด้วยเพื่อความปลอดภัย แต่ถ้ากลัวว่าตั้งยากหรือเปลี่ยนบ่อยๆ แล้วจะจำไม่ได้ก็สามารถบันทึกไว้ในแอพช่วยเก็บรหัสผ่านโดยเฉพาะ (ดูรายชื่อแอพแนะนำหน้า 91) เพื่อช่วยจำอีกทางหนึ่ง

- **ตั้งรหัสให้ปนกัน** ทั้งตัวอักษรใหญ่-เล็ก ตัวเลข และสัญลักษณ์พิเศษ และยาวอย่างน้อย 8 ตัวอักษร อันนี้หลายเว็บเริ่มมีการแนะนำกึ่งเตือนหรือบางที่บังคับแล้วก็มี เช่น K_s1#pr3 หรือ 01aAS25
- **ตั้งรหัสอย่าให้ซ้ำกันสำหรับแต่ละเว็บ** สาเหตุคือถ้าโดนแฮกเกอร์เจาะเอารหัสผ่านไปได้สักที่ ปกติจะเอาไปไล่หาที่อื่นที่เราน่าจะสมัครไว้ด้วยชื่อหรืออีเมล์เดียวกัน เช่น ถ้าขโมยจากอีเมล์ได้ก็จะเอาไปลองล็อกอินที่ Facebook ก่อน ถ้าเราตั้งรหัสผ่านซ้ำกัน แฮกเกอร์ก็เข้าได้สบายเลย โดยไม่ต้องเจาะระบบของ Facebook หรือบางทีแฮกเกอร์ก็เอาชื่อผู้ใช้และรหัสผ่านของเราที่เจาะมาได้ทีละมากๆ จากที่ใดที่หนึ่งไปไล่แจกฟรีบนอินเทอร์เน็ตซะงั้น
- **เปลี่ยนรหัสบ่อยๆ** อันนี้ถ้ามีเป็นร้อยที่ ไล่เปลี่ยนบ่อยๆ ชีวิตคงยากไป แนะนำว่าถ้าตั้งรหัสผ่านแต่ละที่ให้ไม่ซ้ำกันแล้ว นานๆ ครั้งก็เปลี่ยนรหัสผ่านเสียบ้างเฉพาะที่ที่สำคัญหรือเอาไปผูกกับบริการต่างๆ ไว้เยอะ เช่น อีเมล์หลักๆ ที่เราใช้สักสองสามที่ก็น่าจะพอ

ล็อกอินแบบไม่ต้องสร้างแอคเคาท์ใหม่

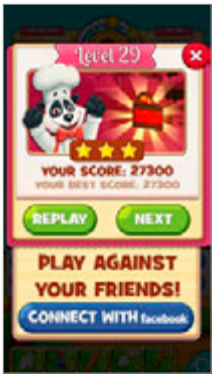
เมื่อต้องเข้าใช้บริการใหม่ๆ บางที่จะสามารถให้ล็อกอินด้วยแอคเคาท์ Facebook หรืออีเมล์ที่มีอยู่แล้วได้เลย สะดวก รวดเร็ว ไม่ต้องกรอกข้อมูลใหม่และไม่ต้องจดจำแอคเคาท์เพิ่ม ในที่นี้จะยกตัวอย่างการล็อกอินด้วย Facebook และ Gmail ดังนี้

ผูกแอพหรือบริการกับ Facebook



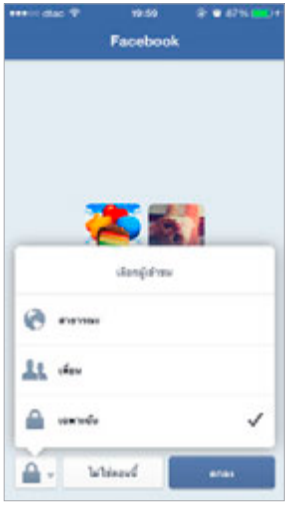
บางแอพหรือบางบริการจะสามารถใช้แอคเคาท์ Facebook ที่มีอยู่มาใช้ผูกกันได้เลย เช่น เกมต่างๆ รวมถึงแอพ LINE ซึ่งมีข้อดีตรงที่ไม่ต้องสร้างและจดจำแอคเคาท์ใหม่เพิ่ม อาศัยระบบความปลอดภัยของ Facebook จัดการแทน แต่ก็มีข้อเสียคือถ้าแอคเคาท์ที่ไปผูกนั้น ถูกแฮกไปก็อาจเข้าใช้แอพหรือบริการที่ผูกไว้ไม่ได้ตามไปด้วย ทำให้ความเสียหายส่งผลต่อเนื่องเป็นลูกโซ่

หลายแอพในโทรศัพท์มือถือและแท็บเล็ตทั้ง iOS และ Android มักจะให้ผูกกับ Facebook เพื่อดึงรายชื่อเพื่อน เข้าถึงข้อมูลส่วนตัว สิทธิ์การโพสต์ หรืออื่นๆ ซึ่งบางสิทธิ์อาจดูก้าวก่ายเรื่องส่วนตัวเกินไป หรืออาจโพสต์เรื่องราวเกี่ยวกับแอพนั้นให้เพื่อนของคุณเห็น ถ้ากลัวว่าเพื่อนจะรำคาญก็ไปตั้งค่าให้โพสต์แบบที่คุณเห็นคนเดียวได้เพื่อไม่ให้โพสต์ไปรบกวนเพื่อนของคุณ หรือไปยกเลิกบางสิทธิ์ที่แอพขอไว้ได้ด้วย ดังตัวอย่างในรูป

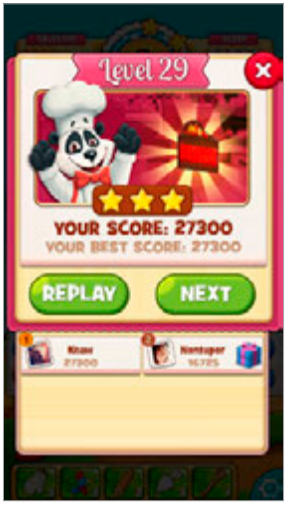


แตะปุ่ม CONNECT WITH facebook พูกเกมเข้ากับแอคเคาท์ Facebook

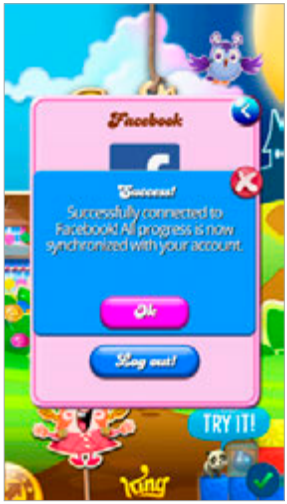
จะให้แตะปุ่ม ตกลง ยินยอมให้เข้าถึงข้อมูลส่วนตัว



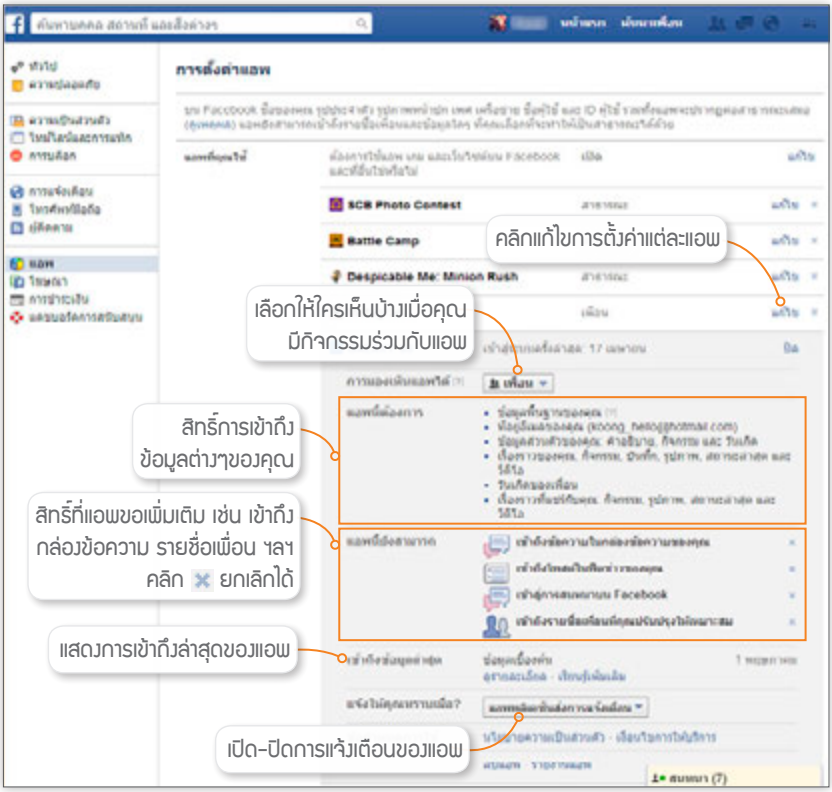
เลือกว่าให้เกมโพสต์ในชื่อของคุณโดยจะให้ใครเห็นบ้าง แล้วแตะปุ่ม **ตกลง**

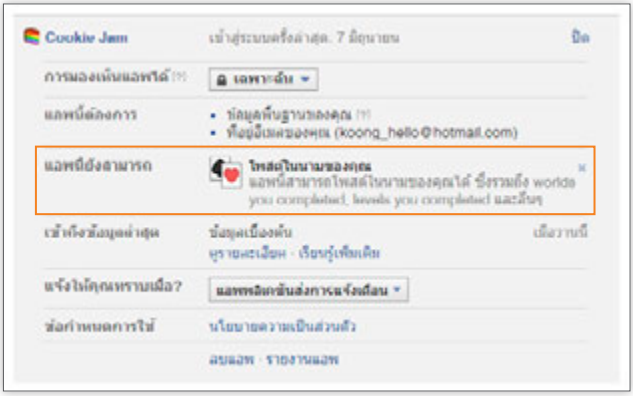


เมื่อผูกกับแอคเคาท์ Facebook แล้วจะแสดงชื่อและคะแนนของเพื่อนที่เล่นเกมเดียวกัน



การขอสิทธิ์จาก Facebook นี้ หลังจากผูกแอคเคาท์และให้สิทธิ์ไปแล้ว คุณสามารถไปเลือกเปิด-ปิดสิทธิ์ต่างๆ ทีหลังได้ โดยเปิดเว็บ Facebook คลิก ▾ ที่มุมขวาบนของหน้าเว็บ (หรือเปิดแอพ Facebook แตะ **เพิ่มเติม**) เลือก **การตั้งค่า** (หรือไปที่ www.facebook.com/settings) แล้วคลิกหัวข้อ **แอพ** จากนั้นคลิกที่ **แก้ไข** บนรายการเพื่อเข้าไปปรับตั้งค่าการอนุญาตสิทธิ์ของแต่ละแอพตามต้องการ (ดูหน้าถัดไป)



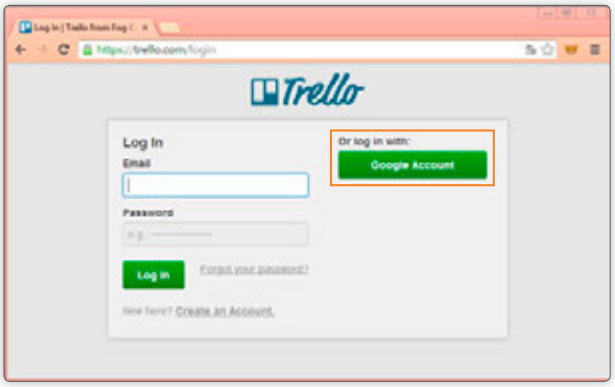


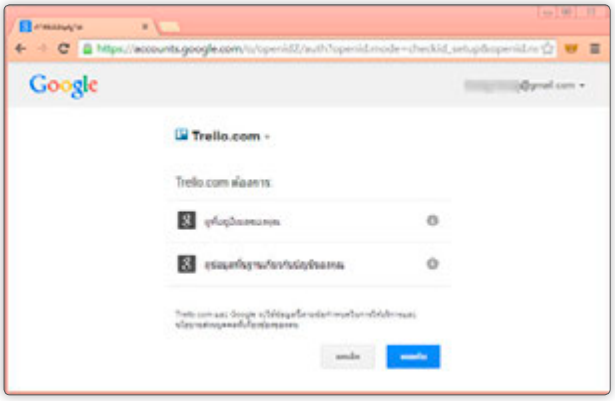
▲ ตัวอย่างแอพที่ขอสิทธิ์การโพสต์ในนามของคุณ คลิก ✕ ยกเลิกได้

ผูกแอพหรือบริการกับอีเมล์

บางแอพหรือบางเว็บให้บริการอาจสมัครโดยล็อกอินด้วยแอคเคาท์อีเมล์ เช่น Gmail ได้โดยไม่ต้องสมัครแอคเคาท์ใหม่ ช่วยให้ไม่ต้องจำชื่อผู้ใช้และรหัสผ่านใหม่เพิ่ม แต่มีข้อเสียคือ ถ้าอีเมล์ถูกแฮกไปได้แล้วเปลี่ยนรหัสผ่าน คุณก็จะไม่สามารถนำแอคเคาท์อีเมล์นั้นมาล็อกอินที่เว็บบริการต่างๆ ที่สมัครไว้ได้อีก

ในที่นี้จะยกตัวอย่างเว็บหนึ่งที่สามารถล็อกอินด้วยแอคเคาท์ Google หรือ Gmail ได้ ในครั้งแรกที่ล็อกอินจะให้ยืนยันการเข้าใช้ด้วยแอคเคาท์ Google โดยจะขออนุญาตขอดูข้อมูลส่วนตัวของคุณด้วย การล็อกอินจะเป็นการล็อกอินผ่าน Google โดยตรง ทางเว็บให้บริการจะไม่มีข้อมูลรหัสผ่านของคุณเลย ดังนั้นการตั้งรหัสผ่านของอีเมล์ที่ใช้ล็อกอินที่อื่นๆ ด้วยนี้ จะต้องรัดกุมกว่าปกติ แนะนำให้ใช้บริการล็อคสองชั้น (ดูหัวข้อถัดไป)



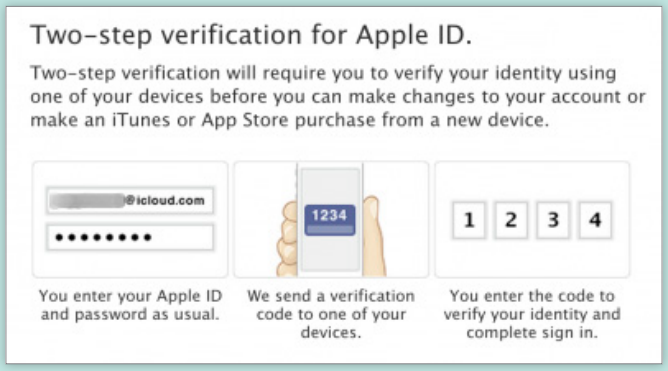


ระบบล็อคสองขั้นตอน (2-Step Verification)

บางเว็บไซต์ที่สำคัญๆ เช่น ผู้ให้บริการอีเมล์อย่าง Gmail ของ Google หรือ Apple ID ของ Apple ที่ใช้กับโทรศัพท์ระบบ iOS มีให้บริการ “ล็อคสองขั้นตอน” หรือ 2-Step Verification โดยจะผูกเบอร์โทรศัพท์กับอีเมล์อย่างแน่นหนา ชนิดที่ว่าถ้าไปล็อกอินเข้าระบบจากเครื่องอื่นที่เราไม่เคยใช้ เช่น แฮกเกอร์แอบเอารหัสผ่านไปล็อกอินจากที่อื่น ก็จะส่งรหัสพิเศษเป็น SMS มาที่มือถือของคุณ (ด้วยความเชื่อที่ว่าแฮกเกอร์คงไม่สามารถขโมยมือถือของคุณไปด้วยได้ และเพราะเค้ากำลังจะเข้าครั้งแรก จึงยังไปแก้เบอร์มือถือที่คุณผูกไว้เดิมไม่ได้) ซึ่งจะต้องนำรหัสนั้นๆ ไปกรอกให้ถูกต้องภายในเวลาที่กำหนดจึงจะเข้าใช้บริการได้ แฮกเกอร์จึงเข้าแอคเคาท์ของคุณไม่ได้

Apple ID

Apple ได้เปิดใช้งานระบบล็อค 2 ขั้นตอนอย่างเป็นทางการในไทยไปเมื่อไม่นานมานี้ (แต่คนยังไม่รู้หรือไม่นิยมใช้กันมากนัก จนมีข่าวภาพลับเฉพาะของดาราดังหลุดออกมาจาก iCloud นั่นแหละ ถึงเริ่มตื่นตัวกัน) โดยผู้ใช้สามารถเข้าไปเปิดใช้งานได้ที่ https://appleid.apple.com คลิกปุ่ม **Manage your Apple ID** จากนั้น Sign in แอคเคาท์ Apple ID ที่คุณใช้อยู่ คลิก **Password & Security** ให้ตอบคำถามของ Apple แล้วคลิกปุ่ม **Continue** จากนั้นให้คลิก **Get Started** เพื่อเปิดใช้งานระบบล็อค 2 ขั้นตอน โดยผู้ใช้จะต้องตั้งว่าจะให้ระบบส่งรหัสผ่านไปที่หมายเลขโทรศัพท์ใดด้วย



Gmail

เข้าไปเปิดใช้งานระบบล็อคสองขั้นตอนที่ https://accounts.google.com/SMSAuthConfig คลิกปุ่ม **เริ่มการตั้งค่า** เพื่อตั้งค่าการล็อคแบบ 2 ขั้นตอน

หลังจากตั้งค่าการล็อค 2 ขั้นตอนแล้ว เมื่อล็อกอินที่เครื่องหรือผ่านโปรแกรม/เว็บ/แอพใหม่ที่ไม่เคยใช้มาก่อนก็ต้องรอรหัสจาก SMS ก่อนเสมอ (หรืออีกวิธีหนึ่ง ให้ติดตั้งแอพ Google Authenticator (รูปซ้าย) – มีให้ใช้ทั้งใน iOS และ Android) ไว้เปิดดูรหัสที่ต้องใช้ได้เลยโดยไม่ต้องรอ SMS เพียงแต่ตั้งให้โปรแกรมผูกกับแอคเคาท์ของคุณให้ถูกก่อนเท่านั้น

ตั้งรหัสผ่านเฉพาะแอพ

การเปิดใช้ระบบล็อค 2 ขั้นตอนของ Google จะทำให้ไม่สามารถเข้าถึงอีเมล์ด้วยแอพต่างๆ บน iPhone, iPad, Android (ยกเว้นแอพ Gmail) รวมถึงโปรแกรม Outlook ที่ใช้บนคอมพิวเตอร์ได้ เนื่องจากยังไม่รองรับการล็อคแบบ 2 ขั้นตอน คุณจะต้องไปตั้งค่า Application Specific password ซึ่งจะเป็นการตั้งรหัสผ่านพิเศษสำหรับยืนยันการเข้าใช้แต่ละแอพที่ติดปัญหาให้เข้าใช้งานได้ปกติ

การตั้งค่า Application Specific password นั้นจะต้องทำกับแต่ละแอพที่ต้องการใช้งานกับแอคเคาท์ Google (หรือ Gmail) โดยจะทำแค่ครั้งแรก (ของแต่ละแอพ) หลังจากนั้นก็จะเข้าใช้แอพได้ตามปกติ โดยให้ทำดังนี้

1 เปิดบราวเซอร์แล้วเข้าไปที่ https://security.google.com/settings/security/apppasswords

2 กรอกชื่อแอพที่ต้องการ แล้วคลิกปุ่ม **สร้างรหัสผ่าน**

3 จะได้รหัสผ่านไปใช้ล็อกอินกับแอพที่ระบุ (กรอกครั้งเดียวในแอพนั้นๆ)

4 คลิกปุ่ม **เสร็จสิ้น** จะปิดหน้านี้ไปและไม่แสดงรหัสขึ้นมาอีก

ล็อคเครื่องไว้ปลอดภัยกว่า

ในโทรศัพท์มือถือหรือแท็บเล็ตที่ใช้งานก็มักจะเก็บข้อมูลส่วนตัวไว้มากมาย ไม่ว่าจะเป็นอีเมล์ รูปถ่ายส่วนตัว จดบันทึกสำคัญ นัดหมายต่างๆ แชท LINE บางคนอาจใช้แอพทำธุรกรรมต่างๆ ซึ่งจะต้องระมัดระวังไม่วางเครื่องทิ้งขว้างให้ใครหยิบไปใช้ได้โดยง่าย นอกจากนี้ยังควรที่จะตั้งรหัสล็อคหน้าจอเอาไว้ด้วย โดยเครื่องรุ่นใหม่ๆ ก็จะมีการสแกนลายนิ้วมือช่วยเพิ่มความปลอดภัยในการใช้งานได้มากยิ่งขึ้น

ล็อคหน้าจอใน iPhone/iPad iOS

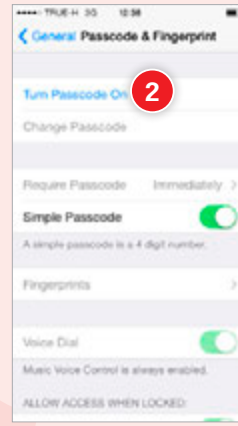
เมื่อกดปุ่มเปิดใช้งานเครื่อง ให้สไลด์หน้าจอไปทางขวา จากนั้นใส่รหัสที่เคยตั้งไว้ให้ถูกต้อง ซึ่งเลือกตั้งได้ 2 แบบคือ ใช้ตัวเลข 4 หลัก (PIN) และแบบตัวอักษรกับตัวเลขรวมกัน (Passcode) และถ้าเป็น iPhone 5s ขึ้นไปจะสามารถตั้งให้ปลดล็อคด้วยการสแกนลายนิ้วมือได้ด้วย

ตั้งรหัสผ่านตัวเลข 4 หลัก (PIN)

1 เข้าไปที่ Settings ▸ Passcode & Fingerprint (ถ้าไม่ใช่ 5s ขึ้นไปจะเป็นคำสั่ง Passcode)

2 แตะ Turn Passcode On

- หากจะตั้งรหัสผ่านได้ไม่จำกัด (เป็นตัวอักษร ตัวเลข หรืออักขระก็ได้ เรียกว่า Passcode) ให้แตะปุ่มปิดที่ Simple Passcode



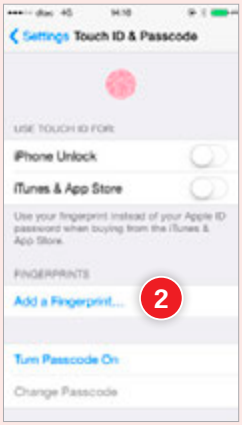
3 ตั้งรหัสเป็นตัวเลข 4 ตัว แล้วยืนยันรหัสอีกครั้ง

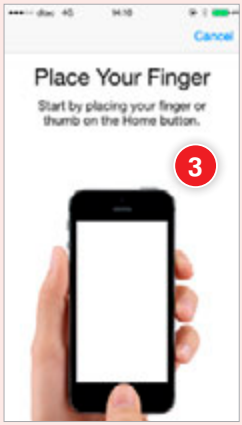
4 แตะ Done

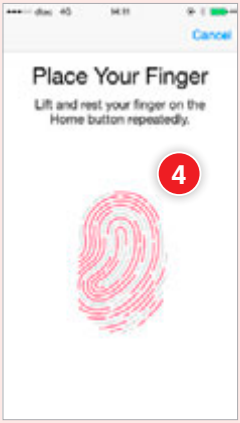
ตั้งค่าสแกนลายนิ้วมือปลดล็อคหน้าจอ (เฉพาะ iPhone 5s ขึ้นไป)

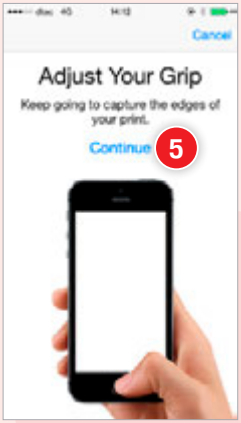
Fingerprint ฟีเจอร์ใหม่ที่เพิ่มความปลอดภัยให้กับ iPhone 5s ขึ้นไปด้วยการสแกนลายนิ้วมือเพื่อปลดล็อคเข้าใช้งานเครื่อง ด้วยเซ็นเซอร์ตรวจสอบลายนิ้วมือของผู้เข้าใช้งานที่อยู่บนปุ่ม Home โดยจะต้องตั้งรหัสผ่านไว้เผื่อใช้กรณีสแกนลายนิ้วมือไม่ได้ด้วย

1. ไปที่ Settings ▸ Touch & Fingerprint
2. แตะ Add a fingerprint...
3. ให้วางนิ้วที่จะใช้ปลดล็อคลงบนปุ่ม Home จนเครื่องสั่นให้ยกนิ้วออก







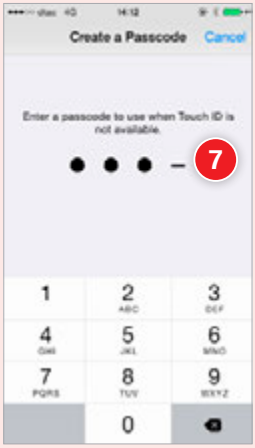


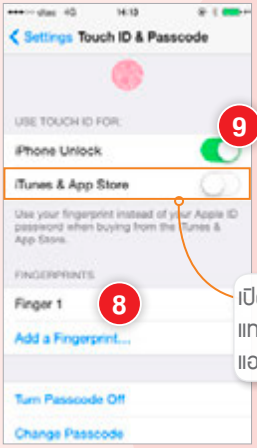
4. วางนิ้วลงใหม่อีกครั้งจนเครื่องสั่น ทำซ้ำจนกว่าเส้นลายนิ้วมือในหน้าจอเป็นสีแดงทั้งหมด
5. จะเข้าสู่หน้า Adjust Your Grip เก็บลายนิ้วมือตรงขอบด้านข้างเพิ่ม ให้แตะ Continue

6 วางนิ้วเดิมลงบนปุ่ม Home เอียงนิ้วไปมาให้เส้นลายนิ้วมือตรงขอบในหน้าจอเป็นสีแดงทั้งหมด เมื่อเก็บลายนิ้วมือเสร็จสมบูรณ์แล้ว ให้แตะ **Continue**

7 จะให้ตั้งรหัสผ่านเพื่อใช้กรณีที่สแกนนิ้วไม่ผ่านและกรอกรหัสอีกครั้งเพื่อยืนยัน

8 ที่หน้าจอ Fingerprints จะเห็นชื่อ Finger 1 แสดงขึ้นมา หากต้องการเพิ่มลายนิ้วมือนิ้วอื่นอีก ให้แตะ **Add a fingerprint...** แล้วทำตามขั้นตอน 3-7 อีกครั้ง





9 ตรง iPhone Unlock จะเห็นว่าถูกเปิดใช้งานอยู่ แสดงว่าตั้งให้ปลดล็อคด้วยลายนิ้วมือแล้ว

ยกเลิกการปลดล็อคด้วยรหัสผ่านหรือสแกนลายนิ้วมือ

ไปที่ **Settings** ▸ **Passcode** ใส่รหัสให้ถูกต้อง แตะเลือก **Turn Passcode Off** ใส่รหัสป้องกันให้ถูกต้อง (ถ้าเป็นแบบตัวอักษรผสมตัวเลข ให้ใส่รหัสแล้วแตะ **Done**)

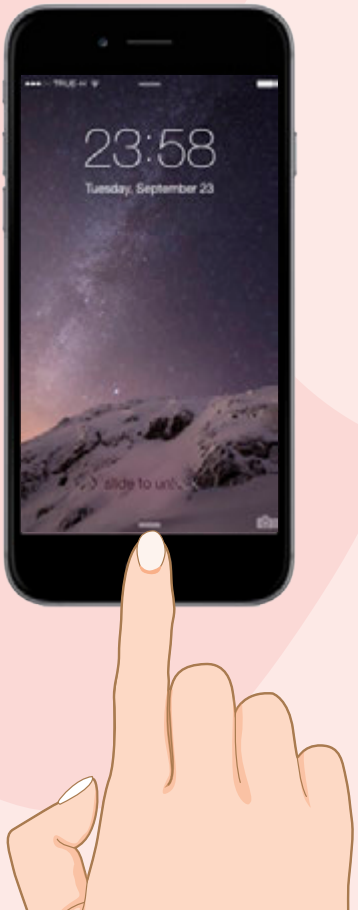
จะกลับไปที่ค่าตั้งต้นของระบบป้องกัน ทำให้ครั้งต่อไปก็ไม่ต้องใส่รหัสผ่านหรือสแกนลายนิ้วมือก่อนเปิดใช้งานเครื่องอีก

ปลดล็อคเข้าใช้งานเครื่อง

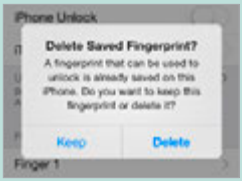
ปลดล็อคด้วยการสแกนนิ้ว

หลังจากตั้งค่าสแกนนิ้ว เมื่อกดปุ่มเปิดใช้งานเครื่อง ในครั้งแรกระบบจะให้ป้อนรหัสผ่านเข้าไปก่อน เพื่อรีเซ็ตให้เข้าสู่การสแกนลายนิ้วมือในครั้งถัดไป

เมื่อจะปลดล็อคครั้งต่อไป ให้วางนิ้ว (ที่เคยตั้งค่าลายนิ้วมือไว้) บนปุ่ม Home เมื่อตรวจสอบว่าถูกต้องก็จะปลดล็อคเข้าสู่หน้า Home ให้ทันที



ถ้าสร้างลายนิ้วมือแล้วยกเลิกการปลดล็อคด้วยรหัสผ่านไป เมื่อเปิดใช้ใหม่โดยแตะที่ **Turn Passcode On** จะถามว่าต้องการเก็บลายนิ้วมือเดิมไว้หรือไม่ (**Keep**) หรือลบทิ้งไปเลย (**Delete**)



ปลดล็อคด้วยรหัสผ่าน

เมื่อกดปุ่มเปิดใช้งานเครื่อง ให้สไลด์หน้าจอไปทางขวา จากนั้นใส่รหัสที่เคยตั้งไว้ให้ถูกต้อง (ถ้าใส่รหัสผิด ให้แตะ **Delete** ลบรหัส แล้วใส่ใหม่)

แตะตัวเลข 4 หลักตามที่ตั้งไว้

พิมพ์รหัสตามที่ตั้งไว้ แล้วแตะ Done

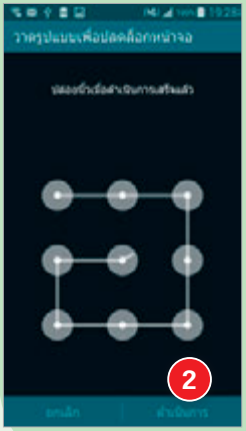
ล็อคหน้าจอใน Android

ในมือถือและแท็บเล็ต Andorid จะมีวิธีล็อคหน้าจอหลากหลายรูปแบบ ซึ่งแต่ละรูปแบบจะมีวิธีการใช้งาน และมีระดับความปลอดภัยที่แตกต่างกันไป วิธีตั้งค่ารูปแบบการล็อคหน้าจอแบบต่างๆ มีให้เลือก 5 รูปแบบด้วยกัน คือ ปัด (Swipe), รูปแบบ (Pattern), ลายนิ้วมือ (Fingerprint), PIN และรหัสผ่าน (Password) กรณีที่ไม่ต้องการล็อคหน้าจอ ให้เลือก ไม่มี (None) โดยไปตั้งค่าได้ที่ **การตั้งค่า** ▸ **ล็อกหน้าจอ** ▸ **ล็อกหน้าจอ** (Settings ▸ Lock screen ▸ Screen lock)

ล็อคหน้าจอแบบ รูปแบบ (Pattern)

การปลดล็อคหน้าจอแบบ รูปแบบ จะใช้การลากเส้นเพื่อปลดล็อคหน้าจอตามรูปแบบที่ตั้งไว้ ซึ่งจะมีระดับความปลอดภัยอยู่ในระดับกลาง

1. แตะที่ **รูปแบบ** (Pattern)
2. วาดผ่านจุดอย่างน้อย 4 จุด (แตะ **ลองใหม่** (Retry) ลองใหม่ได้) เมื่อได้เส้นที่ต้องการแล้วให้แตะ **ดำเนินการ** (Continue)
3. วาดซ้ำอีกครั้งเพื่อยืนยัน เสร็จแล้วแตะ **ยืนยัน** (Confirm)
4. เพื่อเป็นการป้องกันในกรณีที่ลืมรหัสวาดเส้นผ่านจุดจะให้ใส่รหัส PIN สำหรับปลดล็อค แตะ **ดำเนินการ** (Continue) ยืนยันรหัสอีกครั้ง แล้วแตะ **ตกลง** (OK)

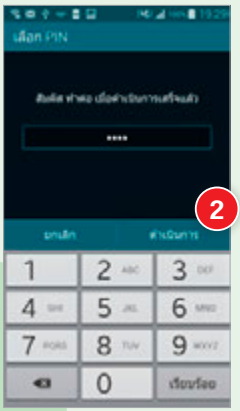


5. เมื่อปลดล็อคเครื่องต้องลากเส้นผ่านจุดให้ถูกต้อง ถ้าลืมก็ต้องใส่รหัส PIN แทน

ล็อคหน้าจอแบบ PIN

การปลดล็อคหน้าจอแบบ PIN จะให้รหัสตัวเลขในการปลดล็อคหน้าจอ ซึ่งมีความปลอดภัยระดับกลางถึงสูง ขึ้นอยู่กับความยากง่ายของรหัสที่คุณกำหนด

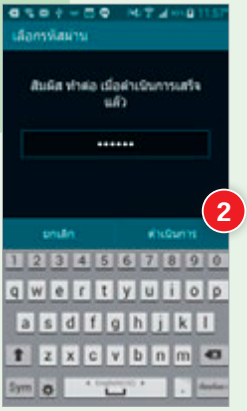
1. แตะที่ **PIN**
2. ป้อนรหัสผ่านตัวเลขที่ต้องการแล้วแตะ **ดำเนินการ** (Continue)
3. ป้อนรหัสผ่านซ้ำอีกครั้ง แล้วแตะ **ตกลง** (OK)
4. เมื่อปลดล็อคเครื่องจะต้องใส่ PIN ให้ถูกต้อง แล้วแตะ **ตกลง** (OK) จึงจะปลดล็อคได้



ล็อคหน้าจอแบบ รหัสผ่าน (Password)

จะคล้ายกับการตั้งค่าการล็อคแบบ PIN แต่จะใช้ตัวอักษรเข้ามาผสมด้วย ซึ่งจะช่วยให้มีความปลอดภัยในระดับที่สูงขึ้น

1. แตะที่ **รหัสผ่าน** (Password)
2. ป้อนรหัสซึ่งประกอบด้วยคีย์อักษรและตัวเลขอย่างน้อย 4 ตัวขึ้นไป เสร็จแล้วแตะ **ดำเนินการ** (Continue)
3. ป้อนรหัสตัวอักษรและตัวเลขที่ตั้งไว้ก่อนนี้อีกครั้งเพื่อยืนยัน เสร็จแล้วแตะ **ตกลง** (OK)

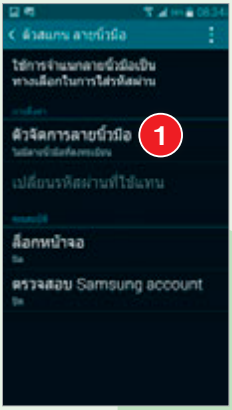


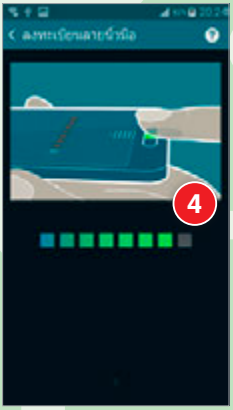
4. เมื่อต้องการจะปลดล็อคเครื่องจะต้องใส่รหัสให้ถูกต้อง แล้วแตะปุ่ม **เรียบร้อย** (Done) บนคีย์บอร์ด

ล็อคหน้าจอแบบ Fingerprint

Fingerprint เป็นการปลดล็อคด้วยลายนิ้วมือ มีความปลอดภัยระดับกลางถึงระดับสูง และเป็น 1 ใน 4 ตัวเลือกสำหรับใช้ปกป้องข้อมูลในโหมดส่วนตัว (Private Mode) อีกด้วย (ใช้ได้เฉพาะเครื่องที่มีอุปกรณ์อ่านลายนิ้วมือเท่านั้น)

1 ไปที่ **การตั้งค่า** (Settings) แตะ **ตัวสแกนลายนิ้วมือ** (Finger Scanner)





2 แตะ **ตัวจัดการลายนิ้วมือ** (Fingerprint manager)

3 แตะ **ตกลง** (OK) ยอมรับการใช้งาน

4 เพิ่มลายนิ้วมือลงไปทั้งหมด 8 ครั้ง จะใช้นิ้วเดิมหรือหลายนิ้วก็ได้ โดยวางนิ้วไว้บนกราฟิกตามรูปตัวอย่าง แล้วลากผ่านปุ่ม Home จนสุด ระบบจะจำรูปแบบและตำแหน่งการวางนิ้วของเรา ให้ทำจนไฟสีเขียวขึ้นครบทุกอัน

5 ให้ตั้งรหัสผ่านสำรองกรณีสแกนลายนิ้วมือไม่ผ่านทั้ง 5 ครั้ง จะต้องใส่รหัสผ่านนี้ให้ถูกต้องถึงจะปลดล็อคหน้าจอได้ โดยใส่รหัสผ่าน (ต้องมีตัวอักษรอย่างน้อย 1 ตัว) แล้วแตะ **ดำเนินการ** (Continue) ยืนยันรหัสผ่านอีกครั้ง แล้วแตะ **ตกลง** (OK)

6 แตะ **ตกลง** (OK) เปิดใช้การปลดล็อคด้วยลายนิ้วมือเลย หรือถ้ายังไม่ใช้ แตะ **ยกเลิก** (Cancel)

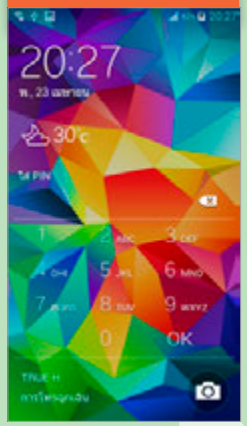
ยกเลิกการปลดล็อคด้วยรหัสผ่านหรือสแกนลายนิ้วมือ

กรณีที่ไม่ต้องการล็อคหน้าจอ ให้เข้าไปตั้งค่าได้ที่ **การตั้งค่า** ▸ **ล็อกหน้าจอ** ▸ **ล็อกหน้าจอ** (Settings ▸ Lock screen ▸ Screen lock) แล้วเลือก **ไม่มี** (None)

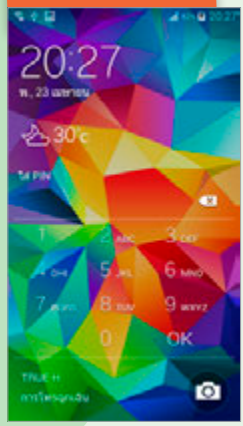
ปลดล็อคเข้าใช้งานเครื่อง

เมื่อเปิดเครื่องจะแสดงหน้า Lock Screen ให้ปลดล็อคตามรูปแบบที่ตั้งไว้ได้เลย ไม่ว่าจะเป็นการสไลด์นิ้วบนหน้าจอ, ใส่รหัสผ่าน, ใส่รหัส PIN, ลากนิ้วไปตามจุด หรือสแกนลายนิ้วมือ

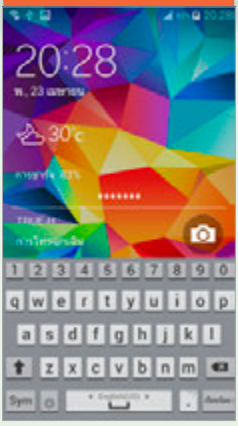
ปลดล็อคแบบสไลด์นิ้ว



ปลดล็อคด้วยตัวเลข



ปลดล็อคด้วยรหัสผ่าน



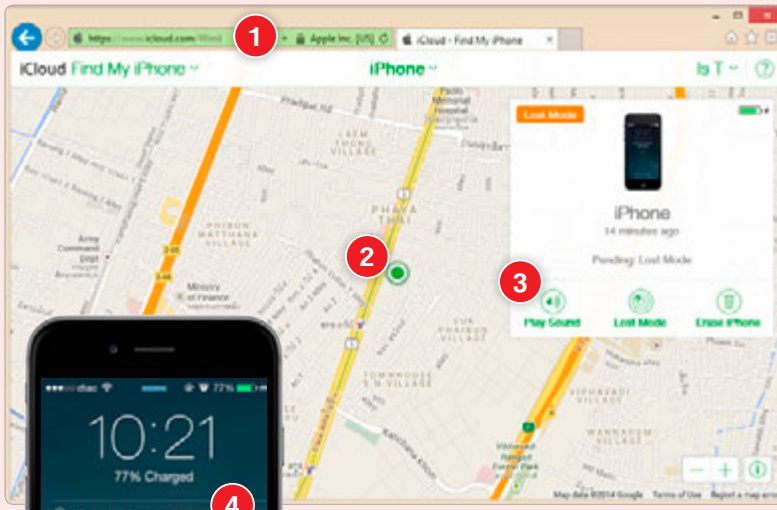
ปลดล็อคด้วยลายนิ้วมือ

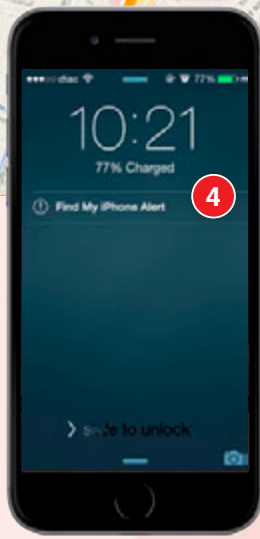
ปลดล็อคแบบลากเส้น

ส่งเสียงเรียกหาอุปกรณ์ที่หายไป

ถ้าหาเครื่องไม่เจอหรือเครื่องหาย คุณสามารถสั่งให้อุปกรณ์ส่งเสียงออกมาเพื่อให้ตามหาได้ หรือถ้าเครื่องตกหายในที่ลับหูลับตาเมื่อส่งเสียงจะได้มีคนพบแล้วติดต่อกลับมาหาคุณได้

เรียกหาอุปกรณ์ iOS





1 เปิดเว็บ www.icloud.com ให้ sign in แอคเคาท์ Apple ID ที่ใส่ไว้ในเครื่องที่จะตามหา แล้วคลิกที่ **Find My iPhone**

2 คลิกหมุดตำแหน่งอุปกรณ์บนแผนที่

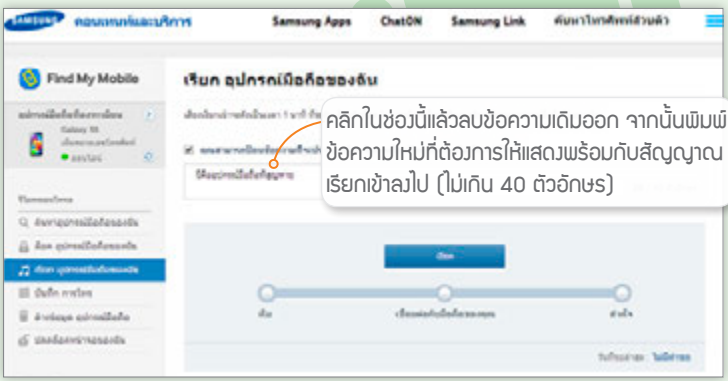
3 คลิก **Play Sound**

4 ที่เครื่อง iPhone จะมีเสียงแจ้งเตือนพร้อมข้อความ Find My iPhone Alert

Android

เรียกหาอุปกรณ์ Android (Samsung)

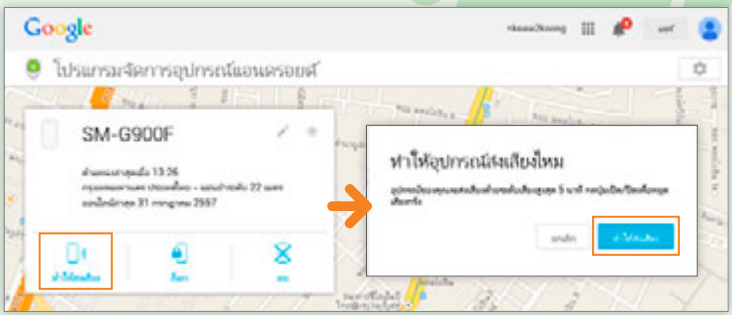
เปิดเว็บ findmymobile.samsung.com แล้ว Sign in แอคเคาท์ Samsung เดียวกับที่ใส่ไว้ในอุปกรณ์ คลิก **เรียกอุปกรณ์มือถือของฉัน** แล้วคลิกปุ่ม **เรียก** ที่มือถือหรือแท็บเล็ตจะส่งเสียงระดับสูงสุด ให้แตะ แล้วสไลด์ไปทางซ้ายหรือขวาเพื่อปิดการเรียกหา



Android

เรียกหาอุปกรณ์ Android (ยี่ห้ออื่นๆ)

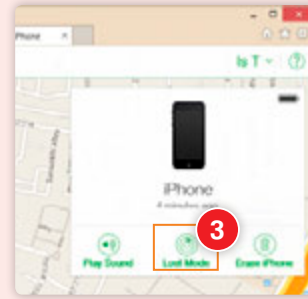
สำหรับอุปกรณ์ Android ที่ไม่ใช่ Samsung ไม่ว่าจะเป็น HTC, LG หรืออื่นๆ คุณก็สามารถเรียกหาอุปกรณ์ได้เช่นกัน ซึ่งเครื่องนั้นจะต้องเปิดอยู่, ล็อกอินแอคเคาท์ Google, เชื่อมต่ออินเทอร์เน็ตได้ และเปิดใช้งาน GPS เอาไว้ โดยค้นหาอุปกรณ์ (ตามขั้นตอนในหัวข้อ “ค้นหาอุปกรณ์ Android (ยี่ห้ออื่นๆ)” หน้า 140) แล้วคลิก **ทำให้ส่งเสียง** คลิก **ทำให้ส่งเสียง** ยืนยัน อุปกรณ์นั้นก็จะส่งเสียงร้องด้วยระดับเสียงสูงสุดเป็นเวลา 5 นาที หรือจนกว่าจะกดปุ่มเปิด/ปิดเครื่อง



ตั้งรหัสผ่านล็อคอุปกรณ์แบบออนไลน์

เมื่อเครื่องหาย ถ้าไม่ได้ตั้งรหัสล็อคเครื่องเอาไว้เราสามารถป้องกันผู้อื่นเข้าใช้งานอุปกรณ์ของเราได้โดยรีโมทเข้าไปล็อคเครื่องด้วยรหัสผ่าน พร้อมทั้งส่งข้อความแจ้งให้โทรกลับได้ด้วย ดังวิธีการดังนี้

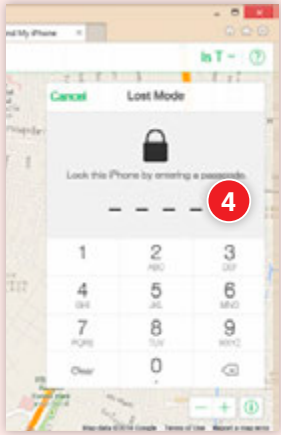
ตั้งรหัสล็อคในอุปกรณ์ iOS

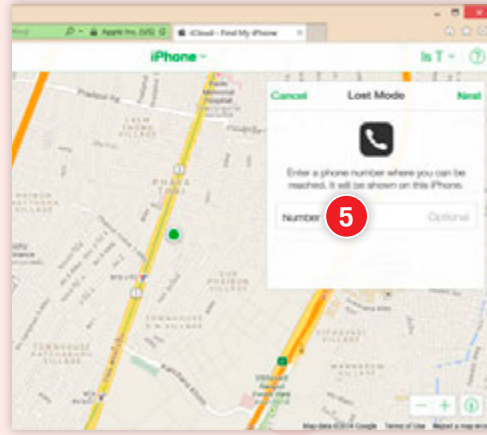


1 เปิดเว็บ www.icloud.com ให้ sign in แอคเคาท์ Apple ID ที่ใส่ไว้ในเครื่องที่จะตามหา แล้วคลิกที่ **Find My iPhone**

2 คลิกหมุดตำแหน่งอุปกรณ์บนแผนที่

3 คลิก **Lost Mode**

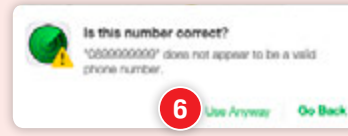


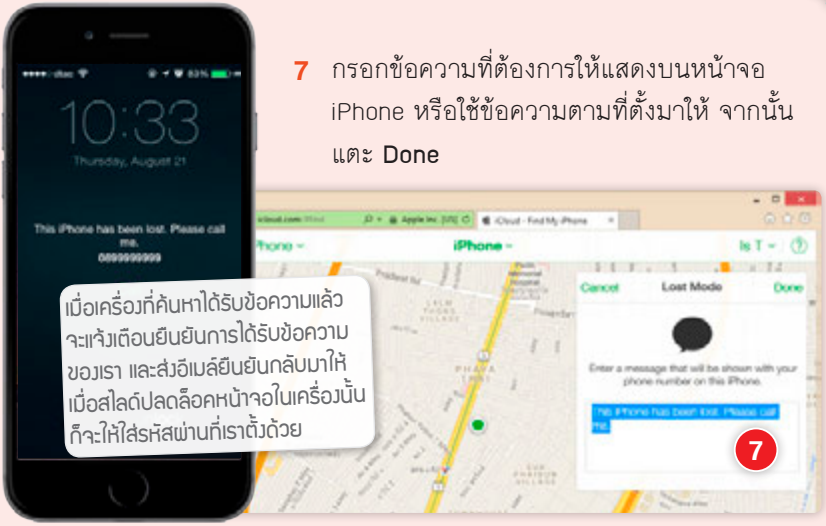


4 พิมพ์รหัสผ่านที่ต้องการตั้งล็อคเครื่องที่หายไป แล้วพิมพ์รหัสผ่านซ้ำอีกครั้งเพื่อยืนยัน

5 กรอกเบอร์โทรศัพท์ที่จะให้ติดต่อกลับ เสร็จแล้วคลิก **Next**

6 จะมีกรอบถามยืนยันว่าเบอร์โทรที่กรอกถูกต้องแล้วใช่หรือไม่ ให้คลิกปุ่ม **Use Anyway**

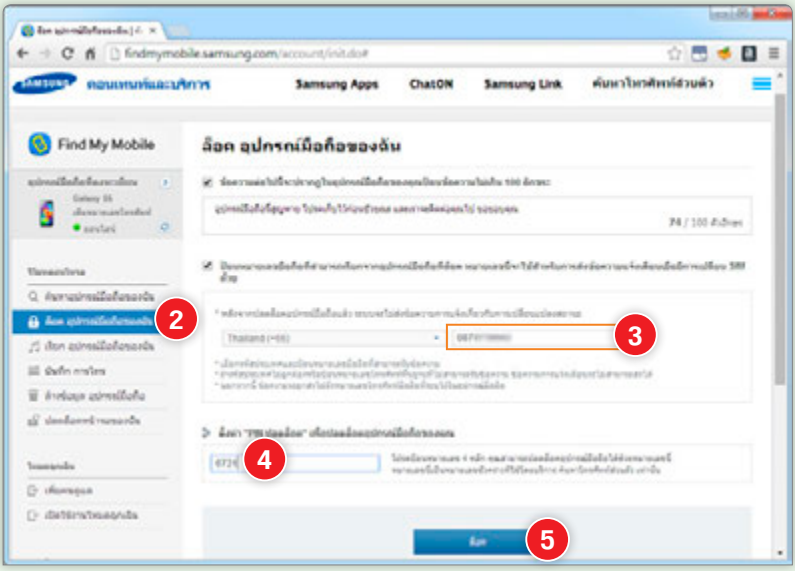




7 กรอกข้อความที่ต้องการให้แสดงบนหน้าจอ iPhone หรือใช้ข้อความตามที่ตั้งมาให้ จากนั้นแตะ **Done**

ตั้งรหัสล็อคในอุปกรณ์ Android (Samsung)

Android



1 เปิดเว็บ findmymobile.samsung.com แล้ว Sign in แอคเคาท์ Samsung เดียวกับที่ใส่ไว้ในอุปกรณ์

2 คลิกที่ **ล็อคอุปกรณ์มือถือของฉัน**

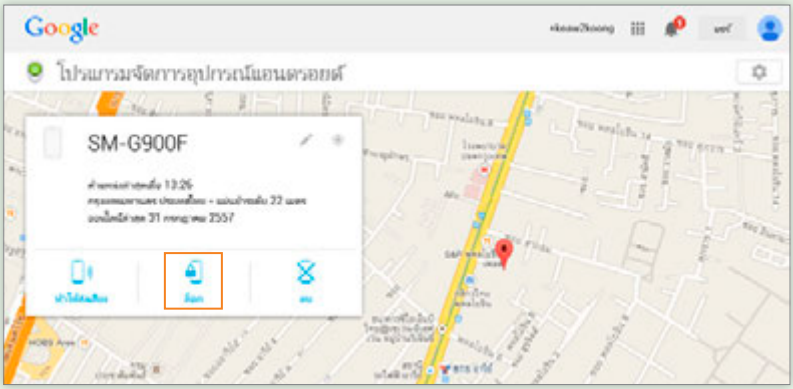
3 ใส่เบอร์โทรศัพท์ที่ต้องการให้ผู้ที่เก็บเครื่องได้ติดต่อกลับ โดยจะมี SMS แจ้งไปยังเบอร์ดังกล่าวให้โดยอัตโนมัติเมื่อล็อคโทรศัพท์เครื่องนั้นเรียบร้อยแล้ว (แก้ไขข้อความได้ตามต้องการและไม่เกิน 100 ตัวอักษร)

4 ใส่รหัสผ่าน เฉพาะตัวเลข 4 หลักลงไป

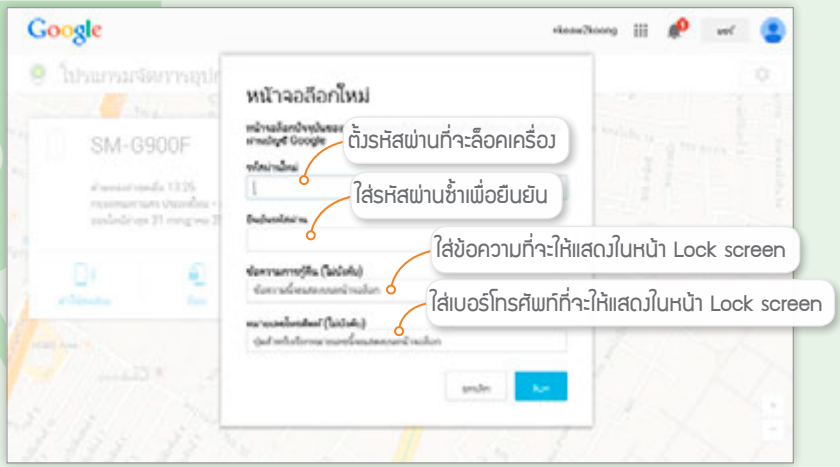
5 คลิกปุ่ม **ล็อค**

ตั้งรหัสล็อคในอุปกรณ์ Android (ยี่ห้ออื่นๆ)

การตั้งรหัสผ่านล็อคอุปกรณ์ Android ที่ไม่ใช่ Samsung คุณสามารถตั้งรหัสผ่านล็อคเครื่องแบบออนไลน์ได้เช่นกัน ซึ่งเครื่องนั้นจะต้องเปิดอยู่, ล็อกอินแอคเคาท์ Google, เชื่อมต่ออินเทอร์เน็ตได้, เปิดใช้งาน GPS และเปิดใช้ Android Device Manager ในอุปกรณ์ด้วย (ดูหน้า 116) โดยค้นหาอุปกรณ์ (ตามขั้นตอนในหัวข้อ “ค้นหาอุปกรณ์ Android (ยี่ห้ออื่นๆ)” หน้า 140) แล้วคลิก **ล็อก**



ให้ตั้งรหัสผ่านและยืนยันรหัสที่กรอกลงไป ใส่ข้อความที่จะแสดงในหน้า Lock screen หลังจากล็อคเครื่องแล้ว (ไม่ใส่ก็ได้) กรอกหมายเลขโทรศัพท์เพื่อโทรกลับหาเจ้าของเครื่อง (ไม่ใส่ก็ได้) แล้วคลิกปุ่ม **ล็อก** ก็จะล็อคอุปกรณ์ด้วยรหัสผ่านที่กำหนดทันที



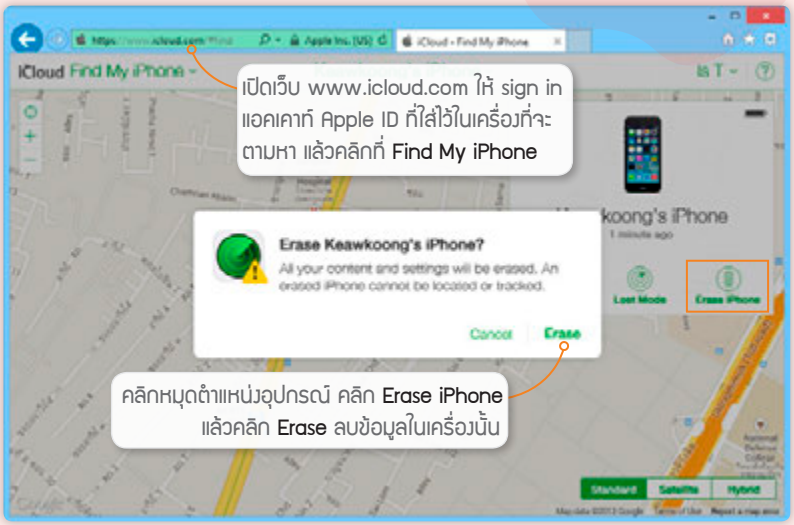
เครื่องหายจะลบข้อมูลในเครื่องอย่างไร

อุปกรณ์ iOS อย่าง iPhone/iPad จะมีฟังก์ชั่น Find My iPhone และ Find My iPad สำหรับติดตามหาอุปกรณ์ ส่วนมือถือหรือแท็บเล็ตที่ใช้ระบบปฏิบัติการ Android ยี่ห้อ Samsung จะมี Find My Mobile ส่วน Android รุ่นอื่นๆ สามารถใช้ Android Device Manager ของ Google ได้เช่นกัน ซึ่งผู้ใช้สามารถตามหา สั่งล็อคเครื่อง หรือลบข้อมูลในเครื่องแบบออนไลน์ได้ โดยจะต้องเปิดเครื่องเอาไว้ รวมทั้งเชื่อมต่อเน็ตและเปิด GPS (Location Services) ด้วยจึงจะค้นหากันเจอ

iOS

ลบข้อมูลใน iPhone/iPad

เมื่อเครื่อง iPhone/iPad สูญหาย โดนขโมย หรือวางลืมไว้ที่ไหนสักแห่ง ก็สามารถค้นหาได้ โดยเครื่องที่จะค้นหานั้นจะต้องเปิดใช้งานฟังก์ชั่น Find My iPhone หรือ Find My iPad ใน iCloud เอาไว้ด้วย (ดูหัวข้อ “เปิดระบบค้นหาเครื่อง” หน้า 135) นอกจากนี้ยังจะต้องเชื่อมต่อเน็ต (ดูหน้า 32) และเปิดการทำงานของ GPS หรือ Location Services ไว้ด้วย (ดูหน้า 133)



ลบข้อมูลในอุปกรณ์ Android ของ Samsung

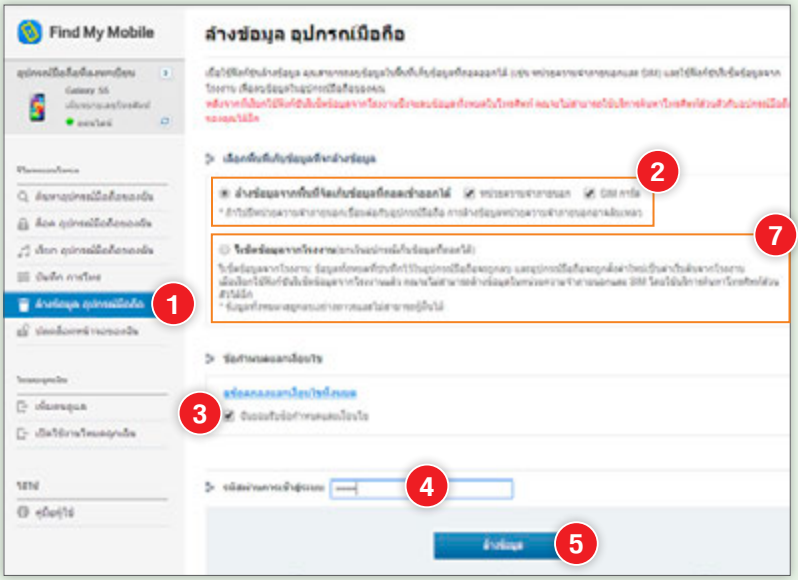
Android

สำหรับมือถือและแท็บเล็ต Samsung ที่ใช้ Android จะมี Find My Mobile ที่ใช้ติดตามค้นหาอุปกรณ์ จะต้อง Sign in แอคเคาท์ Samsung เปิดการทำงานของ GPS หรือLocation Services (ดูหน้า 134) และเชื่อมต่อเน็ตเอาไว้ในเครื่องนั้นด้วย (ดูหน้า 33) จึงจะตามหากันเจอ

หากเครื่องหายแล้วต้องการลบข้อมูลในอุปกรณ์ก็ให้ตามหาเครื่องโดยเปิดเว็บ findmymobile.samsung.com แล้ว Sign in แอคเคาท์ Samsung เดียวกับที่ใส่ไว้ในอุปกรณ์ จากนั้นให้ลบข้อมูลในการ์ดหน่วยความจำที่ใส่เพิ่มก่อน แล้วค่อยรีเซ็ตล้างข้อมูลในเครื่อง (ถ้ารีเซ็ตก่อนจะเป็นการยกเลิกการ Sign in แอคเคาท์ Samsung ทำให้ตามหาเครื่องไม่ได้อีก ก็จะลบข้อมูลในการ์ดไม่ได้)

1 คลิก **ล้างข้อมูลอุปกรณ์มือถือ**

2 คลิกเลือก ◉ **ล้างข้อมูลจากพื้นที่จัดเก็บข้อมูลที่ถอดเข้าออกได้** โดยมีตัวเลือก 2 อย่างคือ หน่วยความจำภายนอก (MicroSD) และ SIM การ์ด (สามารถเลือกทั้ง 2 ตัวเลือกได้)



3 คลิก ☑ **ฉันยอมรับข้อกำหนดและเงื่อนไข**

4 พิมพ์รหัสผ่านของแอคเคาท์ Samsung อันเดียวกันกับที่ใช้ล็อกอิน

5 คลิกปุ่ม **ล้างข้อมูล**

6 คลิกปุ่ม **ตกลง** เพื่อยืนยันการลบข้อมูล

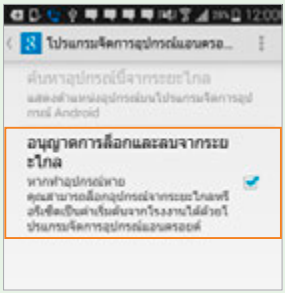
7 คลิกเลือก ◉ **รีเซ็ตข้อมูลจากโรงงาน** แล้วทำซ้ำขั้นตอนที่ 3-6

ลบข้อมูลในอุปกรณ์ Android (ยี่ห้ออื่นๆ)

สำหรับอุปกรณ์ Android ที่ไม่ใช่ Samsung ไม่ว่าจะเป็น HTC, LG หรืออื่นๆ คุณก็สามารถตามไปลบข้อมูลในอุปกรณ์แบบออนไลน์ได้ โดยมีเงื่อนไขว่าเครื่องนั้นจะต้องเปิดอยู่, ล็อกอินแอคเคาท์ Google, เชื่อมต่ออินเทอร์เน็ตได้, เปิดใช้งาน GPS และจะต้องตั้งค่าในอุปกรณ์ก่อนดังนี้

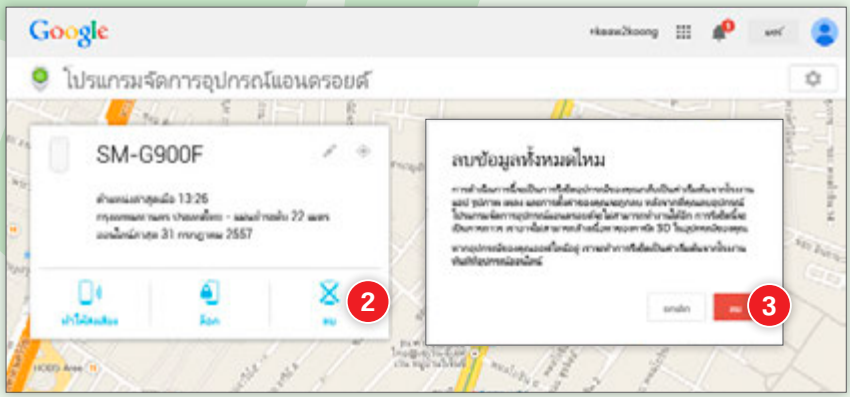
เปิดใช้ Android Device Manager

แตะไอคอน **การตั้งค่า Google** ▸ **โปรแกรมจัดการอุปกรณ์แอนดรอยด์** ให้แตะ ☑ เลือก **อนุญาตการล็อกและลบจากระยะไกล** แล้วแตะ **ทำงาน**

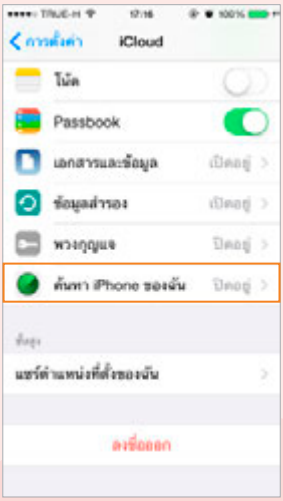


ลบข้อมูลในอุปกรณ์

1. ค้นหาอุปกรณ์ก่อน โดยทำตามขั้นตอนในหัวข้อ “ค้นหาอุปกรณ์ Android (ยี่ห้ออื่นๆ)” (ดูหน้า 140)
2. คลิก **ลบ** เพื่อลบข้อมูลในอุปกรณ์
3. คลิกปุ่ม **ลบ** ยืนยันการลบข้อมูลทั้งหมดในเครื่อง โดยจะรีเซ็ตข้อมูลให้ว่างเปล่าเหมือนเป็นเครื่องใหม่ โดยจะไม่สามารถลบข้อมูลในการ์ดหน่วยความจำภายนอกได้



แสดงความเป็นเจ้าของแม้เครื่องหาย iOS



สำหรับเครื่องที่ใช้ iOS 7 ขึ้นไป เมื่อเปิดใช้งาน Find My iPhone หรือ Find My iPad ใน iCloud ก็จะเป็นการเปิดใช้งาน Activation Lock ด้วย ถ้าคุณทำเครื่องหาย ผู้ที่เก็บเครื่องไปจะต้องใส่รหัสผ่านให้ถูกต้องจึงจะปิดการทำงานของ Find My iPhone ได้ ทำให้คุณสามารถติดตามหาเครื่องต่อไปได้ (ถ้ายังต่อเน็ตและเปิด Location Services เอาไว้) ต่างกับใน iOS รุ่นก่อนๆ ที่ผู้อื่นสามารถปิดการทำงาน Find My iPhone ได้เอง

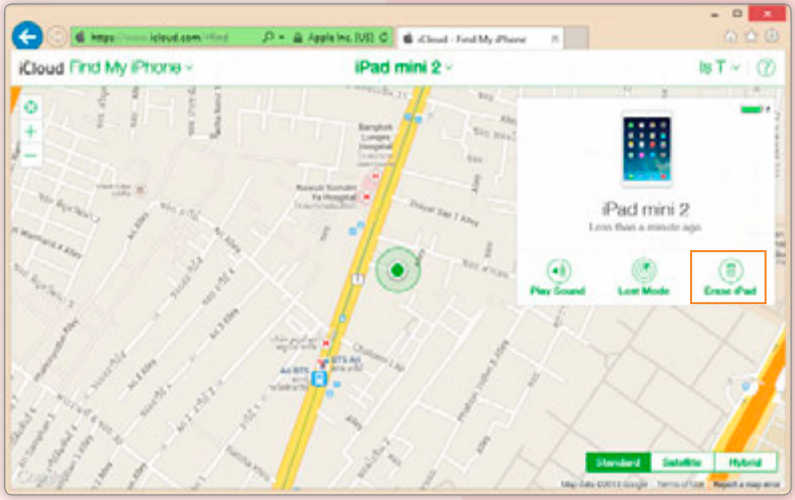
การเปิดหรือปิด Activation Lock ให้ไปที่ **การตั้งค่า** (**Settings**) ▸ **iCloud** แตะ **Find My iPhone** (หรือ **Find My iPad**) แตะเปิดใช้งานที่ **Find My iPhone** แล้วแตะปุ่ม **อนุญาต** (**Allow**) *ที่สำคัญคือคุณห้ามลืมรหัสผ่าน Apple ID ของคุณอย่างเด็ดขาด!!* ไม่เช่นนั้นจะลบข้อมูล หรือรีสโตร์เครื่องไม่ได้เลย

นอกจากนี้เมื่อมีผู้ใดมาสั่งล้างข้อมูลในเครื่องก็จะต้องกรอกรหัสผ่านแอคเคาท์ Apple ID ของเจ้าของเครื่องให้ถูกต้องก่อน รวมถึงการนำเครื่องไปรีสโตร์, ดาวน์เกรด หรืออัพเดทเฟิร์มแวร์ ก็จะติดรหัสผ่าน Apple ID นั้นเช่นเดียวกัน

อย่างไรก็ตาม Activation Lock ก็อาจทำให้เกิดปัญหาในกรณีที่เจ้าของเครื่องลืมรหัสผ่านเสียเอง หรือกรณีซื้อเครื่องมือสอง ก่อนออกจากร้านผู้ซื้อควรตรวจสอบให้เรียบร้อยว่าติด Activation Lock หรือไม่ เพราะไม่เช่นนั้นอาจทำให้ไม่สามารถใช้งานเครื่อง iPhone/iPad มือสองที่ซื้อมานั้นได้

ติดล็อค Find My iPhone ทำไงดี? iOS

ถ้าคุณขาย iPad, iPhone ที่ติดตั้ง iOS 7 ขึ้นไป โดยที่ยังเปิดการทำงานของ Find My iPhone หรือ iPad เอาไว้ ก็จะทำให้ผู้ที่ซื้อเครื่องต่อไม่สามารถรีเซ็ตเครื่อง รีสโตร์ หรือลบแอคเคาท์ iCloud ในเครื่องได้ เจ้าของเครื่องเดิมจะต้องไปใส่รหัสผ่านที่เครื่องหรือบอกรหัสผ่านกับผู้อื่น (ไม่แนะนำ) จึงจะปลดล็อคได้ แต่ถ้าไม่สะดวกที่จะไปทำที่เครื่องก็สามารถลบข้อมูลในเครื่องผ่านเว็บ iCloud ได้ โดยเข้าไปค้นหาเครื่องที่จะปลดล็อค แล้วคลิก **Erase iPhone** หรือ **Erase iPad** กรอกรหัสผ่าน Apple ID แล้วคลิกปุ่ม **Erase** (ดูขั้นตอนหน้า 114) ก็จะล้างข้อมูลทั้งหมดและปลดล็อคแอคเคาท์ของเจ้าของเครื่องไปด้วย แต่อย่าลืมว่าเครื่องนั้นจะต้องเชื่อมต่ออินเทอร์เน็ตและเปิดใช้ GPS หรือ Location Services (บริการหาที่ตั้ง) ไว้ด้วยจึงจะลบได้



การแก้ไขกรณีติดรหัสผ่าน iCloud แล้วจำไม่ได้ ก็ต้องให้ Apple รีเซ็ตให้ โดยโทรไปที่เบอร์ 001-800-65-6957 ซึ่งจะสอบถามข้อมูลหรือขอเอกสารยืนยันการเป็นเจ้าของเครื่องด้วย

แบ็คอัพ/รีสโตร์ข้อมูลบนอุปกรณ์

ระหว่างใช้งานมือถือหรือแท็บเล็ต หลังจากใช้งานไปสักพักก็เริ่มโหลดแอพมาเยอะขึ้น อาจเก็บข้อมูลสารพัดไว้ในเครื่อง คุณควรแบ็คอัพข้อมูลในเครื่องเก็บไว้บ่อยๆ เพื่อรีสโตร์มาใช้ในกรณีที่เครื่องมีปัญหาจนต้องรีเซ็ตเครื่องใหม่ โดยจะทำได้ทั้งใน iPhone/iPad และมือถือ/แท็บเล็ต ที่ใช้ระบบปฏิบัติการ Android

แบ็คอัพข้อมูลใน iPhone/iPad

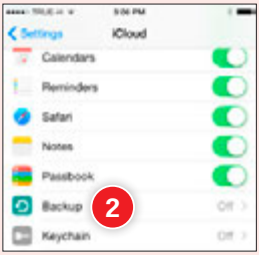
การแบ็คอัพใน iPhone/iPad อาจสั่งทำผ่านโปรแกรม iTunes ที่ติดตั้งในเครื่องคอมพิวเตอร์ ซึ่งเลือกว่าจะแบ็คอัพเก็บไว้ในเครื่องหรือเก็บไว้บน iCloud ก็ได้ อีกวิธีหนึ่งคือแบ็คอัพไว้บน iCloud โดยสั่งจากใน iPhone/iPad เลย ซึ่งจะสามารถแบ็คอัพข้อมูลได้เฉพาะบางอย่างเท่านั้น ดังนี้

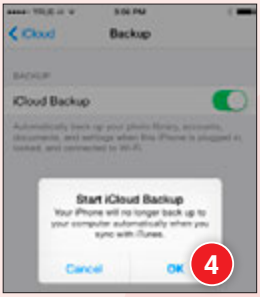
- รายชื่อ Contact, หมายเลขโปรด, รายการโทรออก/รับสาย/ไม่รับ รวมถึง SMS และ MMS
- อีเมล์แอคเคาท์ รวมถึงแอคเคาท์ Game Center
- แอคเคาท์และนัดหมายใน Calendar
- Bookmark และ History ใน Safari, YouTube
- Bookmark และการค้นหาใน Maps
- รูปภาพใน Photos, บันทึก (Notes), Voice Memos
- ข้อมูลในแอพต่างๆ เช่น ข้อความแชทใน LINE รวมทั้งการซื้อของผ่าน In-App Purchase
- การตั้งค่าทั่วไป เช่น วันที่ เวลา รูปแบบวัน/เวลา และรูปแบบชื่อ/นามสกุล การตั้งเวลาล็อคเครื่อง, ตั้งหน้า Home, Lock screen, Wallpaper, Ringtone ฯลฯ

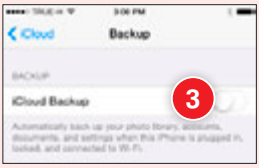
การแบ็คอัพข้อมูลในการใช้งานอุปกรณ์ iOS จะทำได้หลาย 2 แบบ คือ แบ็คอัพข้อมูลไว้ในเครื่องคอมพิวเตอร์ และแบ็คอัพเก็บไว้บน Cloud ซึ่งการแบ็คอัพก็จะต้องทำผ่านโปรแกรม iTunes บนคอมพิวเตอร์ หรือจะทำบนอุปกรณ์เองก็ได้ แต่แบบหลังจะแบ็คอัพได้เฉพาะขึ้น Cloud เท่านั้น ซึ่งการแบ็คอัพข้อมูลจะทำได้ดังนี้

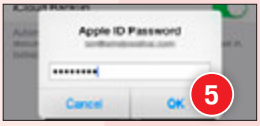
แบ็คอัพข้อมูลไว้บน iCloud ผ่าน iPhone/iPad

เราสามารถแบ็คอัพข้อมูลต่างๆ ไปไว้บน iCloud ได้โดยไม่ต้องเชื่อมต่อกับคอมพิวเตอร์เพื่อแบ็คอัพข้อมูลผ่าน iTunes ซึ่งในขณะที่ชาร์จแบตระบบก็จะแบ็คอัพผ่าน Wi-Fi ให้โดยอัตโนมัติ โดยจะต้องเปิดใช้งาน iCloud Backup เอาไว้ด้วย (ขั้นตอนที่ 1-3 ในหัวข้อนี้) หรือถ้าต้องการแบ็คอัพเดี๋ยวนั้นก็ไปสั่งแบ็คอัพเองได้ ดังนี้









1 ไปที่ **Settings** ▸ **iCloud** (**การตั้งค่า** ▸ **iCloud**)

2 แตะ **Backup/ข้อมูลสำรอง**

3 เปิดใช้งานที่ **iCloud Backup/ข้อมูลสำรอง iCloud**

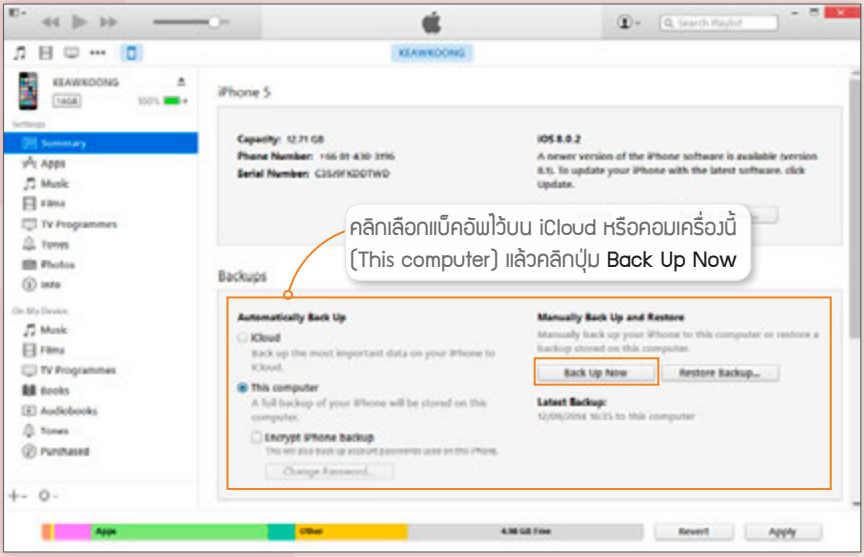
4 แจ้งว่าเมื่อชิงค์ iPhone กับ iTunes จะไม่แบ็คอัพข้อมูลลงคอมอัตโนมัติอีก ให้แตะปุ่ม **OK/ตกลง**

5 ใส่รหัสผ่าน Apple ID แตะ **OK/ตกลง**

- กรณีที่แบ็คอัพครั้งแรก หรือเพิ่ม/ยกเลิกการชิงค์ข้อมูลต่างๆ ให้แตะปุ่ม **Back Up Now /สำรองข้อมูลเดี๋ยวนี้** แทน
- การแบ็คอัพอาจใช้เวลานานขึ้นอยู่กับปริมาณข้อมูล

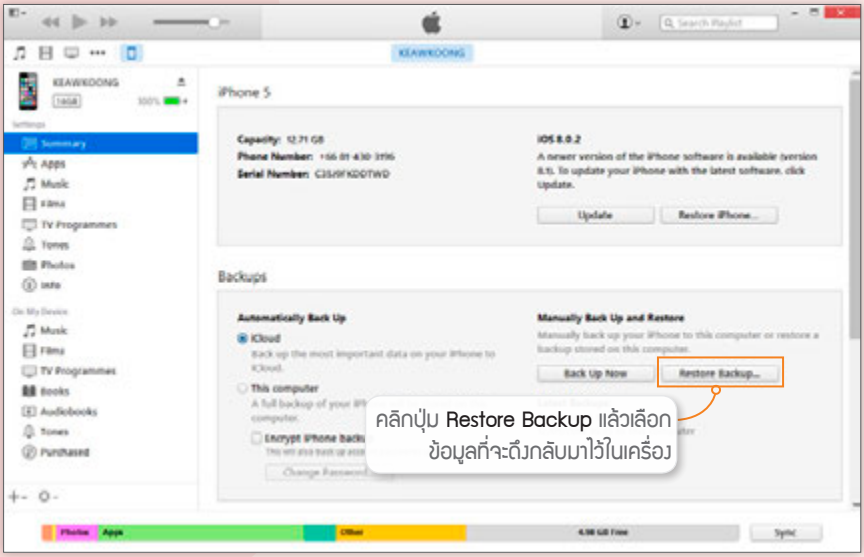
แบ็คอัพข้อมูลด้วยโปรแกรม iTunes

การแบ็คอัพข้อมูลผ่าน iTunes เป็นเรื่องพื้นฐานที่ผู้ใช้อุปกรณ์ iOS ควรรู้ไว้ และควรจะทำบ่อยๆ เพื่อสำรองข้อมูลไว้กรณีเครื่องเสีย, หาย, ซื้อเครื่องใหม่ เป็นต้น เมื่อจำเป็นก็จะสามารถนำข้อมูลเหล่านั้นมาลงใหม่เพื่อใช้งานได้อีกครั้ง ซึ่งการแบ็คอัพด้วยโปรแกรม iTunes นั้นจะเลือกได้ว่าต้องการแบ็คอัพข้อมูลเก็บไว้บนเครื่องคอมพิวเตอร์หรือจะเก็บไว้บน iCloud ก็ได้ **แนะนำให้แบ็คอัพไว้บนคอมพิวเตอร์ แล้วเปิดใช้งาน iCloud Backup ที่อุปกรณ์ iOS เอาไว้เพื่อให้ระบบแบ็คอัพขึ้น iCloud อัตโนมัติ** (ขั้นตอนที่ 1-3 ในหัวข้อก่อนหน้า) การแบ็คอัพบน iTunes จะทำได้ดังนี้



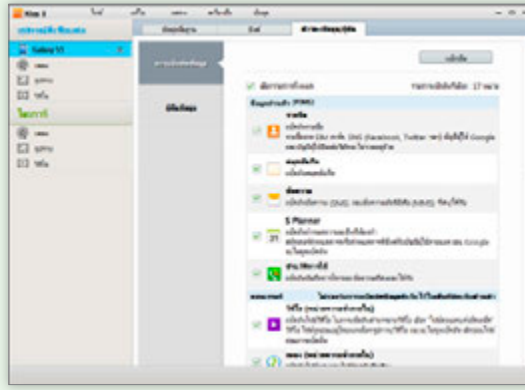
รีสโตร์ข้อมูลที่แบ็คอัพไว้ใน iTunes

หลังจากแบ็คอัพข้อมูลใน iPhone/iPad เก็บไว้แล้ว ถ้าต้องการเรียกข้อมูลเก่าคืนมาจะทำได้ดังนี้

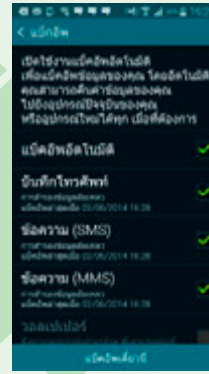


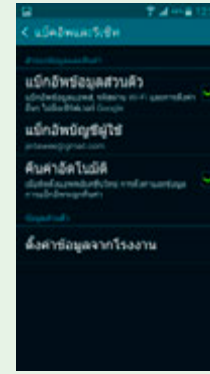
แบ็คอัพข้อมูลในมือถือ/แท็บเล็ต Android

สำหรับมือถือหรือแท็บเล็ต Android สามารถแบ็คอัพข้อมูลได้เช่นกัน ทั้งแบ็คอัพไปเก็บไว้ที่ Cloud ของ Google (ทำได้บน Android เกือบทุกรุ่น) หรือถ้าใช้ Samsung จะเก็บบน Cloud ของแอคเคาท์ Samsung หรือเก็บไว้ในคอมพิวเตอร์ผ่านโปรแกรม Samsung Kies ก็ได้



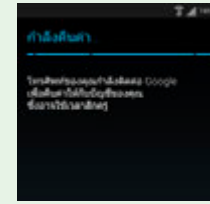
การแบ็คอัพนั้นถ้าใช้เครื่อง Samsung จะเลือกแบ็คอัพข้อมูลแต่ละชนิดได้ค่อนข้างครบ โดยจะเก็บไว้ที่ Cloud ของ Samsung (รูปซ้าย) แต่ถ้าใช้ Android รุ่นอื่นๆ จะต้องแบ็คอัพไว้ที่แอคเคาท์ Google (รูปขวา) ซึ่งจะแบ็คอัพได้เฉพาะข้อมูลส่วนตัว พวกข้อความ SMS หรือประวัติการโทร จะไม่แบ็คอัพให้ต้องหาโปรแกรมเสริมมาทำต่างหากเอง)





รีสโตร์ข้อมูลที่แบ็คอัพไว้

หลังจากแบ็คอัพข้อมูลไว้แล้ว เมื่อล้างเครื่องก็สามารถรีสโตร์กลับมาอัตโนมัติ หรือจะรีสโตร์เองทีหลังหรือทำผ่านโปรแกรม Samsung Kies ก็ได้เช่นกัน



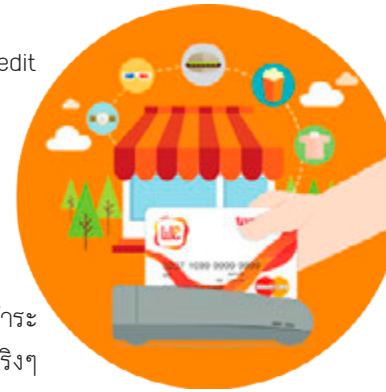
ชำระเงินออนไลน์ได้ทางไหนบ้าง?

การชำระเงินแบบออนไลน์จะทำได้หลายวิธี ซึ่งก็จะมีความปลอดภัยในระดับที่แตกต่างกัน โดยพอจะสรุปได้ดังนี้

- **โอนเงินออนไลน์** ด้วยบริการ Internet Banking ของแต่ละธนาคาร ทำได้ทั้งโอนเงิน เช็คยอด ดูรายการเคลื่อนไหวทางบัญชี ฯลฯ ซึ่งจะต้องไปสมัครใช้บริการกับทางธนาคารที่ใช้บริการก่อนจึงจะทำได้
- **ชำระผ่านตัวกลาง** อย่าง PayPal, PaySbuy, THAIEPAY โดยเป็นการเติมเงินเข้าไปในระบบไว้ใช้ซื้อของออนไลน์แล้วหักจากบัญชี ข้อดีคือถ้าไม่ได้รับของที่ซื้อหรือของที่ได้มีปัญหาก็สามารถขอเงินคืนได้

- **ชำระด้วยบัตรเครดิต** โดยกรอกข้อมูลบัตรให้ครบถ้วน ก็สามารถใช้ชำระค่าสินค้าและบริการต่างๆ ได้สะดวก มีความปลอดภัยกว่าการโอนเงินโดยตรง โดยสามารถยกเลิกการชำระได้ถ้าร้านค้ามีปัญหา

- **ชำระด้วยบัตรเครดิตเสมือน** (Virtual Credit card) ตัวอย่างเช่น mPAY ของ AIS หรือ WeCard ของ True ที่เชื่อมต่อกับ TrueMoney หรือ e-Wallet ได้ในบัตรเดียวกัน และที่ออกให้โดยธนาคารต่างๆ อย่าง กสิกรไทยและกรุงเทพ โดยผู้ใช้จะมีตัวเลขบัตรและรหัส CVV ไว้ใช้กรอกเพื่อชำระด้วยบัตรเครดิตได้เหมือนเป็นบัตรเครดิตจริงๆ



- **บัตรเติมเงิน TrueMoney** ซื้อเป็นบัตรเติมเงินตามมูลค่าที่ต้องการ ใช้เพื่อชำระค่าสินค้าและบริการต่างๆ ไม่ว่าจะเติมเงินโทรศัพท์ของ True, เติมเงินเกมออนไลน์, ซื้อสติกเกอร์ LINE, ซื้อสินค้าออนไลน์ ฯลฯ

- **ชำระรวมกับค่าโทรศัพท์** สำหรับผู้บริการโทรศัพท์เคลื่อนที่แบบรายเดือนของ AIS สามารถซื้อแอพ สติกเกอร์ LINE หรือไอเท็มในเกม โดยชำระรวมบิลมากับค่าโทรศัพท์ได้เลย (ล่าสุดได้ยกเลิกระบบนี้ไปแล้วแต่อาจเปิดใช้อีกในอนาคต)

- **บิตคอยน์ (Bitcoin) เงินบนเน็ตที่ไม่อิงกับใคร** เงินที่ใช้แลกเปลี่ยนหรือชำระค่าสินค้ากันบนอินเทอร์เน็ตนั้น ส่วนมากจะอ้างอิงกับสกุลเงินจริง เช่น ในไทยใช้ทรูมันนี่ (True Money) หรือตัดบัตรเครดิต ทั้งแบบบัตรจริงและบัตรเสมือนที่ต้องเติมเงินต่างหาก เช่น mPay ของ AIS หรือที่มีบัญชีเทียบเท่า เช่น Paysbuy, Paypal แต่ยังมีเงินแบบหนึ่งที่ใช้ได้เฉพาะบนอินเทอร์เน็ตและไม่ผูกกับสกุลเงินใดๆ หรือต้องให้สถาบันการเงินหรือผู้ให้บริการอินเทอร์เน็ตรายใดรองรับเลย เงินนี้เรียกว่า บิตคอยน์ (Bitcoin)

การที่ไม่มีสถาบันการเงินหรือองค์กรใดๆ รองรับ แปลว่าบิตคอยน์ต้องมีระบบควบคุมในตัวเองว่าใครถือเงินสกุลนี้ในกระเป๋าอยู่เท่าไหร่ ไม่ใช่ใครจะบอกว่าฉันมีเงินอยู่เท่านั้นเท่านี้ก็อ้างลอยๆ ได้ วิธีการก็คือ ทุกครั้งที่มีการรับหรือจ่ายเงิน จะต้องมีการเชื่อมต่อเน็ต และส่งข้อมูลไปบอกซอฟต์แวร์บิตคอยน์ในเครื่องอื่นๆ ว่าเงินมีการเปลี่ยนมือมูลค่าเท่าไหร่ (โดยไม่เปิดเผยว่าใครโอนให้ใคร แต่เป็นการจำกัดจำนวนเงินที่มีไม่ให้พิมพ์หรือสร้างเงินขึ้นมาเองลอยๆ จนเกิดภาวะเงินเฟ้อ) ซึ่งจะมีการเข้ารหัสข้อมูลอย่างแน่นหนาไม่ให้แก้ไขตามชอบใจได้

นอกจากนี้เพื่อรองรับการใช้งานที่เพิ่มมากขึ้นเรื่อยๆ บิตคอยน์ก็มีระบบที่ยอมให้สร้างหรือพิมพ์เงินเพิ่มได้ในปริมาณจำกัดทีละน้อย โดยผู้ที่จะทำเพิ่มจะต้องเอาเครื่องคอมพิวเตอร์มาคำนวณตามสูตรเพื่อให้ได้รหัสที่ใช้แทนเงินเพิ่มขึ้น และเป็นการช่วยตรวจสอบ transaction การโอนเงินบิตคอยน์ต่างๆ ที่เกิดขึ้นไปด้วย สูตรคำนวณนี้จะมีการปรับตัวเองให้ซับซ้อนขึ้นเรื่อยๆ ตามการขยายตัวในการใช้งานบิตคอยน์ และยังเผื่อชดเชยความเร็วเครื่องคอมพิวเตอร์รุ่นใหม่ๆ ที่สูงขึ้นเรื่อยๆ ด้วย แปลว่าไม่ใช่จะสร้างเพิ่มกันได้ง่ายๆ หรือมากๆ จึงเรียกกันว่าเป็นการ "ขุด" หรือทำเหมือง (mining) บิตคอยน์ นั่นเอง

อัตราแลกเปลี่ยนของบิตคอยน์นั้นไม่คงที่ อาจจะขึ้นลงทีละมากๆ หรือแกว่งแบบหวือหวามากกว่าเงินสกุลอื่นๆ อยู่สักหน่อย ใครที่จะใช้หรือรับชำระในสกุลเงินบิตคอยน์อาจต้องคอยปรับราคาเพื่อชดเชยอัตราแลกเปลี่ยนให้เหมาะสม ซึ่งปัจจุบันบางพื้นที่ เช่น รัฐแคลิฟอร์เนียของสหรัฐ ก็ให้การรับรองบิตคอยน์แล้ว หรือร้านออนไลน์ เช่น Dell ที่ขายคอมพิวเตอร์ ก็เริ่มรับชำระเงินด้วยบิตคอยน์แล้วเช่นกัน

ข้อดีของบิตคอยน์คือ ใครๆ ก็ใช้ได้ ไม่จำเป็นต้องมีบัญชีธนาคาร และไม่มีการคิดค่าธรรมเนียม (processing fees) แบบสถาบันการเงิน เพราะเจ้าของเครื่องที่ช่วยควบคุมหรือตรวจสอบการรับ-จ่าย จะได้รางวัลหรือรายได้จำนวนหนึ่งจากการทำ mining อยู่แล้ว

ข้อเสียของระบบชำระเงินที่ไม่มีคนกลางแบบนี้ก็คือ ไม่สามารถสร้างทดแทนได้ ดังนั้นถ้าเครื่องหรือฮาร์ดดิสก์ที่เก็บเงินบิตคอยน์ไว้เสียหรือสูญหาย และไม่ได้แบ็คอัพข้อมูลที่จะนำมา restore ในเครื่องใหม่ได้เอาไว้ เงินบิตคอยน์ดังกล่าวก็จะหายไปด้วย

อีกปัญหาของบิตคอยน์คือ การที่มันไม่มีข้อมูลการชำระเงินว่าใครจ่ายใครให้ตามรอยได้อย่างการทำธุรกรรมอื่นๆ ที่ผ่านธนาคาร ทำให้ถูกนำไปใช้ในการโอนเงินที่ผิดกฎหมายได้มาก เช่นเดียวกับการจ่ายด้วยเงินสดที่เป็นธนบัตรหรือเหรียญนั่นเอง

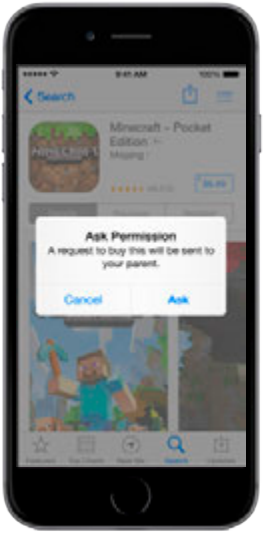
จ่ายเงินออนไลน์ต้องระวังอะไรบ้าง?

ยิ่งสะดวกในการจ่ายมากเท่าไหร่ ก็ต้องระวังอันตรายมากเท่านั้น ซึ่งการชำระเงินแต่ละวิธีก็จะมีข้อดีและข้อด้อยแตกต่างกันไป โดยจะมีข้อควรระวังที่นักช้อปปิ้งออนไลน์ควรรู้ดังนี้

- การโอนเงินให้ร้านค้า เป็นช่องทางการชำระเงินที่มีความเสี่ยงสูง ซึ่งถ้าร้านนั้นโกงไม่ยอมส่งของให้โอกาสที่จะได้เงินคืนนั้นยากมาก
- การชำระผ่านบัตรเครดิต ที่ดูจะปลอดภัยหน่อยก็อาจมีปัญหา ถ้าตอนกรอกข้อมูลบัตรมีแฮกเกอร์มาดักจับเอาข้อมูลไป ซึ่งอาจจะนำไปซื้อสินค้ามูลค่าสูงๆให้เราต้องจ่ายโดยไม่รู้ตัวได้ ซึ่งขั้นตอนการแสดงหลักฐานกับทางธนาคารว่าเจ้าของบัตรไม่ได้เป็นคนซื้อจริงนั้นอาจจะทำได้แต่ค่อนข้างยุ่งยาก
- การใช้บัตรเครดิตเสมือน จะปลอดภัยกว่าบัตรเครดิตจริง เนื่องจากวงเงินในบัตรจะไม่เยอะเท่า โอกาสที่จะเสียเงินจำนวนมากก็น้อยลง
- ระวังการเปิดเผยข้อมูลส่วนตัว เช่น เลขที่บัตรเครดิต และข้อมูลอื่นๆ ที่เกี่ยวข้อง เช่น วงเงิน บัตรเสริม ที่อยู่ที่ส่งใบแจ้งหนี้ รหัส ATM หรือข้อมูลอื่นที่อาจใช้ยืนยันตัวตนของคุณได้ในกรณี (อ้างว่า) ลืมรหัสผ่าน เช่น เลขประจำตัวประชาชน วันเดือนปีเกิด และข้อมูลประเภทคำถามส่วนตัว (Security Question) เช่น รถคันแรก สีที่ชอบ นามสกุลเดิมใครได้ไปอาจแอบอ้างเป็นตัวคุณได้

ระวัง! อย่าให้เด็กรู้รหัสผ่านของคุณ

ถ้าลูกของคุณใช้สมาร์ทโฟนไม่ว่าจะเป็น Android หรือ iPhone/iPad คุณอาจจะระแวงว่าเด็กน้อยจะแอบซื้อแอพต่างๆ ไม่ว่าจะตั้งใจหรือรู้เท่าไม่ถึงการณ์ ซึ่งใน iOS 8 ขึ้นไปจะมีฟังก์ชั่นการแชร์แอพที่ซื้อให้กับคนในครอบครัวได้สูงสุด 6 คนด้วยบัตรเครดิตเดียว เมื่อเด็กอายุต่ำกว่า 13 ปีจะโหลดแอพที่เสียเงินก็จะส่งข้อความมาขออนุญาตผู้ปกครองก่อน หลังจากผู้ปกครองอนุญาตจึงจะซื้อแอพนั้นได้



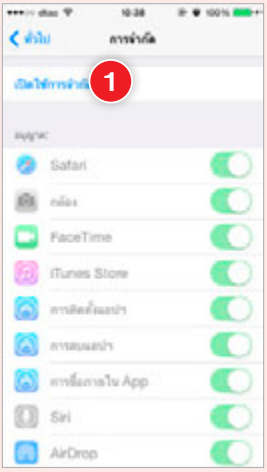
แต่ช่องโหว่ของการที่เด็กจะซื้อแอพด้วยแอคเคาท์ในเครื่องของผู้ปกครองยังทำได้อยู่เหมือนเดิม ถ้าเด็กรู้รหัสผ่านแอคเคาท์ของคุณก็สามารถที่จะมากดซื้อในเครื่องของผู้ปกครอง ซึ่งจะแชร์แอพนั้นให้เครื่องตัวเองเล่นแอพนั้นได้ด้วย ผู้ปกครองจึงควรเก็บรหัสผ่านไว้เป็นความลับไม่ให้เด็กๆ รู้โดยเด็ดขาด ซึ่งรวมถึงผู้ใช้ Android ก็ต้องระวังเช่นเดียวกัน

ป้องกันไม่ให้เด็กซื้อไอเท็มในเกม

ผู้ปกครองหลายคนเห็นข่าวเด็กกดซื้อไอเท็มในเกมเป็นเงินหลักแสนบาท แล้วคงหนาวๆ ร้อนๆ กลัวว่าจะเกิดเหตุกับตัวเอง ก็สามารถไปตั้งค่าป้องกันไม่ให้เด็กหรือใครๆ สามารถซื้อไอเท็มในเกมได้ โดยทำได้ทั้งใน iOS (iPhone/iPad) และ Android ดังนี้

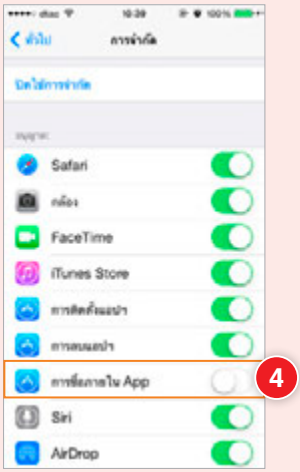
iOS

iOS การซื้อแอพหรือไอเท็มใน iOS ปกติจะให้ใส่รหัสผ่าน Apple ID ให้ถูกต้องก่อนแล้วจะตัดค่าใช้จ่ายผ่านบัตรเครดิต (แอคเคาท์ไทย) หรือตัดจาก iTunes Gift card (แอคเคาท์ US) เพื่อให้แน่ใจว่าจะไม่มีปัญหา คุณสามารถไปปิดบริการซื้อไอเท็มในเกมไว้เลยก็ได้ดังนี้



1 ไปที่ **การตั้งค่า** ▸ **ทั่วไป** ▸ **การจำกัด** (Settings ▸ General ▸ Restrictions) ให้แตะที่ **เปิดใช้การจำกัด** (Enable Restrictions)

2 ตั้งรหัสผ่านเป็นตัวเลข 4 ตัว (ไม่จำเป็นต้องใช้รหัสเดียวกับที่ใช้ปลดล็อคเครื่อง แต่จะตั้งซ้ำกันก็ได้)



3 ยืนยันรหัสผ่านอีกครั้ง

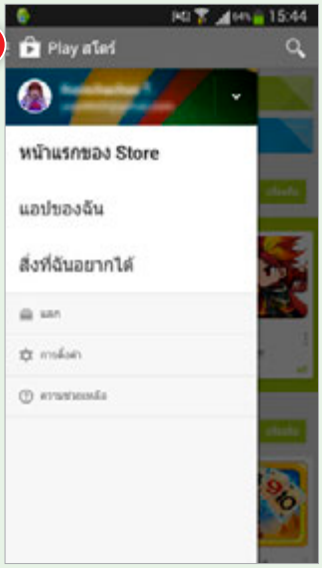
4 แตะปุ่มปิดการใช้งานที่ **การซื้อภายใน App** (In-App Purchases)

- ถ้าจะยกเลิกการจำกัดนี้ ให้มาที่หัวข้อนี้อีกครั้ง (**การตั้งค่า** ▸ **ทั่วไป** ▸ **การจำกัด** (Settings ▸ General ▸ Restrictions)) แล้วกรอกรหัสผ่านที่ตั้งไว้ให้ถูกต้อง เสร็จแล้วแตะ **ปิดใช้การจำกัด** (Disable Restrictions)

Android

Android สำหรับเครื่องที่ใช้ Android ถ้าใช้ AIS จะมีบริการ AIS Google Play ซึ่งอำนวยความสะดวกโดยสามารถซื้อแอพ สติกเกอร์ LINE หรือซื้อไอเท็มในเกมผ่านมือถือโดยจะหักเงินจากเบอร์โทรศัพท์หรือคิดรวมกับค่าบริการรายเดือนได้เลย โดยไม่ต้องตั้งค่าหรือกรอกรหัสผ่านใดๆ ด้วย ซึ่งเป็นช่องโหว่ทำให้หลายคนคิดว่าซื้อได้ฟรีก็ซื้อไม่ยั้ง กว่าจะรู้ตัวอีกทีก็เมื่อมียอดค่าใช้บริการแจ้งมาเป็นหลักแสนตามที่เป็นข่าวกัน (ปิดให้บริการไปแล้ว แต่อาจเปิดใหม่ในอนาคต)

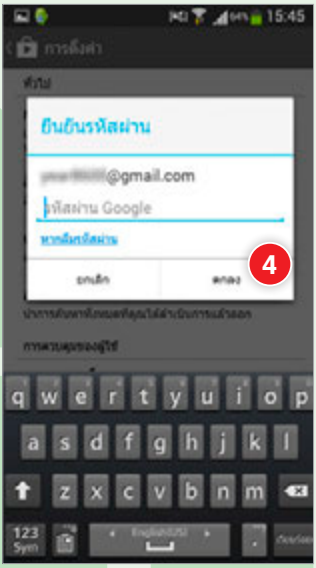
ถ้ากลัวว่าจะมีใครเอาโทรศัพท์ไปซื้ออะไรใน Google Play หรือซื้อไอเท็มโดยไม่รู้ตัวก็ไปตั้งรหัสผ่านป้องกันไว้ก่อนได้ดังนี้



1 เปิดแอพ Play Store แตะที่เมนูมุมบนซ้าย จากนั้นแตะ **การตั้งค่า**

2 แตะที่ **ต้องป้อนรหัสผ่านเพื่อสั่งซื้อ**

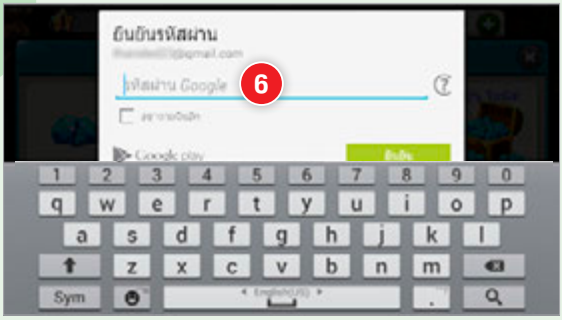
3 เลือกที่ **สำหรับการสั่งซื้อทั้งหมดผ่านทาง Google Play บนอุปกรณ์นี้** หรือจะเลือกที่ ทุก 30 นาที ให้การใส่รหัสผ่านมีอายุ 30 นาที เมื่อมีการโหลดอะไรหลังหมดเวลาก็จะต้องใส่รหัสผ่านใหม่



4 ใส่รหัสผ่านของแอคเคาท์ Google Play ที่ใช้งานอยู่ แล้วแตะ **ตกลง**

5 ที่หัวข้อ ต้องป้อนรหัสผ่านเพื่อสั่งซื้อ จะเปลี่ยนจากค่าดีฟอลต์ที่ตั้งเป็น “ไม่ใช้” ซึ่งจะไม่ต้องใส่รหัสผ่านก่อนโหลดอะไรใน Play Store เป็นแบบที่ตั้งใหม่ หลังจากนี้เมื่อจะดาวน์โหลดอะไรก็ต้องใส่รหัสผ่านตลอด (เพื่อความปลอดภัยก็ไม่ควรให้ใครรู้รหัสผ่านของคุณด้วย)

6 เมื่อไปซื้อแอพหรือไอเท็มในเกมก็จะขึ้นให้ใส่รหัสผ่านก่อน



CHAPTER 4

ระวังอันตรายเรื่องข้อมูลตำแหน่งที่อยู่

การแชร์ตำแหน่งที่อยู่ไว้บนอินเทอร์เน็ต เช่น Social Network ต่างๆ นั้นอาจนำภัยมาถึงตัวได้ เพราะเป็นการป่าวประกาศให้คนทั้งโลกรู้ว่าคุณอยู่ที่ไหน บางทียังบอกว่าอยู่กับใคร อยู่คนเดียว ทำอะไรอยู่ เป็นต้น ถ้าผู้ใดมาพบเห็นตำแหน่งที่อยู่ของคุณแล้วเห็นว่าเป็นโอกาสในการทำผิดคิดร้ายขึ้นมาก็อาจเกิดเหตุการณ์ไม่คาดคิดขึ้นได้เช่นกัน

เปิด-ปิดการทำงานของ GPS

หลายแอพมักขออนุญาตเปิดใช้ GPS บนมือถือหรือแท็บเล็ตเพื่อระบุตำแหน่งที่อยู่ ไม่ว่าจะเป็นแอพแผนที่นำทางต่างๆ, แอพ Social Network อย่าง Facebook, Foursquare หรือแม้แต่แอพถ่ายภาพต่างๆอย่าง Camera ใน iOS และ Android ก็ยังมีการขอใช้ข้อมูล GPS โดยระบบอาจเก็บข้อมูลตำแหน่งที่อยู่ไปตลอด ไม่ว่าเราจะเรียกใช้โปรแกรมที่เกี่ยวข้องหรือไม่ก็ตาม ถ้าเปิด GPS ไว้ตลอดก็อาจเปลืองแบตเตอรี่และใช้งานอินเทอร์เน็ตโดยไม่จำเป็น ถ้าไม่ได้ใช้งานก็ควรที่จะปิดการทำงานของระบบ GPS ไปเสีย

iOS

เปิด-ปิด GPS ใน iPhone/iPad

ระบบ GPS ในเครื่องจะทำงานก็ต่อเมื่อเปิดใช้งาน บริการหาที่ตั้ง (Location Services) เอาไว้ เข้าไปที่ **การตั้งค่า** ▸ **ความเป็นส่วนตัว** ▸ **บริการหาตำแหน่งที่ตั้ง** (Settings ▸ Privacy ▸ Location Services) แตะปุ่มเปิดใช้งานตรง **บริการหาตำแหน่งที่ตั้ง** (Location Services) แล้วเลือกเปิดหรือปิดการใช้ GPS เพื่อช่วยระบุตำแหน่งที่อยู่ของแต่ละแอพได้ตามต้องการ ป้องกันการเข้าถึงข้อมูลตำแหน่งที่อยู่จากแอพที่ไม่จำเป็น (ส่วนถ้าจะปิดทุกแอพ ให้แตะปิดที่ **บริการหาตำแหน่งที่ตั้ง** ที่เดียวได้)

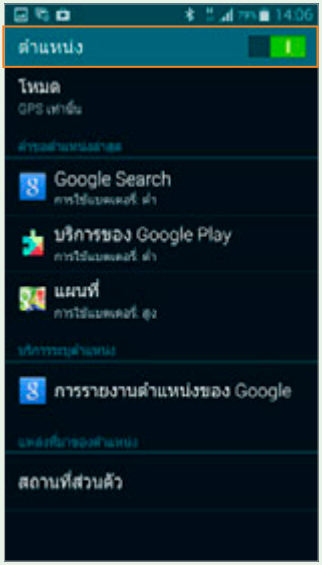
บางแอพจะเก็บข้อมูลว่าเดินทางไปไหนมาบ้างตลอดทั้งวัน เช่น **Moves** ซึ่งควรตั้งค่าการเข้าถึงแอพเหล่านั้นด้วย เช่น มีรหัสผ่านเพื่อความเป็นส่วนตัว

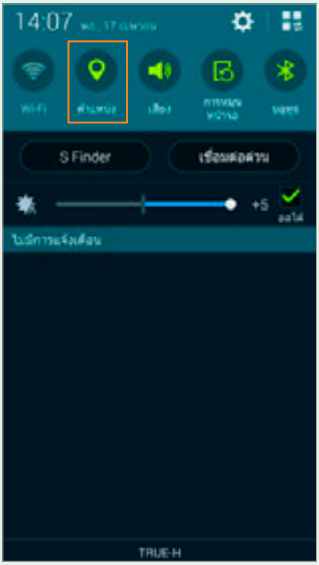
Android

เปิด-ปิด GPS ใน Android

ใน Android จะสามารถเปิด-ปิดการใช้งาน GPS ได้โดยไปที่ **การตั้งค่า** แตะเปิด ที่ **ตำแหน่ง** แตะ **ยอมรับ** อนุญาตให้แสดงข้อมูลตำแหน่ง

หรืออีกวิธีหนึ่ง ให้แตะที่แถบสถานะด้านบนแล้วลากลงมา แตะ **ตำแหน่ง** ให้เป็นสีเขียวเพื่อเปิดใช้งานได้ เมื่อเลิกใช้งานแล้วควรปิดแอพและปิดการใช้งาน GPS ด้วย เพื่อประหยัดแบตเตอรี่





เปิดระบบค้นหาเครื่อง

ถ้ากลัวว่าวันนึงมือถือหรือแท็บเล็ตอาจจะหาย หรือชอบวางลืมไว้แล้วหาไม่เจอบ่อยๆ คุณควรที่จะไปตั้งค่าสำหรับค้นหาเครื่อง ซึ่งทั้งมือถือ/แท็บเล็ตที่ใช้ iOS อย่าง iPhone/iPad และ Android ของ Samsung จะมีวิธีตั้งค่าเตรียมไว้ก่อนที่อุปกรณ์จะหายไปได้ดังนี้

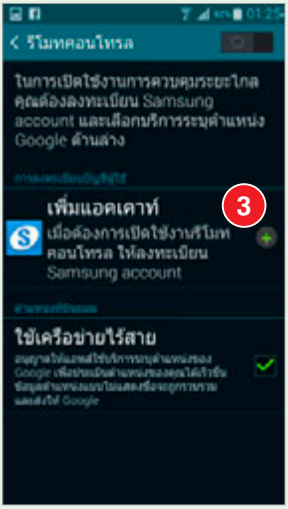
iOS

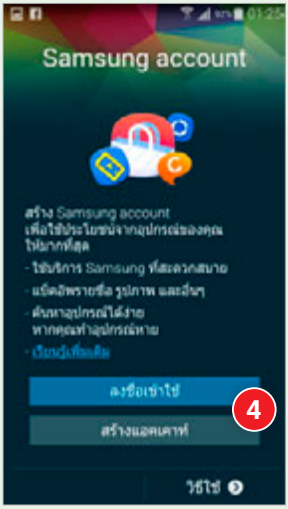
iOS การค้นหา iPhone/iPad ผ่าน iCloud จะต้องตั้งค่า iCloud ก่อน หรือจะทำผ่านแอพ Find My iPhone ก็ได้เช่นกัน การทำผ่าน iCloud ให้ไปที่ **การตั้งค่า** ▸ **iCloud** (**Settings** ▸ **iCloud**) Sign in แอคเคาท์ Apple ID แตะที่ **ค้นหา iPhone ของฉัน** (**Find My iPhone**) หรือ **ค้นหา iPad ของฉัน** (**Find My iPad**) แล้วแตะเปิดใช้งาน **ค้นหา iPhone ของฉัน** (**Find My iPhone**) หรือ **ค้นหา iPad ของฉัน** (**Find My iPad**) จากนั้นแตะปุ่ม **อนุญาต** (**Allow**)

Android

Android ก่อนที่คุณจะเริ่มใช้งาน Find My Mobile เพื่อตามหามือถือและแท็บเล็ต Samsung ของคุณ จะต้องมี Samsung account แล้ว Sign in แอคเคาท์ไว้ในเครื่องเพื่อให้ค้นหาอุปกรณ์นั้นได้ดังนี้

1. แตะไอคอน **การตั้งค่า** เลื่อนหน้าจอลงมาที่หัวข้อ **ระบบ** แตะ **ระบบป้องกัน**
2. แตะ **รีโมทคอลโทรล** แตะ **ตกลง**
3. แตะ **เพิ่มแอคเคาท์**
4. แตะ **สร้างแอคเคาท์** สมัครใหม่ หรือ แตะ **ลงชื่อเข้าใช้** ล็อกอินด้วยแอคเคาท์ Samsung ที่มีได้เลย



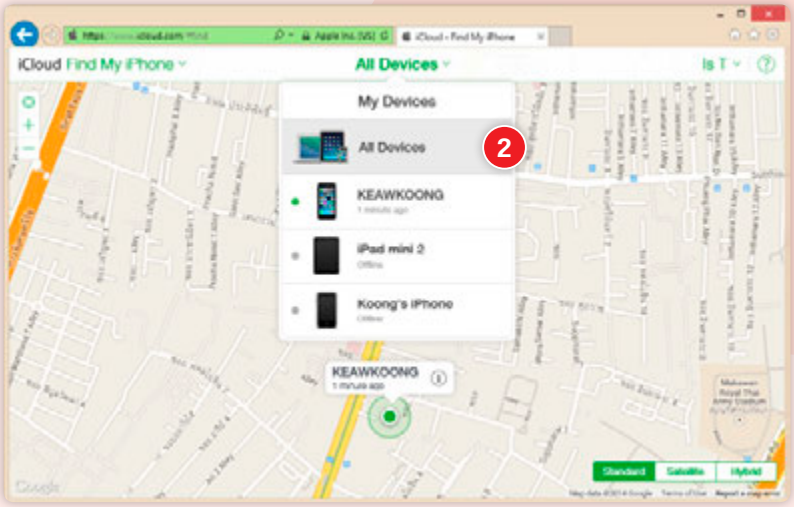


ตามหามือถือหรือแท็บเล็ตที่หายไป

หลังจากตั้งค่าตามขั้นตอนในหัวข้อก่อนหน้าแล้ว ถ้ามือถือหรือแท็บเล็ตหายไปก็สามารถตามหาได้ดังนี้

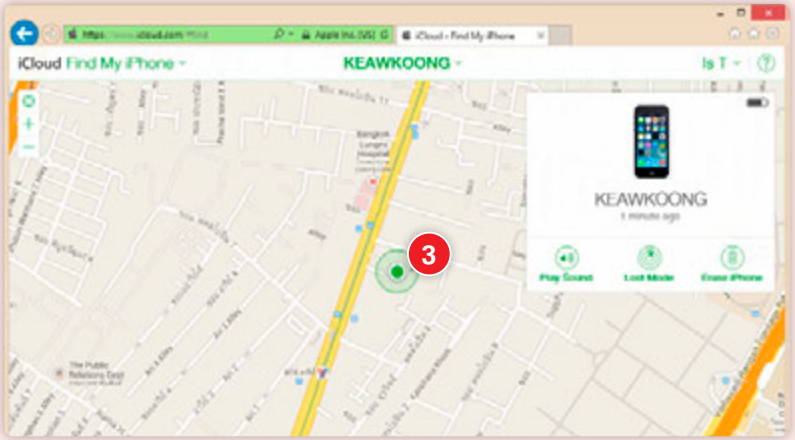
iOS ค้นหาอุปกรณ์ iOS

หลังจากเปิดใช้ Find My iPhone หรือ Find My iPad ถ้าเครื่องหายหรือหาไม่เจอก็สามารถค้นหาผ่านเว็บได้ โดยเครื่องนั้นจะต้องเชื่อมต่ออินเทอร์เน็ตและเปิดใช้ GPS เอาไว้ด้วยจึงจะหากันเจอ



1 เข้าไปที่ www.icloud.com ล็อกอินด้วยแอคเคาท์ iCloud บนอุปกรณ์ คลิกที่ **Find My iPhone** และพิมพ์รหัสผ่านแล้วคลิกปุ่ม **Sign In**

2 คลิก **All Devices** จะเปิดกรอบ My Devices แสดงรายการอุปกรณ์ iOS ที่ล็อกอินแอคเคาท์เดียวกัน และจะแสดงแผนที่พร้อมพิกัดปัจจุบันของอุปกรณ์ให้ทราบ

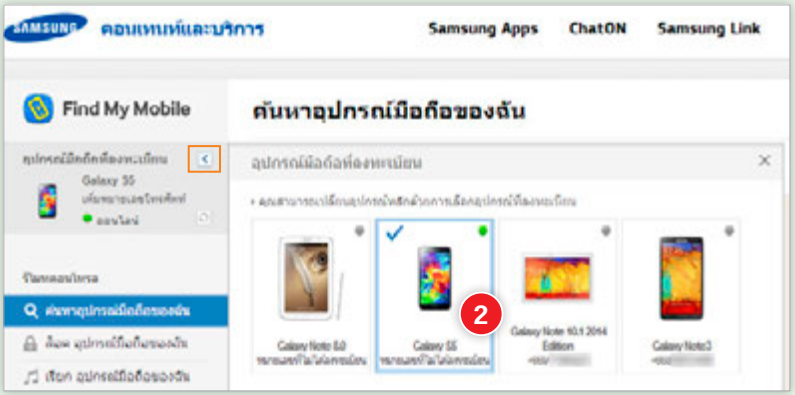


3 แตะเลือกอุปกรณ์ที่ต้องการดูตำแหน่งที่อยู่ จะแสดงตำแหน่งของอุปกรณ์นั้นบนแผนที่

Android

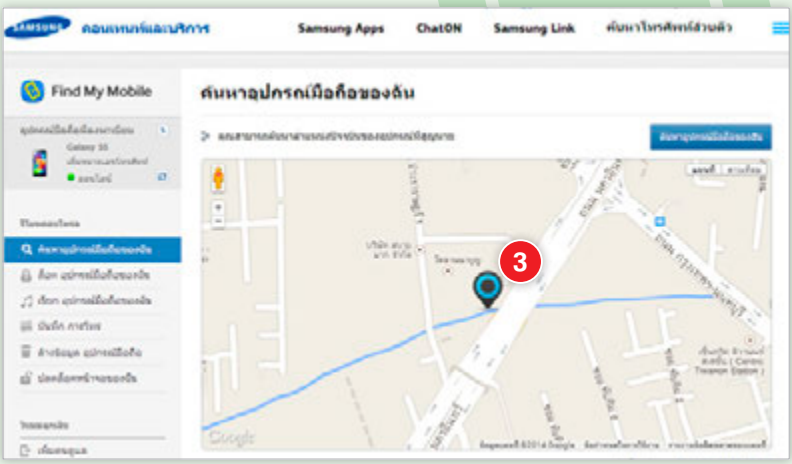
ค้นหาอุปกรณ์ Android (Samsung)

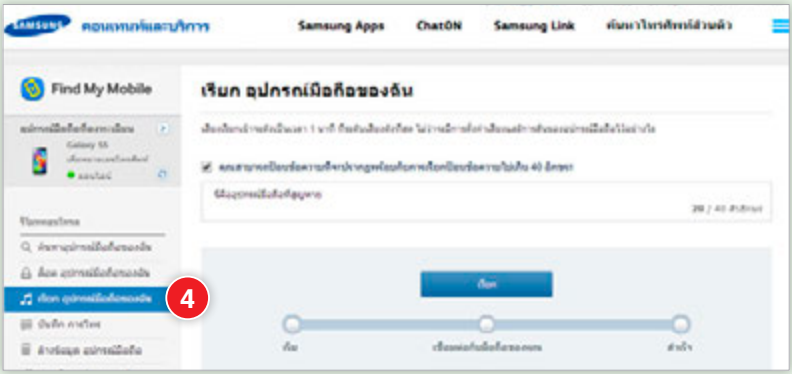
หลังจากลงทะเบียนเปิดใช้งาน Find My Mobile และ Sign in แอคเคาท์ Samsung เรียบร้อยแล้ว คุณสามารถติดตามหาเครื่องได้ว่าอยู่ที่ไหนบนโลกใบนี้ ซึ่งเครื่องนั้นจะต้องเชื่อมต่ออินเทอร์เน็ตอยู่และเปิด GPS ไว้ด้วย ให้เข้าเว็บไซต์ findmymobile.samsung.com ที่เครื่องคอม แล้วทำดังนี้



1 Sign in แอคเคาท์ Samsung ที่ล็อกอินไว้บนแท็บเล็ต จากนั้นคลิกปุ่ม **ลงชื่อเข้าใช้**

2 คลิก > เลือกเครื่องที่ต้องการค้นหา (กรณีมีหลายเครื่องจะแสดงเฉพาะอุปกรณ์ที่ลงทะเบียนเอาไว้ด้วยแอคเคาท์นี้ ให้แตะเลือกอุปกรณ์ที่ต้องการ)



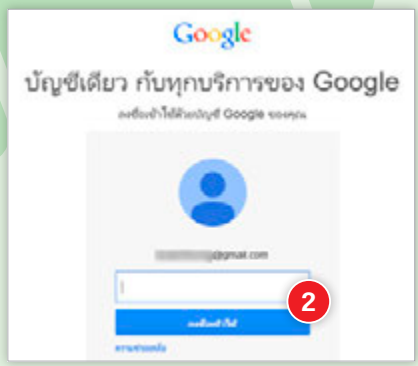


3 จะแสดงตำแหน่งอุปกรณ์บนแผนที่

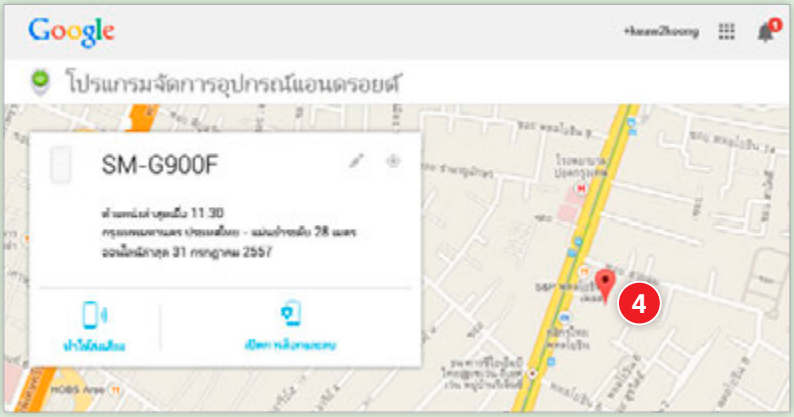
4 ถ้าต้องการให้ส่งเสียงเรียกหาที่อุปกรณ์ ให้คลิก **เรียกอุปกรณ์มือถือของฉัน** แล้วคลิกปุ่ม **เรียก**

ค้นหาอุปกรณ์ Android (ยี่ห้ออื่นๆ)

สำหรับอุปกรณ์ Android ที่ไม่ใช่ Samsung ไม่ว่าจะเป็น HTC, LG หรือ อื่นๆ คุณก็สามารถค้นหาตำแหน่งที่อยู่ของอุปกรณ์ได้ โดยมีเงื่อนไขว่าเครื่องนั้นจะต้องเปิดอยู่, เชื่อมต่ออินเทอร์เน็ต และเปิดใช้งาน GPS



1. เชื่อมต่อเน็ต (ดูหน้า 32) และเปิด GPS (ดูหน้า 134) แล้วเปิดบราวเซอร์เข้าไปที่ www.google.com/android/devicemanager
2. ล็อกอินด้วยแอคเคาท์ Google อันเดียวกับที่ล็อกอินไว้ในอุปกรณ์ที่จะค้นหา
3. ไปที่ www.google.com/android/devicemanager อีกครั้ง โดยครั้งแรกที่เข้าใช้จะขึ้นข้อความต้อนรับ ให้คลิกปุ่ม **ยอมรับ**
4. จะเริ่มค้นหาและแสดงตำแหน่งที่อยู่ของอุปกรณ์บนแผนที่

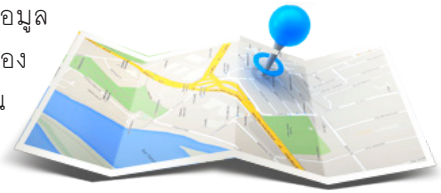


การแชร์ตำแหน่งที่อยู่ออนไลน์ จะมีอันตรายมั้ย?

การโพสต์หรือเช็คอินบน Social Network ต่างๆ รวมถึงขณะแชทด้วยแอพต่างๆ เช่น Messenger ของ Facebook ถ้าเปิดอนุญาตให้เข้าถึงตำแหน่งที่อยู่ก็จะฝังพิกัดแจ้งตำแหน่งไปกับข้อความให้อัตโนมัติเลย ซึ่งการแสดงตำแหน่งที่อยู่ให้ผู้อื่นรู้อาจส่งผลเสียมากกว่าผลดี เนื่องจากอาจเป็นการเปิดช่องให้มิจฉาชีพมาทำร้ายคุณได้ เช่น โพสต์ว่าไปเที่ยวต่างจังหวัดกันหมดทั้งบ้าน แถมคุยกันต่ออีกว่าไปวันไหนกลับเมื่อไหร่ บางทีก็เช็คอินว่าอยู่บ้านโดยบอกตำแหน่ง แจ้งว่าอยู่กับใครยังไงเสร็จสรรพ อาจมีใครแกะรอยตามมาถึงบ้านได้เลย

วิธีป้องกันตัวเบื้องต้น ถ้าเป็นการโพสต์ตำแหน่งที่อยู่บน Facebook ก็ตั้งให้เห็นสิ่งที่โพสต์เฉพาะเพื่อนได้ (ดูหน้า 58) เพื่อป้องกันบุคคลที่ไม่รู้จักมาเห็น แต่ต้องแน่ใจว่าในรายชื่อเพื่อนนั้นมีแต่คนที่ไว้ใจได้ แต่ถ้าเลี่ยงได้ก็ไม่เสี่ยงจะดีกว่า

ระวัง! การเก็บข้อมูลตำแหน่งที่อยู่ของแอพต่างๆ



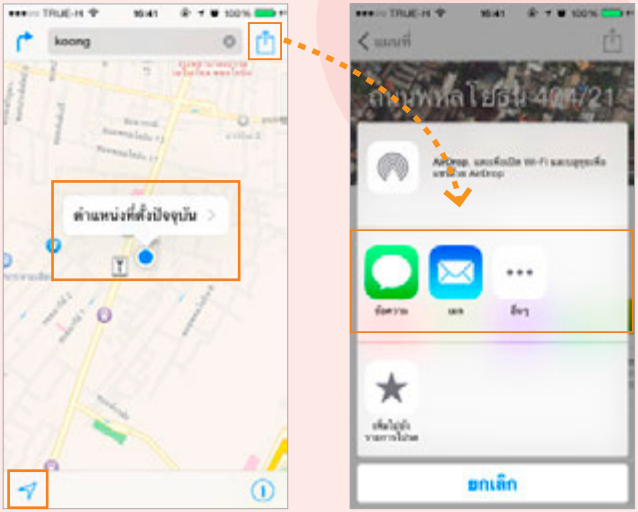
อุปกรณ์บางอย่างสามารถวัดข้อมูลด้านสุขภาพได้ เช่น อัตราการเต้นของหัวใจ วัดชีพจร วัดระยะทางการเดินวิ่ง ในแต่ละวันที่จับจาก GPS สถานที่ออกกำลังกาย วิเคราะห์แคลอรี่ที่ได้รับในแต่ละวัน เป็นต้น ซึ่งจะบันทึกข้อมูลไว้เป็นประวัติส่วนตัวในเครื่อง อาจมีใครบางคนต้องการนำไปใช้หาประโยชน์ได้เช่นกัน ไม่ว่าจะแอบดูว่าคุณมีปัญหาด้านสุขภาพหรือไม่ มีปัญหาด้านไหน แล้วอาจจะนำเสนอขายผลิตภัณฑ์เพื่อสุขภาพต่างๆนานา ดูเส้นทางการวิ่งหรือออกกำลังกายในแต่ละวัน เป็นต้น

แจ้งตำแหน่งปัจจุบันขอความช่วยเหลือ

การแชร์ตำแหน่งที่อยู่นี้จะเหมาะกับกรณีแจ้งตำแหน่งแล้วรอให้คนอื่นมาช่วยเหลือ เช่น รถเสีย เกิดอุบัติเหตุ เป็นต้น แต่อาจจะยังไม่ค่อยสะดวกนักในกรณีฉุกเฉินมากๆ ควรใช้แอพเฉพาะ (ดูหัวข้อถัดไป) ในหัวข้อนี้จะแนะนำการแจ้งตำแหน่งที่อยู่ผ่านแอพแผนที่ที่ให้มาแล้วในเครื่อง สามารถใช้ได้โดยไม่ต้องดาวน์โหลดเพิ่ม

iOS

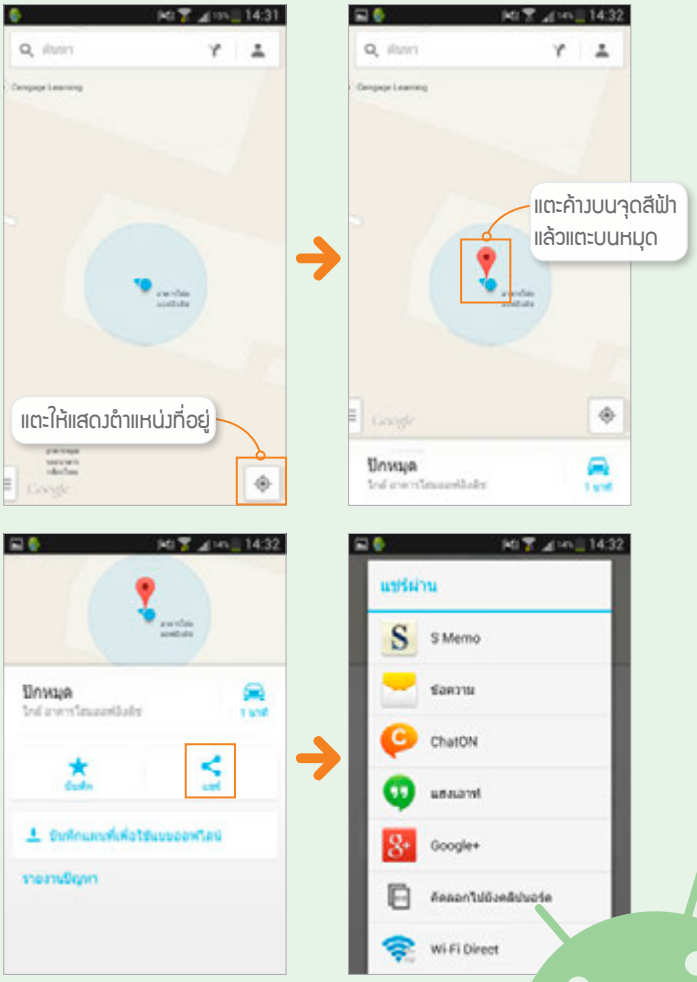
iOS (แอพ Maps) ถ้าอยู่ในกรณีฉุกเฉินจำเป็นจะต้องแจ้งตำแหน่งปัจจุบันให้ใครสักคนรู้ ก็สามารถแชร์ออกไปได้ โดยเปิดแอพ **แผนที่** หรือ Maps แตะ ให้แสดงตำแหน่งปัจจุบันบนแผนที่ แตะป้าย **ตำแหน่งที่ตั้งปัจจุบัน** แล้วแตะ เลือกแชร์ไปยังช่องทางที่สะดวกได้เลย ไม่ว่าจะส่งเป็นข้อความ SMS, ส่งอีเมล์ หรืออื่นๆ



หมายเหตุ การแชร์ตำแหน่งที่อยู่ทั้งใน iOS และ Android นี้คุณจะต้องต่อเน็ตและเปิดใช้งาน GPS เอาไว้ด้วย

Android

Android (แอพ Maps) การแจ้งพิกัดตำแหน่งที่อยู่ในมือถือและแท็บเล็ต Android จะใช้ Google Maps โดยแชร์ออกไปได้โดยเปิดแอพ Maps แตะ แสดงตำแหน่งที่อยู่ปัจจุบัน แตะค้างบนจุดสีฟ้า แล้วแตะบนหมุด แล้วแตะ **แชร์** จากนั้นเลือกแอพที่จะแชร์ เช่น ส่งเป็นข้อความ SMS, โพสต์ลง Facebook, LINE หรืออื่นๆ (รายการแชร์จะขึ้นอยู่กับแอพที่ติดตั้งในเครื่อง) แล้วทำตามขั้นตอนการแชร์ในแต่ละแอพ ซึ่งแตกต่างกันไป

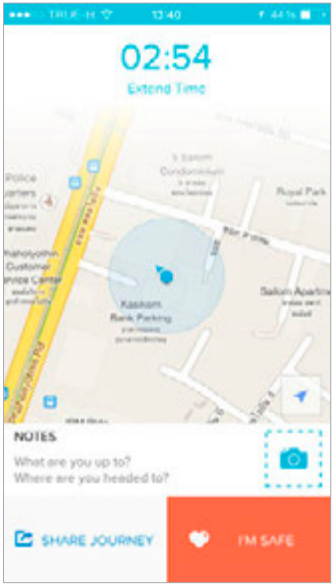


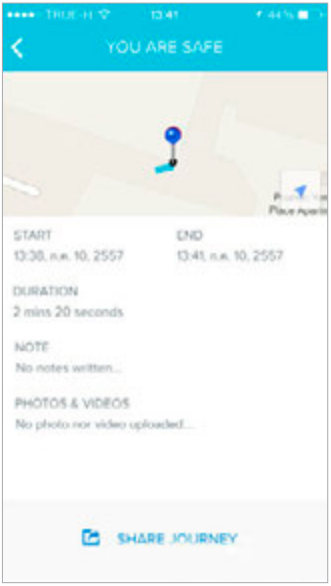
ร้องขอความช่วยเหลือผ่านแอพ

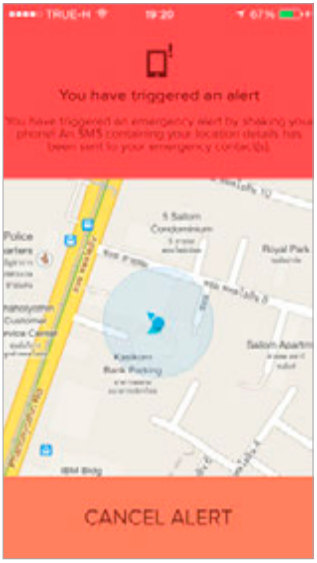
สำหรับคนที่มีความเสี่ยง เช่น ต้องเดินทางคนเดียว กลับบ้านดึกดื่น บ้านอยู่ลึกและเปลี่ยว ฯลฯ โดยเฉพาะผู้หญิง ควรจะป้องกันตนเองโดยดาวน์โหลดแอพขอความช่วยเหลือติดตัวไว้ใช้ในกรณีฉุกเฉินต่างๆ โดยโทรศัพท์จะต้องต่อเน็ตและเปิด GPS ไว้ด้วย

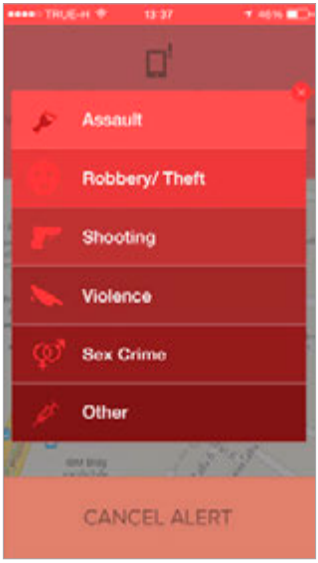
แชร์พิกัดด่วนด้วยแอพ Watch Over Me

แอพ Watch Over Me จะสามารถส่ง SMS ข้อความขอความช่วยเหลือรวมถึงแนบพิกัด GPS ในตำแหน่งที่เราอยู่ไปยังเบอร์ที่เราตั้งค่าเอาไว้ เช่น เบอร์ของคุณพ่อ หรือเบอร์แฟน และหากเกิดเหตุฉุกเฉินเพียงเปิดแอพขึ้นมาแล้วเขย่าตัวเครื่อง ระบบก็จะส่ง SMS แจ้งเตือนพร้อมพิกัดไปยังหมายเลขที่บันทึกไว้ให้ทันทีโดยอัตโนมัติ พร้อมกับภาพวิดีโอคลิปบันทึกเหตุการณ์ดังกล่าวส่งไปพร้อมกันด้วย (แต่ถ้าใช้ฟังก์ชั่นนี้ จะเปิดแฟลชขึ้นมาด้วย ดังนั้นจึงอาจไม่เหมาะหากคนร้ายอยู่กับเรา และควรที่จะปิดเสียง Alert เอาไว้ด้วย)









นอกจากนี้ยังตั้งค่าให้แชร์ข้อความที่ขอความช่วยเหลือไปยัง Facebook ได้ด้วย เมื่อถึงที่หมายก็สามารถแจ้งได้ว่าตอนนี้เราถึงที่หมายอย่างปลอดภัยแล้ว พร้อมแนบรูปหรือโพสต์สถานะเข้าไปด้วยได้

หากคุณอยู่ในพื้นที่เสี่ยงในการเกิดอาชญากรรมบ่อยๆก็จะมีการแจ้งเตือนขึ้นมาด้วย นอกจากนี้เรายังสามารถปักหมุดบนแผนที่ได้ว่าจุดไหนเคยเกิดอาชญากรรมใดขึ้นได้อีกด้วย

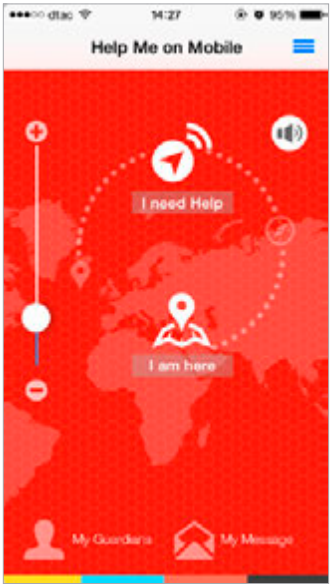
นอกจากนี้ยังสามารถแชร์หรือส่ง SMS ฉุกเฉินโดยอัตโนมัติ หากเราถึงที่หมายแล้วไม่ได้เช็คอินหรือส่งข้อความแจ้งว่าเราปลอดภัยภายในเวลาที่กำหนด ซึ่งฟีเจอร์นี้เป็นที่มาของชื่อแอพ Watch Over Me นั่นเอง

แอพนี้สามารถดาวน์โหลดได้ทั้งผู้ที่ใช้ iOS และ Android สำหรับเวอร์ชั่นฟรีจะเพิ่มเบอร์โทรช่วยเหลือได้แค่ 1 คน และแชร์ไปยัง Facebook หรือ Email ที่ตั้งไว้ได้ แต่ไม่สามารถส่ง SMS กับบันทึกวิดีโอโดยอัตโนมัติได้ อาจจะต้องเสียค่าบริการถึงจะใช้ความสามารถต่างๆของแอพได้ครบ โดยคิดค่าบริการราย 3 เดือน 9.99 เหรียญสหรัฐ และราย 1 ปี 23.99 เหรียญสหรัฐ

ส่งพิกัดและโทรออกฉุกเฉินอัตโนมัติด้วย แอพ Help Me On Mobile

แอพนี้รองรับทั้ง iOS และ Android สามารถดาวน์โหลดมาใช้งานได้ฟรี ซึ่งแอพนี้จะเน้นการใช้งานที่ง่าย ไม่ซับซ้อน เหมาะกับการส่งข้อความแจ้งเตือนในทันทีทันใด สามารถส่ง SMS ฉุกเฉินไปยังหมายเลขที่กำหนดได้

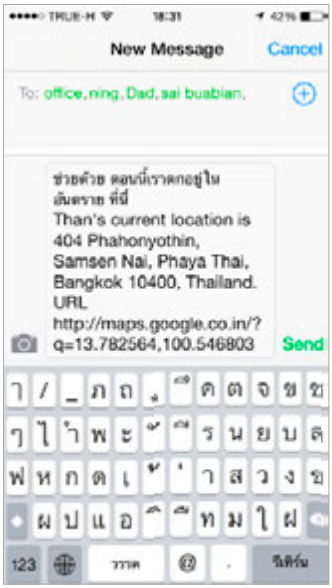
ก่อนอื่นให้เซ็ตเบอร์โทรศัพท์ของผู้ปกครองหรือผู้ที่จะช่วยเหลือเราได้เอาไว้ ซึ่งตั้งได้หลายคน แต่จะตั้งเบอร์โทรหาอัตโนมัติได้เพียงคนเดียว เมื่อเกิดเหตุก็ให้แตะที่ปุ่ม **I need Help** ระบบก็จะส่ง SMS ข้อความไปยังบุคคลที่กำหนดไว้พร้อมพิกัดปัจจุบันและโทรออกไปยังเบอร์หลักให้อัตโนมัติ นอกจากนี้หากไม่ได้ปิดเสียง Alarm เอาไว้เวลาแตะปุ่มขอความช่วยเหลือก็จะส่งเสียงขึ้นมาเพื่อให้คนที่อยู่ใกล้เคียงเข้ามาช่วยเหลือ ข้อเสียคือผู้ร้ายจะรู้แล้วปิดเครื่องก็จะทำให้คนไกลมาช่วยเหลือยากขึ้น จึงควรชั่งใจดีๆว่าจะเปิดหรือปิดเสียง Alarm เอาไว้ดี

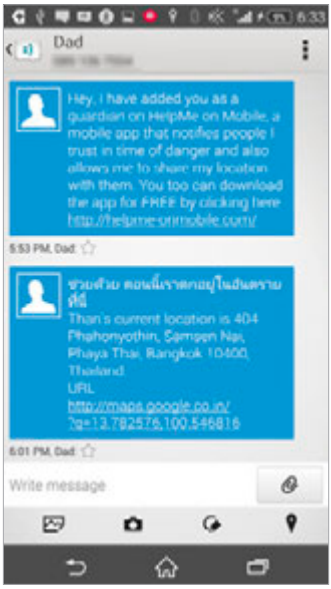


หากต้องการแค่ส่ง SMS ข้อความและพิกัดไปขอความช่วยเหลือ โดยไม่ต้องโทรออก ก็ให้แตะที่ปุ่ม **I am here**

ข้อดีของแอพนี้คือ เราสามารถแก้ไขข้อความที่จะส่งออกไปได้ ดังนั้นจึงสามารถส่งข้อความขอช่วยเหลือเป็นความภาษาไทยได้นั่นเอง และยังคงแนบที่อยู่และพิกัด GPS ให้อัตโนมัติเข้าไปอีกด้วย

สำหรับการเพิ่มชื่อผู้ปกครองหรือคนที่เราจะขอความช่วยเหลือนั้น สามารถเพิ่มได้หลายคน และเลือกให้ส่ง SMS ไปแจ้งเตือนทั้งหมดหรือเฉพาะบางคนก็ได้





ส่วนของการโทรออกอัตโนมัติก็สามารถตั้งหน่วงเวลาได้ตั้งแต่ 5 วินาทีจนถึง 60 วินาที เมื่อผู้ปกครองได้รับข้อความก็แตะตรงพิกัดเพื่อเปิดดูตำแหน่งแผนที่บน Google Map ได้ทันที

CHAPTER 5

ระวังอันตรายจากการหลอกลวงรูปแบบต่างๆ

บนอินเทอร์เน็ตนั้นมีการหลอกลวงสารพัดรูปแบบที่รอให้ผู้โชคร้ายมาติดกับ ไม่ว่าจะสร้างหน้าเว็บหลอกลวงที่หลอกให้เหยื่อกรอกข้อมูลสำคัญบางอย่างแล้วดักจับเอาไป จะซื้อขายสินค้าบนเน็ตก็ต้องระแวดระวัง คนซื้อก็กลัวคนขายจะเบี้ยวไม่ส่งของ คนขายก็กลัวว่าคนซื้อจะโกง นอกจากนี้ยังมีเรื่องราวหลอกลวงที่เชื่อว่าเป็นเรื่องจริงแล้วแชร์ต่อๆ กันมา ผู้ใช้จึงควรใช้วิจารณญาณเป็นอย่างสูงในการเสพข้อมูลต่างๆ ทางอินเทอร์เน็ต

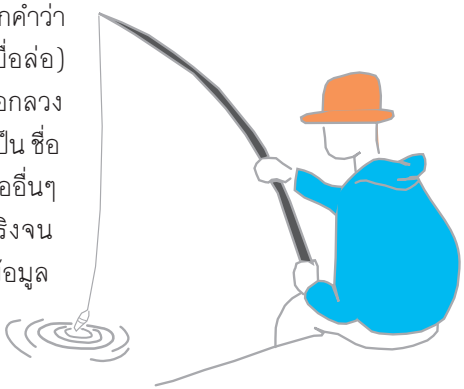
การหลอกลวงโดยอาศัยช่องโหว่ด้านพฤติกรรม

การเจาะระบบเพื่อเข้ามาล้วงความลับในเครื่องเหยื่อด้วยวิธีเดิมๆ นั้น แม้ว่าผู้ใช้จะเผลอติดกับแต่ก็อาจจะโดนบล็อคโดยระบบป้องกันของแต่ละเครื่องที่ติดตั้งไว้เพื่อป้องกันการโจมตีจากภายนอกได้ ซึ่งแฮกเกอร์ก็หาวิธีใหม่ด้วยการหลอกให้เหยื่อเปิดประตูให้เข้าไปด้วยตัวเอง โดยอาศัยช่องโหว่ด้านพฤติกรรมของผู้คนบนอินเทอร์เน็ตที่เรียกว่า *Social engineering* เป็นการใช้สารพัดวิธีการเพื่อหลอกลวงเหยื่อ ซึ่งยังไม่มีระบบใดๆ มาป้องกันได้ยกเว้นสติของผู้ใช้เอง โดยจะยกตัวอย่างวิธีหลอกลวงได้ดังนี้

- **อาศัยความอยากรู้อยากเห็นของแต่ละคน** โดยหลอกด้วยหัวข้อข่าวหรือเรื่องราวที่น่าสนใจ เมื่อคลิกเข้าไปก็จะให้กรอกชื่อและรหัสผ่านของแอคเคาท์อะไรสักอย่างเพื่อเข้าไปอ่านเนื้อหาข้างใน ถึงตรงนี้ถ้าใครไม่เอะใจกรอกลงไปเพื่อสนองความอยากรู้อยากเห็นส่วนตัวก็อาจพบกับอันตรายที่ไม่น่าให้อภัยตัวเองเลยก็ได้
- **อาศัยความกลัว** เช่น หลอกให้ใส่ชื่อและรหัสผ่านเพื่อยืนยันตัวตนไม่เช่นนั้นจะปิดหน้า Facebook หรืออาจหลอกว่าระบบ Internet Banking ของทางธนาคารมีปัญหาให้คลิกลิงค์เข้าไปใส่ชื่อและรหัสผ่านเพื่อยืนยันการใช้งาน เป็นต้น หลอกตื้นๆ แบบนี้อาจไม่ใช่ทุกคนที่หลงเชื่อ แต่ก็มีเหยื่อหลงติดกับได้เรื่อยๆ
- **ชอบของฟรี** หลอกให้โหลดโปรแกรมฟรีต่างๆ แล้วแฝงไวรัส สปายแวร์ หรือโปรแกรมเจาะระบบอื่นๆ เข้ามาโดยผู้ใช้ไม่รู้ตัว หลงติดตั้งระเบิดเวลาลงไปด้วยตัวเองเลย
- **อาศัยความใจดี** ใช้ความเป็น “ดราม่า” หลอกให้บริจาค เช่น เพื่อผู้พิการ ผู้ป่วยระยะสุดท้าย ช่วยเหลือแมว-หมาไร้บ้าน ฯลฯ ด้วยรูปและเรื่องราวที่ทำให้คนที่พบเห็นอดสงสารไม่ได้
- **อาศัยช่องทางออนไลน์** เข้ามาตีสนิท เข้ากลุ่ม หรือแม้แต่เข้าถึงตัวจริงเพื่อหลอกลวงในเรื่องอื่นๆ เช่น ลงทุนร่วมกัน เล่นแชร์ หลอกขายบริการอื่นๆ ล่วงละเมิดทางเพศ ประทุษร้ายต่อร่างกายหรือทรัพย์สิน เป็นต้น

ระวังหน้าเว็บหลอกลวง (Phishing)

Phishing (ฟิชชิ่ง พ้องเสียงมาจากคำว่า Fishing หมายถึงการตกปลาด้วยเหยื่อล่อ) เป็นการสร้างหน้าเว็บไซต์ปลอมมาหลอกลวงเพื่อเอาข้อมูลส่วนตัวของผู้ใช้ ไม่ว่าจะเป็น ชื่อผู้ใช้ รหัสผ่าน หมายเลขบัตรเครดิต หรืออื่นๆ โดยจะสร้างหน้าเว็บเลียนแบบของจริงจนแทบแยกไม่ออก แล้วดักจับการกรอกข้อมูลในหน้าปลอมนั้น ซึ่งมักปลอมได้แนบเนียนจนผู้ใช้ที่ไม่ได้สังเกตจะไม่รู้เลยว่าเป็นหน้าเว็บปลอม



Phishing คือการหลอกลวงให้ไปยังหน้าเว็บปลอม แล้วให้กรอกข้อมูลเพื่อดักจับเอาข้อมูลสำคัญของคุณไป

▲ ตัวอย่างหน้าเว็บปลอมที่แอบอ้างตัวเป็น Facebook สังเกตที่อยู่ของหน้าเว็บของปลอม (ของจริงจะต้องขึ้นด้วย www.facebook.com...)

นอกจากการปลอมหน้าเว็บแล้วยังมีการปลอมอีเมล์แอดเดรส ส่งอีเมล์แอบอ้างเป็นผู้หนึ่งผู้ใดโดยสร้างเรื่องมาหลอกให้ติดกับ เช่น หลอกให้ไปยืนยันตัวตนโดยคลิกลิงค์ไปยังหน้าเว็บที่ดักจับการกรอกข้อมูล, หลอกให้ไปเปลี่ยนชื่อผู้ใช้หรือรหัสผ่านโดยต้องยืนยันชื่อและรหัสผ่านเดิมก่อน เป็นต้น

Facebook นั้นถูกนำไปแอบอ้างอยู่บ่อยครั้ง หลายคนที่ใช้ Facebook อาจเคยพบกับข้อความแจ้งเตือนให้คลิกลิงค์เข้าไปยืนยันตัวตน โดยกรอกชื่อผู้ใช้และรหัสผ่าน ซึ่งเป็นหน้าหลอกลวงไม่ได้มาจาก Facebook จริงๆ ถ้าหลงเชื่อแล้วกรอกไปก็อาจถูกเอาไปเปลี่ยนรหัสผ่านจนทำให้เข้าใช้ Facebook ของตัวเองไม่ได้

บางกรณีก็เป็นการแชร์ลิงค์จากเพื่อนโดยโดนหลอกให้แชร์ต่อๆกันมา เมื่อคลิกลิงค์เข้าไปก็แสดงหน้าล็อกอินปลอมของ Facebook ขึ้นมาหลอกให้กรอกชื่อและรหัสผ่าน เพื่อเอาข้อมูลล็อกอินของเราไป

ป้องกันตัวจาก Phishing

- เมื่อจำเป็นต้องกรอกข้อมูลส่วนตัว ชื่อผู้ใช้ หรือรหัสผ่าน ในหน้าเว็บใด ให้ตรวจสอบทุกครั้งว่าหน้านั้นมีการรับรองและเข้ารหัสแบบ SSL (https) อยู่หรือเปล่า (ดูหน้า 85)
- อีเมล์หรือหน้าเว็บที่แอบอ้างเป็นธนาคารหรือสถาบันการเงิน โดยให้ไปกรอกข้อมูลยืนยันต่างๆ จะเป็นของปลอมทั้งหมด เนื่องจากทุกธนาคารไม่มีนโยบายขอข้อมูลส่วนตัวของลูกค้าผ่านอีเมล์หรือหน้าเว็บต่างๆ
- ถ้าโดนหลอกให้กรอกชื่อผู้ใช้และรหัสผ่านเข้าใช้งานบริการบางอย่าง เช่น Facebook ผู้ไม่หวังดีอาจนำล็อกอินแล้วเปลี่ยนรหัสผ่าน ซึ่งจะมีอีเมล์แจ้งเตือนมาที่คุณให้ยืนยัน ถ้าได้อีเมล์ประเภทนี้ให้รีบไปเปลี่ยนรหัสผ่านที่ Facebook หรือบริการนั้นๆ ทันที (ดูให้แน่ใจก่อนนะว่าอีเมล์ที่ให้ยืนยันนั้นเป็นของจริง และหน้าเว็บที่เข้าไปกรอกก็เป็นของจริง เช่น มี https ตามข้อแรก) โดยจะต้องทำให้ทันก่อนที่จะโดนแฮกอีเมล์เข้ามายืนยันการเปลี่ยนรหัสผ่านไปด้วย และถ้าอีเมล์ของคุณใช้รหัสผ่านเดียวกับ Facebook ก็ให้รีบเปลี่ยนรหัสผ่านของอีเมล์นั้นด้วย (ดูเพิ่มหน้า 81)

การหลอกลวงแบบ Pharming

นอกจาก Phishing แล้วยังมี **Pharming** ซึ่งเป็นการที่แฮกเกอร์โจมตีเซิร์ฟเวอร์ของเว็บต่างๆ หรือผู้ให้บริการอินเทอร์เน็ต โดยเปลี่ยนค่าที่เซิร์ฟเวอร์ให้ส่งผู้ที่เข้าเว็บนั้นด้วย URL ปกติไปยังหน้าเว็บปลอมแทน (ต่างจาก Phishing ที่จะหลอกให้คลิกลิงค์เพื่อไปยังหน้าเว็บปลอม) ซึ่งจุดมุ่งหมายของ Pharming จะเหมือนกับ Phishing คือหลอกให้ไปยังหน้าเว็บที่ปลอมให้เหมือนกับหน้าเว็บจริง แล้วให้ใส่ชื่อผู้ใช้และรหัสผ่าน หรือกรอกข้อมูลส่วนตัวอื่นๆ เช่น วันเดือนปีเกิด หมายเลขบัตรเครดิต หรืออื่นๆ แล้วดักจับข้อมูลที่กรอกเอาไปกระทำการต่างๆ ที่อาจเป็นอันตรายต่อผู้ใช้งานที่ตกเป็นเหยื่อ

Pharming คือการแฮกเข้าไปที่เซิร์ฟเวอร์ของเว็บหรือผู้ให้บริการอินเทอร์เน็ต แล้วเปลี่ยนค่าที่เซิร์ฟเวอร์ให้ส่งผู้ที่เข้าเว็บนั้นด้วย URL ปกติไปยังหน้าเว็บปลอมที่ทำขึ้นเพื่อดักจับข้อมูล

▲ ตัวอย่างหน้าเว็บหลอกลวงที่ทางธนาคารกสิกรไทยแจ้งเตือนไว้

▲ หน้าเว็บจริงของธนาคารกสิกรไทย สังเกตว่าไม่มีปุ่มให้ดาวน์โหลดอะไร

Pharming นั้น อันตรายกว่า Phishing มาก เพราะเราเข้าเว็บตามปกติก็อาจถูกส่งไปยังหน้าเว็บปลอมได้โดยไม่รู้ตัว ซึ่งหน้าเว็บปลอมนั้นก็มักจะใช้ชื่อ URL ที่สอดคล้องกับเว็บจริงให้สังเกตได้ยากยิ่งขึ้น ต่างกับ Phishing ที่ยังจะพอดูได้ง่ายกว่าว่าอาจเป็นการหลอกลวงให้คลิกลิงค์ไปยังหน้าที่สร้างไว้ดักจับข้อมูล ฉะนั้นก่อนที่จะกรอกข้อมูลส่วนตัวใดๆ ลงในหน้าเว็บควรตรวจดูว่าเป็นหน้าเว็บที่เข้ารหัสแบบ https หรือยัง (ดูหน้า 85) และชื่อเว็บที่แสดงในช่องแอดเดรสของบราวเซอร์มีอะไรน่าสงสัยหรือไม่ ถ้าไม่แน่ใจก็ไม่ควรเสี่ยงที่จะกรอกข้อมูลใดๆ ลงไปในหน้าเว็บนั้น

หลอกให้ดาวน์โหลดโปรแกรม/แอพ

นอกจากการหลอกให้ใส่ข้อมูลส่วนตัวต่างๆ ในหน้าเว็บปลอมเพื่อขโมยข้อมูลไปแล้ว ยังมีการหลอกอีกรูปแบบหนึ่งคือ การหลอกให้ดาวน์โหลดโปรแกรมหรือแอพลงในเครื่องคอมพิวเตอร์ แท็บเล็ต หรือมือถือ โดยส่งอีเมล์หรือ SMS มาแจ้งให้โหลด โดยเฉพาะแอพที่เกี่ยวกับการทำธุรกรรมการเงินต่างๆ โดยอาจหลอกว่าเป็นแอพของทางธนาคารเลย เมื่อเหยื่อหลงเชื่อก็จะโหลดมาติดตั้งในเครื่อง ซึ่งอาจจะดักจับข้อมูลส่วนตัว ชื่อผู้ใช้และรหัสผ่านที่กรอกขณะใช้งานแอพ หลังจากติดตั้งโปรแกรมหรือแอพเหล่านั้นก็จะคอยดักจับข้อมูลต่างๆ ทั้งประวัติการเข้าเว็บ การคีย์ข้อมูล การกรอกชื่อ รหัสผ่าน และอื่นๆ แล้วแอบส่งข้อมูลที่ได้ออกไปยังภายนอกโดยที่เราไม่รู้ตัว ซึ่งข้อมูลนี้อาจถูกนำไปแอบอ้างทำการโอนเงิน ถอนเงิน จากบัญชีของเราได้

▲ ตัวอย่างหน้าเว็บหลอกลวงให้ดาวน์โหลดโปรแกรม
และแอพที่ทางธนาคารกสิกรไทยแจ้งเตือนไว้

จริงหรือหลอก? ตอบแบบสอบถามแล้วได้เงิน

งานตอบแบบสอบถามผ่านเน็ตจากที่พบเห็นมาก็มีทั้งที่ว่าหลอกลวงและได้เงินจริง บางที่กว่าจะได้เงินอาจใช้เวลานาน ขึ้นอยู่กับนโยบายของแต่ละเว็บ โดยจะมีอยู่หลายเว็บด้วยกันซึ่งก็มีทั้งแบบสอบถามภาษาไทยและภาษาอังกฤษ บางรายอาจให้ค่าตอบแทนเป็นเงิน (อาจให้เป็นเช็คหรือรับเงินผ่าน Paypal) บางรายก็ให้เป็นบัตรกำนัลต่างๆ โดยจะให้สมัครสมาชิก (บางเว็บฟรี) เพื่อเก็บข้อมูลเบื้องต้น จากนั้นระบบจะส่งแบบสอบถามที่ข้อมูลของคุณตรงกับกลุ่มเป้าหมายของแบบสอบถาม ซึ่งแต่ละแบบสอบถามจะมีกลุ่มเป้าหมายแตกต่างกันไป เช่น อายุไม่เกิน 30, มีรถยนต์ยี่ห้อที่ระบุ, ใช้สมาร์ทโฟนรุ่นที่กำหนด เป็นต้น เมื่อตอบเสร็จก็จะได้รับเป็นคะแนน เมื่อทำหลายๆ ครั้งจนได้คะแนนครบตามที่กำหนดก็สามารถนำไปแลกเป็นเงินได้

นอกจากการตอบแบบสอบถามแล้วยังมีการแนะนำให้คนอื่นมาสมัครสมาชิกที่จะทำให้ได้คะแนนเพิ่มขึ้นอย่างรวดเร็ว แต่ก็ต้องตรวจสอบโดยหาข้อมูลในเน็ตดูก่อนว่าเว็บไหนหลอกลวง เว็บไหนให้เงินจริงๆ

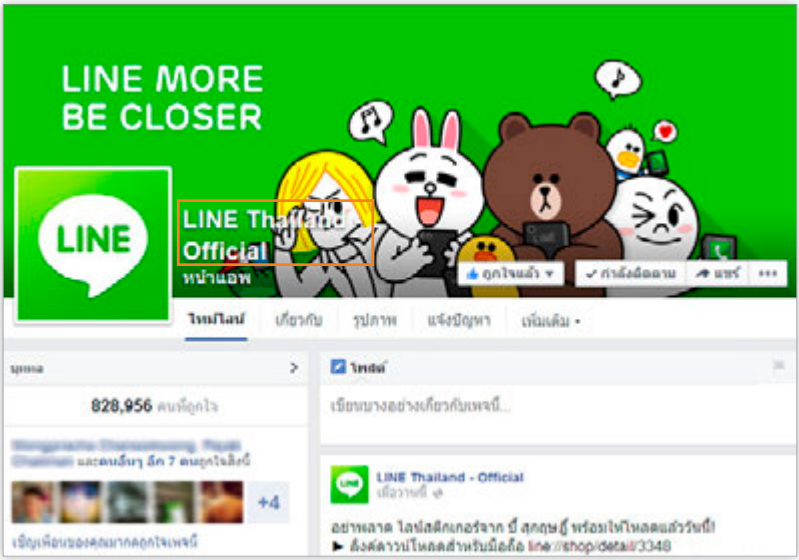
ยืนยันความเป็นตัวจริงใน Social Media

แอคเคาท์หรือหน้าเพจใน Facebook หรือ Social Media ต่างๆ ทั้งของคนดัง ร้านค้า หรือองค์กรนั้น จะมีทั้งแอคเคาท์หรือหน้าเพจจริงของบุคคลหรือองค์กรนั้นซึ่งจะเรียกว่า Official และมีที่แฟนคลับทำขึ้นมาเอง (มักลงท้ายด้วยคำให้สังเกตได้ เช่น Fan, Fan Page, FC หรืออื่นๆ) แม้แต่รายการโทรทัศน์ ภาพยนตร์ หรืออื่นๆ ก็มีการทำ Social Network เป็นของตัวเองด้วย ซึ่งก็จะปะปนกันเยอะแยะมากมายจนยากจะแยกออกว่าอันไหนเป็นหน้าเพจทางการหน้าไหนแฟนคลับทำขึ้น

สำหรับ Facebook ถ้าเป็นบุคคลมีชื่อเสียงหรือเป็นองค์กรใหญ่ๆ ก็จะมีการยืนยันว่าเป็นเจ้าของตัวจริงเสียงจริง หรือเป็นเจ้าขององค์กรหรือธุรกิจนั้นจริงๆ จะสังเกตได้จากสัญลักษณ์ ✔ (Verified คือทาง Facebook ได้ตรวจสอบแล้วว่าเป็นตัวจริง) ที่ท้ายชื่อในหน้าเพจ

การยืนยันหน้าเพจของบุคคลที่มีชื่อเสียงนี้ Facebook จะเป็นผู้ยืนยันให้อัตโนมัติ ซึ่งคุณไม่สามารถร้องขอให้มีการยืนยันเองได้ แต่สามารถแจ้งเพจที่ปลอมเป็นตัวคุณ แบรนด์ หรือธุรกิจของคุณได้ โดยเปิดหน้าเพจนั้น คลิก ••• เลือก **รายงาน/บล็อก**

สำหรับหน้าที่เป็นของบุคคล ธุรกิจ หรือองค์กรที่ยังไม่มีการยืนยันจาก Facebook ก็มักจะต่อท้ายชื่อด้วยคำว่า “Official” เอาไว้ก่อนเพื่อแสดงให้ทราบว่าเป็นหน้าของเจ้าของอย่างเป็นทางการ (แต่การเขียนคำว่า Official นี้ก็อาจปลอมกันได้เช่นกัน โปรดระวัง!)



การบอกต่อเรื่องไม่จริง

อยากจะบอกว่าเดี๋ยวนี้ได้เห็นหรือได้ยินอะไรก็ควรจะฟังหูไว้หูกันเสียทุกอย่างเลยทีเดียว โดยเฉพาะเรื่องราว ข่าวสาร หรือข้อมูล ที่ได้รับมาทางอินเทอร์เน็ต แต่ก่อนนี้มี Forward Mail ที่ส่งต่อๆ กันเป็นทอดๆ ทางอีเมล์ เดี๋ยวนี้เปลี่ยนมาแชร์ผ่านเครือข่าย Social Network กันเป็นว่าเล่น ซึ่งก็มีทั้งเรื่องจริงและไม่จริงปะปนกัน (ส่วนใหญ่จะไม่จริง) บางเรื่องก็เขียนหรือทำภาพกราฟิกเป็นเรื่องเป็นราว อ้างแหล่งที่มาซะน่าเชื่อถือ

บางเรื่องก็มีผู้รู้ที่เชื่อถือได้ออกมาพิสูจน์แล้วว่าเป็นเรื่องไม่จริง แต่เรื่องดีๆ ที่เป็นเรื่องจริงมักไม่ถูกส่งต่อ หรืออาจเป็นเพราะว่าเรื่องหลอกลวงเหล่านี้ได้แพร่กระจายอยู่ในเน็ตมานานมากแล้ว (บางเรื่องก็นานถึง 10 กว่าปีแล้วก็มี) กว่าเรื่องจริงจะกระจายไปทั่วถึงเท่าก็คงจะต้องใช้เวลาอีกพอสมควร ทำให้ยังมีการส่งต่อหรือแชร์เรื่องราวหลอกลวงต่อๆ กันไปอย่างไม่มีที่สิ้นสุด

▲ ตัวอย่างข้อมูลที่แชร์กันไปทั่วเน็ต

▲ ข่าวที่ออกมาแก้ไขว่าเนื้อหาที่แชร์กันนั้นไม่เป็นความจริง

การใช้อินเทอร์เน็ตในปัจจุบันโดยเฉพาะ Social Network ต่างๆ นั้น เราคงจะต้องใช้วิจารณญาณให้มากยิ่งขึ้นกว่าแต่ก่อน เพราะเดี๋ยวนี้ข่าวสารกระจายได้ไวมาก บางทีก็ขาดการกลั่นกรอง เมื่อคนนึงแชร์มาอีกคนก็แชร์ตามเป็นทอดๆ ต่อเนื่องไปเรื่อยๆ แถมไปไวยิ่งกว่าไฟลามทุ่ง ใช้เวลาไม่นานก็รู้เรื่องกันหมด เป็นการสร้างกระแสได้อย่างรวดเร็ว ทำให้มีผู้ไม่ประสงค์ดีมาใช้ช่องทางนี้ในการเผยแพร่ข่าวสารเพื่อประโยชน์ส่วนตัวได้ง่ายๆ เช่น แชร์เรื่องราวดราม่าต่างๆ เพื่อเรียกไลค์ (Like) หรือแชร์หน้าเพจ สร้างข่าวลือ หรือสร้างกระแสให้เพจตัวเองเพื่อหวังผลประโยชน์ต่างๆ นานา ฉะนั้นคุณจึงควรใช้ความระมัดระวังอย่าตกเป็นเครื่องมือของคนเหล่านี้ ขอให้คิดทบทวนดีๆ ก่อนที่จะแชร์อะไรออกไป นอกจากนี้หากเรื่องที่แชร์นั้นทำให้เกิดความเสียหายกับบุคคลอื่น ยังมีความผิดตาม พ.ร.บ. คอมพิวเตอร์ (ดูหน้า 177) ฐานนำเข้าหรือเผยแพร่ข้อมูลอันเป็นเท็จเข้าสู่ระบบ รวมทั้งอาจถูกผู้ที่เสียหายนั้นฟ้องคดีหมิ่นประมาทอีกด้วย

ซื้อสินค้าหรือทำธุรกรรมออนไลน์ให้ปลอดภัย

ปัจจุบันการซื้อสินค้าหรือทำธุรกรรมผ่านอินเทอร์เน็ตเป็นที่นิยมมากขึ้น เพราะใช้งานง่าย สะดวกสบาย แต่ก็ต้องใช้ความระมัดระวังเช่นกัน สำหรับการซื้อสินค้าออนไลน์ถ้าซื้อผ่านบัตรเครดิตที่ต้องกรอกข้อมูลบัตรเครดิตก็ควรเป็นเว็บที่เชื่อถือได้ ถ้าไม่มั่นใจก็ควรหาข้อมูลจากในอินเทอร์เน็ตก่อนว่ามีใครมาโพสต์เตือนภัยเกี่ยวกับร้านนั้นหรือไม่ หรือเช็คกับทางธนาคารผู้ให้บริการก่อน รวมถึงการซื้อสินค้าที่ขายในหน้าเพจ Facebook หรือหน้าเว็บต่างๆ ที่ให้โอนเงินก่อนส่งของ ซึ่งก็มีข่าวที่ให้โอนเงินแล้วปิดร้านหนีไปเลยอยู่บ่อยๆ แล้วจะรู้ได้ยังไงว่าจะโดนหลอกหรือไม่ คำตอบคือไม่มีทางรู้ได้เลย แต่ก็พอจะมีวิธีป้องกันตัวไม่ให้โดนหลอกได้อยู่ดังนี้

- ถ้าจะกรอกข้อมูลบัตรเครดิตต่างๆ ก็อย่าลืมเช็คว่าหน้าเว็บนั้นเป็นระบบ https หรือเปล่าด้วย (ดูหน้า 85) เพื่อป้องกันการดักจับข้อมูลจากแฮกเกอร์ ซึ่งหลายๆ เว็บนิยมส่งภาระนี้ไปที่หน้าเว็บของธนาคารเจ้าของบัตรไปเลย ไม่รับข้อมูลเอง อันนั้นจะน่าเชื่อถือกว่า

และอยากบอกว่าบัตรเครดิตเป็นช่องทางที่ถูกโกงได้ยากกว่า (ไม่นับเว็บปลอม) เพราะเว็บที่รับบัตรเครดิตได้จะต้องถูกสถาบันการเงินตรวจสอบในระดับหนึ่ง

- หลีกเลี่ยงการซื้อสินค้าที่ราคาถูกเว่อร์ อาจเป็นของขโมยมา ของปลอม ของด้อยคุณภาพ ของมีตำหนิ ของใช้แล้ว หรือไม่มีสินค้าจริง หลอกให้โอนเงินแล้วชิ่ง
- ตรวจสอบประวัติของร้านหรือผู้ขาย โดยค้นหาข้อมูลร้านนั้นจากผู้ที่เคยซื้อหรือใช้บริการจาก Google ซึ่งมักจะมีผู้ที่ถูกหลอกมาโพสต์เตือนไว้ไม่ให้ใครตกเป็นเหยื่อเพิ่ม โดยเฉพาะผู้ที่โพสต์ขายตามเว็บบอร์ดซึ่งไม่มีหลักแหล่งที่น่าเชื่อถือยิ่งต้องระวังให้มาก หรือบางที่ เช่น ebay จะมีประวัติผู้ขายให้ตรวจสอบได้ด้วย
- การโอนเงินเป็นช่องทางที่ยังนิยมกันมาก แต่ความจริงช่องทางนี้อันตรายที่สุด เพราะถ้าถูกหลอกก็จะตามตัวผู้รับโอนและขอคืนเงินได้ยากหากมีปัญหา
- แม้ว่าจะเคยซื้อกับทางร้านนั้นๆ มาก่อนแล้วก็อย่าเพิ่งไว้ใจ มีข่าวที่ผู้ขายหลอกให้ตายใจ ครั้งแรกๆ ก็ซื้อขายกันตามปกติ พอซื้อยอดสูงๆ แล้วชิ่งไปเลยก็มี
- แม้ว่าจะบอกว่าเป็นร้านของดาราหรือผู้มีชื่อเสียงก็อย่าเพิ่งหลงเชื่อ เพราะเคยมีกรณีที่แอบอ้างว่าเป็นคนดังเพื่อเรียกลูกค้าเช่นกัน

CHAPTER 6

ระวัง! แอพพลิเคชั่นอันตราย

อุปกรณ์สมาร์ทโฟนหรือแท็บเล็ตในปัจจุบันนั้นมีความสามารถมากมาย ทำงานต่างๆ ได้สารพัดรูปแบบ โดยใช้ทั้งโปรแกรมหรือแอพพลิเคชั่นที่มีให้มากับเครื่องและดาวน์โหลดเพิ่มจาก App Store (iOS) หรือ Play Store (Android) ซึ่งแอพพลิเคชั่นที่ดาวน์โหลดมาติดตั้งเองนี้ก็ต้องเลือกดูดีๆ ด้วย โดยเฉพาะใน Play Store ที่มักมีแอพไม่ดีปะปนอยู่ ซึ่งถ้าแค่หลอกให้ติดตั้งเฉยๆ คงไม่เท่าไหร่ แต่ถ้าเจอแอพประเภทที่ดักจับการพิมพ์หรือข้อมูลสำคัญก็คงจะงานเข้าแน่ๆ

ไวรัสและอันตรายต่างๆ

ปัจจุบันมีไวรัส (Virus), สปายแวร์ (Spyware), โทรจัน (Trojan) และโปรแกรมร้ายกาจ (malware) อยู่มากมาย (ในที่นี้จะขอเรียกรวมๆ ถึงภัยคุกคามที่ไม่พึงประสงค์เหล่านี้ว่าไวรัส) ซึ่งพร้อมที่จะแทรกซึมเข้ามาในเครื่องของผู้เคราะห์ร้ายได้ตลอดเวลาที่สบโอกาส จุดประสงค์ในการทำลายก็แตกต่างกันไป เช่น ทำลายหรือก่อกวนระบบให้เข้าใช้งานไม่ได้, แอบรันโปรแกรมบางอย่างโดยไม่ให้เจ้าของรู้ตัว, ดักจับข้อมูลต่างๆ แล้วส่งออกไปภายนอก, แอบดาวน์โหลดแอพโฆษณามาติดตั้งอัตโนมัติ เป็นต้น

โดยส่วนมากมักจะติดไวรัสมาจากโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ต, อีเมล์ที่แนบไฟล์มาด้วย หรือถ้าเป็นคอมพิวเตอร์ก็ติดจากอุปกรณ์ที่เชื่อมต่อกับเครื่องอย่างแฟลชไดรว์หรือ External Harddisk ซึ่งแต่เดิมไวรัสจะถูกสร้างมาเพื่อโจมตีระบบของเครื่องคอมพิวเตอร์ (ส่วนมากเป็น Windows) แต่ก็เริ่มพัฒนามาที่สมาร์ทโฟนและแท็บเล็ตกันแล้ว

“โทรจัน” นั้นมาจาก Trojan horse หรือม้าโทรจัน หรือเรียกอีกอย่างว่า ม้าไม้เมืองทรอย เป็นม้าไม้ขนาดใหญ่ที่ทหารกรีกออกอุบายทำขึ้นแล้วส่งไปเป็นบรรณาการให้กับเมืองทรอย โดยภายในตัวม้ามีทหารแอบซ่อนอยู่ เมื่อชาวเมืองหลงเชื่อแล้วลากม้าเข้าไปในเมือง พอตกกลางคืนทหารก็ออกมาจากม้าไม้แล้วเผาเมืองทรอยเสียวอดวาย โปรแกรมที่ได้ชื่อว่าเป็นโทรจันก็จะหลอกลวงผู้ใช้ในลักษณะคล้ายๆ กัน คือให้ผู้ใช้โหลดไปติดตั้งในเครื่องเองก่อนค่อยแผลงฤทธิ์ทีหลัง

สำหรับอุปกรณ์ iOS ทั้งมือถือ iPhone และแท็บเล็ต iPad นั้นปกติจะไม่อนุญาตให้ผู้ใช้ติดตั้งแอพนอกเหนือจากใน App Store ลงในเครื่องได้เลย ทำให้ปลอดภัยจากสิ่งแปลกปลอมต่างๆ แต่ถ้าคุณเจลเบรค (Jailbreak) ซึ่งเป็นการเปิดช่องที่ Apple ปิดเอาไว้ (ดูหน้าถัดไป) ก็เป็นการเปิดโอกาสให้ไวรัสเข้ามาในเครื่องได้ง่ายขึ้น

ส่วนอุปกรณ์ที่ใช้ Android นั้นปกติจะไม่อนุญาตให้ติดตั้งแอพที่อยู่นอกเหนือจากใน Play Store เช่นเดียวกัน แต่ก็สามารถที่จะเปิดฟังก์ชั่น **Unknown sources** เพื่อติดตั้งแอพได้เอง (ดูหน้า 166) หลังจากติดตั้งแอพเสร็จแล้วก็ควรปิดฟังก์ชั่นนี้ไว้ ถ้าไฟล์นั้นมีของแถม หรือมีไวรัสเข้ามาในช่วงเวลานั้นพอดีก็มีโอกาสที่จะเกิดความเสียหายได้ นอกจากนี้การ ROOT เครื่อง Android (ดูหน้าถัดไป) ซึ่งเป็นการดัดแปลง OS คล้ายกับการเจลเบรค ก็มีความเสี่ยงเช่นกัน

สำหรับ Android ก็มีเรื่องที่ต้องระมัดระวังอีกอย่างหนึ่งคือการดาวน์โหลดแอพใน Play Store ซึ่งคุณอาจไปเจอแอพหลอกลวงที่โหลดมาแล้วกลายเป็นไวรัสหรือโปรแกรมร้ายกาจได้ เนื่องจากแอพใน Play Store มีจำนวนมากและยังไม่มีการคัดเลือกแอพที่ดีพอ ทำให้มีแอพขยะหรือแอพหลอกลวงปะปนอยู่เป็นจำนวนไม่น้อยเลยทีเดียว

สำหรับ Windows Phone ทางไมโครซอฟท์แจ้งว่าเป็นระบบปิดซึ่งไม่อนุญาตให้ติดตั้งแอพเองเช่นเดียวกับใน iOS ทำให้ไวรัสไม่สามารถเข้ามายุ่งกับระบบได้

ปรับแต่งเครื่องด้วยการเจลเบรคหรือ ROOT คืออะไร?

การเจลเบรค (Jailbreak) ใน iOS และการ ROOT ใน Android คือการดัดแปลงระบบปฏิบัติการ ให้สามารถติดตั้งแอพพลิเคชั่นเสริมอื่นๆ ที่ไม่มีใน Store ของระบบนั้นๆ รวมถึงการเจาะระบบ system ในเครื่องและการติดตั้งแอพที่ไม่มีใน App Store นอกจากนี้ยังสามารถดัดแปลงหรือเปลี่ยน Theme ให้มีลูกเล่นตามสไตล์ที่คุณชอบได้อีกด้วย

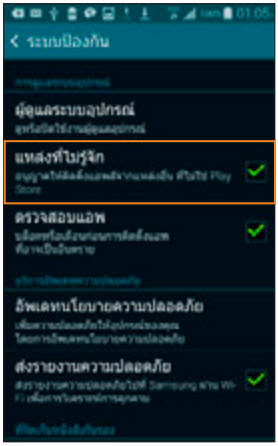
วิธีเจลเบรคนั้นจะต้องรอให้นักแฮกเกอร์ทำการเจาะระบบ และพัฒนาโปรแกรมมาแจกจ่ายให้ใช้กัน ซึ่งวิธีการเจลเบรคในแต่ละเวอร์ชั่นของเฟิร์มแวร์จะมีวิธีเฉพาะสำหรับเวอร์ชั่นนั้น ไม่สามารถทำวิธีเดียวกันได้ เนื่องจากทางแอปเปิลเองเมื่อออก iOS รุ่นใหม่ก็มักจะแก้ไขข้อผิดพลาดโดยปิดช่องโหว่ที่ใช้ในการเจลเบรคในรุ่นก่อนๆ ไป ทำให้การทำเจลเบรคต้องหาวิธีใหม่ไปเรื่อยๆ ตามเฟิร์มแวร์ใหม่

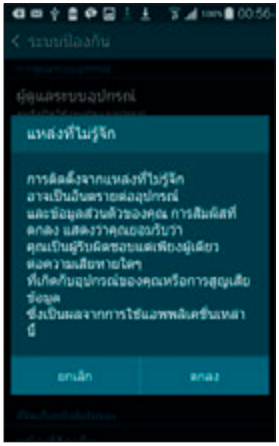
การดัดแปลงเฟิร์มแวร์โดยการเจลเบรคหรือ ROOT นั้นอาจทำให้เครื่องทำงานไม่สมบูรณ์เหมือนเครื่องปกติ เช่น เครื่องอาจค้าง เปิดไม่ติด แบตหมดเร็ว หรืออื่นๆ และที่สำคัญคือเป็นการเปิดโอกาสให้ติดตั้งโปรแกรมที่มีความเสี่ยงสูงกว่าปกติได้ ผู้ใช้จึงควรหาข้อมูลให้ถี่ถ้วนก่อนที่จะเจลเบรคหรือ ROOT เครื่อง

ติดตั้งแอพเองใน Android

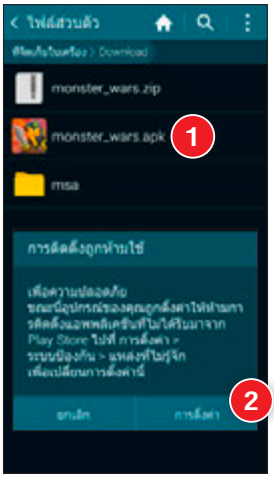
นอกจากแอพบน Google Play Store แล้ว คุณยังสามารถค้นหาไฟล์แอพที่ลงท้ายด้วย .apk (ซึ่งอาจจะเป็นแอพแจกฟรีที่พัฒนาโดยนักพัฒนาแอพและไม่ได้ลงทะเบียนกับ Google เอาไว้ หรือเป็นไฟล์แอพที่เพื่อนแชร์มาให้) ได้จากเว็บแชร์ไฟล์อย่าง 4shared.com, droidshare.com หรือ mediafire.com ฯลฯ มาติดตั้งเองได้ โดยสามารถดาวน์โหลดไฟล์ดังกล่าวจากบราวเซอร์ในอุปกรณ์มาเก็บไว้ก่อน หรือก๊อปปี้จากคอมพิวเตอร์มาก็ได้ แล้วไปตั้งค่าให้ระบบยอมรับการติดตั้งไฟล์จากแหล่งภายนอกเสียก่อน

ปกติระบบ Android จะป้องกันไม่ให้ติดตั้งแอพ .apk เอง เพื่อป้องกันไวรัสไม่ให้เข้ามาในเครื่องได้โดยง่าย แต่ถ้าจำเป็นต้องติดตั้งแอพ .apk ด้วยตัวเอง ก็ต้องเปิดให้เครื่องยอมติดตั้งไฟล์จากแหล่งภายนอกก่อน โดยไปที่ **การตั้งค่า** (Settings) เลื่อนไปที่ **ระบบ** (System) แตะ **ระบบป้องกัน** (Security) แล้วแตะเลือก ☑ **แหล่งที่ไม่รู้จัก** (Unknown sources) ให้แตะ **ตกลง** (OK) เพื่ออนุญาตให้สามารถดาวน์โหลดและติดตั้งไฟล์ต่างๆ โดยไม่ต้องผ่าน Play Store





เมื่อติดตั้งแอพเสร็จแล้วให้มายกเลิกการติดตั้งไฟล์จากภายนอกเพื่อป้องกันไวรัสด้วย โดยแตะยกเลิกการเลือก **แหล่งที่ไม่รู้จัก** (Unknown sources) ถ้าจะติดตั้งไฟล์ .apk อีกค่อยมาเลือกใหม่ ไม่ควรเลือกค้างไว้



1 เปิดแอพจัดการไฟล์ เช่น **ไฟล์ส่วนตัว** (My Files) เปิดไปยังโฟลเดอร์ที่เก็บไฟล์ .apk แล้วแตะเลือกไฟล์ที่ต้องการติดตั้ง

2 แตะ **การตั้งค่า** (Settings) ไปตั้งค่าให้ติดตั้งไฟล์ .apk เองได้ ถ้าไม่ขึ้นคำเตือนนี้ให้ข้ามไปข้อ 3 เลย

3 แสดงข้อมูลการติดตั้งแอพ ให้แตะปุ่ม **ติดตั้ง** (Install) เพื่อเริ่มติดตั้งแอพ ให้รอสักครู่

4 แจ้งให้ทราบเมื่อติดตั้งเสร็จ แตะ **เปิด** (Open) เพื่อเปิดใช้งานแอพทันที หรือแตะ **เรียบร้อย** (Done) ปิดหน้านี้

ป้องกันตัวจากไวรัส

การป้องกันตัวเองจากสิ่งแปลกปลอมไม่พึงประสงค์เหล่านี้ทำได้หลายวิธี โดยควรจะทำทั้งในคอมพิวเตอร มือถือ และแท็บเล็ต โดยเฉพาะ Android

- ติดตั้งโปรแกรมหรือแอพป้องกันและกำจัดไวรัส สปายแวร์ รวมถึงสิ่งแปลกปลอมอื่นๆ เช่น Line Antivirus, Avira Antivirus Security, McAfee Antivirus & Security เป็นต้น
- หลังจากติดตั้งโปรแกรมป้องกันแล้ว จะต้องอัพเดทข้อมูลโปรแกรมเป็นประจำเพื่อให้รู้จักไวรัสใหม่ๆ ซึ่งมีเพิ่มขึ้นทุกวัน (มักทำให้อัตโนมัติอยู่แล้ว)
- หลีกเลี่ยงการเข้าเว็บใต้ดินอินดี้ทั้งหลาย เว็บแจกโปรแกรมแครก โปรแกรมเถื่อน เพราะมีความเสี่ยงว่าจะได้ของแถมติดมาด้วย
- ไม่ดาวน์โหลดไฟล์ .apk (ไฟล์ติดตั้งของ Android) จากแหล่งไม่น่าเชื่อถือเพราะอาจแถมไวรัสหรือมัลแวร์มาด้วย

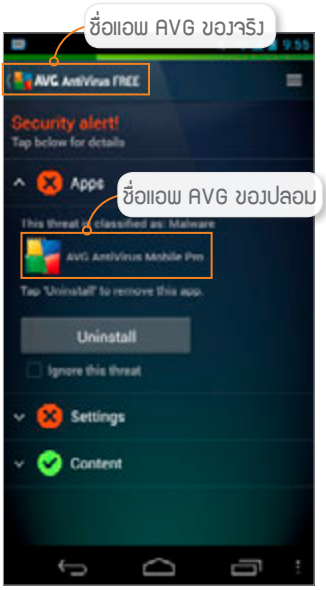
- ไม่ติดตั้งแอพแปลกๆ ที่ไม่รู้ที่มาที่ไป เช่น มีกรณีที่ขึ้นมาแจ้งเตือนระหว่างท่องเว็บว่าพบไวรัส ให้ติดตั้งแอพ xxx เพื่อกำจัด เป็นการหลอกให้ดาวน์โหลดแอพนั้นมาติดตั้ง แล้วกระทำการต่างๆ เพื่อขโมยข้อมูลสำคัญในเครื่องของคุณไป (www.thaicert.or.th/alerts/user/2013/al2013us007.html)
- สำหรับ Android ให้ยกเลิกการอนุญาตให้ติดตั้งแอพจากภายนอก (Unknown sources) หลังติดตั้งโปรแกรมจากไฟล์ .apk เสร็จแต่ละครั้ง อย่าเปิดค้างไว้ (ดูหน้า 166)
- ไม่ใช่เชียนอย่าเจลเบรค iPhone/iPad หรือ Root เครื่อง Android เพราะมีขั้นตอนค่อนข้างยุ่งยาก และต้องทำอย่างระมัดระวัง แถมทำแล้วเครื่องยังจะมีความเสี่ยงต่อแอพอันตรายต่างๆเพิ่มขึ้นด้วย ถ้าไม่แน่ใจควรให้ร้านที่รับทำหรือปรึกษาผู้เชี่ยวชาญก่อน
- ในขั้นตอนการติดตั้งโปรแกรมอย่าเพิ่งรีบแตะ Next ไปเรื่อยๆ ให้ดูรายละเอียดขั้นตอนและอ่านเงื่อนไขอย่างถี่ถ้วนก่อน เพราะบางทีอาจแถมสปายแวร์มาให้ด้วย โดยเฉพาะโปรแกรมฟรีทั้งหลาย
- หมั่นสแกนไวรัส (สำหรับคอมพิวเตอร์) และตั้งให้สแกนอัตโนมัติเมื่อเชื่อมต่ออุปกรณ์ โดยเฉพาะแฟลชไดรว์ (Flash Drive) ที่เป็นตัวแพร่กระจายไวรัสได้ง่ายมาก

แอพขยะและแอพหลอกลวง

App Store ของ Apple (iOS) นั้นจะมีระบบตรวจสอบแอพในระดับสูง จะไม่ค่อยมีพวกแอพขยะหรือแอพหลอกลวงมาให้เห็นเท่าใดนัก ต่างกับ Play Store ใน Android ที่มักจะมีแอพไม่พึงประสงค์ปะปนอยู่ บางแอพก็เขียนคุณสมบัติแอพให้ดูดีแต่พอโหลดมากลับไม่ให้ประโยชน์อะไรรกเครื่องเปล่าๆ เช่น แอพ Virus Shield ซึ่งขายในราคา 3.99 ดอลลาร์ หลอกลวงว่าช่วยสแกนไวรัสได้โดยไม่เปลืองแบตเตอรี่และไม่มีโฆษณา ทำให้ขายดีจนขึ้นอันดับหนึ่งใน Play Store อยู่ช่วงหนึ่ง แต่หลังจากนั้นมีการตรวจสอบพบว่าเป็นแอพขยะ โดยเมื่อเปิดแอพเข้าไปก็แจ้งว่าสแกนไวรัสแล้วแต่ความจริงไม่ได้ทำอะไรเลย ทำให้ Google ต้องคืนเงินให้กับผู้ที่ซื้อแอพนั้นไป (ตัวแอพไม่ได้เป็นภัย แต่หลอกเงินไปฟรีๆ)

ข่าวจาก http://nakedsecurity.sophos.com/2014/04/22/google-refunds-android-users-who-bought-fake-virus-shield-app/

นอกจากนี้ยังมีแบบที่บอกคุณสมบัติไว้อย่างหนึ่งแต่ทำงานอีกอย่างหนึ่ง เช่น แอพ AVG ปลอม (ตั้งชื่อให้สับสนกับแอพ AVG ที่เป็นแอนตี้ไวรัสของจริง) โดยหลอกให้เชื่อว่าเป็นแอพแอนตี้ไวรัส แต่ความจริงทำงานโดยขโมยข้อมูลสำคัญและตั้งให้ส่งต่อ SMS จากเครื่องที่ติดตั้งแอพนั้นกลับไปที่เจ้าของแอพหรือแฮกเกอร์ โดยจะนำข้อมูลที่ขโมยได้ไปใช้ในการทำธุรกรรมออนไลน์ เมื่อธนาคารส่งหมายเลขยืนยัน OTP มาให้ทาง SMS ที่โทรศัพท์เหยื่อ แอพก็จะส่งต่อ SMS นั้นไปยังแฮกเกอร์ จากนั้นแฮกเกอร์ก็จะนำหมายเลข OTP นั้นไปกรอกยืนยันการทำธุรกรรมได้โดยไม่ต้องมีเบอร์โทรศัพท์ของเหยื่อในมือเลย (ดูเพิ่มที่ www.thaicert.or.th/alerts/user/2013/al2013us007.html#1)



▲ ตัวอย่างแอพ AVG ของจริงตรวจพบว่าในอุปกรณ์ได้ติดตั้งแอพ AVG ปลอม

ป้องกันตัวจากแอพขยะหรือแอพปลอม

- ดูจำนวนผู้ใช้/ผู้เขียนคอมเมนต์ อ่านข้อความรีวิวจากผู้ที่โหลดไปใช้แล้ว จากนั้นค่อยตัดสินใจว่าจะโหลดแอพนั้นหรือไม่
- ถ้าเป็นแอพที่ชื่อเหมือนกับโปรแกรมที่มีชื่อเสียง ให้สังเกตที่ชื่อผู้พัฒนาต้องตรงกับเจ้าของโปรแกรม เช็คกับเว็บเจ้าของโปรแกรมด้วยว่ามีบน App Store หรือ Play Store จริงหรือไม่ บางทีมีแต่ชื่อไม่ตรงแสดงว่าไม่ใช่แอพที่เจ้าของทำเอง อาจมีการแอบอ้างได้ ให้ตรวจสอบจากข้อความรีวิวหรือ Google Search
- ไม่ติดตั้งแอพที่ไม่รู้ที่มา หรือโหลดจากเว็บที่ไม่น่าเชื่อถือโดยเด็ดขาด

มือถือ หรือแท็บเล็ตจะติดไวรัสจาก คอมพิวเตอร์ได้หรือไม่?

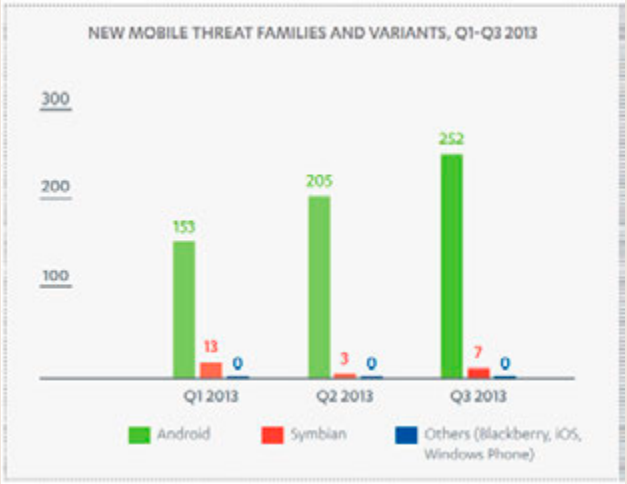
ถ้าในคอมพิวเตอร์มีไวรัส เมื่อเชื่อมต่อมือถือหรือแท็บเล็ตจะติดไวรัสด้วยมั้ย? ขอบอกว่าไวรัสในคอมพิวเตอร์กับมือถือหรือแท็บเล็ตนั้นสร้างมาด้วยโครงสร้างการเขียนโปรแกรมคนละแบบกัน ซึ่งจะทำงานได้เฉพาะบนระบบใดระบบหนึ่งเท่านั้น แม้แต่บน iOS กับ Android ก็ยังใช้วิธีเขียนโปรแกรมที่แตกต่างกันเลย

แต่ถึงแม้ว่าไวรัสจะทำงานบนระบบอื่นไม่ได้ก็ใช่ว่าจะติดไวรัสไม่ได้ ถ้าเชื่อมต่ออุปกรณ์กับคอมพิวเตอร์ เครื่องจะมองอุปกรณ์เป็นเสมือนแฟลชไดรว์ ถ้าฝ่ายใดฝ่ายหนึ่งมีไวรัสก็อาจจะก๊อปปี้ตัวเองไปไว้ในเครื่องของอีกฝ่าย (ถ้าไวรัสนั้นมีความสามารถที่จะทำได้) สแตนบายต์ไว้พร้อมที่จะติดไปยังอุปกรณ์อื่นๆ ที่จะเชื่อมต่อกันหลังจากนี้ก็เป็นได้ ถ้าติดไปยังระบบที่ไวรัสนั้นทำงานได้ก็จะเริ่มกระบวนการทันที

อย่างไรก็ตาม คุณควรที่จะติดตั้งโปรแกรมป้องกันและกำจัดไวรัสไว้ในคอมพิวเตอร์ และอัพเดทข้อมูลไวรัสเป็นประจำด้วย เพื่อป้องกันไม่ให้มีไวรัสในเครื่อง และเมื่อเชื่อมต่ออุปกรณ์ภายนอกก็สามารถสแกนอุปกรณ์นั้นป้องกันไม่ให้ติดไปยังอุปกรณ์และป้องกันไวรัสจากอุปกรณ์ไม่ให้มาติดยังเครื่องคอมพิวเตอร์ได้ด้วย เพื่อยับยั้งการแพร่กระจายของไวรัสต่างๆ

มีภัยร้ายเกิดใหม่ทุกวัน

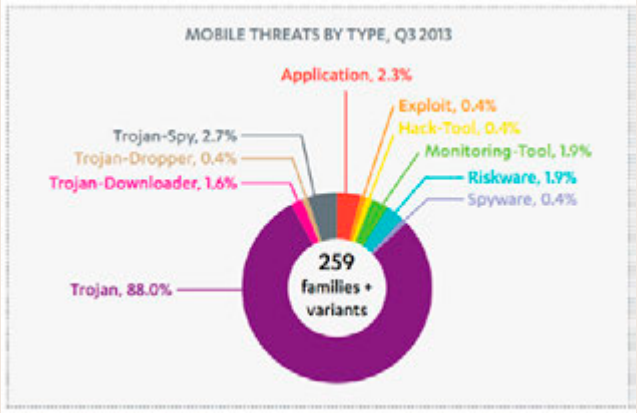
เนื่องจาก Android เป็นระบบปฏิบัติการที่ใช้กันแพร่หลายมากที่สุดในสมาร์ทโฟนและแท็บเล็ต ทั้งรุ่นถูกสุดๆ ไปจนถึงรุ่นท็อปและยังมีสารพัดยี่ห้อ ถือว่าเป็นเป้าใหญ่สำหรับผู้ที่ต้องการเจาะระบบเข้าไปโจมตีหรือขโมยข้อมูลสำคัญต่างๆ (เจาะระบบอื่นไม่คุ้มเหนื่อย ว่างั้น) ดูจากรูปด้านล่างซึ่งเป็นข้อมูลจาก F-Secure ผู้ผลิตซอฟต์แวร์รักษาความปลอดภัยและแอนตี้ไวรัสรายหนึ่ง จะพบว่ามีผู้พัฒนาวิธีการโจมตีอุปกรณ์ในระบบ Android ขึ้นมาใหม่เรื่อยๆ เป็นจำนวนมาก

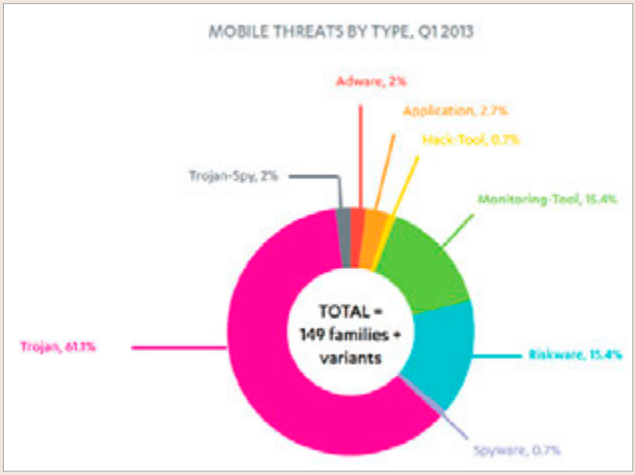


▲ เปรียบเทียบภัยคุกคาม (Threat) ใหม่ๆ ที่พบในระบบปฏิบัติการ Android, Symbian, Blackberrry, iOS และ Windows Phone ในช่วง Q1-Q3 ของปี 2013

อ้างอิงจาก www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf

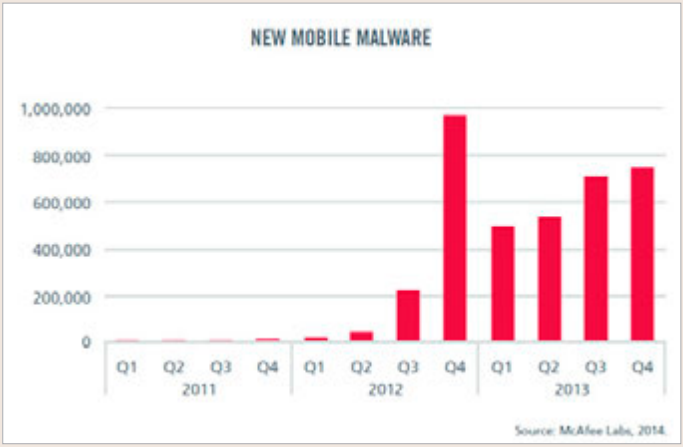
ซึ่งภัยคุกคามที่มีการตรวจพบในอุปกรณ์สมาร์ทโฟนและแท็บเล็ตใน Q3 ของปี 2013 พบว่าเป็นโทรจันที่ชอบแอบเข้ามาล้วงความลับเสียมากถึง 88% เลยทีเดียว





เปรียบเทียบกับเปอร์เซ็นต์ของภัยคุกคามที่มีการตรวจพบในสมาร์ทโฟนและแท็บเล็ตใน Q1 ของปี 2013 เป็นโทรจันเพียง 61.1% แสดงว่ามีการเติบโตของโทรจันอยู่ในระดับสูงขึ้นเป็นอย่างมาก

อ้างอิงจาก www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf



อ้างอิงจาก www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q4-2013.pdf

ข้อมูลจาก McAfee ผู้พัฒนาโปรแกรมป้องกันและกำจัดไวรัสชื่อดังอีกรายหนึ่งก็แจ้งว่าตั้งแต่ช่วงปลายปี 2012 เป็นต้นมา มีโปรแกรมที่เป็นภัยคุกคามหรือที่เรียกว่ามัลแวร์ (Malware) เกิดใหม่เพิ่มขึ้นอย่างรวดเร็ว (ข้อมูลแจ้งว่าในปี 2013 มีมัลแวร์เกิดใหม่ถึง 2.4 ล้านตัว เพิ่มขึ้นจากปี 2012 ถึง 197% ทั้งนี้น่าจะนับในทุกระบบรวมกัน ทั้ง Windows, สมาร์ทโฟน และแท็บเล็ต)

CHAPTER 7

Chat, Comment, Like และ Share อย่างไรให้ปลอดภัย

การเขียน Blog หรือสร้างเว็บไซต์ ที่ให้มีการโพสต์เพื่อแสดงความคิดเห็นในหน้าเว็บได้นั้นต้องระวังผู้อื่นมาโพสต์ภาพหรือข้อความที่ผิด พ.ร.บ. คอมพิวเตอร์ เนื่องจากเจ้าของเว็บหรือ Blog นั้นจะมีความผิดไปด้วย แม้แต่การแชทด้วยแอพต่างๆ กัน 2 คนก็ต้องระวังเรื่องการใช้คำพูดด้วย เพราะอาจถูกจับภาพหน้าจอมาเปิดเผยได้เช่นกัน นอกจากนี้การใช้รูปภาพหรือข้อความต่างๆ บนเว็บ ต้องระวังเรื่องลิขสิทธิ์และการให้เครดิตหรืออ้างอิงที่มาด้วย

ออนไลน์อย่างไร ไม่ให้ผิด พ.ร.บ. คอมพิวเตอร์

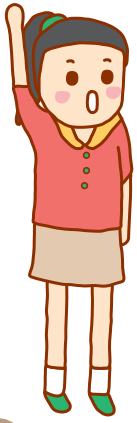
ในการใช้งานอินเทอร์เน็ต ในแต่ละประเทศจะมีกฎหมายควบคุม โดยมีข้อบัญญัติที่มีรายละเอียดแตกต่างกันไป สำหรับประเทศไทยจะใช้ พ.ร.บ. คอมพิวเตอร์ (ฉบับล่าสุดคือ พ.ศ. 2550) ซึ่งมีข้อที่ผู้ให้และผู้ใช้บริการต้องเกี่ยวข้องและควรทราบเพื่อจะได้ใช้ความระมัดระวังไม่ให้กระทำผิด อาทิเช่น

พระราชบัญญัติ
ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. ๒๕๕๐

- การนำเข้าข้อมูลอันเป็นเท็จ หรือก่อให้เกิดความเสียหายหรือเสื่อมเสียชื่อเสียงต่อผู้หนึ่งผู้ใด ซึ่งรวมถึงการส่งต่อหรือแชร์เรื่องเหล่านั้นต่อๆ กันในสื่อสังคมออนไลน์หรือ Social media เช่น เว็บบอร์ด Facebook และอื่นๆ จัดเป็นการกระทำผิดตาม พ.ร.บ. นี้ ซึ่งไม่ใช่แต่เฉพาะผู้ที่เป็นต้นทางเท่านั้น หากยังรวมถึงแต่ละคนที่ส่งต่อๆ กันด้วย
- แม้แต่การเข้าไปโจมตี โต้แย้ง การกระทำดังกล่าว เช่น เข้าไปด่าว่าผู้ที่แชร์ข้อมูลอันเป็นการละเมิดเหล่านั้นบน Facebook ก็อาจมีผลในทางตรงข้ามได้ เช่น กลับทำให้มีการแสดงข้อมูลดังกล่าวให้เห็นกันมากขึ้นไปอีก ทั้ง friend ของฝ่ายผู้เสนอข้อมูลและผู้โต้แย้ง ดังนั้นในกรณีที่สงสัยว่าอาจเป็นข้อมูลที่ไม่ควรเผยแพร่ต่อ แทนที่จะโต้เถียงในหน้านั้นๆ โดยตรง อาจใช้วิธีแจ้งไปยังผู้ให้บริการ (เช่น การ report ไปยัง Facebook) เพื่อให้ระงับการเผยแพร่ข้อมูลนั้นๆ แทน แต่จะได้ผลแค่ไหนก็ขึ้นกับว่าผู้ให้บริการนั้นๆ ยินดีให้ความร่วมมือหรือไม่ เพราะบางรายเช่น Facebook อาจไม่ได้เข้ามาตั้งสำนักงานในประเทศไทยหรืออยู่ภายใต้กฎหมายไทย
- การเผยแพร่ข้อมูลอันเป็นการละเมิดลิขสิทธิ์ เช่น อัพโหลดหนังหรือเพลงที่ละเมิดลิขสิทธิ์ขึ้นไปบนเว็บต่างๆ ผู้ให้บริการจะใช้หลักที่ว่าด้วย user-generated content คือเนื้อหาที่สร้างโดยผู้ใช้ ซึ่งไม่สามารถตรวจสอบได้ครบถ้วน แต่จะใช้วิธีที่เรียกว่า take-down notice คือหากพบมีการละเมิดลิขสิทธิ์ หรือรวมถึงการละเมิดในทางอื่นใด เช่น ให้ข้อมูลเท็จ ทำให้เสื่อมเสียหรือหมิ่นประมาท ผู้เสียหายหรือเจ้าของลิขสิทธิ์สามารถทำเรื่องแจ้งผู้ใช้บริการให้ลบเนื้อหานั้นๆ ออกได้ ซึ่งผู้ให้บริการจะต้องตรวจสอบและถ้าพบว่าจริงก็ต้องดำเนินการตามที่ถูกร้องขอโดยเร็ว (ดูเพิ่มเติมเรื่องลิขสิทธิ์และการอนุญาตให้ใช้งานหรือ license ในแบบต่างๆ ในหัวข้อถัดไป)

ตัวอย่างการกระทำที่มีความผิดตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น

- เข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันเอาไว้โดยไม่ได้รับอนุญาต (แฮกระบบ) มีโทษจำคุกสูงสุด 6 เดือน หรือปรับไม่เกิน 1 หมื่นบาท หรือทั้งจำทั้งปรับ
- เข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันเอาไว้โดยไม่ได้รับอนุญาต (ขโมยข้อมูล) มีโทษจำคุกสูงสุด 2 ปี หรือปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ
- ดักจับข้อมูลคอมพิวเตอร์ของผู้อื่นด้วยวิธีการทางเทคนิคต่างๆ เพื่อดักฟัง ตรวจสอบ ติดตามเนื้อหาของข่าวสารที่ส่งถึงกันระหว่างบุคคล หรือแอบบันทึกข้อมูลที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ ซึ่งเป็นข้อมูลส่วนบุคคล ไม่ใช่ข้อมูลสาธารณะ มีโทษจำคุกสูงสุด 3 ปี หรือปรับไม่เกิน 6 หมื่นบาท หรือทั้งจำทั้งปรับ
- โพสต์ข้อความเท็จเพื่อหลอกลวงผู้อ่านบนเว็บบอร์ดหรือสื่อสังคมออนไลน์ต่างๆ รวมทั้งการเผยแพร่หรือส่งต่อข้อมูลลามกอนาจาร/ข้อความเท็จที่ส่งผลกระทบต่อประเทศ หรือทำให้ผู้อื่นเสียหาย (เช่น ส่งต่อภาพโป๊หรือคลิปแอบถ่ายผ่านอีเมล์) มีโทษจำคุกสูงสุด 5 ปี หรือปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ
- ตัดต่อภาพของผู้อื่น ทำให้ผู้อื่นเสียหาย มีโทษจำคุกสูงสุด 3 ปี ปรับไม่เกิน 6 หมื่นบาท หรือทั้งจำทั้งปรับ



จากตัวอย่างข้างต้น อาจมีสิ่งที่กระทำผิดไปโดยไม่ทันได้ระวังตัว เช่น ส่งต่ออีเมล์ที่มีข้อมูลไม่เหมาะสม แชร์ภาพ/คลิปหลุดที่ทำให้ผู้อื่นเสื่อมเสีย ส่งข้อมูลรบกวนการใช้ระบบคอมพิวเตอร์ของคนอื่น (เช่น สแปมเมล์, ไวรัสคอมพิวเตอร์) นำรหัสผ่านของผู้อื่นไปใช้แล้วเกิดความเสียหาย หรือโพสต์ข้อความแสดงความคิดเห็นโดยที่ไม่ไตร่ตรองให้ดี สิ่งเหล่านี้เมื่อเกิดขึ้นแล้วก็ถือเป็นความผิดตาม พ.ร.บ. จึงควรใช้งานอย่างระมัดระวัง (ศึกษาข้อมูลเพิ่มเติมได้ที่ www.mict.go.th ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือ ICT)

ปัญหาการละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาอื่นๆ บนอินเทอร์เน็ต

ปัญหาอย่างหนึ่งที่ผู้ใช้อาจพบได้บ่อยในการสร้างงานหรือเผยแพร่เนื้อหาบนอินเทอร์เน็ต คือเรื่องของการละเมิด **ลิขสิทธิ์ (Copyright)** และ **ทรัพย์สินทางปัญญา (Intellectual Property)** อื่นๆ ทั้งโดยจงใจและรู้เท่าไม่ถึงการณ์ ซึ่งมีผลกระทบทั้งแก่ผู้สร้างสรรค์ผลงาน ที่จะไม่ได้รับผลตอบแทนอย่างคุ้มค่า หมดกำลังใจหรือทุนที่จะสร้างผลงานใหม่ๆ ต่อไป หรือในทางกลับกันผู้ใช้ที่ขาดความเข้าใจไปก๊อปปี้งานของคนอื่นมาเผยแพร่ ก็อาจก่อให้เกิดปัญหาแก่ทั้งตนเอง หน่วยงานที่ทำงานให้ หรือผู้ให้บริการออนไลน์ที่เกี่ยวข้อง เกิดความเสียหาย กลายเป็นคดีความฟ้องร้องกันยืดยาว ฯลฯ ดังนั้นความรู้พื้นฐานที่ถูกต้องในเรื่องนี้จึงเป็นสิ่งจำเป็นในการใช้อินเทอร์เน็ตให้ปลอดภัย

ตัวอย่างของงานลิขสิทธิ์ ก็เช่น ข้อความ ภาพถ่าย ภาพวาด วิดีโอ หนัง เพลง โปรแกรมคอมพิวเตอร์ งานวรรณกรรมเช่นนิยาย ฟอนต์ (font) หรือโปรแกรมสร้างรูปแบบอักษร ฯลฯ

ปกติให้คิดง่ายๆ ว่าผลงานสร้างสรรค์ทุกอย่างที่เราเห็นบนเว็บ ถ้าไม่ได้มีการบอกไว้อย่างชัดเจนว่า “ไม่สงวนลิขสิทธิ์” หรือประกาศให้เป็น ของสาธารณะ (public domain) แล้ว ให้ถือว่ามีลิขสิทธิ์หมด จะเอามาใช้เลยไม่ได้ ต้องตรวจสอบจนแน่ใจก่อนว่ามีการอนุญาตให้นำไปใช้แบบใดบ้าง ไม่เช่นนั้นอาจถูกฟ้องเรียกค่าเสียหายแพงๆ หรืออย่างเบาะๆ ก็โดนบังคับให้ลบงานนั้นออก หรืออาจโดนทั้งสองอย่างก็ได้

รูปแบบการอนุญาต หรือ license ก็มีหลายแบบ ซึ่งพอจะอธิบายคร่าวๆ ได้ดังนี้

© COPYRIGHTED (C) สงวนลิขสิทธิ์

อันนี้ห้ามเอาไปใช้อย่างเด็ดขาด นอกจากจะติดต่อขออนุญาตเป็นลายลักษณ์อักษร เช่นทางจดหมายหรืออีเมล์ จากเจ้าของก่อน ซึ่งจะอนุญาตโดยคิดค่าตอบแทนในเงื่อนไขอย่างไรก็แล้วแต่เจ้าของ

ตรงนี้มีข้อยกเว้นบางกรณี เช่น

- **หากเป็นการเอาไปใช้เพื่อการอธิบาย** แนะนำถึงงานนั้นๆ ว่าคืออะไร เป็นอย่างไร เช่น เอารูปตัวการ์ตูนมาลงในเว็บ เพื่อบอกว่า ตัวการ์ตูนชื่อนี้ หน้าตาแบบนี้ ใครเป็นคนวาด ใครเป็นเจ้าของลิขสิทธิ์ อย่างนี้ทำได้ แต่ถ้าจะนำไปใช้ในกรณีอื่นๆ ต้องอยู่ภายใต้เงื่อนไขการใช้งานอย่างเหมาะสมหรือ Fair Use ด้วย เช่น จะเอาไปสกรีนลงเสื้อยืดแจกหรือขายไม่ได้
- **ใช้เพื่อการศึกษา การเรียนการสอน** เป็นการใช้ตามหลักการนำไปใช้อย่างเหมาะสม (Fair Use) เช่น เปิดหนังหรือเพลงให้นักเรียนดูในห้องเรียนเฉพาะบางส่วน บางท่อน บางฉาก เพื่อใช้ในการสอน วิพากษ์วิจารณ์ ไม่ใช่เปิดให้ดูทั้งเรื่องหรือเอาไปลงในเว็บแล้วให้เปิดดูเอง โดยอ้างว่าเพื่อการสอน อย่างนี้ไม่ได้

CREATIVE COMMONS (CC)

หรือบางทีเรียกว่า Copyleft (ล้อคำว่า Copyright) เป็นการอนุญาตให้เอาไปใช้หรือไปทำต่อยอดได้เป็นบางกรณี ซึ่งมีเงื่อนไขปลีกย่อยอีกเยอะ เช่น

- **ใช้ในทางการค้าได้หรือไม่** หรือได้เฉพาะแจกฟรี เช่นไปลงเว็บให้อ่านฟรีได้ แต่ห้ามไปขายเป็นคลิปอาร์ตเพื่อทำอย่างอื่นต่อ
- **ดัดแปลงไปใช้ในรูปแบบอื่นๆ ได้** หรือต้องใช้ตามต้นแบบเท่านั้น เช่น ห้ามเอาภาพไปรีทัชหรือตกแต่งเป็นรูปใหม่หรือรวมกับรูปอื่น
- **งานที่เอาไปใช้จะต้องอนุญาตต่อในแบบเดียวกับที่อนุญาตไว้เดิม** คือให้คนอื่นเอางานนั้นๆ ไปทำต่อยอดได้อีกใช่หรือไม่ (ห้ามเอาไปใช้แล้วตั้งว่าเป็น Copyright ของตัวเองใหม่)

กรณีนี้ต้องระบุชื่อเจ้าของงาน แหล่งที่มา พร้อมรูปแบบการอนุญาตหรือ license นั้นๆ ว่าเจ้าของเดิมอนุญาตไว้แบบไหนด้วย เช่น CC BY-SA 3.0 (ดูรายละเอียดเพิ่มที่ https://creativecommons.org/licenses/by-sa/3.0/th)

PUBLIC DOMAIN ไม่สงวนลิขสิทธิ์

เป็นผลงานที่เจ้าของประกาศให้เป็นสาธารณะ จะเอาไปใช้งานอะไรก็ได้ แต่โดยมารยาทแล้วก็ยังควรให้เครดิตหรือลงชื่อเจ้าของผู้สร้างผลงานกำกับไว้เสมอ และห้ามนำไปแอบอ้างว่าเป็นงานของตนเองแล้วสงวนลิขสิทธิ์ใหม่ (นอกจากจะมีการไปดัดแปลง ประกอบ หรือทำเพิ่มเติมให้แตกต่างออกไปแล้วมากพอสมควร)

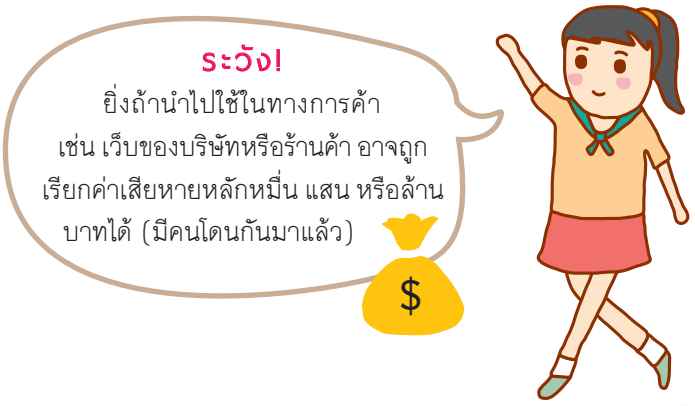
งานประเภทนี้รวมถึงข้อเท็จจริง (fact) เช่นข่าวหรือเหตุการณ์ (แปลว่าเอาเรื่องที่เป็นข่าวไปบอกเล่าต่อด้วยการเรียบเรียงใหม่เองได้ เพราะเป็นของสาธารณะ แต่จะเอาข้อความที่เว็บหนังสือพิมพ์หรือสื่อรายหนึ่งเขียนข่าวลงเน็ตไปเผยแพร่ตามต้นฉบับเดิมทุกคำไม่ได้เพราะอันนั้นกลายเป็นงานที่มีลิขสิทธิ์ไปแล้ว)

ส่วนกฎหมาย ประกาศ หรือข้อมูลของทางราชการที่เผยแพร่ต่อสาธารณะ ถือเป็นข้อมูลที่ไม่มีการสงวนลิขสิทธิ์ สามารถนำไปเผยแพร่ต่อได้

นำภาพหรือข้อความของผู้อื่นไปใช้ อย่าลืมให้เครดิต

จากที่กล่าวมาในหัวข้อก่อนหน้า สรุปได้ว่า ภาพหรือข้อความที่เผยแพร่อยู่บนอินเทอร์เน็ตนั้น ไม่ว่าจะใส่ชื่อหรือไม่ ก็ล้วนแล้วแต่มีลิขสิทธิ์ทั้งสิ้น ถ้าจำเป็นต้องนำมาใช้หรือแชร์หรือส่งต่อก็ควรให้เครดิตเจ้าของไว้ด้วย และถ้าเป็นที่มาจากแหล่งออนไลน์ ควรทำเป็นลิงค์ให้คลิกกลับไปยังที่มาต้นทางได้ด้วย (link back) แต่ก็มีกรณีที่แชร์ต่อๆ กันมาจนไม่รู้ว่าใครเป็นเจ้าของก็มี

มีอีกกรณีหนึ่งคือการเอาข้อความหรือรูปภาพของคนอื่นมาแอ็บว่าเป็นของตัวเอง ไม่ว่าจะบอกว่าถ่ายเอง วาดเอง สร้างสรรค์ภาพขึ้นมาด้วยตัวเอง แถมใส่ลายน้ำแสดงความเป็นเจ้าของเสียเสร็จสรรพ โลกอินเทอร์เน็ตเริ่มแคบลง อาจมีคนมาพบเห็นรู้จักกับเจ้าของตัวจริง หรือเจ้าของมาเห็นเองได้ง่ายๆ อย่างงี้ผิดเต็มๆ เป็นเรื่องเป็นราวกันมาหลายรายแล้ว



ข้อควรระวังในการใช้ LINE หรือแอพแชทอื่นๆ

- การแชทใน LINE และแอพแชทต่างๆ นั้นแม้ว่าจะแชทกัน 2 คนก็ไม่ใช่พื้นที่ส่วนตัวแต่อย่างใด อีกฝ่ายสามารถจับภาพหน้าจอออกมาแชร์จนเป็นข่าวอยู่เป็นประจำ ซึ่งเป็นหลักฐานที่ปฏิเสธได้ยาก แม้ว่าจะมีบางกรณีที่เป็นภาพตัดต่อแต่ก็ค่อนข้างจะพิสูจน์ได้ลำบาก ผู้ใช้จึงควรระวังเรื่องการใช้คำพูดที่จะส่งผลเสียกับตนเองและการพาดพิงถึงผู้อื่น รวมถึงการแชร์ภาพและข้อความต่างๆ ด้วย
- เมื่อส่งข้อความไปแล้วจะตามไปลบที่ผู้รับไม่ได้ จึงต้องระมัดระวังเรื่องการใช้คำพูดให้มาก ควรคิดดีๆ ก่อนส่ง
- คุณสมบัติใหม่ของ LINE เรียกว่า Hidden Chat สามารถซ่อนข้อความแชทได้ โดยจะลบข้อความอัตโนมัติภายในเวลาที่ตั้งไว้ โดยจะลบทั้งของเราและคู่สนทนาด้วย แต่ก็ยังเสี่ยงต่อการจับภาพหน้าจอไว้ก่อนอยู่ดี

- แนะนำให้ลงทะเบียนผูก LINE กับอีเมล์เพื่อยืนยันตัวตนไว้เสมอ เมื่อย้ายหรือเปลี่ยนเครื่องใหม่จะดึงข้อมูลเดิม (บางอย่าง) กลับมาได้
- ระวังเรื่องการ Auto Add Friends ใน LINE ถ้าเปิดใช้งานเอาไว้ก็จะคอยดึงชื่อเพื่อนจากเบอร์โทร, อีเมล์ หรือ Social Network ต่างๆ มาแสดงใน LINE ซึ่งบางทีก็เยอะแยะจนไม่รู้ว่าใครเป็นใคร (ดูหน้า 71)

- ระวังการเปิดใช้ Allow Others to Add ใน LINE ถ้าเปิดไว้เมื่อมีคนมาเพิ่มคุณก็จะทำได้ทันทีโดยไม่ต้องขออนุญาตก่อน อาจมีคนแปลกหน้าที่ไม่รู้จักเพิ่มชื่อเข้ามาได้ (ดูหน้า 72)
- ปกติ LINE จะไม่บันทึกประวัติการสนทนาเอาไว้ ถ้าเปลี่ยนเครื่องหรือลบแอพไปก็จะหายหมด ถ้าต้องการเก็บไว้ให้แบ็คอัพหรือ Export ไปเก็บไว้เอง

แชทและแชร์อย่างไรดี

- แม้จะแชทกันสองคนก็ต้องระวังเรื่องการพูดจา เพราะอีกฝ่ายสามารถจับภาพหน้าจอไปแชร์ได้ (เป็นข่าวบ่อยๆ)
- อย่าแชทหรือแชร์เรื่องไม่จริงหรือเรื่องไม่ดีของคนอื่น ที่อาจกลายเป็นการหมิ่นประมาทบุคคลอื่นได้ ซึ่งจะมีข้อมูลที่แชทเป็นหลักฐานยืนยันการกระทำได้อย่างดี
- ไม่แชทหรือแชร์ข้อความเสียดสี ประชดประชัน หมิ่นพระบรมเดชานุภาพ ละเมิดสิทธิส่วนบุคคล ซึ่งจะมีโทษตามกฎหมายด้วย
- ระวังการแชร์ข้อมูลที่สร้างความเกลียดชัง (hate speech) ต่อๆ กันไป ซึ่งจะสร้างความแตกแยกของคนในชาติ
- ไม่แชร์ความเชื่อที่ผิดตามๆ กัน งมงาย ขัดกับหลักวิชาการ ทำตามแล้วเกิดอันตราย บอกต่อๆ กันโดยไม่ตรวจสอบข้อเท็จจริงก่อน หรืออย่างน้อยถ้าจะแชร์ก็ควรบอกที่มา คนอ่านจะได้ใช้วิจารณญาณดูเองว่าควรเชื่อถือและแชร์ต่อหรือไม่

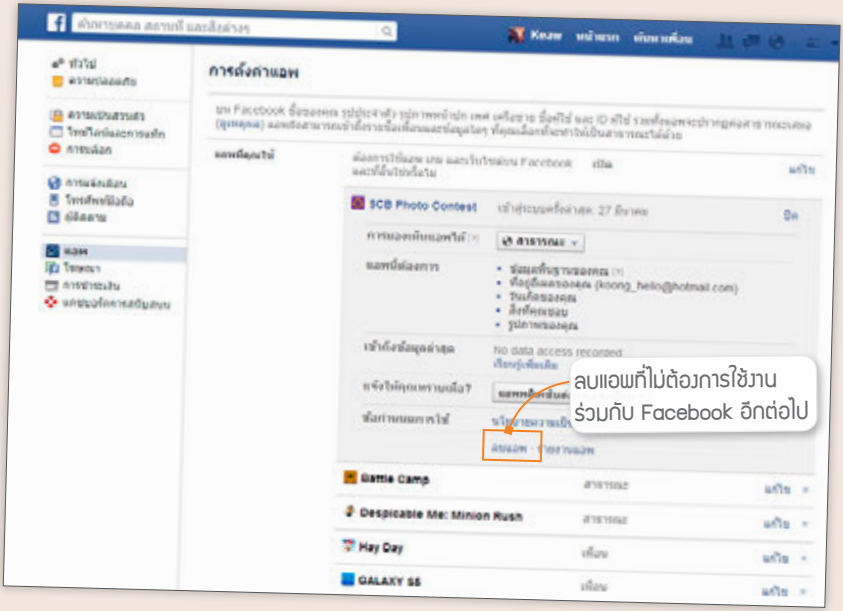
ระวัง! แอพที่ติดตั้งใน Social media

การติดตั้งแอพเพิ่มใน Social media อย่าง Facebook อีกทีหนึ่งก็ต้องระมัดระวัง มีบางแอพซึ่งทำงานไม่ตรงกับที่บอกไว้ เช่น เคยมีแอพกลุ่ม Inwapp (ไม่เกี่ยวกับ Inwshop.com) ที่ตอนติดตั้งจะให้คุณยอมเปิดเผยข้อมูลส่วนตัวที่อยู่ใน Facebook และให้สิทธิ์แอพในการโพสต์ในนามของคุณด้วย ซึ่งเมื่อคุณเปิดเข้าไปดูเพจใดใน Facebook แอพจะกด Like และแชร์หน้านั้นๆ ออกไปในชื่อของคุณ พร้อมใส่ comment (ที่ตัดมาจากเนื้อหานั้นๆ โดยอัตโนมัติ) ให้โดยไม่บอกไม่กล่าว ถ้าติดตั้งไปแล้วก็ไปลบออกได้เช่นเดียวกับแอพอื่นๆ ของ Facebook ดังนี้

เคสนี้เจ้าของแอพอธิบายว่าไม่มีเจตนาร้าย แค่ทำเพื่อเป็นเครื่องมือให้ผู้อื่นมาสร้างแอพได้เท่านั้น แต่ผู้ที่เข้ามาใช้เครื่องมือนี้อาจจะนำไปใช้สร้างแอพที่ก่อให้เกิดความเสียหายกับผู้อื่นได้

Mobile เปิดแอพ Facebook แตะเมนู **เพิ่มเติม** ▸ **การตั้งค่า** แตะหัวข้อ **แอพ** แล้วแตะชื่อแอพที่จะลบ จากนั้นแตะปุ่ม **ลบ ชื่อแอพ** แตะปุ่ม **ลบออก** เพื่อลบแอพนั้นออกจาก Facebook

Computer ขณะเปิดใช้ Facebook ให้คลิก ▾ ที่มุมขวาบนของหน้าเว็บ เลือก **การตั้งค่า** (หรือเข้าไปที่ www.facebook.com/settings) แล้วคลิกหัวข้อ **แอพ** จากนั้นคลิกที่ **แก้ไข** ตรงแอพที่จะลบ จากนั้นคลิกที่ **ลบแอพ** คลิกปุ่ม **ลบออก** ลบแอพนั้นออกจาก Facebook



อันตรายมาก! ถ้าการแชร์จากแอพนี้ (โดยที่เราไม่รู้ตัว) เรื่องที่ไม่ดีซึ่งอาจสร้างความเสียหายกับผู้อื่นหรือผิดกฎหมาย เราอาจต้องรับโทษไปด้วยโดยไม่รู้ตัว

CHAPTER 8

ระวังอันตรายอื่นๆ จากการออนไลน์หรือใช้อุปกรณ์ไม่เหมาะสม

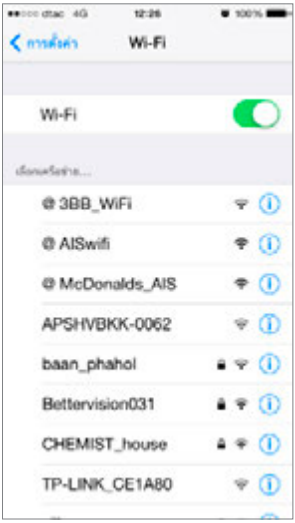
การออนไลน์ผ่านอุปกรณ์ต่างๆ ก็มีข้อควรระวังหลายอย่าง ทั้งการแฮกหรือดักจับข้อมูลที่รับเข้าส่งออก ดักจับการพิมพ์เพื่อขโมยชื่อผู้ใช้และรหัสผ่าน การเข้าใช้งานอินเทอร์เน็ตผ่าน Wi-Fi ในที่สาธารณะก็อาจเป็นอันตราย โดยเฉพาะ Wi-Fi ที่ให้ใช้ได้ฟรี อาจมีคนปล่อยสัญญาณให้เหยื่อเข้าไปใช้งานแล้วดักจับข้อมูลเอาไปทำเรื่องไม่ดีก็เป็นได้

ใช้ Wi-Fi สาธารณะฟรีต้องระวัง

การใช้อินเทอร์เน็ตโดยการเชื่อมต่อ Wi-Fi ในสถานที่สาธารณะนั้นต้องระวังการดักจับข้อมูลจากบุคคลไม่หวังดี โดยเฉพาะ Wi-Fi ที่ให้ใช้ได้ฟรีโดยไม่ต้องใส่รหัสผ่านก่อนเข้าใช้งาน โชคไม่ดีคุณอาจไปเจอ Wi-Fi ปลอมที่มิจฉาชีพทำไว้หลอกโดยตั้งชื่อให้เหมือนกับของจริง เช่น ตั้งชื่อ .@TRЄUWIFI (ของจริงต้องเป็น .@TRUЄWIFI), Dtac Wi-Fi เป็นต้น เมื่อเหยื่อหลงเข้าไปเกาะ Wi-Fi ปลอมก็จะดักจับข้อมูลที่รับส่งระหว่างใช้งาน Wi-Fi ปลอมไปได้

ป้องกันตัวไม่ให้โดนแฮก

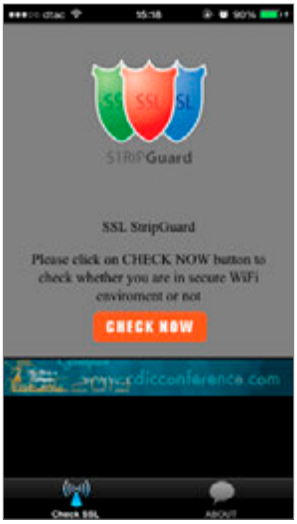
- หลีกเลี่ยงการใช้ Wi-Fi สาธารณะที่ไม่น่าไว้ใจ เช่น Wi-Fi ชื่อแปลกๆ หรือเข้าใช้ได้ฟรีๆ โดยไม่ต้องกรอกชื่อและรหัสผ่านก่อนเข้าใช้
- ถ้าเลี่ยงไม่ได้ก็อย่าทำธุรกรรมหรือใช้บริการที่ต้องกรอกชื่อ, รหัสผ่าน รวมถึงข้อมูลส่วนตัวเพราะอาจมีคนกำลังคอยดักจับข้อมูลที่คุณกรอกลงไปอยู่ก็ได้
- ตรวจสอบว่ากำลังใช้งานแบบ https อยู่หรือไม่ (ดูหน้า 85)
- ถ้าจำเป็นจริงๆ ก็ควรเชื่อมต่ออินเทอร์เน็ตผ่าน 3G/4G แทน (อาจไม่ปลอดภัย 100% แต่ปลอดภัยกว่า Wi-Fi ฟรี)
- ใช้แอพตรวจสอบก่อนว่าเป็น Wi-Fi ที่ปลอดภัยหรือไม่ (ดูหัวข้อถัดไป)

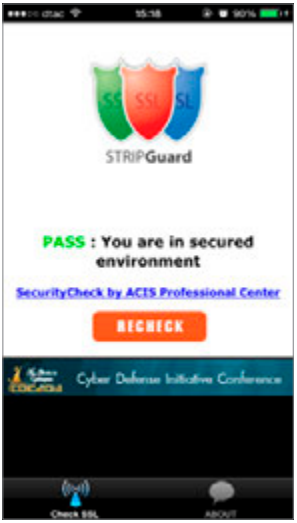


เช็ค Wi-Fi ที่ปลอดภัยก่อนเข้าใช้

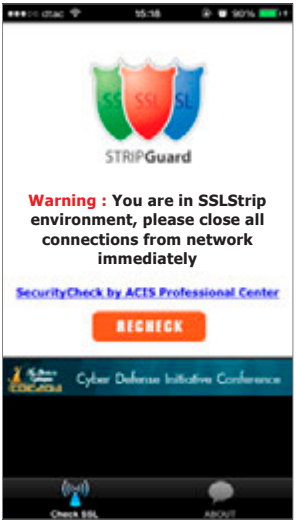
ถ้าจำเป็นต้องเข้าใช้ Wi-Fi ในที่สาธารณะ แต่กังวลใจว่าจะไม่ปลอดภัย ก็ตรวจสอบได้ว่าเครือข่าย Wi-Fi ที่เข้าใช้นั้นเชื่อถือได้หรือไม่ โดยติดตั้งแอพ **SSLSTRIPGuard** (ใน Android ใช้ชื่อ **StripGuard**) แอพฟรีของคนไทย ดาวน์โหลดได้ทั้งจาก App Store (iOS) และ Play Store (Android)

วิธีใช้งานให้เชื่อมต่อ Wi-Fi ที่จะเข้าใช้ แล้วเปิดแอพ SSLSTRIPGuard จากนั้นแตะปุ่ม **CHECK NOW** รอสักครู่ก็จะแจ้งผลการตรวจสอบให้ทราบ





▲ PASS คือยืนยันว่าปลอดภัย



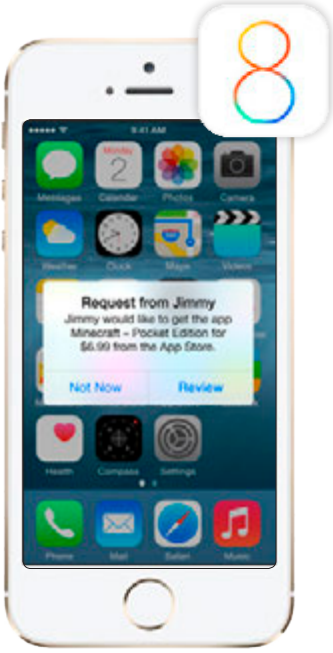
▲ Warning คือเตือนว่าไม่ปลอดภัย

แนะนำให้อัพเดท OS เป็นรุ่นล่าสุด

ถ้าต้องใช้ Wi-Fi ในที่สาธารณะบ่อยๆ เช่น สนามบิน ร้านกาแฟ ห้างสรรพสินค้า หรืออื่นๆ ควรที่จะอัพเดท OS หรือระบบปฏิบัติการของอุปกรณ์ที่ใช้เชื่อมต่อเน็ตให้เป็นรุ่นล่าสุดอยู่เสมอ เนื่องจากเวอร์ชั่นล่าสุดจะมีการแก้ไขบั๊ก (ข้อผิดพลาด) และช่องโหว่ที่ไม่ปลอดภัยต่างๆ ให้ดีขึ้นกว่ารุ่นก่อน เช่น ถ้าใช้โน้ตบุ๊คไปใช้นอกสถานที่บ่อยๆ ก็ควรอัพเดทเป็น Windows เวอร์ชั่นล่าสุดเสมอ และเปิดการทำงานของ Windows Update เอาไว้ให้อัพเดทอัตโนมัติเมื่อมีเวอร์ชั่นใหม่หรือมี patch แก้ไข

สำหรับมือถือและแท็บเล็ตก็ควรจะอัพเดท OS ให้ใหม่อยู่เสมอเช่นเดียวกัน แต่ถ้าคุณไม่ได้ใช้อินเทอร์เน็ตโดยเฉพาะ Wi-Fi ในที่สาธารณะบ่อยๆ และไม่แน่ใจว่าอัพเดทแล้ว OS ใหม่จะใช้งานได้ดีหรือคุ้นเคยเหมือน OS เดิมหรือไม่ (เนื่องจากการอัพเดทบางรุ่นอาจเปลี่ยนหน้าตาใหม่หมดก็มี) อาจรอให้มั่นใจก่อนค่อยอัพเดทก็ได้

▲ OS ล่าสุดใน Android ที่ใช้งานกันอยู่คือเวอร์ชั่น 4.4 (หรืออีกชื่อหนึ่งเรียกว่า Kitkat) และกำลังจะมีเวอร์ชั่นใหม่ 5.0 หรืออีกชื่อหนึ่งคือ Lollipop

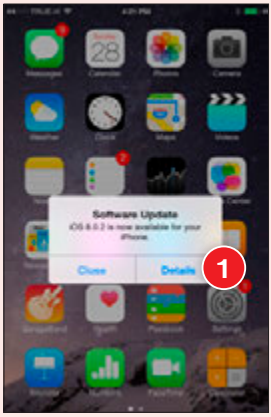


▲ ตัวอย่างคุณสมบัติที่เพิ่มมาใน iOS 8 (ล่าสุด ณ ขณะนี้) จะให้เด็กขออนุญาตผู้ปกครองเพื่อซื้อแอพใน App Store ได้ (ดูเพิ่มหน้า 127)

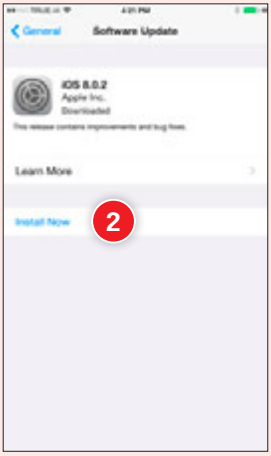
อัพเดท OS ให้เป็นเวอร์ชั่นล่าสุด

iOS เมื่อระบบปฏิบัติการมีเวอร์ชั่นอัพเดทจะแสดงหน้าจอแจ้งเตือนดังรูป ให้แตะปุ่ม **Details** เพื่อเปิดเข้าไปดูรายละเอียดและติดตั้ง (แล้วทำตามขั้นตอนในหัวข้อนี้) หรือแตะปุ่ม **Close** หากยังไม่ต้องการดูและติดตั้งในตอนนี้

1 แตะ **Details** (**รายละเอียด**) เมื่อแจ้งเตือนให้อัพเดท หรือสั่งอัพเดทเองโดยเข้าไปที่ **Settings** ▸ **General** ▸ **Software Update** (**การตั้งค่า** ▸ **ทั่วไป** ▸ **รายการอัพเดทซอฟต์แวร์**)



2 จะแสดงเวอร์ชั่นใหม่ที่อัพเดทได้ (ถ้ามี) พร้อมรายละเอียดหรือข้อมูลที่แก้ไขเพิ่มเติม ให้แตะที่ **Install Now** (**ติดตั้งเดี๋ยวนี้**)



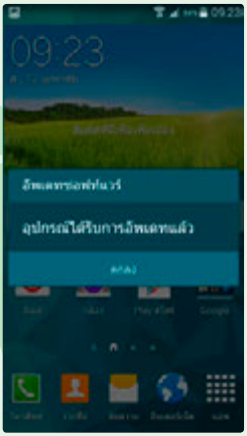
3 จะมีข้อกำหนดและเงื่อนไขต่างๆ แสดงขึ้นมา ให้แตะที่ **Agree** (**ยินยอม**) แล้วแตะ **Agree** (**เห็นด้วย**) เพื่อยอมรับข้อตกลง แนะนำให้เสียบชาร์จไฟไว้ด้วยในขณะที่ดาวน์โหลด เพื่อไม่ให้แบตหมดขณะติดตั้ง และควรต่อผ่าน Wi-Fi เพราะไฟล์อัพเดทมักมีขนาดใหญ่ (ถ้าไฟล์ใหญ่มากระบบอาจบังคับให้อัพเดทผ่าน Wi-Fi เท่านั้น)

4 เมื่ออัพเดทเสร็จแล้ว เครื่องจะบู๊ตใหม่ (หากหน้าจอดับไปให้เปิดเครื่องเอง) รอบู๊ตจนเข้าหน้า Lock Screen และใช้งานได้ปกติ

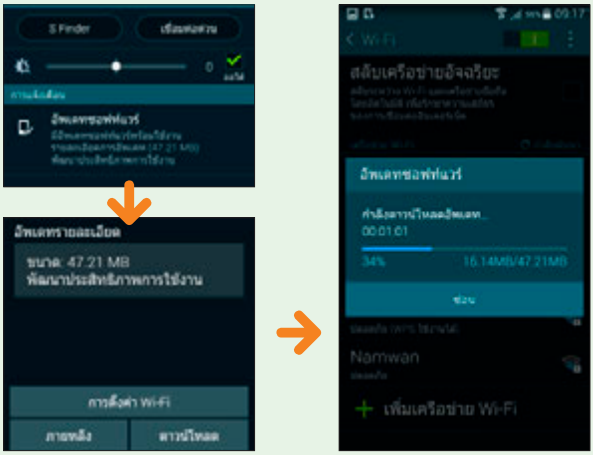
- เช็คเวอร์ชั่นเฟิร์มแวร์ได้ที่ **Settings** ▸ **General** ▸ **About** ▸ **Version** (**การตั้งค่า** ▸ **ทั่วไป** ▸ **เกี่ยวกับ** ▸ **เวอร์ชั่น**)

Android

Android แตะไอคอน **การตั้งค่า** ▸ **เกี่ยวกับอุปกรณ์** ▸ **อัพเดทซอฟท์แวร์** ▸ **อัพเดทตอนนี้** (Settings ▸ About device ▸ Software Update ▸ Update now) แล้วแตะ **ตกลง** (OK)



นอกจากนี้หากมีการแจ้งเตือนการอัพเดทซอฟท์แวร์ ให้แตะลากแถบสถานะจากขอบบนของจอลงมา แล้วแตะที่ **อัพเดทซอฟท์แวร์** (Software update) สังเกตว่าจะมีรายละเอียด เช่น ขนาดไฟล์ เพื่อให้การอัพเดทไม่สะดุด แนะนำให้เลือกใช้ Wi-Fi เป็นหลัก จากนั้นแตะ **ดาวน์โหลด** (Download) รอดาวน์โหลดและอัพเดทซอฟต์แวร์สักครู่จนเครื่องรีสตาร์ท หรือแตะ **ตกลง** (OK) เพื่อรีสตาร์ททันที

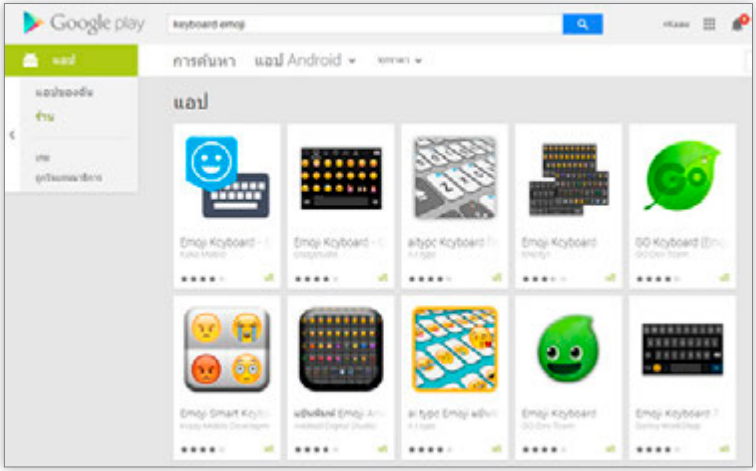


ระวัง! แอพแอบบันทึกการพิมพ์

แอพประเภท Key logger เป็นแอพที่จะคอยแอบเก็บบันทึกการคีย์ข้อความต่างๆ บนแป้นคีย์บอร์ด ไม่ว่าจะเป็นชื่อผู้ใช้ รหัสผ่าน เลขบัญชี เบอร์โทรศัพท์ หรืออื่นๆ ที่เรากรอกขณะใช้งานเครื่องจะถูกบันทึกไว้ทั้งหมด ถึงแม้ว่าเราจะไม่ให้จำรหัสผ่านหรือไปลบข้อมูลการใช้อินเทอร์เน็ตในเครื่องนั้นแล้วก็ตาม เราไม่สามารถไปตามข้อมูลที่ Key logger เก็บไปแล้วได้ ซึ่งข้อมูลที่เก็บได้ก็จะส่งกลับไปยังผู้ที่สร้าง Key logger นั้นขึ้นมา ทำให้ความลับรั่วไหลไปโดยไม่รู้ตัว

Key logger นี้มักจะแอบเข้ามาในเครื่องแบบเนียนๆ เช่น หลอกว่าเป็นแอพแป้นคีย์บอร์ดที่ให้ติดตั้งเพิ่ม, ติดมากับโปรแกรมหรือแอพที่ไปโหลดมา โดยเฉพาะแอพแป้นพิมพ์ หรือถ้าเป็นคอมพิวเตอร์ก็อาจติดมาตอนที่เสียบแฟลชไดรว์หรืออุปกรณ์เก็บข้อมูลต่างๆ โดยโปรแกรมอาจจะติดตั้งตัวเองลงไปอัตโนมัติทันทีที่เชื่อมต่ออุปกรณ์ได้เช่นกัน ซึ่งคุณไม่รู้เลยว่าโดนแอบติดตั้งลงไปตอนไหน แม้ว่าจะใช้เครื่องคอมพิวเตอร์ส่วนตัวก็ไม่สามารถมั่นใจได้ว่าไม่มี Key logger ติดตั้งอยู่

สำหรับเครื่องสาธารณะไม่ว่าจะเป็นเครื่องในร้านเน็ตหรือเครื่องส่วนรวมที่ใช้ร่วมกันในออฟฟิศ ยิ่งต้องใช้งานอย่างระมัดระวังเป็นอย่างมาก



วิธีป้องกันตัวเองจาก Key logger

- ติดตั้งโปรแกรมป้องกันและกำจัดไวรัส บางตัวจะสามารถตรวจพบโปรแกรม Key logger ได้ โดยจะต้องอัพเดทข้อมูลโปรแกรมป้องกันไวรัสนี้บ่อยๆ ด้วย
- ถ้าไม่มั่นใจว่ามี Key logger ในเครื่องหรือไม่ ควรหลีกเลี่ยงการพิมพ์ข้อมูลส่วนตัว ล็อกอินบริการต่างๆ หรือทำธุรกรรมผ่านเน็ต อย่างเด็ดขาด
- เครื่องสาธารณะในร้านเน็ตบางร้านจะมีโปรแกรมรีเซ็ตเครื่องให้เหมือนเครื่องใหม่ทุกครั้งที่รีสตาร์ทเครื่องจะค่อนข้างปลอดภัยกว่า
- ระวังแอพแป้นคีย์บอร์ดที่ให้ติดตั้งเพิ่มทั้งใน iOS (iOS 8 ขึ้นไป) และ Android ให้เลือกติดตั้งเฉพาะตัวดังๆ ที่คนส่วนใหญ่ใช้กันและมีชื่อเสียงว่าไม่มีปัญหา อย่าไปลองตัวแปลกๆ นอกจากคุณจะมั่นใจจริงๆ

สรุปข้อควรระวังในการใช้อินเทอร์เน็ต

เมื่อยุคสมัยเปลี่ยนไป เด็กๆ ในยุคที่การสื่อสารออนไลน์มีอิทธิพลในการใช้ชีวิตประจำวัน ไม่ว่าจะค้นข้อมูล ทำการบ้าน งานกลุ่ม ส่งงาน ปรึกษางานกลุ่ม ก็ต้องมีการใช้อินเทอร์เน็ตแทบทั้งนั้น นอกจากนี้หลายคนยังมีเน็ตซิมใช้ออนไลน์ได้ตลอดเวลาอีกด้วย แต่ด้วยวุฒิภาวะที่ยังไม่มากพออาจทำให้หลงผิดไปกับสิ่งยั่วยุหรือการหลอกลวงในอินเทอร์เน็ตได้ รวมถึงผู้ใหญ่บางคน แม้ว่าจะระวังตัวอย่างดีก็อาจมีบางครั้งที่พลั้งเผลอไปได้ ซึ่งพอจะสรุปข้อควรระวังในการใช้อินเทอร์เน็ตให้ปลอดภัยได้ 10 ข้อดังนี้

01 ออนไลน์แต่พอดีไม่มีโทษ

การออนไลน์ใช้ Social Network มากไปหรือไม่ดูเวลาก็อาจทำให้เกิดอันตรายและเสียสมาธิ เช่น เสียเวลางาน ขาดปฏิสัมพันธ์กับคนตอบข้าง ถ้าควบคุมเครื่องจักร ขับรถ หรือข้ามถนน ไปด้วยเล่นไปด้วย ก็อาจเสียสมาธิเกิดอุบัติเหตุได้ง่าย นอกจากนี้ยังเสียสุขภาพ ใช้สายตามาก อาจปวดหัว ปวดคอ

02 เก็บเรื่องส่วนตัวไว้ไม่ต้องบอกใคร

ไม่เปิดเผยเรื่องส่วนตัวจนเกินไปนัก โดยเฉพาะชื่อ ที่อยู่ เบอร์โทรศัพท์ ตำแหน่งที่อยู่ รวมถึงชื่อและเบอร์โทรของผู้ปกครองหรือบุคคลอื่นๆ ในบ้าน การให้ข้อมูลกับเว็บต่างๆ ก็ควรตรวจสอบว่าเป็นเว็บที่เชื่อถือได้ เช่น มีประกาศชัดว่าไม่มีนโยบายนำข้อมูลส่วนตัวของเราไปขายหรือให้คนอื่นหาประโยชน์อีกต่อหนึ่ง

รหัสผ่านควรเป็นความลับ

ไม่บอกรหัสผ่านต่างๆ กับใคร ตั้งรหัสผ่านให้คาดเดาได้ยาก และห้ามใช้รหัสเดียวกันกับทุกที่ทุกเว็บ

ไม่นัดพบกับคนแปลกหน้า

ไม่นัดพบกับใครที่ได้พูดคุยกันในโลกออนไลน์ คนที่รู้หน้ายังไม่อาจรู้ใจ แล้วนี่หน้าก็ยังไม่เคยเห็นด้วยซ้ำ รูปที่ใช้เป็นรูปโปรไฟล์ก็อาจเป็นรูปปลอมก็ได้

โพสต์สิ่งใดให้ทำด้วยความระมัดระวัง

ไม่โพสต์ข้อความหรือรูปภาพที่ไม่เหมาะสม หรือกล่าวหาผู้อื่นโดยที่ไม่รู้จริง หรือไม่ได้อยู่ในเหตุการณ์ด้วย ระวังคำพูดคำจา ไม่ข้องแวะกับคนที่พูดจาหยาบคายหรือหาเรื่องชวนทะเลาะ

แชร์ต่ออย่างมีสติ

ไม่กุข่าว เมาท์เรื่องที่ไม่ได้รู้จริง สร้างเรื่องเท็จ เผยแพร่หรือส่งต่อคลิปหลุด ข่าวลือ เรื่องเสียๆ หายๆ ที่ทำให้เกิดความเข้าใจผิด ทำให้ผู้อื่นเสียชื่อเสียง และส่งผลเสียต่อประเทศชาติ

07 ไม่หลงผิดไปกับสิ่งผิดกฎหมาย

ไม่ข้องแวะกับการพนัน ยาเสพติด สิ่งลามก อนาจาร เรื่องที่ผิดศีลธรรม หรือผิดกฎหมายต่างๆ

08 เสพสื่ออย่างมีวิจารณญาณ

อย่าไปหลงเชื่อข้อความหรือรูปภาพใดๆ ในอินเทอร์เน็ตโดยไม่วิเคราะห์เหตุและผลก่อน เพราะบางอย่างในเน็ตอาจไม่ใช่เรื่องจริงเสมอไป ควรใช้วิจารณญาณเป็นอย่างมากในการเสพสื่อ ไม่ว่าจะได้พบเห็นอะไรให้ฟังหูไว้หู บางทีนำเสนอข่าวเสียน่าเชื่อถือพอความจริงเปิดเผยก็หงายหลังมานักต่อนักแล้ว

09 ระวังร้านออนไลน์ไม่ซื่อสัตย์

ช้อปปิ้งออนไลน์กับร้านที่เชื่อถือได้ หาข้อมูลร้านก่อนซื้อ อ่านเงื่อนไขของร้านให้เข้าใจก่อนสั่งซื้อ ถ้าโอนเงินแล้วให้เก็บหลักฐานการโอนไว้เป็นอย่างดีจนกว่าจะได้ของครบเรียบร้อย

10 ระวังการละเมิดลิขสิทธิ์

ภาพและข้อความต่างๆ ในอินเทอร์เน็ตล้วนมีเจ้าของ ถ้านำไปใช้หรือแชร์ต่อก็ควรให้เครดิตเจ้าของไว้ด้วย (บางกรณีอาจต้องขออนุญาตก่อนด้วยซ้ำ -ดูหน้า 179)

ข้อควรระวังในการใช้งาน อุปกรณ์มือถือ แท็บเล็ต และอื่นๆ

ทั้งโทรศัพท์มือถือและแท็บเล็ตกลายเป็นสิ่งจำเป็นในชีวิตประจำวันของคนรุ่นใหม่ บางคนก็จะมีอุปกรณ์เหล่านี้ติดตัวอยู่เกือบจะตลอดเวลา ซึ่งการใช้งานอุปกรณ์ก็มีเรื่องที่ควรระวังที่ผู้ใช้ควรทราบอยู่ด้วย ดังนี้

แชร์เน็ตให้คนอื่นต้องระวัง

ถ้าแชร์เน็ตจากมือถือ แท็บเล็ต หรือแม้แต่เน็ตบ้าน ให้คนอื่นใช้ด้วย (ที่เรียกว่า Hotspot, Tethering) ตาม พ.ร.บ. คอมพิวเตอร์แล้วถ้าผู้ที่ใช้เน็ตของเราที่แชร์ไปนั้นเกิดไปโพสต์ข้อความ รูปภาพ หรือกระทำการที่ผิดกฎหมายใดๆ ขึ้นมา เราอาจจะต้องรับผิดชอบสิ่งที่คนนั้นทำด้วยเสมือนว่าเราเป็นผู้กระทำการนั้นเองด้วย ฉะนั้นจึงควรแชร์ให้เฉพาะคนที่รู้จักดี เพื่อนสนิท หรือคนในครอบครัว โดยทำเมื่อจำเป็นเท่านั้น

ระวังคลื่นแม่เหล็กไฟฟ้า

การใช้โทรศัพท์นานๆ หรือวางเครื่องไว้ใกล้ตัวเวลานอนหลับ คลื่นแม่เหล็กไฟฟ้าอาจรบกวนการนอนหรือเป็นอันตรายต่อสุขภาพ (จากข่าว เตือน! “คลื่นแม่เหล็กในมือถือ” เสี่ยงเนื้องอกในสมอง 24 ชม. อ่านเพิ่มที่ www.thairath.co.th/content/191229) แม้ว่าจะยังไม่มีข้อพิสูจน์แน่ชัด แต่ถ้าเลี่ยงการวางไว้ใกล้ตัวตอนนอนได้ก็ดี (ยกเว้นอุปกรณ์พวก Wearable เช่น Smart watch และอื่นๆ ที่ออกแบบให้ติดตัวตลอดเวลาได้)

เปิดดูไฟล์ในแฟลชไดรว์ที่เก็บได้อาจติดไวรัส

ถ้าเก็บแฟลชไดรว์ได้ จะนำไปเสียบกับคอมพิวเตอร์หรือโน้ตบุ๊คเพื่อเปิดดู (รวมถึงแฟลชไดรว์ของคนอื่นๆ ที่มาขอเสียบเข้ากับคอมของคุณ) ควรตรวจดูว่าคอมของคุณติดตั้งโปรแกรมป้องกันและกำจัดไวรัสไว้หรือไม่ เพราะแฟลชไดรว์เป็นอุปกรณ์แพร่กระจายไวรัสเป็นอันดับต้นๆ เลยทีเดียว (ถึงแม้ว่าจะมีโปรแกรมป้องกันไวรัสก็ยังป้องกันได้ไม่ถึง 100% ถ้าไม่มั่นใจก็ไม่ควรเสี่ยง) นอกจากนี้ยังมีไฟล์อื่นๆ ที่แชร์กันมาทางเว็บหรือ Cloud ก็ติดไวรัสได้เช่นกัน

CHAPTER 9

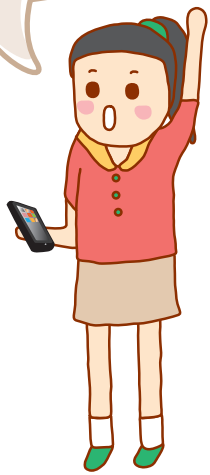
ระวังผลกระทบทาง สังคมและวัฒนธรรม

ปัจจุบันได้เกิดภาวะสังคมก้มหน้า ที่แต่ละคนเอาแต่ก้มหน้าก้มตา กดๆ จิ้มๆ หน้าจอมือถือหรือแท็บเล็ต ไม่ว่าจะเป็นตอนอยู่บ้าน, ที่ทำงาน, ร้านอาหาร, รถเมล์, รถไฟฟ้า, เดินข้างทางหรือสถานที่ต่างๆ ไม่เว้นแม้กระทั่งตอนขับรถ เรียกว่าหยิบขึ้นมาใช้งานทุกที่ที่มีโอกาส ซึ่งหลายคนอาจมีความเข้าใจไม่ถูกต้องทำให้ใช้อุปกรณ์ไม่ถูกกาละเทศะไม่รู้เวล่ำเวลาไม่รู้จักยับยั้งชั่งใจ นอกจากนี้ยังมีบางคนที่ใช้งานโดยไม่รู้ว่ามีค่าใช้จ่ายแอบแฝง โดยเฉพาะผู้เยาว์ที่ยังมีวุฒิภาวะไม่เพียงพอ

มารยาทในการใช้เน็ตซิม

ไม่มีกฎข้อใดที่ห้ามไม่ให้ผู้ใช้โหลดข้อมูลหนักๆ จากเน็ตผ่านเน็ตซิม แต่เนื่องจากการโหลดไฟล์ขนาดใหญ่ (เช่น โหลดบิต (Bittorrent), วิดีโอ Full HD เป็นต้น) ด้วยเน็ตซิมจะใช้ความสามารถของระบบเครือข่ายอย่างมาก ภาษาเทคนิคเรียกว่ากินแบนด์วิธ (Bandwidth) มาก ส่งผลทำให้ผู้ใช้ทั่วไปที่ใช้แค่รับส่งไฟล์เล็กๆ รับส่งอีเมล์ ซึ่งอาจจะเป็นงานสำคัญมากๆ ต้องมาใช้เน็ตที่ช้ากว่าปกติ เพราะแบนด์วิธถูกดึงไปใช้กับผู้ที่รับส่งไฟล์หนักๆ จนเกือบหมด ซึ่งเป็นมารยาททางสังคมในการใช้งานเน็ตซิมซึ่งผู้ใช้ที่ดีจะไม่ทำกัน

นอกจากนี้แพ็กเกจอินเทอร์เน็ตบนมือถือมักเป็นแบบความเร็ว 3G/4G ที่มีจำนวนจำกัดกี่กิ๊กกะไบต์ก็แล้วแต่แพ็กเกจ ถ้าใช้ครบจำนวนตามแพ็กเกจแล้วก็ต้องลดลงมาใช้ความเร็วแบบ EDGE แทนซึ่งช้ากว่ามาก การใช้เน็ตซิมจึงมักสงวนไว้ใช้กับเรื่องสำคัญๆ ซึ่งถ้าจะส่งไฟล์หนักๆ ให้กับคนอื่นก็ควรพิจารณาว่าต้องเป็นเรื่องสำคัญสำหรับผู้รับ ไม่ใช่ไฟล์ไร้สาระที่โหลดมาแล้วก็ต้องลบทิ้ง เพราะถ้าผู้รับใช้เน็ตความเร็วแบบ EDGE ก็จะต้องดาวน์โหลดกันนาน ถ้าใช้แบบ 3G/4G ก็จะเปลืองแบนด์วิธทำให้ใช้หมดเร็ว ดังนั้นถ้าไม่ใช่เรื่องสำคัญผู้รับก็จะเสียทั้งเวลาดาวน์โหลดไฟล์ เสียเวลาเปิดไฟล์ เสียปริมาณอินเทอร์เน็ตในแพ็กเกจที่มีจำกัด และยังเสียความรู้สึกอีกด้วย



ใช้มือถือหรือแท็บเล็ตให้ถูกกาละเทศะ

เมื่อมือถือหรือแท็บเล็ตกลายเป็นอุปกรณ์สำคัญในชีวิตประจำวัน หลายคนก็หยิบใช้กันทุกที่ทุกเวลา ตั้งแต่ตื่นนอน เข้าห้องน้ำ ทานข้าว ดูโทรทัศน์ นั่งรถเมล์รถไฟฟ้าก็แชทหรือเล่น Facebook ได้ตลอดเวลา ถ่ายรูปทุกทีที่มีโอกาส บางทีขับรถก็ยังจะเล่นได้อีก ซึ่งบางอย่างก็ไม่เหมาะสม เราควรเรียนรู้ที่จะใช้อุปกรณ์เหล่านี้แต่พอดีเพื่อไม่ให้มีปัญหาในชีวิตประจำวัน โดยพอจะแนะนำได้ดังนี้

- ปิดโทรศัพท์ขณะอยู่ในโรงภาพยนตร์ แม้ว่าจะปิดเสียงก็ไม่ควรใช้งานใดๆ ในขณะอยู่ในโรงด้วย เนื่องจากแสงไฟจากโทรศัพท์จะรบกวนผู้อื่นที่กำลังชมภาพยนตร์
- แชทกับคนไกลให้น้อยลง พูดคุยกับคนใกล้ให้มากขึ้นไม่ใช่กลับกัน เช่น นัดเพื่อนมาทานอาหารด้วยกันแต่ไม่คุยกับคนรอบข้าง ก้มหน้าก้มตาคุยกับคนไกลเสียอย่างนั้น
- หลายคนคงแซะก่อนทานอาหาร แค่รูปสองรูปคงไม่มีใครว่า (ถ้าไม่ได้เคร่งเรื่องมารยาทมากมาย) แต่ถ้าถ่ายแล้วถ่ายอีก ถ่ายมุมนั้นมุมนี้ ถ่ายเดี่ยว ถ่ายคู่ ถ่ายรูปหมู่ ถ่ายไม่รู้จักเสร็จ ก็อาจโดนตำหนิจากผู้ร่วมโต๊ะอาหารได้

- ขณะใช้งานในสถานที่สาธารณะไม่ควรเปิดเสียงดัง ถ้าจำเป็นควรใช้หูฟังเพื่อไม่ให้รบกวนผู้อื่น
- คอยสังเกตสิ่งรอบข้างตัว บางคนพอคุยโทรศัพท์หรือแชท ก็จะไม่สนใจสภาพแวดล้อมเลย บางทีมีมิจฉาชีพเข้ามาฉกชิงกระเป๋าหรือโทรศัพท์ก็เป็นข่าวบ่อยครั้ง บางครั้งก็อาจทำให้เกิดอุบัติเหตุเนื่องจากมัวแต่จิ้มหน้าจอไปเดินไปไม่ดูทาง บางทีก็เดินช้าเพราะมัวแต่แชท สร้างความรำคาญให้คนรอบข้างได้
- ระหว่างยืนบนรถเมล์ไม่ควรหยิบโทรศัพท์ออกมาเล่น เพราะอาจเบรคกะทันหันทำให้เซล้มจนเกิดอุบัติเหตุได้ ยิ่งผู้หญิงใส่ส้นสูงพอเซก็อาจไปเหยียบเท้าคนข้างๆ ให้บาดหมางใจกันได้ บางรายถือของมือนึง อีกมือนึงก็ถือโทรศัพท์ พอมือไม่ว่างก็ยืนพิงเสาบ้าง ขอบเก้าอี้บ้าง ลักษณะนี้อาจไปรบกวนผู้ร่วมทางที่ต้องการจับเสาหรือไปพิงเบียดกับคนที่นั่งอยู่ก็ได้
- ขับรถอยู่ก็ไม่ควรจะใช้งานโทรศัพท์เลยไม่ว่าจะทำอะไร ยกเว้นจำเป็นต้องโทรออกก็ให้ใช้หูฟังสมอลทอล์ก จะให้ดีจอดรถโทรเลยดีกว่า ไหนจะต้องสไลด์หน้าจอ ใส่รหัสผ่าน กดแอพโทรศัพท์ กดหาเบอร์โทร กดโทรออก ก้มๆ เงยๆ ไม่มีสมาธิก็เกิดอุบัติเหตุได้ง่ายๆ

ปัญหาเกี่ยวกับเกมออนไลน์

หลายคนแบ่งเวลาไม่ได้ พอติดเกมออนไลน์ก็เล่นทั้งวันไม่ทำอย่างอื่น ปัญหานี้มักเกิดกับเด็กๆ ที่ยังไม่มีวุฒิภาวะ ซึ่งนอกจากจะเสียเวลา เสียการเรียน แล้วบางคนอาจเสียเงินค่าเล่นหรือซื้อไอเท็มในเกมอีกด้วย แต่ก่อนจะมีข่าวเด็กติดเกมออนไลน์ในคอมพิวเตอร์ แต่ปัจจุบันเริ่มมาถึงมือถือและแท็บเล็ตแล้ว ที่เป็นข่าวโด่งดังก็ได้แก่ คุ้กกี้รัน ที่ผู้ปกครองหลายคนต้องลมจับมาแล้วเมื่อเห็นบิลค่าโทรศัพท์ โดนเก็บค่าบริการซื้อไอเท็มจากเกมตั้งแต่หลักพันไปจนถึงหลักแสน

หลายคนคงจะผูกเบอร์โทรศัพท์กับบัตรเครดิตเพื่อซื้อแอพ สติกเกอร์ หรือไอเท็มในเกม บางบริการสามารถซื้อโดยชำระพร้อมค่าใช้จ่ายรายเดือนได้เลย เมื่อบุตรหลานนำโทรศัพท์ไปเล่น ด้วยความเป็นเด็กก็มักกดไปเรื่อย อ่านออกบ้าง ไม่ออกบ้าง ไม่ได้อ่านบ้าง พอเล่นเกมออนไลน์ด้วยความที่อยากเล่นต่อ หรือซื้อไอเท็มอัพเกรดอวดกัน ทำให้มีข่าวเด็กเล่นโทรศัพท์หรือแท็บเล็ตจนเสียเงินมากมายอยู่เป็นประจำ (ดูเพิ่มเกี่ยวกับวิธีป้องกันได้ในหน้า 128)

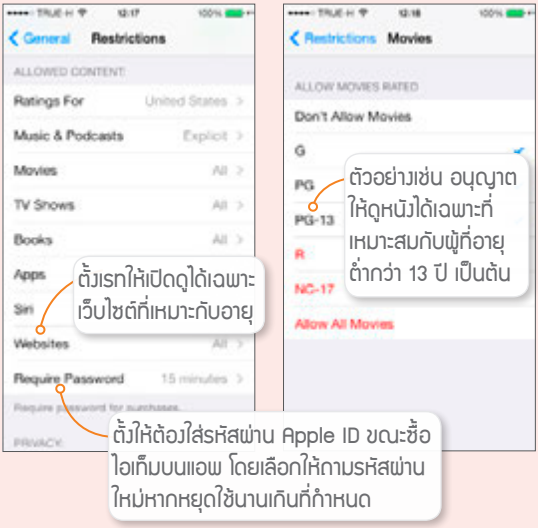
iOS

ตั้งให้ดูได้เฉพาะเนื้อหาที่เรทเหมาะสมกับอายุ

ระบบป้องกันใน iOS ได้เพิ่มระบบป้องกันการเข้าชมวิดีโอใน YouTube หรือการดาวน์โหลดวิดีโอผ่าน iTunes Store, บล็อคเว็บไซต์อนาจาร รวมถึงเกมหรือแอพต่างๆ สำหรับบุตรหลานของคุณ ด้วยการกำหนดเรทอายุของผู้ใช้งานสำหรับบุตรหลานของคุณเอง โดยผู้ปกครองควรดูแลอย่างใกล้ชิด โดยทำดังนี้

1. ไปที่ **Settings** ▸ **General** ▸ **Restrictions** (**การตั้งค่า** ▸ **ทั่วไป** ▸ **การจำกัด**) แล้วแตะ **Enable Restrictions** (**เปิดใช้งานการจำกัด**)
2. ตั้งรหัสผ่านเป็นตัวเลข 4 ตัว (ไม่จำเป็นต้องใช้รหัสเดียวกับที่ใช้ปลดล็อคเครื่องแต่จะตั้งซ้ำกันก็ได้) แล้วยืนยันรหัสผ่านอีกครั้ง
3. จะเห็นว่าแอพหลักถูกเปิดใช้งานไว้ทุกตัว แตะปุ่มปิดการใช้งานแต่ละแอพได้ตามต้องการ

เมื่อเลื่อนลงไปด้านล่างที่หัวข้อ ALLOWED CONTENT จะสามารถกำหนดเรทอายุที่ให้เปิดดูเนื้อหาในรูปแบบต่างๆได้ เช่น เรทอายุของแอพที่ให้ดาวน์โหลด, เรทอายุที่เข้าดูเว็บไซต์ต่างๆ เป็นต้น



ยกเลิกการบล็อคเนื้อหา

เมื่อจะยกเลิกการกำหนดเรทอายุในการเข้าดูเนื้อหาต่างๆ ให้แตะ **Disable Restrictions** (**ปิดใช้การจำกัด**) จากนั้นก็กรอกรหัสผ่านที่ตั้งไว้อีกที

ผู้ปกครองกับการดูแลผู้เยาว์ในเรื่องการใช้อินเทอร์เน็ต

- การทำความเข้าใจและข้อตกลงร่วมกัน ว่าให้ใช้งานได้ระดับไหน เวลาใด หลังเลิกเรียน งดเว้นช่วงสอบ เป็นต้น
- ผู้ปกครองก็ต้องเล่นเน็ตเป็นด้วยในระดับหนึ่ง จึงจะคุยกับลูกหลานได้ไม่ตกยุค รู้เท่าทันกัน เกิดปัญหาจะได้แก้ไขทัน
- เปิดใจให้กว้าง เข้าใจโลกยุคใหม่ที่เปลี่ยนแปลง มีทัศนคติที่ดีกับโลกสมัยใหม่ อย่าใช้ประสบการณ์ของตัวเองมาตัดสิน แต่ให้ใช้เพื่อประสานความคิดและแนะนำผู้เยาว์
- รับฟังและแลกเปลี่ยนความรู้และมุมมองกับผู้เยาว์ หัดใช้เหตุผลอธิบายว่าทำไมควรหรือไม่ควรทำอะไร เพราะอะไร แทนการบังคับ ซึ่งข้อสรุปที่ได้อาจต่างกัน และอาจเปลี่ยนแปลงได้ตามเทคโนโลยีและสถานการณ์ที่เปลี่ยนไป
- บางเรื่องยังคงต้องกวดขันให้ผู้เยาว์มีวินัยในระดับหนึ่ง เช่น การใช้เวลาออนไลน์ แบ่งอย่างไรไม่เสียการเรียนหรือเสียความสัมพันธ์ในครอบครัวหรือในสังคมจริงไป
- คอยตรวจสอบการใช้งาน เรียนรู้เกี่ยวกับการจำกัดการใช้งานบางอย่างเพื่อป้องกันบุตรหลานจากเนื้อหาที่ไม่เหมาะสม เช่น ตั้งให้โหลดได้เฉพาะแอพที่เรทอายุไม่เกิน 18 ปี, ป้องกันการซื้อสติกเกอร์ หรือไอเท็มในเกม จนเกิดค่าใช้จ่ายที่ไม่จำเป็น เป็นต้น
- สำหรับการใช้งานบนคอมพิวเตอร์หรือโน้ตบุ๊ค ไม่ควรวางเครื่องในที่มิดชิดหรืออยู่ในห้องลูก ให้วางในพื้นที่ส่วนรวมที่สามารถดูแลได้ทั่วถึง
- แนะนำเรื่องการนัดพบและเชื่อถือตัวตนของบุคคลในอินเทอร์เน็ต ให้ใช้ความระมัดระวังให้มาก อาจเจอมิจฉาชีพหลอกได้

ปัญหาจากการใช้อุปกรณ์สื่อสารในสังคม

- ปัญหาขาดปฏิสัมพันธ์กับคนรอบข้างที่ใกล้ชิด แต่คุ้นเคยกับคนบนโลกออนไลน์มากกว่า บางทีถึงขั้นแยกไม่ออกว่าอะไรจริงหรือควรเชื่อกว่ากัน
- ความเคยชินและทัศนคติแบบ “คุยได้ทุกที่และทันทีในทุกสถานการณ์” โดยไม่คำนึงถึงกาละเทศะ เช่น คุยโทรศัพท์หรือแชทในโรงหนัง ห้องเรียน แชร์ข้อมูลกิจกรรมส่วนตัวทุกอย่างโดยไม่เกรงใจว่าคนอื่นที่เกี่ยวข้องจะได้รับผลกระทบอย่างไร
- การใช้ภาษา กริยา ท่าทาง การรู้จักกาละเทศะ และวัฒนธรรมอันดีงามอื่นๆ ของไทย ที่ถูกละเลยไปพร้อมๆ กับการออนไลน์ตลอดเวลา และการสื่อสารผ่าน Social media เกิดภาษาวิบัติ สำนวนแปลกๆ การเขียนย่อ เช่น “สวัสดีครับ” เหลือ “ดีคับ” หรือ “ดีครัช” เป็นต้น

โรคไซเบอร์กับวัฒนธรรมไทย

โรคไซเบอร์เป็นการหลงใหลไปกับเทคโนโลยีจนเกินขอบเขต ไม่ใช่เฉพาะเด็กวัยต่างๆ ยังมีผู้ใหญ่ไปจนถึงผู้สูงอายุหลายท่านที่เป็นโรคนี้เช่นกัน ซึ่งถ้าอาการหนักมากอาจทำลายวัฒนธรรมที่ดีงามของไทยได้ ในการใช้งานเทคโนโลยีโดยเฉพาะบนโทรศัพท์มือถือและแท็บเล็ตก็จะมีข้อควรระวังเพื่อรักษาวัฒนธรรมไทยดังนี้

- **กาละเทศะ-กาลเวลา-สถานที่** ใช้งานให้ถูกที่ ถูกเวลา ถูกสถานการณ์ ไม่ใช่ทุกที่ ทุกเวลา ทุกสถานการณ์
- **กิริยาท่าทาง** ขณะใช้งานอาจลืมตัว แสดงกิริยาอาการที่ไม่เหมาะสมในที่สาธารณะ
- **ภาษาพูด** ใช้คำแสลง ผิดเพี้ยน พูดไทยคำอังกฤษคำ คำหยาบ ด่าทอในที่ชุมชน
- **ภาษาเขียนหรือแชท** โดยพิมพ์คำผิด ทั้งที่ตั้งใจและไม่ตั้งใจ อาจติดเป็นนิสัย หรืออาจทำให้คนอ่านเข้าใจไปว่าเขียนถูกได้
- **ภาพ** เดี๋ยวนี้ถ่ายภาพแล้วแชร์ได้ง่าย ให้ระวังการละเมิดสิทธิ์ผู้อื่น หรือถ่ายแล้วส่งต่อภาพไม่เหมาะสม หรือภาพที่ส่งผลกระทบต่อคนในภาพและผู้ที่เกี่ยวข้อง

อธิบายคำศัพท์

เนื่องจากในหนังสือเล่มนี้จะมีการใช้ทั้งคำศัพท์เฉพาะ คำย่อ และคำที่ใช้กันในภาษาพูด ซึ่งจะรวบรวมมาแสดงความหมายไว้ดังนี้

- **เน็ต** มาจากคำว่า อินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายขนาดใหญ่ที่เชื่อมโยงกันทั่วโลก เมื่ออุปกรณ์ต่างๆ เชื่อมต่อเข้ามาในระบบเครือข่ายอินเทอร์เน็ตก็จะสามารถสื่อสารกันได้จากทุกมุมโลก ผ่านโปรแกรมหรือแอพต่างๆ
- **เน็ตซิม** หมายถึง ซิม (SIM Card ของระบบโทรศัพท์มือถือ) ที่สมัครแพ็กเกจอินเทอร์เน็ตจากผู้ให้บริการ เมื่อนำมาใส่ในอุปกรณ์ก็จะเชื่อมต่ออินเทอร์เน็ตได้แบบ 4G/3G/EDGE
- **เน็ตมือถือ (Mobile Internet)** หมายถึง การเชื่อมต่ออินเทอร์เน็ตบนอุปกรณ์พกพาต่างๆ ไม่ว่าจะต่อผ่านเน็ตซิมหรือผ่าน Wi-Fi
- **Data Roaming** คือ การใช้บริการอินเทอร์เน็ตข้ามเครือข่าย ซึ่งจะใช้เมื่อไปต่างประเทศ โดยมีค่าบริการแตกต่างกันไปในแต่ละประเทศและแต่ละผู้ให้บริการ ถ้าไปต่างประเทศแล้วไม่ต้องการใช้ก็ควรปิด Data Roaming ป้องกันการเสียเงินมหาศาลโดยไม่ตั้งใจ

- **Mobile Internet Device (MID)** หมายถึง อุปกรณ์พกพาที่เชื่อมต่ออินเทอร์เน็ตได้ เช่น สมาร์ทโฟน และแท็บเล็ตต่างๆ
- **อุปกรณ์พกพา** หมายถึงอุปกรณ์ที่พกพาไปไหนมาไหนด้วยได้อย่างสะดวก เช่น โทรศัพท์มือถือ, แท็บเล็ต, นาฬิกาอัจฉริยะ เป็นต้น
- **สมาร์ทโฟน (Smart phone)** หมายถึง โทรศัพท์มือถือที่ทำได้มากกว่าโทรออกและรับสาย สามารถเชื่อมต่ออินเทอร์เน็ต และติดตั้งแอพเพิ่มเพื่อทำงานสารพัดรูปแบบได้
- **แท็บเล็ต (Tablet)** หมายถึง อุปกรณ์ที่คล้ายกับสมาร์ทโฟน แต่มีขนาดใหญ่กว่า บางรุ่นสามารถใส่ซิมเพื่อใช้งานโทรศัพท์ บางรุ่นใส่ซิมได้แต่ใช้งานโทรศัพท์ไม่ได้ก็มี บางรุ่นก็ไม่สามารถใส่ซิมได้เลย ต้องต่อเน็ตโดยผ่าน Wi-Fi เท่านั้น

- **เว็บ** เป็นคำเรียกย่อๆ มาจากคำว่า เว็บไซต์ (Web site) ภายในเว็บไซต์จะประกอบด้วยหน้าเว็บเพจหลายๆ หน้าที่มีข้อมูลต่างๆ การเข้าไปที่เว็บไซต์จะต้องระบุที่อยู่เว็บหรือ URL ให้ถูกต้องก่อน
- **ระบบปฏิบัติการ (Operating Systems หรือ OS)** หรือเรียกอีกอย่างหนึ่งว่า *เฟิร์มแวร์* ในโทรศัพท์มือถือและแท็บเล็ตจะมีระบบปฏิบัติการทำหน้าที่บริหาร จัดการ และควบคุมการทำงานของชิ้นส่วนฮาร์ดแวร์ในเครื่อง โดยจะติดต่อกับผู้ใช้ผ่านทางอินเทอร์เฟส (User Interface (UI) หน้าจอการทำงานที่ให้ผู้ใช้สามารถสั่งงานเครื่องด้วยคำสั่งต่างๆ) ที่แตกต่างกันไปในเครื่องแต่ละรุ่น ที่นิยมใช้กันในอุปกรณ์พกพาก็ได้แก่ iOS ที่ใช้ใน iPhone/iPad, Android ที่ใช้ในอุปกรณ์ทั่วไป เช่น Samsung/HTC/LG เป็นต้น, Windows Phone ที่ใช้ใน NOKIA
- **แอพ** เป็นเรียกย่อๆ ของคำว่า แอพพลิเคชั่น (Application) ทำหน้าที่แบบเดียวกับโปรแกรมบนเครื่องคอมพิวเตอร์ แต่แอพพลิเคชั่นนี้จะใช้เรียกโปรแกรมที่ทำงานบนอุปกรณ์พกพาต่างๆ ในระบบปฏิบัติการ iOS, Android, Windows Phone, Symbian รวมถึงโปรแกรมบางประเภทของเครื่องที่ใช้ Windows 8 หรือเครื่องแมคของ Apple ด้วย
- **โพสต์** เป็นการเขียนข้อความ ใส่รูปภาพ คลิปวิดีโอ หรืออื่นๆ ไว้บนอินเทอร์เน็ต ให้ผู้อื่นได้รับรู้
- **แชท (Chat)** เป็นการพูดคุยสนทนากันบนอินเทอร์เน็ตผ่านโปรแกรมหรือแอพพลิเคชั่นต่างๆ
- **ออนไลน์** การกระทำต่างๆ ที่ทำผ่านอินเทอร์เน็ต เช่น เกมออนไลน์ ก็จะหมายถึงเกมที่เล่นผ่านอินเทอร์เน็ต
- **เมล์** คำเรียกย่อๆ มาจากคำว่า อีเมล์ เป็นการส่งจดหมายถึงกันบนอินเทอร์เน็ต โดยผู้ส่งและผู้รับจะต้องมีอีเมล์แอดเดรสสำหรับติดต่อกัน
- **โซเชียลเน็ตเวิร์ก (Social Network)** สังคมออนไลน์ที่ผู้คนมารวมตัวกันบนอินเทอร์เน็ตผ่านโปรแกรมหรือแอพต่างๆ เช่น Facebook, Twitter, Instragram

- **คลาวด์ (Cloud)** เซิร์ฟเวอร์ของผู้ให้บริการบนอินเทอร์เน็ต ซึ่งกระจายอยู่ตามที่ต่างๆ ทั่วโลก จะให้พื้นที่กับผู้ใช้เพื่อเก็บข้อมูลต่างๆไว้บนเน็ต แล้วดึงมาใช้งานได้ในทุกอุปกรณ์และทุกเวลา
- **แบ็คอัพ (Backup)** บันทึกข้อมูลต่างๆ โดยการเก็บสำรองไว้ในเครื่องคอมพิวเตอร์หรือบนอินเทอร์เน็ต (Cloud)
- **รีสโตร์ (Restore)** นำข้อมูลที่แบ็คอัพไว้มาใส่ในอุปกรณ์ให้ใช้งานต่อได้อย่างรวดเร็ว
- **แฮก (Hack)** หมายถึง การเจาะระบบ หรือหลอกลวงด้วยวิธีการต่างๆ เพื่อให้ได้มาซึ่งข้อมูลส่วนตัวของเหยื่อ แล้วนำไปใช้กระทำการต่างๆ เพื่อผลประโยชน์ของแฮกเกอร์ (Hacker ผู้เจาะระบบ)
- **ไวรัส (Virus)** โปรแกรมที่เข้ามาทำงานเพื่อสร้างความเสียหายให้กับอุปกรณ์ และมักแพร่กระจายต่อเพื่อส่งผลกระทบในวงกว้าง
- **โทรจัน (Trojan)** โปรแกรมหรือแอพมุ่งร้ายโดยหลอกให้เจ้าของติดตั้งแล้วลับหลังคอยดักจับข้อมูลหรือทำลายข้อมูลเครื่อง
- **มัลแวร์ (Malware)** โปรแกรมที่มีจุดประสงค์ร้ายต่อเครื่อง ไม่ว่าจะแอบแฝงเข้ามาด้วยวิธีไหนหรือมีการทำงานอย่างไร
- **ฟิชชิ่ง (Phishing)** การหลอกโดยใช้เหยื่อล่อ (เปรียบกับการตกปลา (Fishing)) ให้ไปที่หน้าเว็บปลอมแล้วกรอกชื่อและรหัสผ่านของบริการต่างๆ แล้วดักจับเอาไป
- **ฟาร์มมิ่ง (Pharming)** เป็นการที่แฮกเกอร์โจมตีเซิร์ฟเวอร์ของเว็บหรือผู้ให้บริการอินเทอร์เน็ต โดยเปลี่ยนค่าที่เซิร์ฟเวอร์ให้ส่งผู้ที่เข้าเว็บนั้นด้วย URL ปกติไปยังหน้าเว็บปลอม
- **iTunes** เป็นโปรแกรมที่ติดตั้งในคอมพิวเตอร์เพื่อเชื่อมต่อกับอุปกรณ์ iOS เพื่อซิงค์ข้อมูลต่างๆ รวมถึงแบ็คอัพและรีสโตร์ข้อมูลด้วย
- **เจลเบรค (Jailbreak)** การดัดแปลงระบบปฏิบัติการ iOS เพื่อติดตั้งแอพที่ไม่มีใน App Store หรือแอพเสียเงินแบบฟรีๆ เปลี่ยนธีม (หน้าตาการใช้งาน) หรือทำเพื่อเก็บค่าเฉพาะสำหรับดาวน์เกรดเวอร์ชั่นของระบบปฏิบัติการ
- **รูท (Root)** เป็นการดัดแปลงระบบปฏิบัติการ Android เช่น เพื่อติดตั้งแอพที่ไม่มีใน Play Store, เปลี่ยนธีม เป็นต้น

คู่มือ Cyber Security สำหรับประชาชน

- ท่องเว็บก็โดนเก็บข้อมูลไม่รู้ตัว
- ซ่อนข้อมูลในเครื่อง
- ระวังข้อมูลอัพขึ้น Cloud ไม่รู้ตัว
- เปิดเผยเรื่องส่วนตัวแค่ไหนให้พอดี
- ปิดการแจ้งเตือนจากเกมใน LINE
- แอคเคาท์ถูกแฮกหรือขโมยไป ทำไงดี?
- ตั้งรหัสผ่านอย่างไรให้ปลอดภัย?
- เครื่องหายจะลบข้อมูลในเครื่องอย่างไร
- ตั้งรหัสผ่านล็อคอุปกรณ์แบบออนไลน์
- แสดงความเป็นเจ้าของแม้เครื่องหาย
- ป้องกันไม่ให้เด็กซื้อไอเท็มในเกม
- ตามหามือถือหรือแท็บเล็ตที่หายไป
- แจ้งตำแหน่งปัจจุบันขอความช่วยเหลือ
- ระวังหน้าเว็บหลอกลวง
- ใช้ Wi-Fi สาธารณะฟรีต้องระวัง