ฉลาดรู้เน็ต 2

ตอน Trust on Internet (TOI)

ETDA สพธอ www.etda.or.th

MINISTRY OF ICT Smart Thailand

ฉลาดรู้เน็ต 2

ตอน Trust on Internet (TOI)

ETDA สพธอ

MINISTRY OF ICT Smart Thailand

ฉลาดรู้เน็ต 2

ตอน Trust on Internet (ToI)

หนังสือเผยแพร่เพื่อใช้ในการส่งเสริมการใช้อินเทอร์เน็ต การทำธุรกรรมออนไลน์

ฉลาดรู้เน็ต 2 ตอน Trust on Internet (ToI)
เลขมาตรฐานสากลประจำหนังสือ ISBN 978-616-7956-04-6

พิมพ์ครั้งแรก : มกราคม 2559

สร้างสรรค์โดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
อาคารเดอะไนน์ ทาวเวอร์ เลขที่ 33/4 ตึก B ชั้น 21
ถนนพระรามเก้า แขวงห้วยขวาง เขตห้วยขวาง
กรุงเทพฯ 10310
โทรศัพท์ 0-2123-1234 โทรสาร 0-2123-1200
สพธอ. www.etda.or.th

สุรางคณา วายุภาพ
ผอ.สพธอ.

รัฐศาสตร์ กรสูต
ผู้อำนวยการอาวุโส
สำนักส่งเสริมธุรกรรมทางอิเล็กทรอนิกส์

พายัพ ขาวเหลือง
ผู้จัดการ
งานพัฒนาธุรกิจ

ชณิกา อรัณยกานนท์
ผู้ช่วยผู้จัดการ
งานประชาสัมพันธ์

ทศพร โขมพัตร
เจ้าหน้าที่
ประชาสัมพันธ์อาวุโส

ร่วมแรงกันทำ

กำหนดทิศทาง & แนะนำ	สุรางคณา วายุภาพ (แอน)
กำกับดูแล	รัฐศาสตร์ กรสูต (ดร.เปปเปอร์)
สรรค์สร้างเนื้อหา	พายัพ ขาวเหลือง (ตั้ม)
	ชณิกา อรัณยกานนท์ (กุ้ง)
	ทศพร โขมพัตร (โจ)
ดูแลกราฟิก	ณัฐพงศ์ วรพิวุฒิ (เอ)
	นภดล อุษณบุญศิริ (เฟรม)
	ณัฐนัย รวดเร็ว (ฮอลล์)

คำนำ

ในยุคที่ **“อินเทอร์เน็ต”** เข้ามามีบทบาทกับชีวิตประจำวันของเรา ตั้งแต่ตื่นเช้าถึงเข้านอน อินเทอร์เน็ตช่วยย่อโลกของเราให้เล็กลง สังคมโซเชียลทำให้เรามีเพื่อนมากมายทั่วโลก โดยไม่จำเป็นต้องพบหน้าค่าตา คนทำธุรกิจติดต่อสื่อสารกับลูกค้าผ่านอีเมลได้ตลอด 24 ชั่วโมงทุกมุมโลก การทำธุรกรรมทางการเงินหรือซื้อสินค้าก็สะดวกรวดเร็ว เพียงแค่คลิกตกลง โดยที่ไม่ต้องเดินทางไปถึงธนาคารหรือร้านค้า อย่างไรก็ตาม บางครั้งก็ทำให้เราขาดสติ ไม่ทันได้ระวังตัว หรือลืมนึกถึงความมั่นคงปลอดภัยในการใช้งาน เช่น วัยรุ่นที่นิยม “เช็กอิน” “โพสต์” และ “เช็ต” สเตตัสแบบสาธารณะ เพื่อให้มีคนติดตามหรือเรียกร้องความสนใจจากโลกออนไลน์ ทำให้คนเห็นข้อมูลส่วนตัวได้ทุกคน หรือคนที่ใช้สมาร์ตโฟนละเลยไม่ติดตั้งโปรแกรมแอนตี้ไวรัส บางคนเปลี่ยนเครื่องใหม่แล้วไม่ล้างข้อมูลออกจากเครื่องเก่า บางคนก็ไม่ตั้งพาสเวิร์ดก่อนเข้าใช้เครื่อง ซึ่งล้วนสุ่มเสี่ยงที่จะตกเป็นเหยื่อของผู้ไม่หวังดีที่สามารถเข้าถึงข้อมูลส่วนตัวหรือข้อมูลทางการเงิน และนำข้อมูลเหล่านั้นไปใช้ประโยชน์หรือสวมรอยเป็นตัวเรา นำมาซึ่งความสูญเสีย ตั้งแต่เสียชื่อ เสียทรัพย์ เสียตัว ไปกระทั่งเสียชีวิต

“ฉลาดรู้เน็ต 2 ตอน Trust on Internet (TrI)” มีเป้าหมายให้ผู้อ่านได้เรียนรู้เพื่อที่จะสร้างภูมิคุ้มกันก่อนตกเป็นเหยื่อของภัยคุกคามรูปแบบต่างๆ ด้วยกลเม็ดเคล็ดลับ เช่น เทคนิคการใช้เน็ตให้เป็นส่วนตัว การตั้งและเก็บรักษาพาสเวิร์ด การป้องกันบัญชีอีเมล การใช้โซเชียลมีเดียและการใช้อินเทอร์เน็ตบนอุปกรณ์ต่างๆ อย่างมั่นคงปลอดภัย รวมทั้งการทำความรู้จักกฎหมายไอทีก่อนที่จะกลายเป็นเหยื่อ โดยมีตัวละคร **“พุดน้อย”** และ **“พุดดิ้ง”** จากหนังสือ **“ฉลาดรู้เน็ต 1 ตอน Internet of Things (IoT)”** มาช่วยเติมสีสันและความสนุกสนานเพลิดเพลินไปตลอดทั้งเล่ม

หนังสือเล่มนี้จะเป็นส่วนเติมเต็ม “ฉลาดรู้เน็ต 1” เพื่อให้ผู้อ่านรู้จักโลกอินเทอร์เน็ตอย่างรอบด้าน สามารถใช้งานอย่างเข้าใจ และรับมือกับภัยที่อาจแฝงมากับอินเทอร์เน็ตได้อย่างเท่าทัน ที่สำคัญคือ มีความมั่นใจในการใช้งานอินเทอร์เน็ตยิ่งขึ้น

สุรางคณา วายุภาพ
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
(องค์การมหาชน)

ฉลาดรู้เน็ต 2

ตอน Trust on Internet (ToI)

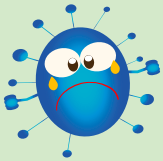
Contents

มาตรวจสุขภาพความมั่นคงปลอดภัย ในการใช้อินเทอร์เน็ตกับพุดดิ้งกันเถอะ

คำถามบทที่ 1

1. เทคนิคการตั้งค่ารหัสผ่าน (Password) E-mail ของเพื่อนๆ เป็นอย่างไร

(1) ฉันสร้างรหัสผ่านจากการใช้การเรียงตามตัวอักษรตามคีย์บอร์ด
(2) ฉันสร้างรหัสผ่านโดยมีความยาวอย่างน้อย 12 ตัวอักษร
(3) ฉันสร้างรหัสผ่านจากเลขที่ วัน/เดือน/ปีเกิด
( ) อื่นๆ (โปรดระบุ).....



2. เพื่อนๆ มีวิธีการปกปิดข้อมูลส่วนตัวอย่างไรไม่ให้ถูกเว็บไซต์ต่างๆ เข้ามาดู

(1) ฉันปกปิดหมายเลขไอพีที่ใช้งาน : โดยอาศัยบริการ VPN หรือ Tor
(2) ฉันเลี่ยงคลิกลิงก์ที่ไม่พึงประสงค์โดยตรง ที่ส่งมาตาม E-mail
(3) ฉันใช้งานโหมดท่องเว็บไซต์แบบส่วนตัว
( ) อื่นๆ (โปรดระบุ).....

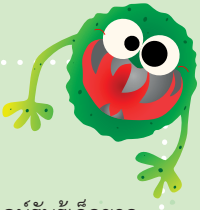
คำถามบทที่ 2

1. วิธีป้องกันไวรัสคอมพิวเตอร์ของเพื่อนๆ เป็นอย่างไร

(1) ฉันติดตั้งโปรแกรมป้องกันไวรัส (Antivirus Software)
(2) ฉันติดตั้งโปรแกรมอินเทอร์เน็ตซีเคียวริตี้ไว้ตรวจจับไวรัส
(3) ฉันใช้โปรแกรม On Screen Keyboard ในการพิมพ์งาน
( ) อื่นๆ (โปรดระบุ).....

2. วิธีป้องกันการถูกขโมยข้อมูลจากแฮกเกอร์ของเพื่อนๆ เป็นอย่างไร

(1) ฉันอัพเดตโปรแกรมแอนตี้ไวรัสอยู่เป็นประจำ
(2) ฉันไม่เคยแอบเล่นอินเทอร์เน็ตไร้สายฟรี นอกจากสัญญาณอินเทอร์เน็ตจากแหล่งที่เชื่อถือได้
(3) ฉันไม่เคยจะดาวน์โหลดโปรแกรมแอนตี้ไวรัสจากเว็บไซต์ที่แจกฟรีมาใช้
( ) อื่นๆ (โปรดระบุ).....



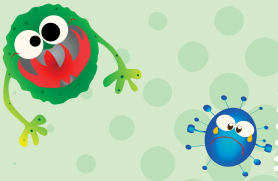
คำถามบทที่ 3

1. เพื่อนๆ มีวิธีพึงระวังให้รอดพ้นจากความเสี่ยงภัยบนโลกออนไลน์อย่างไร

(1) ฉันไม่เคยแสดงข้อมูลสถานที่อยู่จริงบนโลกออนไลน์เลย
(2) ฉันจะไม่ปิดเผยจุดหมายการเดินทางในโลกแห่งความจริงให้คนบนโลกออนไลน์รับรู้เด็ดขาด
(3) ฉันไม่ชอบโพสต์รูปที่แสดงทรัพย์สินภายในบ้านให้คนบนโลกออนไลน์รับรู้เด็ดขาด
( ) อื่นๆ (โปรดระบุ).....

2. สื่อสังคมออนไลน์มีข้อดีอะไรบ้างในความคิดของเพื่อนๆ

(1) ประหยัดค่าใช้จ่ายในการติดต่อสื่อสาร
(2) สื่อสารรวดเร็วทันใจ
(3) เป็นสื่อแสดงศิลปะและความคิดเห็น
( ) อื่นๆ (โปรดระบุ).....



คำถามบทที่ 4

1. แนวทางการใช้งานโทรศัพท์มือถือให้เกิดความมั่นคงปลอดภัยของเพื่อนๆ เป็นอย่างไร

(1) ฉันตั้งค่าการล็อกโทรศัพท์มือถือเมื่อไม่ใช้งานไว้ตลอด

(2) ฉันสำรองข้อมูลจากโทรศัพท์มือถือไว้ในแหล่งอื่นที่มั่นคงปลอดภัยด้วย

(3) ฉันเลือกเก็บเฉพาะข้อมูลที่จำเป็นในโทรศัพท์มือถือ

( ) อื่นๆ (โปรดระบุ).....

2. เทคนิคการใช้สมาร์ตโฟนและแท็บเล็ตให้เกิดความมั่นคงปลอดภัยของเพื่อนๆ เป็นอย่างไร

(1) ฉันอ่านข้อตกลงการใช้งานทุกครั้งก่อนดาวน์โหลดแอพพลิเคชั่นมาใช้

(2) ทุกครั้งที่ซื้อสมาร์ตโฟนและแท็บเล็ตรุ่นใหม่ ฉันจะไม่เคยลืมที่จะดาวน์โหลดแอพพลิเคชั่นป้องกันไวรัสมาใช้

(3) ฉันเรียนรู้ที่จะใช้ประโยชน์จากการโปรแกรมสำรองข้อมูลไว้ใช้ฉุกเฉินในยามที่ข้อมูลหายหรือถูกขโมยไป

( ) อื่นๆ (โปรดระบุ).....

คำถามบทที่ 5

1. วิธีการป้องกันการโดนหลอกจากการซื้อสินค้าผ่านร้านค้าออนไลน์ของเพื่อนๆ เป็นอย่างไร

(1) ฉันเลือกร้านค้าที่มีชื่อเสียงตอบรับในทางที่ดี

(2) ฉันเลือกซื้อสินค้าในเว็บไซต์ที่เปิดร้านมาอย่างน้อย 1 ปี

(3) ฉันพิจารณาเงื่อนไขการรับประกันสินค้าจากร้านค้าก่อนเสมอ

( ) อื่นๆ (โปรดระบุ).....

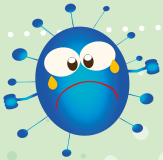
2. พฤติกรรมอย่างไรบ้างที่เพื่อนๆ คิดว่าจะมีความผิดตาม พ.ร.บ. คอมพิวเตอร์

(1) การส่งข้อมูลเท็จเข้าสู่ระบบคอมพิวเตอร์

(2) การขโมย E-mail และรหัสผ่าน (Password) ของผู้อื่นไปใช้งานโดยไม่ได้รับอนุญาต

(3) การโพสต์ข้อความใส่ร้ายผู้อื่น เช่น การคอมเม้นท์เป็นคำหยาบ

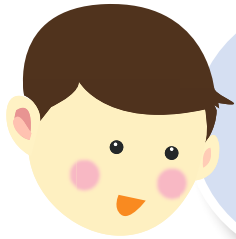
( ) อื่นๆ (โปรดระบุ).....



พลิกหนังสือในหน้าถัดไป
แล้วมาร่วมหาคำตอบ
ด้านความมั่นคงปลอดภัย
บนโลกออนไลน์กันเลยค่ะ

บทที่ 1

เปิดโลกเน็ตกว้าง
แต่ปิดทางให้มี
ความเป็นส่วนตัว



โลกออนไลน์
ใครว่าน่ากลัว หากรู้เทคนิค
การเข้ารหัส (Encryption)
ก็สามารถใช้ชีวิตได้อย่าง
มั่นคงปลอดภัยแล้ว

1.1 เทคนิคการใช้เน็ตให้เป็นส่วนตัว

พุดน้อยเคยได้ยินเพื่อนของคุณพ่อซึ่งมาเยี่ยมที่บ้าน พูดว่าเมื่อไม่นานมานี้ เพิ่งจะถูกแฮกเกอร์ (Hacker) มือดีเข้ามาล้วงข้อมูลใน e-Mail บริษัท แต่ยังดีที่ข้อมูลสำคัญไม่ถูกนำไป เพราะได้ถ่ายโอนข้อมูลไปอยู่ยังคอมพิวเตอร์เครื่องอื่นแล้ว พุดน้อยได้ฟังการสนทนาแล้ว ในวันนั้นก็ได้ความรู้ใหม่ๆ เกี่ยวกับ **"เทคนิคการใช้เน็ตให้เป็นส่วนตัว"** ซึ่งสามารถนำไปปรับใช้ได้เป็นอย่างดีในชีวิตประจำวัน มาฝากเพื่อนๆ กัน

การเรียนรู้เกี่ยวกับ **“เทคนิคการใช้เน็ตให้เป็นส่วนตัว”** นับว่ามีความจำเป็นอย่างมาก เพราะจะช่วยทำให้เราสร้างความมั่นคงปลอดภัยจากภัยคุกคามความเป็นส่วนตัวส่วนใหญ่ที่อาจจะเกิดขึ้น เช่น ภัยจากการถูกดักฟังและการถูกล้วงข้อมูล และยิ่งหากเป็นการใช้บริการผ่านสัญญาณ WiFi ซึ่งมีรัศมีบรรยากาศถึง 40 เมตร ที่เปิดให้ใช้ฟรีตามแหล่งชุมชนหรือห้างสรรพสินค้าต่างๆ แล้วละก็ นับว่าน่ากลัวเลยทีเดียว

การเข้ารหัส (Encryption)

จากในบทสนทนาของคุณพ่อกับเพื่อนคุณพ่อ ทำให้พุดน้อยทราบว่าในโลกของการใช้อินเทอร์เน็ตนั้น มีวิธีการป้องกันการดักฟังในระดับพื้นฐานอยู่เรียกว่า **การเข้ารหัส (Encryption)** ซึ่งการเข้ารหัสลักษณะนี้นับว่าเป็นกระบวนการทางคณิตศาสตร์ที่ซับซ้อน และให้ผลลัพธ์ที่ตรงไปตรงมาที่สุด อธิบายง่ายๆ คือ ข้อมูลทั้งหมดที่ส่งจากเครื่องต้นทาง ไปยังเครื่องปลายทาง แม้จะถูกดักฟังระหว่างทางจากผู้ไม่ประสงค์ดี แต่ผู้ดักฟังก็ไม่สามารถล่วงรู้ได้เลยว่าเราส่งข้อมูลอะไรออกจากเครื่องคอมพิวเตอร์ ดังนั้น การเข้ารหัสจึงนับเป็นวิธีการลำดับแรกๆ ที่ผู้ใช้อินเทอร์เน็ตอย่างเราๆ ควรศึกษาไว้

โดยการเข้ารหัสนั้น พูดน้อยยังทราบอีกว่า สามารถทำได้หลากหลายรูปแบบ ส่วนรูปแบบมาตรฐานที่พบกันบ่อยๆ คือ การเข้ารหัสแบบ WEP WEP2 WPA WPA2 ที่เป็นการเข้ารหัสจากเครื่องของเราไปยังจุดบริการสัญญาณไร้สาย และอีกรูปแบบหนึ่งก็คือ การเข้ารหัสแบบ HTTPS ที่จะมีความมั่นคงปลอดภัยมากกว่า เพราะเราสามารถใช้การรับส่งข้อมูลผ่านเว็บไซต์จากเครื่องของเราไปยังเครื่องเซิร์ฟเวอร์ปลายทางได้ทันที ซึ่งตัวอย่างการใช้บริการผ่านเว็บไซต์ต่างๆ ได้แก่ จีเมล (Gmail), ฮอตเมล (Hotmail), เฟซบุ๊ก (Facebook) และทวิตเตอร์ (Twitter) โดยวิธีการในลักษณะนี้สามารถสร้างความมั่นคงปลอดภัยให้แก่ผู้ใช้บริการทุกท่านเมื่อต้องเชื่อมต่อสัญญาณผ่าน WiFi ได้ดีเลยทีเดียว

เทคนิคการเข้ารหัสในรูปแบบ HTTPS นั้น จะใช้วิธีการพิมพ์ https:// และตามด้วยชื่อเว็บไซต์ เช่น https://www.google.co.th แทนที่จะพิมพ์แค่ชื่อเว็บไซต์อย่างเดียว ซึ่งเว็บไซต์ที่ได้รับความนิยมสูง อย่างเฟซบุ๊ก และทวิตเตอร์ เว็บไซต์ในลักษณะนี้จะมีระบบการเข้ารหัส HTTPS โดยอัตโนมัติ แต่ทั้งนี้ก็มีบางเว็บไซต์ที่ยังไม่รองรับการเข้ารหัสในรูปแบบนี้ โดยผู้ใช้บริการจะต้องทำการพิมพ์เข้ารหัสด้วยตนเอง คิดเสียว่า เราเสียเวลาเพียงน้อยนิด แต่สามารถเพิ่มความมั่นคงปลอดภัยให้กับตนเองได้มากขึ้น ก็นับว่าคุ้มค่าไม่น้อย

การเชื่อมต่อแบบไม่เปิดเผยตัวตนด้วย Tor (Term of Reference)

ส่วนในกรณีที่เราต้องเดินทางไปต่างประเทศ และจำเป็นต้องใช้บริการอินเทอร์เน็ต พุดน้อยเชื่อว่าหลายๆ คน อาจจะไม่มั่นใจว่าผู้ให้บริการโทรคมนาคมในประเทศนั้นๆ มีการรักษาความมั่นคงปลอดภัยต่อข้อมูลส่วนตัวของเราได้ดีมากน้อยแค่ไหน ในที่นี้พุดน้อยจึงขอแนะนำซอฟต์แวร์ตัวหนึ่งที่เรียกว่า Tor

Tor ซึ่งจัดเป็นตัวช่วยที่ดี มีคุณสมบัติที่จะทำให้ผู้ใช้บริการสามารถใช้อินเทอร์เน็ตได้อย่างมั่นคงปลอดภัย โดยเมื่อถูกติดตั้งแล้วจะสร้างเครือข่ายพิเศษขึ้นมา โดยอาศัยคอมพิวเตอร์ของอาสาสมัครจำนวนมากทั่วโลกส่งต่อข้อมูลไปมาหลายครั้ง ทำให้ผู้ให้บริการอินเทอร์เน็ตที่เราเชื่อมต่ออยู่ไม่สามารถรู้ได้ว่าเรากำลังเข้าชมอะไร รวมทั้งผู้ไม่หวังดี ก็ไม่สามารถย้อนรอยหาตัวตนของเราได้โดยง่ายด้วย

ซอฟต์แวร์ Tor สร้างโดย มูลนิธิพรมแดนอิเล็กทรอนิกส์ (อีเอฟเอฟ) (Electronic Frontier Foundation : EFF) ซึ่งเป็นองค์กรไม่แสวงกำไรด้านเสรีภาพอินเทอร์เน็ต และมีสำนักงานใหญ่อยู่ที่ซานฟรานซิสโก สหรัฐอเมริกา (ดาวน์โหลด Tor ได้ที่ https://www.torproject.org/projects/torbrowser.html.en)

การเข้ารหัสแบบ VPN (Virtual Private Network)

เพื่อนๆ รู้ไหมว่า ยังมีการเข้ารหัสข้อมูลอยู่รูปแบบหนึ่งที่ได้รับความนิยมเป็นอย่างมาก เรียกว่า การเข้ารหัสแบบ VPN (Virtual Private Network) ก็คือ การที่เราสามารถเลือกผู้ให้บริการที่มีกฎหมายการคุ้มครองความเป็นส่วนตัวสูง สามารถทำให้เราเชื่อมต่อโครงข่ายสาธารณะมาใช้ในการส่งข้อมูล โดยใช้การสร้างรหัส เป็นระบบเครือข่ายเสมือนขึ้น ซึ่งข้อมูลที่ส่งออกไปยังสามารถรักษาความลับได้อย่างมั่นคงปลอดภัย โดยมีกำหนดราคาค่าใช้จ่ายตั้งแต่เดือนละ 150 บาท (https://www.ibvpn.com/) เรื่อยไปจนถึง 600 บาทต่อเดือน (https://www.goldenfrog.com/vyprvpn) ลงทุนไม่มากแต่ก็ถือว่าคุ้มค่าและมั่นคงปลอดภัยด้วยนะครับ

การตั้งค่าความเป็นส่วนตัวใน Facebook

เริ่มต้นที่ Login เข้า Account Settings / ตั้งค่าบัญชีผู้ใช้ > จากนั้นไปที่ Security / ความปลอดภัย แล้วให้เลือก Secure Browsing / เรียกดูแบบปลอดภัย และให้คลิกเลือกออฟชั่น Browse Facebook on a Secure Connection (https) When Possible / เรียกดู Facebook บนการเชื่อมต่อแบบปลอดภัย https:// เพียงเท่านี้ก็เรียบร้อยแล้ว

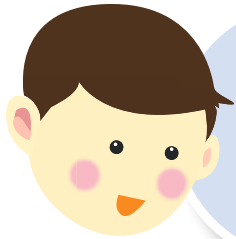
การตั้งค่าความเป็นส่วนตัวใน Twitter

เริ่มต้นที่ Login เข้าเลือกที่หัวข้อ Settings หลังจากนั้นให้คลิกเลือก Always use HTTPS

เท่านี้ผู้ใช้บริการอย่างพุดน้อย คุณพ่อ คุณแม่ และเพื่อนๆ ทุกคน ก็สามารถเข้าใช้บริการ Social Media ได้อย่างมั่นคงปลอดภัยแล้ว

น้องพุดดิ้งชวนรู้

เพื่อนๆ ที่ได้รู้จักเทคนิคการใช้เน็ตให้เป็นส่วนตัวจากพุดน้อยแล้ว ควรจะนำวิธีการเข้ารหัสดังกล่าวไปเลือกใช้ให้เหมาะกับพฤติกรรมการใช้อินเทอร์เน็ตของตนเอง และที่สำคัญควรนำเทคนิคดีๆ เหล่านี้ ไปบอกต่อให้กับเพื่อนๆ หรือญาติพี่น้องให้นำไปปฏิบัติใช้ด้วย เพื่อสร้างความมั่นคงปลอดภัยกันทั้งครอบครัว

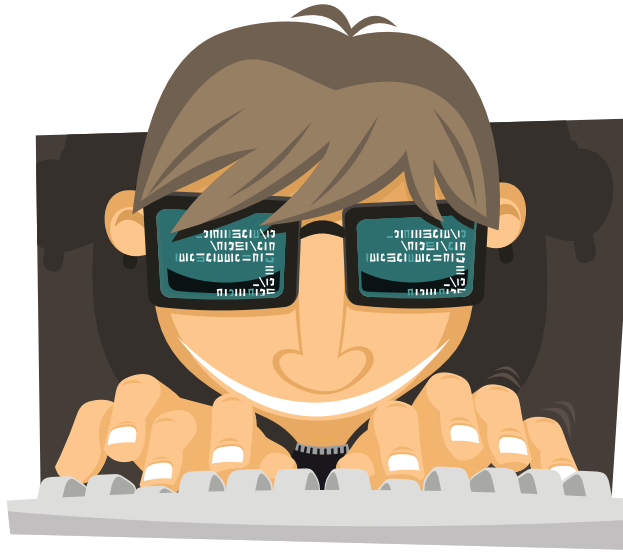


ความเป็นส่วนตัว
ในโลกอินเทอร์เน็ตจะมั่นคงปลอดภัย
และสนุก ถ้าเพื่อนๆ เรียนรู้สูตรการ
สร้างรหัสผ่าน แบบเหมาะสม ง่าย
ไม่ซับซ้อน จากพุดน้อย

1.2 ตั้งพาสเวิร์ดเจ๋งๆ ทำง่ายแต่แฮกยาก

ในเช้าที่อากาศสดใสของวันหยุดสุดสัปดาห์ ภายในห้องรับแขก พุดน้อยสังเกตเห็นคุณอากำลังใช้คอมพิวเตอร์ทำงานผ่านโครงข่ายอินเทอร์เน็ตไร้สายอยู่ และด้วยความที่พุดน้อยเป็นเด็กช่างสงสัย จึงได้ขอความรู้จากคุณอาถึงวิธีการรักษาตัวตนในโลกออนไลน์ ที่มากกว่าวิธีการเข้ารหัสแบบ HTTPS

โดยคุณอาผู้รอบรู้เล่าให้พุดน้อยฟังว่า *“แท้จริงแล้วการรักษาความเป็นส่วนตัวในโลกออนไลน์ในชีวิตประจำวันของเรานั้น ยังมีช่องโหว่อีกมากที่สามารถทำให้บรรดาแฮกเกอร์ทำการล้วงข้อมูลเราได้ โดยเฉพาะผู้ที่ใช้บริการผ่านระบบ e-Mail ที่ต้องยืนยันตัวตนด้วยการ Login รหัสผ่าน เพื่อเป็นการยืนยันตัวตนของผู้ใช้งานว่าเป็นเจ้าของบัญชีที่แท้จริงหรือไม่”*



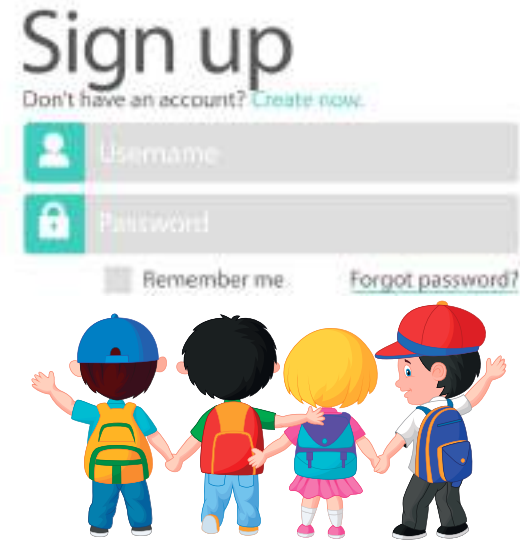
คุณอายังได้อธิบายให้พุดน้อยเข้าใจว่า การขโมยตัวตน หรือที่เรียกว่า Identity Theft นั้น หากเราไม่มีวิธีการระมัดระวังที่ดี อาจเป็นสาเหตุสำคัญที่ทำให้เกิดการสูญเสียกับตัวผู้ใช้งานได้ ซึ่งการขโมยตัวตนในโลกออนไลน์นั้นมักจะทำร่วมกับสิ่งอื่นๆ ที่ไม่ชอบมาพากล เช่น การปลอมแปลงเว็บไซต์เพื่อที่จะหลอกดักข้อมูลชื่อผู้ใช้และรหัสผ่านจากเรา แล้วนำข้อมูลที่ได้มาปลอมแปลงอีกครั้งเพื่อนำไปหลอกลวงผู้ใช้งานอื่นๆ อีกทอดหนึ่ง ไปจนถึงการทำให้ได้รับความเสื่อมเสียชื่อเสียง อับอาย และเสียทรัพย์สิน หรือตกเป็นผู้ต้องสงสัยในคดีอาญา ก็มีให้เห็นกันพอสมควร

แต่ในบางกรณีบรรดา Hacker ก็อาจจะใช้วิธีการคาดเดารหัสผ่านที่มีความสุ่มเสี่ยงต่อการคาดเดา ซึ่งก็เป็นอีกวิธีที่ทำให้ผู้ใช้บริการถูกขโมยตัวตนออนไลน์ไปใช้แบบไม่รู้ตัว เช่น ตั้งรหัสจากตัวเลข วัน/เดือน/ปีเกิด หรือจะเป็นกรณี การละเลยจากตนเองปล่อยให้มีการ Login คอมพิวเตอร์ในเว็บไซต์ต่างๆ ทิ้งไว้ในร้านคอมพิวเตอร์ หรือคอมพิวเตอร์สาธารณะ และเมื่อมีผู้ไม่ประสงค์ดีมาพบข้อมูลของเราก็จะถูกขโมยไป ต่อเนื่องไปจนถึงการถูกสวมรอยเพื่อเข้าถึงบัญชีธนาคาร หรือการทำธุรกรรมที่ผิดกฎหมาย ดังนั้น เราควรที่จะเก็บรักษารหัสผ่านของเราไว้อย่างดีที่สุดนะครับ

แนวทางการสร้างรหัสผ่านที่เหมาะสม

มาถึงวรรคนี้ เพื่อนๆ คงอยากรู้กันแล้วละสิว่า วิธีการตั้งรหัสผ่านที่ยากต่อการคาดเดา ที่จะนำมาฝากเพื่อนๆ นั้น มีวิธีการอย่างไรบ้าง ฟังทางนี้พุดน้อยมีคำแนะนำ

1. ตั้งรหัสผ่าน 8-12 ตัวอักษรขึ้นไป
2. การสร้างรหัสผ่านต้องมีการผสมตัวอักษร ตัวเลข อักษรพิเศษ และอักษรเล็ก/ใหญ่
3. ไม่ควรใช้คำจากพจนานุกรมหรือใช้ข้อมูลส่วนตัวที่หาได้ง่าย ได้แก่ ชื่อ วัน/เดือน/ปีเกิด มาตั้งเป็นรหัสผ่าน
4. หลีกเลี่ยงการใช้ตัวอักษรเรียงลำดับตามการวางของคีย์บอร์ด เช่น “ASDFGHJk”
5. ไม่ควรสร้างรหัสผ่านที่เหมือนกันทุกเว็บไซต์ เพราะเมื่อใดที่รหัสหลุดไปสู่มือ Hacker เราอาจถูกลักขโมยความเป็นตัวตนไปได้



ปกป้องความเป็นตัวตนบนโลกออนไลน์

นอกจากหลักฐานและข้อห้ามในการตั้งรหัสผ่านแล้ว พุดน้อยขอเพิ่มเติมอีกสักนิด เกี่ยวกับเทคนิคการเลือกเว็บไซต์ที่มีความน่าเชื่อถือ เพื่อหลีกเลี่ยงไม่ให้ข้อมูลของเราถูก Hacker ดักขโมยไป ดังนี้

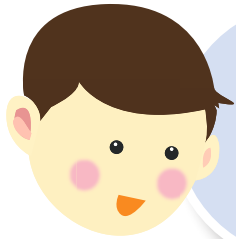
1. เลือกเว็บไซต์ที่มีการเข้ารหัสอย่างถูกต้อง และมีการใช้ SSL Certificates หรือเรียกสั้นๆ ว่า SSL ซึ่งก็คือเครื่องหมายรับรองความมั่นคงปลอดภัยทางอิเล็กทรอนิกส์ ที่ออกโดย CA (Certificate Authority) หน่วยงานที่ตรวจสอบความถูกต้องและมาตรฐานใบรับรองความมั่นคงปลอดภัยทางอิเล็กทรอนิกส์

2. หลีกเลี่ยงการใช้บริการคอมพิวเตอร์สาธารณะกับเว็บไซต์ที่เกี่ยวข้องกับสถาบันการเงิน เช่น เว็บไซต์ธนาคาร และทั้งนี้ควรปิดเบราว์เซอร์ทุกครั้งหลังใช้งานเสร็จสิ้น

3. หลีกเลี่ยงการใช้บริการ WiFi สาธารณะ และเว็บไซต์ที่ไม่มีบริการการเข้ารหัส ซึ่งจะเสี่ยงต่อการถูกดักฟังได้ง่ายๆ

น้องพุดดิ้งชวนรู้

ความสั้น–ยาวของพาสเวิร์ด รวมถึงการใช้ข้อมูลส่วนตัวมาใช้ตั้งพาสเวิร์ด ถือเป็นธรรมเนียมนิยมของผู้ใช้บริการ E-mail จำนวนมาก เนื่องจากไม่ชื่นชอบการจดจำอะไรที่ยาวๆ ยากๆ แต่หารู้ไม่ว่าพฤติกรรมดังกล่าว นับเป็นสิ่งที่โปรดปรานของบรรดา Hacker ให้เข้ามาลักขโมยข้อมูลของเราได้ง่ายมาก ซึ่งท้ายที่สุดแล้วการป้องกันรหัสผ่านที่ดีที่สุด ก็ย่อมมาจากพฤติกรรมของผู้ใช้บริการเอง หากยอมรับการเปลี่ยนพฤติกรรมเสียบ้าง ตามหลักการปฏิบัติที่ได้แนะนำกันไป ข้อมูลส่วนตัวบนโลกออนไลน์ของเราก็จะมั่นคงปลอดภัยขึ้น



ปฏิเสธพฤติกรรม
การจดพาสเวิร์ด แต่รู้รักษาพาสเวิร์ด
ด้วยการจำ สร้างความมั่นคง
ปลอดภัยที่ยั่งยืน

1.3 เคล็ดลับการเก็บรักษาพาสเวิร์ด

การเล่นอินเทอร์เน็ตเป็นความสุขอีกอย่างหนึ่ง ที่พุดน้อยมักทำเป็นประจำทุกวัน แต่หลายครั้งที่พุดน้อยเล่นอินเทอร์เน็ตแล้วได้ยินข่าวคราวการขโมยความเป็นตัวตนในโลกอินเทอร์เน็ตจากบรรดา Hacker เสมอ ทำให้พุดน้อยสงสัยว่าเหตุใด Hacker เหล่านี้จึงสามารถรับรู้ถึงรหัสพาสเวิร์ดของเราได้

ซึ่งหลังจากปรึกษา พุดน้อยก็ได้ข้อมูลที่น่าสนใจว่า เวลาที่เราทำการเชื่อมต่อคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ตเพื่อเข้าสู่เว็บไซต์ต่างๆ บรรดา Hacker จะใช้วิธีการคาดเดารหัสพาสเวิร์ดของเราแบบสุ่ม เช่น คาดเดาจากเลขที่ วัน เดือน ปีเกิด ส่วนบางกรณีก็มาจากความไว้เนื้อเชื่อใจคนใกล้ตัวหรือคนสนิทและบอกรหัสพาสเวิร์ด ของ e-Mail ตนเองไป ซึ่งในความเป็นจริงแล้วถือเป็นข้อห้ามที่ไม่ควรทำเป็นอย่างยิ่ง เนื่องจากเสี่ยงที่พาสเวิร์ดอาจจะหลุดไปสู่มือผู้ไม่ประสงค์ดีได้

1. สร้างรหัสผ่านให้ซับซ้อน : การสร้างรหัสผ่านที่ซับซ้อนและยากต่อการจดจำ นับเป็นปราการด่านสำคัญอันดับแรกที่จะช่วยสร้างความมั่นคงปลอดภัยให้กับความเป็นส่วนตัวของเรา ยกตัวอย่าง การสร้างรหัสผ่านจากการสร้างประโยค เช่น "I always browse to Yahoo! on Monday night." แล้วเลือกอักษรสองตัวแรก จากทุกคำให้กลายเป็นรหัสผ่าน "IalbrtoYaonMoni" จากนั้น ก็อาจจะเพิ่มตัวอักษรพิเศษแทรกเข้าไป เช่น การเพิ่ม "#24" ระหว่างอักษรตัวที่ 2 และ 3 ซึ่งรหัสผ่านก็จะกลายเป็น "Ia#24lbrtoYaonMoni" ซึ่งไม่มีความหมาย และไม่สามารถคาดเดาได้ง่ายๆ เท่านี้บรรดา Hacker ก็เดากันไม่ถูกแล้ว

2. สร้างรหัสผ่านให้ยาว : นอกจากการตั้งรหัสผ่านที่ซับซ้อนและยากต่อการจดจำ การตั้งรหัสผ่านให้ยาวมีตัวหนังสือเยอะๆ อย่างน้อยๆ ก็ให้มีสัก 12 ตัวอักษร ก็นับเป็นอีกหนทางหนึ่งที่ทำให้ Hacker ยากต่อการคาดเดา

3. ไม่จดหรือบันทึกรหัสผ่านติดตัว : ตั้งรหัสผ่านก็ยาวแถมยังซับซ้อนจนยากต่อการคาดเดา แต่กลับจดรหัสผ่านทั้งหมดใส่กระดาษและพฤติกรรมใส่กระเป๋าสตางค์หรือติดไว้ตามฝาผนังบ้าน ให้คิดเสียว่าวันใดก็ตามที่เราวางกระเป๋าสตางค์ไว้ในสถานที่สาธารณะโดยไม่ระวัง วันนั้นอาจเกิดเหตุการณ์ที่มีผลกระทบกับความมั่นคงปลอดภัยขึ้นกับเราก็เป็นได้

4. ไม่ให้รหัสผ่านกับใครโดยไม่จำเป็น : การให้รหัสผ่านกับผู้อื่น แม้จะเป็นคนใกล้ตัว ก็อาจเป็นดาบสองคมซึ่งจะทำให้รหัสผ่านหลุดไปสู่มือ Hacker ได้ แต่หากจำเป็นต้องให้รหัสผ่านแก่ผู้อื่น เช่น คนในครอบครัว หลังจากใช้งานเสร็จก็ควรทำการเข้าไปตั้งค่ารหัสผ่านใหม่ทุกครั้ง

น้องพุดดิ้งชวนรู้

พุดดิ้งสรุปได้ว่า การสร้างปราการด่านสำคัญในการเก็บรักษาพาสเวิร์ด สอนให้เรารู้ว่า ความมั่นคงปลอดภัยจะเกิดกับผู้ใช้อินเทอร์เน็ตได้ก็ต่อเมื่อ ผู้ใช้อย่างเราต้องหมั่นมีสติในการรู้คิดและรักษาพาสเวิร์ดให้อยู่กับตัว (ความคิด) ตลอดเวลา เพราะการจดบันทึกที่เป็นลายลักษณ์อักษร บางครั้งก็อาจเป็นความเคยชินที่พาภัยร้ายมาสู่ตนเองก็เป็นได้

1.4 Search Engine *เสิร์ชเสร็จลบคำค้นหา*

แม้พุดน้อยจะเพิ่งเริ่มใช้คอมพิวเตอร์เล่นอินเทอร์เน็ตเป็นได้ไม่นาน แต่ไม่เชื่อก็ต้องเชื่อว่า ความเคลื่อนไหวในช่วงสิบกว่าปีที่ผ่านมาของโลกออนไลน์นั้นถูกขับเคลื่อนโดยความสามารถอันเก่งกาจของเว็บค้นหา (Search Engine) ซึ่งถูกพัฒนาจนทำให้ผู้ใช้บริการสามารถค้นหาข้อมูลที่ต้องการจากข้อมูลปริมาณมหาศาลได้ภายในเวลาไม่ถึงวินาที เรียกได้ว่าความสามารถของเว็บค้นหาเหล่านี้นับเป็นการสร้างประโยชน์ให้แก่มนุษย์มหาศาล

แต่ทั้งนี้ในความมีประโยชน์อันมหาศาลก็ย่อมต้องแฝงไปด้วยภัยที่ไม่สามารถหลีกเลี่ยงได้ หากมีผู้ใช้บริการที่ประสงค์ไม่ดี นำเทคโนโลยีไปใช้ในทางที่ผิด กล่าวคือ เว็บไซต์ค้นหาที่มีความสามารถในการวิเคราะห์เอกสารและคำค้นหาได้เป็นอย่างดี จะสามารถวิเคราะห์ได้ว่าชื่อที่อยู่ใต้ภาพนั้นเป็นชื่อของใคร และสามารถแสดงภาพของบุคคลเหล่านี้ออกมาได้อย่างถูกต้อง ด้วยเหตุนี้หากมองมุมกลับ เช่น การมีผู้ใดมาค้นหาประวัติของเรา ก็อาจเป็นเหตุทำให้ **ข้อมูลส่วนตัวของเราสุ่มเสี่ยงต่อการถูกเปิดเผยได้จนน่ากังวล**

โดยปัจจุบันนี้มีเว็บไซต์ค้นหาที่สามารถค้นหาจากรูปภาพเพียงอย่างเดียว เช่น Google Images Search ซึ่งสามารถค้นหาเว็บไซต์ที่แสดงรูปภาพเหมือนกับภาพต้นฉบับได้ หลายครั้งที่เราโพสต์อัลบั้มรูปโดยไม่มีข้อความอื่นใดเพื่อแชร์รูปกับเพื่อน แม้เว็บค้นหาทั่วไปจะไม่แสดงผลในเว็บเหล่านั้น แต่สำหรับ Google Images Search ก็ยังสามารถค้นหารูปภาพเหมือนกับภาพต้นฉบับได้ และถ้าหากมีใครนำรูปของเราไปใส่ไว้ในเว็บไซต์ต่างๆ เมื่อมีผู้ไม่ประสงค์ดีมาค้นเจอภาพของเรา ความล้ำสมัยของเว็บไซต์เหล่านี้ก็อาจเป็นดาบสองคม ที่ทำให้ผู้ไม่ประสงค์ดีมาสะกดรอยเราได้

แต่หากเราอยากทราบว่า ในเว็บค้นหาของ Google จะมีการเก็บคำค้นหาทุกคำที่ผู้ใช้บริการอย่างเราเคยค้นหาเอาไว้หรือไม่ ในที่นี้เราสามารถเรียกดูประวัติการค้นหาของตนเองได้ด้วยเช่นเดียวกัน จากบริการที่เรียกว่า Google Search History ที่เว็บไซต์ https://www.google.com/history ซึ่งข้อมูลเหล่านี้หากหลุดลอดออกไป อาจจะนำไปสู่การละเมิดความเป็นส่วนตัวของเราก็ได้นะครับ

https://www.google.com/history

ปกป้องข้อมูลส่วนตัวของเรากันเถอะ

หากเพื่อนๆ กำลังกังวลเรื่องความเป็นส่วนตัวของเรากับเว็บไซต์ค้นหา ในบทนี้พุดน้อยมีวิธีการป้องกันที่จะช่วยไม่ให้ข้อมูลส่วนตัวรั่วไหลไปกับเว็บไซต์ค้นหา ซึ่งวิธีป้องกันดังกล่าวนี้จำเป็นต้องใช้ความรู้ทางด้านเทคนิคในระดับหนึ่ง ดังนี้

1. ไม่วางลิงก์ในเว็บไซต์สาธารณะ : หากมีการวางลิงก์ในเว็บไซต์สาธารณะ เมื่อมีผู้มาใช้เว็บไซต์เหล่านั้น ก็จะสามารถเข้าถึงลิงก์ของเราได้ ซึ่งรวมถึงเว็บไซต์ค้นหาด้วยเช่นกัน

2. ตั้งรหัสผ่านเข้าถึงข้อมูล : ในหลายเว็บไซต์จะมีบริการจากบล็อก ซึ่งบางทีจะเปิดให้เราสามารถตั้งรหัสผ่านกับโพสต์ต่างๆ ได้ และเพื่อจำกัดกลุ่มผู้ใช้งาน การตั้งรหัสในลักษณะนี้จะสามารถป้องกันการสืบค้นจากเว็บไซต์ค้นหาอย่างได้มีประสิทธิภาพ

3. ใช้บริการแจ้งเตือนข้อมูลใหม่ของ Google : สำหรับ Google นั้น มีบริการที่เรียกว่า Google Alerts (http://www.google.com/alerts) ซึ่งบริการนี้มีไว้สำหรับใช้แจ้งเตือนเมื่อมีเว็บไซต์ใหม่ๆ ที่มีข้อความตรงกับที่ผู้ใช้บริการกำหนดไว้เข้ามาในระบบของ Google โดยผู้ใช้บริการอาจใช้บริการดังกล่าวเพื่อตรวจสอบข้อมูลชื่อของเราได้ทันทีที่มีชื่อของเราปรากฏขึ้นมาในเว็บไซต์ใดๆ ที่ Google ไปค้นพบ และ Google จะทำการแจ้งเตือนหากข้อมูลที่พบนั้นมีการล่วงละเมิดความเป็นส่วนตัวของเรา ซึ่งเราก็สามารถแจ้งไปยังผู้ดูแลเว็บไซต์ดังกล่าวให้นำข้อมูลของเราออกได้อย่างทันท่วงที

http://www.google.com/alerts

น้องพุดดิ้งชวนรู้

พุดดิ้งเชื่อว่า การจัดการกับเว็บไซต์ค้นหาเพื่อไม่ให้แสดงข้อมูลส่วนตัวของเรานั้น ยังเป็นเพียงการแก้ไขที่ปลายเหตุ ทั้งนี้เพราะการเผยแพร่ข้อมูลบุคคลของประเทศไทยในปัจจุบันยังไม่มีการจัดระเบียบ หรือมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจนสักเท่าไหร่นัก ดังนั้นผู้ใช้อินเทอร์เน็ตอย่างเราจึงต้องระมัดระวังการใช้จากตนเองด้วยนะคะ

1.5 เข้าเว็บไซต์ไหนก็ไม่ทิ้งประวัติให้ตามติดการใช้งาน

การที่ครอบครัวของพุดน้อยเป็นครอบครัวไซเบอร์ จึงทำให้ทุกคนในบ้านต่างชื่นชอบที่จะค้นหาความรู้ใหม่ๆ เกี่ยวกับไอทีมาแชร์ข้อมูลกันอยู่เสมอ หนึ่งในนั้น คือ คุณแม่ของพุดน้อย ที่ครั้งนี้ได้ฝากข้อมูลดีๆ เกี่ยวกับ IPV6 และหมายเลขไอพี (IP Address) ผ่านพุดน้อยเพื่อมาเล่าให้เพื่อนๆ ได้ศึกษากัน

เพื่อนๆ รู้หรือไม่ว่า กลไกสำคัญในการทำงานของอินเทอร์เน็ตที่เรียกว่า IPV6 นั้น (ย่อมาจาก Internet Protocol Version 6) เปรียบเสมือนการใช้งานโทรศัพท์ในการติดต่อสื่อสารกัน ที่จะต้องมีเลขหมายเบอร์โทรศัพท์เพื่อให้อ้างอิงถึงผู้รับสายได้ เรียกว่า “หมายเลขไอพี” (IP Address) ซึ่งเป็นตัวเลขที่บ่งบอกตัวตนของเราในการเข้าใช้อินเทอร์เน็ต และเพื่อใช้เป็นหมายเลขอ้างอิงจากเครื่องคอมพิวเตอร์ในการเชื่อมต่อเว็บไซต์ต่างๆ โดยผู้ให้บริการแต่ละรายจะได้หมายเลขไอพีมาจำนวนจำกัด

โดยหมายเลขไอพีของผู้ให้บริการนั้น ส่วนใหญ่มักจะแจกจ่ายตามการใช้งานจริงของผู้ใช้บริการ อย่างเช่น เมื่อเราเปิดเครื่องคอมพิวเตอร์ เราก็จะได้รับหมายเลขไอพีจากผู้ให้บริการอินเทอร์เน็ต และเมื่อเราปิดเครื่องคอมพิวเตอร์ ผู้ให้บริการก็จะนำหมายเลขไอพีนั้นไปเก็บไว้ เพื่อนำไปแจกจ่ายให้กับผู้ใช้รายอื่นที่เปิดเครื่องใช้บริการครั้งใหม่ต่อไป

ทั้งนี้ ความจำเป็นของผู้ให้บริการที่ต้องแจกจ่ายหมายเลขไอพีให้กับเราก็เพื่อที่จะทำให้ผู้ให้บริการสามารถย้อนรอยในการตรวจสอบ หรือสืบค้นข้อมูลได้ว่า ลูกค้าที่มาใช้บริการอินเทอร์เน็ตนั้นใช้อินเทอร์เน็ตเพื่อทำสิ่งใดบ้าง ทั้งนี้เมื่อเวลาที่เกิดอาชญากรรม หรือการละเมิดอื่นใดเกิดขึ้น ในทางกฎหมายตาม พ.ร.บ. คอมพิวเตอร์ฯ ผู้ให้บริการจะสามารถสืบค้นย้อนรอยตัวบุคคล เพื่อหาผู้กระทำความผิดมาลงโทษได้ ดังจะเห็นได้ว่า การแจกจ่ายหมายเลขไอพีของผู้ให้บริการนั้น มีความสำคัญและจำเป็นสำหรับการใช้เชื่อมต่ออินเทอร์เน็ตเป็นอย่างมาก

หมายเลขไอพี แจกจ่ายหลายบ้าน เสี่ยงทำผิดกฎหมายไม่รู้ตัว

ในหมายเลขไอพีที่ผู้ให้บริการแจกจ่ายมาให้นั้น เพื่อนๆ ใช้เพียงหนึ่งหมายเลขต่อชื่อลูกค้าหนึ่งคนนั้น ในความเป็นจริงแล้ว ในแต่ละหมายเลขสามารถใช้งานร่วมกันโดยผู้ใช้หลายคนในบ้าน หรือแชร์อินเทอร์เน็ตผ่านโทรศัพท์มือถือ ที่สามารถกระจายสัญญาณ WiFi ได้

พุดน้อยขอเตือนไว้สักนิดหนึ่งว่า อุปกรณ์เหล่านี้มักจะไม่มีระบบจัดการเก็บข้อมูลการใช้งานที่สมบูรณ์แบบแต่อย่างใด เนื่องจากไม่สามารถแยกแยะการใช้งานของผู้ใช้อินเทอร์เน็ตแต่ละคนออกจากกันได้ อย่างเช่นในกรณีที่เราเชื่อมต่ออินเทอร์เน็ตในบ้านพักอาศัย ซึ่งอาจจะมีการเชื่อมต่ออินเทอร์เน็ตร่วมกันหลายคน ในกรณีนี้ การเชื่อมต่อจากเครื่องคอมพิวเตอร์หลายเครื่อง หากมีผู้ใช้บริการในบ้านคนใดโพสต์ข้อความหรือรูปภาพผิดกฎหมาย ก็มีส่วนทำให้ผู้สืบค้นจะสามารถสืบค้นข้อมูลย้อนกลับมาที่หมายเลขไอพีของบ้านได้ แต่ผู้ทำการสืบค้นจะไม่สามารถสืบค้นได้เลยว่าข้อความหรือรูปภาพที่ผิดกฎหมายนั้นๆ ออกจากคอมพิวเตอร์เครื่องใดว่าเป็นเครื่องที่โพสต์จริง

พูดน้อยยังทราบจากคุณแม่อีกว่า เมื่อเราเข้าไปที่หน้าเว็บไซต์ต่างๆ เว็บไซต์เหล่านั้นจะสามารถเก็บข้อมูลการใช้บริการไว้จำนวนหนึ่งเพื่อเป็นหลักฐานในกรณีที่มีเจ้าหน้าที่เรียกดูข้อมูลตามกฎหมายในแต่ละประเทศ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดกับคอมพิวเตอร์ของไทย หรืออาจจะเก็บเกินกว่าที่กฎหมายกำหนด เพื่อตรวจสอบสถิติและพฤติกรรมการใช้งาน โดยทั่วไปแล้วการเก็บข้อมูลตามกฎหมายนั้นมักจะระบุเพียงว่าต้องเก็บหมายเลขไอพีของผู้ที่เข้ามาโพสต์ข้อความ หรือเข้ามาดูข้อความนั้นๆ เพื่อให้ตำรวจสามารถตรวจสอบกลับมายังตัวบุคคลผู้โพสต์ข้อความเหล่านั้นได้สะดวก และอย่างที่พวกเราก็รู้ดีกันอยู่ว่าเว็บไซต์ต่างๆ เหล่านี้จะเก็บล็อกไฟล์ของเว็บเซิร์ฟเวอร์เอาไว้อยู่แล้ว ซึ่งข้อมูลที่จะเก็บนั้นจะเป็นข้อมูลจำพวกยูอาร์แอล จากหมายเลขไอพีที่เราใช้ และบันทึกเวลาที่เราเข้าดู เป็นต้น

พระราชบัญญัติว่าด้วย
การกระทำความผิดกับคอมพิวเตอร์

การติดตามการ Login ด้วย Cookie

แต่ที่น่าสนใจยิ่งไปกว่านั้นก็คือ ถึงแม้เราจะใช้งานจากหมายเลขไอพีที่แตกต่างกัน หรือเปลี่ยนเครื่องใช้งานก็ตามที ผู้ดูแลเว็บไซต์ก็ยังสามารถติดตามการ Login ของผู้ใช้บริการได้ตลอด ด้วยข้อมูลชุดหนึ่งซึ่งเรียกว่าคุกกี้ (Cookie) นั่นเอง

คุกกี้คือ ชุดข้อมูลที่ถูกสร้างขึ้นจาก Web Server ซึ่งผู้ดูแลเว็บไซต์จะใช้ติดตามผู้ใช้งานที่ Login เข้ามาในเว็บไซต์ว่าเป็นเบราว์เซอร์เดียวกันบนเครื่องคอมพิวเตอร์เครื่องเดียวกันหรือไม่ ถึงแม้ว่าจะมีการปกปิดหมายเลขไอพีด้วยกระบวนการต่างๆ ก็ตาม แต่หากมองมุมกลับกันการที่เรามีคุกกี้ ถือว่ามีประโยชน์อย่างมากหากเรานำมาใช้ติดตั้งไว้ในเครื่องคอมพิวเตอร์ เพราะเมื่อมีผู้เข้ามาในระบบเว็บไซต์ที่เราดูแลอยู่ เราก็สามารถตรวจจับข้อมูลจากผู้ที่ Login เข้ามาได้ด้วยเช่นกัน

ข้อมูลส่วนตัวกับผู้ให้บริการเว็บ

รู้ไหมว่าเมื่อใดก็ตามที่เรากดปุ่มถูกใจลงในเว็บไซต์โซเชียลมีเดีย หรือโปรแกรมต่างๆ ที่อยู่ในโลกออนไลน์ สิ่งนี้จะเป็นสาเหตุที่ทำให้เราถูกติดตามและถูกวิเคราะห์พฤติกรรมการใช้งานจากข้อมูลที่เรากดถูกใจได้

4 เคล็ดลับใช้ปกปิดข้อมูลส่วนตัว

แม้ข้อมูลส่วนมากที่เกี่ยวข้องกับความเป็นส่วนตัวของเรา ที่เว็บไซต์ต่างๆ ได้ใช้เก็บเป็นข้อมูลเพื่อใช้สร้างสถิติ แต่หากเราไม่ต้องการให้เว็บไซต์ใดๆ เก็บข้อมูลหรือติดตามการใช้งานของเราโดยไม่จำเป็น การปกปิดข้อมูลเหล่านี้สามารถทำได้ดังนี้

1. ปกปิดหมายเลขไอพีที่ใช้งาน : โดยอาศัยบริการ VPN หรือ Tor เพื่อส่งข้อมูลผ่านเครื่องมืออื่นๆ ทำให้เว็บไซต์ใดๆ ไม่สามารถติดตามการใช้งานด้วยหมายเลขไอพีได้

2. ตั้งค่าความเป็นส่วนตัว : เบราว์เซอร์ส่วนมากสามารถตั้งค่าให้งดส่งข้อมูลเว็บไซต์ที่อ้างอิงถึง หรือปิดการทำงานของ Cookie เมื่อมีเรามีความรู้สึกไม่ไว้ใจในเว็บไซต์นั้นๆ

3. ใช้งานโหมดท่องเว็บไซต์แบบส่วนตัว : เบราว์เซอร์ส่วนมากจะมีระบบท่องเว็บไซต์แบบส่วนตัว (Private Browing) มาในตัว ซึ่งระบบดังกล่าวมีความน่าสนใจอยู่อย่างหนึ่ง คือ ข้อมูลคุกกี้ที่ใช้งานในโหมดปกติจะแยกออกจากโหมดส่วนตัว ทำให้เว็บไซต์ต่างๆ ติดตามพฤติกรรมการใช้งานของเราได้ยากขึ้น รวมทั้งข้อมูลต่างๆ เช่น ประวัติการท่องเว็บไซต์ทั้งหมดก็จะถูกลบออกไปหลังจากปิดหน้าต่างที่ทำงานโหมดส่วนตัวแล้ว

4. เลี่ยงคลิกลิงก์ที่ไม่พึงประสงค์โดยตรง : ทราบหรือไม่ว่าลิงก์ที่ส่งมาถึงเราโดยตรงผ่านช่องทางต่างๆ เช่น ลิงก์เว็บไซต์แปลกๆ ที่ส่งมาทางอีเมลของเราโดยไม่มีเหตุผล หรือลิงก์ที่ถูกส่งมาในระบบข้อความส่วนตัวโดยไม่มีเนื้อหาอื่นๆ หากเลี่ยงได้ก็จะช่วยสร้างความมั่นคงปลอดภัยให้กับข้อมูลส่วนตัวของเราได้เป็นอย่างดี

น้องพุดดิ้งชวนรู้

ก่อนจะจบบทนี้ไป พุดดิ้งขอเป็นตัวแทนของพุดน้อยอยากจะขอเตือนเพื่อนๆ ให้ควรระมัดระวังและตั้งข้อสงสัยก่อนการคลิกลิงก์ที่ส่งมาถึงเราอยู่เสมอ เช่น ลิงก์ ที่อาจจะส่งมาทางอีเมลโดยไม่มีเหตุผล ซึ่งเอาเข้าจริงวิธีการปกป้องข้อมูลดังกล่าว อาจจะเป็นวิธีที่ดีที่สุดก็ได้นะคะ

บทที่ 2

อินเตอร์เน็ต
ใช้อย่างไร
ให้มั่นคงปลอดภัย

2.1 รู้ทันภัยไซเบอร์

คุณลุงของพุดน้อย เคยเล่าให้ฟังว่า หลายสิบปีก่อนในช่วงที่เทคโนโลยียังล้าสมัย คนเราจะส่งข้อมูลถึงกันโดยใช้โทรเลข แต่เมื่อโลกเข้าสู่ยุคออนไลน์ ผู้ใช้บริการหลายร้อยล้านคนจึงต่างค่อยๆ หันมาใช้ e-Mail เป็นตัวส่งผ่านข้อมูลแทน

ด้วยเหตุนี้พุดน้อยเชื่อว่า ในยุคสมัยนี้ที่อินเทอร์เน็ตมีความเร็วเพียงแค่ปลายนิ้วคลิก e-Mail จึงจัดเป็นสิ่งจำเป็นที่เข้ามามีบทบาทในชีวิตประจำวันของเพื่อนๆ หลายคน ซึ่งแทบจะเรียกได้ว่าตัดกันไม่ขาดเลยก็ว่าได้ ไม่ว่าจะเป็นการใช้ส่งข้อมูลรายงาน เพื่อความบันเทิง หรือการใช้บริการผ่านเว็บไซต์บนอินเทอร์เน็ต ซึ่งก็ล้วนแต่ต้องใช้ e-Mail ในการเชื่อมโยงด้วยกันทั้งสิ้น e-Mail จึงถือเป็นสิ่งสำคัญอย่างยิ่งที่เราต้องใส่ใจดูแลเป็นพิเศษ เพราะถ้าพาสเวิร์ดหลุดไปอยู่ในมือผู้อื่นแล้ว ก็เหมือนกับได้ให้กุญแจเขาเข้าไปไขประตูบ้านเราเลยเชียวนะ

ด้วยความที่มีผู้ใช้จำนวนมาก จึงทำให้มีบรรดาวายร้ายไซเบอร์มากมายต่างคิดจะเข้ามาทำทุกวิถีทางเพื่อที่จะขโมยข้อมูลความเป็นส่วนตัวของเราไป โดยพุดน้อยสามารถสรุปข้อมูลภัยคุกคามทางอินเทอร์เน็ตที่ผู้ใช้บริการควรระวังได้ 4 หัวข้อดังนี้

1. ภัยจากสปายแวร์ (Spyware) เป็นไวรัสคอมพิวเตอร์ ที่โปรแกรมป้องกันไวรัสส่วนใหญ่มักมองไม่เห็น ซึ่งบรรดาวายร้ายไซเบอร์จะใช้วิธีการติดตั้งสปายแวร์บนคอมพิวเตอร์ของตนและดักเก็บข้อมูลของผู้ใช้บริการผ่านการท่องเว็บไซต์ โดยใช้วิธีการอ่าน Keylogger หรือการจดจำตัวอักษรที่เราคีย์ลงบน Keyboard และดักข้อมูล Username และ Password อันเป็นสาเหตุของปัญหาการถูกลักลอบโอนเงินจากธนาคารที่เราใช้บริการไปแบบที่เราไม่ทันรู้ตัว ซ้ำยังมีผลทำให้ความเร็วในการเชื่อมต่ออินเทอร์เน็ตช้าลงอีกด้วย

2. ภัยจาก Spam E-mail จัดเป็นภัยคุกคามที่เกิดจากการส่งผ่านอีเมลขยะออนไลน์ ที่ตั้งใจส่งตรงถึงผู้รับในลักษณะของการโฆษณาสินค้าและบริการผ่านการส่งลิงก์ชักชวนให้เข้าไปใช้บริการในเว็บไซต์ต่างๆ ซึ่งหากเราพลั้งเผลอเข้าไปกดลิงก์ดังกล่าว ก็อาจจะถูกทำการดักฟิชชิ่ง (Phishing) เพื่อขโมยข้อมูลส่วนตัวของเราไป

3. ภัยจาก DoS/DDoS เป็นการโจมตีเพื่อทำให้เครื่องคอมพิวเตอร์ของผู้เสียหายหยุดทำงานโดยตรง โดยแบ่งได้เป็น 2 ลักษณะ คือ การโจมตีแบบเครื่องเดียว หรือ Denial of Service (DoS) และการโจมตีแบบเป็นทีมพร้อมๆ กัน หรือ Distributed Denial of Service (DDoS)

4. ภัยจาก Hacker จัดเป็นต้นตอของวายร้ายทั้งปวง ที่จะใช้วิธีการแฮกข้อมูลโดยอาศัยเว็บไซต์ค้นหา เช่น www.google.com และ www.yahoo.com เสาะหาเว็บไซต์ที่ไม่มีการเข้ารหัสหรือมีการป้องกันที่หละหลวมและทำการลักข้อมูลแบบไม่เลือกเหยื่อ

5 แนวทางรับมือภัยคุกคามไซเบอร์

- **เลือกใช้โปรแกรม On-Screen Keyboard** : เป็นโปรแกรมคีย์บอร์ดเสมือนจริง โดยใช้เม้าส์คลิกป้อนข้อมูลบนหน้าจอคอมพิวเตอร์แทนการกดปุ่มคีย์บอร์ด ซึ่งวิธีนี้จะสามารถใช้หลีกเลี่ยงภัยจากการดักเก็บข้อมูลแบบ Keylogger ได้เป็นอย่างดี

- **ใช้การเข้ารหัสแบบ https** : การเข้ารหัสด้วยวิธีนี้จะเป็นตัวช่วยสร้างความมั่นคงปลอดภัยให้กับเรา หลีกเลี่ยงจากการถูก Hacker มาดักขโมยข้อมูลไป

- **เลือกเว็บไซต์ที่มีการใช้ SSL Certificates** : ซึ่งเป็นเครื่องหมายรับรองความปลอดภัยทางอิเล็กทรอนิกส์ ที่ออกโดย CA (Certificate Authority) และจัดเป็นวิธีที่สร้างความมั่นคงปลอดภัยที่ดีที่สุดวิธีหนึ่ง ที่พุดน้อยต้องการย้ำให้เพื่อนๆ นำไปปฏิบัติกัน

- **คอยอัพเดตระบบปฏิบัติการบนเครื่องคอมพิวเตอร์** หรืออุปกรณ์อื่นๆ ที่จะใช้เชื่อมต่อกับอินเทอร์เน็ต

- **ติดตั้งโปรแกรมป้องกันไวรัส**และคอยอัพเดตอยู่เสมอ

อ๊ะ! เพื่อนๆ อย่าเพิ่งตกใจ วิธีป้องกันภัยคุกคามไซเบอร์ยังไม่หมดเท่านี้ เพราะนอกจาก 5 วิธีข้างต้นแล้ว คุณลุงของพุดน้อยยังแอบกระซิบถึงวิธีป้องกันภัยในรูปแบบอื่นๆ มาให้ศึกษากันอีกหลายวิธี ซึ่งอาจต้องใช้พื้นที่อธิบายกันสักนิด พุดน้อยจึงต้องมาเปิดหัวข้อเพื่อให้เพื่อนๆ ได้ศึกษากันได้อย่างไม่สับสน นั่นก็คือ วิธีการเลือกใช้ POP, IMAP หรือ SMTP ที่ปัจจุบันมีผู้นิยมใช้บริการกันมาก ซึ่งพุดน้อยกล้ารับประกันเลยว่าจะสามารถสร้างความมั่นคงปลอดภัยให้กับเพื่อนๆ ได้เป็นอย่างดีแน่นอน

เลือกใช้ POP, IMAP หรือ SMTP

สำหรับเพื่อนๆ ที่สงสัยว่าโปรโตคอลเหล่านี้คืออะไร แล้วมีวิธีเลือกใช้อย่างไร เพื่อให้เหมาะสมกับการทำงานของเรา สามารถศึกษาคุณสมบัติและความหมายได้ตามเนื้อหาต่อไปนี้เลยครับ

- POP (Post Office Protocol) เป็นโปรโตคอลที่ใช้ในการรับและอ่าน E-mail แบบออฟไลน์ ซึ่งจะถูกเก็บเอาไว้ในเซิร์ฟเวอร์ และเมื่อเพื่อนๆ ใช้โปรแกรมในการอ่าน ระบบจะทำการดาวน์โหลด E-mail มาเก็บไว้ในเครื่อง ทำให้สามารถนำกลับมาอ่านซ้ำในภายหลัง และแม้จะอ่านแล้วแต่เผลอลบไปก็ยังสามารถเข้าไปตรวจสอบในเซิร์ฟเวอร์ใหม่ได้อีกครั้งด้วย

- IMAP (Instant Message Access Protocol) เป็นโปรโตคอลที่ใช้ในการติดต่อข้อมูลจาก E-mail เช่นเดียวกัน แต่ว่าจะต่างจาก POP ตรงที่ IMAP จะรองรับการอ่าน E-mail ได้ทั้งแบบออนไลน์และออฟไลน์

- SMTP (Simple Mail Transfer Protocol) เป็นโปรโตคอลที่ใช้ในการส่ง E-mail บนเครือข่ายอินเทอร์เน็ต ที่สามารถส่งผ่านข้อมูลไปได้ทั่วโลก แต่ทั้งนี้กลับนิยมกันมากในการนำไปใช้เพื่อรับส่งข้อมูลถึงกันภายในองค์กร

ไม่ยากอย่างที่คิด! การตั้งค่า POP/IMAP ใน www.gmail.com

- Sign In เข้า www.gmail.com
- คลิกที่ไอคอนรูปฟันเฟืองด้านขวาบน แล้วเลือกเมนู Setting
- เลือกหัวข้อ การส่งต่อ POP/IMAP
- เลือกสถานะว่าจะใช้ POP และ IMAP และบันทึกการเปลี่ยนแปลง

นอกจากนี้สำหรับผู้ที่ใช้บริการ Gmail ในระบบยังมีรูปแบบการยืนยันตัวตนที่เรียกว่า การยืนยันแบบ 2-Step Verification ซึ่งเป็นรูปแบบที่จะช่วยเพิ่มความมั่นคงปลอดภัยจากการถูกแฮก โดยต้องใช้ข้อมูล 2 ใน 3 ส่วนร่วมกัน ได้แก่

1. รหัสผ่าน
2. โทรศัพท์มือถือหรือรหัสบัตรเติมเงิน
3. ลายนิ้วมือหรือม่านตา

การยืนยันด้วยสิ่งต่างๆ เหล่านี้ พูดน้อยอยากจะอธิบายให้เข้าใจกันง่ายๆ ว่า รหัสผ่านนั้นเป็นสิ่งที่คาดเดาได้เสมอ เช่นเดียวกับเบอร์โทรศัพท์มือถือของเรา ดังนั้นเราจึงต้องมีการตั้งตรวจสอบการยืนยันเพิ่มขึ้นอีกชั้นหนึ่ง เพื่อให้เกิดความมั่นคงปลอดภัยมากขึ้น เช่น การเพิ่มรหัสการสแกนลายนิ้วมือหรือม่านตา ที่เป็นเอกลักษณ์เฉพาะบุคคล ยากที่จะลักลอบนำมาใช้ ซึ่งระบบต่างๆ เหล่านี้ ก็เริ่มมีใช้กันไปบ้างแล้วในอุปกรณ์เทคโนโลยีรุ่นใหม่อย่างโน้ตบุ๊ก เป็นต้น

น้องพุดดิ้งชวนรู้

หมั่นตรวจเช็กข้อมูล e-Mail เพื่อความมั่นคงปลอดภัย

ว้าว! ข้อมูลที่พุดน้อยนำมาให้เพื่อนๆ ได้ศึกษากัน ต้องบอกว่าครบถ้วนเลยทีเดียว ไม่ว่าจะเป็นข้อมูลในเรื่องของภัยไซเบอร์ในรูปแบบต่างๆ และวิธีการป้องกันภัยเบื้องต้น ซึ่งพุดดิ้งก็ของเสริมสักนิดสำหรับเพื่อนๆ ที่มี e-Mail ส่วนตัวใช้ ให้ควรหมั่นหาเวลาว่างเปิด e-Mail เพื่อเช็กข้อมูลอัพเดตกันบ่อยๆ เพื่อที่จะได้รู้ว่ามีใครแอบเข้ามาลักลอบใช้ e-Mail ส่วนตัวของเราหรือเปล่า หรืออย่างน้อยหากเกิดปัญหาขึ้น ก็จะสามารถแก้ไขปัญหาได้ทันการ

พุดดิ้งก็มีวิธีการสังเกตง่ายๆ เพียงแค่ Sign In เข้าไปใน e-Mail ที่ใช้อยู่ แล้วคลิกที่หัวข้อ “กิจกรรมล่าสุดของบัญชี” แล้วเลือกคลิกต่อที่หัวข้อ **“รายละเอียด”** ภายในนั้นจะบอกถึงช่วงเวลา และข้อมูลที่ถูกส่งเข้า-ออกจาก e-Mail ของเรา นอกจากนี้ยังสามารถตรวจเช็กได้ว่ามีผู้ลักลอบใช้บริการผ่านระบบเบราว์เซอร์บนคอมพิวเตอร์หรือผ่านระบบโทรศัพท์มือถือเราหรือเปล่า ซึ่งหากตรวจพบให้รีบเปลี่ยน Password ในการ Sign In ใหม่ เพียงเท่านี้ก็ตัดปัญหาถูกรบกวนโดยผู้อื่นได้แล้ว ง่ายไหมคะ

2.2 Anti Virus ขาดไม่ได้

วันนี้คอมพิวเตอร์ของพุดน้อยออกอาการแปลกๆ อยู่ๆ ก็มีเครื่องหมายเตือนขึ้นมาบนหน้าจอเต็มเลย เมื่อคุณพ่อมาช่วยดูให้ ท่านจึงบอกกับพุดน้อยว่าสงสัยคอมพิวเตอร์จะติดไวรัส ซึ่ง**ไวรัสคอมพิวเตอร์**เหล่านี้ต่างถูกสร้างขึ้นมาเพื่อสร้างความเสียหายแก่คอมพิวเตอร์ของเรา ทั้งนี้คุณพ่อยังบอกอีกว่าในฐานะที่พุดน้อยเป็นผู้ที่ใช้อินเทอร์เน็ตคนหนึ่ง ควรจะมีความรู้เรื่องวิธีป้องกันไวรัสเอาไว้บ้าง และที่สำคัญควรมีความรู้ในเรื่องความร้ายกาจของไวรัสคอมพิวเตอร์แต่ละชนิดด้วย

ไวรัสคอมพิวเตอร์ วายร้ายพันธุ์ดิจิทัล

คุณพ่ออธิบายให้พุดน้อยเข้าใจว่า ไวรัสคอมพิวเตอร์ก็เหมือนกับไวรัสที่ติดต่อบนร่างกายของมนุษย์เรา ซึ่งจะหนักหรือเบาขึ้นอยู่กับวิธีโจมตีของไวรัสแต่ละแบบ แต่ท้ายที่สุดแล้วต่างก็มีผลเสียต่อคอมพิวเตอร์ของเราทั้งสิ้น ไม่เพียงเท่านี้ไวรัสบางชนิดยังชอบขโมยข้อมูลสำคัญของเราไปอีกด้วย และเพื่อให้รู้เท่าทันไวรัสเหล่านี้ พุดน้อยขออาสานำความรู้เรื่องไวรัสคอมพิวเตอร์แต่ละชนิดจากคุณพ่อ มาให้เพื่อนๆ ได้ศึกษากัน

☑ มาโคร ไวรัส (Macro Virus) เป็นไวรัสที่ผู้ใช้คอมพิวเตอร์เจอกันบ่อยๆ มักติดมากับไฟล์เอกสารต่างๆ ทั้งไฟล์ Word หรือไฟล์ PDF ที่คุ้นเคยกันดี โดยวิธีการโจมตีของไวรัสชนิดนี้ จะมีตั้งแต่การรบกวนบนหน้าจอคอมพิวเตอร์ ไปจนถึงการลบข้อมูลบางอย่างภายในเครื่องคอมพิวเตอร์ของเรา

☑ เวิร์ม (Worm) หรือตัวหนอนอินเทอร์เน็ต ซึ่งลักษณะการแพร่กระจายคล้ายตัวหนอนชอนไชไปยังเครื่องคอมพิวเตอร์ต่างๆ ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง และยังทำให้ไม่สามารถเชื่อมต่อกับระบบอินเทอร์เน็ตได้ จึงนับเป็นตัวก่อกวนที่เราต้องระวังเป็นพิเศษนะครับ

☑ มัลแวร์ (Malware) เป็นไวรัสที่มุ่งร้ายต่อซอฟต์แวร์ที่เพื่อนๆ ใช้โดยตรง ลักษณะเป็นการโจมตีทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล จัดเป็นสายพันธุ์ของไวรัสที่ต้องระวังให้มากเช่นกัน

☑ ฟิชชิ่ง (Phishing) ไม่ใช่เป็นการตกปลานะครับ แต่เป็นไวรัสที่มักจะหลอกลวงผู้ใช้ ซึ่งอาจมาในรูปแบบ e-Mail แจ้งข่าว หรือสร้างหน้าเว็บปลอมหลอกให้เราเข้าไปใช้บริการ เพื่อขโมยข้อมูลส่วนตัวของเพื่อนๆ ไป

☑ สปายแวร์ (Spyware) ไวรัสตัวนี้ก็น่ากลัว เพราะจัดเป็นนักสอดแนมที่ชอบเข้ามาล้วงข้อมูลสำคัญและเก็บพฤติกรรมการใช้งานของเพื่อนๆ ไม่ว่าจะเป็นชื่อ นามสกุล รหัส Login และ Password บางทีก็เข้ามาสำรวจไฟล์ต่างๆ ภายในเครื่อง เพื่อรอโอกาสส่งกลับไปยังต้นทางนั่นเอง

ไวรัส 3M ผู้หวังร้ายพร้อมบุกคนออนไลน์

นอกจากไวรัส 5 ชนิดที่พูดน้อยอธิบายไว้ในหัวข้อก่อนหน้านี้แล้ว ยังมีไวรัสคอมพิวเตอร์อีกกลุ่มหนึ่ง ซึ่งบอกไว้เลยว่าน่ากลัวเป็นพิเศษ ชนิดที่ถ้าปล่อยทิ้งไว้จะยิ่งทวีความรุนแรงในการโจมตีคอมพิวเตอร์ของเรามากขึ้นทุกขณะ ทั้งจากการแชตและการท่องเว็บไซต์ เรียกว่า ไวรัส 3M ได้แก่ Man-in-the-Middle, Man-in-the-Browser และ Man-in-the-Mailbox

☑ Man-in-the-Middle (MitM) ไวรัสวายร้ายน้องสุดท้องที่คอยดักจับข้อมูลจากผู้ใช้บริการ เช่น Username และ Password รวมถึงการตั้งหน้าเว็บไซต์ลวงผ่าน e-Mail ที่ต่างก็น่ากลัวทั้งสิ้น

☑ Man-in-the-Browser (MitB) ไวรัสวายร้ายตัวรอง ที่เน้นการโจมตีที่ฝังอยู่ในเว็บเบราว์เซอร์ ไม่ว่าจะเป็นการขโมยข้อมูลทางการเงิน การทำธุรกรรมธนาคาร ด้วยวิธีการลวง เช่น การสร้างเว็บไซต์ปลอมให้มีหน้าตาคล้ายกับเว็บไซต์ที่เพื่อนๆ ใช้งานกันบ่อยๆ ได้แก่ หน้าเว็บไซต์ของธนาคาร จากนั้นแจ้งส่งข้อมูลลวงให้ผู้ใช้ที่มีฐานข้อมูลสุ่มออกไป ใครที่เจอแบบนี้ หากไม่พิจารณาให้ดี อาจถูกกลลวงเหล่านี้ สร้างความเสียหายกับตนเองและทรัพย์สินได้ในพริบตา

☑ Man-in-the-Mailbox (MitMb) ไวรัสวายร้ายตัวพี่ใหญ่ที่ร้ายกาจที่สุดในตระกูล M ทั้ง 3 เพราะอาศัยแค่การพิมพ์ผิดหรือการส่งข้อมูลแบบไม่ตั้งใจ ก็จะกลายเป็นการนำส่งข้อมูลสำคัญไปให้กับวายร้ายระดับมืออาชีพได้แล้ว เช่น การนำ e-Mail ที่คล้ายกับ e-Mail ของเรา ไปใช้ส่งข้อมูลผิดๆ หรือใส่ร้ายป้ายสีคนอื่นๆ อันนำไปสู่การถูกดำเนินคดีตามกฎหมายตาม พ.ร.บ. คอมพิวเตอร์ก็เป็นไปได้

ได้รู้จักกับชนิดของไวรัสคอมพิวเตอร์ตัวต่างๆ กันไปแล้ว ตอนนี้พุดน้อยจะพาเพื่อนๆ ไปรู้จักกับยารักษาและวิธีการป้องกันไวรัสคอมพิวเตอร์ ในรูปแบบต่างๆ

ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus Software)

โปรแกรมป้องกันไวรัส เป็นโปรแกรมที่สร้างขึ้นโดยมีวัตถุประสงค์เพื่อใช้ป้องกัน และคอยตรวจจับการคุกคามจากไวรัสคอมพิวเตอร์ อาทิ มาโครไวรัส, เวิร์ม, มัลแวร์ หรือแม้แต่ไวรัสตระกูล 3M ซึ่งปัจจุบันโปรแกรมป้องกันไวรัส ถูกแบ่งออกเป็น 2 ประเภทหลักๆ ได้แก่

- แอนตี้ไวรัส (Anti-Virus) เป็นโปรแกรมป้องกันไวรัสทั่วไป ที่ทำหน้าที่ตรวจจับและทำลายไวรัสในคอมพิวเตอร์ของเรา เช่น KASPERSKY, AVG และ Norton เป็นต้น
- แอนตี้สปายแวร์ (Anti-Spyware) เป็นโปรแกรมป้องกันไวรัสที่มาในรูปแบบของการโจรกรรมข้อมูล เช่น Windows Defender และ Microsoft Security Essentials เป็นต้น

กุญแจป้องกันไวรัส 3M ผู้หวังร้าย

สำหรับวิธีการป้องกันไวรัส 3M นั้น ถ้าไม่รู้จักศึกษาวิธีการให้ดีอาจจะสร้างความเสียหายให้กับผู้ใช้บริการอย่างเราได้โดยไม่ทันตั้งตัว ซึ่งวิธีการป้องกันที่ดีที่สุดคือ **สร้างความตระหนักในเรื่องของความมั่นคงปลอดภัยให้กับผู้ใช้** เช่น ตรวจสอบความถูกต้องของใบรับรองของเว็บไซต์ทุกครั้งที่ต้องทำธุรกรรมทางอิเล็กทรอนิกส์ หมั่นปรับปรุงโปรแกรมตรวจจับไวรัสและไม่ติดตั้งโปรแกรมที่น่าสงสัย หรือในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับผ่านทางอีเมล ควรทำการเข้ารหัสลับข้อมูลก่อนที่จะส่งออกไป เท่านี้ก็สามารถป้องกันจากไวรัส 3M ได้ด้วยตนเองแล้ว

เปลี่ยนพฤติกรรมการใช้อินเทอร์เน็ต ลดปัญหาไวรัสคอมพิวเตอร์รบกวน

นอกจากการติดตั้งโปรแกรมป้องกันไวรัส วิธีง่ายๆ ที่ช่วยให้เราห่างไกลจากการรบกวนของไวรัสชนิดต่างๆ ได้ ก็คือ**การปรับเปลี่ยนพฤติกรรมในการรับข้อมูลอย่างระมัดระวังมากขึ้น** หมั่นใส่ใจในคำเตือนที่ปรากฏบนหน้าจออย่างละเอียด และอย่าลืมอัพเดตโปรแกรมป้องกันไวรัสบ่อยๆ เพียงเท่านี้ก็มั่นคงปลอดภัยไปกว่าครึ่งแล้ว

รู้จักกับอินเทอร์เน็ตซีเคียวริตี้ (Internet Security)

อินเทอร์เน็ตซีเคียวริตี้ คือโปรแกรมการเพิ่มความสามารถในการตรวจจับไวรัสที่ทำงานบนการเชื่อมต่ออินเทอร์เน็ตอัตโนมัติ อย่างเช่น ไวรัสสแปมเมล (Spam Mail) โดยที่มีไฟร์วอลล์ (Firewall) เอาไว้สำหรับป้องกันการ Hacker ซึ่งแตกต่างกับโปรแกรมป้องกันไวรัสทั่วไป ที่เราจะต้องทำการหมั่นเชื่อมต่ออินเทอร์เน็ตเพื่ออัพเดตฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอด้วยตนเอง

น้องพุดดิ้งชวนรู้

ไม่ว่าจะเป็นไวรัสสปายแวร์ (Spyware) ฟิชชิ่ง (Phishing) เวิร์ม (Worm) หรือแม้แต่กลุ่มไวรัส 3M ก็ล้วนแล้วแต่มีวัตถุประสงค์ในการถูกสร้างขึ้นมาเพื่อทำลายและขโมยข้อมูลส่วนตัวของเพื่อนๆ ด้วยกันทั้งนั้น แต่ทั้งนี้แม้การจะป้องกันภัยจากไวรัสคอมพิวเตอร์จะไม่สามารถทำได้อย่าง 100% แต่หากเพื่อนๆ มีการเตรียมความพร้อมที่ดี เช่น การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus Software) และเปลี่ยนพฤติกรรมการใช้อินเทอร์เน็ต ก็สามารถลดปัญหาไวรัสคอมพิวเตอร์เข้ามารบกวนสร้างความมั่นคงปลอดภัยให้กับเราได้ระดับหนึ่งแล้ว

2.3 ล้วงลับตับแตกวิธีการลวงผู้ใช้เน็ต

แฮกเกอร์ (Hacker)! พูดน้อยและครอบครัว เอ่ยถึงบุคคลคนนี้มาตั้งแต่บทที่ 1 ซึ่งเท่าที่ผ่านมาเรารู้แต่เพียงว่า แฮกเกอร์นั้นเป็นบุคคลที่จะมาโจรกรรมข้อมูลส่วนตัวของผู้ใช้บริการอินเทอร์เน็ตไปใช้ในทางเสื่อมเสียชื่อเสียงและเสียทรัพย์

แฮกเกอร์ (Hacker) หรือ แครกเกอร์ (Cracker)

ตามความหมายแล้วก็คือ ผู้ร้ายในโลกไซเบอร์ ที่มีความรู้ในด้านระบบและเครือข่ายคอมพิวเตอร์สูง แต่กลับนำความรู้ที่มีไปใช้ในทางที่ผิด ขาดจริยธรรม เช่น ลักลอบเข้าสู่ระบบความเป็นส่วนตัวเพื่อล้วงความลับข่าวสารของผู้อื่น ยิ่งในปัจจุบันเครือข่ายอินเทอร์เน็ตเชื่อมโยงถึงกันทั่วโลก ปัญหาในเรื่องของการโจรกรรมข้อมูลก็ยิ่งมีมากขึ้นหลายรูปแบบ ซึ่งทำให้ผู้ใช้บริการอินเทอร์เน็ตต้องมีความระแวดระวังในการใช้บริการมากขึ้นเป็นพิเศษ

วิธีการของ Hacker

☑ **สนิฟเฟอร์ (Sniffer)** นับเป็นหนึ่งในวิธีการที่ Hacker นิยมใช้กันมาก จัดเป็นโปรแกรมเล็กๆ ที่ถูกออกแบบมาเพื่อดักจับข้อมูลของผู้ใช้บริการอินเทอร์เน็ต

☑ **บอมเมล (Bomb Mail)** เป็นการก่อกวนผู้ใช้บริการอีเมลชนิดหนึ่ง ที่ Hacker จะใช้จดหมายอิเล็กทรอนิกส์ที่เขียนปลอมแปลงขึ้นมา และส่งไปยังปลายทางที่เครื่องเป้าหมาย โดยส่งจดหมายอิเล็กทรอนิกส์เป็นจำนวนมากๆ หลายพันหลายหมื่นฉบับ เพื่อให้อีเมลของผู้ใช้บริการรับไม่ไหว บ้างก็จะใช้วิธีส่งจดหมายอิเล็กทรอนิกส์จากเครื่องหนึ่งไปอีกเครื่องหนึ่งรับส่งต่อๆ กันไปเรื่อยๆ ไม่จบสิ้น และอีเมลหยุดการทำงานในที่สุด

☑ **โทรจัน (Trojan)** เป็นโปรแกรมไวรัสชนิดหนึ่งที่แฝงมาในรูปแบบของจดหมายอิเล็กทรอนิกส์ ซึ่ง Hacker จะใช้วิธีระบุข้อความกล่าวอ้างว่าเป็นโปรแกรมปรับปรุงด้านการรักษาความปลอดภัยซอฟต์แวร์ และเมื่อผู้ใช้บริการเผลอไปกดลิงก์ดังกล่าว ก็จะกลายเป็นถูกโทรจันแฝงเข้ามาโจรกรรมข้อมูลและทำลายระบบในคอมพิวเตอร์ของเราในที่สุด

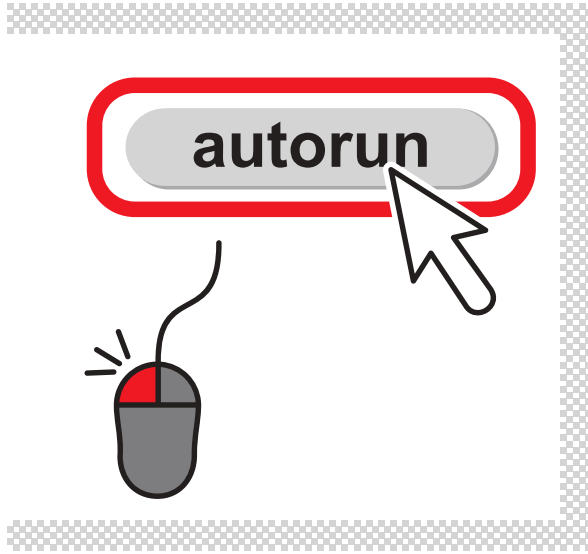
ลดพฤติกรรมความเสี่ยง ป้องกันภัยจาก Hacker

☑ **อ่านให้ละเอียดก่อนติดตั้งโปรแกรม :** เมื่อพูดถึงการติดตั้งโปรแกรมคอมพิวเตอร์ ผู้ใช้ส่วนใหญ่มักจะเข้าใจว่าเป็นการคลิกที่ปุ่ม Next, Next และ Next ต่อไปเรื่อยๆ จนท้ายที่สุด คือ คลิกปุ่ม Finish โดยไม่อ่านข้อตกลงที่ผู้สร้างโปรแกรมระบุไว้ ซึ่งแน่นอนว่าผู้ใช้บริการหลายคนยังไม่ทราบด้วยซ้ำว่าโปรแกรมติดตั้งเสร็จแล้ว พฤติกรรมในลักษณะนี้จะเป็นตัวทำให้ Hacker ลักลอบเข้ามาโจรกรรมข้อมูลของเราได้

☑ **ไม่แอบเล่นอินเทอร์เน็ตไร้สายฟรี :** สำหรับคนที่ใช้งานอินเทอร์เน็ต การที่มีสัญญาณ WiFi ฟรีจากบ้านใครไม่รู้ที่จู่ๆ ก็สแกนเจอ ท้ายสุดแล้วก็ทนความต้องการที่อยากจะได้ของฟรีไม่ได้ ให้เข้าไปใช้งานได้แบบไม่ทันได้ยั้งคิด ซ้ำร้ายก็ไม่พ้นบรรดา Hacker มาขุดบ่อล่อปลา ซึ่งแทนที่จะได้ใช้งาน WiFi ฟรีๆ แต่กลับถูกย้อนรอยด้วยการตักตวงเอาสิ่งสำคัญต่างๆ ไป ไม่ว่าจะเป็นชื่อผู้ใช้ รหัสผ่านหรือข้อมูลจำเป็นต่างๆ ออกไป

☑ **แอนตี้ไวรัสปลอม ของต้องระวัง :** ใครเคยใช้อินเทอร์เน็ตแล้วโดนหลอกให้ดาวน์โหลดไฟล์บ้าง...ยกมือขึ้น เชื่อว่าจริงๆ แล้วเหตุการณ์แบบนี้หลายต่อหลายคนก็น่าจะเคยได้สัมผัส ยิ่งบางคนขวัญอ่อนด้วยแล้ว อยู่ๆ มี Banner หรือ Pop Up เด้งขึ้นมาจากหน้าเว็บไซต์ที่เปิดอยู่ แล้วบอกว่าเวลานี้มีไวรัสกำลังทำงานอยู่บนระบบ หากต้องการใช้โปรแกรมสแกนให้คลิก ก็รีบคลิกในทันที แต่ที่ไหนได้ กลับโดนไวรัสที่แฮกเกอร์ตั้งไว้หลอกเข้ามาติดตั้งในระบบ ทางที่ดีก็ควรตั้งสติก่อนกดดาวน์โหลดนะครับ

☑ **เปิดฟังก์ชัน Autorun ใน Removable Drive :** อีกหนึ่งพฤติกรรมเสี่ยง ที่ผู้ใช้คอมพิวเตอร์ส่วนใหญ่มักทำไปโดยปราศจากการไตร่ตรอง ก็คือการเชื่อมต่ออุปกรณ์ เช่น แฟลชไดรฟ์หรือฮาร์ดดิสก์ จากภายนอกคอมพิวเตอร์แล้วเปิดใช้งาน Autorun ทันที โดยที่ไม่ได้ทำการสแกนไวรัส แต่พุดน้อยอยากให้เพื่อนๆ มองย้อนดูดีๆ เพราะการเสียเวลาสแกนไวรัสเพียงเล็กน้อยจะช่วยลดความเสี่ยงจากการถูกไวรัสโจมตีจนคอมพิวเตอร์อ่อนแอ จน Hacker สามารถเจาะเข้ามาล้วงความลับในคอมพิวเตอร์ของเราได้โดยง่าย



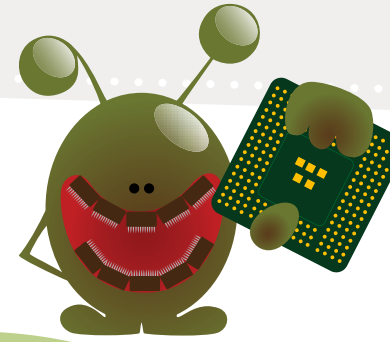
☑ **ไม่อัพเดตโปรแกรมป้องกันไวรัส :** การที่มีแอนตี้ไวรัสแต่ไม่เคยอัพเดต ก็เหมือนมีร่างกายที่แข็งแรง แต่ไม่เคยได้ออกกำลัง กล้ามเนื้อหรือกำลังที่เคยมี ก็เริ่มที่จะหย่อนยานไปตามกาลเวลา แต่ถ้ามีเวลาออกกำลัง หมั่นสร้างกล้ามเนื้อ เหมือนกับการอัพเดตแอนตี้ไวรัส ก็ทำให้ร่างกายเฟิร์มยิ่งขึ้น ดีกว่าจะมาเสียใจเมื่อติดไวรัสในภายหลัง

☑ **ปิดวินโดวส์อัพเดต อาจเกิดเหตุไม่คาดคิด :** การที่เพื่อนๆ ได้ติดตามข่าวสารและอัพเดตข้อมูลรอบตัว ย่อมทำให้ไม่ตกข่าวและทันเหตุการณ์อยู่เสมอ การอัพเดตวินโดวส์ก็เช่นกัน เพราะเป็นการเปิดให้ระบบรับรู้และปิดช่องโหว่จากการคุกคามของผู้ไม่หวังดี แต่อย่าลืมว่า ไม่ว่าเพื่อนๆ จะซื้อวินโดวส์มาติดตั้งหรือเครื่องที่ซื้อติดตั้งวินโดวส์มาด้วยก็ตาม สิ่งที่สำคัญคือ ต้องใช้งานและใช้สิทธิ์อย่างเต็มที่ ยิ่งเป็นเรื่องความมั่นคงปลอดภัยก็ควรจะต้องใส่ใจมากขึ้น โดยเฉพาะวินโดวส์จะมีการอัพเดตอยู่เป็นประจำ เพื่อลดช่องโหว่ในการโจมตีจากการคุกคามภายนอกนั่นเอง

☑ **Remember Password :** พูดน้อยเชื่อว่าเพื่อนๆ หลายคนมักชอบตั้งให้ระบบจดจำรหัสผ่าน Remember Password ในการเข้าใช้งานเว็บไซต์ต่างๆ เรียกว่าเปิดปุ๊บก็ใช้ได้ทันที ไม่เสียเวลา แต่ข้อเสียก็คือหากวันดีคืนดีโดนขโมยคอมพิวเตอร์ไป ผลเสียก็อาจจะเกิดขึ้นกับเจ้าของ e-Mail ได้ทันที เช่น การถูกสวมรอยเป็นเจ้าของตัวตน เป็นต้น

ลบ Remember Password ใน Internet Explorer

ถ้าเลือกใช้ระบบ Remember Password ไปแล้ว และต้องการยกเลิก สามารถเข้าไปลบ Internet Temp หรือ History File โดยเข้าไปที่ Internet Option > General > Browsing History คลิกที่ปุ่ม Delete แล้วใส่เครื่องหมายหน้าหัวข้อ Password จากนั้นคลิกที่ Delete อีกครั้งหนึ่ง เท่านี้ ก็ใช้วิธีการล็อกอินด้วยตัวเองได้แล้วครับ



น้องพุดดิ้งชวนรู้

ก่อนจะจบหัวข้อนี้ พุดดิ้งขอเสริมอีกสักนิด สำหรับเพื่อนๆ ควรรู้จักตั้งสติและรับรู้ไว้ว่าในโลกออนไลน์ ทุกวันนี้ยังมีภัยไซเบอร์อีกหลากหลายวิธีที่บรรดา Hacker จะนำมาใช้เพื่อเข้ามาขโมยตัวตนของเราไป ทั้งการส่ง e-Mail มาขอรับบริจาค บ้างก็อ้างว่าเป็นเพื่อนเรา แต่ไปลำบากอยู่ต่างประเทศ ขอให้ส่งเงินมาให้ มุกแบบนี้เจอทีไรก็แทบอยากจะส่ายหัวทุกที แต่ท้ายที่สุดแล้วหากเราตั้งสติให้ดี ก็จะช่วยลดความเสี่ยงและสร้างความมั่นคงปลอดภัยไปได้อีกต่อหนึ่ง

2.4 หยุดความเสี่ยงได้ด้วยมือคุณ

ครั้งหนึ่งคุณยายเคยบอกกับพุดน้อย ในขณะที่พุดน้อยกำลังเล่นอินเทอร์เน็ตกับเพื่อนใหม่ในโซเชียลมีเดีย ว่า *"พุดน้อย ในโลกเรานี้มีทั้งคนดีและคนไม่ดี หากเราไม่ระวังให้ดี อาจจะมีผลร้ายส่งมาถึงเราได้นะ"* ประโยคข้างต้นของคุณยายเสมือนทำให้พุดน้อยได้สติ และฉุกคิดได้ ไม่ว่าจะเป็นโลกแห่งความจริง หรือโลกแห่งโซเชียลมีเดีย ก็ล้วนแล้วแต่มีคนดีและคนร้ายปะปนมั่วกันไปหมด และยิ่งคนที่เล่นอินเทอร์เน็ตส่วนใหญ่เป็นเยาวชนอายุรุ่นราวคราวเดียวกับพุดน้อยด้วยแล้ว พุดน้อยจึงยิ่งต้องเพิ่มความใส่ใจ หาข้อมูลดีๆ มาช่วยเพิ่มความมั่นคงปลอดภัยกันแบบเต็มที่เลยทีเดียว

ข้อควรระวังในการใช้อินเทอร์เน็ต

1. ไม่บอกข้อมูลส่วนตัวกับใครในโลกออนไลน์ : หากมีเพื่อนๆ ในโลกออนไลน์ที่เราสนิทด้วย แต่ไม่เคยพบตัวจริงกันมาก่อน มาถามถึงข้อมูลประวัติส่วนตัว เช่น อายุ วัน เดือน ปี เกิด ที่อยู่ เบอร์โทรศัพท์ หรือแม้แต่สถานศึกษาที่เรากำลังศึกษาอยู่ในกรณีนี้ ทางที่ดีควรบอกปฏิเสธไปแบบถนอมน้ำใจ เพราะการบอกข้อมูลที่ถูกต้องไปนั้น เราจะทราบได้อย่างไรว่า คนผู้นั้นจะไม่นำข้อมูลที่ได้จากเรามาทำเรื่องร้ายๆ เช่น สร้างตัวปลอมของเราขึ้นมาในโลกออนไลน์ หรืออาจจะมาเฝ้าสะกดรอยตามเราในโลกแห่งความเป็นจริงก็ได้

2. ไม่ส่งรูปให้ใครโดยขาดการไตร่ตรอง : หากเป็นไปได้ผู้ใช้อินเทอร์เน็ตทุกท่าน ไม่ควรส่งรูปให้บุคคลที่รู้จักทางอินเทอร์เน็ต แม้ว่าบุคคลนั้นจะเป็นเพื่อนแท้หรือคนรู้จักที่สนิทกันมาก ซึ่งเราก็ไว้ใจไม่ได้เช่นกันว่า รูปเหล่านั้นจะหลุดไปถึงมือผู้ไม่ประสงค์ดี นำไปใช้ตัดต่อหรือทำเรื่องร้ายแรงอะไรบ้างก็ไม่ทราบ

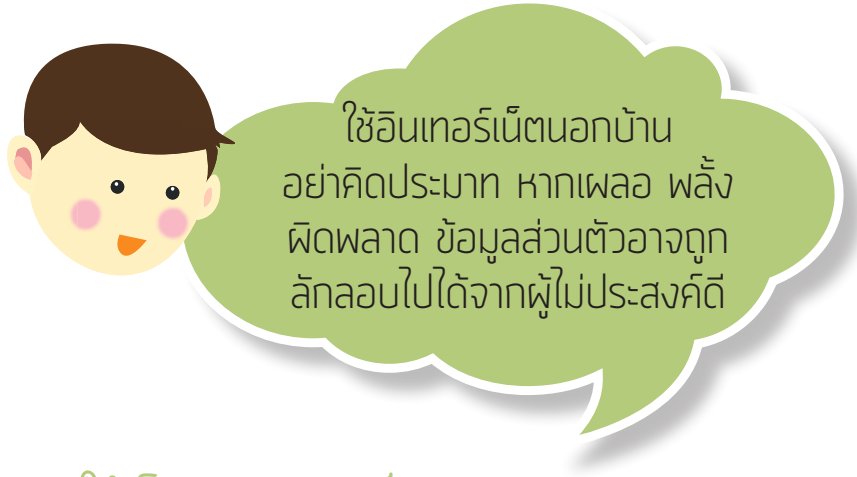
3. หลีกเลี่ยงการพบเพื่อนในโลกออนไลน์ในชีวิตจริง : เป็นที่รู้กันว่าคนที่รู้จักคุ้นเคยเห็นหน้ากันทุกวันยังหลอกลวงกันได้ แล้วประสาอะไรกับเพื่อนในโลกออนไลน์ที่อาจจะมาลวงหลอกเราก็เป็นได้ แต่หากจำเป็นที่จะต้องพบจริงๆ ก็ควรที่จะอยู่ในสายตาของผู้ปกครอง เพื่อให้มีคนคอยติดตามไปด้วย และที่สำคัญควรไปพบกันในที่สาธารณะ เพื่อป้องกันอันตรายจากในที่ลับตาคน

4. ไม่เสวนากับผู้ที่หยาบคายในโลกออนไลน์ : เป็นเรื่องที่ปกติธรรมชาติอยู่แล้ว หากว่าเราจะไม่ตอบคำถามหรือเสวนาโต้วาทีกับบรรดานักเลงคีย์บอร์ดที่ชอบพิมพ์ข้อความหยาบคาย สาเหตุเพราะการที่เราพิมพ์โต้ตอบกันด้วยข้อความที่หยาบคายนั้น ประโยคเหล่านี้อาจจะนำไปสู่การฟ้องร้องฐานหมิ่นประมาทกันได้

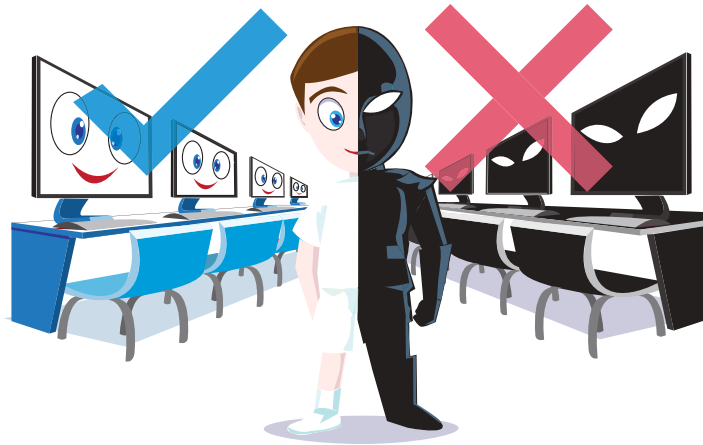
5. หากเป็นหนูๆ ต้องได้รับการอนุญาตจากผู้ปกครอง : จะเป็นเรื่องดีมากๆ หากเพื่อนๆ ที่เป็นเยาวชนวัยน่ารักแบบพุดน้อยทุกคน ก่อนจะเล่นอินเทอร์เน็ตได้ทำการขออนุญาตจากผู้ปกครอง เพื่อให้อยู่ในสายตาและดุลพินิจของท่าน สิ่งนี้จะเป็นการช่วยเพิ่มความมั่นคงปลอดภัยให้กับเรามากขึ้น เพราะหากเรามีการกระทำใดก็แล้วแต่ที่ส่อถึงความไม่มั่นคงปลอดภัย ก็จะมีผู้ใหญ่คอยช่วยแก้ไขและตักเตือนได้

น้องพุดดิ้งชวนรู้

ข้อมูลเรื่อง ข้อควรระวังในการใช้อินเทอร์เน็ต ที่พุดน้อยนำมาฝากนั้น พุดดิ้งสรุปได้ใจความว่า การแสดงออกในรูปแบบใดก็แล้วแต่ที่เกี่ยวข้องกับการใช้อินเทอร์เน็ต เช่น การส่งรูปภาพ การเสวนากับเพื่อน หรือการบอกข้อมูลส่วนตัวกับเพื่อนในโลกออนไลน์ ทุกสิ่งล้วนแล้วแต่สามารถทำได้ (และไม่ได้) แต่ควรมีสติและพิจารณาอย่างรอบคอบ เช่น เด็กหรือเยาวชนบางคนอาจทำการหมกมุ่นกับการเล่นอินเทอร์เน็ตมากเกินไป บ้างก็เล่นจนมีนิสัยก้าวร้าวเพราะได้คุยกับเพื่อนที่ชอบพูดจาหรือพิมพ์คำหยาบคาย การมีผู้ปกครองคอยเฝ้าดูแล ก็จะเป็นการช่วยให้ผู้ใช้บริการอย่างเราไม่ตกอยู่ในสถานการณ์ที่ไม่มั่นคงปลอดภัยนั่นเอง



2.5 ฉลาดใช้เน็ตคอมพิวเตอร์สาธารณะ



พูดน้อยว่าการใช้อินเทอร์เน็ตในบ้านเรานั้นมีความมั่นคงปลอดภัยดีแล้ว แต่สำหรับการต่ออินเทอร์เน็ตในที่สาธารณะ อันนี้นับว่ายังเป็นเรื่องน่าเป็นกังวลอยู่บ้าง ซึ่งทางที่ดีควรศึกษาวิธีป้องกันไว้น่าจะดีที่สุด แต่จะมีสิ่งใดที่ต้องระวังกันบ้าง ต้องมาดูกันครับ

คุณป้าของพุดน้อยเล่าให้พุดน้อยฟังอยู่เสมอ ด้วยความที่ต้องเดินทางไปทำงานต่างจังหวัดอยู่บ่อยครั้ง ประกอบกับในบางสถานการณ์ไม่สามารถที่จะจัดเตรียมโน้ตบุ๊กได้ทัน จึงทำให้ต้องไปใช้บริการคอมพิวเตอร์จากโรงแรมที่พักหรือร้านอินเทอร์เน็ตอยู่เป็นประจำ

คุณป้าอธิบายให้เข้าใจอีกว่า **การใช้งานคอมพิวเตอร์สาธารณะนั้นนับว่ามีความมั่นคงปลอดภัยต่ำ** เพราะเราไม่อาจทราบได้เลยว่าเครื่องคอมพิวเตอร์ที่เราใช้นั้นได้ถูกผู้ไม่ประสงค์ดี หรือ Hacker มาติดตั้งโปรแกรมดักโจรกรรมข้อมูลของเราหรือเปล่า อย่างไรก็ตาม ในบางสถานการณ์เราอาจมีความจำเป็นที่จะต้องใช้งานอินเทอร์เน็ตผ่านคอมพิวเตอร์สาธารณะจริงๆ การใช้บริการจึงไม่สามารถหลีกเลี่ยงได้ และเพื่อช่วยให้มีความมั่นคงปลอดภัยมากขึ้น เพื่อนๆ จึงควรศึกษาข้อแนะนำต่างๆ ต่อจากนี้ไป ที่พุดน้อยและคุณป้าจะนำมาฝากกัน

ข้อแนะนำในการใช้งานคอมพิวเตอร์สาธารณะ

1. เลือกใช้คอมพิวเตอร์ที่ไม่มีคนเดินผ่านไปมาบ่อย : เพื่อป้องกันการถูกแอบมองจากผู้ไม่ประสงค์ดี (Shoulder Surfing) การใช้คอมพิวเตอร์สาธารณะจึงไม่ควรเลือกเครื่องที่วางอยู่ในตำแหน่งที่มีวัตถุสามารถสะท้อนแสงจากหน้าจอได้

2. ตรวจสอบ Keylogger แบบ Hardware : เมื่อมีความจำเป็นที่จะต้องใช้คอมพิวเตอร์สาธารณะ ก่อนที่จะเริ่มเปิดเครื่อง ควรมีการสังเกตที่สายต่อระหว่าง Keyboard กับช่องเสียบด้านหลังคอมพิวเตอร์สักนิด หากพบว่ามีอุปกรณ์น่าสงสัยถูกเสียบอยู่ ให้ตั้งข้อสงสัยว่าอาจจะเป็น Keylogger และยกเลิกการใช้บริการคอมพิวเตอร์เครื่องนั้นในทันที

3. บู๊ตเครื่องโดยใช้ Bootable CD หรือ Bootable USB : จัดเป็นวิธีที่สามารถช่วยป้องกันอันตรายจากซอฟต์แวร์ที่ไม่พึงประสงค์ ที่อาจถูกติดตั้งอยู่ในคอมพิวเตอร์ดังกล่าวก็ได้ อย่างไรก็ตาม วิธีดังกล่าวนี้อาจไม่สามารถใช้กับคอมพิวเตอร์ได้ทุกเครื่อง เนื่องจากต้องมีการตั้งค่าการเชื่อมต่อกับเครือข่ายและอุปกรณ์อื่นๆ ในระบบ และตัวเราเองก็จำเป็นต้องพกแผ่น Bootable CD หรือ Bootable USB ติดตัวไปด้วย

4. สแกนไวรัสและใช้โปรแกรม On Screen Keyboard : เมื่อตรวจสอบแล้วพบว่าในเครื่องคอมพิวเตอร์ที่เรากำลังจะใช้งานมีโปรแกรมป้องกันไวรัสติดตั้งอยู่ ก่อนใช้งานควรทำการอัพเดตฐานข้อมูลและสแกนไฟล์ในเครื่องเพื่อตรวจสอบและกำจัดโปรแกรมไม่พึงประสงค์ ต่อมาแม้จะสแกนแล้วไม่พบโปรแกรมไม่พึงประสงค์อยู่ แต่ก็ควรใช้โปรแกรมประเภท On Screen Keyboard ในการพิมพ์ Username และ Password แทนจะดีที่สุด

5. ใช้การเชื่อมต่อผ่าน HTTPS : เมื่อได้ทำการเปิดคอมพิวเตอร์ และเบราว์เซอร์เพื่อต้องการท่องเว็บไซต์แล้ว เพื่อเป็นการไม่ให้ผู้ไม่ประสงค์ดีมาแกะรอยตามข้อมูลสำคัญของเรา ก็ควรใช้การเข้ารหัสแบบ HTTPS ตามวิธีที่พุดน้อยได้เคยนำมาให้ศึกษากันก่อนหน้านี้

6. ไม่บันทึกไฟล์ข้อมูลสำคัญลงในเครื่องสาธารณะ : ไม่ควรบันทึกไฟล์ลงบนคอมพิวเตอร์สาธารณะเด็ดขาด เนื่องจากถึงแม้จะลบไฟล์ไปแล้ว แต่ผู้ไม่หวังดีก็อาจจะใช้โปรแกรมกู้คืนไฟล์ที่ถูกลบไปได้ หากจำเป็นต้องบันทึกไฟล์เพื่อเปิดอ่านหรือแก้ไข ควรบันทึกลงในอุปกรณ์เทคโนโลยีจากภายนอก เช่น USB Drive

7. Log out ออกจากการท่องเว็บไซต์ทุกครั้งหลังใช้งาน : เนื่องจากในหลายเว็บไซต์จะมีการตั้งค่าให้จำสถานะของผู้ใช้ไว้ว่ากำลังทำการ Login อยู่ ถึงแม้จะปิดเบราว์เซอร์ไปแล้ว แต่หากมีผู้ไม่ประสงค์ดีมาเปิดเบราว์เซอร์นั้นใหม่ก็จะยังคงสถานะเป็น Login อยู่ ซึ่งอาจส่งผลให้เราถูกจดจำสถานะผู้ใช้และขโมยตัวตนในโลกออนไลน์ไปได้

8. Restart เครื่องหลังใช้งาน : การใช้งานคอมพิวเตอร์จะมีการเก็บข้อมูลไว้ใน Ram เพื่อใช้ในการประมวลผล ซึ่งหากเครื่องดังกล่าวมี Ram น้อย เครื่องจะทำการนำข้อมูลที่เกินมาเก็บไว้ใน Hard Disc ซึ่งเรียกว่า Virtual Memory, Swap หรือ Pagefile ถึงแม้จะมีการปิดเครื่องไปแล้วก็ยังจะมีข้อมูลหลงเหลืออยู่ใน Ram ดังนั้นการ Restart จะเป็นการล้างข้อมูลทั้งหมดออกไป

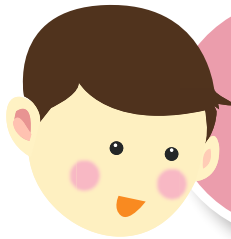
9. หลีกเลี่ยงการใช้ธุรกรรมทางการเงินรูปแบบออนไลน์ : เพื่อนๆ สามารถแน่ใจได้แล้วหรือว่าคอมพิวเตอร์สาธารณะไว้ใจได้ และเพื่อความไม่ประมาทจึงไม่ควรเข้าใช้งานที่เกี่ยวข้องกับการทำธุรกรรมทางการเงิน หรือถ้าจำเป็นต้องใช้บริการ ภายหลังจากใช้บริการก็ควรรีบเปลี่ยนรหัสผ่านทันทีเพื่อป้องกันในกรณีที่รหัสผ่านหลุดลอดออกไป

น้องพุดดิ้งชวนรู้

เมื่อมีเหตุจำเป็นที่ทำให้เราต้องใช้งานคอมพิวเตอร์สาธารณะอยู่บ่อยครั้ง สิ่งสำคัญจึงควรมีการเตรียมความพร้อมเรื่องการฝึกฝนใช้โปรแกรมป้องกันต่างๆ เช่น โปรแกรม On Screen Keyboard หรือโปรแกรมสแกนไวรัสอยู่เป็นประจำ นอกจากนี้หากมีเหตุต้องทำธุรกรรมทางการเงิน ควรเลี่ยงการทำธุรกรรมผ่านคอมพิวเตอร์ แต่ให้เลือกใช้การทำธุรกรรมผ่านเครื่องมือสื่อสารอื่นๆ เช่น แท็บเล็ต หรือสมาร์ตโฟน จะดีที่สุด

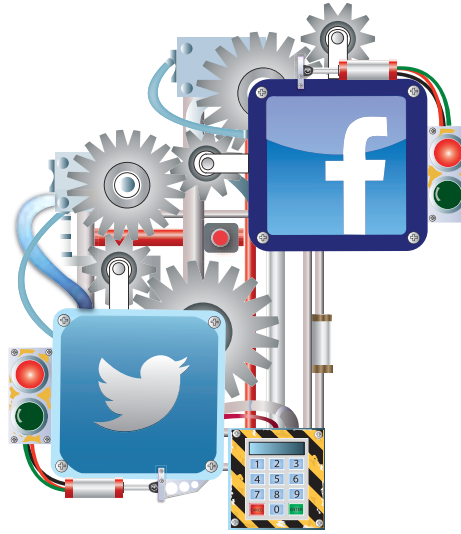
บทที่ 3

รู้จักโซเชียลมีเดีย รอบทิศทาง สร้างความมั่นใจ ในการใช้



โซเชียลมีเดีย (Social Media)
ลูกเล่นเยอะแพรวพราว
ศึกษาความเป็นมากันสักนิด

3.1 ความเป็นมาของโซเชียลมีเดีย



อยากจะน้อยใจเสียจริงๆ! ภายในห้องรับแขกวันนี้ไม่มีใครสนใจพูดน้อยเลย มองไปทางซ้ายก็เห็นคุณพ่อเล่น Facebook มองไปทางขวาคุณแม่ก็กำลังติดตามข่าวสารผ่าน Twitter ส่วนคุณอาก็กำลังสนุกกับการดาวน์โหลด Wechat มาใช้กับเพื่อนๆ ไม่เพียงเท่านี้นะ ตามสถานที่สาธารณะหากสังเกตให้ดีก็จะมีผู้ใช้บริการสื่อโซเชียลมีเดียเต็มไปหมด อะไรจะมีมากมายขนาดนี้

ความหมายของโซเชียลมีเดีย

นั่นสิ แล้วเพื่อนๆ เคยทราบกันหรือไม่ว่า ความหมายและความเป็นมาที่แท้จริงของโซเชียลมีเดีย นั้นมีความเป็นมาอย่างไร ถ้าไม่รู้ก็ตามมาเลย พุดน้อยจะอธิบายให้ทราบกัน

โซเชียล (Social) หมายถึง สังคม หรือ การรวมกลุ่ม

มีเดีย (Media) หมายถึง สื่อตัวกลางหรือเครื่องมือที่ใช้ทำการสื่อสาร

แล้วเมื่อนำมารวมกัน โซเชียลมีเดีย (Social Media) จึงหมายถึง สื่ออิเล็กทรอนิกส์ ที่ทำให้บุคคลทั่วไปมีส่วนร่วมในการปฏิสัมพันธ์และแบ่งปันข้อมูลกัน ส่วนคำว่า โซเชียลเน็ตเวิร์ก (Social Network) นั้นก็ถูกต่อยอดความหมายมาจากคำว่า โซเชียลมีเดีย ซึ่งแปลว่า **“เครือข่ายสังคม”** หรือกลุ่มบุคคลที่ติดต่อสื่อสารโดยใช้โซเชียลมีเดียเป็นสื่อกลางนั่นเอง

เหตุผลที่ทำให้โซเชียลมีเดียได้รับความนิยม

ปัจจุบันโซเชียลมีเดียนั้น แม้จะเพิ่งเกิดขึ้นมาในโลกออนไลน์ได้ไม่นาน หรือประมาณไม่ถึง 10 ปีที่ผ่านมา แต่ด้วยความที่เป็นสื่อสมัยใหม่และยังมีอานุภาพที่ทำให้โลกออนไลน์แคบขึ้น เพื่อนที่อยู่ห่างไกลกันข้ามทวีปก็สามารถเห็นหน้าหรือคุยกันได้ไม่ยาก (Real-Time Communication) ด้วยเหตุนี้จึงทำให้สื่อชนิดนี้สามารถสร้างความนิยมจนมียอดผู้ใช้บริการมากกว่าพันล้านคน ถือว่าเป็นนวัตกรรมที่เปลี่ยนโฉมหน้าของการสื่อสารในยุคปัจจุบันเลยทีเดียว

นอกจากความน่าสนใจข้างต้นที่พุดน้อยหยิบยกมาให้ดูกันแล้ว โซเชียลมีเดียยังนับว่าเป็นสื่อสังคมออนไลน์ที่ผู้บริการทุกเจ้าเปิดให้ใช้กันอย่างแพร่หลายแบบฟรีๆ และด้วยความที่ผู้พัฒนาในแต่ละค่ายต่างเพิ่มลูกเล่นที่น่าสนใจเพิ่มขึ้นเรื่อยๆ เพื่อให้ผู้ใช้บริการดาวน์โหลดหรือติดตั้งการใช้งานผ่านสมาร์ตโฟนหรือคอมพิวเตอร์ เช่น สามารถโพสต์ข้อความแสดงความรู้สึกได้ มีบริการแชตให้สามารถพูดคุยกับเพื่อนได้ มีบริการอัพโหลดรูปเพื่อโชว์ภาพ หรือแม้แต่วิดีโอคอลที่ทำให้เห็นหน้ากันอย่างชัดเจน ด้วยเหตุนี้จึงทำให้สื่อโซเชียลมีเดียมีอิทธิพลอย่างกว้างขวางกับกลุ่มคนทุกเพศ ทุกวัย และเกือบจะทุกสาขาอาชีพ อาทิ สื่อมวลชน ดารานักแสดง นักศึกษา และนักธุรกิจ

น้องพุดดิ้งชวนรู้

พุดดิ้งคิดว่า ธรรมชาติของมนุษย์เรา เดิมทีก็เป็นสัตว์สังคมอยู่แล้ว ดังนั้น การที่จะเปิดใช้บริการโซเชียลมีเดียให้มาเป็นหนึ่งในกิจกรรมของชีวิตก็ถือว่าน่าสนใจไม่น้อยเลยทีเดียว แต่ทางที่ดี ขณะใช้งานควรมีสติในการเรียนรู้ที่จะใช้งานให้เกิดประโยชน์แก่ตนเองและไม่เบียดเบียนต่อความเป็นส่วนตัวของผู้อื่นจะดีที่สุดนะคะ

3.2 สังคมออนไลน์ประโยชน์มากมาย

เนื่องจากเรื่องก่อนหน้านี้ จะเห็นว่าพุดน้อยได้บรรยายถึงบรรยากาศภายในห้องรับแขกของครอบครัวพุดน้อย ซึ่งทั้งคุณพ่อ คุณแม่ และคุณอา ต่างก็กำลังใจจดใจจ่อในการใช้สื่อสังคมออนไลน์กันอย่างสนุก ในจุดนี้จึงทำให้พุดน้อยเล็งเห็นถึงประโยชน์ที่มากมายของสื่อสังคมออนไลน์อีกหลายข้อครับ

6 ข้อดีของสื่อสังคมออนไลน์

1. ประหยัดค่าใช้จ่าย : นับเป็นประโยชน์แรกๆ ของสังคมออนไลน์เลยก็ว่าได้ เพราะไม่ว่าจะเป็นสื่อโซเชียลมีเดียค่ายไหนก็เปิดให้มีการใช้บริการในแบบไม่เสียค่าใช้จ่ายกันทุกเจ้าแล้วทั้งสิ้น

2. สื่อสารรวดเร็วทันใจ : คุณสมบัติอีกอย่างของสังคมออนไลน์ ก็คือ ความรวดเร็วและง่ายในการติดต่อสื่อสาร ขอเพียงแค่มีเครือข่ายอินเทอร์เน็ตอยู่รอบตัว และมีเครื่องมือสื่อสาร เช่น สมาร์ตโฟนหรือแท็บเล็ตดีๆ สักเครื่อง เท่านี้ก็สามารถสื่อสารกับเพื่อนๆ ในสังคมออนไลน์ได้อย่างไม่ติดขัดแล้ว

3. เป็นสื่อแสดงศิลปะและความคิดเห็น : ไม่ว่าจะเป็นบุคคลสาขาอาชีพไหน หากได้เจอประสบการณ์ดีๆ หรือมีภาพถ่ายสวยๆ ก็อยากจะนำมาโพสต์หรือแชร์ให้คนรู้จักได้ชื่นชมด้วยกันทั้งนั้น ซึ่งสังคมออนไลน์ในปัจจุบันจึงถูกพัฒนาให้เป็นสื่อในการนำเสนอผลงานของผู้ใช้บริการ เช่น ภาพถ่าย งานเขียน หรือวิดีโอ ได้หมดแล้ว

4. เล่นสนุกเพลิดเพลิน : สำหรับผู้ใช้บริการที่ต้องการหาเพื่อนคุยเล่นสนุกๆ สังคมออนไลน์นี่แหละ ถือเป็นสื่อกลางในการสร้างความสัมพันธ์ที่ดีจากเพื่อนสู่เพื่อนได้เป็นอย่างดี รวมถึงโซเชียลมีเดีย ในหลายแอพพลิเคชัน ก็ได้มีการพัฒนาลูกเล่นเสริมเป็นเกมสนุกๆ ให้ผู้ใช้บริการเลือกเล่นกันได้อย่างสนุกเพลิดเพลินบันเทิงใจ

5. สื่อสารกับคนมีชื่อเสียง : คงจะไม่ผิดแน่ ถ้าจะบอกว่าสังคมออนไลน์ทำให้เราได้ลดช่องว่างระหว่างเรากับดารา นักแสดง และบุคคลมีชื่อเสียงในวงการต่างๆ ได้แคบขึ้น

6. ใช้เป็นสื่อประชาสัมพันธ์ : โซเชียลมีเดีย นับว่าเป็นสื่อที่ถูกนำมาใช้โฆษณาและประชาสัมพันธ์ให้กับองค์กรนั้นๆ อย่างแพร่หลาย ทั้งหน่วยงานจากภาครัฐ และบริษัทเอกชนน้อยใหญ่ในการสร้างความเชื่อมั่นให้แก่ผู้ติดตาม เช่น การประชาสัมพันธ์กิจกรรมดีๆ หรือสร้างผลพวงเป็นหน้าร้านขายสินค้าแบบฟรีๆ โดยไม่เสียค่าใช้จ่ายอีกด้วย

น้องพุดดิ้งชวนรู้

เห็นไหมคะว่า สังคมออนไลน์นั้นสามารถนำไปใช้ประโยชน์ได้มากมาย ยิ่งศึกษาก็ยิ่งทำให้พุดดิ้งได้เห็นภาพของโลกออนไลน์ชัดเจนมากขึ้น ทั้งการนำไปใช้เพื่อความบันเทิง การศึกษา หรือแม้แต่การใช้เป็นสื่อเพื่อประชาสัมพันธ์ผลงานของตนเอง ซึ่งก็นับว่าน่าสนใจไม่น้อย

3.3 สังคมออนไลน์อาจกลายเป็นมหันตภัยที่ไม่คาดคิด

พุดน้อยจำคำสอนของคุณครูที่โรงเรียนประโยคหนึ่งได้ว่า ในโลกนี้ทุกอย่างถ้ามีด้านสว่างก็ต้องมีด้านมืดควบคู่กันไป สิ่งนี้ทำให้พุดน้อยฉุกคิดถึงสื่อสังคมออนไลน์ได้ว่า แม้จะมีประโยชน์ต่อผู้ใช้มหาศาล แต่ทั้งนี้ก็ยังมีผู้ที่คิดไม่ดีนำเทคโนโลยีดีๆ ไปใช้ในทางที่ผิด เช่น การใช้ในการหลอกลวงล่อลวง หรือขโมยข้อมูลส่วนตัวผู้อื่น อย่างที่เราเคยเห็นข่าวในหน้าหนังสือพิมพ์อยู่เสมอๆ สะท้อนออกมาให้เห็นว่าในโลกออนไลน์นั้นก็มีทั้งด้านขาวและดำ และในฐานะที่พุดน้อยเป็นผู้ที่ศึกษาข้อมูลเกี่ยวกับโลกออนไลน์มานาน พุดน้อยจึงอยากจะขอยกตัวอย่างภัยร้ายที่มาจากสังคมออนไลน์ให้เพื่อนๆ ได้ศึกษาควบคู่กันไปด้วย เพื่อที่เพื่อนๆ จะได้ระมัดระวังในการใช้ชีวิตในโลกออนไลน์มากขึ้น

1. ระวังพิษภัยจากเพื่อนตัวปลอม

จะเป็นไปได้ไหม ถ้าเพื่อนในโซเชียลมีเดียที่เราคุยด้วยกันอยู่ทุกวันจะเป็นพวกต้มตุ๋นปลอมตัวมาหลอกสอบถามข้อมูลส่วนตัวกับเรา พูดน้อยขอตอบเลยว่าเป็นไปได้ครับ สาเหตุก็เพราะนักต้มตุ๋นประเภทนี้มีอยู่ทั่วทุกหนทุกแห่ง ไม่เว้นแม้แต่โลกออนไลน์ ที่สามารถสร้างโปรไฟล์ปลอม เป็นดารา นักร้อง นักแสดง ผู้มีชื่อเสียง มาแสร้งทำเป็นตีสนิทและใช้ความรู้สึกอ่อนไหวของมนุษย์ หลอกลวงและทำให้เราตายใจ อาทิ ขอความช่วยเหลือแล้วให้โอนเงินไปให้ หรือขอทราบถึงข้อมูลส่วนตัวจากเราเพื่อไปหลอกเพื่อนๆ เราต่อไปเป็นทอดๆ ดังนั้น **การรับ “Add” เพื่อนหรือพูดคุยกับคนไม่รู้จักจึงควรตั้งสติและระมัดระวังให้ดีนะครับ**

2. โพสต์และแชร์อย่างมีสติ

นอกจากจะต้องระวังเพื่อนตัวปลอมในโลกออนไลน์แล้ว เรายังต้องระวังเรื่องการโพสต์ข้อมูลหรือการคอมเมนต์รูปภาพด้วยนะครับ เพราะถึงแม้ว่าการแสดงความรู้สึกดังกล่าวจะเป็นเรื่องปกติในโลกออนไลน์ที่ทุกคนก็ทำกัน และสามารถทำได้อย่างอิสระด้วย แต่อย่าลืมว่าโลกออนไลน์ คือ **"พื้นที่ส่วนตัวบนโลกสาธารณะ"** ไม่ว่าเราจะโพสต์อะไร คนที่ติดตาม (Follow) หรือเป็นเพื่อน (Friend) ก็จะเห็นเหมือนกันหมด ยิ่งหากเราตั้งค่าการแสดงผลเป็นแบบสาธารณะ (Public) คนทั่วโลกจะสามารถเห็นข้อความของเราได้ทันที หากโพสต์ดีก็ไม่มีอะไรเสียหาย แต่หากโพสต์ข้อความหรือรูปภาพที่ล่อแหลมก็อาจจะเป็นสาเหตุเล็กๆ ที่ทำให้เรากลายเป็นผู้เดือดร้อนในภายหลังได้ เช่น ถูกนำรูปภาพไปตัดต่อหรือถูกวิจารณ์จากผู้ที่มีความคิดเห็นไม่ตรงกับเรา แม้จะโพสต์หรือแชร์เพียงไม่กี่นาทีแล้วลบออกก็ตาม ดังนั้น เราจึงต้อง**คิดให้ดีก่อนที่จะโพสต์นะครับ**

3. อย่าเปิดเผยข้อมูลส่วนตัวมากเกินไป

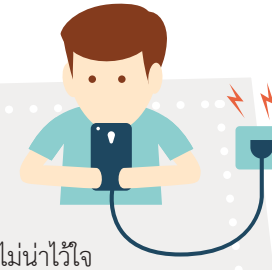
เว็บไซต์หรือแอพพลิเคชันโซเชียลมีเดีย ที่เปิดให้บริการส่วนใหญ่จะมีการให้ผู้ใช้บริการกรอกข้อมูลประวัติส่วนตัวลงไปเพื่อระบุความมีตัวตนในโลกออนไลน์ แต่ทั้งนี้ หากผู้ใช้บริการไม่ระมัดระวังในการกรอกข้อมูล หรือเปิดเผยข้อมูลที่เป็นความจริงมากเกินไป ก็อาจจะส่งผลร้ายที่ไม่คาดคิดตามมา เช่น **มีผู้ไม่ประสงค์ดีนำประวัติของเราไปแอบอ้างนำมาใช้ในทางเสียหายหรือละเมิดสิทธิส่วนบุคคลได้**

4. อัพโหลดภาพขึ้นสังคมออนไลน์ เรื่องง่ายๆ ที่ต้องระวัง

ในปัจจุบัน การถ่ายภาพแล้วอัพโหลดขึ้นสู่อินเทอร์เน็ตกำลังเป็นที่นิยม โดยเฉพาะการอัพโหลดขึ้นไปบนสังคมออนไลน์ หรือนำไปโพสต์ในเว็บบอร์ดต่างๆ ซึ่งผู้ใช้บริการทั่วไปมักเข้าใจว่าข้อมูลในรูปภาพนั้นเป็นเพียงแค่ภาพถ่ายธรรมดา แต่น้อยคนที่จะรู้ว่า **ภาพบางภาพนั้นอาจมีข้อมูลที่ก่อให้เกิดการละเมิดสิทธิส่วนบุคคลหรือความเป็นส่วนตัว** จนถึงขั้นก่อให้เกิดอันตรายต่อผู้ที่ถ่ายภาพหรือผู้ที่อยู่ในภาพได้ เช่น ข้อมูลตำแหน่งพิกัดที่อยู่ในเวลาที่ภาพนั้นถูกถ่าย และเมื่อไหร่ก็ตามที่ผู้ไม่ประสงค์ดีมาพบเจอก็อาจจะส่งผลร้ายที่ไม่คาดคิดขึ้นมากับเราหรือคนใกล้ชิดก็ได้

5. ความเสี่ยงของเพื่อน คือ ความเสี่ยงของเรา

เพื่อนของเราอาจทำให้เราเสี่ยงไปด้วย หากโปรไฟล์ของเพื่อนในสังคมออนไลน์ถูกผู้ไม่หวังดีเจาะข้อมูลเข้ามา ทำให้ Hacker เห็นข้อมูลทุกอย่างที่ผู้ใช้ส่งให้เพื่อนของตัวเองได้ ดังนั้น หากเพื่อนของเราไม่ได้ระมัดระวังให้ดี ความเป็นส่วนตัวของเราเองก็อาจได้รับผลเสียไปด้วย



เทคนิคง่ายๆ ระวังเพื่อนในสังคมออนไลน์

☑ ไม่ควรคุย (Chat) กับบุคคลที่ไม่รู้จัก หรือไม่ไว้ใจ

☑ ไม่ใส่ชื่อที่อยู่จริงในโซเชียลเน็ตเวิร์ก หรือเว็บไซต์ที่ไม่น่าไว้ใจ

☑ คิดอยู่เสมอว่า เพื่อนที่เรารู้จักทางสังคมออนไลน์ ที่ไม่เคยเจอหน้ากัน อาจจะเป็นบุคคลที่ไม่พึงประสงค์

☑ ไม่มีอะไรได้มาฟรีๆ หากมีคนมาชวนทำงานง่ายๆ สร้างรายได้สูงๆ คิดได้เลยว่าน่าจะเป็นการหลอกลวง

☑ การนัดพบปะกับคนที่ติดต่อผ่านทางสังคมออนไลน์ ไม่ควรไปอยู่ในที่ลับตา แต่ควรอยู่ในที่ที่มีคนพลุกพล่าน เช่น ห้างสรรพสินค้า และที่สำคัญควรพาเพื่อน ญาติ หรือคนรู้จักไปด้วย

น้องพุดดิ้งชวนรู้

ได้ข้อแนะนำดีๆ จากพุดน้อยกันไปแล้ว เพื่อนๆ ก็อย่าลืมนำไปปรับใช้กับชีวิตประจำวันของตนเองล่ะ และทางที่ดีควรจะนำความรู้ที่ได้มา ไปส่งต่อให้ญาติสนิท มิตรสหาย หรือคนในครอบครัวได้ทราบกันด้วย รวมไปถึงการร่วมสังเกตพฤติกรรมคนเหล่านี้ว่ามีใครทำตัวผิดปกติไปจากชีวิตจริงหรือเปล่า เอาใจใส่กันสักนิดก่อนที่จะมีอันตรายเกิดขึ้นกับคนที่เรารักนะคะ

3.4 เฟซบุ๊กมั่นคงปลอดภัยหรือไม่ กำหนดได้ด้วยตัวเอง

พุดน้อยจัดว่าเป็นหนึ่งในผู้ที่ชื่นชอบการเล่นเฟซบุ๊กเป็นชีวิตจิตใจ เพราะว่านอกจากจะได้แชตกับเพื่อนๆ แล้ว ยังได้เล่นเกมสนุกๆ ทุกวัน โดยจากข้อมูลสถิติของเว็บไซต์ www.thenextweb.com ที่พุดน้อยไปสำรวจมา พบว่าไม่ใช่เพียงแค่พุดน้อยเท่านั้นที่ชอบเล่นเฟซบุ๊ก แต่ในโลกนี้ยังมีผู้ใช้งานคนอื่นๆ สูงถึง 1,190 พันล้านยูสเซอร์ทั่วโลกเลยทีเดียว โอ้โห!

สำหรับในประเทศไทย ก็มีการสำรวจโดย Zocial Inc บริษัทวิเคราะห์ข้อมูลออนไลน์เช่นกัน พบว่า ประเทศไทยมีผู้ใช้งานสื่อสังคมออนไลน์สูงถึง 25 ล้านคน และเป็นตัวเลขของผู้ใช้งานเฟซบุ๊ก มากถึง 18.5 ล้านคน จะเยอะอะไรขนาดนั้น

ข้อมูลที่พุดน้อยไปศึกษามา ยังทำให้ทราบอีกว่า ในขณะที่เราเล่นเฟซบุ๊กกันอย่างเพลิดเพลินนั้น เราก็ได้เสพสื่อโฆษณาที่แฝงมาในหน้าเพจ (Page) ของเฟซบุ๊กโดยไม่รู้ตัว สาเหตุก็เพราะเฟซบุ๊กแม้จะถูกสร้างขึ้นเพื่อให้เราใช้กันแบบฟรีๆ แต่สำหรับผู้พัฒนาเฟซบุ๊กนั้น ต่างก็ต้องมีค่าใช้จ่ายในการพัฒนาหรือปรับปรุงโปรแกรมการใช้งานเช่นกัน ซึ่งวิธีที่จะทำให้ได้เงินมาปรับปรุงระบบก็คือ การขายข้อมูลส่วนตัวของผู้ใช้บริการอย่างเราให้แก่นักการตลาดเพื่อนำไปวิเคราะห์ ก่อนจะนำเสนอสินค้ากลับมาให้เราชนิดที่เนียนแบบสุดๆ ทั้งๆ ที่เราไม่เคยให้ข้อมูลใดๆ กับเฟซบุ๊กมาก่อนเลย

ข้อมูลเราหลุดไปได้อย่างไร?

ข้อแรก...เมื่อใดก็ตามที่คลิกโฆษณาบนเฟซบุ๊ก เจ้าหน้าที่ของทางเฟซบุ๊กจะทำการรวบรวมข้อมูลของผู้ใช้รายนั้นมาเก็บไว้ แม้ว่าในแถลงการณ์ของเฟซบุ๊กเองจะเคยบอกไว้ว่าไม่สามารถทำได้ก็ตาม

ข้อสอง...เมื่อใดก็ตามที่ทำการให้สิทธิการเข้าถึงข้อมูลความเป็นส่วนตัว ผ่านการตอบรับเล่นเกม หรือตอบปัญหาทายสนุกในเฟซบุ๊ก ยกตัวอย่าง *“คุณเป็นตัวละครใดในเรื่องทองเนื้อเก้า”* หรือ *“นิสัยของคุณตรงกับรถชนิดใด”* เพียงเท่านี้ ข้อมูลส่วนตัวของผู้ใช้บริการได้ถูกเฟซบุ๊กรวบรวมไปแล้วนั่นเอง

คำถามคือ แล้วเราจะสามารถปกป้องข้อมูลส่วนตัวจากเฟซบุ๊กได้อย่างไร? คำตอบคือ พูดน้อยได้เตรียมวิธีการป้องกันข้อมูลส่วนตัวมาฝากเพื่อนๆ แล้วนั่นเอง

หยุดไม่ให้ใครมาล้วงข้อมูล

หากเพื่อนๆ ติดตั้งโปรแกรมเกมหรือโปรแกรมเสริมในเฟซบุ๊ก เจ้าโปรแกรมเหล่านี้จะสามารถเข้ามาแอบดูข้อมูลของเราได้ ซึ่งการป้องกันข้อมูลรั่วไหลเราก็ทำได้ไม่ยาก

วิธีการ

1. เข้าไปที่เมนู Account > Privacy Setting > Apps and Websites
2. เลือก Edit your settings
3. เลือก Info accessible through your friends
4. คลิกที่ Edit Settings
5. จากนั้นเราจะพบว่าข้อมูลอะไรของเราบ้างที่อาจถูกเปิดเผยได้
6. คลิกตรงที่ข้อมูลที่ต้องการซ่อนไม่ให้คนอื่นเห็น และคลิกที่ปุ่ม Save เพียงเท่านี้ก็จะสามารถป้องกันข้อมูลหลุดได้แล้วครับ

ปิดโฆษณากวนใจ

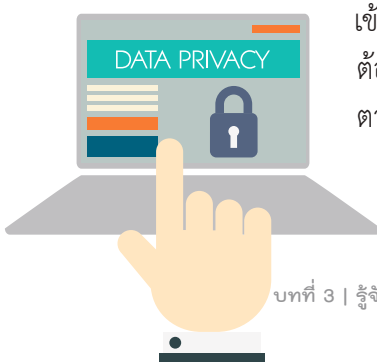
โฆษณาทั้งหลายที่อยู่ในเฟซบุ๊ก อาจแฝงไปด้วยโฆษณาที่เหล่าโจรไซเบอร์แอบซ่อนไวรัสหรือสปายแวร์ไว้ เพื่อหลอกให้เราคลิกและแอบดึงข้อมูลเราไป ดังนั้น เพื่อเป็นการป้องกันภัยที่อาจจะเกิดขึ้น เราจึงต้องเข้าไปตั้งค่าเฟซบุ๊กดังต่อไปนี้

1. เข้าไปที่เมนู Account เลือก Accounting Settings
2. เลือกแถบเมนู Facebook Ads
3. ในช่อง Allow ads on platform pages to show my information to... ให้เลือกเป็น Only my friends หรือ No one และคลิกปุ่ม Save Changes เท่านี้ก็จะหลุดพ้นจากโฆษณาชวนเชื่อได้แล้ว

กำหนดสิทธิ์ที่จะเข้าถึง

หากต้องการจะหลีกหนีจากการถูกดึงข้อมูลไปใช้ หลังจากทำการติดตั้งแอพพลิเคชันต่างๆ ในเฟซบุ๊ก เพื่อให้แอพพลิเคชันเหล่านั้นสามารถเข้าถึงข้อมูลของเราได้เพียงบางส่วน ต้องเข้าไปตั้งค่าด้วยวิธีการดังนี้ครับ

1. เข้าไปที่เมนู Account และเลือก Privacy Settings
2. เลือกเมนู Apps and Websites และเลือก Edit your settings
3. ในหัวข้อ Apps you use คลิกที่ปุ่ม Edit Settings เราจะพบว่ามีแอพพลิเคชันใดบ้างที่เราติดตั้งไว้และแอพพลิเคชันเหล่านั้นสามารถเข้าถึงข้อมูลอะไรของเราได้บ้าง ซึ่งตรงนี้เราต้องเลือกว่าจะเปิดเผยข้อมูลส่วนตัวอะไรบ้างตามความเหมาะสมครับ



ล็อกเอาท์ให้ติดเป็นนิสัย

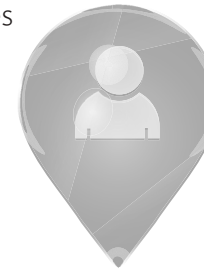
การออกจากระบบหรือ Sign Out (ออกจากระบบ) ของเฟซบุ๊กหลังจากที่ใช้งานเสร็จ เป็นเรื่องที่สำคัญมากยิ่งในกรณีที่เราใช้เฟซบุ๊ก ด้วยเครื่องคอมพิวเตอร์ตามที่สาธารณะ ซึ่งต้องใช้วิธีการ Sign Out จากเครื่องคอมพิวเตอร์เหล่านี้ แต่ผู้ใช้บริการอย่างเราก็สามารถตรวจสอบได้ว่า มีผู้ใดแอบเข้ามาใช้เฟซบุ๊กของเราบ้างหรือเปล่า ด้วยการเลือกหัวข้อ ดังนี้

1. เข้าไปที่เมนู Account และเลือก Account Settings
2. เลือกหัวข้อ Account Security ในแถบ Settings
3. เลือก Send me an email และคลิกที่ปุ่ม Save

ปิด *Check In* เพื่อความมั่นคงปลอดภัย

หากมีการเปิดใช้ Check In ให้เพื่อนๆ ได้รับรู้ว่าเราอยู่ ณ ที่ใดในโลกใบนี้ คุณสมบัติข้อนี้ของเฟซบุ๊ก นับว่าน่ากลัวมากๆ ครับ เพราะถ้าหากเป็นเพื่อนของเพื่อนเราจริงๆ ก็คงไม่เป็นไร แต่หากเป็นผู้ไม่หวังดีไปพบเข้าจะเกิดเหตุร้ายขึ้นกับเราหรือเปล่าก็ไม่รู้ ดังนั้นต้องรีบป้องกันตัว โดยเข้าไปที่

1. เข้าไปที่เมนู Account และเลือก Privacy Settings
2. เลือกหัวข้อ Customize settings
3. ไปที่หัวข้อ Things others share
4. ไปที่หัวข้อ Friends can check me in to Places
5. คลิกที่ปุ่ม Edit Settings
6. ในหัวข้อ Friends can check me in to Places ให้เลือกเป็น Disabled และคลิกที่ปุ่ม OK เท่านี้ก็มั่นคงปลอดภัยแล้วครับ



ซ่อนตัวไว้ไม่ให้ใครเห็น

สิ่งที่สำคัญอีกประการของการรักษาความเป็นส่วนตัวในเฟซบุ๊ก คือ การซ่อนตัวเองไม่ให้ไปปรากฏในรายชื่อผู้ที่อยู่ในตำแหน่งที่เรา Check In ในที่สาธารณะ ลองคิดดูว่าหากคนที่เราไม่อยากพบ รู้ว่าเราอยู่ในตำแหน่งเดียวกับเขา เราจะเดือดร้อนแค่ไหน รีบปิดคุณสมบัตินี้ของเฟซบุ๊กกันเถอะครับ

1. เข้าไปที่เมนู Account และเลือก Privacy Settings
2. เลือกหัวข้อ Customize settings
3. ไปที่หัวข้อ Include me in “People Here Now” after I check in
4. เอาเครื่องหมายถูกจากกล่อง Enable ออก

หายังไงก็หาไม่เจอ

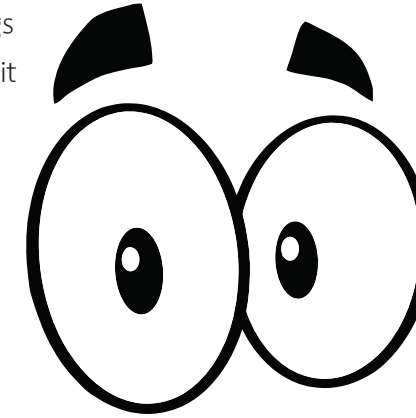
Google เป็นเครื่องมือในการค้นหาข้อมูลขั้นเทพที่ใช้ค้นหาอะไรก็เจอในโลกอินเทอร์เน็ต สำหรับข้อมูลจากเฟซบุ๊กของเรา Google ก็สามารถเข้าถึงข้อมูลรูปภาพของเราได้เช่นเดียวกัน ดังนั้น หากไม่มีการป้องกันที่ดี ผู้อื่นอาจเข้าถึงข้อมูลของเราได้โดยง่าย เราจึงต้องทำตามขั้นตอนดังนี้ครับ

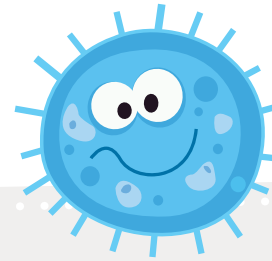
1. เข้าไปที่เมนู Account และเลือก Privacy Settings
2. เลือกเมนู Apps and Websites และเลือก Edit your settings
3. ในหัวข้อ Public search คลิกที่ปุ่ม Edit Settings
4. เอาเครื่องหมายถูกจากกล่อง Enable public search ออก

รูปนี้มีให้เพื่อนดูเท่านั้น

รูปภาพต่างๆ ในเฟซบุ๊กของเราอาจจะถูกเข้ามาถ้ำมองโดยคนที่เราไม่อยากให้ดูก็ได้ หากเราไม่มีการกำหนดค่าความเป็นส่วนตัวที่เหมาะสม โดยเฉพาะรูปใน Photo Albums ที่มีชื่อว่า “Profile Pictures”, “Mobile Uploads” และ “Wall Photo” ดังนั้น เราจึงต้องเข้าไปกำหนดค่าในเฟซบุ๊กดังนี้ครับ

1. เข้าไปที่เมนู Account และเลือก Privacy Settings
2. คลิกที่หัวข้อ Customize settings
3. ในหัวข้อ Things I share คลิกที่ Edit privacy settings for existing photo albums and videos และเลือกกลุ่มคนที่เราอยากให้เห็นรูปภาพของเราตามความเหมาะสม





โฆษณาในเฟซบุ๊กอาจมีไวรัส

การลงโฆษณาในเฟซบุ๊ก ผู้ลงโฆษณาจะต้องสร้างแบนเนอร์ด้วยตัวเองตามขนาดที่เฟซบุ๊กกำหนดไว้ แล้วจึงมีการอัพโหลดแบนเนอร์ขึ้น โดยพื้นฐานแล้วเฟซบุ๊กเองมีการตรวจสอบโฆษณาที่ค่อนข้างไม่ถี่ถ้วน จึงอาจทำให้ผู้ใช้บริการที่คลิกไปยังป้ายโฆษณา เช่น โฆษณาโปรแกรมป้องกันไวรัสคอมพิวเตอร์ แต่ในความเป็นจริงกลับกลายเป็นการดาวน์โหลดตัวไวรัสมาแทนซะงั้น...ว้า! แย่จัง

น้องพุดดิ้งชวนรู้

ท้ายที่สุดแล้ว ภัยร้ายจะเกิดขึ้นกับเราหรือไม่ สิ่งนั้นไม่ใช่ความผิดของเฟซบุ๊ก แต่ตัวการสำคัญอยู่ที่ตัวเราเองที่ได้เรียนรู้ทฤษฎีแล้ว แต่กลับไม่นำไปปรับใช้ให้เกิดประโยชน์สูงสุด ความมั่นคงปลอดภัยที่แท้จริงก็จะไม่บังเกิดขึ้นกับเราในโลกออนไลน์นี้แน่นอน

3.5 สิ่งที่พึงระวังบนโลกสังคมออนไลน์

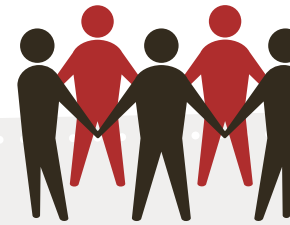
วันหยุดสุดสัปดาห์นี้ คุณแม่จะพาพุดน้อยไปเที่ยวบ้านคุณตาที่ต่างจังหวัด พุดน้อยดีใจมาก เพราะบ้านคุณตากว้างขวางและมีสวนสนามหญ้าให้วิ่งเล่น ส่วนคุณแม่ก็บอกกับพุดน้อยว่าอยากจะถ่ายรูปและโพสต์รูปแบ่งปันให้เพื่อนๆ ในโซเชียลมีเดียได้ดูด้วยบ้างจัง แต่ใจหนึ่งคุณแม่ก็กังวลว่าสิ่งที่กำลังจะทำนั้น เป็นพฤติกรรมที่เสี่ยงต่อภัยร้ายในโลกออนไลน์หรือเปล่า

เอาล่ะ! ทั้งคุณแม่และเพื่อนๆ นักอ่าน ที่ทราบถึงปัญหาเช่นนี้แล้ว อย่าเพิ่งรู้สึกหมดสนุกนะครับ เรื่องแบบนี้ปล่อยให้เป็นหน้าที่ของพุดน้อยเอง ที่จะทำการศึกษาถึงเกร็ดความรู้ดีๆ มาให้เพื่อนๆ ได้ศึกษากันกับหัวข้อที่ว่า พึงระวังพฤติกรรมบนโลกออนไลน์อย่างไร เพื่อให้รอดพ้นจากความเสี่ยงภัยบนโลกออนไลน์

Step 1 อย่าแสดงข้อมูลที่อยู่จริงบนโลกออนไลน์ : ยังไม่ทันจะได้ออกจากบ้านไปเที่ยวก็เสี่ยงจะถูกภัยจากโลกออนไลน์เข้าเล่นงานให้แล้ว ทางที่ดีหากพบว่าในโซเชียลมีเดีย โปรแกรมใดก็ตามที่เราสมัครใช้บริการไว้ได้เผลอทำการระบุสถานที่อยู่ ที่ทำงานไว้ให้รีบไปทำการแก้ไขลบประวัติทิ้ง สาเหตุเพราะการที่เราประกาศออกไปปาวๆ ว่ากำลังจะไปเที่ยวในวันหยุดสุดสัปดาห์ แต่กลับปล่อยให้ข้อมูลที่อยู่ลอยค้างเติ่งอยู่บนโซเชียลมีเดีย สิ่งนี้ก็คงไม่ต่างจากการบอกให้บรรดามิจฉาชีพรู้ความเคลื่อนไหวของเราและแอบมายกเค้าทรัพย์สินในบ้านเราแบบสนุก

Step 2 อย่าโพสต์รูปที่แสดงทรัพย์สินภายในบ้าน ในโลกออนไลน์ : คนรวยอยากจะโชว์ความมั่งคั่งบ้างแล้วผิดตรงไหน ยิ่งทรัพย์สินมีค่าภายในบ้านมีมาก ก็ยิ่งอยากจะประกาศให้คนทั้งโลกได้เห็น แต่ความคิดแบบนี้ถือว่าผิดมหันต์ เพราะอาจนำไปสู่การวางแผนของบรรดามิจฉาชีพให้เข้ามาคอยสอดส่องลักลอบยกเค้าทรัพย์สินของท่านจนหมดบ้านในเวลาที่ท่านนอนหลับหรือไม่อยู่บ้านก็เป็นได้

Step 3 อย่าเปิดเผยจุดหมายปลายทางบนโลกออนไลน์ : เดินทางไปท่องเที่ยวบ้านญาติหรือคนรู้จัก เห็นว่าตกแต่งสวยงาม พื้นที่กว้างขวางและมีสวนสนามหญ้าให้วิ่งเล่น จนเกิดความรู้สึกอยากจะถ่ายรูปมาเก็บไว้ดูเล่น และแบ่งปันให้เพื่อนชาวโซเชียลมีเดีย พร้อมกับเช็กอินสถานที่ให้เพื่อนๆ ได้ดูกันเดี๋ยวนั้น แต่หารู้ไหมว่า พฤติกรรมดังกล่าวนั้นเป็นหนทางเสี่ยงไปสู่การวางแผนร้ายของบรรดามิจฉาชีพที่อาจจะกำลังคอยดักส้วงสับตับแตกข้อมูลที่ตั้งของคุณอยู่ ทางที่ดีควรรู้จักอดใจกันสักนิด ไว้รอกลับมาถึงบ้านก่อนค่อยอัพโหลดรูปภาพให้เพื่อนฝูงดูก็ยังทัน

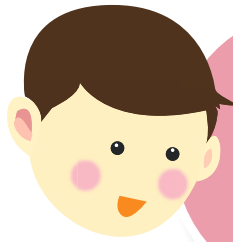


คิดก่อนโพสต์ เช็กก่อนแชร์
สร้างความมั่นคงปลอดภัยในโซเชียลมีเดีย

ไม่นำเรื่องภายในบริษัทมาเปิดเผย : การทำงานภายในองค์กรอาจจะมีเรื่องขัดแย้งหรือความคิดเห็นไม่ตรงกันบ้าง แต่หากอยากจะระบายก็ไม่ควรมาทำบนโลกโซเชียลมีเดีย เพราะสักวันหนึ่งเพื่อนร่วมงานหรือหัวหน้างานที่เราไม่ลงรอยด้วย อาจมาพบเห็นข้อความเหล่านี้โดยบังเอิญ ซึ่งก็อาจจะส่งผลถึงความมั่นคงปลอดภัยในชีวิตการงานของเราก็เป็นได้

น้องพุดดิ้งชวนรู้

ทั้ง 3 Step ที่นำมาเป็นหัวข้อตัวอย่างให้เพื่อนๆ ได้อ่านนั้น พุดดิ้งอ่านแล้วรู้สึกสนุกมาก เพราะได้ทั้งสาระและได้ทั้งข้อคิดต่างๆ มากมาย แม้จะเป็นการผูกเนื้อหาจากการใช้ครอบครัวของพุดน้อยในการเล่าเรื่อง แต่ทั้งนี้เพื่อนๆ ก็สามารถนำไปปรับใช้ เพื่อให้สามารถพึงระวังภัยได้ในชีวิตจริงนะคะ



อันตราย
จากการถูกคุกคาม
ความเป็นส่วนตัวในโลกออนไลน์
เจอแล้วเลี่ยงยาก แต่หากปรับเปลี่ยน
นิสัยการใช้งาน ก็สามารถสร้างความ
มั่นคงปลอดภัยในชีวิตได้ไม่ยาก

3.6 9 พฤติกรรมเสี่ยงอันตราย เรื่องง่ายๆ ที่ไม่ควรมองข้าม

พุดน้อยว่าเป็นสิ่งที่ยากพอสมควรสำหรับการหักห้ามใจไม่ให้ทดลองลูกเล่นใหม่ๆ ในโซเชียลมีเดีย เพราะแต่ละโปรแกรมต่างพากันพัฒนาเสริมให้ผู้ใช้บริการเล่นกันมากขึ้นเรื่อยๆ เช่น เกม แชต หรือการเล่นเกมแบบสอบถามสนุกๆ ซึ่งแรกเริ่มก็มีเพียงแค่การเปิดให้โพสต์ข้อความหรืออัพโหลดรูปภาพได้เท่านั้น ซึ่งความเพลิดเพลินที่มากขึ้นในระดับนี้ทำให้บางครั้งพุดน้อยเกือบจะลืมตัวไปว่านั่นเป็นพฤติกรรมที่เสี่ยงอันตรายกับเราอย่างมาก แม้ว่าจะสนุกก็ตามที เพราะไม่ว่าจะเป็นโปรแกรมเสริมชนิดใด ผู้พัฒนาก็ล้วนแล้วแต่ต้องการข้อมูลความเป็นส่วนตัวของเราเป็นการแลกเปลี่ยนด้วยกันทั้งนั้น ครั้งนี้พุดน้อยจึงได้รวบรวม 9 พฤติกรรมเสี่ยงอันตราย ที่ผู้ใช้โซเชียลมีเดียอย่างเราควรรับรู้และระวังไว้มาฝากกัน

9 พฤติกรรมออนไลน์เสี่ยงอันตราย ที่ไม่ควรมองข้าม

1. การเช็กอินเพื่อบอกสถานที่อยู่ตลอดเวลา : นับเป็นความสนุกสนานเพลิดเพลินรูปแบบหนึ่ง ที่หนุ่มๆ สาวๆ ชาวโซเชียลนิยมใช้กัน เพื่อแสดงสถานที่ให้แก่คนที่รู้จัก เช่น เช็กอินบอกสถานที่ท่องเที่ยว บอกสถานที่ทำงาน บอกที่พัก แต่หารู้ไม่ว่าการเช็กอินบอกสถานที่โดยไร้ซึ่งขอบเขตเช่นนี้ อาจถูกใช้เป็นเบาะแสให้ผู้ไม่ประสงค์ดี นำมาสะกดรอยตามเรา ซ้ำร้ายอาจจะส่งผลร้ายต่อร่างกายและทรัพย์สินของเราได้

2. แชร์รูปส่วนตัวในที่สาธารณะ : ใครมีรูปสวยๆ ก็อยากโชว์ เช่น รูปตนเอง รูปแฟน รูปครอบครัว หรือรูปลูกหลานภายในบ้าน แต่บางครั้งการโพสต์รูปบ่อยๆ บวกกับการโชว์สถานที่ (Location) เข้าไปอีก สิ่งนี้อาจกลายเป็นการส่งสัญญาณให้มิจฉาชีพในโลกออนไลน์ให้รับรู้ ว่าควรจะเริ่มต้นสะกดรอยตามคุณและคนใกล้ชิดอย่างไร ภัยใกล้ตัวลักษณะนี้ หลายคนมองไม่เห็น แต่หากวันใดเกิดกับตัวคุณเองหรือคนใกล้ตัว เช่น ลูกหลานในบ้าน อาจจะคิดว่าสายไปเสียแล้วก็ได้

3. โชว์สถานะเป็นสาธารณะ : เรื่องง่ายๆ ที่ไม่ควรมองข้ามอีกประการก็คือ การเป็นคนที่มีนิสัยใจกว้าง ตั้งต้นเป็นบุคคลสาธารณะ (Public) ไม่ว่าจะใครก็อนุญาตให้สามารถเห็นความเคลื่อนไหวของเราได้หมด ทั้งเพื่อน เพื่อนของเพื่อน และเพื่อนของเพื่อนในโซเชียลมีเดีย แต่ทางที่ดีควรปรับเปลี่ยนสถานะให้เป็นส่วนตัว (Privacy) ดีกว่า เพื่อความมั่นคงปลอดภัยในโลกออนไลน์นะครับ

4. เปลี่ยนรหัสผ่านทุก 3 เดือน : แม้ว่าเราจะมีการตั้งรหัสผ่านที่มั่นใจว่ายากต่อการคาดเดาแล้ว แต่ทั้งนี้เราจะมั่นใจได้อย่างไรว่า รหัสผ่านที่ตั้งไว้นั้นไม่เคยหลุดลอดออกไปให้ใครทราบ ดังนั้นจึงควรมีการเปลี่ยนรหัสผ่านทุก 3 เดือน เพื่อสร้างความมั่นคงปลอดภัยอย่างต่อเนื่องให้กับตนเองด้วยครับ

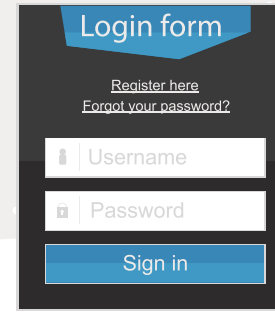
5. ให้ข้อมูลส่วนตัวกับเว็บไซต์ที่ใช้บริการ : พุดน้อยขอย้ำอีกครั้งว่าในโลกออนไลน์นี้มีภัยที่น่ากลัวอยู่รอบด้าน ไม่เว้นแม้แต่การให้ข้อมูลส่วนตัวกับเว็บไซต์ที่ใช้บริการ ซึ่งนับเป็นพฤติกรรมที่สุ่มเสี่ยงอันตรายมากในโลกออนไลน์ที่เราไม่ควรมองข้าม เพราะเราไม่สามารถมั่นใจได้เลยว่าเว็บไซต์เหล่านั้นจะไม่นำข้อมูลส่วนตัวของเราไปแชร์หรือส่งต่อไปถึงมือผู้ที่ไม่ประสงค์ดีหรือเปล่า

6. ไม่กำหนดสิทธิ์ในการเข้าถึงข้อมูล : นับเป็นพฤติกรรมที่สุ่มเสี่ยงต่อการที่ผู้ใช้งานจะถูกคุกคามหรือก่อให้เกิดความไม่มั่นคงปลอดภัยต่อชีวิตและทรัพย์อีกเช่นกัน อันเนื่องมาจากการเปิดเผยตัวตนหรือเปิดเผยข้อมูลส่วนบุคคลว่าผู้ใช้งานเป็นใคร

7. อ่านเงื่อนไขการให้บริการ : เป็นลักษณะความเคยชินของผู้ใช้บริการโซเชียลมีเดียส่วนใหญ่ ที่มักจะไม่อ่านเงื่อนไขการให้บริการจากโปรแกรมเสริมที่เราเลือกมาติดตั้ง เพราะโดยส่วนใหญ่เห็นว่าเป็นเงื่อนไขข้อตกลงที่เป็นภาษาอังกฤษ และชื่นชอบความรวดเร็ว สะดวกสบาย ซึ่งพฤติกรรมเช่นนี้อาจเป็นการนำไปสู่การถูกคุกคามความเป็นส่วนตัวโดยที่เราไม่รู้ตัว

8. ตรวจสอบการแชร์/ส่งต่อภาพ/ข้อความก่อนส่งต่อ : จัดเป็นภัยที่มาจากความรู้เท่าไม่ถึงการณ์ของตัวผู้ใช้บริการเอง เช่น การไม่ตรวจสอบที่มาของรูปภาพหรือข้อมูลที่แน่ชัด ก่อนจะทำการส่งแชร์ต่อไปยังผู้อื่น ซึ่งมีความผิดตามพระราชบัญญัติว่าด้วยการทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

9. บอกรหัสผ่านให้กับผู้อื่น : อย่าเชื่อใจหรือบอกรหัสผ่านให้กับผู้อื่นรู้ง่ายๆ แม้ว่าบุคคลนั้นจะเป็นที่รู้จักและสนิทกับเรามากแค่ไหนก็ตาม แต่หากจำเป็นต้องบอกรหัสผ่านก็ให้ย้อนกลับปฏิบัติตามข้อที่ 4 (เปลี่ยนรหัสผ่านทุก 3 เดือน) เท่านี้ความมั่นคงปลอดภัยก็จะกลับมาหาเราอีกครั้ง

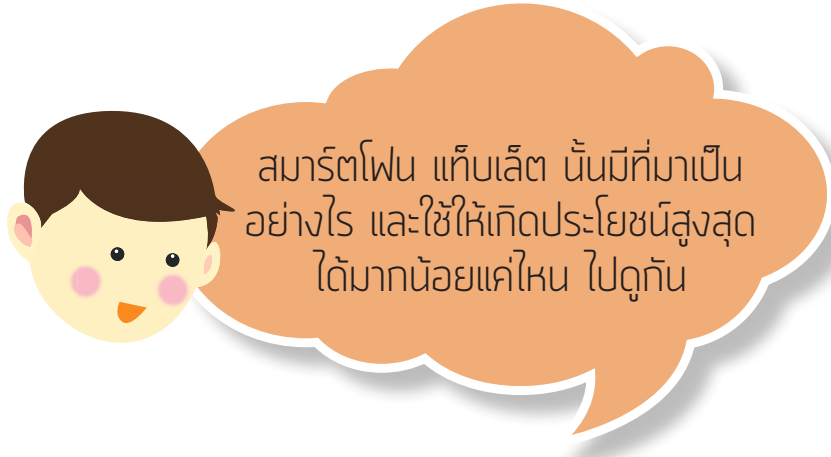


น้องพุดดิ้งชวนรู้

ทั้งหัวข้อ *"สิ่งที่พึงระวังบนโลกสังคมออนไลน์"* และ 9 พฤติกรรมออนไลน์เสี่ยงอันตราย ที่ไม่ควรมองข้าม" ที่หยิบยกมาให้เพื่อนๆ ได้ศึกษากัน หากทำความเข้าใจให้ดี ประโยชน์ทั้งหมดจะมีเนื้อหาที่สอดคล้องกัน ซึ่งท้ายที่สุดแล้ว ก็คือ การนำเสนอเนื้อหาที่ต้องการเน้นย้ำให้เพื่อนๆ ผู้อ่านนำไปปฏิบัติใช้อย่างเคร่งครัด สร้างความมั่นคงปลอดภัยกับตัวผู้ใช้งานบนโลกออนไลน์

บทที่ 4

มือถือ-แท็บเล็ต
อินเทอร์เน็ตในมือ
เข้าถึงได้ทุกเมื่อ



4.1 อินเทอร์เน็ตบนสมาร์ตโฟน-แท็บเล็ต

สมาร์ตโฟน และแท็บเล็ต เพื่อนนักอ่านคงรู้จักกันดี อีกทั้งพุดน้อยได้เคยอธิบายถึงความหมายของสมาร์ตโฟน และแท็บเล็ต ผ่านหนังสือฉลาดรู้เน็ต 1 ตอน Internet of Things (IoT) มาแล้ว แต่พุดน้อยก็เชื่อว่ายังมีเพื่อนนักอ่านอีกจำนวนมากที่ยังไม่รู้จักความหมายของอุปกรณ์ 2 ชนิดนี้ดีพอ ในบทนี้พุดน้อย จึงอยากจะขอหยิบยกข้อมูลดีๆ มาให้ทุกคนได้ศึกษากันอีกครั้งนะครับ

ปัจจุบันสมาร์ตโฟนหรือแท็บเล็ตถือว่าเป็นอุปกรณ์คู่กายของคนทุกวัย เสมือนเป็นอวัยวะชิ้นที่ 33 และ 34 ไปแล้ว ซึ่งถ้ามองไปรอบๆ ตัวของพุดน้อยก็จะพบว่า ทั้งคุณพ่อ คุณแม่ คุณลุง คุณป้า คุณน้า คุณอา และเพื่อนๆ ของพุดน้อย เกือบทุกคนมีสมาร์ตโฟนหรือแท็บเล็ตอยู่อย่างน้อยคนละ 1 เครื่องแน่ๆ เอาละ! ลองมาดูกันว่าทำไมเจ้าอุปกรณ์สองชิ้นนี้ถึงได้ฮอตฮิตขนาดนี้

สมาร์ตโฟน

สมาร์ตโฟน เป็นอุปกรณ์การสื่อสารหลักที่เราเกือบทุกคนมีใช้ ซึ่งล่าสุดถูกพัฒนาขึ้นจนทำให้โทรศัพท์เครื่องไม่กี่พันบาท ก็สามารถเล่นได้อย่างเพลิดเพลิน **โดยสมาร์ตโฟนถือเป็นการรวมตัวกันระหว่างโทรศัพท์มือถือและอุปกรณ์อิเล็กทรอนิกส์พกพาขนาดเล็ก** ที่เรียกย่อๆ ว่า PDA (Personal Digital Assistant) ซึ่งมีความแตกต่างจากมือถือทั่วไปตรงที่สามารถยัดใส่ฟังก์ชันการทำงานได้มากมาย อาทิ กล้องดิจิทัล เข็มทิศ แผนที่ หน้าจอระบบสัมผัส ซึ่งเพลินกว่าการกดปุ่มโทรศัพท์มือถือแบบเดิมๆ แถมยังมีให้ดาวน์โหลดแอพพลิเคชันเกมสนุกๆ เพื่อช่วยให้การเล่นโทรศัพท์ในยุคนี้มีสีสันมากขึ้น

ปัจจุบันมีสมาร์ตโฟนให้เลือกใช้มากมาย หลากหลายรุ่น หลายยี่ห้อ ราคาก็มีตั้งแต่หลักพันไปจนถึงหลักหลายหมื่นบาท โดยเราสามารถแบ่งสมาร์ตโฟนตามระบบปฏิบัติการได้ 3 รูปแบบ ได้แก่ iOS, Android และ Windows ส่วนใครชอบแบบไหนก็เลือกใช้กันตามสะดวกเลยครับ

แท็บเล็ต

แท็บเล็ตหรือบางคนเรียกว่า กระดานชนวนอิเล็กทรอนิกส์ ถือเป็นอุปกรณ์ไอทีที่ได้รับความนิยมมากพอๆ กับสมาร์ตโฟนเลยทีเดียว ในที่นี้พูดน้อยจะพาย้อนอดีตไปสักนิดครับ แต่เดิมแท็บเล็ตยังไม่ได้มีหน้าตาเหมือนทุกวันนี้ เพราะแต่ก่อนแท็บเล็ตคืออุปกรณ์ที่ใช้ทำงานเฉพาะทางในงานด้านวิศวกรรมและการขนส่ง ส่วนสเปกภายในก็ใช้อุปกรณ์แบบเดียวกับโน้ตบุ๊กหรือเครื่องพีซี จึงทำให้แท็บเล็ตไม่ค่อยได้รับความนิยมเท่าที่ควร

จนมาถึงยุคปัจจุบัน บรรดาบริษัทต่างๆ ต่างก็ได้ทำการปรับตัวและพัฒนาให้แท็บเล็ตกลายเป็นอุปกรณ์ไอทีที่ใช้ง่ายขึ้น เช่น ให้มีรูปร่างที่บาง เบา หน้าตาทันสมัย และมีการใช้งานที่ง่าย ตอบสนองการใช้งานทั่วไป และที่สำคัญคือ เน้นใช้ประโยชน์ด้านความบันเทิงเป็นหลัก เช่น ถ่ายรูปคมชัด ดูหนัง ฟังเพลง สื่อสารผ่านการแชตกับเพื่อนๆ ได้สะดวก เหตุนี้จึงทำให้แท็บเล็ตได้รับความนิยมแบบถล่มทลายอย่างที่ไม่เคยมีมาก่อน ทั้งยังมีให้เลือกหลายยี่ห้อ หลายขนาด และแบ่งประเภทตามระบบปฏิบัติการที่ใช้เหมือนกับสมาร์ตโฟน คือ iOS, Android และ Windows

การใช้อินเทอร์เน็ตบนสมาร์ตโฟนและแท็บเล็ต

เมื่อเปรียบสมาร์ตโฟนและแท็บเล็ตเป็นเสมือนร่างกาย อินเทอร์เน็ตก็คงไม่ต่างจากสารอาหารที่หล่อเลี้ยงให้อุปกรณ์สองประเภทนี้ขับเคลื่อนและดูมีชีวิตชีวามากขึ้น นั่นก็เพราะอินเทอร์เน็ตช่วยให้สมาร์ตโฟนและแท็บเล็ตสามารถทำงานได้อย่างเต็มที่ ทั้งดูหนัง ฟังเพลง โหลดแอพท่องเน็ต เข้าเว็บไซต์ หรือแชตได้จากทุกที่ทุกเวลา

โดยอินเทอร์เน็ตที่ใช้กันอยู่ก็มีทั้งรูปแบบเป็นแพ็กเกจจากผู้ให้บริการ และรูปแบบการเชื่อมต่อกับ WiFi ตามบ้านหรือ WiFi สาธารณะ เป็นต้น

LINE โหลดง่าย ใช้คล่อง

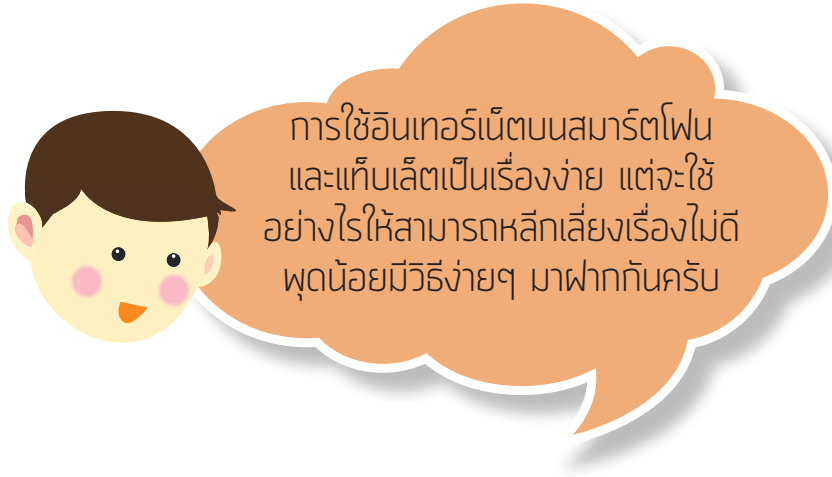
หากจะให้พุดน้อยหยิบยกตัวอย่างแอพพลิเคชันสำหรับการสื่อสารที่คนไทยนิยมใช้มากที่สุดในขณะนี้ ก็คงหนีไม่พ้น “LINE” ส่วนการดาวน์โหลดก็ไม่ยากครับ

- ☑ ผู้ที่ใช้บริการระบบ iOS ดาวน์โหลดได้ที่ App Store
- ☑ ผู้ที่ใช้บริการระบบ Android ดาวน์โหลดได้ที่ Play Store
- ☑ ผู้ที่ใช้บริการระบบ Windows ดาวน์โหลดได้ที่ Windows Store

ส่วนการเริ่มต้นใช้งานแนะนำว่าให้ลงทะเบียน (Register) ด้วย E-mail แล้วทำตามขั้นตอนจนลงทะเบียนเสร็จ โดยระบบจะทำการดึงชื่อเพื่อนในเบอร์โทรศัพท์ซึ่งกำลังใช้ LINE อยู่เหมือนกันมาแสดง หรือจะใช้วิธีการค้นหาจาก ID ที่เพื่อนให้มาก็ได้ครับ

น้องพุดดิ้งชวนรู้

ข้อมูลที่พุดน้อยนำมาให้ศึกษากัน พุดดิ้งว่ายังแน่นปึ้กเหมือนเดิมเลยนะคะ ส่วนเรื่องความน่าสนใจของสมาร์ตโฟนและแท็บเล็ตนั้น พุดดิ้งเห็นว่าในปัจจุบันแม้จะมีผู้นิยมใช้กันมากขึ้น แต่หากเราเลือกที่จะใช้โดยไม่ระมัดระวังและยืนอยู่บนความประมาท ก็อาจจะเป็นบ่อเกิดแห่งภัยร้ายที่จะส่งมาถึงตัวเราได้ ยกตัวอย่าง การโหลดซื้อแอพพลิเคชันกันจนเพลิน โดยเมื่อรู้สึกตัวอีกครั้งเงินในกระเป๋าก็พร่องหายไปจนเกือบจะกระเป๋าฉีกหมดแล้ว เป็นต้น



4.2 ตรวจจับความเสี่ยงเรื่องออนไลน์ในสมาร์ตโฟน-แท็บเล็ต

สมาร์ตโฟนและแท็บเล็ตเป็นอุปกรณ์ที่ต้องใช้งานคู่กับอินเทอร์เน็ต สำหรับดูหนัง ฟังเพลง ช้อปปิ้งออนไลน์ได้ทุกที่ ทุกเวลา แค่เพียงปลายนิ้วสัมผัส แต่รู้กันไหมว่าการใช้งานอินเทอร์เน็ตที่แสนจะเพลิดเพลินใจนั้นมีความเสี่ยงที่ต้องระวังอยู่ พุดน้อยจะพาไปดูกันว่าความเสี่ยง 5 อย่าง ที่เรามองไม่เห็นหรือละเลยไม่ได้ใส่ใจนั้น มีอะไรบ้าง

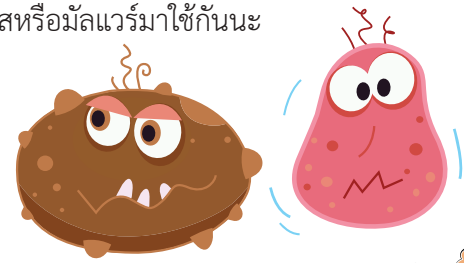
เสี่ยงที่ 1 ข้อตกลงการใช้งาน อ่านบ้างก็ดีนะ

เวลาเราใช้งานอินเทอร์เน็ตเพื่อดาวน์โหลดแอพพลิเคชัน ก่อนการติดตั้งจะมีการแสดง**ข้อตกลงการใช้งาน (Term of Service)** แสดงเป็นกรอบเล็กๆ น่ารักๆ หรือไม่ก็ยาวเหยียดจนไม่อยากอ่าน พร้อมกับมีปุ่ม “ยอมรับ” หรือ “Agree” ตัวโตๆ ให้เรารีบกดผ่านไป ซึ่งคนส่วนใหญ่จะรีบคลิกปุ่มดังกล่าวให้ผ่านไปโดยเร็ว

ถ้าคิดอย่างนี้ก็ผิดถนัดครับ เพราะข้อตกลงการใช้งานจะเป็นการแสดงว่าแอพพลิเคชันนั้นๆ มีข้อตกลงกับผู้ใช้อย่างไรบ้าง เช่น สามารถเข้าถึงข้อมูลผู้ใช้ได้แค่ไหน หรือสามารถแชร์ข้อความออกไปโดยไม่ต้องขออนุญาต รวมไปถึงการเก็บข้อมูลส่วนตัวของผู้ใช้โดยที่ไม่ต้องบอกล่วงหน้า รู้อย่างนี้แล้วครั้งต่อไปอ่าน ข้อตกลงการใช้งานสักนิดจะได้ไม่ต้องมานั่งปวดหัวทีหลังนะครับ

เสี่ยงที่ 2 ไวรัส...วายร้าย

ไม่ว่าจะเป็นคอมพิวเตอร์ สมาร์ตโฟนหรือแท็บเล็ตต่างก็ไม่สามารถหนีพ้นไวรัสไปได้ครับ ซึ่งรูปแบบไวรัสของสมาร์ตโฟนและแท็บเล็ตจะมาในรูปแบบที่เรียกว่ามัลแวร์ ส่วนใหญ่จะเป็นการขโมยข้อมูลส่วนตัวของผู้ใช้ผ่านการติดตั้งแอพพลิเคชัน นอกจากนี้ ไวรัสยังอาจจะมาในรูปแบบการส่งผ่านไวรัสไปยังผู้ใช้คนอื่นๆ และส่งต่อไปจนถึงเป้าหมายที่แฮกเกอร์ต้องการ ส่วนการป้องกันก็ง่ายๆ คือ อย่าดาวน์โหลดแอพพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ อย่าเห็นแก่ของฟรีจนลืมตัว และสุดท้าย อย่าลืมดาวน์โหลดแอพพลิเคชันสำหรับป้องกันไวรัสหรือมัลแวร์มาใช้กันนะ



เสี่ยงที่ 3 สินค้าออนไลน์ เช็กให้ชัวร์ก่อนซื้อ

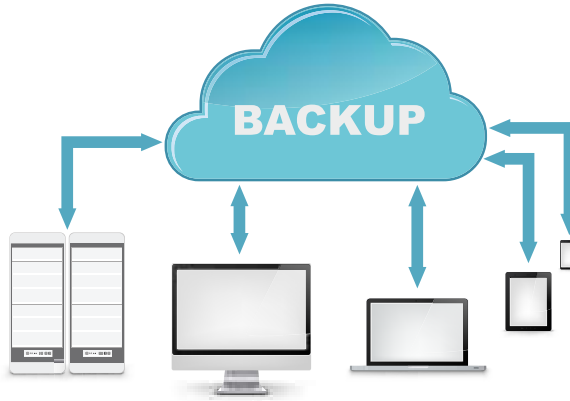
เรื่องการซื้อของออนไลน์แล้วถูกโกง เราเห็นข่าวตามหน้าหนังสือพิมพ์กันเป็นประจำ โดยวายร้ายจะใช้ความอยากของคนเป็นตัวกระตุ้นในการสั่งซื้อ แล้วบอกว่าของที่สั่งจะถูกกว่าที่อื่น สั่งปุ๊บได้ปั๊บ และยังมีสีหรือลวดลายที่หายากอีก

ดังนั้น หากต้องการจะซื้อสินค้าออนไลน์ ก็ควรซื้อจากร้านที่น่าเชื่อถือ เช่น เว็บไซต์ขายสินค้าออนไลน์อย่าง eBay หรือ Amazon ถ้าเป็นเว็บไซต์ดังในบ้านเราก็เป็น Tarad.com หรือจะเป็นเว็บไซต์ Thaiemarket.com ของ ETDA โดยร้านค้าออนไลน์ที่ดีจะมีการจดทะเบียนกับกรมพัฒนาธุรกิจการค้า และจะแสดงเลขการจดทะเบียนที่หน้าเว็บไซต์อย่างชัดเจน

แต่สำหรับร้านค้าบนสื่อโซเชียลเน็ตเวิร์ก บางร้านอาจจะไม่มีเลขทะเบียนการค้า เพราะไม่มีที่ตั้งชัดเจน เนื่องจากเป็นการตั้งร้านค้าแบบประหยัด วิธีการเลือกร้านค้าแบบนี้ ก่อนอื่นจึงต้องเข้าไปดูคอมเมนต์ในแฟนเพจก่อนว่า มีคนมาแสดงความเห็นอย่างไรบ้าง เป็นแนวบวกหรือลบ มีโพสต์แสดงการส่งสินค้าที่ชัดเจนไหม เช่น การส่งของจะโพสต์ชื่อผู้รับพร้อมเลขที่ EMS เพื่อตรวจสอบได้

เสี่ยงที่ 4 อย่าลืมทิ้งร่องรอยให้โทรศัพท์มือถือ

ด้วยเทคโนโลยีที่ล้ำหน้าแบบสุดๆ ลองตรวจสอบว่าระบบปฏิบัติการบนมือถือของเรามีบริการติดตามตำแหน่งที่ตั้งหรือไม่ ถ้ามีก็ควรเปิดใช้งาน หรือถ้าไม่มีก็ไปดาวน์โหลดมาครับ เช่น Windows ที่มีแอพพลิเคชัน Find My Phone, iOS ที่มี Find My iPhone และ Android ที่มี Android Device Manager โดยบริการเหล่านี้จะช่วยให้เราสามารถค้นหาตำแหน่งที่อยู่ของโทรศัพท์มือถือของเราบนแผนที่ออนไลน์ได้ หรือถ้าหาไม่เจอแอพพลิเคชันเหล่านี้ก็ยังสามารถสั่งล็อกโทรศัพท์ และลบข้อมูลทั้งหมดได้โดยการสั่งงานผ่านระบบรีโมท อย่างน้อยคิดซะว่าเสียเครื่องดีกว่าถูกนำข้อมูลไปใช้ครับ

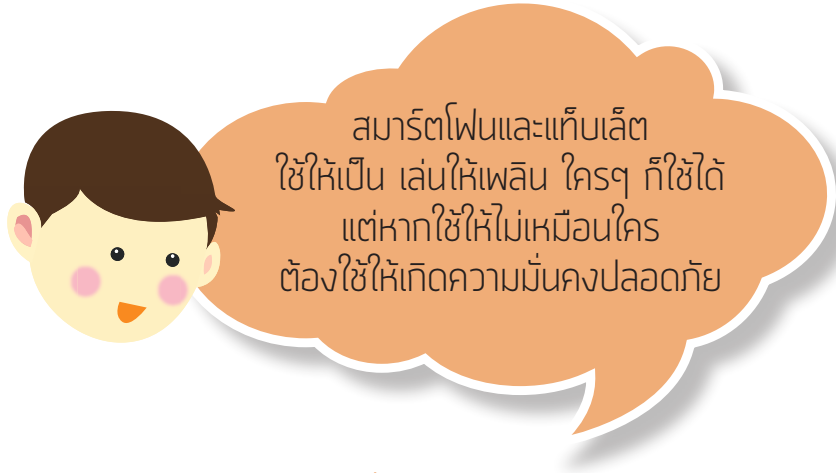


เสี่ยงที่ 5 สำรองข้อมูลให้เกิดความเคยชิน

แอพพลิเคชันบนสมาร์ตโฟนรุ่นใหม่ๆ จะมีความสามารถในการเก็บข้อมูลของเครื่อง เช่น เบอร์โทรศัพท์ รูปภาพ และข้อมูลที่จำเป็นอื่นๆ ไปไว้บนอินเทอร์เน็ต เช่น iCloud ของ iOS ถ้าโทรศัพท์ของเรามีแอพพลิเคชันเหล่านี้อยู่ให้รีบเปิดใช้งานโดยทันที และสั่งให้โปรแกรมทำงานอัตโนมัติ เรียกว่าถ้ามีข้อมูลใหม่ก็สามารถอัพโหลดได้เรื่อยๆ ทีนี้เราก็สบายใจได้ว่าถ้าโทรศัพท์หายหรือถูกขโมย เรายังสามารถดึงข้อมูลทั้งหมดกลับมาได้ทันที ไม่ต้องเสียเวลามานั่งขอเบอร์เพื่อนใหม่ เรียกว่ามีประโยชน์สุดๆ

น้องพุดดิ้งชวนรู้

กรณีความเสี่ยงจากข้อมูลที่พุดน้อยนำมาให้ ทำให้พุดดิ้งเล็งเห็นในเวลาที่ผ่านมาได้ทำผิดพลาดอะไรไปบ้าง นับแต่นี้ไปพุดดิ้งสัญญาว่าจะระมัดระวังในการใช้สมาร์ตโฟนและแท็บเล็ตมากขึ้น โดยเฉพาะการซื้อของผ่านร้านค้าออนไลน์ที่พุดดิ้งในฐานะผู้หญิงคนหนึ่ง จะเช็กข้อมูลทุกอย่างแบบละเอียดถี่ถ้วน และจะนำข้อมูลดีๆ เหล่านี้ไปบอกต่อคนรู้จัก เพื่อให้ทุกคนได้ฝึกปฏิบัติตามขั้นตอนกันอยู่เรื่อยๆ จนเกิดความเคยชินติดตัวไปเลยค่ะ



4.3 ใช้มือถืออย่างไรให้มั่นคงปลอดภัยจากภัยคุกคาม

ในบทนี้พุดน้อยขอแนะนำบทความดีๆ จากเว็บไซต์ www.thaicert.or.th ที่พุดน้อยไปพบโดยบังเอิญ และคิดว่ามีความสำคัญอย่างมากสำหรับเพื่อนๆ ที่ใช้สมาร์ตโฟนในปัจจุบัน จากบทความเรื่องแนวทางการใช้งานโทรศัพท์มือถือให้มั่นคงปลอดภัยจากภัยคุกคาม มีเนื้อหาที่น่าสนใจดังนี้ครับ

เนื่องด้วยความเจริญก้าวหน้าของเทคโนโลยีการสื่อสาร ส่งผลให้มีผู้พัฒนาและผลิตโทรศัพท์เคลื่อนที่ หรือโทรศัพท์มือถือ ออกมาเป็นจำนวนมาก โดยแต่ละผู้พัฒนาก็มีแนวคิดคล้ายกันคือต้องการอำนวยความสะดวกให้ผู้ใช้งานมากที่สุด สังเกตได้จากสื่อโฆษณาทั่วไปที่มีการโฆษณาถึงความสามารถของโทรศัพท์มือถือในแต่ละฟังก์ชันการทำงาน เช่น สามารถเชื่อมต่อกับเครือข่ายไร้สายเพื่อความสะดวกในการเข้าถึงอินเทอร์เน็ตบนโทรศัพท์มือถือ สามารถรับชมวิดีโอบนโทรศัพท์มือถือเพื่อความบันเทิง เป็นต้น

แต่จากความสามารถและข้อดีหลายประการของโทรศัพท์มือถือก็ยังถูกเจือปนหรือแอบแฝงไปด้วยภัยอันตรายหรือภัยคุกคามหลายประการ ซึ่งผู้ใช้งานอีกจำนวนมากที่อาจจะยังไม่เคยทราบถึงภัยคุกคามจากการใช้งานโทรศัพท์มือถือ ส่งผลให้ผู้ไม่หวังดีสามารถโจมตีหรือขโมยข้อมูลต่างๆ ได้โดยง่าย เช่น การปลดล็อกโทรศัพท์มือถือเพื่อนำไปติดตั้งซอฟต์แวร์ผิดกฎหมาย ส่งผลให้ระบบปฏิบัติการบนโทรศัพท์มือถือมีช่องโหว่ เป็นต้น

1. ภัยคุกคามจากการใช้งานโปรแกรมบนโทรศัพท์มือถือ (Application-Based Threats)

โปรแกรมจำนวนมากที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนอุปกรณ์มือถือ พบว่ายังไม่สามารถตรวจสอบลักษณะการทำงานในด้านความมั่นคงปลอดภัยได้ ทำให้ผู้ใช้งานไม่สามารถล่วงรู้ได้เลยว่าโปรแกรมที่ติดตั้งไปเพื่อใช้ประโยชน์มากมายนั้น จะถูกแฝงมาด้วยปัญหาด้านความมั่นคงปลอดภัยหรือไม่ โดยภัยคุกคามที่มากับโปรแกรมที่ติดตั้งสามารถมีได้มากกว่าหนึ่งประเภทดังที่จะกล่าวต่อไปนี้

☑ มัลแวร์ (Malware) : คือโปรแกรมที่ถูกออกแบบมาเพื่อแสดงพฤติกรรมที่เป็นอันตรายต่อข้อมูลในโทรศัพท์มือถือนั้นๆ ตัวอย่างเช่น สั่งให้โทรศัพท์มือถือเครื่องนั้นๆ ส่งข้อความที่ไม่พึงประสงค์ออกไปยังรายการผู้ติดต่อในโทรศัพท์ โดยที่ผู้ใช้งานหรือเจ้าของโทรศัพท์นั้นไม่รู้ตัว หรือขโมยข้อมูลบนโทรศัพท์มือถือนั้น ซึ่งในกรณีที่ผู้ใช้งานเก็บข้อมูลบัญชีผู้ใช้ของตนเองหรือของผู้เกี่ยวข้องไว้ในโทรศัพท์ก็อาจทำให้เกิดการเข้าโจรกรรมข้อมูลที่เกี่ยวข้องต่อไปได้

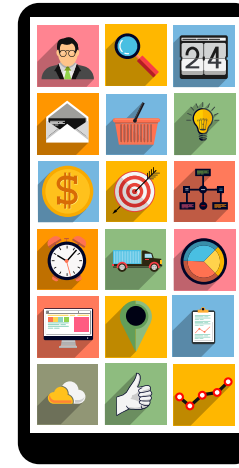
☑ สปายแวร์ (Spyware) : คือโปรแกรมที่ถูกออกแบบมาเพื่อเก็บรวบรวมข้อมูลต่างๆ ของผู้ใช้งาน โดยเป้าหมายส่วนใหญ่ของสปายแวร์มักมุ่งไปยังประวัติการใช้งานโทรศัพท์ ข้อความ ที่อยู่ รายชื่อผู้ติดต่อ อีเมล รวมถึงภาพถ่าย ซึ่งสปายแวร์โดยทั่วไปมักได้รับการออกแบบสำหรับการเฝ้าติดตามการใช้งานของบุคคลใดบุคคลหนึ่ง หรือการใช้งานที่เกี่ยวข้องกับองค์กร ทั้งนี้ขึ้นอยู่กับวิธีการที่จะใช้สปายแวร์ที่กำหนดเป้าหมาย ซึ่งไม่จำเป็นเสมอไปที่ผู้ลักลอบติดตั้งโปรแกรมประเภทนี้จะเป็นผู้มีจุดประสงค์ร้ายทั้งหมด เนื่องจากมีความเป็นไปได้ว่าโปรแกรมประเภทนี้ถูกติดตั้งโดยผู้ที่เป็นผู้ปกครองซึ่งมีความหวังดีต่อผู้ใช้งาน เช่น ผู้ปกครองติดตั้งโปรแกรมการตรวจสอบสถานที่การใช้งานบนโทรศัพท์มือถือของลูกที่อยู่ในการดูแล

เทคนิค Repackaging

นอกจากนี้การเข้าโจมตีผู้ใช้งานและโทรศัพท์มือถือด้วยมัลแวร์และสปายแวร์แล้ว บรรดาแฮกเกอร์ยังมีวิธีการหลอกลวงในลักษณะที่พบเห็นได้บ่อยครั้งคือ การ Repackaging ซึ่งเป็นเทคนิคที่พบบ่อยมากในนักเขียนมัลแวร์ที่พยายามจะใช้ชื่อโปรแกรมที่มีการทำงานถูกต้องตามกฎหมาย แต่ได้มีการปรับเปลี่ยนการทำงานของโปรแกรม รวมถึงแทรกโค้ดที่เป็นอันตรายไว้ในเวอร์ชันที่เตรียมจะเผยแพร่ จากนั้นจึงทำการเผยแพร่ไปยังแหล่งให้ดาวน์โหลดโปรแกรมต่างๆ ทั่วไป รวมถึงบนเว็บไซต์ที่ให้ดาวน์โหลดโปรแกรมบนโทรศัพท์มือถือ เพื่อหลอกให้ผู้ใช้งานเข้าใจผิดและติดตั้งโปรแกรมดังกล่าวบนโทรศัพท์มือถือ ซึ่งเทคนิคการ Repackaging ได้ผลลัพธ์ในการโจมตีค่อนข้างสูงเนื่องจากการอ้างอิงชื่อโปรแกรมที่เคยพัฒนา

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์บนโทรศัพท์มือถือ (Web-Based Threats)

เนื่องจากโทรศัพท์มือถือส่วนใหญ่สามารถใช้งานเชื่อมต่ออินเทอร์เน็ตได้จากเครือข่ายไร้สายทั่วไป ซึ่งทำให้เกิดความสะดวกสำหรับผู้ใช้งานในการเข้าถึงเว็บไซต์หรือบริการอื่นๆ ซึ่งโดยทั่วไปบริการส่วนใหญ่สามารถใช้งานผ่านหน้าเว็บไซต์ได้เป็นหลัก และเป็นบริการที่ผู้ใช้งานมีความต้องการใช้งาน เช่น การอ่านอีเมล การใช้งานธุรกรรมออนไลน์ การเข้าระบบที่เป็นสื่อสังคมออนไลน์ เป็นต้น โดยภัยคุกคามที่เกิดขึ้นกับเว็บไซต์มักไม่มีข้อจำกัดทางด้านระบบปฏิบัติการที่ใช้อยู่ ณ ขณะนั้น เช่น การโจมตีแบบฟิชชิ่ง ซึ่งจะกล่าวในรายละเอียดต่อไป โดยภัยคุกคามดังที่กล่าวนี้แต่ก่อนอาจพบว่ามีแต่ที่เจอในการใช้งานบนเครื่องคอมพิวเตอร์ทั่วไป ในปัจจุบันได้ขยายวงกว้างมายังโทรศัพท์มือถือด้วย เนื่องจากลักษณะการใช้งานที่ค่อนข้างจะใกล้เคียงกันมากในทุกวันนี้ โดยสามารถระบุภัยคุกคามต่างๆ ได้ดังนี้



ฟิชชิ่ง (Phishing) : คือการหลอกลวงชนิดหนึ่งโดยใช้หน้าเว็บไซต์หรือส่วนติดต่อผู้ใช้อื่นๆ ที่ออกแบบให้มีลักษณะคล้ายคลึงกับของจริง เพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้หลอกลวง เช่น ผู้หลอกลวงพัฒนาหน้าเว็บไซต์ล็อกอินของเฟซบุ๊ก และส่งลิงก์หลอกลวงโดยแจ้งข้อมูลอันเป็นเท็จให้ผู้ใช้งานเข้าอัพเดตข้อมูลส่วนบุคคลโดยเป็นลิงก์ของหน้าล็อกอินที่ทำขึ้นมาดังที่กล่าวไว้ตอนต้น เมื่อผู้ใช้งานพยายามล็อกอินเข้าไปยังระบบ จะทำให้ผู้หลอกลวงดังกล่าวสามารถดักจับข้อมูลอันน่าเชื่อได้ว่าเป็นข้อมูลล็อกอินของผู้ใช้งานคนนั้นๆ ทำให้ข้อมูลหรือบัญชีการใช้งานนั้นๆ มีความเสี่ยงที่จะโดนขโมยข้อมูลออกไป ซึ่งลิงก์ที่เป็นการฟิชชิ่งเหล่านี้ส่วนใหญ่มักจะแนบไปกับอีเมล หรือเป็นลิงก์ซึ่งมีเนื้อหาเชิญชวนต่างๆ โดยความรุนแรงของการถูกขโมยข้อมูลดังกล่าวอาจไม่ส่งผลกระทบในทันทีถ้าหากมีการเข้ายับยั้งได้ทัน เช่น เมื่อทราบว่าได้มีการส่งข้อมูลเข้าหน้าเว็บไซต์ฟิชชิ่งไปแล้ว ให้รีบเข้าไปเปลี่ยนรหัสผ่านในหน้าเว็บไซต์ของระบบจริงทันที ก็จะทำให้ความเสียหายเกิดขึ้นลดลง แต่หากผู้ใช้งานปล่อยให้ผู้หลอกลวงสามารถเข้าถึงบัญชีการใช้งานต่างๆ ซึ่งในกรณีที่เป็นระบบที่มีความเสียหายรุนแรง เช่น ระบบธุรกรรมออนไลน์ (e-Transaction) นั่นเท่ากับผู้หลอกลวงจะสามารถใช้เงินในบัญชีผู้ใช้งานนั้นได้ทันที

ช่องโหว่ของโปรแกรมประเภทเบราว์เซอร์ : เป็นช่องโหว่ที่ถูกพบในโปรแกรมเบราว์เซอร์หรือโปรแกรมปลั๊กอินที่สามารถติดตั้งเพิ่มเติมได้ในเบราว์เซอร์ เช่น Flash Player หรือ PDF Reader เพื่อวัตถุประสงค์อันตราย โดยลักษณะและวิธีการโจมตีอาจเป็นเพียงแค่การให้ผู้ใช้งานเข้าชมหน้าเว็บไซต์เท่านั้น จากนั้นจะทำให้ผู้ใช้งานติดมัลแวร์หรือโปรแกรมอันตรายต่างๆ ที่ผู้โจมตีใช้สำหรับช่องโหว่ดังกล่าว

3. ภัยคุกคามจากการใช้งานเครือข่าย (Network Threats)

โทรศัพท์มือถือในปัจจุบันมักจะสนับสนุนการใช้งานเครือข่ายไร้สาย ซึ่งมีผู้ให้บริการเป็นจำนวนมาก ทั้งที่น่าเชื่อถือและไม่สามารถตรวจสอบได้ โดยมีภัยคุกคามที่สามารถส่งผลกระทบต่อการใช้งานบนโทรศัพท์มือถือต่างๆ ได้ดังนี้

☑ **การเปลี่ยนสถานะจากผู้ใช้งานเป็นผู้โจมตี :** นับเป็นการผ่านข้อบกพร่องของระบบปฏิบัติการบนโทรศัพท์เคลื่อนที่ ส่งผลให้โทรศัพท์เคลื่อนที่สามารถส่งต่อหรือแพร่กระจายมัลแวร์ได้โดยอัตโนมัติผ่านการทำงานบนเครือข่าย เช่น เครือข่ายไร้สาย (WiFi) หรือบลูทูธ (Bluetooth)

☑ **การถูกดักจับข้อมูลบนเครือข่ายไร้สาย (WiFi Sniffing)** : คือ ลักษณะการขโมยข้อมูลบนเครือข่ายไร้สาย ซึ่งโดยทั่วไปเป็นข้อมูลที่รับส่งกันโดยไม่ได้มีการเข้ารหัสความมั่นคงปลอดภัยที่เหมาะสม ทำให้มีโอกาสถูกลักลอบขโมยข้อมูลได้โดยง่าย เพียงแค่ใช้เทคนิคและวิธีในการดักจับข้อมูลจากโปรแกรมประเภท Sniffer ซึ่งหาข้อมูลได้ตามเว็บไซต์ทั่วไป โดยในที่นี้ขอยกตัวอย่างวิธีการใช้งานโปรแกรมชื่อ Firesheep ซึ่งเป็นปลั๊กอินบนเบราว์เซอร์ Firefox ที่ใช้ในการดักจับข้อมูลในเครือข่ายเดียวกัน ซึ่งส่วนใหญ่เป้าหมายมักใช้งานเครือข่ายไร้สายสาธารณะ และไม่ได้เชื่อมต่อบริการเว็บไซต์ที่มีการเข้ารหัส HTTPS โดยลักษณะการทำงานของโปรแกรมจะมีการดักจับข้อมูลแล้วกรองข้อมูลเพื่อค้นหา Cookie ซึ่งคือข้อมูลที่ใช้ระบุตัวตนกับเว็บไซต์ที่เข้าใช้บริการ โดยข้อมูล Cookie ที่กล่าวถึงจะถูกเก็บไว้ในเบราว์เซอร์ของผู้ใช้งานหลังจากที่มีการล็อกอินเว็บไซต์ จากนั้นโปรแกรมจะแสดงรายการที่ดักจับได้ทั้งหมด ซึ่งผู้ใช้งานโปรแกรมสามารถคลิกที่รายการดังกล่าวเพื่อสวมรอยเข้าเป็นผู้ใช้งานนั้นๆ ได้

4. ภัยคุกคามจากการดูแลรักษาโทรศัพท์ (Physical Threats)

เนื่องจากโทรศัพท์มือถือเป็นอุปกรณ์ซึ่งออกแบบให้พกพาและติดตัวไปมาได้สะดวก จึงมีรูปแบบที่ค่อนข้างเล็ก ซึ่งจากสภาพการณ์ปัจจุบันโทรศัพท์เป็นของมีค่าสำหรับมิจฉาชีพ รวมไปถึงมีค่าสำหรับกลุ่มคนบางกลุ่มที่ต้องการได้มาซึ่งข้อมูลส่วนบุคคล จึงได้แยกภัยคุกคามที่เกิดจากการดูแลรักษาโทรศัพท์มือถือไว้เพื่อพิจารณาความสำคัญอยู่ 2 ประเภทดังนี้

การสูญหายหรือการถูกขโมยโทรศัพท์มือถือ เนื่องด้วยปัจจุบันโทรศัพท์มือถือมีราคาสูงขึ้น อาจเพราะสาเหตุของเทคโนโลยีที่อยู่ในอุปกรณ์โทรศัพท์มือถือ หรือเพราะค่านิยมทางสังคมที่ทำให้ต้องใช้โทรศัพท์มือถือราคาแพง แต่ไม่ว่าจะกรณีไหนก็ตามการใช้งานโทรศัพท์มือถือในปัจจุบันนับเป็นเป้าหมายของกลุ่มมิจฉาชีพทั่วไป เนื่องจากเป็นอุปกรณ์พกพาขนาดเล็ก มีโอกาสถูกขโมยได้ง่าย และมีตลาดที่มีความต้องการหรือรองรับการซื้อขายได้มากมายโดยที่ไม่มีการตรวจสอบแหล่งที่มา ทำให้มีความเสี่ยงสูงที่ผู้ใช้งานจะมีโอกาสถูกกลุ่มมิจฉาชีพขโมยโทรศัพท์มือถือหรือด้วยขนาดของอุปกรณ์มือถือที่เล็กอยู่แล้วอาจทำให้มีโอกาสที่จะลืมหรือทำตกหล่นได้ง่าย

การถูกขโมยข้อมูลส่วนบุคคล สามารถเกิดขึ้นได้ตลอดเวลาและทุกสถานการณ์ทั้งโดยตั้งใจแต่แรกหรือเป็นเพราะโอกาสที่เปิดกว้างจนทำให้ผู้อื่นสบโอกาสที่จะขโมยข้อมูลส่วนบุคคล มักเกิดขึ้นจากความไม่ใส่ใจและความไม่ตระหนักถึงความมั่นคงปลอดภัยของข้อมูลภายในโทรศัพท์มือถือ ทำให้ผู้ไม่หวังดีขโมยข้อมูลส่วนบุคคลไปได้โดยง่าย เช่น การแอบดูข้อมูลการล็อกอินเข้าสู่ระบบจากโทรศัพท์มือถือ หรือการนำโทรศัพท์มือถือไปซ่อมที่ร้านโดยไม่ได้ทำการเคลียร์ข้อมูลการใช้งานก่อน โดยข้อมูลส่วนบุคคลที่หมายถึงอาจไม่ใช่เพียงข้อมูลส่วนตัวเพียงเท่านั้นแต่จะพบว่าเป็นข้อมูลขององค์กรด้วย อาจเป็นเอกสารขององค์กร ข้อมูลรายชื่อผู้ติดต่องาน รวมไปถึงข้อมูลที่อยู่ในระบบต่างๆ เช่น ข้อมูลบัญชีธนาคาร ข้อมูลอีเมลขององค์กร ซึ่งข้อมูลทั้งหมดที่กล่าวมานั้นหากถูกขโมยข้อมูลขึ้นมาจริงๆ แล้ว คงไม่สามารถประเมินมูลค่าความเสียหายได้อย่างแน่นอน

11 วิธีง่ายๆ ในการใช้โทรศัพท์มือถืออย่างมั่นคงปลอดภัย

1. ดูแลรักษาโทรศัพท์มือถืออย่างใกล้ชิด
2. ตั้งค่าการล็อกโทรศัพท์มือถือเมื่อไม่ใช้งาน
3. สำรองข้อมูลจากโทรศัพท์มือถือไว้ในแหล่งอื่นที่ปลอดภัย
4. พิจารณาเก็บเฉพาะข้อมูลที่จำเป็นในโทรศัพท์มือถือ
5. ปิดโหมดการเชื่อมต่อบลูทูธหรือหลีกเลี่ยงการเชื่อมต่อบลูทูธจากแหล่งที่มาที่ไม่รู้จัก
6. แจ้งผู้ให้บริการต่างๆ ที่เกี่ยวข้องเมื่อโทรศัพท์สูญหาย
7. เลือกติดตั้งโปรแกรมในโทรศัพท์มือถือเท่าที่จำเป็น และจากแหล่งที่มาที่น่าเชื่อถือ
8. พิจารณาลิงก์ที่อยู่บนเว็บไซต์ก่อนการคลิกทุกครั้ง
9. ใช้โทรศัพท์มือถือทำธุรกรรมออนไลน์อย่างระมัดระวัง
10. อัพเดตระบบปฏิบัติการหรือโปรแกรมบนโทรศัพท์มือถือที่ใช้อยู่ให้เป็นเวอร์ชันใหม่อย่างสม่ำเสมอ
11. เชื่อมต่อไปยังระบบงานต่างๆ ผ่าน VPN หรือช่องทางการเชื่อมต่อเครือข่ายที่มีการเข้ารหัสลับ

น้องพุดดิ้งชวนรู้

นับเป็นบทความที่มีเนื้อหาจุใจหนอนหนังสืออย่างพุดดิ้งเลย ยิ่งอ่านก็ยิ่งทำให้พุดดิ้งและเพื่อนๆ รู้สึกถึงความมั่นคงปลอดภัยในการใช้สมาร์ตโฟนและแท็บเล็ตมากขึ้นอย่างต่อเนื่อง ซึ่งพุดดิ้งก็จะนำ 11 วิธีง่ายๆ ในการใช้งานโทรศัพท์มือถือดังกล่าวไปใช้อย่างเคร่งครัด และสุดท้ายขอขอบคุณทั้งพุดน้อย ที่ได้แนะนำบทความดีๆ มาให้ได้ศึกษากันด้วยนะคะ

4.4 ภัยบน iOS

ณ ขณะนี้ในมือพุดน้อย ข้างซ้ายถือสมาร์ตโฟนในระบบปฏิบัติการแบบ iOS หรือเป็นโอเอสระบบปิด มือข้างขวาถือสมาร์ตโฟนในระบบปฏิบัติการแบบ Android หรือระบบโอเอสแบบเปิด ซึ่งทั้ง 2 ระบบนี้ต่างมีจุดเด่นที่ชวนน่าหลงใหลกันคนละแบบ แต่ทั้งนี้ไม่ว่าจะเป็นระบบปฏิบัติการจากค่ายไหนก็ต่างมีช่องโหว่ในการเกิดภัยร้ายต่อผู้ใช้บริการด้วยกันทั้งสิ้น

เพื่อไม่ให้เพื่อนๆ รอนาน พุดน้อยจะขอยกตัวอย่างสมาร์ตโฟนและแท็บเล็ตจากค่าย Apple กันก่อนนะครับ อย่างที่พุดน้อยได้กล่าวในข้างต้น โดย iPhone และ iPad เป็นสินค้าที่มีจุดเด่นอยู่ที่ระบบปฏิบัติการที่เป็นของ iOS หมายถึง โอเอสระบบปิด ทั้งยังมีการพัฒนาเพื่อการค้าในบริษัท Apple เท่านั้น ทำให้ระบบค่อนข้างมีความเสถียร เพราะถูกออกแบบมาให้ใช้งานกับอุปกรณ์นั้นๆ โดยเฉพาะ

นอกจากนี้ทาง Apple ยังมีความเข้มงวดและหวงแหน ไม่ยอมรับแอพพลิเคชันจากระบบปฏิบัติการอื่นๆ มาติดตั้งในเครื่องของบริษัทตน ทั้งยังเป็นนักตรวจสอบแอพพลิเคชันที่จะเข้ามาให้ดาวน์โหลดฟรีหรือเปิดขายผ่าน App Store อย่างละเอียด เพื่อให้สาวกชาว Apple ได้ดาวน์โหลดแอพพลิเคชันที่มีประสิทธิภาพ เรียกว่าถ้าทดสอบแล้วไม่ผ่าน มีปัญหากับเครื่อง ก็ไม่มีสิทธิ์มาวางเฉิดฉายใน App Store แน่นอน

App Store ช่องโหว่ที่มองไม่เห็น

แม้ว่าจะตรวจสอบกันเข้มงวดขนาดนี้ แต่อย่าเพิ่งวางใจไป เพราะในโลกนี้ไม่มีสิ่งใดไว้ใจได้ 100% เนื่องจากในระบบ iOS นั้นก็มีวายร้ายซ่อนอยู่เหมือนกัน โดยช่องโหว่ของ iOS นั้น จะอยู่ตรงที่ผู้ใช้บริการต้องทำการใส่เลขที่บัตรเครดิตลงใน App Store เวลาจะซื้อแอพพลิชันที่มีค่าใช้จ่ายมาใช้ แต่ทั้งนี้ปัญหาไม่ได้อยู่ที่เลขที่บัตรเครดิตหรอกครับ แต่อยู่ที่การต้องตรวจสอบเช็กให้ดีก่อนว่า ก่อนที่จะใส่ข้อมูลอะไรลงไป App Store ที่เราจะเข้าไปใช้งาน มันใช่หน้าเว็บไซต์จริงๆ ของ Apple รึเปล่า ไม่อย่างนั้นจะกลายเป็นว่าให้เลขที่บัตรเครดิตกับแฮกเกอร์ไป ทีนี้ล่ะยุ่งกันใหญ่แน่

ถ้าไม่มั่นใจการใส่เลขที่บัตรเครดิต แต่อยากจะซื้อแอพพลิเคชันโดนๆ มาใช้ แนะนำว่าให้ซื้อ iTunes Gift Card จากร้านตัวแทนของ Apple มาใช้แทนซึ่งปลอดภัยกว่า และที่สำคัญควบคุมเงินที่จะใช้ได้ด้วยครับ

Jailbreak แหกคุก เจอโจร

ใครที่ใช้ iPhone หรือ iPad คงเคยได้ยินเรื่องการแหกคุกกันมาบ้าง แต่บางคนก็ยังงงๆ ว่าแหกคุกคืออะไร ทำไมใช้ iPhone, iPad แล้วต้องแหกคุก ทำแล้วได้อะไร ผิดกฎหมายไหม อย่ารอช้ารีบไปศึกษากัน

การแหกคุกในภาษาบ้านเรา มีชื่อเป็นทางการว่า Jailbreak ซึ่งหมายถึงการทำอะไรสักอย่าง เพื่อให้ iPhone หรือ iPad สามารถติดตั้งแอพพลิเคชันที่ไม่มีขายอยู่บน App Store ได้ นอกจากนี้ยังเป็นการยอมรับให้อุปกรณ์อื่นๆ สามารถติดตั้งแอพพลิเคชันได้โดยไม่ผ่าน iTune นั่นหมายความว่าเราสามารถดาวน์โหลดแอพพลิเคชันตัวเต็มจากเว็บไซต์ที่ปล่อยมาติดตั้งได้แบบฟรีๆ

iTunes Gift Card คืออะไร

สำหรับบัตร iTunes Gift Card นี้ เปรียบได้เหมือนบัตรเติมเงินที่เอาไว้สำหรับซื้อ App, Game, ของในแอพต่างๆ เช่น สติ๊กเกอร์ Line หรือเพชรในเกม, เพลง และหนังต่างๆ สำหรับคนที่ใช้อุปกรณ์ของ Apple ครับ เช่น iPhone, iPad, iPod และเครื่อง Mac

โดยหลักการทำงานจะคล้ายๆ กับบัตรเติมเงินโทรศัพท์ครับ แต่เป็นการเติมเข้า Apple ID แทน โดยเมื่อเราต้องการใช้งานก็ซื้อบัตรมาเติมเข้าไปใน Apple ID ของท่าน เช่น สมมุติเราเติมเข้าไป $10 เราก็จะสามารถนำเงินที่เติมเข้าไปนี้ซื้อ App, Game, เพลง และหนังต่างๆ ได้ทันที และเมื่อซื้อแล้ว ยอดเงินก็จะค่อยๆ ถูกหักจากยอดที่ท่านเติมเข้าไปตามราคาของของที่ท่านซื้อครับ และเมื่อเงินที่ท่านเติมเข้าไปใกล้หมด เราก็สามารถซื้อบัตรใหม่ไปเติมเพิ่มเข้าไปได้ทันที โดยยอดเงินที่เติมเข้าไปใหม่ก็จะไปรวมกับยอดเก่าที่เหลืออยู่ให้อัตโนมัติครับ

ขอขอบคุณข้อมูลจาก http://www.itunesgiftcard.in.th/what/

น้องพุดดิ้งชวนรู้

เห็นไหมคะ ไม่ว่าจะเป็นระบบปฏิบัติการที่มีระบบรักษาความมั่นคงปลอดภัยผู้ใช้บริการมากแค่ไหน ก็ล้วนแล้วแต่มีช่องโหว่ด้วยกันทั้งสิ้น ดังนั้นหากไม่ต้องการให้ภัยร้ายบน iOS เกิดขึ้นกับตนเอง เพื่อนๆ ก็ควรเช็กเว็บไซต์ให้ดีก่อนนะคะว่าเว็บไซต์ที่กำลังจะกรอกรหัสบัตรเครดิต เป็น App Store ของแท้หรือเปล่า

4.5 ภัยบน Android

มาถึงสมาร์ตโฟน ในระบบ Android บนมือขวาของพุดน้อยกันบ้าง ระบบโอเอสแบบเปิดชนิดนี้มีผู้ผลิตโทรศัพท์มือถือนำไปพัฒนาใช้กันหลายค่าย หากเพื่อนๆ อยากรู้ว่ามีความน่าสนใจอย่างไร พุดน้อยเองก็ไม่อยากรอช้า ไปรู้จักกันได้เลย

โอเอสแบบเปิดต้อง Android

Android เป็นระบบโอเอสแบบเปิดจาก Google หรือโอเอสแบบเปิด หมายถึง เป็นโอเอสที่ใครๆ ก็สามารถนำไปพัฒนาใช้ได้ฟรีตามเงื่อนไขที่ Google กำหนดไว้ เช่น หากนำไปพัฒนาต่อต้องทำการเปิดเผยโค้ดที่พัฒนาแล้วให้นักพัฒนารายอื่นๆ ได้รู้ด้วย ด้วยเหตุนี้จึงทำให้ Android ได้รับความนิยมจากผู้ผลิตหลายราย จัดว่าเป็นคู่แข่งรายสำคัญของ iOS เลยทีเดียว ซึ่งการที่เป็นระบบโอเอสแบบเปิด จึงทำให้บริษัทต่างๆ จ้างนักพัฒนาเข้ามาปรับเสริมเติมแต่งเวอร์ชันต่างๆ ของ Android กันอย่างสนุกสนาน ปรับแต่งให้เป็นโอเอสในลักษณะของตนเองเพื่อให้เหมาะกับอุปกรณ์ต่างๆ ที่ผลิตขึ้น รวมไปถึงระบบการรักษาความมั่นคงปลอดภัยด้วย

โดยเราเรียกโอเอสลักษณะนี้ว่า Official ROM ในมุมกลับกันยิ่งเทคโนโลยีมีประโยชน์ หากใช้โดยไม่มีการเตรียมการที่ดีก็อาจจะส่งผลเสียมาสู่ผู้ใช้ เพราะแม้จะมีการพัฒนาก้าวหน้าไปมากแค่ไหนแต่ Android ก็ยังมีวายร้ายแวะมาเยี่ยมอยู่เสมอ ซึ่งวิธีการป้องกันความมั่นคงปลอดภัยนั้นไม่ยาก เพียงปฏิบัติดังนี้

1. ตั้งสติ คิดสักนิดก่อนดาวน์โหลดแอพพลิเคชัน : เพราะ Android เป็นระบบปฏิบัติการที่สามารถติดตั้งแอพพลิเคชันต่างๆ ได้โดยง่าย แต่ความสะดวกสบายเช่นนี้แหละที่จะเป็นช่องทางหนึ่งในการทำให้บรรดาวายร้ายเข้ามาทำการขโมยข้อมูลจากเครื่องของเราได้

2. ศึกษาข้อมูลก่อนคลิกปุ่ม Install : เพื่อความมั่นคงปลอดภัยในการดาวน์โหลดแอพพลิเคชัน จาก Play Store ก่อนจะตัดสินใจคลิกปุ่ม Install บนหน้าติดตั้งแอพพลิเคชัน หากไม่ต้องการมาเสียใจภายหลังทางที่ดีควรศึกษาข้อมูล อ่านรีวิวการพูดถึงแอพพลิเคชันดังกล่าวจากผู้ใช้ก่อนหน้าไว้บ้าง เช่น มีปัญหาการใช้งานอะไรไหม ไปจนถึงการแจ้งระวังมัลแวร์ว่ามีหรือเปล่า และหากต้องการความมั่นใจยิ่งขึ้น แนะนำให้คลิกเข้าไปศึกษายังเว็บไซต์บริษัทผู้พัฒนาแอพพลิเคชันว่ามีอยู่จริงหรือไม่

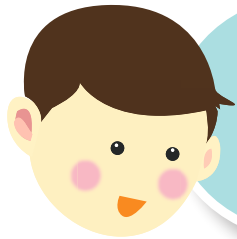
นอกจากการอ่านรีวิวจากคอมเมนต์ของผู้ใช้แอพพลิเคชันแล้ว ยังมีอีกวิธีหนึ่งที่ช่วยในด้านการตรวจสอบความมั่นคงปลอดภัย นั่นก็คือการตรวจสอบการรีวิวจากเว็บไซต์ ซึ่งสามารถลองเสิร์ชชื่อแอพพลิเคชันดังกล่าวได้จาก Google หรือบล็อกทางด้านเทคโนโลยีดังๆ สร้างหลักประกันให้เราได้อีกชั้นหนึ่ง

น้องพุดดิ้งชวนรู้

ท้ายนี้พุดดิ้งขอเสริมสักนิด เพราะไม่ว่าจะใช้ระบบปฏิบัติการแบบไหน ในฐานะผู้ใช้งานก็ควรดาวน์โหลดติดตั้งแอพพลิเคชันป้องกันไวรัสหรือมัลแวร์ติดเครื่องไว้ด้วย รวมไปถึงการอัพเดตโอเอสในเครื่องให้เป็นเวอร์ชันล่าสุดอยู่เสมอ เท่านี้ก็จะช่วยให้เรามั่นคงปลอดภัยในการใช้สมาร์ตโฟนและแท็บเล็ตมากขึ้นแล้วค่ะ

บทที่ 5

กฎหมาย...
รู้ไว้ก็ดีกับตัวเอง



"กฎหมายไซเบอร์รู้ไว้ได้ประโยชน์
อ่านแล้วไม่มีโทษ มีแต่ความรู้โดนๆ
ทั้งยังทำให้เราอยู่ในโลกออนไลน์ได้
อย่างสบายใจ"

5.1 รู้จักมั้ย "กฎหมายไซเบอร์"

บ่ายวันหนึ่ง... คุณพ่อเล่นทายคำถามเกี่ยวกับเรื่องไอทีกับพุดน้อยว่า

คุณพ่อ : ทำอย่างไรคนในสังคมจะอยู่กันอย่างเป็นระเบียบ (คุณพ่อถาม)

พุดน้อย : ทุกคนต้องเคารพกฎหมายครับ

คุณพ่อ : แล้วสังคมออนไลน์จะเป็นระเบียบได้อย่างไร

พุดน้อย : อืม... เรามีกฎหมายไซเบอร์ไหมครับ

คุณพ่อตอบว่า “ใช่แล้วครับ การเคารพกฎหมายเป็นส่วนหนึ่งที่จะช่วยให้สังคมอยู่ร่วมกันได้อย่างมีความสุขซึ่งรวมถึงโลกออนไลน์ด้วย ลองคิดดูว่าหากไม่มีกฎหมายไซเบอร์แล้ว ในโลกออนไลน์ที่เราคุยกับคนไม่รู้จักหรือมองไม่เห็นหน้าคนที่คุยด้วยจริงๆ คงมีการหลอกลวงกันจนมีผู้เสียหายนับไม่ถ้วนแน่นอน”

คุณพ่อเล่าให้ฟังต่อว่า ประเทศไทยมีกฎหมายไซเบอร์ที่สำคัญอย่างน้อยอยู่ 2 ฉบับ คือ กฎหมายธุรกรรม หรือชื่อเต็มคือ “พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544” และกฎหมายคอมพิวเตอร์ที่มีชื่อเรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550” ซึ่งเป็นกฎหมายพื้นฐานที่ชาวออนไลน์ไม่ว่าจะเป็นมือเก่า มือใหม่ ควรรู้ไว้ เพราะทุกวันนี้ชีวิตประจำวันของเราเกี่ยวข้องกับคอมพิวเตอร์แทบจะทุกเวลา การใช้งานหรือทำกิจกรรมต่างๆ เช่น การส่งข้อมูลคอมพิวเตอร์ การกดเงินผ่านตู้เอทีเอ็ม การแชทผ่านโปรแกรมในโทรศัพท์มือถือ หรือกระทั่งการดูโทรทัศน์ดาวเทียม จึงเป็นกิจกรรมที่ผู้ใช้งานต้องระมัดระวังถึงผลและบทลงโทษต่างๆ ตามกฎหมายด้วย

คราวนี้.. พุดน้อยจะถ่ายทอดที่คุณพ่อเล่าให้ฟังว่ากฎหมายไซเบอร์ทั้งสองเรื่องเป็นยังไงบ้างนะครับ

5.2 กฎหมายกับการช้อปปิ้งออนไลน์

เดี๋ยวนี้เพื่อนๆ ของพุดน้อยมักจะชอบดูสินค้าออนไลน์ซึ่งบางทีพุดน้อยก็ได้ยินเพื่อนคุยกันว่าการซื้อของออนไลน์เนี่ยจะทำได้ไหม ถ้าไม่ได้ของจะทำยังไง เรียกร้องอะไรได้บ้าง คำถามพวกนี้พุดน้อยมีคำตอบให้ครับ

ที่จริงแล้วการซื้อขายของผ่านอินเทอร์เน็ต หรือการช้อปปิ้งออนไลน์ก็เป็นการซื้อขายตามกฎหมายทั่วไปคือประมวลกฎหมายแพ่งและพาณิชย์ที่มีเงื่อนไขพื้นฐานว่า ถ้าสินค้านั้นต่ำกว่า 20,000 บาท สามารถซื้อขายกันได้โดยการชำระเงินและส่งมอบสินค้า ซึ่งสามารถจะฟ้องร้องกันได้แม้ไม่มีหลักฐานเป็นหนังสือ แต่ถ้าเมื่อไหร่ก็ตามที่เป็นสินค้าที่มีราคา 20,000 บาท หรือแพงกว่านั้นก็จะต้องมีหลักฐานเป็นหนังสือ หรือมีมัดจำ หรือจ่ายเงินบางส่วนแล้วถึงจะฟ้องร้องกันได้ โดยเมื่อเป็นการซื้อของออนไลน์ก็จะมีกฎหมายอีกเรื่องหนึ่งที่มาเกี่ยวข้องคือ กฎหมายธุรกรรม ที่จะบอกว่าการซื้อขายออนไลน์ก็มีผลเหมือนการซื้อขายกันตามปกตินั่นเอง

กฎหมายธุรกรรมหรือ “พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544” ที่พุดน้อยพูดถึงเป็นกฎหมายที่มีขึ้นเพื่อส่งเสริมและดูแลให้การทำธุรกรรมต่างๆ ผ่านทางอิเล็กทรอนิกส์มีความน่าเชื่อถือ เช่น การติดต่อซื้อของทางอีเมล์ การโอนเงินผ่าน e-banking การลงชื่อทางอิเล็กทรอนิกส์ เป็นต้น ซึ่งมีสาระสำคัญที่เราควรรู้ไว้ดังนี้

- **การทำกิจกรรมผ่านทางอิเล็กทรอนิกส์...** กฎหมายธุรกรรมบอกว่าเราสามารถที่จะทำกิจกรรมต่างๆ ในรูปของข้อมูลอิเล็กทรอนิกส์ได้ เช่น การทำหรือการเก็บเอกสารอิเล็กทรอนิกส์ การส่ง-รับข้อมูลผ่านทางอิเล็กทรอนิกส์ การลงลายมือชื่ออิเล็กทรอนิกส์ แต่สำหรับบางกิจกรรมต้องดูถึงความน่าเชื่อถือและเงื่อนไขเฉพาะเรื่องตามที่กฎหมายกำหนดด้วย
- **ผลของการติดต่อทางอิเล็กทรอนิกส์...** ข้อความหรือข้อมูลที่มีการติดต่อสื่อสารทางอิเล็กทรอนิกส์นั้นมีผลเหมือนการติดต่อกันแบบปกติ เช่น แม้จะตกลงซื้อขายกันผ่านอีเมล์ กฎหมายก็บยอมรับให้ใช้ได้เหมือนติดต่อกันบนกระดาษ นอกจากนี้ ข้อมูลอิเล็กทรอนิกส์ยังสามารถนำมาใช้เป็นพยานหลักฐานได้อีกด้วย

● **แล้วอะไรจะถือว่าเป็นหลักฐานได้บ้าง...** ข้อมูลอิเล็กทรอนิกส์ทุกอย่างถือเป็นหลักฐานได้ตามกฎหมาย ไม่ว่าจะเป็น อีเมล์ fax ข้อความบนมือถือ ไฟล์ข้อมูล สิ่งต่างๆ เหล่านี้สามารถนำมาใช้ได้โดยผู้ที่เกี่ยวข้องกับเรื่องดังกล่าวจะไม่ยอมรับแค่เพราะเห็นว่าเป็นข้อมูลอิเล็กทรอนิกส์ไม่ได้

คุณพ่อของพุดน้อยยกตัวอย่างให้ฟังว่า ถ้าพุดน้อยอยากซื้อนาฬิกาที่ขายอยู่บนเว็บไซต์ พุดน้อยจะสอบถามราคาและวิธีการสั่งซื้อจากคนขายทางอีเมล์ ต่อมาก็มีการอีเมล์ติดต่อกันจนได้รุ่นที่ต้องการ คนขายจึงให้พุดน้อยโอนเงินผ่านธนาคาร แล้วคนขายก็จะส่งของให้ แบบนี้ถ้าหากว่าพุดน้อยไม่ได้ของ พุดน้อยก็สามารถใช้อีเมล์ และใบสลิปโอนเงินผ่านธนาคารมาเป็นหลักฐานได้นะครับ

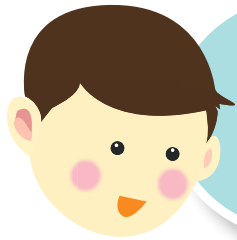
เห็นมั้ยครับ ใจความหลักของกฎหมายที่พุดน้อยเล่าให้ฟังล้วนเป็นเรื่องใกล้ตัวที่น่าสนใจ เพราะแม้กระทั่ง e-Mail ก็เป็นหลักฐานยืนยันการซื้อขายออนไลน์ทางกฎหมายได้

ต้องการทราบข่าวสาร กิจกรรม และเอกสารเกี่ยวกับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เข้าไปดูข้อมูลได้ที่ http://ictlawcenter.etda.or.th/

หากมีข้อสงสัยเกี่ยวกับเรื่องการซื้อขายสินค้าและ บริการออนไลน์ ติดต่อได้ที่ ศูนย์รับเรื่องร้องเรียนออนไลน์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) อาคารเดอะไนน์ ทาวเวอร์แกรนด์ พระรามเก้า (อาคาร B) ชั้น 21 เลขที่ 33/4 ถนนพระรามเก้า แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310 หรือโทร. 0-2123-1223

น้องพุดดิ้งชวนรู้

จากที่พุดน้อยเล่าให้ฟังเกี่ยวกับกฎหมายธุรกรรม จะเห็นว่าข้อมูลต่างๆ ไม่ว่าจะเป็นข้อความที่ได้ตกลงซื้อขาย หรือข้อมูลทางอิเล็กทรอนิกส์อื่นใดก็ตามที่สามารถยืนยันความสัมพันธ์ระหว่างผู้ซื้อและผู้ขาย เราสามารถเอามาใช้เป็นหลักฐานได้ พุดน้อยจึงอยากจะบอกเพื่อนๆ ว่า หากเราได้รับความเสียหายจากการซื้อขายสินค้าในเว็บไซต์ สิ่งแรกคือควรตั้งสติ และรวบรวมข้อมูลและเอกสารต่างๆ ที่สามารถบอกได้ว่าเราได้ทำกิจกรรมนั้นจริง เพราะข้อมูลทุกชนิดนั้นสามารถใช้ในการเรียกร้องหรือเอาผิดกับบรรดาพ่อค้าในโลกไซเบอร์ได้



"รู้ลึกที่มาร้านค้าออนไลน์บทเรียนง่ายๆ สำหรับนักช้อปยุคไอทีเพื่อให้เกิดความมั่นคงปลอดภัย"

5.3 ช้อปปิ้งออนไลน์เชื่อใจได้อย่างไร?

จากเรื่องเล่าในตอนที่แล้ว พุดน้อยยอมรับว่าการซื้อสินค้าออนไลน์ในปัจจุบันเป็นเทรนด์ที่กำลังมาแรงหยุดไม่อยู่ แม้ว่านิสัยคนไทยส่วนใหญ่ถ้าไม่เห็นของจริง หรือไม่เคยจับสินค้ารับรองไม่มีทางซื้อแน่นอน แต่หากสินค้าหน้าตาเหมือนๆ กัน มีสินค้ามาให้เลือกถึงที่ (หน้าจอคอมพิวเตอร์) ไม่ต้องเดินหาซื้อให้เหนื่อยแถมราคายังถูกกว่าในห้างสรรพสินค้าเกือบครึ่ง อีกทั้งส่งตรงถึงบ้าน รับประกันว่ามีผู้สนใจแน่นอน

แต่จะช้อปปิ้งออนไลน์ให้สบายใจ พุดน้อยว่าเพื่อนๆ ควรศึกษาวิธีการช้อปปิ้งอย่างมั่นคงปลอดภัยเอาไว้บ้าง เพื่อจะได้ไม่ต้องเสียเงินและเสียใจในภายหลังนะครับ

“ข้อเตือนใจ”...ฝากถึงนักช้อปออนไลน์

เพื่อระวังไม่ให้โดนหลอกขายสินค้าบนโลกออนไลน์ เราควรศึกษาข้อมูลสินค้าและความน่าเชื่อถือของผู้ขายด้วยวิธีการง่ายๆ ดังนี้

1. เช็คความมีตัวตนของร้านค้า โดยดูเครื่องหมายรับรองการจดทะเบียน หรือที่เรียกว่า “DBD Registered” เพราะผู้ค้าขายออนไลน์มีหน้าที่ต้องจดทะเบียนกับ กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ และถ้าผู้ขายอยากให้ผู้ซื้อมั่นใจในตัวตนของผู้ขายก็สามารถขอเครื่องหมายรับรองมาแปะไว้ที่ร้านค้าของตัวเองได้ซึ่งมีหน้าตาแบบนี้นะครับ

2. เลือกร้านค้าที่มีชื่อเสียงตอบรับในทางที่ดี วิธีสังเกตง่ายๆ อาจจะอ่านกระทู้ (Web board) ย้อนหลัง หรือจำนวนการส่งสินค้า การรีวิว (Review) ของลูกค้าว่าเป็นไปในทางบวกหรือลบ เพียงเท่านี้เราก็พอจะประเมินได้แล้วว่าควรจะช้อปกับร้านค้าออนไลน์เจ้านี้หรือเปล่า

3. เลือกซื้อสินค้าจากเว็บไซต์ที่มีอายุอย่างน้อย 1 ปี เราสามารถตรวจสอบได้ง่ายๆ ผ่านทาง https://who.is/ โดยการใส่ชื่อเว็บไซต์นั้นๆ ลงไป ยิ่งร้านค้าที่เปิดขายออนไลน์มานานและยังเปิดอยู่ แสดงว่ามีความน่าเชื่อถือที่ดี ในทางกลับกันถ้าเป็นเว็บไซต์หลอกลวงก็คงไม่เปิดมานานนับปีเป็นแน่

4. สังเกตการตอบคำถามของผู้ขาย สามารถตรวจสอบได้จากการตอบคำถามในกระทู้ว่าผู้ขายตอบคำถามของลูกค้าบ่อยแค่ไหน มีการตอบคำถามอย่างไร และเอาใจใส่ลูกค้าหรือไม่ หากในกระทู้มีลูกค้าเข้ามาคุยเป็นจำนวนมาก แล้วผู้ขายมีการให้ความใส่ใจในการตอบคำถามของลูกค้าที่ดี เราก็สามารถมั่นใจได้ในระดับหนึ่งว่ามั่นคงปลอดภัย

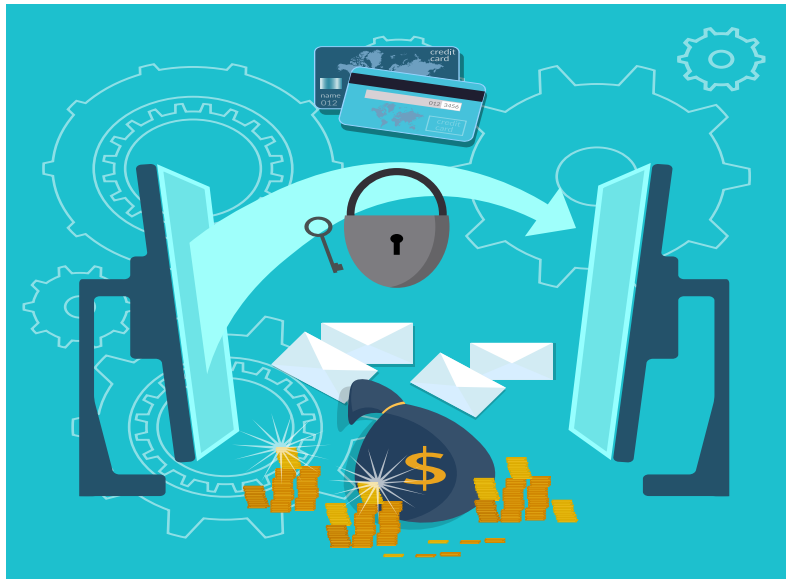
5. ดูเงื่อนไขการรับประกันสินค้า หรือบริการหลังการขาย เนื่องจากการซื้อสินค้าผ่านทางเว็บไซต์ หากสินค้ามีปัญหาไม่ว่าจะเป็นการส่งที่ผิดพลาดหรือสินค้าไม่ได้มาตรฐาน ทางร้านจะมีการรับประกันหรือสามารถเปลี่ยนหรือคืนสินค้าได้หรือไม่ ระยะเวลาในการรับประกันมีมากน้อยเพียงใด หากทางผู้ขายไม่ได้ระบุไว้ เราก็ควรถามให้เข้าใจและชัดเจนก่อนการตัดสินใจซื้อ ซึ่งทางที่ดีควรสอบถามผ่านทางเว็บบอร์ด หรืออีเมล เพื่อจะได้มีหลักฐานที่เป็นลายลักษณ์อักษร และไม่ควรตกลงซื้อขายกันทางโทรศัพท์

6. ตรวจสอบ Social Media ของผู้ขาย เพราะผู้ขายบางร้านมีหลายบัญชีผู้ใช้ ดังนั้นจึงควรสืบค้นบัญชีผู้ใช้งานจริงให้แน่ชัด เพื่อที่จะได้สามารถตรวจสอบกลุ่มเพื่อนหรือผู้ติดตาม และพฤติกรรมของการใช้งานจริงได้โดยถ้าผู้ขายผ่านทาง Social Media มีความจริงใจก็ต้องยินดีในการให้บัญชีผู้ใช้งานจริง

7. สินค้าที่เลือกซื้อไม่ใช่ของผิดกฎหมาย เช่น ยาที่ไม่ได้รับการรับรอง ของเลียนแบบ เพราะถ้าของมีปัญหา หรือโดนโกง คุณก็คงจะไปเอาผิดกับคนที่หลอกขายคุณไม่ได้ด้วยเช่นกัน

น้องพุดดิ้งชวนรู้

ปัจจุบัน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ ETDA ในกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้เสริมความเชื่อมั่นให้แก่ผู้ซื้อผู้ขายสินค้าออนไลน์โดยเปิดให้บริการ “ศูนย์รับเรื่องร้องเรียนซื้อขายออนไลน์” ผ่านเว็บไซต์ http://occ.thaiemarket.com ซึ่งจะคอยให้คำแนะนำแก่บุคคลทั่วไปในกรณีที่เกิดปัญหาจากการซื้อขายสินค้าออนไลน์ด้วย



5.4 กฎหมายที่ควรรู้ไว้... จะได้ไม่ใช้คอมพิวเตอร์แบบผิดๆ

การใช้คอมพิวเตอร์มีทั้งข้อดีและข้อเสีย ซึ่งบางคนก็ใช้แบบไม่ถูกต้อง และบางทีคนดีอย่างเราๆ ก็ใช้คอมพิวเตอร์แบบรู้เท่าไม่ถึงการณ์ ทำให้กลายเป็นผิดกฎหมายได้เหมือนกันนะครับ เราจึงต้องระมัดระวังและอย่างน้อยๆ ก็ต้องรู้ว่าทำอะไรบ้างที่กฎหมายบอกว่าผิดและอาจจะต้องโดนลงโทษ

คุณพ่อของพุดน้อยได้เล่าว่ามีกฎหมายที่ชื่อว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550” หรือเรียกสั้นๆ ว่า กฎหมายคอมพิวเตอร์ เป็นกฎหมายอีกเรื่องหนึ่งที่เราควรรู้ไว้ คุณพ่อได้เล่าให้พุดน้อยฟังว่ากฎหมายนี้สำคัญอย่างไร

นักเจาะ นักแฮก ต้องโดน...!!

คอมพิวเตอร์ มือถือ อีเมล์ หรืออะไรก็ตามที่เป็นอุปกรณ์หรือข้อมูลอิเล็กทรอนิกส์ของเรา เราก็คงไม่อยากให้ใครเข้ามายุ่งใช่ไหมครับ เพราะฉะนั้น กฎหมายถึงต้องกำหนดว่าใครก็ตามที่เข้าไปยุ่งกับระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของคนอื่น โดยเฉพาะพวกที่เรียกว่า แฮกเกอร์ นั้นอาจถูกลงโทษได้หากว่าไปทำอะไรไม่ดีกับระบบหรือข้อมูลคอมพิวเตอร์ของคนอื่นๆ หรือทำโดยไม่ได้รับอนุญาต ซึ่งมีกรณีที่กฎหมายกำหนดว่าเป็นความผิดและอาจต้องถูกลงโทษดังนี้

- Hacker การแฮกระบบคอมพิวเตอร์หรือแฮกข้อมูลคอมพิวเตอร์เป็นพวกที่ชอบแอบเข้าไปในระบบคอมพิวเตอร์หรือเข้าไปดูข้อมูลของคนอื่น โดยที่เจ้าของเครื่องหรือเจ้าของข้อมูลเค้าใส่รหัสป้องกันไว้ เหมือนกับโจรที่แอบเข้าไปในบ้านที่ล็อคกุญแจไว้นั่นหล่ะครับ
- รู้แล้วอยากบอกต่อ... คือคนที่รู้รหัสสำหรับเข้าระบบคอมพิวเตอร์ของคนอื่นแล้วเอาไปบอกต่อ แบบนี้ก็ผิดนะครับ

- **ส่งอะไรชั้นอยากรู้บ้าง** พวกนี้คือพวกดักข้อมูลนั่นเอง เป็นพวกอยากรู้ว่าคนอื่นเค้าส่งอะไรกัน เลยไปคอยเฝ้าอยู่กลางทางคอยดักจับข้อมูลคอมพิวเตอร์ที่วิ่งไปมาตามเส้นทางต่างๆ คล้ายกับการดักฟังโทรศัพท์ที่ไปแอบฟังว่าเค้าคุยอะไรกันนั่นเอง
- **ก่อกวนหรือทำลาย** คือการเข้าไปยุ่งกับระบบคอมพิวเตอร์จะทำให้ระบบล่ม หรือใช้ไม่ได้ เช่น ยิงไวรัสเพื่อโจมตีคอมพิวเตอร์คนอื่น หรือเข้าไปยึดเครื่องคอมพิวเตอร์ เป็นต้น นอกจากนี้ ยังรวมถึงการแอบเข้าไปแก้ไขหรือทำลายข้อมูลของคนอื่นด้วย ซึ่งพวกชอบก่อกวนหรือทำลายไปยุ่งกับระบบหรือข้อมูลนั้นเป็นเรื่องสำคัญมากๆ เช่น ระบบคอมพิวเตอร์สำหรับจ่ายกระแสไฟ ข้อมูลคอมพิวเตอร์ของระบบการเงินธนาคาร แบบนี้โทษจะหนักขึ้นอีกหนึ่งเท่าเลยนะ
- **พวกชอบแจก..** แจกอะไรถึงจะผิด ?? ก็แจกโปรแกรมที่เอาไว้ทำผิดไงครับ สำหรับนักโปรแกรมเมอร์ผู้ร้อนวิชา ซึ่งมักจะมีเวลาว่างสร้างไวรัส หรือมัลแวร์ แล้วนำไปปล่อยให้กับเพื่อนร่วมอุดมการณ์ขายหรือให้ผู้อื่นหยิบยืมไปใช้ เช่น ไวรัสที่ยิงเข้าไปเพื่อทำลายระบบคอมพิวเตอร์ โทรจันที่เข้าไปฝังตัวในเครื่องเพื่อขโมยข้อมูล ก็ยิ่งเท่ากับส่งเสริมให้คนอื่นทำผิด กฎหมายจึงต้องห้ามปรามเสียแต่เนิ่นๆ เพื่อไม่ให้มีคนทำผิดเยอะขึ้นอีก

ฮั่นแน่... ชอบแกล้ง ชอบโพสต์ ส่งหรือแชร์ ระวังจะผิดไม่รู้ตัว

นอกจากพวกเทคนิคต่างๆ ที่ไปยุ่งกับคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของคนอื่นแล้ว ยังมีเรื่องที่คนใช้งานทั้งหลายต้องระวังไว้ด้วยเหมือนกัน ยิ่งชอบส่งหรือแชร์แล้วล่ะก็เราอาจจะทำผิดกฎหมายโดยที่เราไม่รู้ตัวเลยก็ได้นะครับ

- **ส่งแล้วไม่บอก?** พวกที่ส่งข้อมูลคอมพิวเตอร์หรืออีเมล์แล้วไม่ยอมบอกชื่อ ไม่บอกตัวตน หรือบอกว่าเป็นคนอื่นส่งมา ไปก่อกวนคนที่ได้รับข้อมูลจนใช้งานคอมพิวเตอร์แบบไม่เป็นสุข ต้องคอยบล๊อกคอยลบ แบบนี้กฎหมายถือว่าทำผิดนะครับ เพราะจะส่งข้อมูลทั้งที คนรับเค้าก็อยากรู้ว่าใครส่ง ส่งมาจากไหน เชื่อถือได้หรือไม่ เพราะอาจจะมีของที่ไม่ต้องการติดมา เช่น มีไวรัสแถมมากับอีเมล์ พอเปิดอีเมล์ปุ๊บ เครื่องก็ถูกก่อกวนหรือถูกยึดเครื่อง เป็นต้น

- **ข้อมูลหลอกลวงหรือลามก** ข้อนี้จะเป็นความผิดหากว่าเป็นข้อมูลที่คนอื่นเข้าไปดูได้นะครับ ซึ่งมีความผิดที่เกิดขึ้นได้หลายรูปแบบ อย่างแรกเลยคือ พวกชอบหลอกลวงคนอื่นโดยการใช้ข้อมูลปลอม เช่น สร้างเว็บเพจปลอมทำให้คนเข้าใจผิด ซึ่งส่วนมากจะเป็นพวกเว็บธนาคารปลอมที่คนใช้งานถูกเอาข้อมูลส่วนตัว หรือเลขบัตรสำคัญต่างๆ ไป แล้วคนสร้างเว็บก็เอาข้อมูลที่ได้ไปปลอมเป็นเจ้าของบัตร เจอแบบนี้ระวังจะเสียเงินโดยไม่ทันตั้งตัวนะครับ

ถัดมาคือการลงข้อมูลหรือโพสต์ข้อความที่ไม่เป็นความจริง ซึ่งเป็นข้อมูลที่อาจมีผลให้ประเทศชาติเสียหาย หรือทำให้ผู้คนแตกตื่น เช่น จะมีการทิ้งระเบิดที่จังหวัด ก. ให้ประชาชนรีบอพยพ แม้จะเขียนเล่นๆ แต่ถ้าลองมีการโพสต์หรือส่งต่อกันไปมากๆ โดยที่คนส่งต่อก็ไม่รู้ว่าจริงหรือไม่

อีกรูปแบบหนึ่งคือ ข้อความหรือข้อมูลนั้นเป็นความผิดร้ายแรงที่เกี่ยวกับประเทศชาติ หรือเป็นการก่อการร้าย เช่น ชักชวนให้รวมตัวกันแบ่งแยกประเทศ เป็นต้น และสุดท้ายก็คือพวกรูปลามกทั้งหลาย

ผู้ให้บริการอาจต้องรับผิดด้วย.. แล้วผู้ให้บริการเกี่ยวอะไร?? ผู้ให้บริการ ในที่นี้คือคนที่ทำให้เราเข้าไปเล่นอินเทอร์เน็ตได้ เป็นคนที่คอยให้บริการต่างๆ เกี่ยวกับอินเทอร์เน็ตนั่นเอง เช่น ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการเว็บบอร์ด เป็นต้น และเพราะว่าคนที่เข้าใช้อินเทอร์เน็ตที่อยู่มากมาย ทำให้ข้อมูลที่เข้าสู่อินเทอร์เน็ตมีจำนวนมหาศาล หากว่ามีข้อมูลหลอกลวงหรือลามกเข้าสู่ระบบการจัดการย่อมทำได้ยาก ผู้ให้บริการจึงเป็นผู้ที่ช่วยเหลือรัฐในการป้องกันปัญหาที่เกิดขึ้นได้เร็วที่สุด ดังนั้น หากผู้ให้บริการรายใดรู้ว่ามีข้อมูลที่ผิดกฎหมายอยู่ในความดูแลของตัวเองแล้วไม่ยอมจัดการหรือปล่อยให้ข้อมูลนั้นยังคงเผยแพร่อยู่แบบนี้ก็เข้าข่ายว่าผู้ให้บริการจงใจหรือสนับสนุนข้อมูลนั้นนั่นเอง กฎหมายจึงให้ผู้บริการมีความผิด

● **ตัดต่อรูปคนอื่นทำให้เสียหาย** การเผยแพร่รูปของผู้อื่นที่มีการตัดต่อ ไม่ว่าจะตัดต่อเองหรือไม่ก็ตาม ถ้ารูปนั้นอาจทำให้เจ้าของรูปเสียหายหรือถูกดูถูก เช่น เอาภาพดารามาตัดต่อเป็นภาพโป๊ เป็นต้น

อย่างที่พุดน้อยได้เล่าให้ฟังน่าจะทำให้เพื่อนๆ รู้จักกับกฎหมายคอมพิวเตอร์ขึ้นบ้าง แต่พุดน้อยก็เชื่อว่ายังมีเพื่อนๆ อีกหลายคนที่ยังไม่รู้จักอีกเช่นกัน บางคนอาจจะคิดว่าสิ่งที่ทำนั้นไม่ผิดกฎหมาย เพราะตัวเองไม่ได้ไปยุ่งกับใครเพียงแค่แสดงความคิดเห็นในออนไลน์เท่านั้น หรือแม้แต่การแอบใช้ ID และ Password ของแฟนเพื่อน พี่ น้อง ครอบครัว โดยที่เจ้าตัวเองไม่ได้อนุญาต ก็ไม่น่าผิดกฎหมายเพราะข้ออ้างที่ว่า เราก็รู้จักคนเหล่านี้ เป็นต้น

พุดน้อยว่า ที่เราใช้คอมพิวเตอร์ แทปเล็ต หรือมือถือกันจนติดเป็นส่วนหนึ่งของชีวิตในทุกวันนี้ เพื่อนๆ อย่าคิดว่าการกระทำเพียงเล็กน้อยของเรานั้นไม่เป็นไรนะครับ บางทีข้อมูลบางอย่างเราไม่รู้ว่าจริงหรือไม่ เราก็กดแชร์ กดส่งกันไป แต่ถ้าเมื่อไหร่ที่มีคนเสียหายแล้วเค้าเอาเรื่องขึ้นมาล่ะก็ เราต้องเสียทั้งเงิน เวลา เพื่อเคลียร์คดีความกันที่สถานีตำรวจ สื่อออนไลน์เป็นสื่อที่สามารถให้ทุกคนทำอะไรก็ได้ตามอิสระจริง แต่ก็ต้องระวังไม่ให้ไปกระทบกับคนอื่นเค้านะครับ

ระวังสักนิดก่อนคลิ๊ก...

การเป็นยังไงกันบ้างครับที่เล่าให้ฟังเกี่ยวกับกฎหมายคอมพิวเตอร์ที่จะทำให้เราระมัดระวังเวลาใช้งานมากขึ้น แต่พุดน้อยว่า นอกจากการใช้งานแล้วพวกเราเองที่เป็นฝ่ายรับข้อมูลก็ต้องระวังเหมือนกันนะครับ มาดูกันว่าเราควรระวังอะไรไว้บ้าง

- **ข้อมูลหรืออีเมล์จากคนไม่รู้จัก** เพราะอีเมล์ที่มาจากคนไม่รู้จักอาจจะมีของแถมมาด้วยก็ได้โดยเฉพาะพวกไวรัส พุดน้อยคนนึงหล่ะที่ไม่ค่อยยอมเปิดอีเมล์ที่มาจากไหนก็ไม่รู้ เพราะไม่ชอบของแถม บรื๋อออ...
- **เว็บไซต์ปลอม** นอกจากนี้ เวลาใช้งานเว็บไซต์ต่างๆ เรามักจะเคยชินกับการคีย์ตัวอักษรเพียงไม่กี่ตัว แล้วบราวเซอร์ก็จะเด้งรายชื่อขึ้นมาให้เลือกแบบอัตโนมัติใช่มั้ยครับ นั่นแหละ.. ระวังให้ดี !!! เพราะอะไรรู้มั้ยครับ บางทีคนร้ายก็สร้างเว็บปลอมโดยสร้างให้โดเมน หรือ ชื่อเว็บไซต์มีความใกล้เคียงกับชื่อเว็บไซต์จริงมาก เช่น www.bangkok.or.th เป็น www.bamgkok.or.th เป็นต้น พอเด้งขึ้นมาอัตโนมัติเราก็มักจะกดกันทันทีโดยไม่ได้สังเกตรายละเอียดเล็กๆ น้อยๆ ทำให้เราเข้าไปที่เว็บไซต์ปลอมแทน ดังนั้น เวลาเราจะเข้าเว็บไซต์อะไร ก็ลองตรวจดูสักนิดนึงนะครับว่าใช่เว็บไซต์ที่เราจะใช้งานจริงหรือเปล่า และหากเราพิมพ์ชื่อเว็บไซต์เองได้ก็จะดีกว่านะครับ

● Check ก่อน Share... ไม่เสี่ยงผิดกฎหมาย การตรวจสอบข้อมูลก่อนที่จะส่งต่อนั้นเป็นอีกเรื่องนึงที่เราต้องระมัดระวังให้มากนะครับ เพราะว่ายุค Social Network ทำให้การรับรู้ข่าวสารและส่งต่อข่าวรวดเร็ว แต่ความรวดเร็วนี้อาจทำให้มีข้อมูลหรือข่าวมากมายที่ส่งต่อนั้นมาจากเพียงแค่กดแชร์โดยไม่ได้ตรวจสอบก่อน หลายคนเมื่อได้รับข่าว รูปภาพหรือข้อมูลเรื่องใดๆ มา ก็เชื่อและกดแชร์ในทันที โดยไม่ได้ตรวจสอบก่อนว่าข่าวดังกล่าวนั้นจริงหรือไม่ นั่นอาจจะทำให้คุณลำบากได้นะครับ เพราะอาจจะทำให้คุณกลายเป็นผู้ร่วมเผยแพร่ข่าวลวงได้ โดยที่คุณไม่รู้ตัว

น้องพุดดิ้งชวนรู้

พุดดิ้งขอแนะนำอีกหนึ่งหน่วยงานที่เป็นมืออาชีพด้านภัยคุกคามไซเบอร์ นั่นก็คือ ศูนย์ประสานการรักษาความมั่นคงปลอดภัย หรือ ไทยเซิร์ต (ThaiCERT) ภายใต้ ETDA ซึ่งมีภารกิจหลักในการจัดการปัญหาภัยคุกคามทางไซเบอร์ รับแจ้งเหตุภัยคุกคาม รวมทั้งการประสานงานและการแจ้งเตือนเหตุร้ายต่างๆ ให้พวกเราได้ระวังกันล่วงหน้า ซึ่งสามารถติดต่อได้ที่ โทร. 0-2123-1212 และสายด่วน 1212 หรือศึกษาข้อมูลเพิ่มเติมได้ที่เว็บไซต์ https://www.thaicert.or.th

รู้ไว้...เมื่อโดนโกง

ปัญหานี้คงไม่มีใครอยากให้เกิดขึ้น แต่ถ้าเกิดปัญหาอะไรขึ้นพุดน้อยอยากให้เพื่อนๆ ตั้งสติ แล้วพยายามรวบรวมข้อมูลทั้งหมดที่มีเอาไว้นะครับ เช่น อีเมล์ติดต่อซื้อขาย ข้อความที่ติดต่อกันด้วยช่องทางต่างๆ หน้าตาเว็บไซต์ที่เราเข้าไปใช้บริการ รายการโอนเงิน เป็นต้น แล้วรีบไปแจ้งความที่สถานีตำรวจ แต่อย่าบอกแค่ว่า “แจ้งเป็นหลักฐาน” นะครับ ควรจะบอกว่า “แจ้งความเพื่อดำเนินคดี” ซึ่งปกติเราสามารถแจ้งความได้ที่สถานตำรวจประจำท้องที่

นอกจากสถานีตำรวจแล้ว มีอีกที่หนึ่งที่พูดน้อยจะแนะนำ นั่นคือ “กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี” หากว่าเพื่อนๆ สงสัยว่าอาจเป็นการโจมตีคอมพิวเตอร์ ถูกแฮก หรือมีข้อมูลเกี่ยวกับความผิดคอมพิวเตอร์หล่ะก็ติดต่อไปได้นะครับที่ “กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา อาคาร B ชั้น 4 ถ.แจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210 หมายเลขติดต่อ 0-2142-2555-60” หรือสามารถแจ้งผ่านทางเว็บไซต์นี้ก็ได้นะครับ http://www.tcsd.in.th/petition

พูดน้อยว่าทางที่ดีติดต่อ หรือซื้อของอะไรกับใครไว้ ก็อย่าเพิ่งลบข้อมูลนั้นจนกว่าจะเรียบร้อยนะครับ เพราะข้อมูลเหล่านี้จะช่วยท่านได้หากมีปัญหา

Android Device Manager (แอนดรอย ดีไวซ์ เมเนเจอร์) :

ระบบฟีเจอร์สำหรับการระบุตำแหน่งของสมาร์ตโฟนหรือแท็บเล็ตที่ใช้ระบบปฏิบัติการของ Android ซึ่งมีความคล้ายกับ Find My iPhone ของ iOS และ Find My Phone ของค่าย Windows ทั้งยังสามารถสั่งล็อกโทรศัพท์ และลบข้อมูลทั้งหมดได้โดยการสั่งงานผ่านระบบรีโมท

Antivirus Software (แอนตี้ไวรัส ซอฟต์แวร์) :

ซอฟต์แวร์ที่ถูกสร้างขึ้นเพื่อนำมาใช้ในการป้องกัน ตรวจจับ และกำจัดโปรแกรมที่เป็นภัยคุกคามทางคอมพิวเตอร์ เช่น ไวรัสเวิร์ม โทรจัน และสปายแวร์ เป็นต้น

Encryption (เอนคริปชัน) :

การเข้ารหัสข้อมูลเพื่อให้เกิดความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์ โดยเปลี่ยนจากข้อมูลที่สามารถอ่านได้ ให้เป็นข้อมูลที่ไม่สามารถอ่านได้

Internet Security (อินเทอร์เน็ต ซีเคียวริตี้) :

โปรแกรมการเพิ่มความสามารถในการตรวจจับไวรัสที่ทำงานบนการเชื่อมต่ออินเทอร์เน็ตอัตโนมัติ เช่น ไวรัสสแปมเมล เป็นต้น

Internet Service Provider (อินเทอร์เน็ต เซอร์วิส โพรไวเดอร์) :

เป็นหน่วยงานให้บริการเชื่อมต่อเข้ากับเครือข่ายอินเทอร์เน็ต ทำหน้าที่เสมือนเป็นประตูเปิดการเชื่อมต่อให้บุคคลหรือองค์การให้สามารถใช้งานอินเทอร์เน็ตได้

IP Address (ไอพี แอดเดรส) :

Internet Protocal Address หมายเลขประจำเครื่องคอมพิวเตอร์ที่บ่งบอกถึงความมีตัวตนของผู้ใช้อินเทอร์เน็ต

iTunes Gift Card (ไอทูน กิ๊ฟ การ์ด) :

เป็นบัตรเติมเงินที่มีไว้สำหรับซื้อแอพพลิเคชันต่างๆ ใน App Store ของ Apple ซึ่งมีความมั่นคงปลอดภัยมากกว่าการซื้อแอพพลิเคชันผ่านบัตรเครดิต

Keylogger (คีย์ล็อกเกอร์) :

วิธีการดักขโมยข้อมูลรูปแบบหนึ่งที่บรรดาแฮกเกอร์ใช้ โดยมีลักษณะการดักจับตัวอักษรที่ผู้ใช้คอมพิวเตอร์ทำการคีย์ลงบน Keyboard

On-Screen Keyboard (ออน สกรีน คีย์บอร์ด) :

โปรแกรมคีย์บอร์ดเสมือนจริง โดยใช้เมาส์คลิกป้อนข้อมูลบนหน้าจอคอมพิวเตอร์ แทนการพิมพ์บนคีย์บอร์ด ซึ่งวิธีนี้สามารถใช้เพื่อหลีกเลี่ยงภัยจากการดักขโมยข้อมูลแบบ Keylogger ได้

Phishing (ฟิชชิ่ง) :

เทคนิคการขโมยข้อมูลชนิดหนึ่งของ Hacker โดยใช้หน้าเว็บไซต์ที่ออกแบบให้มีลักษณะคล้ายคลึงกับของจริง เพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบ

Privacy Setting (ไพรเวซี่ เซ็ตติ้ง) :

การตั้งค่านโยบายความเป็นส่วนตัวของผู้ที่ใช้บริการโซเชียลเน็ตเวิร์กต่างๆ ที่มีข้อกำหนดเกี่ยวกับการใช้งาน ซึ่งกำหนดจากโซเชียลเน็ตเวิร์กนั้นๆ

Real-Time Communication (เรียล-ไทม์ คอมมูนิเคชัน) :

การสื่อสารระหว่างบุคคลที่สามารถโต้ตอบกันได้ผ่านโครงข่ายอินเทอร์เน็ตและเครื่องมือสื่อสาร อาทิ คอมพิวเตอร์ สมาร์ตโฟน และแท็บเล็ต

Repackaging (รี แพคเกจจิ้ง) :

เทคนิคการขโมยข้อมูลชนิดหนึ่งของ Hacker ที่จะใช้ชื่อโปรแกรมที่มีการทำงานถูกต้องตามกฎหมาย แต่แทรกไปด้วยมัลแวร์ เผยแพร่ให้ดาวน์โหลดผ่านเว็บไซต์ต่างๆ เพื่อดักขโมยข้อมูลของผู้ที่หลงไปดาวน์โหลดโปรแกรมมาใช้งาน

Restart (รี สตาร์ท) :

การปิดและเปิดระบบคอมพิวเตอร์ใหม่ โดยไม่มีการเปลี่ยนแปลงค่าเริ่มต้นแต่อย่างใด ทั้งนี้ ยังเป็นการช่วยล้างข้อมูลจากแรม หากผู้ใช้งานใช้บริการจากคอมพิวเตอร์สาธารณะอีกด้วย

Review (รีวิว) :

หากตีตามความหมายตรงๆ จะแปลว่า การทบทวน แต่หากเป็นภาษาไอที จะมีความหมายในเชิงการตรวจสอบความเป็นมาของเว็บไซต์ แอพพลิเคชัน และอุปกรณ์ไอทีต่างๆ เช่น สมาร์ตโฟน และแท็บเล็ต

Shoulder Surfing (โชลเดอร์ เซิร์ฟฟิง) :

การถูกแอบมองจากผู้ไม่ประสงค์ดีในระหว่างการใช้คอมพิวเตอร์ในที่สาธารณะ ซึ่งนับภัยคุกคามทางคอมพิวเตอร์รูปแบบหนึ่ง ที่ผู้ใช้บริการต้องระวังตัว

Sign Out (ไซน์ เอาท์) :

การออกจากระบบโปรแกรมคอมพิวเตอร์ และเว็บไซต์ต่างๆ ที่ต้องทำการ Login เข้า และยังถือเป็นข้อควรระวังที่จะช่วยสร้างความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์ได้อีกวิธีหนึ่งด้วย

Spam Mail (สแปม เมล) :

จดหมายอิเล็กทรอนิกส์ที่ส่งเข้าสู่อีเมลของผู้ใช้บริการ โดยมีวัตถุประสงค์ เช่น การโจมตีจาก Hacker การโฆษณาสินค้า เป็นต้น

Terms of Service (เทริมส์ ออฟ เซอร์วิส) :

ข้อกำหนดในการใช้บริการโปรแกรมต่างๆ ก่อนทำการตกลงติดตั้งโปรแกรมหรือซอฟต์แวร์ ลงบนคอมพิวเตอร์ สมาร์ตโฟน และแท็บเล็ต

Tor Browser (ทอร์ เบราว์เซอร์) :

โปรแกรมการเชื่อมต่อแบบไม่เปิดเผยตัวตน ซึ่งสร้างโดยมูลนิธิพรมแดนอิเล็กทรอนิกส์ (อีเอฟเอฟ)

SSL Certificates :

หรือเรียกสั้นๆ ว่า SSL ย่อมาจาก Secure Socket Layer คือ เครื่องหมายรับรองความมั่นคงปลอดภัยทางอิเล็กทรอนิกส์ ที่ออกหรืออนุมัติโดย CA (Certificate Authority) เครื่องหมายเหล่านี้จะเป็นการรับรองมาตรฐานความมั่นคงปลอดภัย SSL ซึ่ง CA เป็นผู้อนุมัติ SSL Certificate ให้แก่เว็บไซต์ เพื่อยืนยันการมีตัวตนของเจ้าของเว็บไซต์และรับรองความมั่นคงปลอดภัยในการเข้ารหัส-ถอดรหัสข้อมูลด้วยระบบ SSL ผ่านการเรียกโปรโตคอล https:// ช่วยเพิ่มความมั่นใจให้กับผู้ใช้งานในการรับส่งข้อมูลสำคัญ

www.thaicert.or.th :

เป็นเว็บไซต์ที่รวบรวมข้อมูลสถิติข่าวสาร และบทความด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ เพื่อแจ้งเตือนและให้ข้อมูลแนะนำแก่ผู้ใช้งานทั่วไปและผู้ดูแลระบบ เป็นศูนย์การประสานงานเพื่อตอบสนองและจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ของไทย และให้การสนับสนุนข้อมูลต่างๆ ที่จำเป็นต่อหน่วยงานเพื่อดำเนินการแก้ไขเหตุการณ์ที่ได้รับแจ้งอีกด้วย

www.truehits.net :

ระบบให้บริการตรวจสอบสถิติการเยี่ยมชมเว็บไซต์ จุดมุ่งหมายของการจัดทำระบบให้บริการดังกล่าว คือ เพื่อให้หน่วยงานภาครัฐและเอกชน มีระบบการตรวจสอบสถิติการเยี่ยมชมเว็บไซต์ภายในประเทศ ซึ่งจะเป็นประโยชน์อย่างมากในการวิเคราะห์ความนิยมในเว็บไซต์ และเป็นเครื่องมือหนึ่งที่จะช่วยส่งเสริมให้เกิดการพัฒนาและปรับปรุงการนำเสนอข้อมูลผ่านเว็บไซต์ให้ดียิ่งขึ้นด้วย

www.cleanweb-thailand.com :

ชุมชนออนไลน์ใสสะอาด เป็นเว็บไซต์ที่รวบรวมข่าวสารและบทความเกี่ยวกับการกระทำความผิดทางเทคโนโลยีคอมพิวเตอร์ และเป็นศูนย์กลางข้อมูลของผู้ประกอบการเว็บไซต์และประชาชนในการติดตามความเคลื่อนไหวของผู้กระทำผิด หรืออาชญากรคอมพิวเตอร์ ซึ่งจะเป็นประโยชน์ในด้านการเฝ้าระวังภัยต่างๆ ทางออนไลน์ รวมทั้งยังเตือนภัยและเผยแพร่กลโกงต่างๆ ที่ทุกคนควรระมัดระวัง

หากจะให้ยกตัวอย่างแอพพลิเคชันสำหรับการสื่อสารที่คนไทยนิยมใช้มากที่สุดในขณะนี้ ก็คงหนีไม่พ้น LINE (ไลน์) โดยเฉพาะในกลุ่มผู้ใช้สมาร์ตโฟนและแท็บเล็ตในประเทศไทย

- ผู้ที่ใช้บริการระบบ iOS ดาวน์โหลดได้ที่ App Store
- ผู้ที่ใช้บริการระบบ Android ดาวน์โหลดได้ที่ Play Store
- ผู้ที่ใช้บริการระบบ Windows ดาวน์โหลดได้ที่ Windows Store

เมื่อทำการดาวน์โหลดและลงทะเบียน (Register) ด้วย E-mail หรือเบอร์โทรศัพท์แล้ว ความน่าสนใจต่างๆ ของ LINE ก็จะปรากฏขึ้นมาต่อหน้าของผู้ใช้บริการ รวมถึงทำการดึงชื่อเพื่อนในเบอร์โทรศัพท์ซึ่งกำลังใช้ Line อยู่เหมือนกันมาแสดง เพื่อให้เราไม่อยู่เหงาคนเดียวในโลกออนไลน์ นอกจากนี้ วิธีการเพิ่มเพื่อนใน LINE ยังมีวิธีอีกมาก ซึ่งกำลังจะนำเสนอต่อจากนี้

นานาวิธีเพิ่มเพื่อนใน LINE

1. เพิ่มจาก Contacts โทรศัพท์ : หากมีเพื่อนคนไหนใช้ LINE อยู่เช่นเดียวกับเรา โปรแกรมจะทำการดึงรายชื่อเพื่อนซึ่งกำลังใช้ LINE อยู่เหมือนกันมาแสดงโดยอัตโนมัติ

2. เพิ่มจาก QR Code : ในสมาร์ตโฟนหรือแท็บเล็ตทุกเครื่องที่ดาวน์โหลด Line ลงเครื่อง ภายในโปรแกรมจะมี QR Code เฉพาะไว้ให้เพื่อให้เราสามารถเพิ่มเพื่อนใหม่ๆ ที่อยู่ใกล้ตัวได้ไม่ยาก

3. เพิ่มจาก Shake It : เพื่อความเร้าใจในการค้นหาเพื่อน นี่จึงเป็นอีกวิธีหนึ่งที่ Line เพิ่มเข้ามา โดยสมาร์ตโฟนหรือแท็บเล็ตทั้ง 2 เครื่องจะต้องทำการเปิดโปรแกรมและเขย่าเครื่อง เท่านี้ก็สามารถเป็นเพื่อนกันได้แล้ว แถมยังได้ออกกำลังกายอีกด้วย

4. เพิ่มจาก Search by ID : หลายครั้งที่เราไม่สะดวกให้เบอร์โทรศัพท์ใคร แต่อยากให้มีการติดต่อเพียงผ่าน LINE เท่านั้น โปรแกรมจึงมีการกำหนดให้สามารถตั้ง ID ของผู้ใช้บริการ เพื่อให้ค้นหาเพื่อนผ่าน ID ที่ตั้งไว้แทนได้

การสื่อสารในหลายรูปแบบ

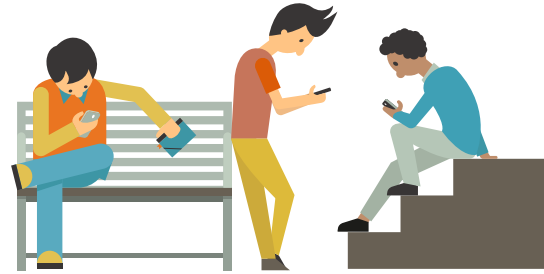
อีกหนึ่งลักษณะเด่นที่สำคัญของ LINE ซึ่งทำให้เป็นที่นิยมของผู้ใช้บริการในประเทศไทย ก็คือ การเป็นแอพพลิเคชันที่มีรูปแบบการสื่อสารมากมาย ไม่ว่าจะเป็น แชต (Chat) โทรด้วยเสียงฟรี (Free Voice Calls) และการคุยแบบเห็นหน้า (Video Calls) ขอเพียงแค่ทำการติดตั้งอินเทอร์เน็ตความเร็วสูงไว้บนเครื่องมือสื่อสาร เท่านี้ก็สามารถเลือกสนทนากันเพื่อนๆ ได้อย่างสนุกแล้ว

ส่งได้ทั้งภาพนิ่ง ภาพเคลื่อนไหวและคลิปเสียง

หากผู้ใช้บริการมีรูปภาพสวยๆ ที่ต้องการส่งให้เพื่อนๆ ได้เห็นด้วย แอพพลิเคชัน LINE ปัจจุบันก็ได้พัฒนาไปจนสามารถสนองความต้องการให้สามารถแนบรูปภาพ ไม่ว่าจะเป็น ภาพนิ่ง ภาพเคลื่อนไหว (Send Videos) หรือกระทั่งคลิปเสียง (Voice Message) ให้เพื่อนๆ ได้ทั้งหมด

สติ๊กเกอร์การ์ตูนน่ารักโดนใจ

นอกจากจะมีสัญลักษณ์แสดงความรู้สึก (Emoticons) แบบแอพพลิเคชันอื่นๆ แล้ว อีกหนึ่งความสนุกที่ทำให้ LINE ฮิตกันจนทั่วบ้านทั่วเมือง ก็คงจะหนีไม่พ้นการมีสติ๊กเกอร์ (Stickers) น่ารักๆ ไว้เล่นสนุกกับเพื่อนๆ ซึ่งก็มีให้ดาวน์โหลดมาเล่นกันทั้งแบบที่เสียค่าใช้จ่าย และแบบให้ดาวน์โหลดใช้ฟรี



การตั้งค่าความเป็นส่วนตัวใน LINE

อธิบายความน่าสนใจมาตั้งหลายข้อ จนเกือบจะลืมอธิบายถึงวิธีการสร้างความเป็นส่วนตัวในแอพพลิเคชัน LINE ซึ่งถือว่าสำคัญมาก เพราะจะช่วยทำให้เราสามารถใช้ LINE ได้อย่างมั่นคงปลอดภัย โดยมีขั้นตอนดังนี้

1. เปิดโปรแกรม LINE เข้าไปที่หน้า Setting

2. ในหน้า Setting จะพบกับหมวดต่างๆ มากมาย ให้เราตั้งค่าความเป็นส่วนตัว ดังนี้

- โปรไฟล์ส่วนตัว : หมวดการตั้งชื่อผู้ใช้ สถานะผู้ใช้ การตั้งค่าไอดี และการสร้างคิวอาโค้ด โดยปัจจุบันในหมวดนี้ได้ถูกพัฒนาไปให้สามารถกำหนดค่าได้แล้วว่า ทุกครั้งที่โพสต์รูปภาพ เราจะอนุญาตให้ภาพดังกล่าวแชร์ออกไปสู่สาธารณะหรือไม่

- บัญชี : ในหมวดนี้เราสามารถตั้งค่า และตรวจสอบทะเบียนบัญชีอีเมล หมายเลขโทรศัพท์ หรือลิงก์จากเฟซบุ๊ก ที่เราทำการลงทะเบียนใช้งานไว้ได้

- แชต-โทร : ในหมวดนี้เราสามารถตั้งค่าฟีเจอร์ เช่น การอนุญาตให้เพื่อนโทรเข้า ดาวน์โหลดรูปอัตโนมัติ หรือขนาดของตัวอักษรในระหว่างการแชตได้

- บริหารรายการเพื่อน : ในหมวดนี้เราสามารถตรวจสอบ การตั้งค่าเพิ่มเพื่อนได้ว่า จะอนุญาตให้เพิ่มโดยอัตโนมัติหรือไม่ อีกทั้งยังสามารถบล็อกลิสต์เพื่อนที่ไม่ต้องการให้เข้าถึงความเป็นส่วนตัวของเราได้ด้วย


มืออาชีพ
ด้านภัยคุกคาม
ไซเบอร์

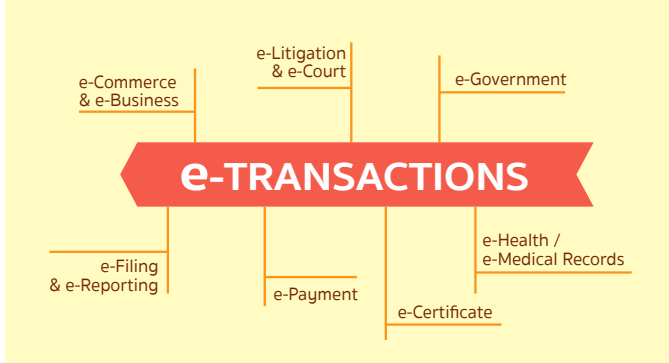
หน่วยงาน	เว็บไซต์	ติดต่อ	ภารกิจ
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ภายใต้เอ็ทด้า กระทรวงไอซีที	https://www.thaicert.or.th	โทร. 0-2123-1212 และสายด่วน 1212 อีเมล office@thaicert.or.th, report@thaicert.or.th	รับแจ้งเหตุภัยคุกคาม รวมทั้งประสานงานระหว่างหน่วยงานภาครัฐ เอกชน มหาวิทยาลัย เพื่อจัดการกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
ศูนย์รับเรื่องร้องเรียนออนไลน์ ภายใต้เอ็ทด้า กระทรวงไอซีที	https://www.etda.or.th	โทร. 0-2123-1223 อีเมล occ@etda.or.th	ให้คำปรึกษาด้านปัญหาที่เกิดจากการซื้อขายสินค้าและบริการออนไลน์ เช่น การฉ้อโกงเงินออนไลน์ การแก้ปัญหากับคู่กรณี และไกล่เกลี่ยข้อพิพาทผ่านระบบออนไลน์
ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย	https://www.1213.or.th	สายด่วนโทร. 1213 อีเมล fcc@bot.or.th	เป็นศูนย์กลางในการดำเนินงานการคุ้มครองผู้ใช้บริการทางการเงินในรูปแบบต่างๆ
กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร	https://www.hightechcrime.org	โทร. 0-2205-2627 อีเมล team@hightechcrime.org	ให้องค์ความรู้ในการทำงานของเจ้าหน้าที่ตำรวจและองค์ความรู้ด้านเทคโนโลยี เพื่อช่วยสนับสนุนเจ้าหน้าที่ตำรวจทั่วประเทศในการดำเนินคดีอาชญากรรมทางด้านเทคโนโลยี
สำนักงานคณะกรรมการคุ้มครองผู้บริโภค	https://www.ocpb.go.th	สายด่วนโทร. 1166 อีเมล consumer@ocpb.go.th	รับเรื่องราวร้องทุกข์จากผู้บริโภคที่ได้รับความเดือดร้อนจากการกระทำของผู้ประกอบธุรกิจที่ทำกับลูกค้าหากไม่เป็นธรรม

เกี่ยวกับ ETDA

ETDA เพื่อชีวิต เศรษฐกิจ ดิจิทัล เดินหน้าอย่างมั่นคงปลอดภัย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ ETDA (เอ็ตด้า) เป็นองค์กรสำคัญในการผลักดัน พัฒนา ส่งเสริมและสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทยให้เติบโตอย่างมั่นคงปลอดภัย ทัดเทียมผู้นำในภูมิภาค ภายใต้กระบวนการพัฒนาที่เรียกว่า “เศรษฐกิจดิจิทัล” (Digital Economy)

ETDA ส่งมอบการพัฒนาการทำธุรกรรมอิเล็กทรอนิกส์ของประเทศอย่างครบวงจร



➔ e-Commerce & e-Business ส่งเสริมการซื้อขายสินค้าและบริการผ่านอินเทอร์เน็ต รวมถึงสร้างขีดความสามารถในการแข่งขันและสร้างโอกาสในการเข้าสู่ตลาดโลกแก่ผู้ประกอบการไทย โดยเฉพาะ SME และ OTOP

➔ e-Litigation & e-Court ผลักดันการดำเนินคดีอิเล็กทรอนิกส์และจัดเก็บข้อมูลเกี่ยวกับการทำธุรกรรมออนไลน์เพื่อเข้าสู่ระบบศาลอิเล็กทรอนิกส์อย่างเต็มรูปแบบ

➔ e-Government บริการภาครัฐด้วยระบบออนไลน์ที่สะดวก รวดเร็ว แก่ภาคธุรกิจและประชาชน

➔ e-Filing & e-Reporting จัดทำระบบการยื่นคำร้องคำขอหนังสือ / เอกสารทางอิเล็กทรอนิกส์ /การจัดทำรายงานและเผยแพร่ในรูปแบบอิเล็กทรอนิกส์

➔ e-Payment พัฒนาระบบการทำธุรกรรมทางการเงินผ่านอินเทอร์เน็ต เพื่อเพิ่มประสิทธิภาพของระบบการชำระเงินทางอิเล็กทรอนิกส์

➔ e-Certificate จัดทำระบบให้บริการออกหนังสือรับรองทางอิเล็กทรอนิกส์

➔ e-Health / e-Medical Records จัดทำระบบเชื่อมโยงข้อมูลด้านสุขภาพไทย เพื่อยกระดับสาธารณสุขไทย

ก้าวต่อไปของ ETDA จะพิสูจน์ให้เห็นว่า ธุรกรรมออนไลน์ของไทยจะเปี่ยมไปด้วยประสิทธิภาพ ทำให้ผู้ใช้งานเกิดความเชื่อมั่น สามารถเพิ่มโอกาสทางเศรษฐกิจของประเทศได้อย่างมหาศาล ควบคู่ไปกับสร้างสรรค์คุณภาพชีวิตที่ดีให้กับคนไทยอย่างแท้จริง

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
อาคารเดอะไนน์ ทาวเวอร์ เลขที่ 33/4 ตึก B ชั้น 21 ถนนพระรามเก้า
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310 โทรศัพท์ 0-2123-1234 โทรสาร 0-2123-1200
สพธอ. www.etda.or.th

ฉลาดรู้เน็ต 2

ตอน Trust on Internet (ToI)

เราปั้นหนังสือเล่มนี้เพื่อคุณ :

- ○ เถ้าแก่ยุคไอที
- ○ นักช้อปออนไลน์
- ☑ ครอบครัวไซเบอร์

สร้างสรรค์โดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
อาคารเดอะไนน์ ทาวเวอร์ เลขที่ 33/4 ตึก B ชั้น 21 ถนนพระรามเก้า
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310
โทรศัพท์ 0-2123-1234 โทรสาร 0-213-1200
สพธอ. www.etda.or.th
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร www.mict.go.th

ISBN 978-616-7956-04-6