



การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

องค์ความรู้ (One Point Knowledge)

10 ภัยอันตรายจาก Social Network

กลุ่ม SGA : รู้ทัน Social เปรี้ยวกว่าใคร หน่วยงาน สายงานเทคโนโลยีสารสนเทศ	ผู้อนุมัติ (คณะกรรมการย่อยสายงาน) (ลงชื่อ)..... <i>จิราภา งาม</i> (นางพิศวาท ภาพสุวรรณ) ตำแหน่ง <i>ผอ.ฝ่ายท.</i>
องค์ความรู้เรื่อง 10 ภัยอันตรายจาก Social Network	23/05/60 รหัส OPK <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

10 ภัยอันตรายจาก Social Network

OPK ฉบับนี้เป็นการบอกรายละเอียดของภัยอันตรายของ Social Network เพื่อเป็นแนวทางให้ผู้ใช้ใช้งาน Social Network อย่างระมัดระวัง เพื่อความปลอดภัย เพื่อให้รู้เท่าทันภัยคุกคามจากการเข้าใช้งาน Social Network

10 ภัยอันตรายจาก Social Network มีดังนี้

1. หลอกว่ามาดีแต่จริง ๆ ประสงค์ร้าย (Social Engineering Attack on Social Network) – การโจมตีที่ตัวบุคคลในลักษณะที่คาดไม่ถึง ในรูปแบบ Application/Game บน Facebook เมื่อคลิกเข้าไปใช้งาน Application/Game ดังกล่าว ก็จะตกเป็นเหยื่อของอาชญากรโดยไม่ทันตั้งตัว
2. ล่อเหยื่อตกปลาออนไลน์ (Phishing Attack) – เทคนิคการล่อลวงโดยการส่ง URL Link ปลอมไปยังอีเมลล์ หรือ URL Shorten ในลักษณะของ Clip Video/File รูปภาพ ในการนำไปสู่เว็บไซต์ปลอม เพื่อดักขโมยข้อมูลส่วนตัวของผู้ใช้
3. โค้ดร้ายฝังลึก (Cross Site Scripting Attack) – เทคนิคการโจมตี Facebook โดยการฝัง Code/Script ของอาชญากรเข้าไปบนเว็บไซต์ที่มีช่องโหว่ ซึ่งข้อมูลสำคัญของผู้ใช้งาน Facebook เช่น Username/Password จะถูกส่งกลับมาให้อาชญากรทันที
4. ถูกสวมรอยง่าย ๆ แค่อ่าน Facebook อย่างไม่ระวัง (Cross Site Request Forgery Attack) – เทคนิคที่อาชญากรโจมตีผู้ใช้ Facebook/Internet Banking โดยการขโมยสิทธิ (Credential) ที่ผู้ใช้ได้ล็อกอินเว็บไซต์ค้างไว้ไปใช้งานต่อ เช่น ทำการโอนเงินออกจากบัญชีของผู้ใช้งานระบบ Internet Banking โดยผู้ใช้ไม่รู้ตัว
5. หลอกให้คลิกแต่แอบซ่อนมีดไว้รอเชือด (Click jacking or UI Redressing Attack) – เทคนิคการโจมตีผู้ใช้งาน โดยหลอกให้คลิกรูปที่ล่อตาต่อใจบนเว็บไซต์ ซึ่งอาชญากรจะแอบซ่อน Invisible frame ไว้ โดยมี Script มุ่งร้ายแอบซ่อนอยู่
6. โดนหลอกล่อให้ไปเจอ Link ที่อาชญากร รออยู่ (Drive-by Download Attack) – เทคนิคโจมตี ด้วยโปรแกรมประสงค์ร้าย ที่สามารถทำการติดตั้งลงบนเครื่องของผู้ใช้งาน Facebook เพียงแค่ผู้ใช้งานเข้าไปเว็บไซต์ที่อาชญากรโพสต์ เป็น Link ล่อเหยื่อไว้บน Facebook Page และผู้ใช้งานเผลอตาวนโหลดโดยไม่รู้ตัว
7. เทคนิคการโจรกรรมข้อมูลขั้นสูงแบบต่อเนื่อง - APT (Advance Persistent Threat) and MitB (Man-In-The-Browser Attack) เป็นเทคนิคการโจมตีขั้นสูงที่มุ่งเน้นเป้าหมายผู้ใช้งาน Internet Banking ผู้ใช้งานคอมพิวเตอร์ในระดับองค์กร หรือ รัฐบาล โดยอาชญากรสามารถฝังโปรแกรมมุ่งร้าย เข้าไปในระบบคอมพิวเตอร์ของเป้าหมาย เพื่อแอบโจรกรรมข้อมูลลับ อย่างต่อเนื่อง เป็นระยะเวลานาน ซึ่งยากต่อการตรวจสอบด้วยโปรแกรม Anti-virus ทั่วไป

8. โดนดักข้อมูลลับระหว่างทาง (Identity Theft) - เทคนิคการโจมตีผู้ใช้งาน Facebook โดยอาชญากรจะทำการดักจับข้อมูลที่ส่งไปมาระหว่างผู้ใช้งาน Facebook กับ www.facebook.com แบบเงียบ เพื่อขโมย Username และ Password ของผู้ใช้ และอาจลุกลามไปถึง E-mail Account ด้วย ถ้าใช้ Username และ Password เดียวกัน กับ Facebook
9. บอกเพื่อนว่าเราอยู่ที่ไหน (บอกโจรว่าเราไม่อยู่บ้าน) (Your GPS Location Exposed) - การใช้งานเครือข่ายสังคมออนไลน์อย่าง Facebook หรือ Twitter นั้น อาจทำให้ข้อมูลตำแหน่งที่อยู่ปัจจุบัน (GPS Location) ของผู้ใช้งาน Facebook หรือ Twitter สามารถถูกเปิดเผยสู่สาธารณะได้ โดยที่เราไม่รู้ตัว จากการใช้งานโปรแกรม ประเภท Foursquare, Google Latitude และ Facebook Place
10. ระวังข้อมูลส่วนตัวหลุดรั่วขณะเล่น Facebook เพลินๆ (Your Privacy Exposed) - ข้อมูลส่วนตัวของผู้ใช้ Facebook อาจถูกเปิดเผยสู่สาธารณะได้ ถ้าผู้ใช้งาน Facebook ไม่ได้ปรับแก้การตั้งค่าแบบ Default ให้เป็นแบบที่ปลอดภัยมากขึ้น



การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

องค์ความรู้ (One Point Knowledge)

เล่น Social อย่างไรไม่ผิด พรบ.

กลุ่ม SGA : รู้ทัน Social เปรี้ยวกว่าใคร หน่วยงาน สายงานเทคโนโลยีสารสนเทศ	ผู้อนุมัติ (คณะกรรมการย่อยสายงาน.....) (ลงชื่อ)..... <i>วิมล งาม</i> (นางพิศวาท ภาพสุวรรณ) ตำแหน่ง ผอ.ฝ่ายท.
องค์ความรู้เรื่อง เล่น Social อย่างไรไม่ผิด พรบ.	23/05/60 รหัส OPK <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

เล่น Social อย่างไรไม่ผิด พรบ.

OPK ฉบับนี้เป็นการบอกรายละเอียดเกี่ยวกับ พรบ.คอมพิวเตอร์ เพื่อเป็นแนวทางให้ผู้ใช้งาน ไม่กระทำการเข้าข่ายทำผิด พรบ.คอมพิวเตอร์ นั้นเอง

บทนำ



พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ช่วงเวลานี้ ผู้ใช้อินเทอร์เน็ตมีจำนวนมากขึ้น โดยเฉพาะ Social network ก็ใช้กันแพร่หลาย ในการติดต่อสื่อสารหาเพื่อนๆ ตลอดจนดาราใช้ติดต่อกับแฟนคลับจำนวนมาก ไม่เว้นแบรนด์เอเจนซี โฆษณาต่างๆยังใช้ Social Network ด้วย แต่ก็มีหลายเหตุการณ์ที่คุณอาจไม่ทราบว่า สิ่งที่ทำแบบนี้ อาจทำให้ตนเองทำผิด พรบ.คอมพิวเตอร์ ปี 2550 ด้วย ซึ่งตอนนี้มีผลบังคับใช้ในไทยแล้ว ณ เวลานี้

พรบ.คอมพิวเตอร์ปี 50 (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550) เริ่มบังคับใช้เมื่อ 10 มิถุนายน 2550 จนถึงเวลานี้ก็บังคับใช้มาถึง 6 ปีแล้ว ซึ่งมีหลายมาตรา ที่ผู้ใช้งานอินเทอร์เน็ตต้องทำความเข้าใจและปฏิบัติให้อยู่ในกรอบของกฎหมาย หากฝ่าฝืนอาจถูกดำเนินคดีได้

ผู้ใช้อินเทอร์เน็ต หรือเล่น Social network ต้องมีความรู้ในเรื่องนี้เพื่อป้องกันไม่ให้ผิด พรบ. หรือผิดกฎหมายโดยไม่รู้ตัวนั่นเอง

ตัวอย่างการกระทำ หรือการโพสต์ ข้อมูลปลอม ข้อมูลเท็จ อย่างกรณีของอดีตเนรค่าที่มีการโพสต์ข้อความแสดงอิทธิฤทธิ์อวดอ้างผ่านทางเว็บไซต์ให้คนหลงเชื่อ หรือ ให้ข้อมูลเท็จ ที่จะเกิดความเสียหายต่อความมั่นคงของประเทศ ประชาชนต้นตระหนัก , โปสข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้าย รวมทั้งการเผยแพร่ข้อมูล ลามก อนาจาร

ซึ่งกรณีทั้งหมดนี้ ผิด พรบ.คอม มาตรา 14 ระบุไว้ว่า “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือ ข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔) “

อีกกรณีที่ต้องระวังสำหรับผู้ใช้อินเตอร์เน็ต Social Network โดยเฉพาะกลุ่มคนที่ เจออะไร ขอกดแชร์ หรือส่งต่อ เช่นได้ข้อความมาใน Line, หรือทาง Facebook , Twitter เจอปุ๊บ share ปุ๊บ หรือส่งต่อให้กับเพื่อนๆ ทั้งทาง Line หรือทางอีเมล โดยที่ไม่ได้ตรวจสอบก่อนว่าข้อความนั้น จริงรึเปล่า....? หากเฟลแชร์ทันที ทั้งๆเป็นข้อมูลเท็จ การกระทำลักษณะแบบนี้ ผิด พรบ.คอมพิวเตอร์ ซึ่งหากตรวจสอบว่าผิดจริง ผู้แชร์ก็อาจถูกดำเนินคดี ได้ และอาจถึงขั้นจำคุก หรือปรับ

ก่อนส่งต่อ หรือแฮร์ ลองตรวจสอบข้อมูลก่อนว่าเนื้อหาจริงหรือไม่ เพราะถ้าคุณส่งข้อมูลเท็จ ข้อมูลที่เกิดความเสียหายต่อผู้อื่น หรือต่อความมั่นคงของประเทศ ข้อมูลลามก อนาจาร ตามข้อมูลที่มีความผิดตาม พรบ. คอม คุณก็จะมีผิดตามมาตรา 14 วรรค 5 โดนด้วย!...รับโทษเหมือนกัน

อีกเรื่องที่เจอบ่อย คือการติดต่อภาพที่ทำให้ผู้อื่นเสียหายแล้ว เผยแพร่ทางอินเทอร์เน็ต อันนี้ มีความผิดตามมาตรา 16 ระบุไว้ว่า

“ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูล คอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือ ปรับไม่เกิน หกหมื่นบาท หรือทั้งจำทั้งปรับ”

สำหรับผู้ให้บริการ ก็ต้องระวัง หมั่นดูแลข้อมูลต่างๆที่คนอื่นโพสต์ทิ้งไว้ในเว็บเราด้วย เช่นพวกเว็บบอร์ด กระหู่ หรือ ความเห็นต่างๆ เพราะมีคนมาโพสต์ข้อความ โพสต์รูปที่ทำให้บุคคลอื่นเสียหาย หรือภาพอนาจาร มีเนื้อหาพาดพิงสถาบัน แล้วคุณเพิกเฉย ปล่อยให้มีการกระทำนั้น คุณก็จะมีผิด พรบ.คอมพิวเตอร์ ในมาตรา 15 ข้อหาสนับสนุน ยินยอมให้คนอื่น เผยแพร่ข้อมูลที่กระทบให้ผู้อื่นเดือดร้อน เสียหาย กระทบความมั่นคงของรัฐ และอื่นๆตามที่ พรบ.คอม มาตรา 14 ซึ่งกรณีนี้เกิดขึ้นมาแล้วตั้งแต่เริ่มใช้ พรบ.คอม ช่วงแรกๆด้วย มีเว็บมาสเตอร์ถูกจำคุกมาแล้ว ทั้งๆที่ไม่ได้เป็นผู้กระทำผิด แต่ตรวจสอบพบเนื้อหาที่ผิด พรบ.คอม ก็โดนติดคุกได้เช่นกัน และมีการตรวจสอบข้อมูลของผู้ให้บริการโฮสต์ด้วย

พรบ.คอมพิวเตอร์ เป็นเรื่องใกล้ตัวที่ผู้ใช้อินเทอร์เน็ตต้องรู้ และปฏิบัติให้อยู่ในกฎหมาย ด้วย หากกระทำผิด พรบ. คุณก็ จะถูกดำเนินคดี จำคุก และปรับ ได้ ซึ่งคุณอาจไม่ได้ว่าคุณไม่รู้!! เพราะคุณคือผู้ใช้อินเทอร์เน็ต ต้องอยู่ภายใต้กฎหมาย พรบ.คอมพิวเตอร์



การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

องค์ความรู้ (One Point Knowledge)

9 ข้อระวัง “ติดคุก” ไม่ควรโพสต์ลงโซเชียล

กลุ่ม SGA : รู้ทัน Social เปรี้ยวกว่าใคร หน่วยงาน สายงานเทคโนโลยีสารสนเทศ	ผู้อนุมัติ (คณะกรรมการย่อยสายงาน.....) (ลงชื่อ)..... <i>วิมล งาม</i> (นางกิสวาท ภาพสุวรรณ)
องค์ความรู้เรื่อง 9 ข้อระวัง “ติดคุก” ไม่ควรโพสต์ลงโซเชียล	ตำแหน่ง <i>ผ.ฝ่ายท.</i> 23/05/60 รหัส OPK <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

9 ข้อระวัง “ติดคุก” ไม่ควรโพสต์ลงโซเชียล

OPK ฉบับนี้เป็นการบอกรายละเอียดของเรื่องราวต่างๆ ที่ไม่ควรโพสต์ลง Social Media เพื่อเป็นแนวทางให้ผู้ใช้งาน ไม่กระทำการเข้าข่ายกระทำความผิดกฎหมาย

บทนำ

ปัจจุบันยอดผู้ใช้โซเชียลมีเดียไทยพุ่งแตะเป็นอันดับ 3 ของอาเซียน โดยเฉพาะโซเชียลมีเดียอย่าง Facebook ที่มีผู้ใช้ไทยกว่า 35 ล้านบัญชี เฉพาะแค่กรุงเทพมหานครมีผู้ใช้ถึง 20 ล้านบัญชีไปแล้ว ยังมีผู้ใช้เยอะขึ้นเท่าไร ดูเหมือนปัญหาจากพฤติกรรมโพสต์และแชร์ของผู้ใช้ก็มีมากขึ้นเป็นเงาตามตัว เนื่องจากคิดว่าเป็นบริการที่อิสระ สามารถโพสต์อะไรไปก็ได้ และคิดว่าไม่มีกฎหมายรองรับ

แต่หารู้ไม่ว่าความผิดฐานโพสต์ข้อมูล ความคิดเห็น หรือรูปภาพต่างๆ ที่ไม่เหมาะสมนั้น เข้าข่ายกระทำความผิดกฎหมาย ซึ่งวันนี้เราได้นำข้อมูลจาก TCSD หรือ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ที่ดูแลเรื่องนี้โดยเฉพาะมาเตือนผู้ใช้โซเชียลมีเดียกัน

9 ข้อที่เสี่ยงติดคุก เมื่อโพสต์ลงโซเชียลมีเดีย มีอะไรบ้าง?

1. สร้างข่าวลือและเผยแพร่

ไม่ว่าจุดประสงค์ของคุณจะทำไปโดยเจตนาหรือแค่ขำๆ แต่การสร้างข่าวลือให้ผู้คนแตกตื่นหรือตกใจในวงกว้าง ไปจนถึงทำให้สังคมและบ้านเมืองเกิดความสับสนและวุ่นวาย ถือเป็นความผิดตามกฎหมายซึ่งมีโทษจำคุกถึง 5 ปี ปรับ 100,000 บาท หรือทั้งจำทั้งปรับ

2. โพสต์รูปเปลือยกาย รูปลามก

แม้จะเป็นแอคเคาท์ส่วนตัว และคุณคิดว่าการโพสต์ลงบนพื้นที่ของตัวเองจะมีสิทธิ์เสนอข้อมูลอะไรก็ได้ แต่ผิดนัดครับ โดยเฉพาะการลงรูปโป๊เปลือย ภาพอนาจารของตัวเองหรือแม้แต่ภาพคนอื่น ก็มีความผิดทางกฎหมาย และมีโทษปรับ 100,000 บาท โทษจำคุก 5 ปี หรือทั้งจำทั้งปรับครับ

3. แต่งเรื่องให้ร้ายผู้อื่น

คุณเองก็คงไม่ชอบใจหากมีใครใส่ร้ายคุณ เช่นเดียวกันกับผู้อื่นที่ถูกประนามและหยามเหยียด เพื่อใส่ความโดยไม่ใช่เรื่องที่เกิดขึ้นจริง ซึ่งเมื่อถูกโพสต์ลงโซเชียลไปแล้วทำให้เกิดความอับอายแก่ผู้ถูกใส่ร้าย โดยความผิดนี้มีโทษตามกฎหมายปรับถึง 100,000 บาท จำคุก 5 ปี หรือทั้งจำทั้งปรับทีเดียว

4. ใช้เทคนิคตัดต่อภาพทำให้คนอื่นเสียหาย

การนำภาพบุคคลใดๆ ไปตัดต่อเล่นแล้วโพสต์หรือจงใจตัดต่อภาพ ทั้งภาพนิ่งและภาพเคลื่อนไหว เพื่อทำลายความน่าเชื่อถือหรือสร้างความเสียหายให้แก่ผู้อื่น รู้หรือไม่ว่านั้นเป็นความผิดตามกฎหมาย ซึ่งมีโทษปรับ 60,000 บาท และจำคุก 3 ปี หรือทั้งจำทั้งปรับ

5. ตั้งใจขโมยข้อมูลส่วนตัว

การส่องโซเชียลมีเดียส่วนตัวของผู้อื่น เพื่อนำข้อมูลผู้ใช้หรือรหัสของบุคคลอื่นไปแสวงหาผลประโยชน์หรือนำไปใช้ในการกระทำใดๆ ที่ส่งผลเสียต่อเจ้าของแอคเคาท์ ถือว่าเข้าข่ายความผิด พ.ร.บ คอมพิวเตอร์ตามข้อกฎหมายเรื่องลิขสิทธิ์

6. แก๊ซ ดัดแปลงข้อความผู้อื่น

โทษปรับ 100,000 บาท จำคุก 5 ปี หรือทั้งจำทั้งปรับเลยทีเดียว หากมีการนำข้อมูลในโซเชียลมีเดียของผู้อื่นไปแก๊ซหรือดัดแปลง และทำให้เกิดความเสื่อมเสียหรือเสียหายต่อเจ้าของข้อมูล

7. แชรต์ต่อๆ กันมาอีกที

ความรู้เท่าไม่ถึงการณ์ ก็อาจทำให้คุณติดคุกได้จากการแชร์ข้อมูลไม่เลือก และไม่ตรวจสอบข้อเท็จจริงก่อน เมื่อเห็นคนแชร์มาก็แชร์ต่อหรือนำไปโพสต์ต่อ ซึ่งอาจเป็นข้อมูลเท็จที่ส่งผลกระทบต่อสังคมโดยรวมและทำลายชื่อเสียงของบุคคลอื่นได้ ซึ่งการแชร์ลักษณะนี้ถือเป็นการผิดตามกฎหมายอีกด้วย

8. แชรต์ข้อความลูกโซ่

มีโทษปรับ 100,000 บาท จากความผิดฐานแชร์ข้อความลูกโซ่ที่ไม่เป็นความจริงหรือทำให้เกิดความเสียหายต่อผู้ใดผู้หนึ่ง ซึ่งอาจทำให้คนรับสารเกิดความเข้าใจผิดและกระทำตามข้อความที่แชร์นั้นหรือมีไวรัสติดมากับแชร์ดังกล่าวได้ เช่น แชรต์ต่อไปอีก 10 คนจะโชคดี หรือแชร์ลูกโซ่รูปแบบอื่นๆ เป็นต้น

9. โปสต์หมิ่นเบื้องสูง

การหมิ่นสถาบันเบื้องสูงด้วยการโพสต์ข้อความ ทำรูปภาพ สร้างเพจหรือเว็บไซต์หมิ่น อันเป็นการทำให้เสื่อมเสียต่อสถาบันซึ่งกระทบต่อความมั่นคงภายในประเทศ จะมีโทษจำคุก 15 ปี ตาม พ.ร.บ.คอมพิวเตอร์

ทีนี้จะโพสต์จะแชร์อะไร ลองคิดก่อนซึกนิตดีกว่าว่าไปกระทบต่อผู้ใดและสร้างความวุ่นวายต่อสังคมหรือไม่ เพราะเมื่อทำการโพสต์โดยเจตนาไปแล้ว “กฎหมายก็พร้อมทำงานทันที”



การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

One Point Lesson: OPL

ชื่อเรื่อง	การแชร์ข้อมูลบน Facebook	ลำดับ	5	
		วันที่เขียน	4 พ.ค. 2560	
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		สมโภช เกียรติกสิกร	เบญจมาศ อรรถวิเศษชัยกุล	จิราภา อภินันท์
		04/05/60	23/05/60	23/05/60

วัตถุประสงค์

เพื่อความปลอดภัยในการแชร์ข้อมูล

เนื้อหา



การแชร์ข้อมูลบน Facebook นั้นสามารถกำหนดการเข้าถึงได้ ซึ่งมีรูปแบบให้เลือกคือ Public, Friends, Friends except..., Specific Friends, Only me

โดยในการแชร์ข้อมูลต่างๆ ถ้าต้องการให้เห็นเฉพาะเพื่อน ให้เลือก Friends เพื่อความปลอดภัยในการเข้าถึงข้อมูล

ส่วน Public เป็นการแชร์ข้อมูลแบบสาธารณะ ซึ่งผู้ใช้งาน Facebook ทั้งที่เป็นเพื่อนและไม่ได้เป็นเพื่อนจะเห็นโพสต์นี้ ซึ่งในการแชร์ข้อมูลที่สำคัญต่าง นั้นไม่ควรแชร์แบบ Public เพื่อความปลอดภัยนั่นเอง

วันที่สอน						
ผู้สอน						
ผู้เรียน						
ผลการเรียนรู้						



การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

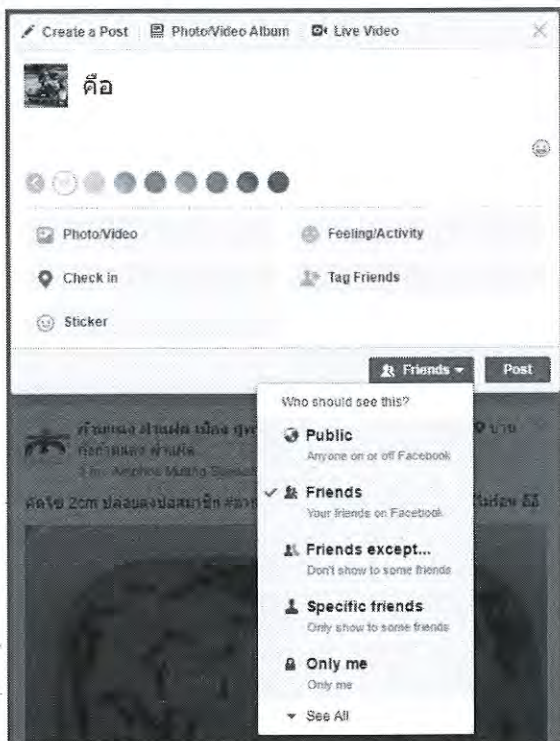
One Point Lesson: OPL

ชื่อเรื่อง	การเข้าถึงโพสต์บน Facebook	ลำดับ	6	
		วันที่เขียน	4 พ.ค. 2560	
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		สมโภช เกียรติกสิกร	นางนุช กอด้งภักดิ์	วิมล งาม
		04/05/60	23/05/60	23/05/60

วัตถุประสงค์

เพื่อความปลอดภัยในการโพสต์ข้อมูล

เนื้อหา



การโพสต์ข้อความบน Facebook นั้นสามารถกำหนดการเข้าถึงได้ ซึ่งมีรูปแบบให้เลือกคือ Public, Friends, Friends except..., Specific Friends, Only me

โดยในการโพสต์ข้อความ ถ้าต้องการให้เห็นเฉพาะเพื่อน ให้เลือก Friends เพื่อความปลอดภัยในการเข้าถึงข้อมูล

ส่วน Public เป็นการโพสต์ข้อมูลแบบสาธารณะ ซึ่งผู้ใช้งาน Facebook ทั้งที่เป็นเพื่อนและไม่ได้เป็นเพื่อนจะเห็นโพสต์นี้ ซึ่งในการโพสต์ข้อมูลที่สำคัญต่าง นั้นไม่ควรโพสต์แบบ Public เพื่อความปลอดภัยนั่นเอง

วันที่สอน						
ผู้สอน						
ผู้เรียน						
ผลการเรียนรู้						



การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

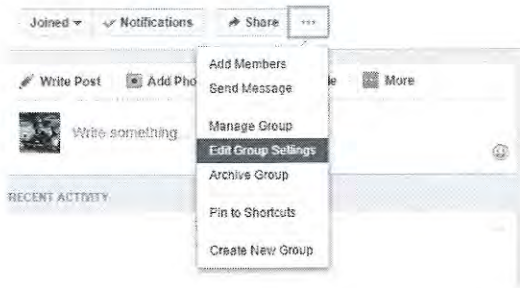
One Point Lesson: OPL

ชื่อเรื่อง	เทคนิคการตั้งค่ากรุปใน Facebook	ลำดับ	7	
		วันที่เขียน	4 พ.ค. 2560	
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		สมโภช เกียรติกสิกร	ชวรงค์ เวรกันณศิริ	วิวัฒน์
		04/05/60	23/05/60	23/05/60

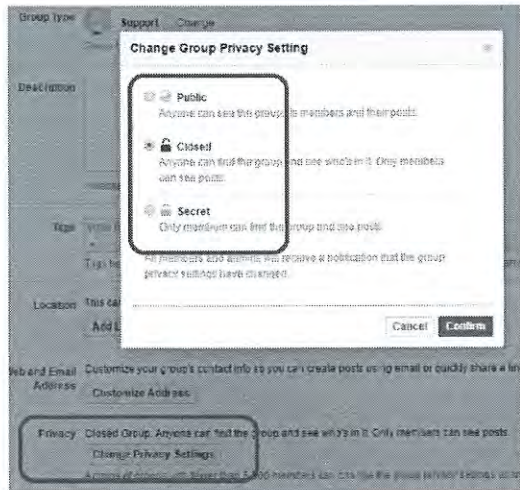
วัตถุประสงค์

เพื่อความปลอดภัยของข้อมูล และการเข้าถึงกรุปใน Facebook

เนื้อหา



เมื่อตั้งกรุปของ Facebook ขึ้นมาแล้ว Admin ของ Group สามารถตั้งค่าการเข้าถึงกรุปได้ โดยเข้าที่ Edit Group Settings และคลิกที่ Change Privacy Setting



Admin ของ Group สามารถตั้งค่ากรุปให้เป็น Public (สาธารณะ), Closed (กลุ่มปิด) หรือ Secret (กลุ่มลับ) ได้ตามต้องการ

วันที่สอน						
ผู้สอน						
ผู้เรียน						
ผลการเรียนรู้						



การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

องค์ความรู้ (One Point Knowledge)

เทคนิคการใช้งาน Facebook อย่างปลอดภัย

กลุ่ม SGA : รู้ทัน Social เปรี้ยวกว่าใคร หน่วยงาน สายงานเทคโนโลยีสารสนเทศ	ผู้อนุมัติ (คณะกรรมการย่อยสายงาน) (ลงชื่อ)..... <i>จิตติมา งาม</i>
องค์ความรู้เรื่อง เทคนิคการใช้งาน Facebook อย่างปลอดภัย	ตำแหน่ง <i>นางพิศวาท ภาพสุวรรณ</i> <i>ผอ.ฝ่ายท.</i> 23/05/60 รหัส OPK <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

จากสถิติการใช้ Social Media จากรายงานที่บริษัท Hootsuite เก็บข้อมูลจาก 238 ประเทศทั่วโลก ช่วงต้นปี 2017 (ที่มา <http://www.ihdigital.co.th>) Facebook ยังคงเป็นสื่อ Social Media ที่มีผู้ใช้งานมากที่สุดในโลก โดยประเทศไทยติดอันดับ 7 ของโลกในการเข้าถึง Social Media คือ 67% ของประชากรทั้งหมด และกรุงเทพฯ เป็นเมืองที่ผู้ใช้ Facebook มากที่สุดในโลก มีจำนวนมากถึง 24 ล้านคน หรือ 1.3% ของผู้ใช้ Facebook ทั้งหมด จึงขอแนะนำการใช้ Facebook อย่างปลอดภัย ดังนี้

1. ใช้เครือข่าย Internet ที่มีความปลอดภัยน่าเชื่อถือ

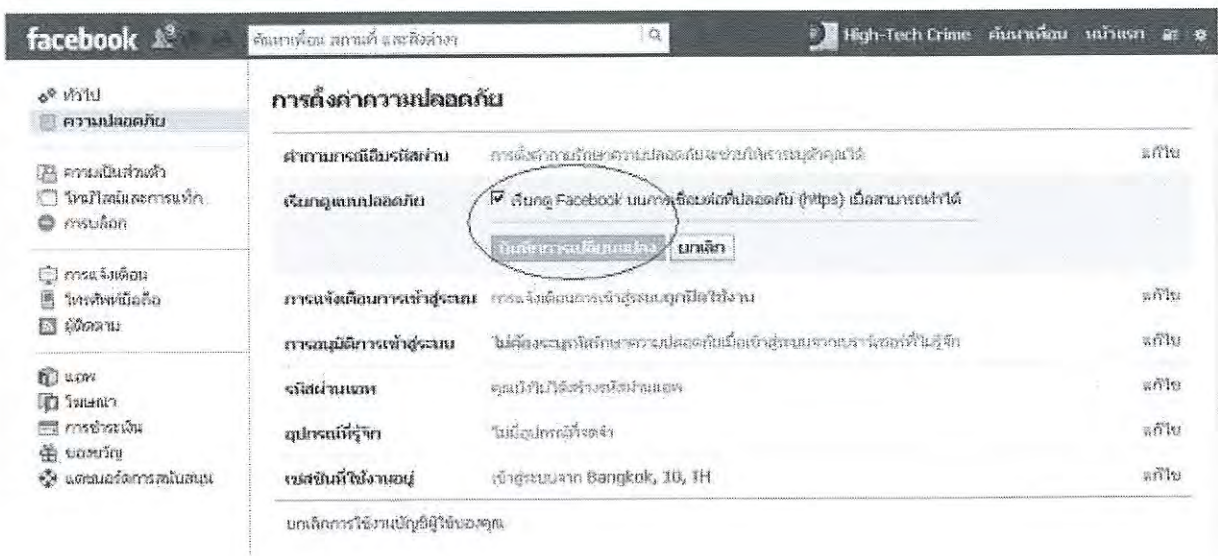
2. รักษาความปลอดภัยรหัสผ่าน โดยต้องไม่แชร์รหัสผ่าน โดยคุณควรจะเป็นเพียงคนเดียวที่ทราบรหัสผ่าน และรหัสผ่านควรจะเดาได้ยาก หลีกเลี่ยงการใช้ชื่อของคุณหรือคำที่คาดเดาง่ายเป็นส่วนหนึ่งของรหัสผ่าน

3. อย่าแชร์ข้อมูลการเข้าสู่ระบบ ผู้หลอกลวงอาจสร้างเว็บไซต์ปลอมที่ดูเหมือน Facebook และขอให้คุณเข้าสู่ระบบด้วยที่อยู่อีเมลและรหัสผ่านของคุณ ตรวจสอบ URL ของเว็บไซต์ก่อนจะป้อนข้อมูลการเข้าสู่ระบบของคุณเสมอ เมื่อมีข้อสงสัย ให้พิมพ์ www.facebook.com ลงในเบราว์เซอร์ของคุณเพื่อไปยัง Facebook

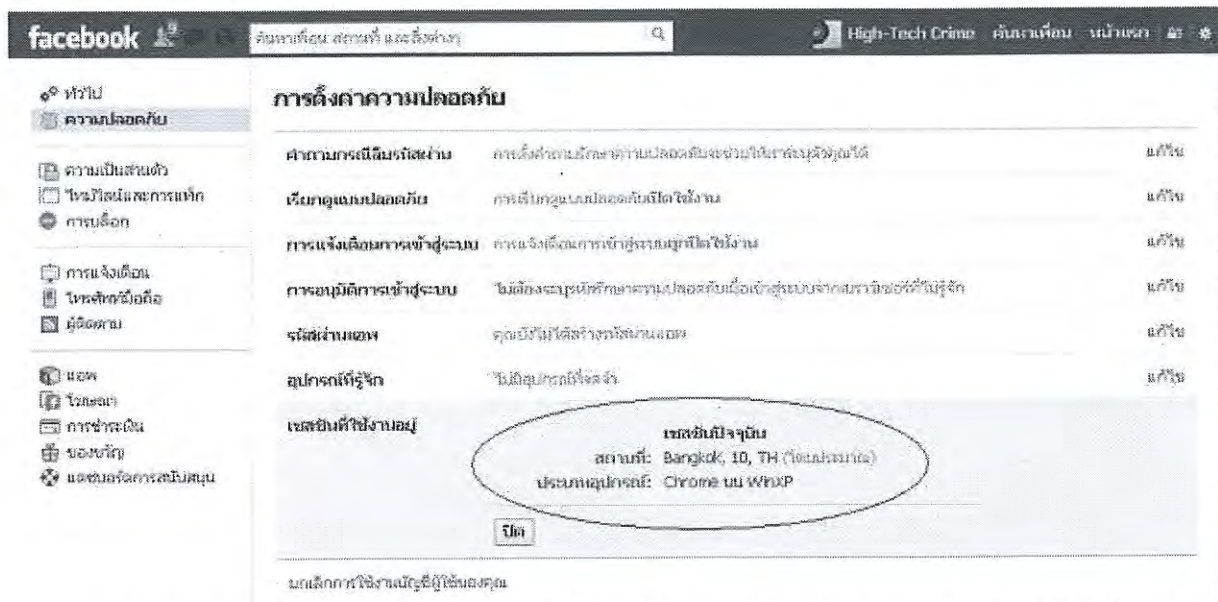
4. ออกจากระบบ Facebook เมื่อใช้เครื่องคอมพิวเตอร์ร่วมกับบุคคลอื่น ๆ

5. ไม่ควรรับคำขอเป็นเพื่อนจากบุคคลที่คุณไม่รู้จัก ผู้หลอกลวงอาจสร้างบัญชีผู้ใช้ปลอมขึ้นมาเพื่อเป็นเพื่อนกับผู้คน การเป็นเพื่อนกับผู้หลอกลวงอาจทำให้พวกเขาสามารถเข้าถึงเพื่อส่งสแปมในไทม์ไลน์ของคุณ แท็กคุณในโพสต์ และส่งข้อความที่เป็นอันตรายถึงคุณ

6. ควรตั้งค่าการเชื่อมต่อที่ปลอดภัย (https)



ถ้าพบว่าเซสชันปัจจุบัน ถูกใช้จากระบบปฏิบัติการและ Browser อื่นที่แตกต่างจากเครื่องคอมพิวเตอร์ที่
ใช้เชื่อมต่อ ให้รีบปิดเซสชันดังกล่าว แล้วรีบเปลี่ยนรหัสผ่านใหม่ทันที



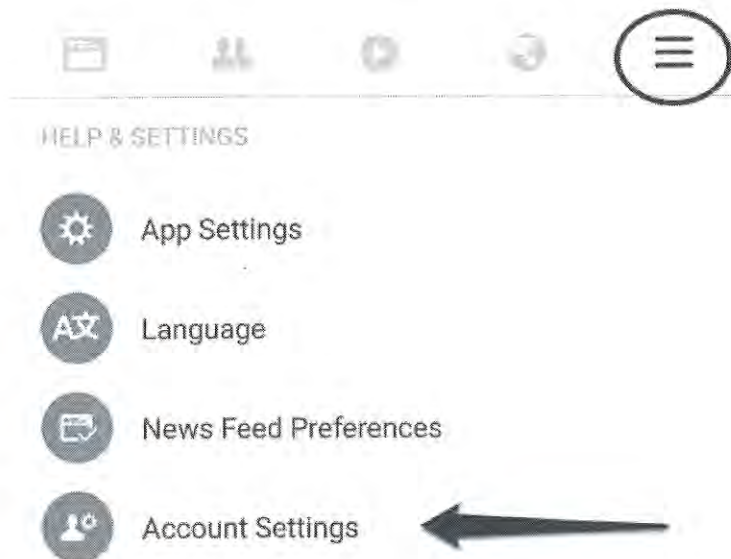
7. อย่าคลิกลิงก์ต้องสงสัยโดยเด็ดขาด แม้ว่าลิงก์นั้นจะดูเหมือนว่ามาจากเพื่อนหรือบริษัทที่คุณรู้จักก็
ตาม ลิงก์ต้องสงสัยนี้ยังรวมถึงลิงก์บน Facebook (เช่น ในโพสต์) หรือทางอีเมล โปรดจำไว้ว่า Facebook จะไม่

ขอรหัสผ่านของคุณทางอีเมลโดยเด็ดขาด หากคุณเห็นลิงก์ที่น่าสงสัยใน Facebook ให้รายงานไปที่ Facebook ด้วยการใส่ link รายงานที่ปรากฏใกล้กับเนื้อหานั้น

8. หมั่นตรวจสอบความเคลื่อนไหวของกิจกรรมและรายละเอียดในการเชื่อมต่อใช้งาน เมื่อไม่ใช้งานให้ออกจากระบบทุกครั้ง

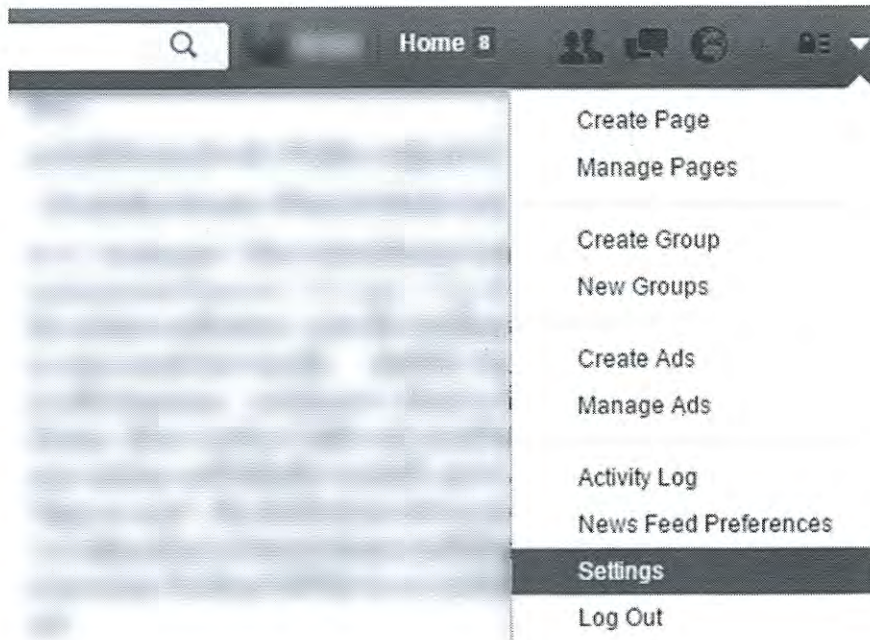
9. ตั้งค่าความปลอดภัย ใน Facebook Account Settings เพื่อเสริมความปลอดภัยให้บัญชี Facebook (ที่มา <https://www.blognone.com/node/80737>)

เชื่อว่าผู้ใช้ Facebook หลายคนคงไม่รู้ว่าหน้าจอตั่งค่าของ Facebook อยู่ตรงไหน ถ้าใช้งานบนมือถือให้เลือกรูปสามขีดด้านขวาสุด แล้วเลื่อนลงไปล่างสุด จะเห็นตัวเลือก Account Settings

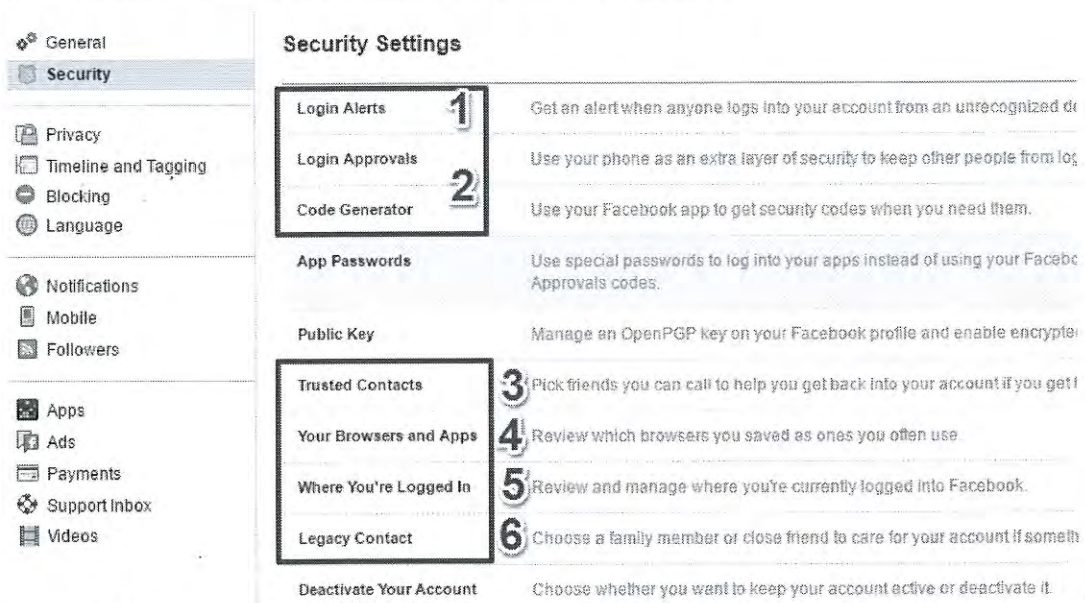


ส่วนผู้ที่ใช้นคอมพิวเตอร์ ให้เลือกลูกศรชี้ลงที่อยู่มุมขวาบนของหน้าจอ แล้วเลือกเมนู Settings

หมายเหตุ: ภาพหน้าจอจากนี้ไปจะใช้เวอร์ชันคอมพิวเตอร์เป็นหลัก แต่บนมือถือก็มีวิธีการเรียงเมนูแบบเดียวกัน ในตัวอย่างจะใช้เมนูภาษาอังกฤษ ซึ่งถ้าใครใช้เมนูภาษาไทยก็สามารถเทียบตำแหน่งเมนูเดียวกันได้ หรือไม่ก็เปลี่ยนเมนูเป็นภาษาอังกฤษจากหมวด Language ได้



จากนั้นให้เลือกการตั้งค่าหมวด Security จากเมนูด้านซ้ายมือดังภาพ ฝั่งขวาจะเห็นตัวเลือกชื่อ Security Settings ซึ่งเอาไว้ตั้งค่าเกี่ยวกับระบบความปลอดภัยทั้งหมดของ Facebook



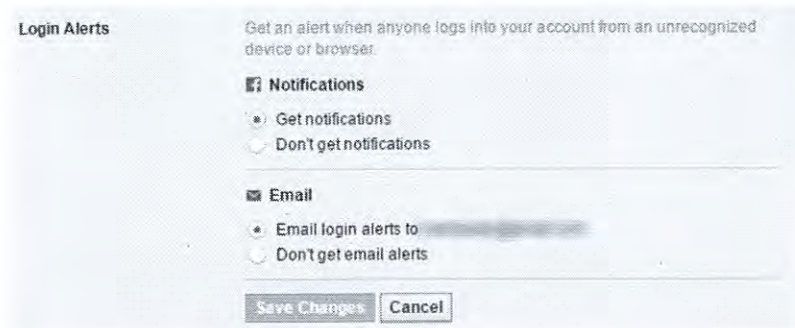
เนื่องจากหน้าจอนี้มีตัวเลือกค่อนข้างมาก เราจะขอแนะนำเฉพาะตัวเลือกที่สำคัญ 6 อย่างตามหมายเลขที่เขียนกำกับไว้ โดยจะแยกอธิบายทีละหัวข้อ ดังนี้

1. Login Alerts แจ้งเตือนเมื่อมีคนล็อกอินบัญชีของเรา

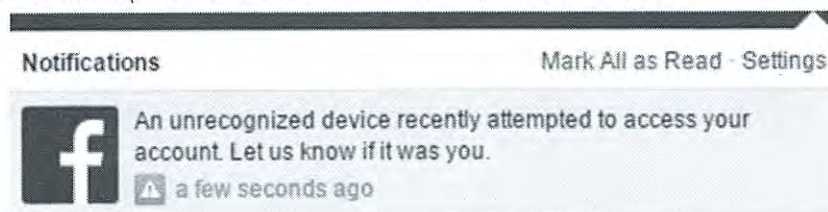
ฟีเจอร์นี้เป็นความปลอดภัยพื้นฐานของบัญชี Facebook ที่ทุกคนควรเปิดใช้งานไว้ เพราะไม่ยุ่งยากอะไร และช่วยให้เรารู้ว่ามีคนอื่นมาล็อกอินบัญชีของเราได้ตลอดเวลา

แนวคิดของฟีเจอร์ Login Alerts คือผู้ใช้งาน Facebook จากอุปกรณ์ชิ้นเดิม คอมพิวเตอร์เครื่องเดิม ถ้ามีการล็อกอินจากคอมพิวเตอร์เครื่องใหม่ที่ Facebook ไม่เคยเห็นมาก่อน ย่อมมีโอกาสสูงที่จะเป็นผู้อื่นล็อกอินเข้ามา ตัวเลือกรนี้จะแจ้งเตือนผู้ใช้งาน 2 ช่องทางโดยแนะนำให้เปิดใช้งานทั้งสองระบบคือ

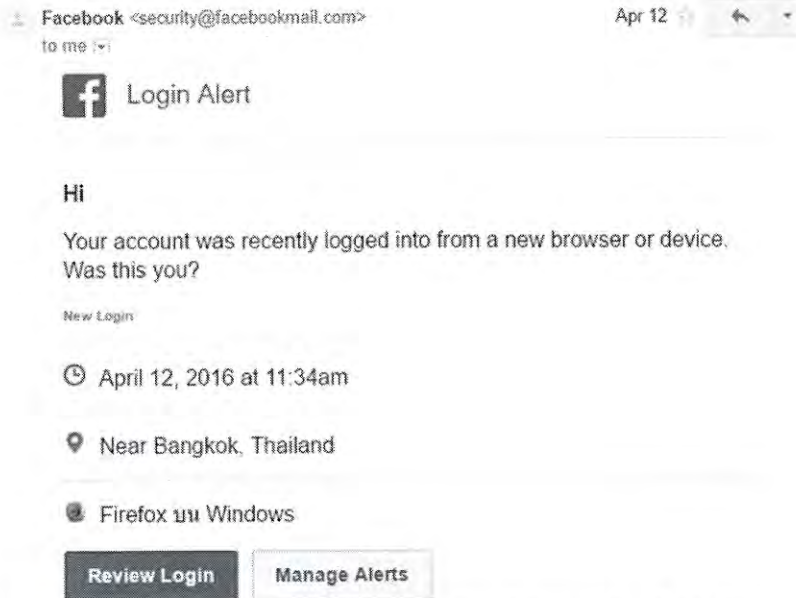
- ระบบแจ้งเตือนของ Facebook เอง (ทั้งเว็บและแอป เช่น กรณีที่เราใช้งาน Facebook ในเครื่องอื่นอยู่ มันจะขึ้นเตือน)
- อีเมลที่เราสมัครใช้งาน Facebook



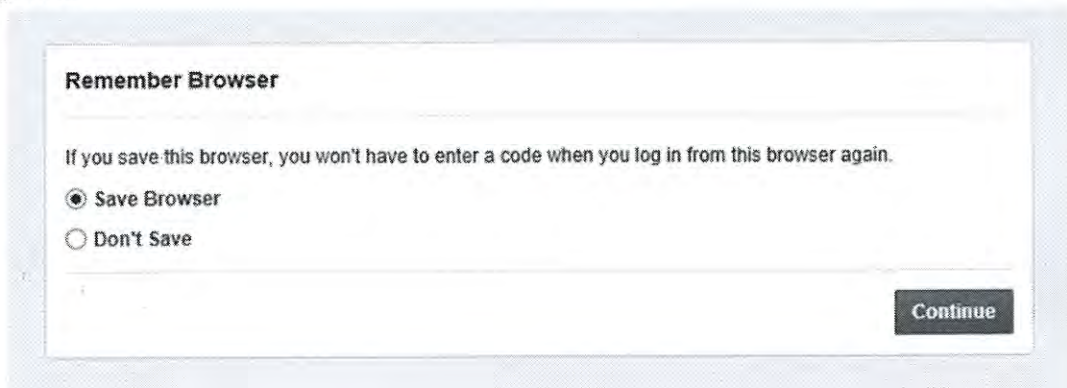
ถ้าเราเปิดตัวเลือกนี้ไว้ และมีอุปกรณ์อื่นพยายามล็อกอินเข้าบัญชีของเรา จะเห็นการแจ้งเตือนแบบนี้โผล่ขึ้นมา



ส่วนการแจ้งเตือนทางอีเมล จะมีหน้าตาดังภาพ (อีเมลจะถูกส่งมาจาก security@facebookmail.com)



ในกรณีที่เราล็อกอินจากมือถือหรือคอมพิวเตอร์เครื่องใหม่ แล้วจะใช้งานเครื่องนี้ต่อไปในระยะยาว เราก็สามารถตั้งให้ Facebook จดจำ (Remember Browser หรือ Save Browser) เพื่อที่มันจะได้ไม่ต้องเตือนทุกครั้งให้รำคาญได้ด้วย

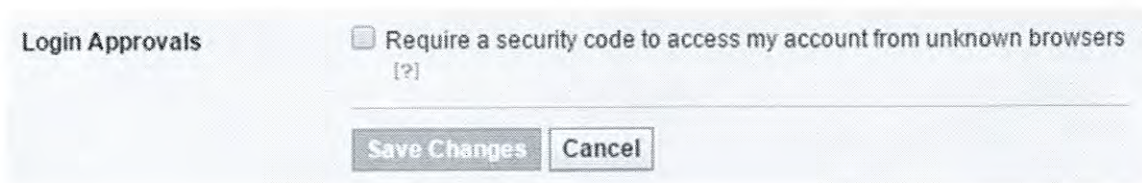


2. Login Approvals ระบบล็อกอินสองชั้น ใส่รหัสผ่านจากมือถือ

ในหัวข้อแรก กล่าวถึงระบบล็อกอินสองชั้นไปแล้ว Facebook ก็มีระบบล็อกอินสองชั้น โดยใช้ชื่อว่า Login Approvals และใช้คู่กับ Code Generator

แนวคิดของ Facebook คือผู้ใช้ส่วนใหญ่มีแอป Facebook บนมือถืออยู่แล้ว ดังนั้นแทนที่จะรับโค้ดยืนยันตัวตนจาก SMS เหมือนกับที่พวกร้านอาหารออนไลน์ทำ ก็ให้แอป Facebook ของเราเป็นตัวส่งโค้ดให้แทน ตามปกติแล้ว

บัญชี Facebook จะไม่เปิดใช้งาน Login Approvals ดังนั้นขั้นแรกเราต้องเปิดใช้ก่อน ให้ติ๊กหน้าคำว่า Require a security code แล้วกด Save Changes



จากนั้น Facebook จะขึ้นหน้าจออธิบายสั้นๆ ว่า Login Approvals คืออะไร ให้กด Get Started เพื่อไปต่อ



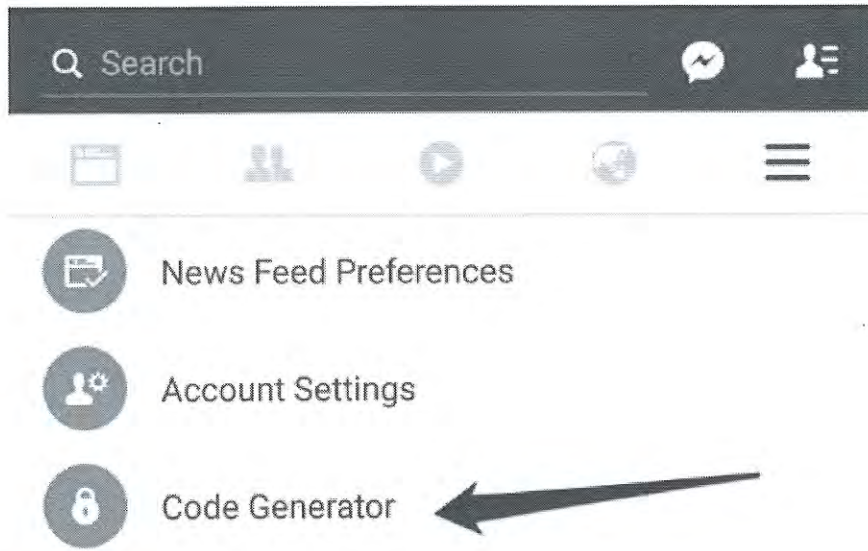
Facebook จะถามเราว่าใช้แอป Facebook บน Android/iPhone หรือไม่ ให้เลือกอันบนแล้วกด Continue



ขั้นต่อไปเราต้องใช้แอป Facebook บนมือถือเพื่อเรียกตัวสุ่มโค้ด (Code Generator) แล้ว ตามคำอธิบายข้างล่าง ให้กด Continue บนหน้าจอคอมพิวเตอร์ก่อน



วิธีการคือให้เปิดแอป Facebook บนมือถือขึ้นมา เลือกเมนูสามขีดเหมือนเดิม เลื่อนลงไปหาคำว่า Code Generator



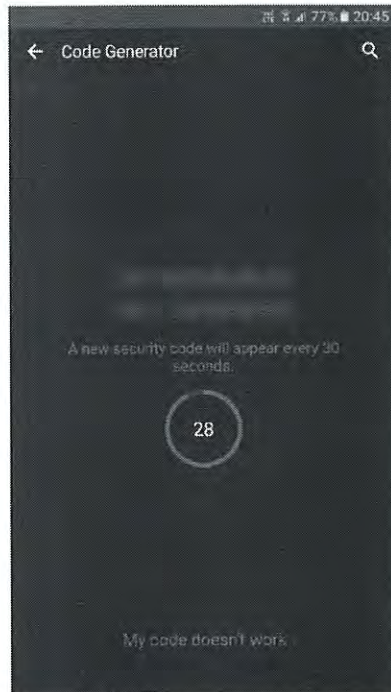
ระบบจะแจ้งให้เราเปิดใช้งาน Code Generator เป็นครั้งแรก โดยกดปุ่ม Activate



Code Generator helps protect your account from hacking and unauthorized account access.

Activate

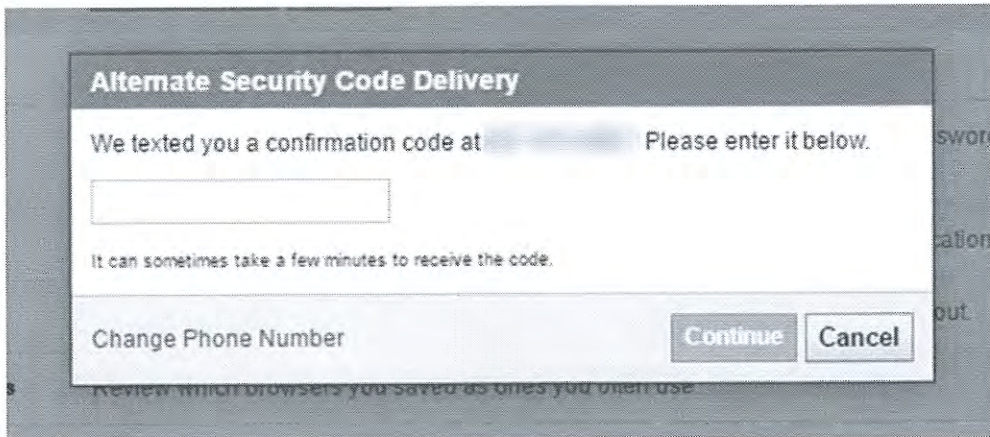
หน้าจอของเราจะเปลี่ยนเป็นสี่เหลี่ยม พร้อมแสดงโค้ด 6 หลักที่เปลี่ยนไปทุก 30 วินาที นี่คือโค้ดขั้นที่สองของเราที่ใช้แทนการรับโค้ดทาง SMS



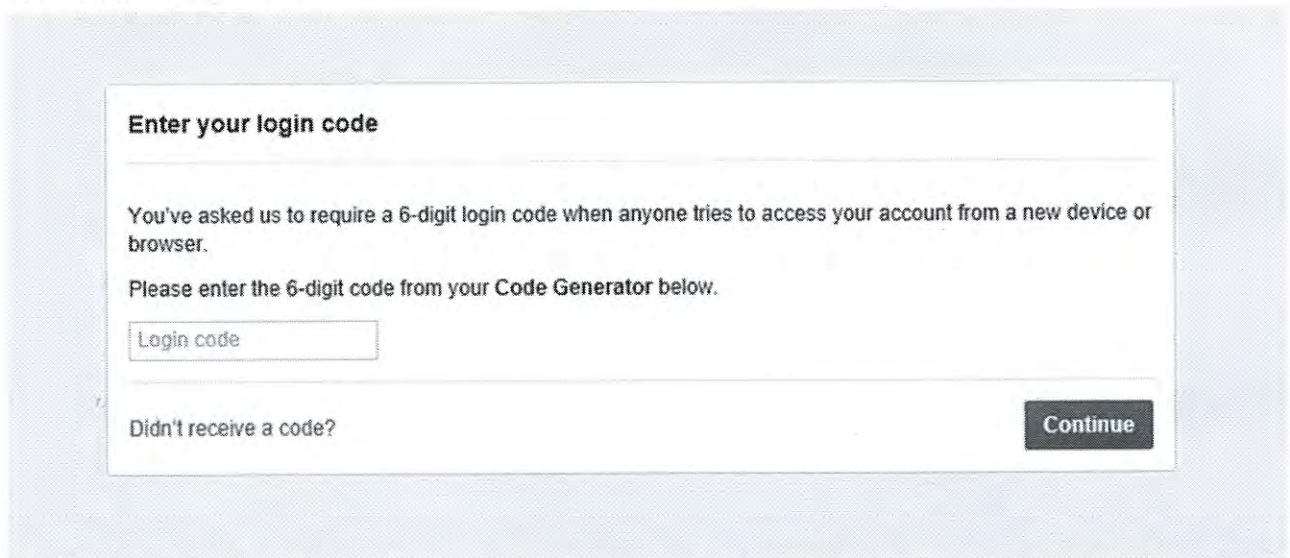
นำโค้ดที่ได้ไปกรอกในหน้าเว็บบนคอมพิวเตอร์เพื่อยืนยันว่าเรามีโค้ดจริง ถ้าโค้ดถูกต้องจะเห็นคำว่า It worked!



ขั้นสุดท้าย Facebook จะยืนยันตัวตนของเราอีกรอบ โดยส่ง SMS มายังเบอร์มือถือของเรา เพื่อใช้เป็นช่องทางรับโค้ดสำรอง หากไม่สามารถเปิดโค้ดจาก Code Generator ก็ยังสามารถรับโค้ดทาง SMS แทนได้ อันนี้ก็ทำตามกระบวนการปกติคือรอโค้ดจาก SMS ส่งมา แล้วกรอกลงในช่อง แค่นี้ก็เรียบร้อย



ถ้าหากมีคนพยายามล็อกอินเข้าบัญชีของเรา (หรือเราจะลองเองก็ได้) เมื่อผ่านขั้นของรหัสผ่านไปแล้ว จะเจอขั้นของการใส่โค้ด 6 หลักตามภาพ

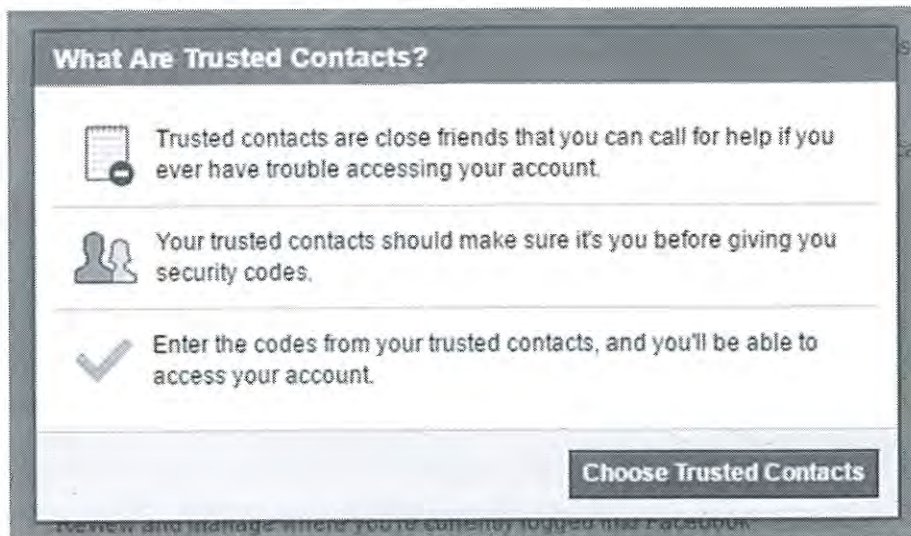


เท่านี้ถือว่าเราตั้งค่าล็อกอินสองชั้นของ Facebook เสร็จเรียบร้อยแล้ว คนที่พยายามล็อกอินเข้าบัญชีเราจะทำงานยากขึ้นมาก เพราะต่อให้รู้รหัสผ่าน ก็ต้องหาโค้ดชุดนี้มาล็อกอินควบคู่ไปด้วย (อาจยกเว้นกรณีนี้มีมือถือหาย โดนขโมย หรือโดนยึด ซึ่งคนที่เข้าถึงมือถือของเราได้ ก็จะเข้าถึงโค้ดชุดนี้ได้เช่นกัน ซึ่งเป็นสิ่งที่ต้องระวัง)

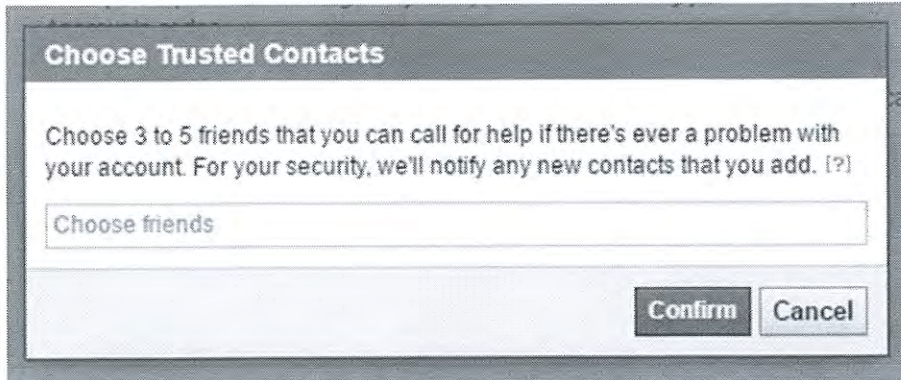
3. Trusted Contacts เพื่อนที่ไว้ใจได้

ในกรณีที่บัญชี Facebook ของเราโดนแฮ็ก สิ่งที่เราต้องทำคือขอบัญชีคืนผ่านระบบของ Facebook ที่แสนจะยุ่งยาก ทางแก้ทางหนึ่งที่ Facebook เตรียมไว้ให้เรา (แต่คนไม่ค่อยรู้จักเท่าไร) คือ Trusted Contacts ซึ่งเป็นการให้เพื่อนใน Facebook ที่เรารู้จักในโลกจริง มาช่วยยืนยันตัวตนให้เราแทน

การทำงานของ Trusted Contacts คือเราต้องเลือกเพื่อนสนิท 3-5 คน (แนะนำให้เลือกญาติหรือเพื่อนสนิทจริงๆ ที่เราไว้ใจได้) เลือกเก็บไว้เฉยๆ เพื่อบอก Facebook ว่าคนที่เราไว้ใจได้คือใคร ถ้าในอนาคตเรามีปัญหาล็อกอินเข้าบัญชีตัวเองไม่ได้ เราสามารถร้องขอให้ Facebook ส่งโค้ดยืนยันตัวตนไปให้เพื่อนของเรา (ที่ล็อกอินเข้าระบบได้ตามปกติ) แล้วให้เพื่อนบอกโค้ดเรามายืนยันว่าเราเป็นเจ้าของบัญชีนี้จริงๆ



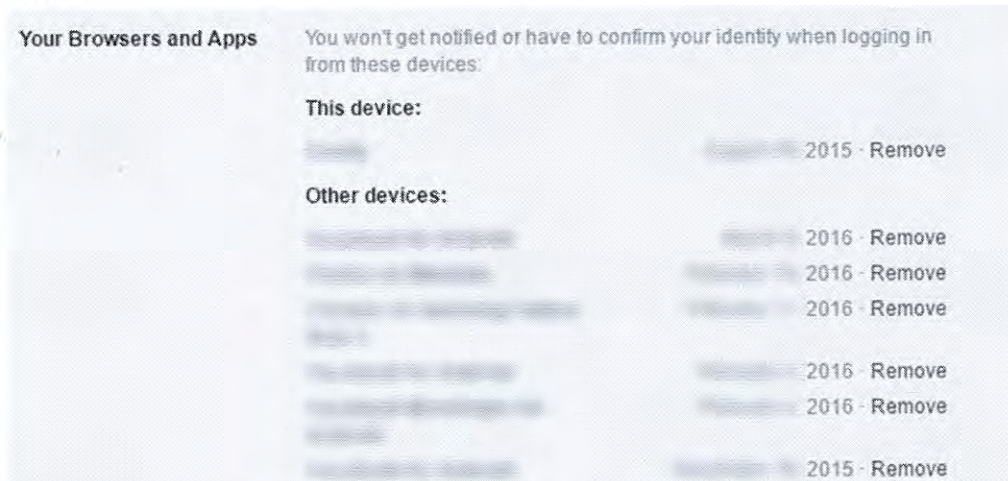
ขั้นตอนการใช้งานก็ไม่มีอะไรยาก กรอกชื่อเพื่อน 3-5 คน แค่นี้ก็เรียบร้อยแล้ว (กรอกเก็บไว้เฉยๆ เอาไว้ใช้งานเมื่อยามยาก) เพื่อนของเราจะได้รับแจ้งว่าเป็น Trusted Contacts ด้วย ดังนั้นควรบอกเพื่อนไว้ล่วงหน้า จะได้ไม่ตกใจเกินเหตุ



ในการกู้บัญชีกลับคืน เราจำเป็นต้องขอโค้ดยืนยันตัวตนจากเพื่อนทุกคนใน Trusted Contacts (ถ้าเลือกไว้ 5 ก็ต้องโทรขอให้ครบ) รายละเอียดสามารถอ่านได้จาก Facebook: Introducing Trusted Contacts (พีเจอร์นี้มีตั้งแต่ปี 2013)

4. Your Browsers and Apps ย้อนดูสิทธิการเข้าถึงบัญชี

เมื่อใดก็ตามที่เราล็อกอิน Facebook ผ่านเว็บเบราว์เซอร์ หรือมีแอปขอสิทธิใช้งานบัญชีของเรา (โดยเฉพาะพวกเกม) หลายคนคงเคยเห็นหน้าจอยืนยันขอสิทธิการเข้าถึงบัญชี ซึ่งโดยส่วนใหญ่แล้วเราก็ให้สิทธิไป ประวัติการขอสิทธิทั้งหมดของแอปต่างๆ จะถูกเก็บไว้ในหน้าจอตั้งค่า Your Browsers and Apps ย้อนไปตั้งแต่อดีตชาติของเรา

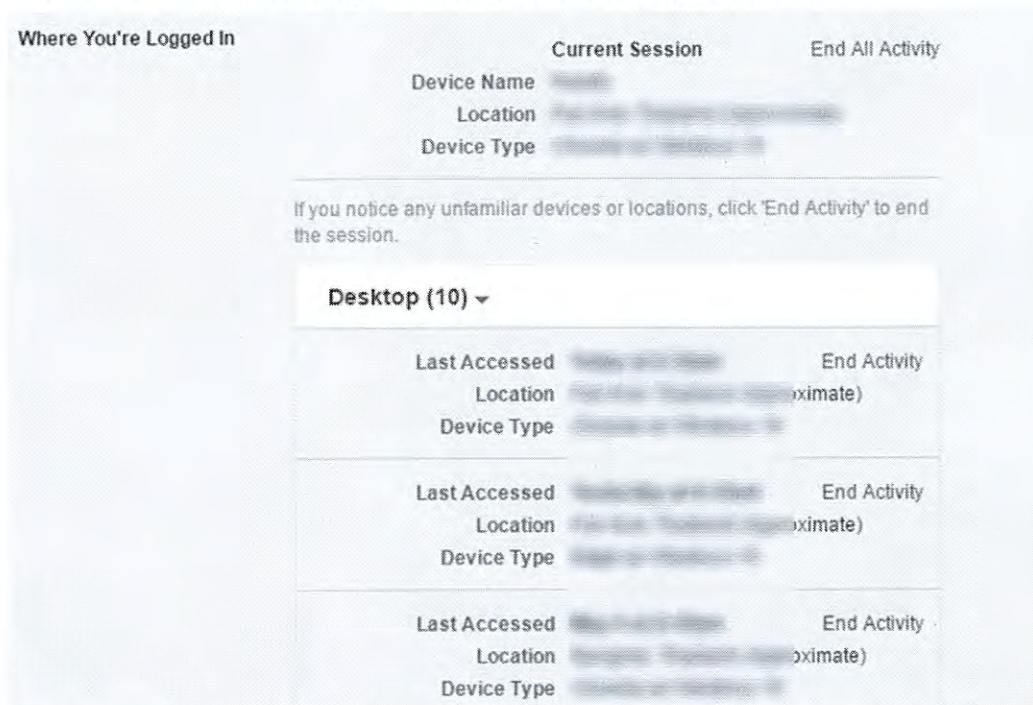


เพื่อความปลอดภัยของเราเอง ขอแนะนำให้เราสั่ง Remove ลบแอปเก่าๆ ทิ้งให้หมด (ถ้าเผลอลบแอปที่ใช้งานอยู่ก็ไม่เสียหาย เพราะมันจะขอสิทธิเราใหม่) ให้เหลือเฉพาะการใช้งานเพียง 3-4 อันล่าสุดเท่านั้นพอ หรือง่ายๆ คืออะไรเก่ากว่าปีปัจจุบัน ลบออกให้หมด

5. Where You're Loggen In ล็อกอินมาจากที่ไหนบ้าง

ข้อ 5. คล้ายกับข้อ 4. แต่จะแสดงให้เห็นเราดูว่าเราล็อกอิน Facebook มาจากคอมพิวเตอร์ มือถือ แท็บเล็ต ฯลฯ เครื่องไหน เมื่อไร จากตำแหน่งไหนของโลก

หน้าจอนี้จะช่วยให้เราตรวจสอบประวัติย้อนหลังได้ว่า มีการล็อกอินแปลกๆ จากที่อื่นที่เราไม่รู้จักหรือไม่ (เช่น ไม่ได้ไปต่างประเทศเลย แต่ถ้าพบการล็อกอินจากนอกประเทศไทย ก็แปลว่าไม่ใช่เรา)

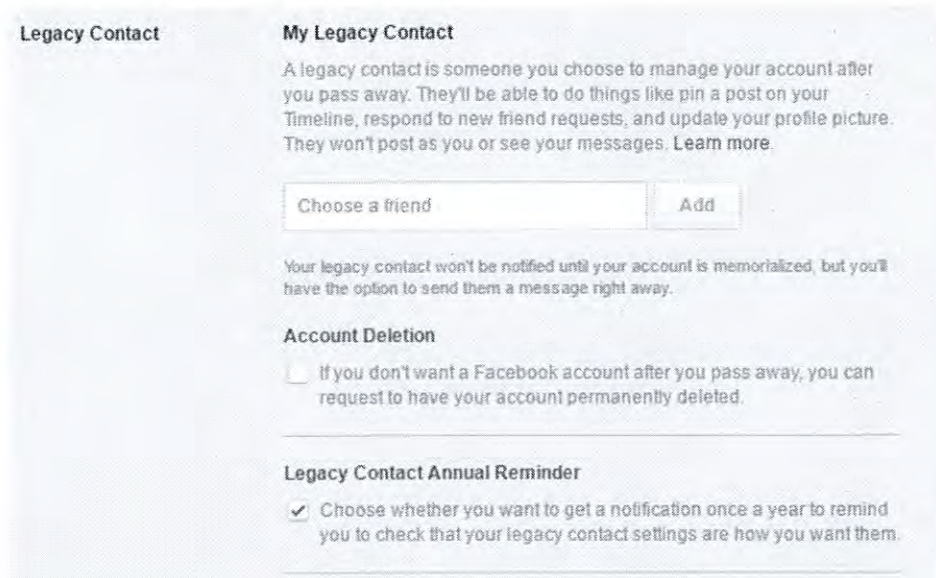


ประวัติการล็อกอินเหล่านี้คือการล็อกอินที่เราทำค้างเอาไว้ แนะนำให้กดปุ่ม End Activity เพื่อล็อกเอาต์ออกจากระบบทั้งหมด (กด End All Activity) หรือจะเหลือไว้เฉพาะอันใหม่ล่าสุดก็ได้ เพื่อความปลอดภัยที่ดีของบัญชีเราเอง

6. Legacy Contact ถ้าหากเป็นอะไรขึ้นมา ผากบัญชีไว้ที่ใคร

ข้อนี้อาจไม่ได้ใช้งานในตอนนี แต่ควรรับรู้และตั้งค่าไว้เผื่อจำเป็น หน้าจอ Legacy Contact คือการระบุว่าถ้าหากเราในฐานะเจ้าของบัญชีเกิดเสียชีวิตขึ้นมา เราจะยกสิทธิการดูแลบัญชี (บางส่วน) ให้ใครแทน ซึ่งตรงนี้ควรเลือกญาติหรือคนในครอบครัวที่ไว้ใจได้จริงๆ

คนที่ดูแลบัญชีจะทำได้เฉพาะบางอย่างเท่านั้น เช่น ปักหมุดโพสต์ งดรับคำขอเป็นเพื่อน หรือเปลี่ยนภาพประจำตัว แต่ไม่สามารถล็อกอิน และโพสต์หรือแชทแทนเจ้าของบัญชีได้ และในกรณีที่เราไม่ยอมให้ใครดูแลบัญชีแทน จะเลือก Account Deletion หรือให้ลบบัญชีทิ้งไปเลยก็ได้เช่นกัน



ข้อนี้จะตั้งค่าเลยหรือไม่ก็ได้ แล้วแต่ความต้องการของเจ้าของบัญชี

สรุป: ควรทำอะไรบ้างเพื่อเสริมความปลอดภัยให้บัญชี Facebook

จากที่กล่าวมาทั้งหมด ขอแนะนำให้

- o เปิดใช้ฟีเจอร์ Login Alerts เพื่อแจ้งเตือนเมื่อการล็อกอินบัญชีที่น่าสงสัย ทั้งทางระบบแจ้งเตือนของ Facebook และทางอีเมล
- o เปิดใช้ฟีเจอร์ Login Approvals เพื่อบังคับให้ต้องล็อกอินสองชั้น ผ่านตัวสุ่มโค้ด Code Generator ในแอป Facebook บนมือถือ
- o เพิ่มชื่อ Trust Contacts เผื่อไว้ สำหรับโอกาสที่ล็อกอินเข้าบัญชีตัวเองไม่ได้
- o ตรวจสอบสิทธิการเข้าถึงบัญชีในหน้า Your Browsers and Apps และลบการขอสิทธิเก่าๆ ที่ไม่ต้องใช้แล้ว
- o ตรวจสอบประวัติการล็อกอินในหน้า Where You're Logged In และล็อกเอาต์การล็อกอินเก่าๆ ที่ค้างเอาไว้ และไม่ต้องใช้แล้ว

ทั้งนี้ ผู้ใช้ควรรับทราบว่า การตั้งค่าความปลอดภัยตามที่อธิบายในบทความนี้ เป็นการป้องกัน "บัญชี" (Account) จากบุคคลอื่นที่อาจเจาะบัญชีของเรา จากการรู้รหัสผ่านของเรา และพยายามล็อกอินเข้ามาใช้งานจากคอมพิวเตอร์หรือมือถือเครื่องอื่นเท่านั้น แต่ระบบความปลอดภัยเหล่านี้ไม่สามารถคุ้มครองเราได้มากนัก ถ้าหากฝ่ายผู้ประสงค์ร้ายเข้าถึงคอมพิวเตอร์หรือมือถือของเราได้โดยตรง

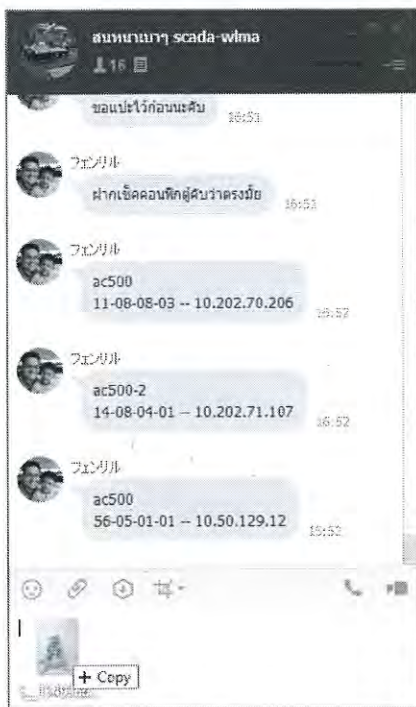
One Point Lesson: OPL

ชื่อเรื่อง	การโพสต์รูปบน Line (PC)	ลำดับ	9	
		วันที่เขียน	4 พ.ค. 2560	
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		สมโภช เกียรติกสิกร	พงษ์สุข วัฒนพงษ์สินธุ์	จตุพร สมบูรณ์
		04/05/60	23/05/60	23/05/60

วัตถุประสงค์

เพื่อความรวดเร็วในการโพสต์รูปบน Line (PC)

เนื้อหา



การโพสต์รูปบน Line (PC) นั้นมีวิธีง่ายๆ คือเลือกรูปภาพที่เราต้องการจากโฟลเดอร์ ในเครื่อง PC แล้วลากรูปที่ต้องการเข้ามาใน Line group ที่ต้องการโพสต์ (จากภาพตัวอย่าง)

ซึ่งวิธีนี้เป็นวิธีที่สะดวก รวดเร็วในการโพสต์รูป โดยที่ไม่ต้องคลิกแนบรูปแล้วไปหารูปเพื่อมาโพสต์ นั่นเอง

วันที่สอน							
ผู้สอน							
ผู้เรียน							
ผลการเรียนรู้							



การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

องค์ความรู้ (One Point Knowledge)

ข้อปฏิบัติในการใช้รหัสผ่าน (Active Directory : AD)

กลุ่ม SGA : รู้ทัน Social เปรี้ยวกว่าใคร หน่วยงาน สายงานเทคโนโลยีสารสนเทศ	ผู้อนุมัติ (คณะกรรมการย่อยสายงาน.....) (ลงชื่อ)..... <i>จิรภัทร กุศล</i>
องค์ความรู้เรื่อง ข้อปฏิบัติในการใช้รหัสผ่าน (Active Directory : AD)	ตำแหน่ง <i>(นางพิศวาท ภาพสุวรรณ)</i> <i>วอ.พืชก.</i>
	23/05/60 รหัส OPK <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

ข้อปฏิบัติในการใช้รหัสผ่าน (Active Directory : AD)

OPK ฉบับนี้ จัดทำขึ้นเพื่อให้พนักงาน มีความรู้และปฏิบัติตามระเบียบการประปานครหลวง ฉบับที่ ๑๘ ว่าด้วย การรักษาความปลอดภัยระบบสารสนเทศ ซึ่งในที่นี้จะกล่าวถึงการใช้รหัสผ่าน (Active Directory : AD)

บทนำ

เพื่อให้มีการควบคุมการพัฒนาของระบบสารสนเทศ การเปลี่ยนแปลงแก้ไขการปฏิบัติงานในศูนย์คอมพิวเตอร์ การเข้าถึงอุปกรณ์คอมพิวเตอร์ การเข้าถึงอุปกรณ์คอมพิวเตอร์ การเข้าถึงระบบงาน การเข้าถึงข้อมูลและทรัพยากรสารสนเทศ การจัดเก็บข้อมูล การกำหนดมาตรฐานของเอกสารระบบสารสนเทศ ลดความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ และการวางแผนการแก้ไขความเสียหายจากเหตุฉุกเฉิน จึงจำเป็นต้องมีแนวทางปฏิบัติที่สามารถปกป้องข้อมูลสำคัญมิให้สูญหาย เพื่อปกป้องความเสียหายที่จะเกิดขึ้นกับองค์กร และลดความเสี่ยงจากการใช้งานระบบสารสนเทศ

ข้อปฏิบัติในการใช้รหัสผ่าน

1. รหัสผ่าน ควรมีความยาวของตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร
2. ผู้ปฏิบัติงานที่ได้รับอนุญาตและได้รับสิทธิในการใช้ระบบงานสารสนเทศและระบบข้อมูลที่เกี่ยวข้อง เมื่อได้รับจัดสรรรหัสผ่านแล้ว จะต้องเปลี่ยนรหัสผ่านเป็นของตนเองที่เหมาะสมและเป็นความลับเฉพาะตัวชุดใหม่ทันที
3. ผู้ปฏิบัติงานต้องเปลี่ยนรหัสผ่านใหม่ทุกๆ ๙๐ วัน หรือตามระยะเวลาที่ระบบงานกำหนด
4. การเปลี่ยนแปลงรหัสผ่านใหม่ในแต่ละครั้ง จะต้องไม่นำรหัสผ่านที่หมดอายุแล้วมาใช้ซ้ำอีก
5. ผู้ปฏิบัติงานจะต้องล็อกหน้าจอทุกครั้งเมื่อไม่ได้ปฏิบัติงานอยู่ที่เครื่องคอมพิวเตอร์ และต้องพิสูจน์ตัวตนก่อนใช้งานทุกครั้ง
6. ผู้ปฏิบัติงานทุกคนต้องรับผิดชอบในการเลือก และ/หรือเปลี่ยนแปลงรหัสผ่านที่เหมาะสมและปลอดภัย รวมทั้งปกปิดและรักษา รหัสผ่านของตนอย่างดีที่สุดโดยห้ามจดบันทึกรหัสผ่านในที่ที่สามารถพบเห็นได้โดยง่าย
7. ห้ามเปิดเผยรหัสผ่านให้บุคคลอื่นรับรู้ หากรหัสผ่านถูกเปิดเผยต้องเปลี่ยนใหม่โดยเร็ว

8. ห้ามนำหรือเปิดเผยรหัสผ่านให้แก่บุคคลอื่นที่ไม่ได้รับอนุญาตหรือที่มีได้เกี่ยวข้องแสดงตนเข้าไปใช้ระบบงานสารสนเทศและระบบข้อมูล หากตรวจสอบพบว่ามี การเปิดเผยหรือนำรหัสผ่านให้แก่บุคคลอื่นที่ไม่ได้รับอนุญาต กระทำการที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศ และการรักษาความปลอดภัยระบบข้อมูล ผู้ปฏิบัติงานที่ได้รับอนุญาตและสิทธิให้ใช้ระบบงานสารสนเทศนั้น จะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
9. หากผู้ปฏิบัติงานพบเห็นหรือสงสัยถึงการล่วงละเมิดต่อความปลอดภัยในการใช้งานหรือประเด็นอื่นใดที่เกิดขึ้น เนื่องจากรหัสผ่านถูกนำไปใช้โดยผู้ที่ไม่ใช่เจ้าของ จะต้องรายงานการใช้ต่อผู้บังคับบัญชาหรือหน่วยงานที่ดูแลระบบสารสนเทศหรือผู้ดูแลระบบงานทันที เพื่อทำการตรวจสอบและแก้ไขต่อไป

การลงโทษทางวินัย ไม่เป็นเหตุให้ผู้กระทำหลุดพ้นจากความผิดทางอาญา หรือความรับผิดทางแพ่ง หรือความรับผิดตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550



ncfc-ปณศรทวง
NATIONAL COMPUTER FORENSIC CENTER

One Point Article: OPA

ชื่อเรื่อง	เทคนิคการตั้ง password สิ่งสำคัญที่ไม่ควรมองข้าม	ลำดับ	11	
		วันที่เขียน	5 พ.ค. 2560	
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		ธนาพันธ์ โดมทอง	ชวณัฐ กอวิเศษ	วิมลทิพย์ ทรัพย์
		05/05/60	23/05/60	23/05/60

เทคนิคการตั้ง password สิ่งสำคัญที่ไม่ควรมองข้าม

ในการเริ่มต้นของทุกๆเช้าวันทำงาน สิ่งแรกที่เราทุกคนต้องทำเป็นอย่างแรกก็คือ การ login เข้าสู่ระบบงานต่างๆ ไม่ว่าจะเป็น email หรือการใส่ user name และ password เพื่อเข้าใช้งานคอมพิวเตอร์ของเรา และเนื่องจากเป็นสิ่งที่เราทำทุกวันจะเป็นกิจวัตรจึงทำให้บางคนมองข้ามความสำคัญของการตั้ง password โดยไม่ได้มุ่งเน้นที่การปกป้องข้อมูลส่วนตัวของเรา แต่กลับคำนึงถึงความสะดวกสบายในการเข้าใช้งานมากกว่า ซึ่งอาจก่อให้เกิดความอันตรายต่อข้อมูลส่วนตัวของเราได้มากอย่างที่คาดไม่ถึง อันจะเห็นได้จากข่าว เช่น การขโมย password ของ email, line หรือ facebook และปลอมตัวเป็นเจ้าของเพื่อใช้การขโมยเงินจากเพื่อนของเจ้าของ account

ดังนั้น เราจึงไม่ควรมองข้ามความสำคัญของการตั้ง password ให้ปลอดภัย โดยจะพูดถึงสิ่งที่ไม่ควรทำในการตั้ง password รวมถึงคำแนะนำในการตั้ง password ที่ดี

สิ่งที่ไม่ควรทำ

1. ใช้ Default Password

Default Password คือ รหัสผ่านเริ่มต้นที่มาพร้อมกับโปรแกรมหรืออุปกรณ์ เช่น wifi router ซึ่งอาจจะถูกตั้งมาเหมือนกัน ดังนั้นหลังจากที่เราได้เริ่มใช้งานอุปกรณ์นั้นๆแล้ว จึงควรเปลี่ยนรหัสใหม่เพื่อความปลอดภัย เพราะปัจจุบันข้อมูลรหัสผ่านเหล่านี้สามารถค้นหาได้ทั่วไปบนเว็บไซต์อินเทอร์เน็ต เช่น <https://cirt.net/passwords> ซึ่งเป็นแหล่งรวบรวมข้อมูล Default Password จากผู้ให้บริการเกี่ยวกับระบบคอมพิวเตอร์ทั่วโลก

2. ใช้password เดียวกับ email

ในปัจจุบัน website ส่วนใหญ่ จะให้ผู้ใช้งานตั้ง user name ด้วย email ทำให้ผู้ใช้งานบางส่วน ใช้รหัสผ่านเป็นรหัสเดียวกันกับรหัสผ่าน email ซึ่งจะอันตรายมาก เพราะจะทำให้เจ้าของ website สามารถเข้าถึงข้อมูลใน email ได้เลย

3. ตั้ง pw เหมือน user name

หลีกเลี่ยงการตั้ง password ให้เหมือนกับชื่อ user name เพราะง่ายต่อการคาดเดา

4. ตั้ง password ด้วยข้อมูลที่คาดเดาได้ง่าย

ไม่ควรตั้ง password ด้วย ชื่อ นามสกุล เบอร์โทรศัพท์ เลขบัตรต่างๆ ชื่อหนังที่ชอบ นักกีฬา หรือบุคคลที่นับถือ เพราะหาข้อมูลได้ง่ายๆ เช่น Facebook

5. ตั้ง password ด้วยตัวอักษรที่เรียงบน key board

เช่น asdfgh , qwerty หรือ zxcvbrวมถึงตัวเลข 123456789 , 1111111

6. จดรหัสผ่านไว้ใกล้ๆเครื่องคอมพิวเตอร์

ไม่ควรจดรหัสผ่านลงในกระดาษ หรือจดไว้ในสมุด ที่วางอยู่บริเวณใกล้ๆกับเครื่องคอมพิวเตอร์
ของคุณ

การตั้ง password ที่ดี

1. เปลี่ยนรหัสผ่านทุกๆ 3 เดือน

เพื่อลดโอกาสการถูกแกะรหัสผ่าน

2. ความยาวเกิน 8 ตัวอักษร

Website ในทุกวันนี้ส่วนใหญ่มักจะบังคับให้ตั้งรหัสผ่าน 8 ตัวอักษรเป็นขั้นต่ำอยู่แล้ว เพราะ ยิ่งรหัสผ่านของเรามีความยาวมากขึ้น การเดารหัสผ่านก็จะต้องใช้เวลามากขึ้นด้วย นอกจากนี้ถ้า password ประกอบด้วยอักษรตัวใหญ่ และตัวเล็ก ตลอดจนตัวเลข และสัญลักษณ์ ยิ่งผสมกันได้มาก เท่าไร จะยิ่งปลอดภัยเท่านั้น

3. พิมพ์รหัสผ่านภาษาอังกฤษด้วยkeyboard ภาษาไทย

เป็นเทคนิคในการตั้ง password ที่ง่าย และคาดเดาได้ยาก วิธีการคือให้ทดลองพิมพ์รหัสผ่าน ภาษาไทย แต่ใช้แป้นพิมพ์เป็นภาษาอังกฤษ ยกตัวอย่างเช่น จะตั้งรหัสผ่านว่า “ข้าวหน้าเป็ด” เมื่อเราพิมพ์ ด้วยแป้นพิมพ์ภาษาอังกฤษก็จะได้รหัสผ่านเป็น “-hk;sohkgxHf” ซึ่งจะได้ทั้งตัวอักษรตัวใหญ่ และตัว อักษรพิเศษ อีกทั้งยังง่ายต่อการจดจำอีกด้วย

กลุ่ม ปันโตความรู้

KM 2560

ภาคผนวก

แผนปฏิบัติงาน ประจำปีงบประมาณ 2560
หัวข้อ รู้ทัน Social เสรีกว่าใคร
กิจกรรม SGA ปีโนโตความรู้ สาขางานเทคโนโลยีสารสนเทศ

กิจกรรม/แนวทางการดำเนินงาน	ตัวชี้วัด	ระยะเวลาดำเนินการ											งบประมาณ (บาท)					
		ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.		ก.ย.				
1. จัดตั้งกลุ่ม SGA ในสาขางาน																		
2. ประชุมกลุ่ม เพื่อศึกษา วิเคราะห์ รวบรวม และเก็บข้อมูล																		
3. เรียบเรียง องค์กรความรู้ พิจารณาการใช้สื่อในการเผยแพร่องค์ความรู้																		
4. นำเสนอผลงานในสาขางาน																		
5. ปรับปรุงองค์ความรู้พร้อมจัดทำรายงานส่งคณะกรรมการ																		
6. จัดเตรียมการนำเสนอผลงานในงานสัปดาห์วิชาการ																		
6. นำเสนอผลงานในงานสัปดาห์วิชาการ																		
																	รวมเป็นเงิน	5,000

ลงชื่อ *Putth Boonru*..... หัวหน้า SGA

(นางมนขวัญ กาศพิณรัตน์)

ผู้อำนวยการกองวิชาการเทคโนโลยี

ฝ่ายยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ

วันที่ 31 / 03 / 2560