รู้ทัน SOCIAL เปรี้ยวกว่าใคร

SGA : กลุ่ม ปิ่นโตความรู้

การจัดการความรู้ (Knowledge Sharing) ปี 2560

สายงานเทคโนโลยีสารสนเทศ

สารบัญ

บทนำ

ตามที่ การประปานครหลวง ได้จัดทำยุทธศาสตร์การบริหาร การประปานครหลวง ฉบับที่ 4 (2560-2564) เพื่อกำหนดกรอบการดำเนินงาน มีความมุ่งมั่นในการยกระดับองค์กรสู่การเป็นองค์กรสมรรถนะสูง (High Performance Organization : HPO) ที่ได้รับการยอมรับในระดับสากล โดยมุ่งเน้นการบริหารจัดการที่ยึดหลักธรรมาภิบาล (Corporate Governance) และความรับผิดชอบต่อสังคม (Social Responsibility) การพัฒนาสู่องค์กรแห่งการเรียนรู้ (Learning Organization) และสร้างนวัตกรรมงานประปามืออาชีพ การบูรณาการเทคโนโลยีสารสนเทศทั่วทั้งองค์กรเพื่อก้าวสู่เป้าหมาย SMART MWA ตลอดจนการใช้เทคโนโลยีสมัยใหม่เพื่อเพิ่มประสิทธิภาพการดำเนินการ ประกอบกับนโยบายภาครัฐเรื่องการพัฒนาเศรษฐกิจของประเทศไทยไปสู่เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม เพื่อก้าวสู่ยุคไทยแลนด์ 4.0 โดยเปลี่ยนจากการขับเคลื่อนประเทศด้วยภาคอุตสาหกรรม ไปสู่การขับเคลื่อนด้วยเทคโนโลยี ความคิดสร้างสรรค์ และนวัตกรรม และเปลี่ยนจากภาคการผลิตสินค้าไปสู่ภาคการบริการ จำเป็นต้องมีการปรับเปลี่ยนภาครัฐและเอกชนเข้าสู่ยุครัฐบาลดิจิทัล (Digital Government) โดยกำหนดให้บุคลากรในหน่วยงานจำเป็นต้องมีความรู้เรื่องเทคโนโลยีดิจิทัล เพื่อสร้างความตระหนัก สร้างความเข้าใจ และนำเทคโนโลยีดิจิทัลมาใช้เป็นเครื่องมือในการสนับสนุนการทำงานตามภารกิจขององค์กร และปัจจุบันอินเทอร์เน็ตเข้ามามีบทบาทในชีวิตมากขึ้นหลากหลายรูปแบบ รูปแบบหนึ่งที่เป็นที่นิยมมากคือ Social Network ทำให้การใช้บริการ Social Network มีแนวโน้มเพิ่มมากขึ้น เป็นส่วนหนึ่งในการติดต่อสื่อสาร และรับข้อมูลต่าง ๆ เพิ่มขึ้น และอาจใช้เป็นช่องทางหนึ่งในการติดต่อสื่อสารระหว่างบุคลากรภายในองค์กร หรือติดต่อสื่อสารกับบุคคลภายนอกองค์กรเป็นการสร้างภาพลักษณ์ที่ดีกับองค์กรได้

ดังนั้นทางกลุ่มปิ่นโตความรู้ ได้นำเสนอองค์ความรู้เรื่อง "รู้ทัน Social เปรี้ยวกว่าใคร" เพื่อให้พนักงานสามารถใช้ Social Network ได้อย่างปลอดภัยทั้งแก่ตนเองและองค์กร และสนับสนุนโครงการความเข้าใจดิจิทัล (Digital Literacy) สำหรับบุคลากรทุกระดับของ กปน. ตามที่สายงานเทคโนโลยีสารสนเทศจัดทำขึ้นในปีงบประมาณ 2560 เพื่อลดช่องว่างทางดิจิทัล สร้างโอกาสและความเท่าเทียมในการเข้าถึงข้อมูล ข่าวสารสารสนเทศและใช้ประโยชน์จากเทคโนโลยีดิจิทัลในชีวิตประจำวัน การปฏิบัติงาน และเตรียมพร้อมสู่การเป็นพลเมืองดิจิทัล (Digital Citizenship) ในอนาคต เป็นการตอบสนองนโยบายภาครัฐในการเตรียมความพร้อมสู่ยุค Thailand 4.0 และสนับสนุนกลยุทธ์ที่ 1.5 เพิ่มประสิทธิภาพกระบวนการโดยการบูรณาการเทคโนโลยีและสารสนเทศ ยุทธศาสตร์ที่ 1 ยุทธศาสตร์สร้างการเติบโตและความยั่งยืนขององค์กร ของยุทธศาสตร์การบริหารการประปานครหลวง ฉบับที่ 4 (2560-2564) อีกด้วย

SGA : กลุ่ม ปิ่นโตความรู้
การจัดการความรู้ (Knowledge Sharing) ปี 2560
สายงานเทคโนโลยีสารสนเทศ

บทสรุปผู้บริหาร

ในปัจจุบันบทบาทของเทคโนโลยีได้เข้ามามีผลกระทบต่อมนุษย์มากขึ้น ซึ่งบางคนอาจจะถือว่าเทคโนโลยีเป็นอีกปัจจัยหนึ่งที่ขาดไม่ได้ หรือเป็นส่วนหนึ่งของชีวิตไปโดยไม่รู้ตัว ไม่ว่าจะเป็นการทำธุรกรรมผ่านอินเทอร์เน็ต การติดต่อสื่อสารต่างๆ ซึ่งเป็นที่นิยมกันอย่างแพร่หลายในกลุ่มของคนที่ติดตามเทคโนโลยี นอกจากจะสามารถเข้าถึงเทคโนโลยีเหล่านี้ผ่านคอมพิวเตอร์ ปัจจุบันก็สามารถที่จะเข้าถึงได้โดยผ่านทางโทรศัพท์มือถือได้เป็นอีกทางเลือกหนึ่ง ซึ่งมีความสะดวกและรวดเร็วในการเข้าถึงอินเทอร์เน็ตมากยิ่งขึ้น เพราะสามารถพกติดตัวได้ตลอดเวลา และสื่อประเภทใหม่ที่สามารถเข้าถึงได้ผ่านอินเทอร์เน็ต ซึ่งมีอิทธิพลกับสังคมไทยอย่างรวดเร็ว ได้แก่ Social Network ที่ผู้ใช้บริการสามารถเข้าถึงสังคมเสมือนจริง (Virtual Communities) ในโลกของอินเทอร์เน็ต โดย Social Network นั้นยังไม่มีคำไทยเป็นทางการ มีการใช้คำว่า “เครือข่ายสังคม”, “เครือข่ายมิตรภาพ” หรือ “กลุ่มสังคมออนไลน์” โดยคำเหล่านี้ล้วนแต่ชี้ให้เห็นถึงความหมายของ Social Network ทั้งสิ้น

สำหรับกระแสความนิยมของ Social Network ในประเทศไทย ทำให้หลายคนมองว่าสิ่งเหล่านี้ที่เข้ามาสร้างผลกระทบหรือผลเสียอย่างไรบ้างกับผู้คนที่ใช้บริการ Social Network เหล่านั้นและภายในสังคม นอกจากนั้นทำให้ตระหนักถึงพฤติกรรมการบริโภคข้อมูลข่าวสารที่เปลี่ยนแปลงไป โดยไม่มีใครทราบได้ว่าในอนาคตข้างหน้าผลกระทบเหล่านี้จะเกิดขึ้นกับคนอื่นๆ เป็นจำนวนมาก เพราะเป็นสังคมออนไลน์ที่เปิดโอกาสให้เข้าไปใช้เผยแพร่ข้อมูลส่วนตัว บทความ รูปภาพ ผลงาน พบปะ แสดงความคิดเห็น แลกเปลี่ยนประสบการณ์ ความสนใจร่วมกัน และกิจกรรมอื่น ซึ่งกิจกรรมเหล่านี้อาจจะเป็นเหมือนดาบสองคมหากมองถึงผลกระทบของ Social Network ซึ่งอาจจะเกิดขึ้นจากการใช้งานในทางที่ผิดวัตถุประสงค์ ซึ่งการกระทำนั้นอาจจะก่อให้เกิดความเดือดร้อนแก่ผู้อื่น หรือเป็นการกระทำให้ผู้อื่นเกิดความเสื่อมเสีย เพราะ Social Network นั้นสามารถกระจายข้อมูลให้กับผู้คนจำนวนมากได้อย่างรวดเร็ว ยังรวมไปถึงผลกระทบที่เกิดจากตัวผู้ใช้เอง นั่นเพราะ Social Network นั้นมีทั้งคนที่รู้จัก และไม่รู้จักปะปนอยู่ ซึ่งอาจมีผู้ที่ไม่ประสงค์ดีเข้ามาใช้เป็นช่องทางในการทำเรื่องเสื่อมเสียให้เกิดขึ้นก็เป็นได้

ปัจจุบันพนักงานและผู้ปฏิบัติงาน กปน. มีการใช้งาน Social Network อาทิ Facebook, LINE ผ่านระบบเครือข่ายของ กปน. ซึ่งควรต้องมีความตระหนักถึงภัยและผลกระทบที่จะเกิดขึ้นกับองค์กรโดยตรง จึงเห็นควรให้พนักงานและผู้ปฏิบัติงาน รู้เท่าทันเกี่ยวกับการใช้งาน Social Network

1. วัตถุประสงค์

1.1. เพื่อให้พนักงานและผู้ปฏิบัติงานได้เรียนรู้เกี่ยวกับ Social Network

1.2. เพื่อให้พนักงานและผู้ปฏิบัติงานรู้เท่าทันภัยคุกคามจากการใช้ Social Network

1.3. เพื่อให้พนักงานและผู้ปฏิบัติงานเกิดความตระหนักในการใช้ Social Network

1.4. เพื่อให้พนักงานและผู้ปฏิบัติงาน ทราบถึงสิ่งที่ควรและไม่ควรกระทำ ในการใช้ Social Network

2. ประโยชน์ที่ได้รับ

2.1. พนักงานและผู้ปฏิบัติงาน ได้นำความรู้ที่ได้ไปประยุกต์ใช้กับชีวิตประจำวัน

2.2. พนักงานและผู้ปฏิบัติงาน สามารถใช้งาน Social Network ได้อย่างมีประสิทธิภาพ

2.3. พนักงานและผู้ปฏิบัติงาน มีความระมัดระวังในการใช้ Social Network

2.4. พนักงานและผู้ปฏิบัติงาน สามารถใช้ Social Network ได้อย่างปลอดภัย

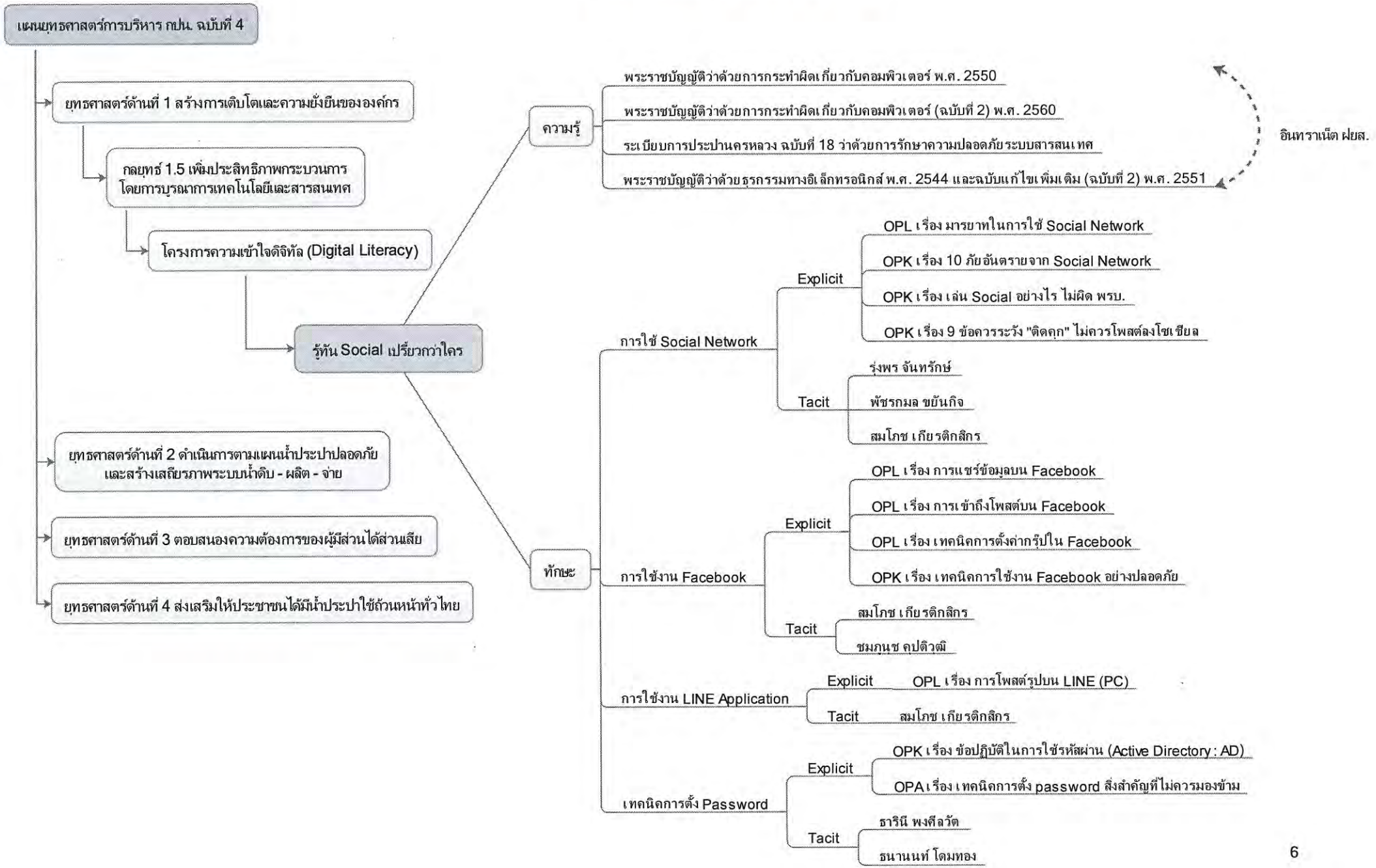
3. กลุ่มเป้าหมาย

พนักงานและผู้ปฏิบัติงาน การประปานครหลวง

SGA กลุ่ม ปิ่นโตความรู้

	นางนงนุช วงศ์กาฬสินธุ์	ผอ.กวก.ฝยท.	หัวหน้ากลุ่ม
	นางสาวพัลลภา มุสิกูล	นักคอมพิวเตอร์ 7 กวก.ฝยท.	สมาชิกกลุ่ม
	นางรุ่งพร จันทรักษ์	นักคอมพิวเตอร์ 7 กวม.ฝยท.	สมาชิกกลุ่ม
	นายสมโภช เกียรติกสิกร	นักคอมพิวเตอร์ 5 สพว.กพว.ฝพท.	สมาชิกกลุ่ม
	นายธนานนท์ โดมทอง	นักคอมพิวเตอร์ 5 กวก.ฝยท.	สมาชิกกลุ่ม
	นางสาวธารินี พงศีลวัต	นักคอมพิวเตอร์ 4 กวม.ฝยท.	สมาชิกกลุ่ม
	นางสาวพัชรกมล ขยันกิจ	นักคอมพิวเตอร์ 4 กวม.ฝยท.	สมาชิกกลุ่ม
	นางสาวชมภูนุช คุปติวุฒิ	นักคอมพิวเตอร์ 6 กวม.ฝยท.	สมาชิกกลุ่มและเลขานุการกลุ่ม

Knowledge Mapping



การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

ผังความรู้ (Knowledge Landscape) การประปานครหลวง

ฝ่ายยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ

นักจัดการความรู้ : ปิ่นโตความรู้

กลุ่มความรู้ที่ใช้หรือ Knowledge Domain	กระบวนการปฏิบัติงาน	ความรู้/ทักษะที่สนับสนุนการปฏิบัติงาน	Explicit Knowledge	Tacit Knowledge	ผู้ใช้ความรู้
	รู้ทัน Social เปรี้ยวกว่าใคร	1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ 2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ 3. ระเบียบการประปานครหลวง ฉบับที่ ๑๘ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ 4. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และฉบับแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ 5. การใช้ Social Network 6. การใช้งาน Facebook 7. การใช้ Line Application 8. เทคนิคการตั้ง Password	1. หน้าอินทราเน็ตของฝ่ายเทคโนโลยีและสื่อสารแบนเนอร์ คู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กฎหมายและกฎระเบียบที่เกี่ยวข้อง ที่ - http://intra.mwa.co.th/fpc_dept_law.html - http://intra.mwa.co.th/fpc_rule.html 2. OPL เรื่อง มารยาทในการใช้ Social Network 3. OPK เรื่อง 10 ภัยอันตรายจาก Social Network 4. OPK เรื่อง เล่น Social อย่างไรไม่ผิด พรบ. 5. OPK เรื่อง 9 ข้อระวังติดคุกไม่ควรโพสต์ลง Social 6. OPL เรื่อง การแชร์ข้อมูลบน Facebook 7. OPL เรื่อง การเข้าถึงโพสต์บน Facebook 8. OPL เรื่อง เทคนิคการตั้งค่ากรุ๊ปใน Facebook 9. OPK เรื่อง เทคนิคการใช้งาน Facebook อย่างปลอดภัย 10. OPL เรื่อง การโพสต์รูปบน LINE (PC) 11. OPK เรื่อง ข้อปฏิบัติในการใช้รหัสผ่าน (Active Directory : AD) 12. OPA เรื่อง เทคนิคการตั้ง Password สิ่งสำคัญที่ไม่ควรมองข้าม	1. นางรุ่งพร จันทรักษ์ 2. นางสาวชมภูนุช คุปติวุฒิ 3. นายสมโภช เกียรติกสิกร 4. นางสาวธารินี พงศีลวัต 5. นายธนานนท์ โดมทอง 6. นางสาวพัชรกมล ขยันกิจ	- พนักงาน - ผู้ปฏิบัติงาน กปน.

การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

One Point Lesson: OPL

ชื่อเรื่อง	มารยาทในการใช้ Social Network		ลำดับ	1
			วันที่เขียน	09/05/60
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		รุ่งพร จันทรักษ์	[illegible]	[illegible]
		09/05/60	23/05/60	23/05/60

วัตถุประสงค์

เพื่อให้พนักงานและผู้ปฏิบัติงานทราบเรื่องมารยาทในการใช้ Social และสิ่งที่ไม่ควรกระทำบนสังคมออนไลน์

เนื้อหา มารยาท และสิ่งที่ไม่ควรกระทำบนสังคมออนไลน์ มีดังนี้

1. มารยาททั่วไป การสนทนาผ่าน Social Network ทำได้สะดวก ง่ายดาย แต่ต้องคำนึงถึงมารยาทในการสนทนาด้วย ทั้งเนื้อหาที่ต้องการสื่อตลอดจนการใช้ภาษาในอินเทอร์เน็ต ควรคิดให้ดีและรอบคอบก่อนที่จะสื่อออกไป
2. อย่าคาดเดาข้อความบนแถบสถานะส่วนตัวของคนอื่น Social Network หลายโปรแกรมมีแถบให้แสดงชื่อและสถานะตัว เพื่อให้เราสามารถบ่งบอกถึงความเป็นตัวเองได้เต็มที่ (Facebook, Line อื่นๆ) ซึ่งแต่ละคนก็จะมีแบบฉบับเป็นของตัวเอง เราจึงไม่ควรคาดเดาข้อความบนสถานะส่วนตัวของคนอื่น เช่น บางคนตั้งสถานะว่า “เบื่อคนจริงๆ เลย” แล้วเราไปถามว่า “เบื่อใครหว่า เบื่อฉันเหรอ” อาจเป็นต้นเหตุให้ทะเลาะกันได้
3. ดูกาลเทศะก่อนส่งข้อความ บน Social Network สามารถส่งข้อความโต้ตอบกันได้ แต่เวลาเราส่งไปก็ใช่ว่าจะได้รับคำตอบกลับในทันทีเสมอไป ดังนั้นจึงไม่ควรทวงคำตอบตลอดเวลาควรคำนึงถึงอีกฝ่ายด้วย โดยทั่วไปเวลา 8:00 – 18:00 น. จะเป็นช่วงเวลาทำงานของหลายๆ คน ดังนั้นจึงไม่ควรคุยเรื่องที่ไม่จำเป็น
4. อย่าบล็อกคนอื่นโดยไม่จำเป็น ถึงแม้จะมีปัญหาหรือไม่เข้าใจกัน ก็ไม่ควรบล็อกเขาทันที อย่างมากก็ลบชื่อออกหรือไม่ตอบในกรณีที่มีเรื่องไม่สำคัญ แม้บางคนจะไม่ค่อยได้คุยแต่การบล็อกโดยไม่ต้องการคบหาเลยก็เป็นเรื่องที่ไม่ถูกต้องเท่าไหร่ เพราะการบล็อกก็เหมือนกับการตัดสัมพันธ์กัน หากภายหลังเขารู้ว่าเราบล็อกเขาโดยไม่มีเหตุผล จะทำให้เขามองคุณในแง่ลบ
5. อย่ารบกวนคนอื่น ไม่ใช่ว่าทุกคนจะอยู่ที่หน้าจอตลอดเวลา และพูดคุยโต้ตอบกับคุณได้ ดังนั้นก่อนจะเข้าไปทักทายควรดูสถานะที่เขาตั้งไว้ หรืออาจจะสอบถามไปก่อนว่าสามารถคุยได้หรือไม่ เพราะหากเขากำลังทำงานอยู่หรือไม่สามารถพูดคุยได้ การส่งข้อความไปให้เขาอาจทำให้เขาเสียสมาธิที่กำลังจดจ่ออยู่กับงานได้

วันที่สอน							
ผู้สอน							
ผู้เรียน							
ผลการเรียนรู้							

การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

องค์ความรู้

(One Point Knowledge)

10 ภัยอันตรายจาก Social Network

กลุ่ม SGA : รู้ทัน Social เปรี้ยวกว่าใคร หน่วยงาน สายงานเทคโนโลยีสารสนเทศ	ผู้อนุมัติ (คณะกรรมการย่อยสายงาน) (ลงชื่อ)..... (นางพิศวาท ภาพสุวรรณ) ตำแหน่ง ผอ.ฝยท.
องค์ความรู้เรื่อง 10 ภัยอันตรายจาก Social Network	23/05/60 รหัส OPK

10 ภัยอันตรายจาก Social Network

OPK ฉบับนี้เป็นการบอกรายละเอียดของภัยอันตรายของ Social Network เพื่อเป็นแนวทางให้ผู้ใช้งานใช้งาน Social Network อย่างระมัดระวัง เพื่อความปลอดภัย เพื่อให้รู้เท่าทันภัยคุกคามจากการเข้าใช้งาน Social Network

10 ภัยอันตรายจาก Social Networkมีดังนี้

1. หลอกว่ามาดีแต่จริงๆประสงค์ร้าย (Social Engineering Attack on Social Network)–การโจมตีที่ตัวบุคคลในลักษณะที่คาดไม่ถึง ในรูปแบบ Application/Game บน Facebook เมื่อคลิกเข้าไปใช้งาน Application/Game ดังกล่าว ก็จะตกเป็นเหยื่อของอาชญากรโดยไม่ทันตั้งตัว

2. ล่อเหยื่อตกปลาออนไลน์ (Phishing Attack)–เทคนิคการล่อล่วงโดยการส่ง 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. ถูกสวมรอยง่ายๆ แค่เล่น 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 โดยหลอกให้คลิกรูปที่ล่อตาล่อใจบนเว็บไซต์ 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 และผู้ใช้งานเผลอดาวน์โหลดโดยไม่รู้ตัว

7. เทคนิคการโจรกรรมข้อมูลขั้นสูงแบบต่อเนื่อง - APT (Advance Persistent Threat) and MitB(Man-In-The-Browser Attack)เป็นเทคนิคการโจมตีขั้นสูงที่มุ่งเน้นเป้าหมายผู้ใช้งาน Internet Banking ผู้ใช้งานคอมพิวเตอร์ในระดับองค์กร หรือ รัฐบาล โดยอาชญากรสามารถฝังโปรแกรมมุ่งร้าย เข้าไปในระบบคอมพิวเตอร์ของเป้าหมาย เพื่อแอบโจรกรรมข้อมูลลับ อย่างต่อ เนื่อง 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. บอกเพื่อนว่าเราอยู่ไหน (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)..... (นางพิศวาท ภาพสุวรรณ) ตำแหน่ง ผอ.ฝยท.
องค์ความรู้เรื่อง เล่น Social อย่างไรไม่ผิด พรบ.	23/05/60 | รหัส OPK

เล่น Social อย่างไรไม่ผิด พรบ.

OPK ฉบับนี้เป็นการบอกรายละเอียดเกี่ยวกับ พรบ.คอมพิวเตอร์ เพื่อเป็นแนวทางให้ผู้ใช้งาน ไม่กระทำการเข้าข่ายทำผิด พรบ.คอมพิวเตอร์ นั่นเอง

บทนำ

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ช่วงเวลานี้ ผู้ใช้อินเตอร์เน็ตมีจำนวนมากขึ้น 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 ที่ผู้ใช้งานอินเตอร์เน็ตต้องทำความเข้าใจและปฏิบัติให้อยู่ในกรอบของกฎหมาย หากฝ่าฝืนอาจถูกดำเนินคดีได้

ผู้ใช้อินเตอร์เน็ต หรือเล่น Social network ต้องมีความรู้ในเรื่องนี้เพื่อป้องกันไม่ให้ผิด พรบ. หรือผิดกฎหมายโดยไม่รู้ตัวนั่นเอง

ตัวอย่างการกระทำ หรือการโพสต์ ข้อมูลปลอม ข้อมูลเท็จ อย่างกรณีของอดีตเณรคำที่มีการโพสต์ข้อความแสดงอิทธิฤทธิ์อวดอ้างผ่านทางเว็บไซต์ให้คนหลงเชื่อ หรือ ให้ข้อมูลเท็จ ที่จะเกิดความเสียหายต่อความมั่นคงของประเทศ ประชาชนตื่นตระหนก , โพสข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร 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) "

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

ก่อนส่งต่อ หรือแชร์ ลองตรวจสอบข้อมูลก่อนว่าเนื้อหานี้จริงหรือไม่ เพราะถ้าคุณส่งข้อมูลเท็จ ข้อมูลที่เกิดความเสียหายต่อผู้อื่น หรือต่อความมั่นคงของประเทศ ข้อมูลลามก อนาจาร ตามข้อมูลที่มีความผิดตาม พรบ. คอม คุณก็จะมีความผิดในมาตรา 14 วรรค 5 โดนด้วย!....รับโทษเหมือนกัน

อีกเรื่องที่เจอบ่อย คือการตัดต่อภาพที่ทำให้ผู้อื่นเสียหายแล้ว เผยแพร่ทางอินเทอร์เน็ต อันนี้ มีความผิดตามมาตรา 16 ระบุไว้ว่า

"ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูล คอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือ ปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ"

สำหรับผู้ให้บริการ ก็ต้องระวัง หมั่นดูแลข้อมูลต่างๆที่คนอื่นโพสทิ้งไว้ในเว็บเราด้วย เช่นพวกเว็บบอร์ด กระทู้ หรือ คาความเห็นต่างๆ เพราะมีคนมาโพสต์ข้อความ โพสต์รูปที่ทำให้บุคคลอื่นเสียหาย หรือภาพอนาจาร มีเนื้อหาพาดพิงสถาบัน แล้วคุณเพิกเฉย ปล่อยให้มี การกระทำนั้น คุณก็จะ มีความผิด พรบ.คอมพิวเตอร์ ในมาตรา 15 ข้อหาสนับสนุน ยินยอมให้คนอื่นเผยแพร่ข้อมูลที่กระทบให้ผู้อื่นเดือดร้อน เสียหาย กระทบความมั่นคงของรัฐ และอื่นๆตามที่ พรบ.คอม มาตรา 14 ซึ่งกรณีนี้เกิดขึ้นมาแล้วตั้งแต่เริ่มใช้ พรบ.คอม ช่วงแรกๆด้วย มีเว็บมาสเตอร์ถูกจำคุกมาแล้ว ทั้งๆที่ไม่ได้เป็นผู้กระทำผิด แต่ตรวจสอบพบเนื้อหาที่ผิด พรบ.คอม ก็โดนติดคุกได้เช่นกัน และมีการตรวจสอบข้อมูลของผู้ให้บริการโฮสด้วย

พรบ.คอมพิวเตอร์ เป็นเรื่องใกล้ตัวที่ผู้ใช้อินเตอร์เน็ตต้องรู้ และปฏิบัติให้อยู่ในกฎหมาย ด้วย หากกระทำผิด พรบ. คุณก็จะถูกดำเนินคดี จำคุก และปรับ ได้ ซึ่งคุณอ้างไม่ได้ว่าคุณไม่รู้!!! เพราะคุณคือผู้ใช้อินเตอร์เน็ต 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)..... (นางพิศวาท ภาพสุวรรณ) ตำแหน่ง ผอ.ฝยท.
องค์ความรู้เรื่อง 9 ข้อระวัง “ติดคุก” ไม่ควรโพสต์ลงโซเชียล	23/05/60 | รหัส OPK

9 ข้อระวัง "ติดคุก" ไม่ควรโพสต์ลงโซเชียล

OPK ฉบับนี้เป็นการบอกรายละเอียดของเรื่องราวต่างๆ ที่ไม่ควรโพสต์ลง Social Media เพื่อเป็นแนวทางให้ผู้ใช้งาน ไม่กระทำการเข้าข่ายกระทำความผิดกฎหมาย

บทนำ

ปัจจุบันยอดผู้ใช้โซเชียลมีเดียไทยพุ่งแตะเป็นอันดับ 3 ของอาเซียน โดยเฉพาะโซเชียลมีเดียอย่าง Facebook ที่มีผู้ใช้ไทยกว่า 35 ล้านบัญชี เฉพาะแค่กรุงเทพมหานครมีผู้ใช้ถึง 20 ล้านบัญชีไปแล้ว ยิ่งมีผู้ใช้เยอะขึ้นเท่าไหร่ ดูเหมือนปัญหาจากพฤติกรรมการโพสต์และแชร์ของผู้ใช้ก็มีมากขึ้นเป็นเงาตามตัว 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

แม้จะเป็นแอคเค้าท์ส่วนตัว และคุณคิดว่าการโพสต์ลงบนพื้นที่ของตัวเองจะมีสิทธิ์เสนอข้อมูลอะไรก็ได้ แต่ผิดถนัดครับ โดยเฉพาะการลงรูปโป๊เปลือย ภาพอนาจารของตัวเองหรือแม้แต่ภาพคนอื่น ก็มีความผิดทางกฎหมายและมีโทษปรับ 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 ที่ส่งผลเสียต่อเจ้าของแอคเค้าท์ ถือว่าเข้าข่ายความผิด พ.ร.บ คอมพิวเตอร์ตามข้อกฎหมายเรื่องลิขสิทธิ์

6. แก้ไข ดัดแปลงข้อความผู้อื่น

โทษปรับ 100,000 บาท จำคุก 5 ปี หรือทั้งจำทั้งปรับเลยทีเดียว หากมีการนำข้อมูลในโซเชียลมีเดียของผู้อื่นไปแก้ไขหรือดัดแปลง และทำให้เกิดความเสื่อมเสียหรือเสียหายต่อเจ้าของข้อมูล

7. แชร์ต่อๆ กันมาอีกที

ความรู้เท่าไม่ถึงการณ์ ก็อาจทำให้คุณติดคุกได้จากการแชร์ข้อมูลไม่เลือก และไม่ตรวจสอบข้อเท็จจริงก่อน เมื่อเห็นคนแชร์มาก็แชร์ต่อหรือนำไปโพสต์ต่อ ซึ่งอาจเป็นข้อมูลเท็จที่ส่งผลเสียต่อสังคมโดยรวมและทำลายชื่อเสียงของบุคคลอื่นได้ ซึ่งการแชร์ลักษณะนี้ถือเป็นความผิดตามกฎหมายอีกด้วย

8. แชร์ข้อความลูกโซ่

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

9. โพสต์หมิ่นเบื้องสูง

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

ทีนี้จะโพสต์จะแชร์อะไร ลองคิดก่อนซักนิดดีกว่าว่าไปกระทบต่อผู้ใดและสร้างความวุ่นวายต่อสังคมหรือไม่ 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	[illegible]	[illegible]
		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 ถ้าต้องการให้เห็นเฉพาะเพื่อนให้เลือก Friends เพื่อความปลอดภัยในการเข้าถึงข้อมูล

ส่วน Public เป็นการแชร์ข้อมูลแบบสาธารณะ ซึ่งผู้ใช้งาน Facebook ทั้งที่เป็นเพื่อนและไม่ได้เป็นเพื่อนจะเห็นโพสต์นี้ ซึ่งในการแชร์ข้อมูลที่สำคัญต่าง นั้นไม่ควรแชร์แบบ Public เพื่อความปลอดภัยนั่นเอง

วันที่สอน							
ผู้สอน							
ผู้เรียน							
ผลการเรียนรู้							

การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

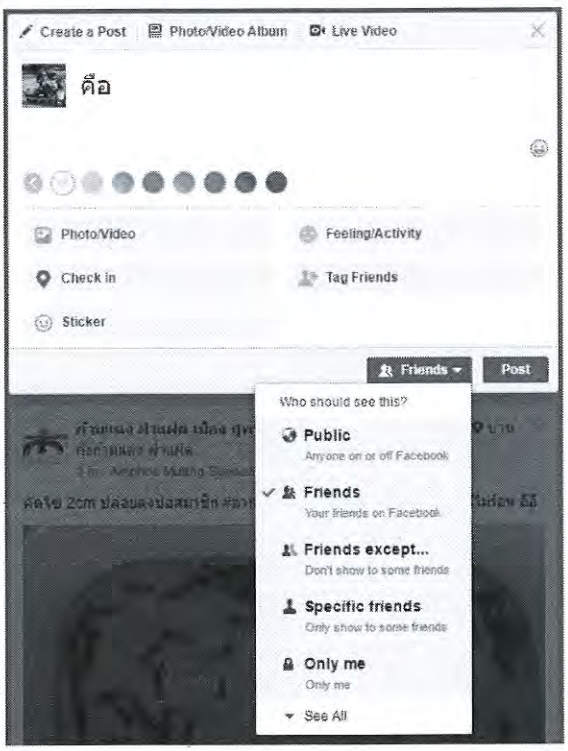
One Point Lesson: OPL

ชื่อเรื่อง	การเข้าถึงโพสต์บน Facebook		ลำดับ	6
			วันที่เขียน	4 พ.ค. 2560
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		สมโภช เกียรติกสิกร		
		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 ถ้าต้องการให้เห็นเฉพาะเพื่อนให้เลือก Friends เพื่อความปลอดภัยในการเข้าถึงข้อมูล

ส่วน Public เป็นการโพสต์ข้อมูลแบบสาธารณะ ซึ่งผู้ใช้งาน Facebook ทั้งที่เป็นเพื่อนและไม่ได้เป็นเพื่อนจะเห็นโพสต์นี้ ซึ่งในการโพสต์ข้อมูลที่สำคัญต่าง นั้นไม่ควรโพสต์แบบ Public เพื่อความปลอดภัยนั่นเอง

วันที่สอน							
ผู้สอน							
ผู้เรียน							
ผลการเรียนรู้							

การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

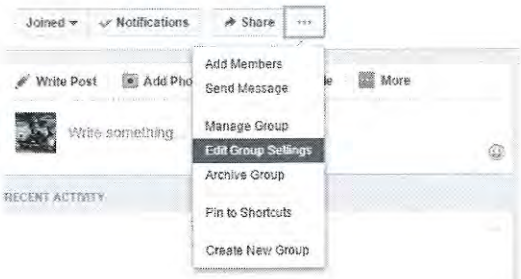
One Point Lesson: OPL

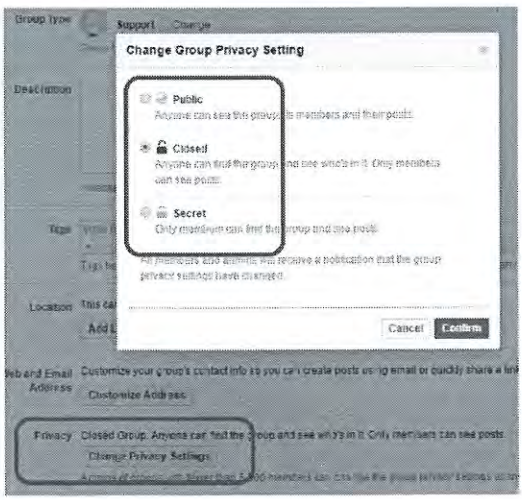
ชื่อเรื่อง	เทคนิคการตั้งค่ากรุ๊ปใน Facebook		ลำดับ	7
			วันที่เขียน	4 พ.ค. 2560
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		สมโภช เกียรติกสิกร		
		04/05/60	23/05/60	23/05/60

วัตถุประสงค์

เพื่อความปลอดภัยของข้อมูล และการเข้าถึงกรุ๊ปใน Facebook

เนื้อหา





เมื่อตั้งกรุ๊ปของ Facebook ขึ้นมาแล้ว Admin ของ Group สามารถตั้งค่าการเข้าถึงกรุ๊ปได้ โดยเข้าที่ Edit Group Settings และคลิกที่ Change Privacy Setting

Admin ของ Group สามารถตั้งค่ากรุ๊ปให้เป็น Public (สาธารณะ), Closed (กลุ่มปิด) หรือSecret (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)..... (นางพิศวาท ภาพสุวรรณ) ตำแหน่ง ผอ.ฝยท.
องค์ความรู้เรื่อง เทคนิคการใช้งาน Facebook อย่างปลอดภัย	23/05/60 รหัส OPK

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 และกรุงเทพเป็นเมืองที่ผู้ใช้ Facebook มากที่สุดในโลก มีจำนวนมากถึง 24 ล้านคน หรือ 1.3% ของผู้ใช้ Facebook ทั้งหมด จึงขอแนะนำการใช้ Facebook อย่างปลอดภัย ดังนี้

1. ใช้เครือข่าย Internet ที่มีความปลอดภัยน่าเชื่อถือ

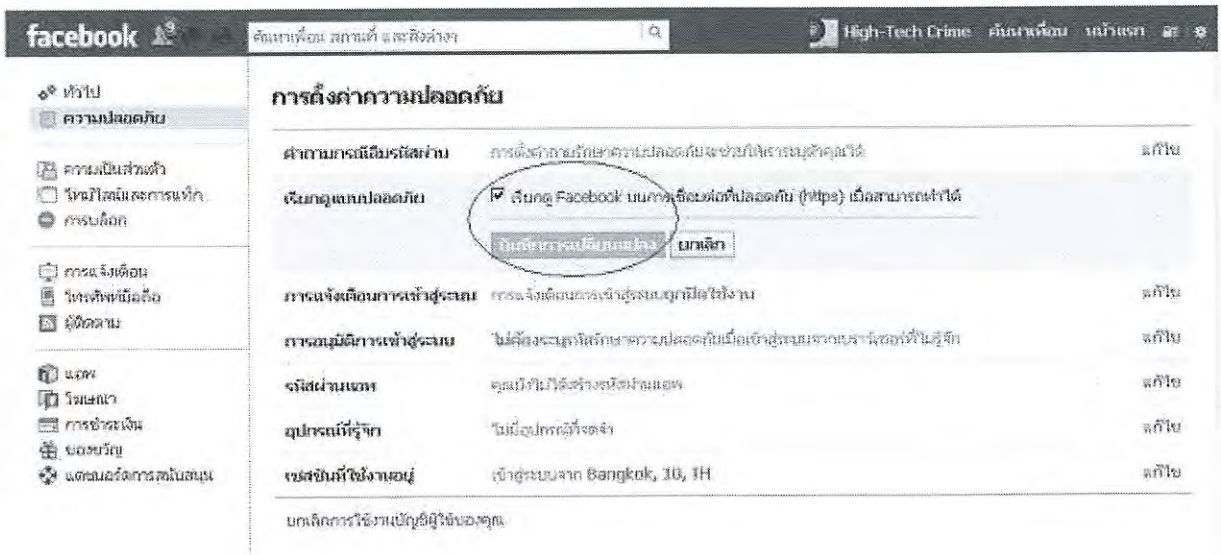
2.รักษาความปลอดภัยรหัสผ่าน โดยต้องไม่แชร์รหัสผ่าน โดยคุณควรจะเป็นเพียงคนเดียวที่ทราบรหัสผ่าน และรหัสผ่านควรจะเดาได้ยาก หลีกเลี่ยงการใช้ชื่อของคุณหรือคำที่คาดเดาง่ายเป็นส่วนหนึ่งของรหัสผ่าน

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

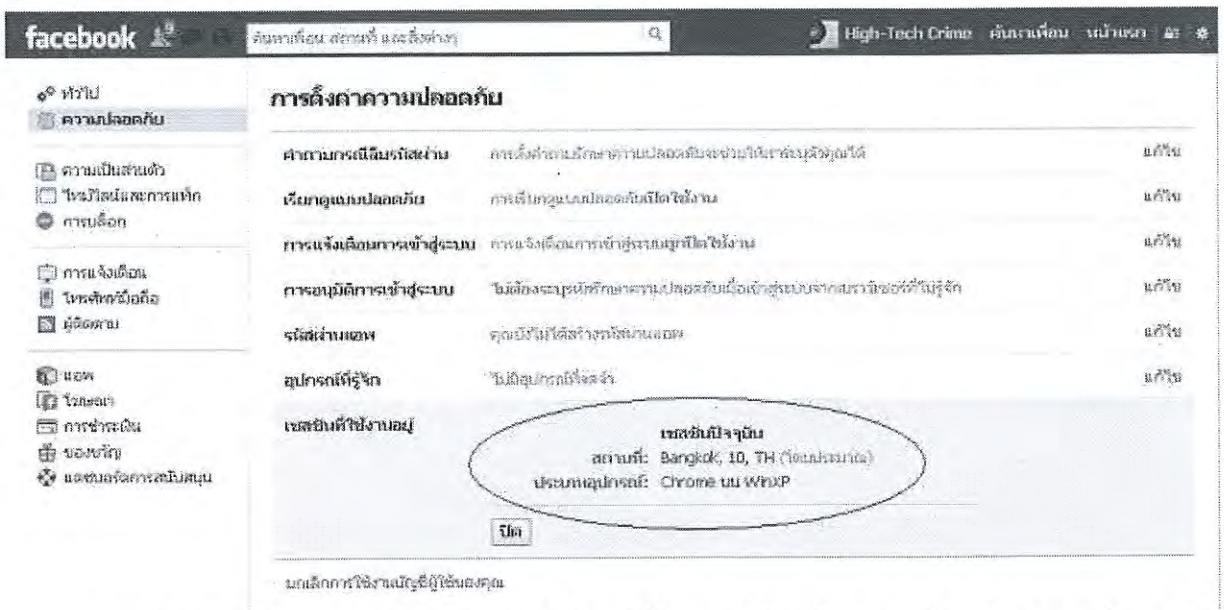
4.ออกจากระบบ Facebook เมื่อใช้เครื่องคอมพิวเตอร์ร่วมกับบุคคลอื่น ๆ

5.ไม่ควรรับคำขอเป็นเพื่อนจากบุคคลที่คุณไม่รู้จัก ผู้หลอกลวงอาจสร้างบัญชีผู้ใช้ปลอมขึ้นมาเพื่อเป็นเพื่อนกับผู้คน การเป็นเพื่อนกับผู้หลอกลวงอาจทำให้พวกเขาสามารถเข้าถึงเพื่อส่งสแปมในไทม์ไลน์ของคุณ แท็กคุณในโพสต์ และส่งข้อความที่เป็นอันตรายถึงคุณ

6. **ควรตั้งค่าการเชื่อมต่อที่ปลอดภัย (https)**



ถ้าพบว่าเซสชั่นปัจจุบัน ถูกใช้จากระบบปฏิบัติการและ Browser อื่นที่แตกต่างจากเครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อ ให้รีบปิดเซสชั่นดังกล่าว แล้วรีบเปลี่ยนรหัสผ่านใหม่ทันที



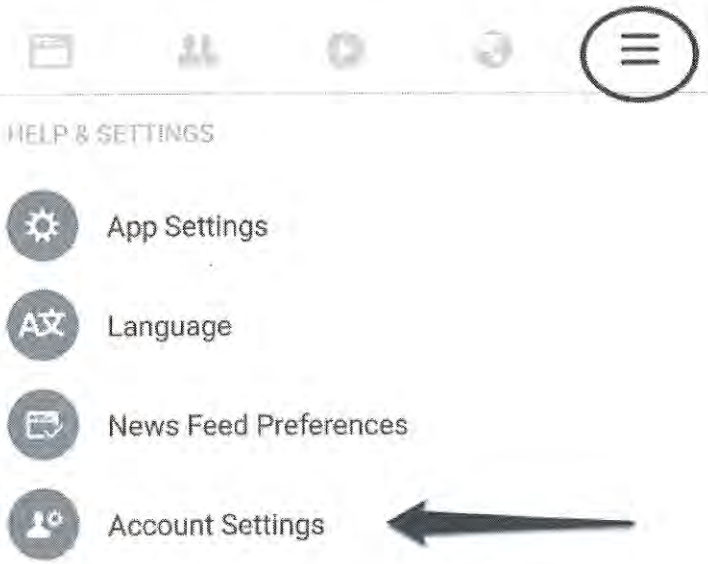
7. อย่าคลิกลิงก์ต้องสงสัยโดยเด็ดขาด แม้ว่าลิงก์นั้นจะดูเหมือนว่ามาจากเพื่อนหรือบริษัทที่คุณรู้จักก็ตาม ลิงก์ต้องสงสัยนี้ยังรวมถึงลิงก์บน Facebook (เช่น ในโพสต์) หรือทางอีเมล โปรดจำไว้ว่า Facebook จะไม่

ขอรหัสผ่านของคุณทางอีเมลโดยเด็ดขาด หากคุณเห็นลิงก์ที่น่าสงสัยใน Facebook ให้รายงานไปที่ Facebook ด้วยการใช้ link รายงานที่ปรากฏใกล้กับเนื้อหานั้น

8.หมั่นตรวจสอบความเคลื่อนไหวของกิจกรรมและรายละเอียดในการเชื่อมต่อใช้งาน เมื่อไม่ใช้งานให้ออกจากระบบทุกครั้ง

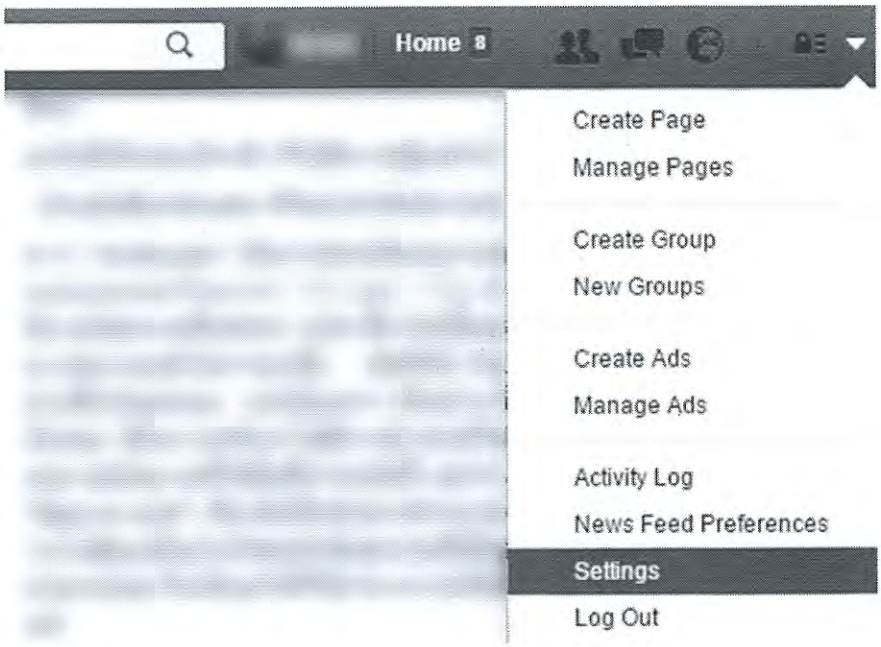
9. **ตั้งค่าความปลอดภัย ใน Facebook Account Settingsเพื่อเสริมความปลอดภัยให้บัญชี Facebook(ที่มา https://www.blognone.com/node/80737)**

เชื่อว่าผู้ใช้ Facebook หลายคนคงไม่รู้ว่าหน้าจอตั้งค่าของ Facebook อยู่ตรงไหน ถ้าใช้งานบนมือถือให้เลือกปุ่มสามขีดด้านขวาสุด แล้วเลื่อนลงไปล่างสุด จะเห็นตัวเลือก **Account Settings**

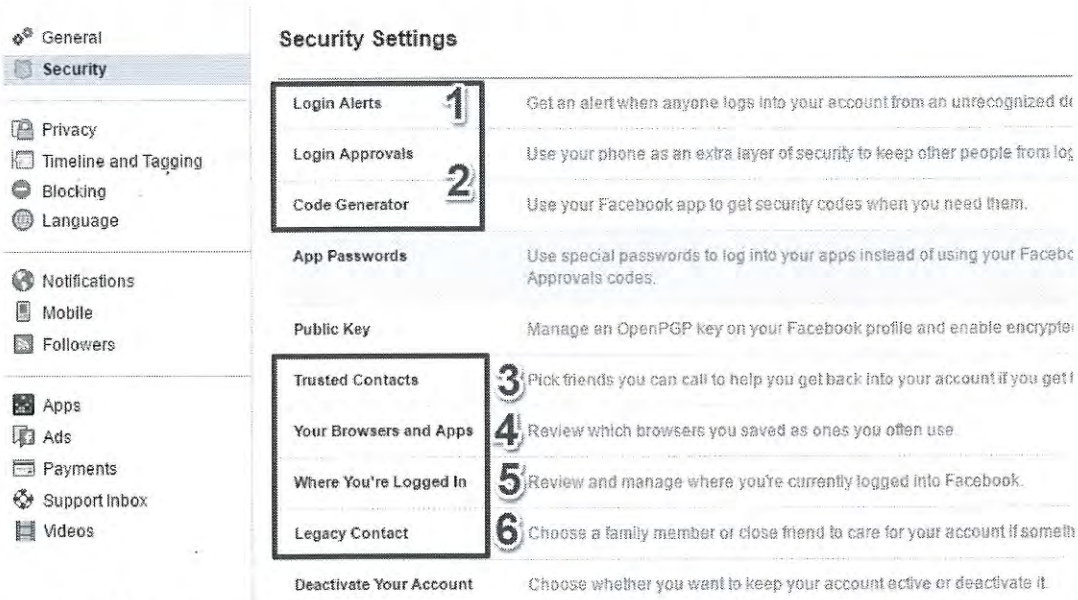


ส่วนผู้ที่ใช้บนคอมพิวเตอร์ ให้เลือกลูกศรชี้ลงที่อยู่มุมขวาบนของหน้าจอ แล้วเลือกเมนู **Settings**

หมายเหตุ: ภาพหน้าจอจากนี้ไปจะใช้เวอร์ชันคอมพิวเตอร์เป็นหลัก แต่บนมือถือก็มีวิธีการเรียงเมนูแบบเดียวกัน ในตัวอย่างจะใช้เมนูภาษาอังกฤษ ซึ่งถ้าใครใช้เมนูภาษาไทยก็สามารถเทียบตำแหน่งเมนูเดียวกันได้ หรือไม่ก็เปลี่ยนเมนูเป็นภาษาอังกฤษจากหมวด Language ได้



จากนั้นให้เลือกการตั้งค่าหมวด **Security** จากเมนูด้านซ้ายมือดังภาพ ฝั่งขวาจะเห็นตัวเลือกชื่อ Security Settings ซึ่งเอาไว้ตั้งค่าเกี่ยวกับระบบความปลอดภัยทั้งหมดของ Facebook



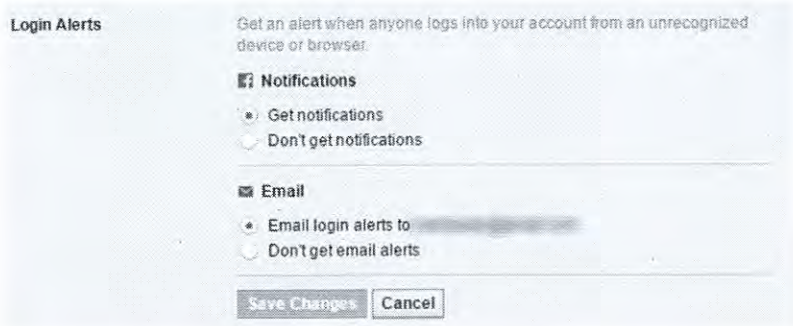
เนื่องจากหน้าจอนี้มีตัวเลือกค่อนข้างมาก เราจะขอแนะนำเฉพาะตัวเลือกที่สำคัญ 6 อย่างตามหมายเลขที่เขียนกำกับไว้ โดยจะแยกอธิบายทีละหัวข้อ ดังนี้

1. Login Alerts แจ้งเตือนเมื่อมีคนล็อกอินบัญชีของเรา

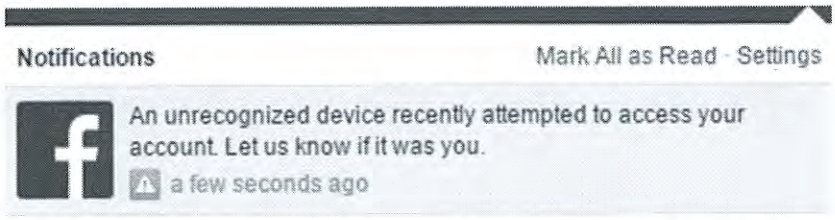
ฟีเจอร์นี้เป็นความปลอดภัยพื้นฐานของบัญชี Facebook ที่ทุกคนควรเปิดใช้งานไว้ เพราะไม่ยุ่งยากอะไร และช่วยให้เรารู้ว่ามีคนอื่นมาล็อกอินบัญชีของเราได้ตลอดเวลา

แนวคิดของฟีเจอร์ Login Alerts คือผู้ใช้มักใช้งาน Facebook จากอุปกรณ์ชิ้นเดิม คอมพิวเตอร์เครื่องเดิม ถ้ามีการล็อกอินจากคอมพิวเตอร์เครื่องใหม่ที่ Facebook ไม่เคยเห็นมาก่อน ย่อมมีโอกาสสูงที่จะเป็นผู้อื่นล็อกอินเข้ามา ตัวเลือกนี้จะแจ้งเตือนผู้ใช้ผ่าน 2 ช่องทางโดยแนะนำให้**เปิดใช้งาน**ทั้งสองระบบคือ

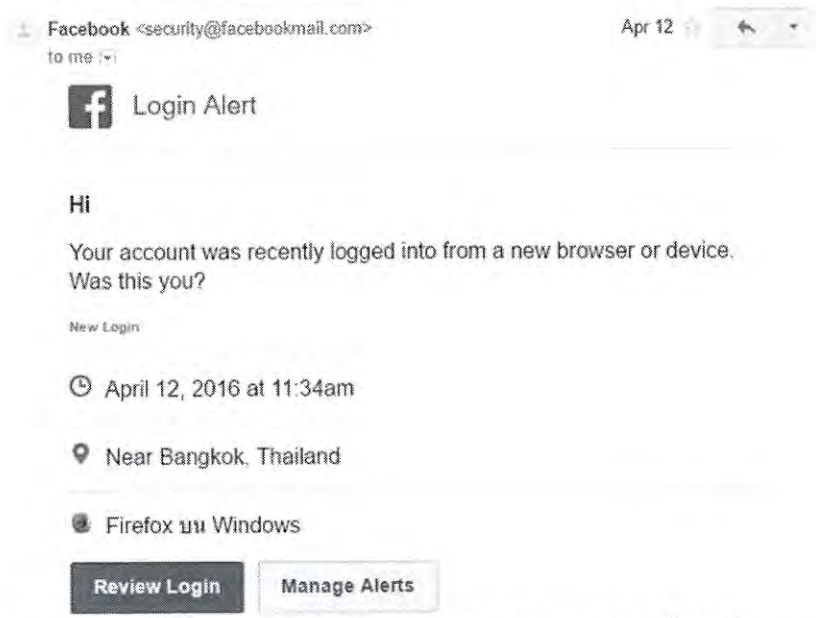
- ระบบแจ้งเตือนของ Facebook เอง (ทั้งเว็บและแอพ เช่น กรณีที่เราใช้งาน Facebook ในเครื่องอื่นอยู่มันจะขึ้นเตือน)
- อีเมลที่เราสมัครใช้งาน Facebook



ถ้าเราเปิดตัวเลือกนี้ไว้ และมีอุปกรณ์อื่นพยายามล็อกอินเข้าบัญชีของเรา จะเห็นการแจ้งเตือนแบบนี้โผล่ขึ้นมา



ส่วนการแจ้งเตือนทางอีเมล จะมีหน้าตาดังภาพ (อีเมลจะถูกส่งมาจาก security@facebookmail.com)



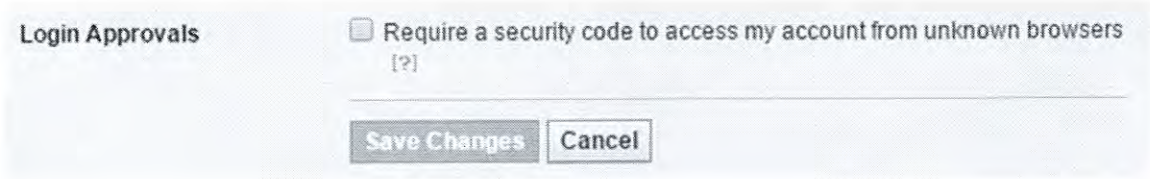
ในกรณีที่เราล็อกอินจากมือถือหรือคอมพิวเตอร์เครื่องใหม่ แล้วจะใช้งานเครื่องนี้ต่อไปในระยะยาว เราก็สามารถตั้งให้ Facebook จดจำ (Remember Browser หรือ Save Browser) เพื่อที่มันจะได้ไม่ต้องเตือนทุกครั้งให้รำคาญได้ด้วย

2. Login Approvals ระบบล็อกอินสองชั้น ใส่รหัสผ่านจากมือถือ

ในหัวข้อแรก กล่าวถึงระบบล็อกอินสองชั้นไปแล้ว Facebook ก็มีระบบล็อกอินสองชั้น โดยใช้ชื่อว่า **Login Approvals** และใช้คู่กับ **Code Generator**

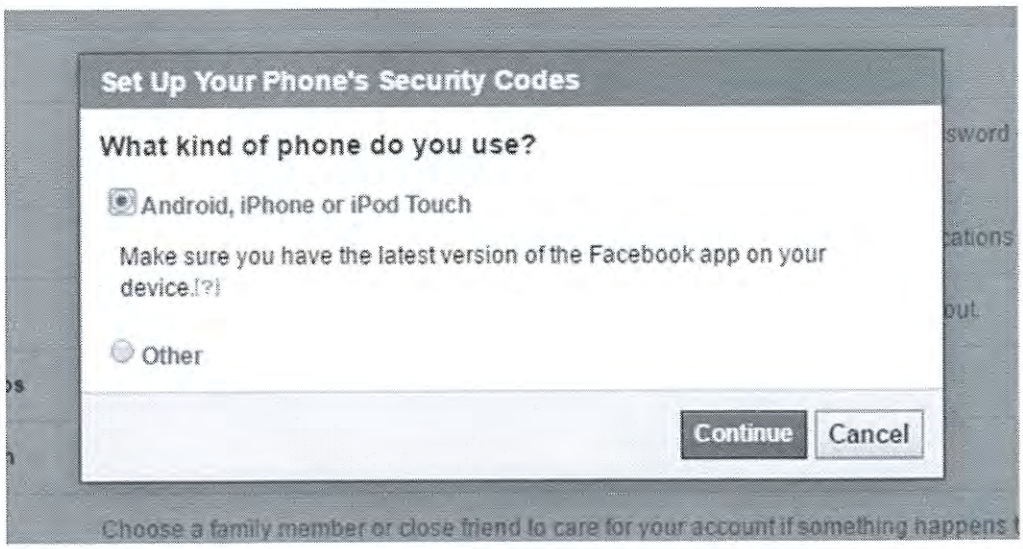
แนวคิดของ Facebook คือผู้ใช้ส่วนใหญ่มีแอพ Facebook บนมือถืออยู่แล้ว ดังนั้นแทนที่จะรับโค้ดยืนยันตัวตนจาก SMS เหมือนกับที่พวกธนาคารออนไลน์ทำ ก็ให้แอพ Facebook ของเราเป็นตัวสุ่มโค้ดให้แทน ตามปกติแล้ว

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



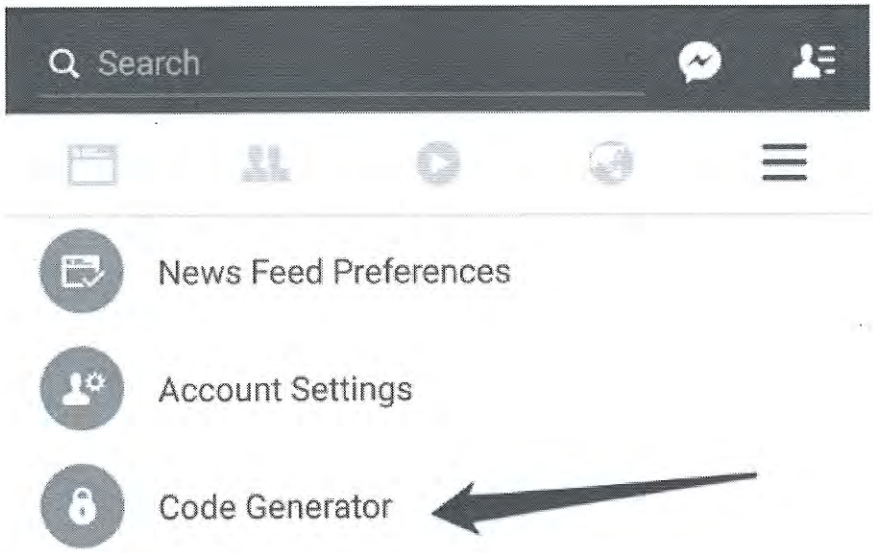
จากนั้น Facebook จะขึ้นหน้าจอมาอธิบายสั้นๆ ว่า Login Approvals คืออะไร ให้กด Get Started เพื่อไปต่อ

Facebook จะถามเราว่าใช้แอพ Facebook บน Android/iPhone หรือไม่ ให้เลือกอันบนแล้วกด Continue

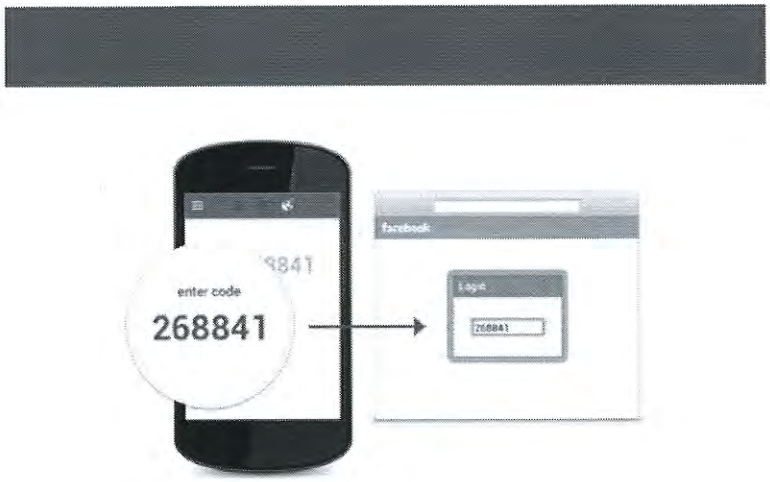


ขั้นต่อไปเราต้องใช้แอพ Facebook บนมือถือเพื่อเรียกตัวสุ่มโค้ด (Code Generator) แล้ว ตามคำอธิบายข้างล่าง ให้กด Continue บนหน้าจอคอมพิวเตอร์ก่อน

วิธีการคือให้เปิดแอพ Facebook บนมือถือขึ้นมา เลือกเมนูสามขีดเหมือนเดิม เลื่อนลงไปหาคำว่า Code Generator



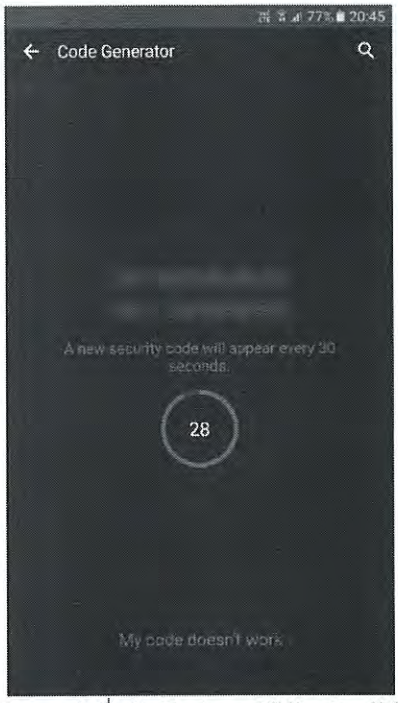
ระบบจะแจ้งให้เราเปิดใช้งาน Code Generator เป็นครั้งแรก โดยกดปุ่ม Activate



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

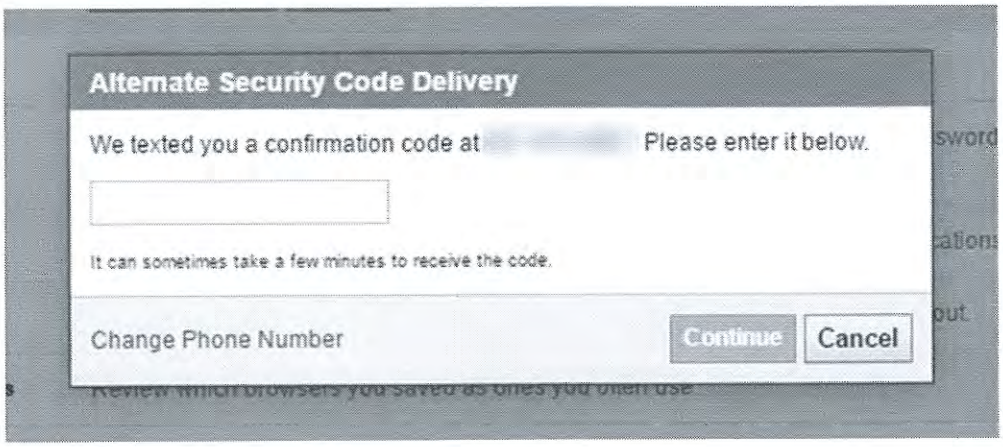
Activate

หน้าจอของเราจะเปลี่ยนเป็นสีเข้ม พร้อมแสดงโค้ด 6 หลักที่เปลี่ยนไปทุก 30 วินาที นี่คือโค้ดชั้นที่สองของเรา ที่ใช้แทนการรับโค้ดทาง SMS

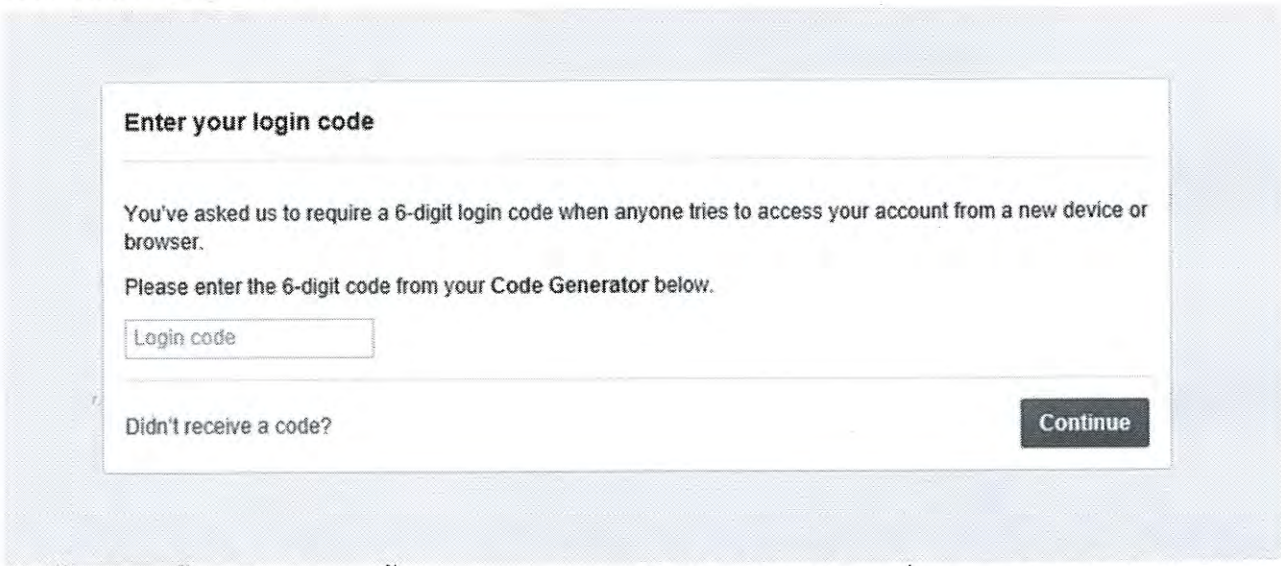


นำโค้ดที่ได้ไปกรอกในหน้าเว็บบนคอมพิวเตอร์เพื่อยืนยันว่าเรามีโค้ดจริง ถ้าโค้ดถูกต้องจะเห็นคำว่า It worked!

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



ถ้าหากมีคนพยายามล็อกอินเข้าบัญชีของเรา (หรือเราจะลองเองก็ได้) เมื่อผ่านชั้นของรหัสผ่านไปแล้ว จะเจอชั้นของการใส่โค้ด 6 หลักตามภาพ

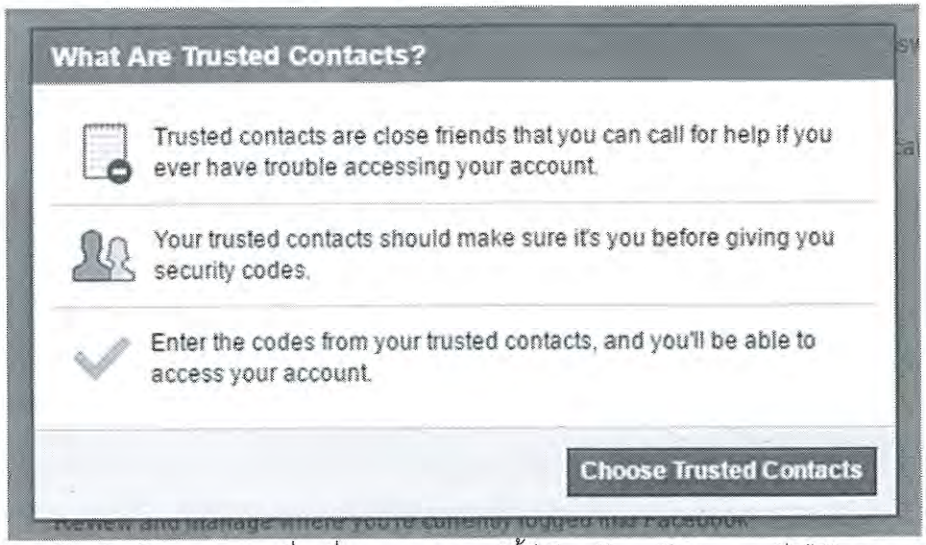


เท่านี้ถือว่าเราตั้งค่าล็อกอินสองชั้นของ Facebook เสร็จเรียบร้อยแล้ว คนที่พยายามล็อกอินเข้าบัญชีเราจะทำงานยากขึ้นมาก เพราะต่อให้รู้รหัสผ่าน ก็ต้องหาโค้ดชุดนี้มาล็อกอินควบคู่ไปด้วย (อาจยกเว้นกรณีนี้มือถือหาย โดนขโมย หรือโดนยึด ซึ่งคนที่เข้าถึงมือถือของเราได้ ก็จะเข้าถึงโค้ดชุดนี้ได้เช่นกัน ซึ่งเป็นสิ่งที่ต้องระวัง)

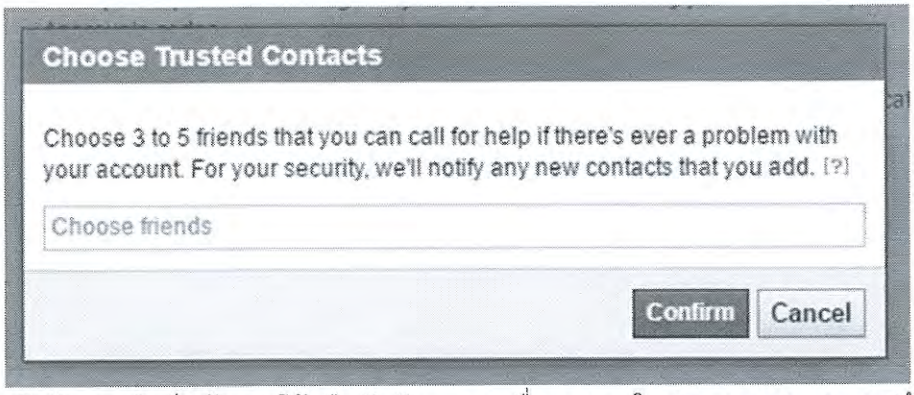
3. Trusted Contacts เพื่อนที่ไว้ใจได้

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) แล้วให้เพื่อนบอกโค้ดเรามาเพื่อยืนยันว่าเราเป็นเจ้าของบัญชีนี้จริงๆ



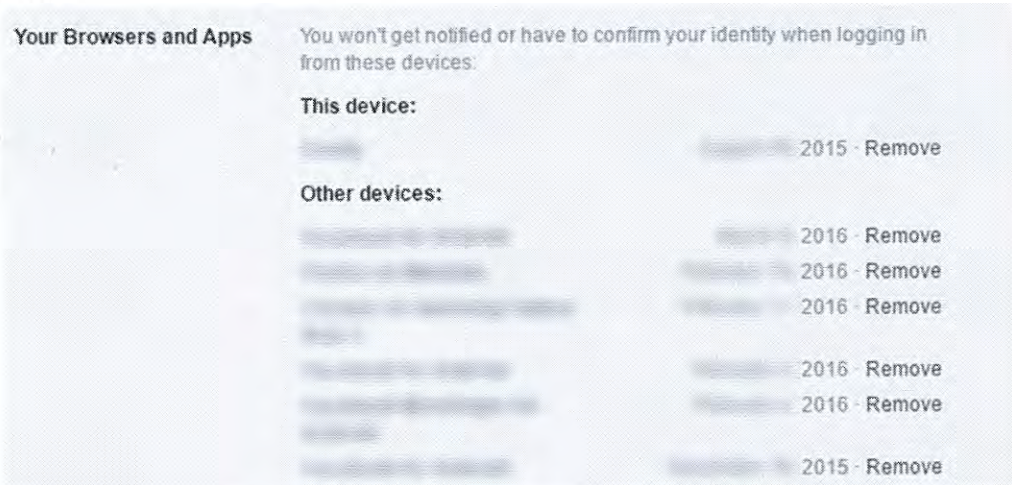
ขั้นตอนการใช้งานก็ไม่มีอะไรยาก กรอกชื่อเพื่อน 3-5 คน แค่นี้ก็เรียบร้อยแล้ว (กรอกเก็บไว้เฉยๆ เอาไว้ใช้งานเมื่อยามยาก) เพื่อนของเราจะได้รับแจ้งว่าเป็น Trusted Contacts ด้วย ดังนั้นควรบอกเพื่อนไว้ล่วงหน้า จะได้ไม่ตกใจเกินเหตุ



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

4. Your Browsers and Apps ย้อนดูสิทธิการเข้าถึงบัญชี

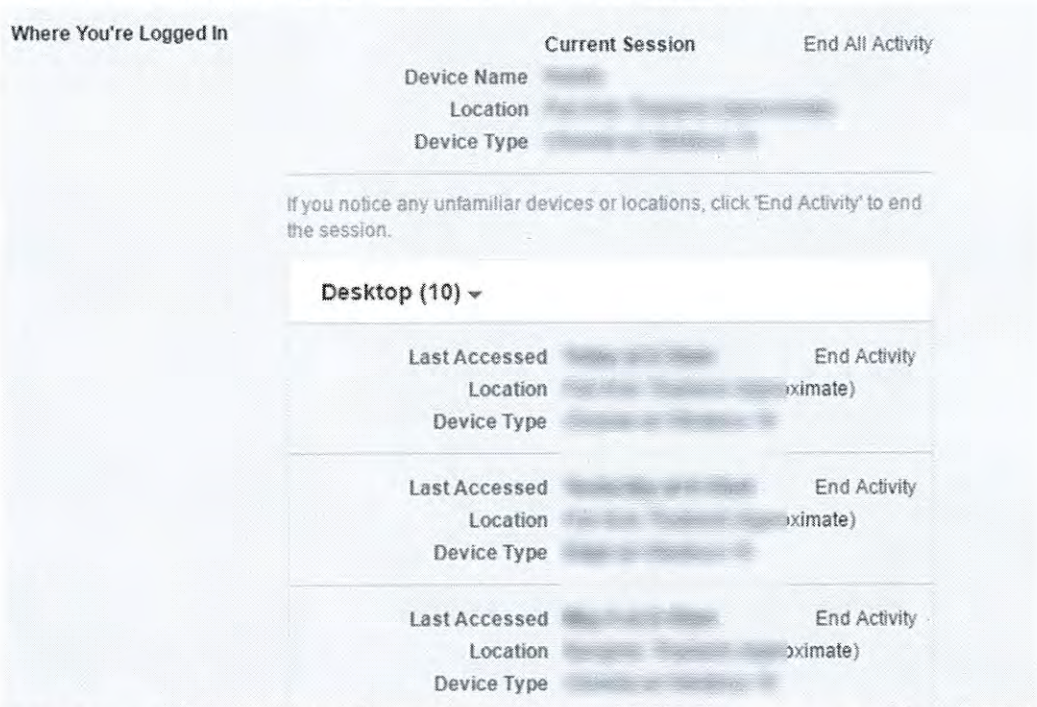
เมื่อใดก็ตามที่เราล็อกอิน Facebook ผ่านเว็บเบราว์เซอร์ หรือมีแอพขอสิทธิใช้งานบัญชีของเรา (โดยเฉพาะพวกเกม) หลายคนคงเคยเห็นหน้าจอยืนยันขอสิทธิการเข้าถึงบัญชี ซึ่งโดยส่วนใหญ่แล้วเราก็ให้สิทธิไป ประวัติการขอสิทธิทั้งหมดของแอพต่างๆ จะถูกเก็บไว้ในหน้าจอตั้งค่า Your Browsers and Apps ย้อนไปตั้งแต่อดีตชาติของเรา



เพื่อความปลอดภัยของเราเอง ขอแนะนำให้เราสั่ง Remove ลบแอพเก่าๆ ทิ้งให้หมด (ถ้าเผลอลบแอพที่ใช้งานอยู่ก็ไม่เสียหาย เพราะมันจะขอสิทธิเราใหม่) ให้เหลือเฉพาะการใช้งานเพียง 3-4 อันล่าสุดเท่านั้นพอ หรือง่ายๆ คือ อะไรเก่ากว่าปีปัจจุบัน ลบออกให้หมด

5. Where You're Loggen In ล็อกอินมาจากที่ไหนบ้าง

ข้อ 5. คล้ายกับข้อ 4. แต่จะแสดงให้เราดูว่าเราล็อกอิน Facebook มาจากคอมพิวเตอร์ มือถือ แท็บเล็ต ฯลฯ เครื่องไหน เมื่อไร จากตำแหน่งไหนของโลก
หน้าจอนี้จะช่วยให้เราตรวจสอบประวัติย้อนหลังได้ว่า มีการล็อกอินแปลกๆ จากที่อื่นที่เราไม่รู้จักหรือไม่ (เช่น ไม่ได้ไปต่างประเทศเลย แต่ถ้าพบการล็อกอินจากนอกประเทศไทย ก็แปลว่าไม่ใช่เรา)

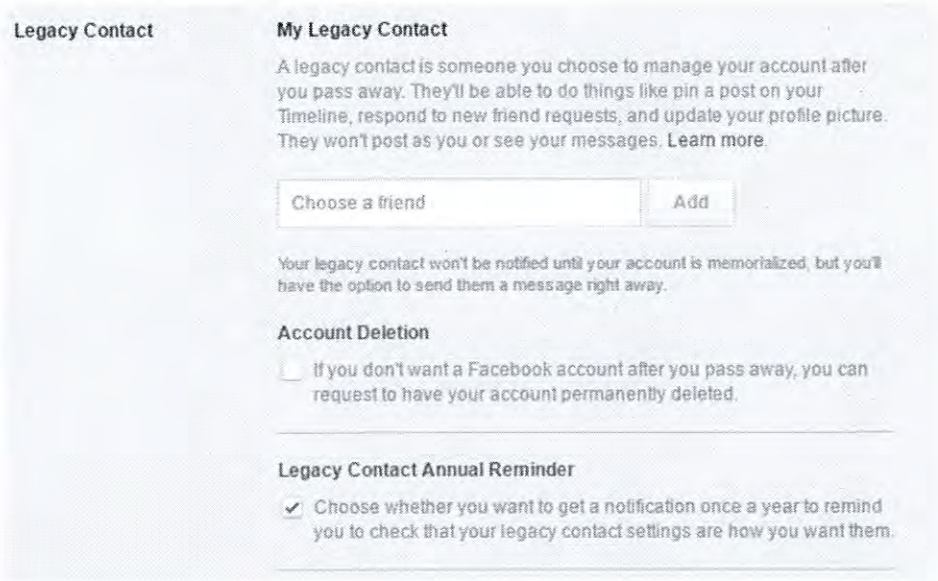


ประวัติการล็อกอินเหล่านี้คือการล็อกอินที่เราทำค้างเอาไว้ แนะนำให้กดปุ่ม End Activity เพื่อล็อกเอาท์ออกจากระบบให้หมด (กด End All Activity) หรือจะเหลือไว้เฉพาะอันใหม่ล่าสุดก็ได้ เพื่อความปลอดภัยที่ดีของบัญชีเราเอง

6. Legacy Contact ถ้าหากเป็นอะไรขึ้นมา ฝากบัญชีไว้ที่ใคร

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

คนที่ดูแลบัญชีจะทำได้เฉพาะบางอย่างเท่านั้น เช่น ปักหมุดโพสต์ กดรับคำขอเป็นเพื่อน หรือเปลี่ยนภาพประจำตัว แต่ไม่สามารถล็อกอิน และโพสต์หรือแชทแทนเจ้าของบัญชีได้ และในกรณีที่เราไม่อยากให้ใครดูแลบัญชีแทน 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 ในแอพ Facebook บนมือถือ

o เพิ่มชื่อ Trust Contacts เผื่อไว้ สำหรับโอกาสที่ล็อกอินเข้าบัญชีตัวเองไม่ได้

o ตรวจสอบสิทธิการเข้าถึงบัญชีในหน้า Your Browsers and Apps และลบการขอสิทธิเก่าๆ ที่ไม่ต้องใช้แล้ว

o ตรวจสอบประวัติการล็อกอินในหน้า Where You're Logged In และล็อกเอาท์การล็อกอินเก่าๆ ที่ค้างเอาไว้และไม่ต้องใช้แล้ว

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

การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

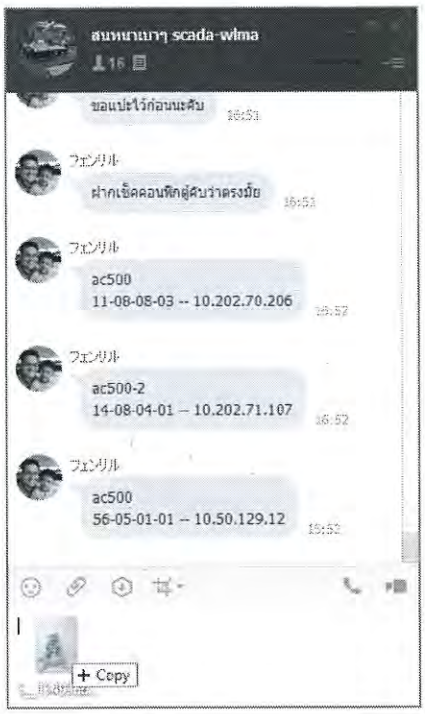
One Point Lesson: OPL

ชื่อเรื่อง	การโพสต์รูปบน Line (PC)		ลำดับ	9
			วันที่เขียน	4 พ.ค. 2560
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		สมโภช เกียรติกสิกร		
		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)..... (นางพิศวาท ภาพสุวรรณ) ตำแหน่ง ผอ.ฝชท.
องค์ความรู้เรื่อง ข้อปฏิบัติในการใช้รหัสผ่าน (Active Directory : AD)	23/05/60 รหัส OPK

ข้อปฏิบัติในการใช้รหัสผ่าน (Active Directory : AD)

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

บทนำ

เพื่อให้มีการควบคุมการพัฒนาระบบสารสนเทศ การเปลี่ยนแปลงแก้ไขการปฏิบัติงานในศูนย์คอมพิวเตอร์ การเข้าถึงอุปกรณ์อมพิวเตอร์ การเข้าถึงอุปกรณ์คอมพิวเตอร์ การเข้าถึงระบบงาน การเข้าถึงข้อมูลและทรัพยากรสารสนเทศ การจัดเก็บข้อมูล การกำหนดมาตรฐานของเอกสารระบบสารสนเทศ ลดความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ และการวางแผนการแก้ไขความเสียหายจากเหตุฉุกเฉิน จึงจำเป็นต้องมีแนวทางปฏิบัติที่สามารถปกป้องข้อมูลสำคัญมิให้สูญเสีย เพื่อปกป้องความเสียหายที่จะเกิดขึ้นกับองค์กร และลดความเสี่ยงจากการใช้งานระบบสารสนเทศ

ข้อปฏิบัติในการใช้รหัสผ่าน

1. รหัสผ่าน ควรมีความยาวของตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร
2. ผู้ปฏิบัติงานที่ได้รับอนุญาตและได้รับสิทธิในการใช้ระบบงานสารสนเทศและระบบข้อมูลที่เกี่ยวข้อง เมื่อได้รับจัดสรรรหัสผ่านแล้ว จะต้องเปลี่ยนรหัสผ่านเป็นของตัวเองที่เหมาะสมและเป็นความลับเฉพาะตัวชุดใหม่ทันที
3. ผู้ปฏิบัติงานต้องเปลี่ยนรหัสผ่านใหม่ทุกๆ ๙๐ วัน หรือตามระยะเวลาที่ระบบงานกำหนด
4. การเปลี่ยนแปลงรหัสผ่านใหม่ในแต่ละครั้ง จะต้องไม่นำรหัสผ่านที่หมดอายุแล้วมาใช้ซ้ำอีก
5. ผู้ปฏิบัติงานจะต้องล็อคหน้าจอทุกครั้งเมื่อไม่ได้ปฏิบัติงานอยู่ที่เครื่องคอมพิวเตอร์ และต้องพิสูจน์ตัวตนก่อนใช้งานทุกครั้ง
6. ผู้ปฏิบัติงานทุกคนต้องรับผิดชอบในการเลือก และ/หรือเปลี่ยนแปลงรหัสผ่านที่เหมาะสมและปลอดภัย รวมทั้งปกปิดและรักษารหัสผ่านของตนอย่างดีที่สุดโดยห้ามจดบันทึกรหัสผ่านในที่ที่สามารถพบเห็นได้โดยง่าย
7. ห้ามเปิดเผยรหัสผ่านให้บุคคลอื่นรับรู้ หากรหัสผ่านถูกเปิดเผยต้องเปลี่ยนใหม่โดยเร็ว

8. ห้ามนำหรือเปิดเผยรหัสผ่านให้แก่บุคคลอื่นที่ไม่ได้รับอนุญาตหรือที่มิได้เกี่ยวข้องแสดงตนเข้าไปใช้ระบบงานสารสนเทศและระบบข้อมูล หากตรวจสอบพบว่ามีการเปิดเผยหรือนำรหัสผ่านให้แก่บุคคลอื่นที่ไม่ได้รับอนุญาต กระทำการที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศ และการรักษาความปลอดภัยระบบข้อมูล ผู้ปฏิบัติงานที่ได้รับอนุญาตและสิทธิให้ใช้ระบบงานสารสนเทศนั้น จะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
9. หากผู้ปฏิบัติงานพบเห็นหรือสงสัยถึงการล่วงละเมิดต่อความปลอดภัยในการใช้งานหรือประเด็นอื่นใดที่เกิดขึ้น เนื่องจากรหัสผ่านถูกนำไปใช้โดยผู้ที่ไม่ใช่เจ้าของ จะต้องรายงานการใช้ต่อผู้บังคับบัญชาหรือหน่วยงานที่ดูแลระบบสารสนเทศหรือผู้ดูแลระบบงานทันที เพื่อทำการตรวจสอบและแก้ไขต่อไป

การลงโทษทางวินัย ไม่เป็นเหตุให้ผู้กระทำหลุดพ้นจากความผิดทางอาญา หรือความรับผิดทางแพ่ง หรือความรับผิดตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

การประปานครหลวง

One Point Article: OPA

ชื่อเรื่อง	เทคนิคการตั้ง password สิ่งสำคัญที่ไม่ควรมองข้าม		ลำดับ	11
			วันที่เขียน	5 พ.ค. 2560
หน่วยงาน	สายงานเทคโนโลยีสารสนเทศ	ผู้เขียน	ผู้ตรวจสอบ	ผู้อนุมัติ
		ธนานนท์ โดมทอง		
		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 การขโมยpassword ของ email, line หรือ facebookและปลอมตัวเป็นเจ้าของเพื่อใช้การขอยืมเงินจากเพื่อนของเจ้าของ 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 ทำให้ผู้ใช้งานบางส่วนใช้รหัสผ่านเป็นรหัสเดียวกันกับรหัสผ่าน 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 นักกีฬาหรือบุคคลที่นับถือ เพราะหาข้อมูลได้ง่ายๆ เช่น Facebook

5. ตั้ง password ด้วยตัวอักษรที่เรียงบน key board

เช่น asdfgh , qwerty หรือ zxcvbรวมถึงตัวเลข 123456789 , 1111111

6. จดรหัสผ่านไว้ใกล้ๆเครื่องคอมพิวเตอร์

ไม่ควรจดรหัสผ่านลงในกระดาษ หรือจดไว้ในสมุด ที่วางอยู่บริเวณใกล้ๆกับเครื่องคอมพิวเตอร์ของคุณ

<u>การตั้ง password ที่ดี</u>

1. เปลี่ยนรหัสผ่านทุกๆ 3 เดือน

เพื่อลดโอกาสการถูกแกะรหัสผ่าน

2. ความยาวเกิน 8 ตัวอักษร

Website ในทุกวันนี้นั้นส่วนใหญ่มักจะบังคับให้ตั้งรหัสผ่าน 8 ตัวอักษรเป็นขั้นต่ำอยู่แล้ว เพราะยิ่งรหัสผ่านของเรามีความยาวมากขึ้น การเดารหัสผ่านก็จะต้องใช้เวลามากขึ้นด้วย นอกจากนั้นถ้า password ประกอบด้วยอักษรตัวใหญ่ และตัวเล็ก ตลอดจนตัวเลข และสัญลักษณ์ ยิ่งผสมกันได้มากเท่าไร จะยิ่งปลอดภัยเท่านั้น

3. พิมพ์รหัสผ่านภาษาอังกฤษด้วยkeyboard ภาษาไทย

เป็นเทคนิคในการตั้ง password ที่จำง่าย และคาดเดาได้ยาก วิธีการคือให้ทดลองพิมพ์รหัสผ่านภาษาไทย แต่ใช้แป้นพิมพ์เป็นภาษาอังกฤษ ยกตัวอย่างเช่น จะตั้งรหัสผ่านว่า “ข้าวหน้าเป็ด” เมื่อเราพิมพ์ด้วยแป้นพิมพ์ภาษาอังกฤษก็จะได้รหัสผ่านเป็น “-hk;sohkgxHf” ซึ่งจะได้ทั้งตัวอักษรตัวใหญ่ และตัวอักขระพิเศษ อีกทั้งยังง่ายต่อการจดจำอีกด้วย

กลุ่ม ปิ่นโตความรู้

KM 2560

ภาคผนวก

เอกสารแนบ 2

แผนปฏิบัติงาน ประจำปีงบประมาณ 2560
หัวข้อ รู้ทัน Social เปรี้ยวกว่าใคร
กิจกรรม SGA ปิ่นโตความรู้ สายงานเทคโนโลยีสารสนเทศ

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 ในสายงาน							■				-	-	-	
2.ประชุมกลุ่ม เพื่อศึกษา วิเคราะห์ รวบรวม และเก็บข้อมูล								■■			-	-	-	
3.เรียบเรียง องค์ความรู้ พิจารณาการใช้สื่อในการเผยแพร่องค์ความรู้								■■	■■		-	-	-	
4.นำเสนอผลงานในสายงาน									■		-	-	-	
5.ปรับปรุงองค์ความรู้พร้อมจัดทำรายงานส่งคณะทำงานย่อยฯ									■		-	-	-	
6.จัดเตรียมการนำเสนอผลงานในงานสัปดาห์วิชาการ										■■	-	-	-	
6.นำเสนอผลงานในงานสัปดาห์วิชาการ											■	-	-	
											รวมเป็นเงิน			5,000

ลงชื่อ ..... หัวหน้าSGA

(นางนงนุช วงศ์กาฬสินธุ์)

ผู้อำนวยการกองวิชาการเทคโนโลยี

ฝ่ายยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ

วันที่ 31 / 03 / 2560