

แบบฟอร์มการถ่ายทอดประสบการณ์
ผ่านบทเรียน 1 ประเด็น (One Point Lesson)

คือบทเรียนที่อธิบายวิธีการทำงาน การใช้เครื่องมือ หรืออื่นๆ โดยมุ่งเน้นการเขียนเพียงประเด็นเดียว เพื่อให้มี
 ความคล่องตัวในการศึกษาและนำไปใช้

การแบ่งปันความรู้ 1 บทเรียน : 1 องค์ความรู้ Knowledge Sharing by One Point Lesson (OPL)			
ชื่อเรื่อง	การสร้างความปลอดภัยทางไซเบอร์เบื้องต้น	เลขที่เอกสาร	-
		วันที่จัดทำ	17 กันยายน 2568
ประเภท	☒ ความรู้พื้นฐาน ☐ การพัฒนาปรับปรุง	ผู้จัดทำ	นายฐภณ ไกรเลิศมงคล
	☐ กระบวนการทำงาน ☒ เทคนิคการทำงาน	ตำแหน่ง	พนักงาน (ระดับ 3)
		ผู้อนุมัติ	
		ตำแหน่ง	
บทเรียนที่ได้จากการปฏิบัติงาน 1. รู้จักภัยคุกคามไซเบอร์แต่ละประเภท 2. ต้องไม่ประมาท – แกดดลิงก์มั่ว ๆ หรือบอกรหัส OTP ก็ฟังทั้งบัญชีได้ 3. ป้องกันดีกว่า – ตั้งรหัสผ่านโหด ๆ + ใช้ 2FA ลดโอกาสโดนเจาะ 4. สถิติสำคัญที่สุด – ไม่ว่าจะ เป็น SMS, อีเมล, โทรศัพท์ที่น่าสงสัย ต้องเช็กก่อนเชื่อ 5. ข้อมูลส่วนตัวคือทรัพย์สิน – ยิ่งเก็บดีเท่าไร ยิ่งปลอดภัย			
ผลลัพธ์ที่ได้จากการปฏิบัติงาน 1. ลดความเสี่ยงในการถูกหลอกลวง (phishing, SMS ปลอม, Website ปลอม ,โทรมาหลอก OTP) 2. ปกป้องข้อมูลส่วนตัว 3. มีภูมิคุ้มกันทางไซเบอร์มากขึ้น			

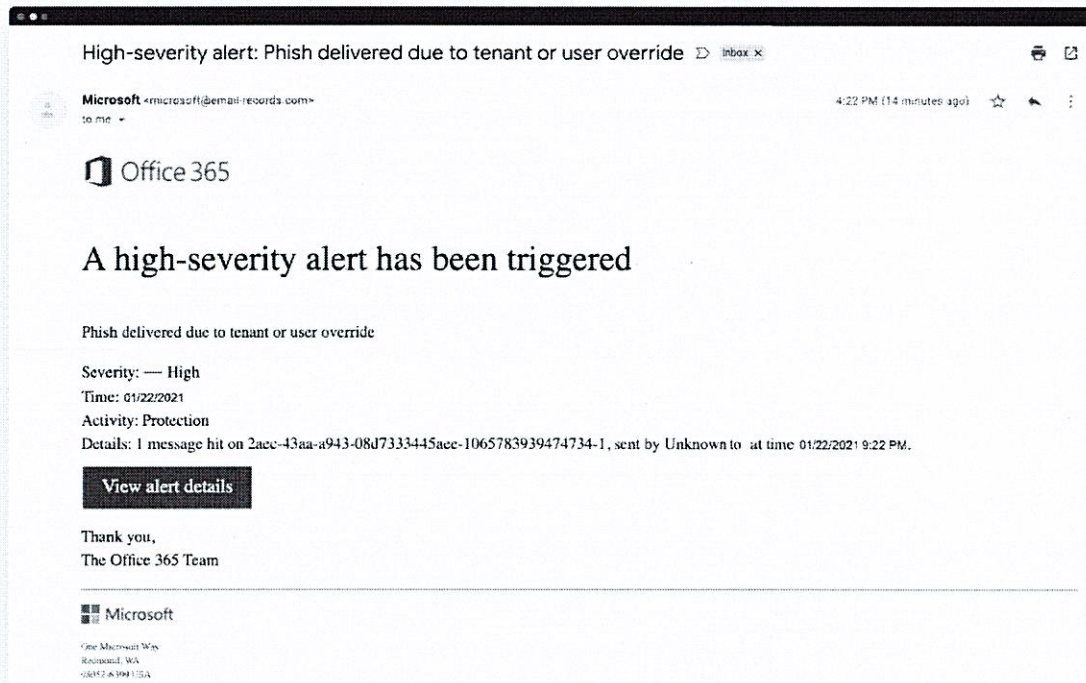
การสร้างความปลอดภัยทางไซเบอร์เบื้องต้น

1. ระวัง Email และข้อความ Phishing (ฟิชชิ่ง) คือกลโกงที่พยายามหลอกให้ผู้ใช้เปิดเผยข้อมูลส่วนตัวหรือคลิกลิงก์อันตราย อย่าเชื่อข้อความที่ขอข้อมูลส่วนตัวหรือเร่งให้คลิกลิงก์

ตัวอย่างข้อความฟิชชิ่ง: "ธนาคารแจ้งว่าบัญชีของคุณถูกระงับ กรุณาคลิกเพื่อยืนยันตัวตน"

"คุณได้รับรางวัลล้านบาท! คลิกรับเงินทันที"

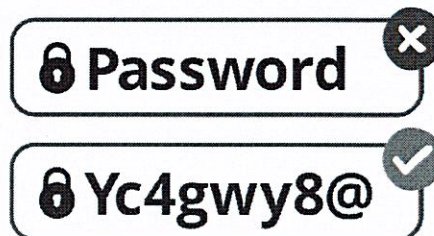
วิธีตรวจสอบ: "ติดต่อธนาคารโดยตรงผ่านหมายเลขที่ทราบแน่ชัด หรือเข้าเว็บไซต์จากการพิมพ์ URL เอง"



2. รหัสผ่านต้องปลอดภัย

- ใช้รหัสผ่านที่เดายาก (ผสมตัวเลข ตัวอักษร พิเศษ)
- อย่าใช้รหัสซ้ำหลายที่
- เปิด 2FA (Two-Factor Authentication) ไว้ถ้าเปิดได้

เช่น รหัสผ่านที่แย่ 123456789 รหัสผ่านที่ดี Pu@sy!#78248#



3.ตรวจสอบ URL ก่อนใส่ข้อมูลสำคัญ การตรวจสอบที่อยู่เว็บไซต์ (URL) ก่อนที่จะกรอกข้อมูลสำคัญ เพื่อให้แน่ใจว่าเป็นเว็บไซต์ของจริงและไม่ใช่วีปไซด์ปลอมที่สร้างขึ้นมาเพื่อหลอกลวง

- ดูให้ดีว่าเว็บไซต์เป็นของจริงหรือไม่
- ตัวอย่าง URL:  เว็บจริง: <https://www.scb.co.th>
-  เว็บปลอม: <https://scb-online.net> หรือ <https://www.scb.co.th.fake.com>
- วิธีตรวจสอบ: "ดูไอคอน  หน้า URL, สะกดชื่อเว็บไซต์ให้ถูก,

รู้กันมีจาชีฟ! ระวังเกิดเว็บไซต์ปลอม



ระวัง เว็บไซต์ธนาคารกรุงเก่าปลอม

- URL มีการสะกดที่แปลก ผิดปกติ เช่น BangkOkbank.com หรือ globangkokbank.net
- เนื้อหาข้อมูลน้อยผิดปกติ
- การใช้ภาษาและไวยากรณ์ที่แปลก หรือผิด ทั้งภาษาไทยและอังกฤษ

ปัจจุบันที่อยู่เว็บไซต์ของธนาคารมี 4 URL ดังนี้คือ

www.bangkokbank.com	www.bangkokbank.co.th
www.bangkokbank.net	www.bbl.co.th

ทั้งนี้หากไปแม่ใจ หรือพบปัญหาเกี่ยวกับการรักษาความปลอดภัยในการใช้เว็บไซต์ของธนาคาร โปรดติดต่อ บัฟหลวงโฟน โทร. 1333

4. ระวังการแชร์ข้อมูลบน Social Media การเปิดเผยข้อมูลส่วนตัวมากเกินไปบนโซเชียลมีเดียอาจนำไปสู่การถูกใช้ประโยชน์หรือทำร้ายได้

- อย่าเปิดเผยข้อมูลที่สามารถนำไปใช้ทำร้ายได้ : Location
- ตัวอย่างที่ควรหลีกเลี่ยง: "รูปบัตรประชาชน, ป้ายทะเบียนรถ, ticket เครื่องบิน"
- สิ่งที่ต้องทำ: "ปิดการค้นหายกจากเบอร์โทร, ตั้งโพสต์เป็น Friends Only"

SOCIAL MEDIA

กับภัยคุกคามใกล้ตัวเรา



1. ความเสี่ยงจากการแฮกบัญชี



2. การแพร่กระจายข้อมูลปลอม



3. ภัยจากการแชร์ข้อมูลส่วนตัว



4. บุคคลที่อาจไม่ใช่เพื่อน



5. โฆษณาที่ก่อความรำคาญ