รายละเอียดผลการดำเนินงาน
ตามแผนปฏิบัติการจัดการความรู้ของศูนย์คอมพิวเตอร์ ประจำปีงบประมาณ พ.ศ. 2569
เรื่อง "การสร้างความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity 101)
แก่ผู้ใช้งานทั่วไปภายในมหาวิทยาลัย"
****

กำหนดแผนการดำเนินงาน/กิจกรรม เป็นรายไตรมาส และเป้าหมายการดำเนินงาน โดยมีรายละเอียดดังนี้

แผนการดำเนินงาน/กิจกรรม	ไตรมาสที่ 1			ไตรมาสที่ 2			ไตรมาสที่ 3			ไตรมาสที่ 4		
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
ประชุมคณะทำงานการจัดการความรู้ของหน่วยงาน												
หาแนวทางการศึกษาข้อมูลความรู้ ความหมาย ศัพท์ที่เกี่ยวข้อง, ปัญหาที่พบ, การป้องกัน												
สรุปชุดองค์ความรู้ด้าน Cybersecurity 101 ที่เหมาะสมกับมหาวิทยาลัย												
จัดทำสื่อ และเผยแพร่ความรู้/สื่อประชาสัมพันธ์ ด้าน Cybersecurity												
จัดหาช่องทางส่งบุคลากรของหน่วยงานเข้าร่วมอบรมภายนอก												
จัดหาวิทยากรผู้เชี่ยวชาญ ด้าน Cybersecurity 101												
เชิญวิทยาการเข้าร่วมกิจกรรมแลกเปลี่ยนเรียนรู้												
จัดกิจกรรมแลกเปลี่ยนเรียนรู้และถ่ายทอดความรู้												
รวบรวมชุดองค์ความรู้และเผยแพร่บนเว็บไซต์หน่วยงานและช่องทางต่างๆ ของมหาวิทยาลัย												
ทดสอบการหลอกลวง ผู้เข้าร่วมกิจกรรม (Phishing Attack)												
สรุปรวบรวมข้อมูลและรายงานผลการจัดการความรู้ประจำไตรมาส												

ไตรมาสที่ 1

1) **ระบุความรู้พื้นฐานที่จำเป็น ชุดที่ 1**

1. ความหมายและคำจำกัดความที่เกี่ยวข้อง

การรู้จักคำศัพท์พื้นฐานทางด้านความปลอดภัยไซเบอร์ช่วยให้ผู้ใช้งานเข้าใจภัยคุกคามและแนวทางการป้องกันได้ถูกต้อง

- **มัลแวร์ (Malware)**

ย่อมาจาก "Malicious Software" หมายถึง ซอฟต์แวร์ที่ถูกออกแบบมาเพื่อสร้างความเสียหายหรือรบกวนการทำงานของระบบคอมพิวเตอร์ เช่น ไวรัส (Virus), เวิร์ม (Worm), โทรจัน (Trojan) และสปายแวร์ (Spyware)

- **โทรจัน (Trojan Horse)**

ซอฟต์แวร์อันตรายที่แฝงตัวมากับโปรแกรมหรือไฟล์ที่ดูเหมือนปลอดภัย เมื่อเปิดใช้งานจะเปิดช่องทางให้ผู้ไม่หวังดีเข้าควบคุมเครื่องคอมพิวเตอร์หรือขโมยข้อมูลได้

- **แรนซัมแวร์ (Ransomware)**

มัลแวร์ที่เข้ารหัสไฟล์ขององค์กรและ เรียกค่าไถ่เพื่อปลดล็อกข้อมูล

- **การปลอมตัวเป็นหน่วยงาน IT**

การที่ผู้ไม่ประสงค์ดีแอบอ้างว่าเป็นเจ้าหน้าที่ของหน่วยงานด้าน IT เพื่อหลอกลวงให้เหยื่อ เชื่อถือ และปฏิบัติตามคำสั่งบางอย่าง ซึ่งมักนำไปสู่การเข้าถึงระบบ โดยไม่ได้รับอนุญาต หรือการทำให้เกิดความเสียหายด้านความปลอดภัยไซเบอร์

- **ฟิชชิ่ง (Phishing)**

การหลอกลวงให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่าน เลขบัตรเครดิต หรือข้อมูลบัญชี ผ่านอีเมล เว็บไซต์ หรือข้อความที่ปลอมแปลงให้เหมือนของจริงจากองค์กรที่น่าเชื่อถือ

2. การระวังอีเมลหลอกลวง (Phishing)

ฟิชชิ่งเป็นภัยไซเบอร์ที่พบบ่อยที่สุดในมหาวิทยาลัย โดยเฉพาะอีเมลที่แอบอ้างเป็นผู้บริหารหรือหน่วยงานศูนย์คอมพิวเตอร์

แนวทางป้องกัน:

- ตรวจสอบที่อยู่อีเมลผู้ส่ง ว่าสอดคล้องกับหน่วยงานจริงหรือไม่ โดยจัดทำวิธีการตรวจสอบ
- หลีกเลี่ยงการคลิกลิงก์หรือดาวน์โหลดไฟล์แนบจากอีเมลที่ไม่รู้จัก
- หากมีความสงสัย ให้ติดต่อเจ้าหน้าที่ศูนย์คอมพิวเตอร์โดยตรงก่อนดำเนินการใด ๆ
- เปิดใช้ระบบกรองอีเมลขยะ (Spam Filter) และตั้งค่าความปลอดภัยในโปรแกรมอีเมล

3. การตั้งรหัสผ่านอย่างปลอดภัย

รหัสผ่านเป็นกุญแจสำคัญในการป้องกันบัญชีผู้ใช้งานไม่ให้ถูกเข้าถึงโดยไม่ได้รับอนุญาต

แนวทางที่แนะนำ:

- ใช้รหัสผ่านที่มีความยาว อย่างน้อย 12 ตัวอักษร
- ประกอบด้วย ตัวอักษรใหญ่–เล็ก ตัวเลข และอักขระพิเศษ
- หลีกเลี่ยงการใช้ข้อมูลส่วนตัว เช่น วันเกิด ชื่อเล่น หมายเลขโทรศัพท์
- ไม่ใช้รหัสผ่านเดียวกันในทุกระบบ
- เปิดใช้งานระบบยืนยันตัวตนแบบสองชั้น (Two-Factor Authentication: 2FA)

4. การใช้งานอินเทอร์เน็ตอย่างปลอดภัย

การใช้อินเทอร์เน็ตในชีวิตประจำวันอาจเสี่ยงต่อการถูกโจมตีทางไซเบอร์ หากไม่ระมัดระวัง

แนวทางการใช้งานอย่างปลอดภัย:

- หลีกเลี่ยงการเชื่อมต่อ Wi-Fi สาธารณะในการทำธุรกรรมสำคัญ
- เข้าเว็บไซต์ที่มีการเข้ารหัสข้อมูล (ขึ้นต้นด้วย https://)
- อัปเดตซอฟต์แวร์ ระบบปฏิบัติการ และแอนติไวรัสอย่างสม่ำเสมอ
- ตรวจสอบสิทธิ์การเข้าถึงของแอปพลิเคชันก่อนอนุญาต

5. การป้องกันข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลเป็นเป้าหมายหลักของผู้ไม่หวังดี เช่น ข้อมูลบัญชีผู้ใช้ หมายเลขบัตรประชาชน หรือข้อมูลทางการเงิน

แนวทางปฏิบัติ:

- เก็บรักษาข้อมูลส่วนตัวอย่างปลอดภัย ไม่เผยแพร่ในสื่อสาธารณะ
- ใช้รหัสผ่านหรือการเข้ารหัสป้องกันไฟล์สำคัญ
- ไม่กรอกข้อมูลส่วนตัวในเว็บไซต์ที่ไม่น่าเชื่อถือ
- ระมัดระวังการแชร์ข้อมูลในโซเชียลมีเดีย
- ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของมหาวิทยาลัย

2) **จัดทำแผ่นภาพสำหรับประชาสัมพันธ์ตามข้อมูลความรู้ที่กำหนด ชุดที่ 1**

ไตรมาสที่ 2

1) **ระบุความรู้พื้นฐานที่จำเป็น ชุดที่ 2 เรื่อง ภัยคุกคามจาก Phishing Mail และ Phishing Attack**

หลักการและความสำคัญ

ปัจจุบันการใช้งานระบบสารสนเทศและอีเมลภายในองค์กรมีความสำคัญอย่างยิ่งต่อการดำเนินงาน แต่ในขณะเดียวกันก็เป็นช่องทางที่ผู้ไม่หวังดีใช้ในการโจมตีทางไซเบอร์ โดยเฉพาะ Phishing ซึ่งเป็นรูปแบบการหลอกลวงเพื่อขโมยข้อมูลสำคัญ เช่น ชื่อผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน

ความหมายของ Phishing

Phishing Mail คือ อีเมลปลอมที่ถูกสร้างขึ้นให้มีลักษณะคล้ายคลึงกับอีเมลจากหน่วยงานที่น่าเชื่อถือ เช่น หน่วยงานภายในองค์กร ธนาคาร หรือผู้ให้บริการระบบ เพื่อหลอกให้ผู้รับเปิดลิงก์ ดาวน์โหลดไฟล์ หรือกรอกข้อมูลส่วนตัว รหัสผ่าน

Phishing Attack คือ การโจมตีทางไซเบอร์ในภาพรวมที่ใช้เทคนิคหลอกลวง (Social Engineering) ผ่านช่องทางต่าง ๆ เช่น อีเมล เว็บไซต์ หรือข้อความ เพื่อให้เหยื่อเปิดเผยข้อมูลสำคัญ หรือดำเนินการบางอย่างตามที่ผู้โจมตีต้องการ

ลักษณะของ Phishing Mail ที่ควรระวัง

- ใช้ชื่อผู้ส่งหรือโดเมนที่คล้ายของจริง แต่มีการสะกดผิดเล็กน้อย
- มีข้อความเร่งด่วน เช่น “ต้องดำเนินการทันที” หรือ “บัญชีจะถูกระงับ”
- มีลิงก์ให้คลิกเพื่อนำไปสู่เว็บไซต์ปลอม
- แนบไฟล์ที่อาจเป็นอันตราย เช่น .exe, .zip หรือเอกสารที่มี Macro
- ใช้ภาษาผิดปกติ หรือรูปแบบไม่เป็นทางการ
- ขอข้อมูลสำคัญ เช่น รหัสผ่าน หรือ OTP

รูปแบบของ Phishing Attack ที่พบบ่อย

- **Email Phishing**: หลอกผ่านอีเมล
- **Spear Phishing**: เจาะจงบุคคลหรือหน่วยงาน
- **Whaling**: มุ่งเป้าผู้บริหารระดับสูง
- **Smishing**: หลอกผ่าน SMS
- **Vishing**: หลอกผ่านการโทรศัพท์

ผลกระทบจาก Phishing

- ข้อมูลบัญชีผู้ใช้งานถูกขโมย
- ระบบสารสนเทศขององค์กรถูกเข้าถึงโดยไม่ได้รับอนุญาต
- เกิดความเสียหายทางการเงิน
- ข้อมูลสำคัญขององค์กรรั่วไหล
- ส่งผลกระทบต่อภาพลักษณ์และความน่าเชื่อถือขององค์กร

แนวทางการป้องกันและรับมือ

- **สำหรับผู้ใช้งาน**

- ตรวจสอบอีเมลผู้ส่งและ URL อย่างละเอียดก่อนคลิก
- หลีกเลี่ยงการคลิกลิงก์หรือดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ
- ไม่กรอกข้อมูลส่วนตัวผ่านลิงก์ในอีเมล
- ใช้รหัสผ่านที่รัดกุม และเปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (MFA)
- รายงานอีเมลต้องสงสัยให้หน่วยงานที่เกี่ยวข้องทันที

- **สำหรับองค์กร**

- จัดอบรมและสร้างความตระหนักรู้ด้าน Cybersecurity อย่างสม่ำเสมอ
- ติดตั้งระบบกรองอีเมล (Email Security Gateway)
- ใช้นโยบายด้านความปลอดภัยของข้อมูล (Information Security Policy)
- จัดทำแนวปฏิบัติ (SOP) สำหรับการรับมือเหตุการณ์
- ทดสอบการโจมตีจำลอง (Phishing Simulation) เพื่อประเมินความเสี่ยง

แนวทางการดำเนินการเมื่อพบ Phishing

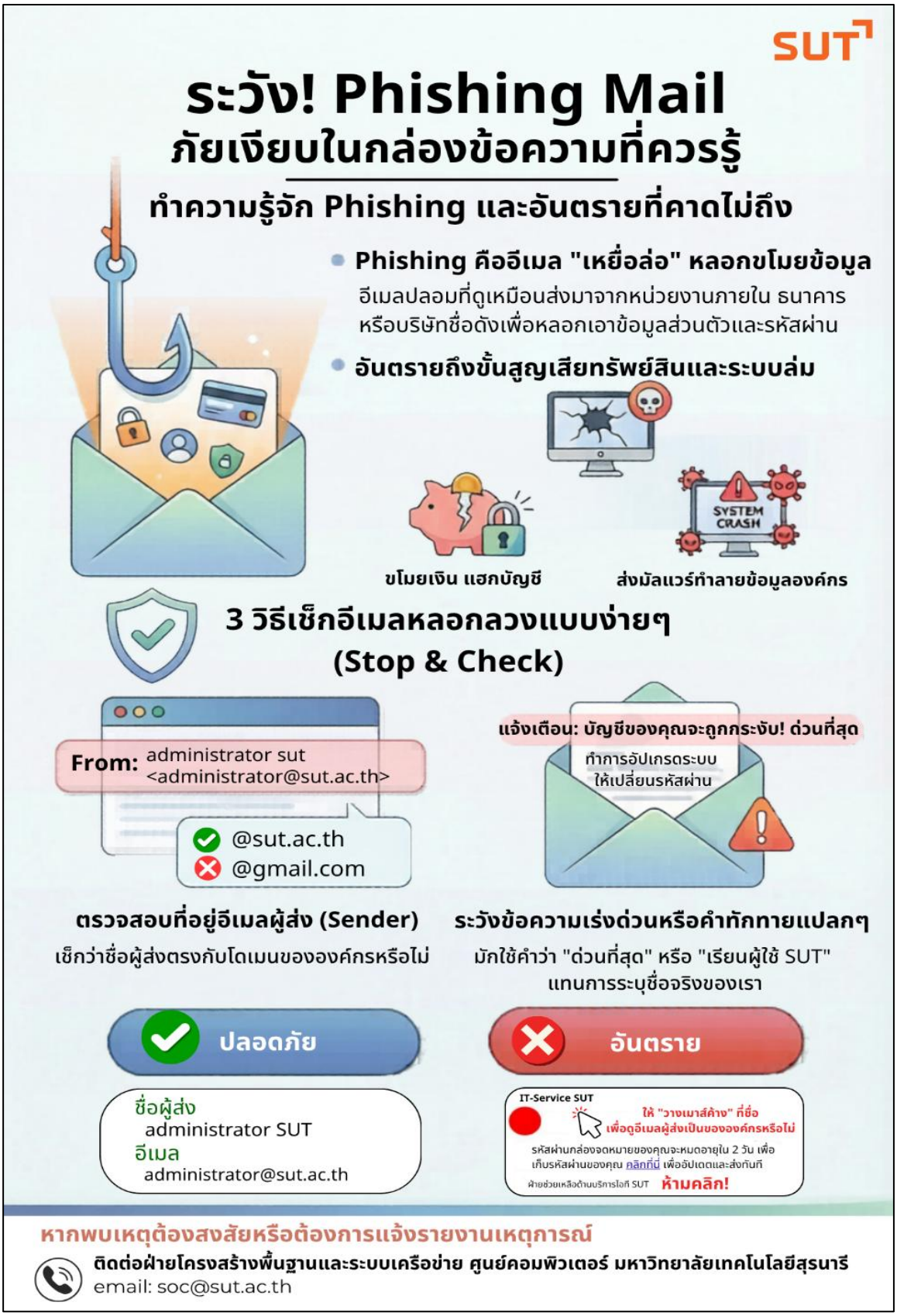
- ห้ามคลิกลิงก์หรือเปิดไฟล์แนบ
- แจ้งหน่วยงานด้าน IT ภายในองค์กรหรือผู้ดูแลระบบทันที
- ลบอีเมลออกจากระบบ
- หากเผลอกรอกข้อมูล ให้รีบเปลี่ยนรหัสผ่านและแจ้งหน่วยงานด้าน IT ภายในองค์กรหรือผู้ดูแลระบบ

สรุป

Phishing เป็นภัยคุกคามที่อาศัยความผิดพลาดของผู้ใช้งานเป็นหลัก การสร้างความรู้ ความเข้าใจ และการมีระบบป้องกันที่เหมาะสม จะช่วยลดความเสี่ยงและป้องกันความเสียหายที่อาจเกิดขึ้นกับองค์กรได้อย่างมีประสิทธิภาพ

2) **จัดทำแผ่นภาพสำหรับประชาสัมพันธ์ตามข้อมูลความรู้ที่กำหนด ชุดที่ 2**

- จัดทำแผ่นภาพสำหรับประชาสัมพันธ์การเผยแพร่ความรู้/สื่อประชาสัมพันธ์ด้าน Cybersecurity 101 แก่บุคลากรภายในมหาวิทยาลัย ครั้งที่ 2
- จัดทำคลิปวีดีโอตัวอย่างการตรวจสอบ https://go.sut.ac.th/e4fnid เรื่อง ระวัง Phishing Mail ภัยเงียบในกล่องข้อความที่ควรรู้



ไตรมาสที่ 3

1) **ระบุความรู้พื้นฐานที่จำเป็น ชุดที่ 3 การสร้างความตระหนักรู้ด้านการจัดการรหัสผ่านอย่างปลอดภัย**

1. ความสำคัญของรหัสผ่าน

รหัสผ่าน (Password) เปรียบเสมือนปราการด่านแรกในการปกป้องข้อมูลส่วนบุคคลและสินทรัพย์สารสนเทศของมหาวิทยาลัย ปัจจุบันผู้ใช้งานภายในมหาวิทยาลัย (นักศึกษา อาจารย์ และบุคลากร) ต้องเข้าถึงระบบสารสนเทศที่หลากหลาย เช่น ระบบลงทะเบียน ระบบการเรียนการสอนออนไลน์ และระบบบริหารจัดการภายใน

อย่างไรก็ตาม จากสถิติภัยคุกคามทางไซเบอร์พบว่า การโจมตีส่วนใหญ่สำเร็จเนื่องจากการใช้รหัสผ่านที่คาดเดาง่าย (Weak Password) หรือการใช้รหัสผ่านซ้ำกันในหลายระบบ ส่งผลให้เกิดความเสี่ยงต่อการถูกโจมตีแบบสุ่มรหัสผ่าน หรือการรั่วไหลของข้อมูล ดังนั้น การสร้างความตระหนักรู้และให้แนวปฏิบัติที่ถูกต้อง ในการตั้งและการบริหารจัดการรหัสผ่าน จึงเป็นสิ่งจำเป็นเร่งด่วนเพื่อยกระดับความปลอดภัยทางไซเบอร์ในภาพรวมของมหาวิทยาลัย

2. ความเสี่ยงจากการใช้รหัสผ่านที่ไม่ปลอดภัย ตัวอย่างความเสี่ยงที่เกิดขึ้นจากการใช้รหัสผ่านที่อ่อนแอ ได้แก่

- การคาดเดารหัสผ่านได้ง่าย
- การโจมตีแบบ Brute Force Attack
- การนำข้อมูลบัญชีผู้ใช้ที่รั่วไหลไปทดลองใช้กับระบบอื่น
- การเข้าถึงอีเมลหรือระบบงานโดยไม่ได้รับอนุญาต
- การรั่วไหลของข้อมูลสำคัญของหน่วยงาน

3. หลักการสร้างรหัสผ่านที่ปลอดภัย รหัสผ่านที่ดีควรมีลักษณะดังนี้

- มีความยาวอย่างน้อย 12 ตัวอักษรขึ้นไป
- ประกอบด้วยตัวอักษรพิมพ์ใหญ่และพิมพ์เล็ก
- มีตัวเลขและอักขระพิเศษ
- หลีกเลี่ยงการใช้ข้อมูลส่วนตัว
- หลีกเลี่ยงคำศัพท์ทั่วไปที่คาดเดาได้ง่าย

4. แนวปฏิบัติที่ดีในการจัดการรหัสผ่าน

- ใช้รหัสผ่านที่แตกต่างกันในแต่ละระบบ เพื่อลดความเสี่ยงกรณีบัญชีใดบัญชีหนึ่งถูกโจมตี
- ไม่เปิดเผยรหัสผ่านแก่ผู้อื่น รวมถึงไม่ส่งรหัสผ่านผ่านอีเมล โปรแกรมสนทนา หรือช่องทางสื่อสารอื่น
- เปลี่ยนรหัสผ่านเมื่อพบเหตุผิดปกติ เช่น สงสัยว่าข้อมูลรั่วไหล หรือพบการเข้าสู่ระบบที่ไม่รู้จัก
- ใช้ Password Manager เพื่อช่วยจัดเก็บและสร้างรหัสผ่านที่มีความซับซ้อนอย่างปลอดภัย

5. การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) MFA เป็นมาตรการเพิ่มความปลอดภัยโดยกำหนดให้ผู้ใช้งานยืนยันตัวตนมากกว่าหนึ่งวิธี และช่วยลดความเสี่ยงแม้ว่ารหัสผ่านจะถูกเปิดเผยหรือรั่วไหล เช่น

- รหัสผ่าน
- รหัส OTP
- แอปพลิเคชันยืนยันตัวตน
- ลายนิ้วมือหรือ Face ID

6. สิ่งที่ไม่ควรปฏิบัติ

- ใช้รหัสผ่านง่าย ๆ เช่น 123456 หรือ password
- ใช้วันเกิดหรือหมายเลขโทรศัพท์เป็นรหัสผ่าน
- ใช้รหัสผ่านซ้ำหลายระบบ
- จดรหัสผ่านไว้ในที่ที่ผู้อื่นมองเห็นได้
- แชร์รหัสผ่านให้บุคคลอื่นใช้งาน

7. ประโยชน์ที่องค์กรได้รับ

- ลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์
- ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ลดโอกาสการรั่วไหลของข้อมูลสำคัญ
- สร้างวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร
- สนับสนุนการดำเนินงานตามมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ

สรุปองค์ความรู้

การจัดการรหัสผ่านอย่างปลอดภัยถือเป็นพื้นฐานสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ บุคลากรควรตระหนักถึงความสำคัญของการสร้างรหัสผ่านที่มีความแข็งแรง การใช้รหัสผ่านที่แตกต่างกันในแต่ละระบบ และการเปิดใช้งาน MFA เพื่อช่วยป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นในปัจจุบัน

ผลลัพธ์การเรียนรู้ที่คาดหวัง (Learning Outcome)

1. บุคลากรมีความรู้ความเข้าใจเกี่ยวกับหลักการตั้งรหัสผ่านที่ปลอดภัย
2. บุคลากรสามารถประเมินความเสี่ยงจากการใช้รหัสผ่านที่ไม่เหมาะสมได้
3. บุคลากรสามารถนำแนวปฏิบัติด้านการจัดการรหัสผ่านไปประยุกต์ใช้ในการปฏิบัติงานได้
4. บุคลากรมีความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้นและสามารถป้องกันตนเองจากภัยคุกคามเบื้องต้นได้

ข้อมูลอ้างอิง

1. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. https://www.dga.or.th/document-sharing/infographic/49252/
2. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) แนวปฏิบัติและสื่อเผยแพร่ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและประชาชน https://www.ncsa.or.th/ https://www.facebook.com/photo?fbid=1323624243292571&set=a.276119591376380
3. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ https://www.thaicert.or.th/

3) **จัดทำแผ่นภาพสำหรับประชาสัมพันธ์ตามข้อมูลความรู้ที่กำหนด ครั้งที่ 3**
เรื่อง “เสริมความปลอดภัยบัญชีผู้ใช้งาน ด้วยรหัสผ่านที่คาดเดาได้ยาก”