ที่ อว ๐๒๑๙/ว๑๒๓๓๗

กระทรวงการอุดมศึกษา
วิทยาศาสตร์ วิจัยและนวัตกรรม
ถนนศรีอยุธยา เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐

๒๖ มิถุนายน ๒๕๖๖

เรื่อง การดำเนินการตรวจสอบและดำเนินการป้องกัน กรณีบัญชีโซเชียลมีเดียของหน่วยงานถูกแฮ็ก

เรียน อธิการบดีสถาบันอุดมศึกษา

สิ่งที่ส่งมาด้วย เอกสารแจ้งเตือนกรณีกำชับให้หน่วยงานมีความระมัดระวังการโจมตีระบบหรือข้อมูลโซเชียล

ด้วย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้ตรวจพบข่าวสารการแฮ็กบัญชีโซเชียลมีเดียของหน่วยงาน เช่น Facebook Line Twitter และ Instagram เป็นต้น โดยอาศัยการโจมตีผ่านเครื่องคอมพิวเตอร์ ซึ่งผู้ไม่หวังดีใช้บัญชีของหน่วยงานไปเผยแพร่ภาพลามกอนาจารหรือโฆษณาเว็บพนันออนไลน์ ทำให้หน่วยงานเข้าข่ายการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และพระราชบัญญัติการพนัน พ.ศ. ๒๔๗๘ ส่งผลให้เสื่อมเสียชื่อเสียง และทำให้เกิดผลกระทบต่อหน่วยงานที่ถูกโจมตีในวงกว้าง

ในการนี้ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม จึงขอให้หน่วยงานของท่าน มีความระมัดระวังการโจมตีระบบหรือข้อมูลโซเชียลมีเดีย ตามคำแนะนำการป้องกันการถูกแฮ็กบัญชีโซเชียลมีเดียของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดพิจารณา และดำเนินการในส่วนที่เกี่ยวข้องต่อไปด้วย จะขอบคุณยิ่ง

ขอแสดงความนับถือ

(ศาสตราจารย์ศุภชัย ปทุมนากุล)
รองปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ปฏิบัติราชการแทน
ปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

สำนักงานปลัดกระทรวงการอุดมศึกษาฯ
สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (สบทศ.)
โทรศัพท์ ๐ ๒๒๓๒ ๔๐๐๐ ต่อ ๕๖๙๐ (ภูมิ)
e-mail : noc@uni.net.th

เอกสารการแจ้งเตือนกรณีกำชับให้หน่วยงานมีความระมัดระวังการโจมตีระบบหรือข้อมูลบัญชีโซเชียลมีเดีย

คำแนะนำการป้องกันการถูกแฮ็กบัญชีโซเชียลมีเดีย

ตามที่ปรากฏข่าวสารการแฮ็กบัญชีโซเชียลมีเดียหน่วยงาน เช่น Facebook Line Twitter และ Instagram เป็นต้น อาศัยการโจมตี ผ่านเครื่องคอมพิวเตอร์ โทรศัพท์มือถือหรืออินเทอร์เน็ต โดยส่วนใหญ่เป็นการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากผู้ใช้งาน แฮ็กเกอร์สามารถเข้าโจมตีผ่านการคาดเดารหัสผ่าน การล็อกอินบัญชี Facebook ค้างไว้บนแพลตฟอร์มหรือการถูกติดตั้งซอฟต์แวร์ขโมยข้อมูล โดยที่ผู้ใช้งานไม่ได้รับอนุญาตให้เข้าถึงข้อมูล ทำให้เกิดผลกระทบต่อหน่วยงานที่ถูกโจมตีในวงกว้าง เพื่อรับมือกับเหตุการณ์มั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน นั้น ๆ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) จึงขอแจ้งกำชับให้ผู้ดูแลสื่อโซเชียลมีเดียของหน่วยงานให้ความสำคัญกับการรักษาความมั่นคงปลอดภัย โดยเฉพาะหน่วยงานที่มีความเสี่ยงจะตกเป็นเป้าหมายของกลุ่มผู้ที่โจมตี ควรจะดำเนินการตรวจสอบความมั่นคงปลอดภัยของระบบเพื่อลดความเสี่ยงที่จะถูกโจมตีและควรดำเนินการโดยทั่วไป ดังนี้

1. ไม่ควรใช้รหัสผ่านที่คาดเดาได้ง่าย ควรตั้งรหัสผ่านให้มีความซับซ้อน มีอักขระพิเศษ อักษรตัวเล็ก ตัวใหญ่ มีตัวเลขผสมผสานกัน และใช้การยืนยันตัวตนแบบ Multi-Factor Authentication (MFA) เป็นอย่างน้อย [1] ตัวอย่าง เช่น การสแกนลายนิ้วมือ คำถามเฉพาะเพื่อกู้รหัสผ่าน การส่งรหัสผ่านแบบครั้งเดียวที่ส่งผ่านข้อความสั้นเข้าโทรศัพท์มือถือ (SMS OTP) การใช้กุญแจรักษาความปลอดภัย เป็นต้น

2. กรณีของผู้ใช้งานที่มีบัญชีโซเชียลมีเดีย ที่ใช้รหัสผ่านเดียวกันกับอีเมล (Email) หรือรหัสผ่านเดียวกับแพลตฟอร์มอื่น ๆ อาจมีความเสี่ยงสูงที่จะถูกเข้าถึงอีกระบบหนึ่งที่ใช้รหัสผ่านเดียวกันได้โดยง่าย ซึ่งแสดงให้เห็นว่าการเลือกใช้รหัสผ่านเดียวกันในทุกระบบย่อมส่งผลเสียได้เร็วและง่ายขึ้น ผู้ใช้งานควรตั้งรหัสผ่านที่แตกต่างกันเพื่อป้องการกันถูกเข้าถึงข้อมูลที่สำคัญ [2]

3. เปิดรับการแจ้งเตือนเมื่อมีการเข้าสู่ระบบโซเชียลมีเดีย หากมีใครเข้าสู่ระบบจากอุปกรณ์หรือเบราว์เซอร์ที่ปกติไม่ได้ใช้งานทางแพลตฟอร์มจะส่งข้อความแจ้งเตือนให้เรารู้ทันที เมื่อมีการเข้าสู่ระบบ

4. อย่าหลงกลเชื่ออีเมลที่แจ้งให้เปลี่ยนรหัสผ่านโดยที่ผู้ใช้งานไม่ได้ดำเนินการ ผู้ใช้งานจะต้องไม่คลิกลิงก์ที่แนบมากับอีเมลเป็นอันขาด หากต้องการเปลี่ยนรหัสผ่าน ให้ผู้ใช้งานเข้าไปยังหน้าแพลตฟอร์มโดยตรงและทำการเปลี่ยนรหัสผ่านด้วยตนเอง

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) ขอแนะนำการยืนยันตัวตนแบบ Multi-Factor Authentication (MFA) [3] มีขั้นตอน ดังนี้

1. การลงทะเบียน ผู้ใช้งานสร้างบัญชีด้วยชื่อผู้ใช้และรหัสผ่าน จากนั้นผู้ใช้จะเชื่อมโยงรายการอื่น ๆ เช่น หมายเลขโทรศัพท์มือถือหรือกุญแจรีโมท เข้ากับบัญชีของผู้ใช้งาน รายการเหล่านี้ช่วยระบุผู้ใช้งานที่ไม่เหมือนกันและไม่ควรแบ่งปันกับผู้อื่น

2. การยืนยันตัวตน เมื่อผู้ใช้งานที่มีการเปิดใช้งานยืนยันตัวตนแบบ Multi-Factor Authentication (MFA) ได้ลงชื่อเข้าใช้เว็บไซต์ระบบจะแจ้งขอชื่อผู้ใช้และรหัสผ่านและการตอบสนองเพื่อยืนยันตัวตนจากอุปกรณ์ผู้ใช้งาน หากยืนยันความถูกต้อง ระบบจะเชื่อมโยงไปยังรายการอื่น ๆ ตัวอย่างเช่น ระบบอาจออกรหัสตัวเลขให้กับอุปกรณ์ฮาร์ดแวร์หรือส่งโค้ดทาง SMS ไปยังอุปกรณ์เคลื่อนที่ของผู้ใช้งาน

3. การโต้ตอบ ผู้ใช้งานสามารถยืนยันตัวตนด้วยการยืนยันความถูกต้องของรายการอื่นๆ ตัวอย่างเช่น ผู้ใช้งานอาจป้อนรหัสที่ได้รับ หรือกดปุ่มบนอุปกรณ์ฮาร์ดแวร์ ผู้ใช้จะสามารถเข้าถึงระบบได้ต่อเมื่อข้อมูลทั้งหมดได้รับการยืนยันความถูกต้อง

4. การนำกระบวนการมาใช้ คือการยืนยันตัวตนโดยใช้หลายปัจจัยอาจนำมาใช้ได้ในหลายวิธี ระบบขอเพียงรหัสผ่าน และข้อมูล ID อีกหนึ่งอย่าง เรียกว่าการยืนยันตัวตนโดยใช้สองปัจจัยหรือการยืนยันตัวตนโดยใช้สองขั้นตอน แทนที่จะใช้ระบบ จะใช้แอปพลิเคชันของบุคคลภายนอกที่เรียกว่าเครื่องมือยืนยันตัวตนจะยืนยันความถูกต้องของตัวตนของผู้ใช้งาน ซึ่งผู้ใช้งานสามารถป้อนรหัสผ่านเข้าในเครื่องมือยืนยันตัวตน เครื่องมือยืนยันตัวตนจะยืนยันผู้ใช้งานกับระบบ ในระหว่างการยืนยันความถูกต้องผู้ใช้งานจะป้อนข้อมูลไบโอเมตริกด้วยการสแกนลายนิ้วมือ ม่านตา หรือส่วนอื่น ๆ ของร่างกาย โดยระบบอาจขอให้มีการยืนยันตัวตนหลายครั้งต่อเมื่อผู้ใช้งานเข้าถึงระบบเป็นครั้งแรกบนอุปกรณ์ใหม่ หลังจากนั้นระบบจะจดจำเครื่องและถามเพียงรหัสผ่านเท่านั้น

กรณีหน่วยงานที่ใช้บัญชี Facebook ส่วนตัวในการสร้างเพจ หากถูกผู้ไม่หวังดีแฮ็กเพจ Facebook อาจจะไม่รับผิดชอบกับเหตุการณ์ที่เกิดขึ้น แนะนำให้ใช้ Facebook Business[4] ที่สามารถเพิ่มความปลอดภัยด้วยฟีเจอร์ยืนยัน 2 ขั้นตอน(Two-Factor Authentication) ซึ่งเป็นระบบความปลอดภัยที่อยู่เบื้องหลังการทำงานของ Facebook Business ช่วยเพิ่มความปลอดภัยในการเข้าถึงข้อมูลสำคัญ

อ้างอิง

1. https://www.facebook.com/help/213481848684090
2. https://www.etda.or.th/th/Our-Service/ThaiCERT/Incident-Coordination/Information/Published-documents/General/papers-general/Password1-สญญาณอนตรายทมากบรหสผาน.aspx
3. https://aws.amazon.com/th/what-is/mfa/
4. https://www.facebook.com/business/help/1710077379203657?id=180505742745347