☐ ฝ.ปห.
☐ กง.บถ.
☐ กง.สส.
☑ กง.กม.
☐ กง.กง.
☐ กง.บป.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

สกจ. ปัตตานี
รับที่ 10465
วันที่ 09 พ.ย. 2566
เวลา 9.18

**ด่วนที่สุด**

ที่ สกมช ๐๘๑๐/ว๗๒๐

๗ พฤศจิกายน ๒๕๖๖

เรื่อง ขอเชิญประชุมเพื่อป้องกัน รับมือ และลดความเสี่ยง กรณีบัญชี Facebook ของหน่วยงานราชการถูกแฮ็กเพื่อนำไปเผยแพร่ข้อมูลผิดกฎหมายสร้างความเสื่อมเสียชื่อเสียงต่อภาครัฐ

เรียน หัวหน้าส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน องค์กรอิสระ หน่วยงานภาคเอกชน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สิ่งที่ส่งมาด้วย ๑. เอกสารแจ้งเตือนกรณีบัญชี Facebook ของหน่วยงานราชการถูกแฮ็กเพื่อนำไปเผยแพร่ข้อมูลผิดกฎหมายสร้างความเสื่อมเสียชื่อเสียงต่อภาครัฐ
๒. กำหนดการประชุมชี้แจงแนวทางการป้องกันและแก้ไขปัญหาการกรณี Facebook ของหน่วยงานราชการถูกแฮ็ก

ตามอ้างถึง มาตรา ๔๕ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรา ๒๒ (๖) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ “เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์” ได้ตรวจพบบัญชี Facebook ของหน่วยงานภาครัฐ ถูกกลุ่มมิจฉาชีพแฮ็กเพื่อนำไปเผยแพร่ข้อมูลลามกอนาจารสร้างความเสื่อมเสียชื่อเสียงต่อภาครัฐ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย (๑) นั้น

ในการนี้ เพื่อให้การดำเนินการแก้ไขปัญหาเชิงรุก และเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นกับหน่วยงานภาครัฐต่าง ๆ จึงขอเรียนเชิญเข้าร่วมรับฟังประชุมชี้แจงแนวทางการป้องกันและแก้ไขปัญหากรณี Facebook ของหน่วยงานราชการถูกแฮ็กเพื่อนำไปเผยแพร่ข้อมูลผิดกฎหมายสร้างความเสื่อมเสียชื่อเสียงต่อหน่วยงาน **ในวันอังคารที่ ๑๔ พฤศจิกายน ๒๕๖๖ เวลา ๐๙.๓๐ – ๑๑.๐๐ น. รูปแบบออนไลน์ผ่านระบบ Zoom Meeting** ทั้งนี้ ขอให้ท่านลงทะเบียนตาม QR CODE แนบท้ายหนังสือ ภายในวันจันทร์ที่ ๑๓ พฤศจิกายน ๒๕๖๖ โดยมี นางสาวจิรานันท์ รื่นสนธิ์ เป็นผู้ประสานงาน โทรศัพท์ ๐๒ ๑๔๒ ๖๘๘๕ อีเมล jiranan.r@ncsa.or.th

จึงเรียนมาเพื่อโปรดพิจารณาส่งผู้แทนเข้าร่วมรับฟังความรู้ดังกล่าวด้วย จะขอบคุณยิ่ง

ขอแสดงความนับถือ

พลอากาศตรี

(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
โทร. ๐ ๒๑๔๒ ๖๘๘๕
อีเมล thaicert@ncsa.or.th

ลงทะเบียนตอบรับ

Link Zoom

TLP:CLEAR

# เอกสารข้อมูลการแจ้งเตือนระวัง Facebook Account Compromise

เอกสารข้อมูลการแจ้งเตือนระวัง Facebook Account Compromise

ตามที่ สกมช. ได้ติดตามและตรวจพบการโจมตีหน่วยงานในประเทศไทยบน Facebook โดยการหลอกลวงผู้ใช้งานลักษณะ Facebook Account Compromise ซึ่งเป็นภัยคุกคามในรูปแบบ Phishing scams โดยการส่งข้อความหรือลิงก์ถึงผู้ใช้งาน เพื่อขอข้อมูลส่วนบุคคล เช่น ชื่อบัญชีผู้ใช้ รหัสผ่าน หรือเกี่ยวกับการละเมิดบัญชี ทำให้ผู้ใช้งานที่หลงเชื่อ กรอกข้อมูลบัญชีในลิงก์ปลอม และผู้โจมตีอาจนำข้อมูลดังกล่าวไปประพฤติในทางที่มิชอบ ซึ่งหากผู้โจมตีเข้าถึงบัญชีเพจ Facebook ของหน่วยงานได้จะทำให้เกิดผลกระทบต่อความน่าเชื่อถือของหน่วยงาน

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) จึงขอแจ้งให้ผู้ดูแลเพจ Facebook ของหน่วยงานให้ความสำคัญกับการรักษาความมั่นคงปลอดภัย โดยเฉพาะหน่วยงานที่มีความเสี่ยงอาจจะตกเป็นเป้าหมายของผู้โจมตี หากตรวจพบ ควรปฏิบัติเบื้องต้น ดังนี้

1. เปลี่ยนรหัสผ่านบัญชีผู้ใช้งานหรือทำการรีเซ็ตรหัสผ่าน
2. เปิดการตรวจสอบสิทธิ์แบบ Two-Factor Authentication
3. ตรวจสอบอุปกรณ์ที่เชื่อมต่อและลบอุปกรณ์ที่ไม่รู้จักออก
4. เพิกถอนแอปที่เชื่อมกับบัญชีผู้ใช้งานหรือบัญชีเพจ Facebook
5. เปลี่ยนรหัสผ่านอีเมลของท่านที่มีการล็อกอินกับบัญชีเพจ Facebook เพื่อรักษาความปลอดภัย

แนะนำสำหรับผู้ดูแลให้ทำการขอ Verified บน Facebook เพื่อสร้างความเชื่อมั่นให้กับผู้ติดตามบัญชี เครื่องหมายนี้จะช่วยยืนยันว่าเจ้าของบัญชีมีตัวตน ไม่ใช่มิจฉาชีพ ระบบสามารถทำหน้าที่ตรวจสอบและป้องกันการปลอมแปลงบัญชีให้กับท่านและการตรวจสอบสิทธิ์แบบ Two-Factor Authentication เป็นการช่วยปกป้องบัญชี โดยผู้ใช้งานสามารถเปิดใช้งานหรือปิดใช้งานระบบ หากเปิดใช้งาน จะมีการส่ง OTP แจ้งบนอุปกรณ์เพื่อให้ยืนยันตัวตนและสามารถใช้ได้หลังจากได้รับการยืนยันเท่านั้น

ทั้งนี้ แนะนำให้หน่วยงานเฝ้าระวังและตรวจสอบให้ความสำคัญกับการรักษาความมั่นคงปลอดภัย หากผู้ดูแลหรือผู้ใช้งานเพจ Facebook ตรวจพบการโจมตีสามารถแจ้ง Meta Support Pro ได้ที่ https://facebook.com/gpa/help และติดตามข่าวสารข้อมูลเพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

TLP:CLEAR

**กำหนดการ**

**การประชุมหน่วยงานที่เกี่ยวข้อง กรณีบัญชี Facebook ของหน่วยงานราชการถูกแฮกเพื่อนำไปเผยแพร่ข้อมูลผิดกฎหมายสร้างความเสื่อมเสียชื่อเสียงต่อภาครัฐ**

**ในรูปแบบออนไลน์ (Online)**

**วันอังคารที่ ๑๔ พฤศจิกายน ๒๕๖๖ เวลา ๐๙.๓๐ - ๑๑.๐๐ น.**

**********

๐๙.๓๐ - ๐๙.๔๕ น. - กล่าวเปิดประชุมชี้แจงโดย พลอากาศตรี อมร ชมเชย

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๐๙.๔๕ - ๑๐.๔๕ น. - การบรรยายในหัวข้อ “นโยบายความปลอดภัย และการรักษาความปลอดภัยบัญชี Facebook”

ผู้แทนจาก บริษัท เฟซบุ๊ก (ประเทศไทย) จำกัด

๑๐.๔๕ - ๑๑.๐๐ น. - การถาม-ตอบ

๑๑.๐๐ น. - ปิดการประชุม

**********

**หมายเหตุ : กำหนดการอาจมีการเปลี่ยนแปลง**