บันทึกข้อความ

ส่วนราชการ ทสส.ทอ.(สนผ.โทร.๒-๑๐๘๒)

ที่ กห ๐๖๐๙.๓/ ๓๓๒ **วันที่** ๑๐ มี.ค.๖๓

เรื่อง ขอแจ้งแนวทางปฏิบัติในการตรวจสอบ ป้องกัน และแก้ไขการถูกละเมิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ Facebook

สนผ.๑ ๑๑ มี.ค.๖๓

เสนอ นขต.ทอ.

๑. ตามอนุมัติ ผบ.ทอ.เมื่อ ๒๘ พ.ค.๕๗ ท้ายหนังสือ ทสส.ทอ.ที่ กห ๐๖๐๙.๖/๕๐๐ ลง ๒๑ พ.ค.๕๗ แนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ของ ทอ.กำหนดแนวทางการใช้สื่อสังคมออนไลน์ของข้าราชการ ทอ. เป็นไปในทางสร้างสรรค์ไม่มีผลกระทบต่อ ทอ. นั้น

๒. เพื่อให้การใช้งานสื่อสังคมออนไลน์ Facebook เป็นไปด้วยความเรียบร้อย ปลอดภัย และป้องกันความเสียหายที่อาจจะเกิดขึ้นกับเจ้าของบัญชี หรืออาจถูกผู้ไม่ประสงค์ดีนำบัญชีไปใช้ในลักษณะที่ก่อให้เกิดผลกระทบต่อภาพลักษณ์ของ ทอ. ให้ข้อมูลข่าวสารที่ทำให้เกิดความเสียหายต่อทางราชการหรือตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๔ (๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ จึงขอแจ้งแนวทางปฏิบัติในการตรวจสอบ ป้องกัน และแก้ไขการถูกละเมิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ Facebook ให้ นขต.ทอ.ได้รับทราบ (แนบ ๑) โดยสามารถดาวน์โหลดแนวทางปฏิบัติฯ ได้ที่เว็บไซต์ ทสส.ทอ. https://dict.rtaf.mi.th/images/documents/download/Facebook_guideline.pdf หรือแสกน QR Code (แนบ ๒) และขอให้ประชาสัมพันธ์ให้กำลังพลภายในหน่วยยึดถือเป็นแนวทางการปฏิบัติต่อไป

จึงเสนอมาเพื่อดำเนินการต่อไป

พล.อ.ท.
จก.ทสส.ทอ.

แนวทางปฏิบัติในการตรวจสอบ ป้องกัน และแก้ไขการถูกละเมิด บัญชีผู้ใช้งานสื่อสังคมออนไลน์ Facebook

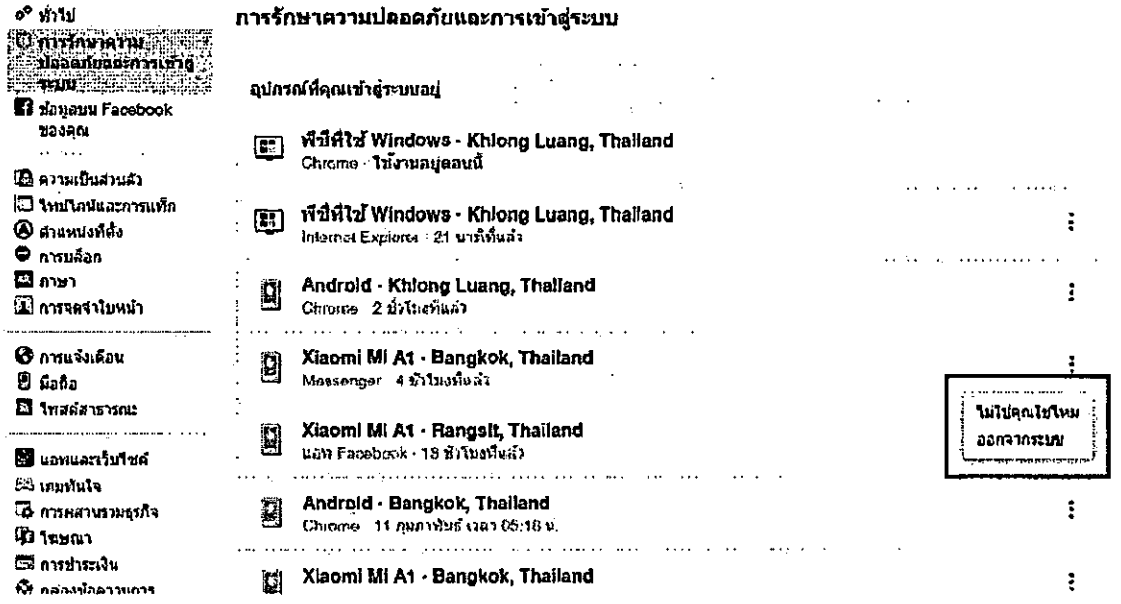
๑. วัตถุประสงค์และขอบเขต

แนวทางปฏิบัติในการตรวจสอบ ป้องกัน และแก้ไขการถูกละเมิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ Facebook จัดทำขึ้นเพื่อให้ทราบวิธีการตรวจสอบ ป้องกัน และแก้ไขการถูกละเมิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ Facebook ได้อย่างถูกต้อง ปลอดภัย อีกทั้งเป็นการลดความเสี่ยงของการเกิดความเสียหายต่อเจ้าของบัญชีผู้ใช้งานหรือการถูกละเมิดการใช้งานในลักษณะที่ส่งผลกระทบต่อภาพลักษณ์ของ ทอ.

๒. การนำไปใช้งาน บุคลากรสังกัด ทอ.ใช้คำแนะนำนี้ เป็นแนวทางปฏิบัติในการตรวจสอบ ป้องกัน และแก้ไขการถูกละเมิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ Facebook โดยให้ปฏิบัติตามขั้นการตรวจสอบ ป้องกัน และแก้ไขการละเมิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ Facebook ทั้งนี้ การใช้สื่อสังคมออนไลน์ในปัจจุบันมีการนำมาใช้งานอย่างแพร่หลายผู้ใช้งานจะต้องมีความรู้ในการใช้สื่อสังคมออนไลน์อย่างถูกต้อง และเพื่อให้การใช้งานสื่อสังคมออนไลน์ Facebook ของบุคลากรภายใน ทอ.มีความมั่นคงปลอดภัย ให้ปฏิบัติตามแนวทางปฏิบัติฯ และติดตามการแจ้งเตือนจาก ทสส.ทอ. และ ศซบ.ทอ. อยู่เสมอ

๓. การตรวจสอบบัญชีผู้ใช้งานสื่อสังคมออนไลน์ Facebook

๓.๑ ตรวจสอบอุปกรณ์ที่กำลัง Login อยู่ในระบบ โดยเข้าไปที่ตั้งค่า > การรักษาความปลอดภัยและการเข้าสู่ระบบ > อุปกรณ์ที่คุณเข้าสู่ระบบอยู่ จะทำให้สามารถเห็นอุปกรณ์ที่กำลังใช้งานและอุปกรณ์ที่เคยเข้าใช้งาน หากพบอุปกรณ์ที่ไม่ได้ Login โดยเจ้าของบัญชีให้บันทึกภาพไว้เป็นหลักฐานและเลือก “ออกจากระบบ” เพื่อหยุดการใช้งานอุปกรณ์นั้นกับบัญชี Facebook



รูปที่ ๑ ตรวจสอบอุปกรณ์ที่กำลังใช้งานและอุปกรณ์ที่เคยเข้าใช้งาน

๓.๒ การตรวจสอบ...

๓.๒ การตรวจสอบบัญชีผู้ใช้ หากมีการโพสต์หรือส่งข้อความที่ไม่ได้สร้างจากเจ้าของบัญชี หรือมีบุคคลอื่นเข้าถึงบัญชีโดยไม่ได้รับอนุญาต ให้ทำการตรวจสอบบัญชีโดยเข้าไป www.facebook.com/hacked เพื่อตรวจสอบการเคลื่อนไหวของบัญชี ระบบจะเข้าสู่กระบวนการรักษาความปลอดภัยของบัญชีทั้งหมด ตั้งแต่การตรวจสอบข้อมูลส่วนตัว การแสดงความคิดเห็น จำนวนการเข้าสู่ระบบ และมีการเคลื่อนไหวของการโพสต์หรือส่งข้อความเวลาใดบ้าง หากมีการโพสต์หรือการกระทำใด ๆ ที่ก่อให้เกิดความเสียหาย ให้บันทึกภาพหน้าจอเก็บเป็นหลักฐานเพื่อใช้ในการดำเนินคดีต่อไป

รูปที่ ๒ การตรวจสอบบัญชีผู้ใช้

๔. คำแนะนำในการป้องกันการถูกละเมิดบัญชีผู้ใช้สื่อสังคมออนไลน์ Facebook

๔.๑ การตั้งค่าในการป้องกันการถูกละเมิดบัญชีผู้ใช้สื่อสังคมออนไลน์ Facebook

๔.๑.๑ เปลี่ยนรหัสผ่านใหม่ให้มีความแข็งแกร่งและคาดเดาได้ยาก เข้าไปที่ การตั้งค่า > การรักษาความปลอดภัยและการเข้าสู่ระบบ > การเข้าสู่ระบบ จากนั้นทำการเปลี่ยนรหัสผ่านใหม่โดยไม่ใช้รหัสผ่านเดียวกันกับรหัสผ่านอีเมลหรือการลงทะเบียนในบริการอื่น ๆ เพราะอาจมีโอกาสที่ถูกผู้ประสงค์ร้ายซึ่งทราบรหัสผ่านของบัญชีผู้ใช้งานในบริการอื่นขยายผลมายังบัญชี Facebook โดยข้อแนะนำการตั้งรหัสผ่านให้มีความปลอดภัย มีดังนี้ มีความยาวอย่างน้อย ๘ ตัวอักษรหรือมากกว่า ประกอบด้วยตัวอักษร (a-z, A-Z) ตัวเลข (0-9) และเครื่องหมายหรือตัวอักขระพิเศษ

๔.๑.๒ ตั้งค่าเปิดใช้งาน การยืนยันตัวตนแบบสองชั้น เข้าไปที่ การตั้งค่า > การรักษาความปลอดภัยและการเข้าสู่ระบบ > การยืนยันตัวตนแบบสองชั้น ในขั้นตอนนี้จะเป็นวิธีการยืนยันตัวตนซึ่งช่วยเสริมให้การเจาะรหัสเข้าบัญชีได้ยากขึ้น โดยเลือกใช้ข้อความ (SMS) สำหรับการยืนยันตัวตนเพื่อเข้าสู่ระบบด้วย เมื่อตั้งค่าเสร็จเรียบร้อย ต่อไปทุกครั้งเมื่อเข้าสู่ระบบจะมีหน้าต่าง “ป้อนรหัสเข้าสู่ระบบของคุณ” ถามรหัสที่ส่งมาทางข้อความ (SMS) บนสมาร์ทโฟนเพื่อใช้ยืนยันตัวตนเข้าสู่ระบบ ซึ่งจะช่วยสร้างความปลอดภัยของบัญชีได้เพิ่มมากขึ้น

๔.๑.๓ ตั้งค่าเปิดรับการแจ้งเตือนจากอุปกรณ์ที่ไม่รู้จัก เข้าไปที่ การตั้งค่า > การรักษาความปลอดภัยและการเข้าสู่ระบบ > การตั้งค่าการรักษาความปลอดภัยพิเศษ โดยสามารถเปิดรับการแจ้งเตือนได้ ๓ ช่องทางคือ Facebook, Messenger และอีเมล ซึ่งเมื่อมีการเข้าถึงบัญชีผู้ใช้จากอุปกรณ์ที่ปกติไม่ได้ใช้งาน ระบบจะส่งการแจ้งเตือนเพื่อยืนยันการเข้างานบัญชีตามช่องทางที่ได้ตั้งค่าเอาไว้

๔.๑.๔ หากต้อง...

๔.๑.๔ หากต้องการเพิ่มระดับของความปลอดภัยยิ่งขึ้น (Optional) สามารถตั้งค่าเลือกผู้ติดต่อที่ไว้ใจได้เพื่อช่วยเหลือในการเข้าสู่ระบบ เข้าไปที่ การตั้งค่า > การรักษาความปลอดภัยและการเข้าสู่ระบบ > การตั้งค่าการรักษาความปลอดภัยพิเศษ โดยให้เลือกเพื่อนในบัญชี Facebook จำนวน ๓ ถึง ๕ คน เพื่อช่วยเหลือในการเข้าสู่ระบบ เมื่อเจ้าของบัญชีไม่สามารถลงทะเบียนเข้าสู่ระบบได้ สามารถเลือกให้ระบบส่งรหัสผ่านไปยังเพื่อนที่เลือกไว้ โดยเข้าไปที่ www.facebook.com/recover จากนั้นนำรหัสผ่านที่ได้จากทุกคนมาป้อนเข้าสู่ระบบ เพื่อใช้ในการยืนยันตัวตนเข้าสู่ระบบบัญชีได้อีกครั้ง

๔.๒ ข้อควรปฏิบัติในการป้องกันการถูกละเมิดบัญชีผู้ใช้สื่อสังคมออนไลน์ Facebook

๔.๒.๑ ออกจากระบบ (Logout) ทุกครั้งเมื่อใช้อุปกรณ์คอมพิวเตอร์สาธารณะ โดยเมื่อใช้อุปกรณ์คอมพิวเตอร์สาธารณะทั่วไปจะมีโอกาสลืมออกจากระบบ เช่น คอมพิวเตอร์สาธารณะ สมาร์ทโฟนของบุคคลอื่น เป็นต้น ดังนั้นพยายามหลีกเลี่ยงการเข้าสู่ระบบบัญชีบนอุปกรณ์อื่น ๆ ที่ไม่ใช่อุปกรณ์ส่วนตัว หากจำเป็นต้องใช้งานให้ออกจากระบบทุกครั้งและต้องไม่เลือกให้ระบบจำรหัสผ่าน

๔.๒.๒ หลีกเลี่ยงการเชื่อมต่อกับ Wi-Fi สาธารณะ การตั้งค่า Wi-Fi สาธารณะส่วนใหญ่ไม่มีการเข้ารหัสข้อมูล ผู้ไม่ประสงค์ดีที่ใช้งานอยู่ภายในเครือข่ายเดียวกัน อาจดักจับข้อมูลที่ส่งออกไปได้ เช่น การกรอกข้อมูลส่วนตัว ข้อมูลทางการเงิน เป็นต้น หรือในพื้นที่สาธารณะอาจมีผู้ไม่ประสงค์ดีตั้ง Wi-Fi ปลอมโดยตั้งชื่อให้คล้ายกับของจริงเพื่อหลอกให้เชื่อมต่อ ดังนั้นจึงไม่ควรใช้ Wi-Fi สาธารณะ หากมีความจำเป็นให้ตรวจสอบชื่อ Wi-Fi ให้ถูกต้อง

๔.๒.๓ หลีกเลี่ยงการลงทะเบียนเข้าร่วมกิจกรรมบนหน้าไทม์ไลน์ การลงทะเบียนเข้าร่วมกิจกรรมหรือเข้าเล่นเกมส์ต่าง ๆ ที่อยู่บนหน้าไทม์ไลน์ อาจมีการเชื่อมโยงไปยังเว็บไซต์ปลอม หรือมีความเสี่ยงซึ่งจะมีการขออีเมลหรือข้อมูลส่วนตัวเจ้าของบัญชี ซึ่งอาจทำให้ผู้ไม่ประสงค์ดีนำข้อมูลส่วนนี้ไปใช้ในการสุ่มรหัสผ่านก่อให้เกิดความเสียหาย ดังนั้นจึงไม่ควรกรอกข้อมูลส่วนตัวในการลงทะเบียนเข้าร่วมกิจกรรมหรือเล่นเกมส์ต่าง ๆ

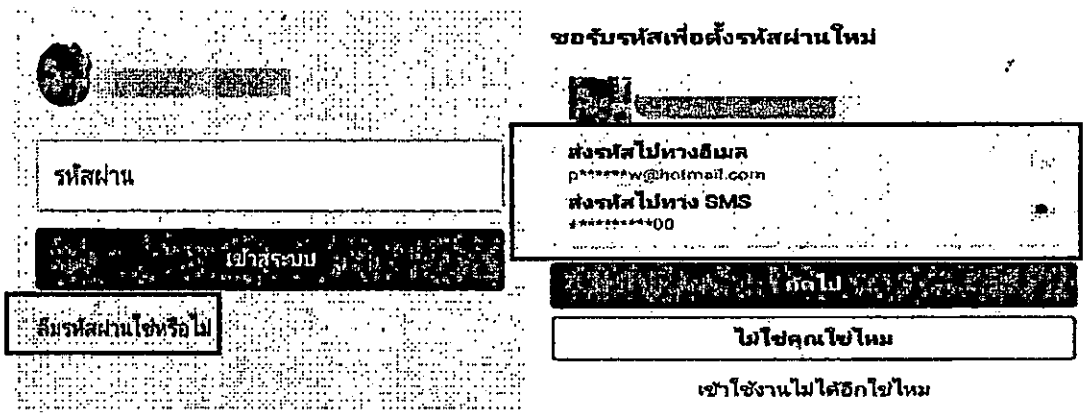
๕. คำแนะนำในการแก้ไขเมื่อถูกละเมิดบัญชีผู้ใช้สื่อสังคมออนไลน์ Facebook

๕.๑ เก็บหลักฐานและเข้าแจ้งความ หากพบว่าบัญชี Facebook ถูกละเมิด แล้วมีการนำไปใช้สร้างความเสียหาย ควรรวบรวมข้อมูลหลักฐานที่เกี่ยวข้องเพื่อนำไปใช้ลงบันทึกประจำวันหรือแจ้งความดำเนินคดี เช่น ข้อมูลสถานะการเข้าใช้งานบัญชี Facebook จากบุคคลอื่น อีเมลแจ้งเตือนการเข้าสู่ระบบหรือแจ้งเตือนการเปลี่ยนรหัสผ่าน เป็นต้น โดยการรวบรวมข้อมูลหลักฐาน ควรทำทั้งการบันทึกภาพหน้าจอและสั่งพิมพ์ออกมาเป็นกระดาษ พร้อมระบุวันเวลาที่เกิดเหตุ แล้วนำข้อมูลดังกล่าวไปแจ้งความ ณ สถานีตำรวจในพื้นที่หรือกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีเพื่อใช้ในการดำเนินคดี และปฏิบัติตามข้อ ๔ ต่อไป

๕.๒ ตรวจสอบอุปกรณ์ที่เข้าใช้งานในระบบอยู่เป็นประจำ ก่อนที่จะพยายามกู้คืนบัญชีให้ลองตรวจสอบก่อนว่า เราสามารถเข้าสู่บัญชีผ่านอุปกรณ์อื่น ๆ ได้หรือไม่ เช่น คอมพิวเตอร์ที่ทำงาน หรือโน้ตบุ๊คส่วนตัว เพราะเว็บบราวเซอร์ที่ใช้ในอุปกรณ์นั้นอาจยังไม่ถูก Logout ออกจากระบบ และให้รีบเข้าไปเปลี่ยนรหัสผ่านเพื่อป้องกันความเสียหายที่อาจเพิ่มมากขึ้น

๕.๓ การกู้คืนบัญชีผู้ใช้กรณีถูกเปลี่ยนรหัสผ่าน เมื่อผู้ใช้งานถูกละเมิดบัญชีและถูกเปลี่ยนรหัสผ่าน ผู้ใช้จึงจำเป็นต้องกู้บัญชี Facebook กลับคืนมาโดยไปที่แอปพลิเคชันและเข้าไปที่ “ลืมรหัสผ่าน” ระบบจะให้เลือกว่าจะให้ส่งข้อมูลไปที่อีเมลหรือเบอร์โทรศัพท์ที่มีการลงทะเบียนไว้ เพื่อทำการรีเซ็ตรหัสผ่านใหม่

รูปที่ ๔ ...



รูปที่ ๔ การกู้บัญชีเมื่อถูกเปลี่ยนรหัสผ่าน

๕.๔ กู้คืนบัญชีผู้ใช้กรณีถูกเปลี่ยนอีเมลหรือเบอร์โทร หากถูกเปลี่ยนแปลงข้อมูลสำคัญ ๒ อย่างคือ อีเมล หรือ เบอร์โทรศัพท์ กรณีนี้ให้เข้าไปที่ศูนย์ช่วยเหลือที่ https://m.facebook.com/help/contact เพื่อยืนยันตัวตน โดยระบบจะให้แนบสำเนาไฟล์เอกสารสำหรับระบุตัวตน ที่ออกให้โดยหน่วยงานราชการ เช่น สำเนาบัตรประชาชน สำเนาใบขับขี่ โดยสำเนาเอกสารที่ส่งไปต้องมีความชัดเจนเพื่อใช้ในการตรวจสอบและการกู้คืนบัญชี หากกู้คืนบัญชีสำเร็จระบบจะส่งอีเมลเพื่อทำการ Login และตั้งค่ารหัสผ่านใหม่อีกครั้ง

๖. วงรอบการปรับปรุงแนวทางการปฏิบัติฯ นี้ มีการปรับปรุงตามความจำเป็นที่เกี่ยวข้องกับการเปลี่ยนแปลงของสื่อสังคมออนไลน์ Facebook และมาตรฐานความปลอดภัยระบบสารสนเทศที่มีความทันสมัย

แนวทางปฏิบัติในการตรวจสอบ ป้องกัน
และแก้ไขการถูกละเมิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ Facebook
ดาวน์โหลด ได้ที่เว็บไซต์ ทสส.ทอ.
https://dict.rtaf.mi.th/images/documents/download/Facebook_guideline.pdf