

# ข้อมูลเบื้องต้นเกี่ยวกับการโจมตีทางไซเบอร์ที่ส่งผลกระทบต่อผู้ใช้งาน MU Webmail ของ มหาวิทยาลัยมหิดล ในเดือนกรกฎาคม 2564

## เหตุการณ์ที่เกิดขึ้น

ในวันที่ 22 กรกฎาคม 2564 ทางกองเทคโนโลยีสารสนเทศ สำนักงานอธิการบดี มหาวิทยาลัยมหิดล ได้ตรวจพบว่าผู้ไม่หวังดีเข้าถึงระบบเครือข่ายสื่อสารโดยไม่ได้รับอนุญาต และมีความพยายามทำสำเนาข้อมูล การเข้าใช้งานระบบไปรษณีย์อิเล็กทรอนิกส์ของมหาวิทยาลัย อันประกอบด้วยชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ตั้งแต่วันที่ 20 กรกฎาคม 2564 เวลา 20.36 น. ซึ่งทางกองเทคโนโลยีสารสนเทศ ได้ ตรวจพบและเร่งระงับเหตุเพื่อปิดการเข้าถึงดังกล่าวแล้วเสร็จในวันที่ 22 กรกฎาคม 2564 เวลา 21.20 น. ทำให้ข้อมูลชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานระบบไปรษณีย์อิเล็กทรอนิกส์ของ มหาวิทยาลัย ที่ใช้งานและยืนยันตัวตนผ่าน Webmail (<https://webmail.mahidol.ac.th>) ในช่วงเวลา ดังกล่าว อาจรั่วไหลไปยังผู้ไม่หวังดี โดยในเบื้องต้น กองเทคโนโลยีสารสนเทศตรวจสอบพบว่าในช่วงเวลา ดังกล่าว มีผู้ใช้งานที่ได้รับผลกระทบจำนวน 5,979 ราย

หากท่านได้รับแจ้งจากผู้บังคับบัญชา หัวหน้าหน่วยงาน หรือผู้แทนฝ่ายสารสนเทศของส่วนงาน ว่าท่านเป็นหนึ่งในผู้ได้รับผลกระทบดังกล่าว แสดงว่าท่านอยู่ในรายชื่อที่กองเทคโนโลยีสารสนเทศของ มหาวิทยาลัยตรวจพบว่า Username และ Password รั่วไหลออกไปแล้ว

จากการตรวจสอบโดยละเอียด กองเทคโนโลยีสารสนเทศพบว่า ข้อมูลที่รั่วไหล มีเพียง Username และ Password ของผู้ที่ใช้ใช้งานระบบไปรษณีย์อิเล็กทรอนิกส์ของมหาวิทยาลัย ที่ใช้งานและยืนยันตัวตนผ่าน Webmail ในช่วงเวลาดังกล่าวเท่านั้น ไม่รวมถึงการใช้งานระบบไปรษณีย์อิเล็กทรอนิกส์ผ่านช่องทางอื่น ๆ (เช่น POP3 หรือ IMAP) และไม่รวมผู้ที่ใช้ใช้งานระบบสารสนเทศอื่นๆ ของมหาวิทยาลัยมหิดลหรือของส่วนงาน

ผลกระทบที่เกิดขึ้น คือ ผู้ไม่หวังดีอาจใช้ข้อมูล Username และ Password ดังกล่าว เพื่อเข้าถึงข้อมูล เนื้อหา e-mail ในบัญชีผู้ใช้ (User Account) ดังกล่าว ทำให้ล่วงรู้เนื้อหาของ e-mail ของผู้ใช้งานได้ และอาจ สวมรอยเป็นผู้ใช้งานในการส่งเมลหาบุคคลอื่นได้ นอกจากนี้ เนื่องจากมหาวิทยาลัยมหิดลใช้ Username และ Password ชุดเดียวกันในระบบต่าง ๆ ผู้ไม่หวังดีจึงอาจใช้ข้อมูล Username และ Password ดังกล่าว เพื่อ เข้าถึงระบบอื่นๆ ของมหาวิทยาลัยมหิดล ที่ใช้ Username และ Password ชุดเดียวกัน และเรียกดูข้อมูลที่ อาจเป็นความลับ หรือแก้ไขข้อมูล หรือกระทำการอย่างอื่นในระบบตามสิทธิของผู้ใช้งานรายนั้น (ถ้ามี) โดย ไม่ได้รับอนุญาตได้

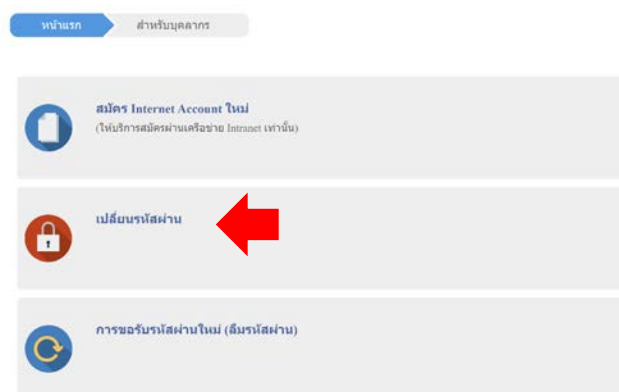
ทั้งนี้ ข้อมูลส่วนบุคคลอื่นของผู้ใช้งาน เช่น ที่อยู่ หมายเลขโทรศัพท์ติดต่อ หมายเลขประจำตัว ประชาชน ข้อมูลอื่น ๆ ด้านทรัพยากรบุคคล ฯลฯ ยังมีความมั่นคงปลอดภัยและไม่ได้ถูกเปิดเผยแต่อย่างใด นอกจากนี้ ปัจจุบัน กองเทคโนโลยีสารสนเทศได้ตรวจสอบให้แน่ใจแล้วว่า การใช้งานระบบ Webmail หลังจาก

วันที่ 22 กรกฎาคม 2564 เวลา 21.20 น. จนถึงปัจจุบัน มีความปลอดภัย และไม่มีข้อมูลของผู้ใช้งานคนอื่นรั่วไหลเพิ่มเติมอีกต่อไป

### สิ่งที่ขอให้ผู้ได้รับผลกระทบดำเนินการ

**สำหรับท่านที่ได้รับแจ้ง**จากผู้บังคับบัญชา หัวหน้าหน่วยงาน หรือผู้แทนฝ่ายสารสนเทศของส่วนงาน **ว่าท่านเป็นหนึ่งในผู้ได้รับผลกระทบดังกล่าว** แสดงว่าท่านอยู่ในรายชื่อที่กองเทคโนโลยีสารสนเทศของมหาวิทยาลัยตรวจพบว่า Username และ Password รั่วไหลออกไปแล้ว ซึ่งกองเทคโนโลยีสารสนเทศของมหาวิทยาลัย มอบหมายให้ผู้แทนของส่วนงาน เป็นผู้ประสานงานไปยังผู้ใช้งานที่ได้รับผลกระทบผ่านช่องทางภายในส่วนงาน (เนื่องจากหากใช้ช่องทางอื่นอาจทำให้ผู้ไม่หวังดีทราบและฉวยโอกาสสวมรอยเพิ่มเติมได้) **ขอให้ดำเนินการเปลี่ยนรหัสผ่านโดยเร่งด่วน เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลและระบบสารสนเทศของมหาวิทยาลัยโดยมิชอบจากผู้ไม่หวังดี** โดยท่านสามารถเปลี่ยนรหัสผ่านด้วยตนเองได้ที่เว็บไซต์ <https://myinternet.mahidol.ac.th/indexstaff.php> ด้วยการกรอก Username เป็น ชื่อ.นามสกุล3ตัวแรก (เช่น firstname.las) และ **ไม่ต้องลงท้ายด้วย @mahidol.ac.th แต่อย่างใด** จากนั้นกรอกรหัสผ่านเดิมและรหัสผ่านใหม่ เมื่อเปลี่ยนรหัสผ่านสำเร็จแล้ว ขอให้รอ 15-30 นาที ก่อนเริ่มทดสอบการใช้งาน เพื่อให้รหัสผ่านใหม่มีผลในทุกระบบก่อน หลังจากนั้นท่านสามารถเปลี่ยนรหัสผ่านในโปรแกรมแอปพลิเคชันที่ใช้เข้าถึง MU E-mail ของท่าน (เช่น Microsoft Outlook, Thunderbird หรือ E-mail application ใน mobile device) ให้เป็นรหัสผ่านใหม่ต่อไป (หากท่านใช้งานผ่าน Webmail เท่านั้น ท่านไม่ต้องแก้ไขรหัสผ่านในโปรแกรมหรือแอปพลิเคชันอื่นใด) ทั้งนี้ เมื่อท่านแก้ไขรหัสผ่านของ MU account @mahidol.ac.th ของท่านแล้ว รหัสผ่านใหม่จะมีผลสำหรับ @mahidol.edu account ของท่าน (ถ้ามี) ด้วยโดยท่านไม่ต้องไปแก้ไขรหัสผ่านของ @mahidol.edu account ของท่านเองแต่อย่างใด

หากท่านจำรหัสผ่านเดิมไม่ได้ หรือมีปัญหาในการเปลี่ยนรหัสผ่าน สอบถามข้อมูลเพิ่มเติมได้ที่ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล โทรศัพท์ 0 2849 6228 ทุกวันในช่วงเวลา 10.00 – 16.00 น.



<https://myinternet.mahidol.ac.th/indexstaff.php>

ชื่อผู้ใช้งาน   
รูปแบบ ชื่อ.ตัวอักษรและตัวเลข

รหัสผ่านปัจจุบัน

รหัสผ่านใหม่   
ใช้เฉพาะตัว A-Z, a-z, 0-9 ขนาด 7-15 ตัวอักษรเท่านั้น

ยืนยันรหัสผ่านใหม่

ยืนยันการเปลี่ยนรหัสผ่าน

**กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล จะ Lock User Account ของท่านที่ได้รับแจ้งให้เปลี่ยนรหัสผ่าน แต่ยังไม่เปลี่ยนรหัสผ่านภายในวันพฤหัสบดีที่ 29 กรกฎาคม 2564 เวลา 11.30 น. โดยหลังจากเวลาดังกล่าว ท่านที่ได้รับผลกระทบ จะไม่สามารถใช้งาน MU Account ได้ และจะต้องติดต่อกองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล โทรศัพท์ 0 2849 6228 ทุกวันในช่วงเวลา 10.00 – 16.00 น. หรือติดต่อผู้แทนส่วนงาน (ฝ่ายสารสนเทศ) เพื่อประสานงานในการ reactivate account ต่อไป**

นอกจากนี้ หากท่านใช้รหัสผ่านชุดเดียวกันนี้ กับระบบอื่น ๆ เช่น ระบบสารสนเทศของบัณฑิตวิทยาลัยหรือของส่วนงานของท่าน ที่ไม่ได้เชื่อมโยงกับ MU Account โดยตรง (รหัสผ่านจึงยังไม่ถูกเปลี่ยนเมื่อท่านเปลี่ยนรหัสผ่านของมหาวิทยาลัย) รวมทั้ง User Account อื่น ๆ ส่วนตัวของท่าน (เช่น Gmail, Facebook ฯลฯ) ท่านควรเปลี่ยนรหัสผ่านใน Account ต่าง ๆ เหล่านี้ด้วย เพื่อความปลอดภัย

กองเทคโนโลยีสารสนเทศ สำนักงานอธิการบดี มหาวิทยาลัยมหิดล รู้สึกเสียใจกับเหตุการณ์ที่เกิดขึ้น และขอภัยผู้เกี่ยวข้องทุกท่านในความไม่สะดวกที่เกิดขึ้น ทั้งนี้ มีความจำเป็นต้องขอให้ท่านดำเนินการดังกล่าวเพื่อประโยชน์ของผู้ใช้งานเองและทางมหาวิทยาลัย

กองเทคโนโลยีสารสนเทศ  
สำนักงานอธิการบดี มหาวิทยาลัยมหิดล