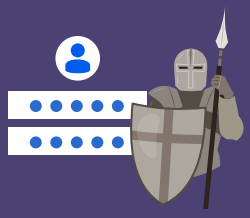
มหาวิทยาลัยมหิดล
คณะวิทยาศาสตร์
งานสารสนเทศและ
ห้องสมุดสตางค์ มงคลสุข

หมั่นดูแลและรักษา PASSWORD

การตั้งรหัสผ่าน

การตั้งรหัสผ่าน (Password) ช่วยป้องกันการเข้าถึงข้อมูลส่วนบุคคลหรือองค์กร เป็นการพิสูจน์ตัวตนให้ทราบว่าเป็นผู้ที่มีสิทธิ์สามารถเข้าสู่ระบบเพื่อการใช้งานได้ รหัสผ่านที่ปลอดภัยควรมีลักษณะดังนี้



- ไม่ควรตั้งรหัสผ่านที่เดาง่าย เช่น วันเดือนปีเกิด หมายเลขโทรศัพท์ ฯลฯ
- ประกอบด้วยตัวอักษรเล็กและใหญ่ ตัวเลข อักขระพิเศษ ความยาวไม่น้อยกว่า 8 ตัวอักษร
- ไม่ใช้รหัสผ่านชุดเดียวกันในทุกบัญชี
- หากจำเป็นต้องใช้อุปกรณ์สาธารณะ ต้อง Log Out ทุกครั้งหลังใช้เสร็จ
- ควรเปลี่ยนรหัสผ่านเป็นประจำ

รหัสผ่านถูกแฮก...ต้องทำอย่างไร

- เปลี่ยนรหัสผ่านทันที และเลือกใช้รหัสใหม่ที่ไม่เกี่ยวข้องกับรหัสเดิม
- หากอีเมลถูกแฮก ให้รีบกู้คืนด้วยอีเมลสำรองเพื่อยืนยันตัวตนตามขั้นตอนของแต่ละผู้ให้บริการ
- เปิดใช้งานการยืนยันตัวตนแบบสองระดับ (Two - Factor Authentication)
- ตรวจสอบการตั้งค่าต่าง ๆ เพื่อลดความเสี่ยงในการรั่วไหลข้องข้อมูล
- ติดตั้งโปรแกรม Anti-Malware

คิดให้ดีก่อนลงมือแฮก

บทลงโทษตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- **เข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ:**
  จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 1 หมื่นบาท หรือทั้งจำทั้งปรับ
- **เข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ:**
  จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ
- **ดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ:**
  จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ

ศึกษาเพิ่มเติม
1. บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน). (2 เมษายน 2564). **8 ขั้นตอนที่ต้องทำ เมื่ออีเมลโดนแฮก.** เข้าถึงได้จาก https://www.catcyfence.com
2. พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พ.ศ. 2560
3. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2 เมษายน 2564). **คู่มือคนไทยรู้ทันภัยไซเบอร์.** เข้าถึงได้จาก https://www.etda.or.th

https://stang.sc.mahidol.ac.th
StangMongkolsukLibrary
@StangLibrary
@StangLibrary