เทคนิคตั้งรหัสผ่าน (Password) ให้ปลอดภัย

โลกนี้กลายเป็นโลกของที่เราต้องใส่รหัสผ่านแทบจะทุกอย่างที่เป็นเกี่ยวกับ Social Media เพราะถือว่าเป็นพื้นที่ส่วนตัว ข้อมูลส่วนตัว ที่เราต้องหวงแหนแลรักษาเอาไว้ มิหนำซ้ำเมื่อโลกมีการพัฒนา สิ่งต่างๆ รวมไปถึงเทคโนโลยีต่างๆ ก็เข้ามาสู่โลกของอินเทอร์เน็ตมากขึ้น และสิ่งที่เกิดขึ้นต่อมาคือ เมื่อหลายสิ่งที่เราต้องทำการ Log in เข้าใช้งานอยู่เสมอ การตั้ง Password จึงอาจตั้งง่ายเพื่อให้จำได้ แต่หารู้ไม่ว่ามีความเสี่ยงมากเพียงใด เช่นกันการตั้ง Password เพื่อการใช้งานทั่วไปก็ต้องมีความปลอดภัยด้วย และเทคนิคต่อไปนี้จะช่วยให้ตั้งรหัสผ่าน Password ได้อย่างปลอดภัยมากขึ้น

สิ่งที่ไม่ควรนำมาตั้งเป็นรหัสผ่าน

1.ข้อมูลที่ใช้ในการระบุตัวตน เช่น ชื่อ นามสกุล เลขบัตรประจำตัวต่างๆ วันเดือนปีเกิด

2.ข้อมูลติดต่อ เบอร์โทรศัพท์

3.ชื่อบุคคลใกล้ชิด คนสนิท สัตว์เลี้ยง

4.คำที่พบในพจนานุกรม

5.คำทั่วไปที่สะกดจากข้างหลังมาข้างหน้า เช่น password > drowssap, admin > nimda

6.ใช้รูปแบบการตั้งรหัสผ่านที่คล้ายคลึงกันในแต่ละบัญชี เช่น secret1, 1secret

<u>สำหรับคำแนะนำในการตั้งรหัสผ่าน มีดังนี้</u>

1.ควรมีความยาวอย่างน้อย 8 ตัวอักษร หรือมากกว่านั้น

2.ประกอบด้วยอักขระต่อไปนี้ (อย่างน้อย 2 ใน3)

- ตัวอักษร (a-z, A-Z)
- ตัวเลข (0-9)
- เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=`{}[]:";'<>?,./)

<u>*คำแนะนำและข้อปฏิบัติเพิ่มเติม</u>

1.แต่ละบัญชีควรมีการตั้งรหัสผ่านที่แตกต่างกัน ไม่ควรใช้รหัสผ่านเดิม

2.หากแอปพลิเคชั่นใดมีการยืนยันตัวตนแบบ 2 ขั้นตอน ควรเปิดใช้งานด้วย

3.เปลี่ยนรหัสผ่านทุกๆ 3-6 เดือน

4.ตรวจสอบการเข้าถึงบัญชีเป็นประจำ

5.ออกจากระบบทุกครั้งหลังใช้งาน

6.ไม่ควรเลือกใช้งาน จำรหัสผ่าน (Remember me) บนเว็บไซต์

7.ไม่ควรจดรหัสผ่านลงกระดาษ หรือในไฟลีเอกสารที่ไม่มีการป้องกันการเข้าถึง

8.ไม่ควรเปิดเผยรหัสผ่านให้ผู้อื่นทราบ

อย่าละเลยการให้ความสำคัญกับรหัสการเข้าล็อกอินตามที่ต่างๆ เพราะไม่แน่ว่ากลุ่มมิจฉาชีพหรือภัยอันตรายอื่นๆ อาจตามมาได้ นอกจากจะเสียทรัพย์สินของตนเองแล้วอาจทำให้ผู้อื่นต้องถูกหลอกและเดือดร้อนได้ จากเพียงแค่เราละเลยสิ่งเหล่านี้นั่นเอง

ที่มา : it.chula.ac.th