ตั้ง PASSWORD อย่างไรให้ปลอดภัย

โดย **นายวิทยา สีระวัตร** นักวิชาการคอมพิวเตอร์

รหัสผ่านเป็นส่วนหนึ่งที่มีความสำคัญในการรักษาความปลอดภัยของบัญชีผู้ใช้งานหรือในระบบที่ต้องการความปลอดภัย ซึ่งรหัสผ่านถือเป็นสิ่งที่ใช้สำหรับยืนยันความถูกต้องของตัวบุคคลนั้น ๆ การใช้งานรหัสผ่านจึงช่วยป้องกันความปลอดภัย การเข้าถึงข้อมูลโดยมิชอบนั้นได้

หากผู้ใช้งานไม่ให้ความสำคัญในการตั้งค่ารหัสผ่านก็จะทำให้ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านและเข้าถึงข้อมูลของท่านได้อย่างง่ายดาย โดยแนวทางและข้อแนะนำในการตั้งค่ารหัสผ่านให้ปลอดภัยมีดังนี้

1. ยิ่งยาวยิ่งปลอดภัย *******

“ควรตั้งรหัสผ่าน 8-12 ตัวอักษรขึ้นไป”

เพราะรหัสผ่านที่มีความยาว 10 ตัวอักษรนั้นก็คาดเดาได้ยากกว่ารหัสผ่าน 8 ตัวอักษรถึง 4,000 เท่า! หรืออาจต้องใช้เวลาถึง 4,000 วัน! และถ้าจะเอาแบบแฮ็กยาก ๆ เราแนะนำที่ 14 ตัว ยิ่งยาวยิ่งเดายาก แต่ถ้าคุณตั้งรหัสผ่านแบบ 88888888888888 เลขแปด 14 ตัว แบบนี้ก็ท่าทางจะไม่รอดนะครับ *อย่าทำนะ...*

นอกจากนั้นเรื่องความยาวเดี๋ยวนี้หลาย ๆ เว็บกำหนดความยาวรหัสผ่านที่ 8 ตัวอักษรเป็นขั้นต่ำอยู่แล้ว แต่ถ้าให้ปลอดภัยจริง ๆ **แนะนำว่าตั้งเริ่มต้นที่ 10 ตัวอักษรจะดีกว่า**

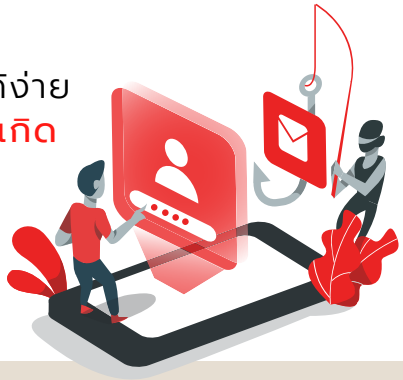
2. ใช้ทุกอย่างบนแป้นพิมพ์

สร้างรหัสผ่านด้วยการใช้คีบอร์ดแบบกระจาย ๆ ด้วยการผสมตัวอักษรภาษาอังกฤษทั้งพิมพ์เล็ก/ใหญ่ ตัวเลข เครื่องหมายพิเศษ เข้าด้วยกัน เพราะเมื่อเราใช้แบบนั้นแล้วโอกาสที่จะเดารหัสผ่านถูกจะมีแค่ 1 ในหลาย 100,000,000,000 (แสนล้าน) เช่น **การสร้างรหัสผ่าน 1A!2B@3C#4D$ ต่อให้เดาสุ่ม หรือแม้ว่าปัจจุบันจะมีโปรแกรมที่ใช้ช่วยเดาก็ยังถือว่าเข้าถึงได้ยาก** ดังนั้นเพื่อความปลอดภัยควรผสานรหัสผ่านด้วยตัวอักษรหลากหลายแบบเอาไว้เสมอ

PaS$*W0rD!

3. หลีกเลี่ยงข้อมูลส่วนตัว

ไม่ควรใช้ข้อมูลส่วนตัวที่หาได้ง่าย ได้แก่ ชื่อ นามสกุล วันเดือนปีเกิด เลขบัตรประชาชน มาตั้งรหัสผ่าน หรือ ข้อมูลส่วนตัวที่หาเจอได้ง่าย เช่น ชื่อแฝงที่เราชอบใช้มาผูกกับรหัสผ่าน เช่น ถ้าคุณชอบใช้ชื่อใน INTERNET ว่า WITTAYA ก็เลยตั้งรหัสผ่านว่า “WITTAYA123456” อย่างนี้ก็ให้หลีกเลี่ยงไปเลยจะดีกว่า



4. หลีกเลี่ยงคำในพจนานุกรม

อย่าใช้คำที่ปรากฏอยู่ในพจนานุกรมเลย เพราะคำศัพท์เหล่านั้นถูกนำไปบรรจุลงในโปรแกรมคาดเดารหัสผ่านเป็นที่เรียบร้อยแล้ว ต่อให้คำนั้นสะกดยากและยาวแค่ไหน โปรแกรมก็คาดเดาคำได้อยู่ดี เพราะฉะนั้นอย่าตั้งให้พวกแฮ็กเกอร์อ่านได้รู้เรื่องด้วยตัวอักษรธรรมดา

5. หลีกเลี่ยงรหัสยอดแย่แห่งปี

ในแต่ละปีจะมีรายงานว่าผู้คนตั้งรหัสผ่านยอดแย่ว่าอะไรบ้าง ดังตัวอย่าง --->

หากพบรหัสผ่านของคุณในรายการ ? คุณควรเปลี่ยนโดยเร็วที่สุดเท่าที่จะเป็นไปได้ อย่างน้อยก็ก่อนที่ผู้ไม่หวังดีจะสังเกตเห็น ตรวจสอบให้แน่ใจว่าคุณใช้รหัสผ่านแบบสุ่มที่รัดกุมในครั้งนี้

ลอง search หาดูได้จาก keyword นี้ “the Worst Passwords of 2022” ปกติผลจะออกช่วงสิ้นปี ลองดูสิว่าคุณเข้าข่ายรหัสผ่านยอดแย่แห่งปีกับเขารึเปล่า ?

รายชื่อรหัสผ่าน 20 อันดับ ยอดแย่ล่าสุด

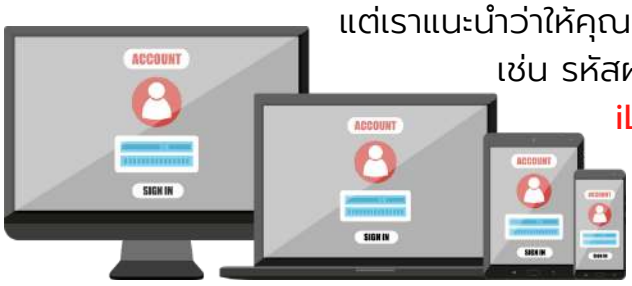
- 123456
- 123456789
- Qwerty
- Password
- 12345
- 12345678
- 111111
- 1234567
- 123123
- Qwerty123
- 1q2w3e
- 1234567890
- DEFAULT
- 0
- Abc123
- 654321
- 123321
- Qwertyuiop
- lloveyou
- 666666

อ้างอิงจาก https://locker.io/blog/worst-passwords

6. ใช้ความคิดสร้างสรรค์

ตั้งรหัสผ่านโดยสิ่งที่คุณชอบ สถานที่ที่คุณจำไม่เคยลืม สื่อบันเทิงที่คุณชอบ เช่น หนังสือ เพลง หรืออะไรก็ตามที่คุณนึกถึงเป็นอันดับต้น ๆ เช่น ถ้าคุณชอบกินชาบู คุณก็อาจจะตั้งว่า i love shabu แล้วลองพยายามแปลงตัวอักษรเหล่านั้นให้เป็นหลาย ๆ อย่างบนแป้นพิมพ์ เอาให้ครบเหมือนข้อ 2 ก็อาจจะได้ประมาณนี้ iL0v3@Sh@Bu หรือลองตั้งชื่อเป็นภาษาไทยที่พิมพ์ด้วยภาษาอังกฤษแล้วใส่เครื่องหมายและตัวเลขเข้าไป เช่น ถ้าคุณชื่อ วิทยา ไอซีที ก็จะได้ ;bmpkwv:umu ให้ลองบริหารการใช้อักษรตามข้อ 2 ลองปรับเป็น ;BmPkwV:Umu แค่นี้ก็ปลอดภัยครับ (แนะนำว่าให้จำด้วยนะครับเพราะเวลาจะสลับใช้ระหว่างคอมพิวเตอร์มาใช้มือถือ)

7. อย่าใช้รหัสผ่านซ้ำ



ไม่ควรใช้รหัสผ่านซ้ำเหมือนกันทุกเว็บไซต์ เพราะเมื่อไหร่ที่รหัสหลุดไปอยู่ที่ผู้หวังร้าย ข้อมูลส่วนตัวเราอาจถูกขโมยไปได้ แต่เราแนะนำว่าให้คุณตั้งให้เป็นเอกลักษณ์ของเว็บนั้น ๆ เลยจะดีกว่า เช่น รหัสผ่านของ เว็บ Gmail เราอาจใช้ตัวย่อมาตั้งต่อจากที่เราเคยตั้งก็ได้ iL0v3@Sh@Bu แล้วต่อด้วย GM คุณจะได้ iL0v3@Sh@BuGM ส่วนของ Hotmail ก็เป็น iL0v3@Sh@BuHM ไม่ซ้ำแต่มีนัยยะ

8. ไม่บอกออกไป

รหัสผ่านของคุณอย่าบอกใครเลย ยิ่งถ้าเกี่ยวข้องกับความเป็นส่วนตัว หรือเกี่ยวข้องกับเรื่องเงิน ๆ ทอง ๆ แล้ว เก็บไว้ในใจของคุณเองก็น่าจะดีกว่า

DID YOU KNOW?

บอกรหัส/CODE ลับ หรือ NSRU ACCOUNT กับเพื่อนผิดกฎหมายหรือไม่?

ในชีวิตประจำวันของเราทุกวันนี้จะต้องวนเวียนกับการใช้ username และ password เพื่อเข้าถึงอุปกรณ์คอมพิวเตอร์ เครื่องมือสื่อสาร ระบบปฏิบัติการ รวมไปถึงเว็บไซต์ต่างๆที่เรามีบัญชีผู้ใช้ (account) อยู่ ไม่ว่าจะเป็น E-mail Facebook Twitter Instagram หรือเข้าสู่หน้าเว็บไซต์ที่เราเป็นสมาชิกอยู่

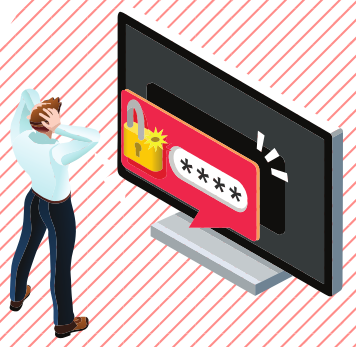
username และ password นั้นก็ถูกสร้างขึ้นมาเพื่อยืนยันตัวบุคคลก่อนที่จะมีการเข้าถึงข้อมูลต่าง ๆ ในระบบคอมพิวเตอร์ เพราะในแต่ละบัญชีผู้ใช้นั้นจะมีข้อมูลส่วนตัวสำคัญ ๆ ของผู้ใช้แต่ละคน นอกจากนี้บัญชีผู้ใช้บางประเภทก็เชื่อมต่อกับการจ่ายเงินผ่านบัตรเครดิต เช่น PayPal iTunes เป็นต้น

การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นที่มีการตั้งรหัสไว้โดยไม่ได้รับอนุญาตนั้นจึงถูกกำหนดโทษทางอาญาไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ความรับผิดเกี่ยวกับการเข้าใช้ username และ password ตามพระราชบัญญัติฯ หลักๆ จะมีอยู่ 3 เรื่อง

1. การเข้าถึงอุปกรณ์ ชุดคำสั่ง ระบบปฏิบัติการที่มีการตั้งรหัสของคนอื่น โดยไม่ได้รับอนุญาต
   ความผิดในมาตรา 5 มีโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ
2. การเปิดเผยรหัสการเข้าถึงระบบคอมพิวเตอร์ของบุคคลอื่น
   ความผิดในมาตรา 6 แล้ว โดยมีโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ
3. การเข้าถึงข้อมูลคอมพิวเตอร์ที่มีการตั้งรหัสของคนอื่น โดยไม่ได้รับอนุญาต
   มาตรา 7 นั้นสูงกว่าในมาตรา 5 มีโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

ข้อควรปฏิบัติเพิ่มเติม



- ในแต่ละบัญชีควรมีการตั้งรหัสผ่านที่แตกต่างกัน ไม่ควรใช้รหัสผ่านเดิม
- หากแอพพลิเคชั่นหรือเว็บไซต์ใดมีการเปิดยืนยันตัวตนแบบ 2 ขั้นตอน ควรเปิดใช้งานในส่วนนี้ด้วย
- ตรวจสอบการเข้าถึงบัญชีเป็นประจำ
- ออกจากระบบทุกครั้งหลังใช้งาน
- ไม่ควรเลือกใช้งาน “จำรหัสผ่าน” (Remember me) บนเว็บไซต์
- ไม่ควรจดรหัสผ่านลงกระดาษหรือในไฟล์เอกสารที่ไม่มีการป้องกันการเข้าถึง
- ไม่เปิดเผยรหัสผ่านให้ผู้อื่นรับทราบ
  ทั้งนี้ทางสำนักบริหารเทคโนโลยีสารสนเทศไม่มีนโยบายสอบถามรหัสผ่านจากผู้ใช้บริการทั้งทางโทรศัพท์หรืออีเมล

CSI ThaiElaws (2559).**บอกรหัส/CODE ลับกับเพื่อนผิดกฎหมายหรือไม่?**. สืบค้นเมื่อ 30 พฤศจิกายน 2565, จาก https://www.facebook.com/CSIThaiElaws/posts/1694044800812751/

Jenny Duong (2022). **Top 20 Worst Passwords in 2022**. สืบค้นเมื่อ 30 พฤศจิกายน 2565, จาก https://locker.io/blog/worst-passwords

มทนา วิบูลยเสข (2561). **8 เทคนิคการตั้งพาสเวิร์ด (รหัสผ่าน) ให้ปลอดภัย**. สืบค้นเมื่อ 30 พฤศจิกายน 2565, จาก https://www.aware.co.th/