สำนักงาน ป.ป.ท.
สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ
PACC NEWS
OFFICE OF PUBLIC SECTOR ANTI - CORRUPTION COMMISSION

ตั้งรหัสผ่านอย่างไรให้ปลอดภัยและจำได้

พูดถึงเรื่องการตั้งรหัสผ่าน ไปเว็บไหนก็จะเจอแต่กูรูแนะนำให้ตั้งรหัสแบบที่ซับซ้อน จำนวนตัวอักษรเยอะ ๆ เข้าไว้ รวมถึงอย่าใช้ข้อมูลส่วนตัวที่ใคร ๆ ก็รู้ข้อมูลส่วนนี้ (เช่น วันเดือนปีเกิด เบอร์มือถือ หรือ เลขที่บ้าน) แต่นั่นก็เป็นเหมือนดาบสองคม ตั้งยากก็จำยาก ลองจินตนาการดูว่าจะยุ่งยากแค่ไหน หากตั้งรหัสที่ซับซ้อนมากจนเราก็ยังจำไม่ได้ ยิ่งไม่ให้ซ้ำกันในแต่ละเว็บด้วยแล้วยิ่งยากขึ้นไปอีก ถึงแม้ว่าหลายคนจะใช้บริการ Password Manager เพื่อบันทึกรหัสผ่านจากหลาย ๆ เว็บไซต์หรือแอปฯ ให้รวมอยู่ในที่เดียวกันและสามารถนำไปใช้งานได้ทันที โดยเราไม่ต้องจำรหัสผ่านเหล่านั้นก็ตาม แต่เราก็ยังต้องตั้งรหัสหลัก (Master Password) เพื่อเข้าสู่บัญชี Password Manager อยู่ดี

National Cyber Security Center (NCSC) แห่งสหราชอาณาจักร ได้รวบรวมรหัสผ่านที่พบบ่อยที่สุด 10 ชุด โดยศึกษาจากรหัสผ่านจำนวน 100 ล้านชุดที่รั่วไหลออกมาในปีนี้ ซึ่งล้วนแต่เป็นรหัสผ่านที่จดจำได้ง่าย แต่ห้ามนำมาใช้เด็ดขาด เพราะรหัสผ่านแบบนี้ ใคร ๆ ก็สามารถคาดเดาได้เช่นกัน

อันดับ	2562
1	123456
2	123456789

3	qwerty
4	password
5	1111111
6	12345678
7	abc123
8	1234567
9	password1
10	12345

วิธีการตั้งรหัสผ่านที่ปลอดภัย มีดังนี้

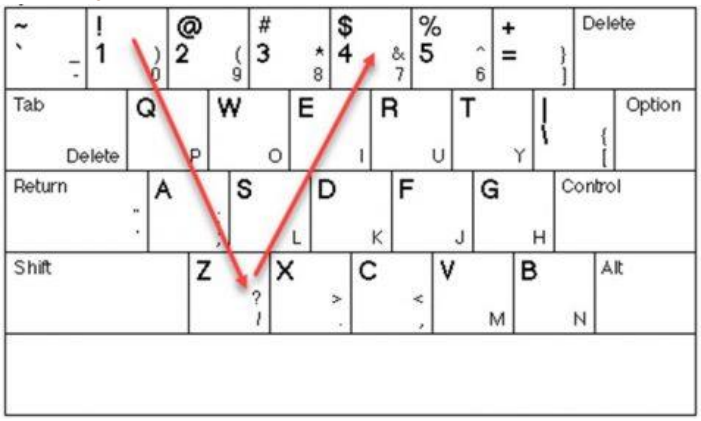
- **ควรใช้รหัสความยาวอย่างน้อย 12 -14 ตัวอักษร**
  แม้ว่าการตั้งรหัสที่จำนวนตัวอักษรเยอะ จะไม่ช่วยจากการโดน Phishing หรือ การโดน Key Logger แต่การตั้งความยาวตัวอักษรที่น้อยเกินไป อาจโดน Brute Force ได้ จึงแนะนำว่าอย่างน้อยก็ควรใช้รหัสผ่านที่ยาว 12 ตัวอักษรขึ้นไป โดยเฉพาะสำหรับป้องกันข้อมูลด้านการเงิน คละ ตัวเลข สัญลักษณ์ ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก เพื่อเป็นการสร้างรหัสที่ยากต่อการเดาสุ่ม
- **ไม่ควรใช้คำศัพท์ในพจนานุกรม (Dictionary)**
  ไม่ว่าจะเป็นคำศัพท์แบบเดี่ยว เช่น building หรือนำหลาย ๆ คำมารวมกัน เช่น NiceGreenBuilding เนื่องจากแฮกเกอร์สามารถใช้โปรแกรมการเดารหัสผ่านโดยเปรียบเทียบจากฐานข้อมูลคำศัพท์
- **หลีกเลี่ยงการตั้งรหัสผ่านที่เป็นรูปแบบ (Pattern) ที่นิยมใช้กันทั่วไป**
  หน่วยงานวิจัยของกระทรวงกลาโหมของสหรัฐฯ (Darpa) เคยทำการศึกษาและพบว่ามีรูปแบบหลัก ๆ 3 รูปแบบ ดังนี้
  – ตัวพิมพ์ใหญ่ 1 ตัว + ตัวอักษรพิมพ์เล็ก 5 ตัว + ตัวเลข 3 หลัก เช่น Komand123
  – ตัวพิมพ์ใหญ่ 1 ตัว + ตัวพิมพ์เล็ก 6 ตัว + ตัวเลข 2 หลัก เช่น Komando12
  – ตัวพิมพ์ใหญ่ 1 ตัว + ตัวพิมพ์เล็ก 3 ตัว + ตัวเลข 5 หลัก เช่น Koma12345
- **อย่าแทนตัวอักษรหรืออักขระบางตัวด้วยตัวเลขที่ดูคล้ายกัน**
  เช่น ตั้งรหัสผ่านว่า H0use โดยใช้เลข 0 (เลขศูนย์) แทน o (อักษรโอ) คนทั่วไปก็สามารถคาดเดาได้ถึงแม้จะผสมกัน หรือ BigHouse$123 มี 12 ตัวอักษร ได้แก่ ตัวอักษรตัวพิมพ์ใหญ่ ตัวอักษรตัวพิมพ์เล็ก สัญลักษณ์และตัวเลข ซึ่งมันเป็นคำจากพจนานุกรม มีสัญลักษณ์ตัวเดียวและตัวเลขเรียงทั้งหมดอยู่ท้าย รหัสผ่านลักษณะนี้ก็คาดเดาได้ง่ายเช่นกัน

วิธีตั้งรหัสผ่านที่ยากแต่จำได้ ทำอย่างไร

1. **ตั้งรหัสผ่านด้วยตัวอักษรแรกของประโยคหรือวลีที่เราชอบ**และจำได้ง่าย เช่น เนื้อเพลงจาก The Beatles ท่อนหนึ่งมาใช้เพื่อแปลงเป็นรหัสผ่านโดยใช้ตัวอักษรแรกของแต่ละคำ ดังนี้
   ก่อนแปลง : “Yesterday, all my troubles seemed so far away / Now it looks as though they’re here to stay / Oh, I believe in yesterday”
   หลังแปลง : Y,amtssfa/Nilatt’h2s/O,Ibiy

2. **ตั้งรหัสผ่านจากคำหรือชื่อสั้น ๆ 2 – 3 ตัวอักษร และกดปุ่ม QWERTY Keyboard** เลียนการลากเส้นเมื่อเขียนตัวอักษร (Pattern-based)
   เช่น ตัวอักษร V ให้กดปุ่ม 1qazse4 หรือหากต้องการให้ซับซ้อนขึ้น สามารถใช้วิธีกด SHIFT เพื่อสร้างรูปแบบคละตัวอักษร

พิมพ์ใหญ่และพิมพ์เล็ก ได้ตามนี้



– V เมื่อคละตัวอักษรพิมพ์ใหญ่ + พิมพ์เล็ก จะได้รหัสผ่าน !qAzSe$

– V เมื่อคละตัวอักษรพิมพ์เล็ก+ พิมพ์ใหญ่ จะได้รหัสผ่าน 1QaZsE4

– V เมื่อคละตัวอักษรพิมพ์ใหญ่ + พิมพ์เล็ก + พิมพ์เล็ก จะได้รหัสผ่าน !qaZse$

– V เมื่อคละตัวอักษรพิมพ์เล็ก + พิมพ์เล็ก + พิมพ์ใหญ่ จะได้รหัสผ่าน 1qAzsE4

– V เมื่อพิมพ์แบบย้อนศรจากปลายหาง V มายังหัวแทน (1qazse4) จะได้รหัสผ่าน 4eszaq1

3. **ออกแบบรหัสผ่านของตัวเองโดยเพิ่มความซับซ้อนไปเรื่อย ๆ**
   สร้างรหัสผ่านจากคำที่เราชอบแล้วออกแบบให้มีความซับซ้อนยิ่งขึ้น เช่น ถ้าชอบการร้องเพลง แล้วเนื้อเพลงมาคละตัวอักษร เช่น เพลง นิทานหิ่งห้อย มีประโยคแรกของเพลงว่า “เด็กน้อยได้ยินเรื่องราว” เมื่อพิมพ์สลับแป้นเป็นภาษาอังกฤษแล้ว จะเป็น
   – gfHdohvpwfhpboginjv’ik;
   และเมื่อ สลับตัวพิมพ์เล็กพิมพ์ใหญ่แล้วจะเป็น
   – GfhdOhvpWfhPboGinjv’Ik;
   ถ้าเพิ่มความซับซ้อนขึ้นไปอีก ก็ทำการแทรกตัวเลขระหว่างคำลงไป ก็จะกลายเป็น
   – GfHd3Ohvp6Wf2Pbo9Ginjv’1Ik;
   เป็นต้น

เมื่อรหัสเข้มแข็งแล้ว สิ่งที่ควรทำเพิ่มเติมมีอะไรบ้าง

1. ถ้าเป็นไปได้ควรเปิดใช้งาน 2FA เพื่อยืนยันตนเข้าระบบแบบสองชั้น
2. ไม่ใช้รหัสผ่านซ้ำ ๆ กันในแต่ละเว็บไซต์ การใช้รหัสผ่านซ้ำกันดูเหมือนจะไม่มีผลกระทบอะไร แต่จริง ๆ แล้ว การใช้รหัสผ่านซ้ำกันในแต่ละเว็บไซต์ส่งผลร้ายแรงกว่าที่คิด เพราะไม่ใช่ทุกเว็บไซต์จะดูแลรหัสผ่านของเราได้อย่างปลอดภัย อาจเกิดเหตุการณ์ Password รั่วไหล หรือโดนแฮก จนทำให้ Hacker นำรหัสผ่านชุดเดียวกันมา Login ในเว็บอื่น ๆ ของเราได้
3. เลือกใช้ Password Manager ที่น่าเชื่อถือในการบันทึกรหัสผ่าน แม้จะมีค่าใช้จ่าย แต่เมื่อเทียบกับความคุ้มค่าแล้ว ถือว่าคุ้มมาก

อ้างอิงที่มา: - www.catcyfence.com

– https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

– https://www.techadvisor.co.uk/how-to/internet/create-strong-password-3357177/

– https://www.skyhighnetworks.com/cloud-security-blog/how-to-create-a-strong-password-you-actually-remember/

– https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

– https://searchsecurity.techtarget.com/tip/Pattern-based-passwords-Easy-to-remember-non-dictionary-based-passwords

– https://wpengine.com/unmasked/