การตั้ง **Password** ให้จำง่ายแต่ **Crack** ยาก

Password นั้นถือเป็นกุญแจสำคัญประจำตัวของทุกคนซึ่งจะต้องไม่เปิดเผยให้ผู้ใดล่วงรู้ได้ แม้แต่เจ้านาย เลขาหรือผู้ดูแลระบบก็ตาม เพราะหากมีผู้ใดล่วงรู้ password ของเราไปแล้ว ผู้นั้นสามารถนำไปใช้เข้าระบบต่างๆ เสมือนว่าเป็นตัวเรา เพราะระบบ Access Control จะคิดว่าเป็นตัวเรา และระบบการ log ต่างๆ ก็จะบันทึกว่าเราเป็นผู้เข้าไปใช้เอง ซึ่ง log ดังกล่าวอาจถูกนำมาใช้อ้างอิงในการสืบสวนสอบสวนในกรณีที่มีการกระทำความผิดเกิดขึ้น และอาจใช้เป็นหลักฐานในศาลได้ต่อไป ตามที่ พ.ร.บ. ใหม่ได้กล่าวไว้

หลักพื้นฐานที่เป็นที่ยอมรับกันสากล Password ซึ่งมีหลักง่ายๆ 3 ข้อคือ

1. Password Length: ความยาวไม่ต่ำกว่า 8 ตัวอักษร(และตัวเลข)
2. Password Expiration: จะหมดอายุใน 90 วัน
3. Password History: ไม่สามารถใช้ password ซ้ำกับ password 3 ตัวก่อนหน้านี้

จากแนวทางดังกล่าวจะเห็นได้ว่า user จะถูกบังคับให้เปลี่ยน password ทุกๆ 3 เดือน ซึ่งจะนำไปสู่ความยุ่งยากในการจดจำ และนำไปสู่การจดบันทึกซึ่งจะกลายเป็นความเสี่ยงใหม่ ดังนั้นจึงขอแนะนำวิธีการในการตั้ง password ให้ง่ายต่อการจดจำ และในขณะเดียวกัน ก็ให้ยากต่อการถูก crack (ถอดรหัส password) ด้วย

ก่อนอื่นมาดูกันก่อนว่า Password ที่ยากต่อการถูก crack นั้นมีลักษณะเป็นเช่นไร อันดับแรก ต้องไม่เป็นคำทีง่ายต่อการคาดเดา เช่น guest, password, mydog, iloveu เป็นต้น ซึ่งคำเหล่านี้มักจะมีอยู่ใน list ที่ hacker มีอยู่ ที่เราเรียกกันว่า Password Dictionary

Password ที่ดีนั้น ควรมีความยาวตั้งแต่ 8-14 ตัวหรือมากกว่านั้น และมีส่วนผสมของอักขระทั้ง 4 ประเภทดังต่อไปนี้

1. Lowercase Alphabet หรือตัวอักษรเล็ก เช่น a b c d
2. Uppercase Alphabet หรือตัวอักษรใหญ่ เช่น A B C D
3. Numeric หรือ ตัวเลข เช่น 1 2 3 4
4. Special Character หรือ อักขระพิเศษ เช่น ! @ # $ % ^ & * ( ) _ +

<u>เทคนิคที่ 1 สร้าง Password จาก Phrase ที่จำง่าย</u>

เช่น ICT is Excellence, cms 3456 ready

<u>เทคนิคที่ 2 ใช้อักษรตัวแรกของคำจาก Phrase</u>

เช่น I know I can do it better for PTT → ikicdibfptt หรือ

I bet Man U must win this season → ibmumwts

<u>เทคนิคที่ 3 แทนสระหรืออักษรด้วยตัวเลขหรืออักขระพิเศษ</u>

อักษรเดิม	อักษรแทน
A	4 หรือ @
E	3
I	1 หรือ !
O	0
S	$
And	&
for	4 (four)

เทคนิคที่ 4 กดปุ่ม "Shift" ค้างไว้ขณะที่กดตัวเลขบนแป้นพิมพ์ด้านบน

เทคนิคนี้จะทำให้ได้อักขระพิเศษมาแทนที่ตัวเลข เช่น หากใช้เบอร์ต่อ **3456** ก็จะได้อักขระ **#$%^** แทน

จากการใช้เทคนิคที่กล่าวมาข้างต้นผสมผสานกัน ก็จะทำให้เราสามารถสร้าง password ที่มีความหลากหลาย ยากแก่การคาดเดา และง่ายในการจดจำครับ ลองมาดูตัวอย่างการประยุกต์ใช้กันนะครับ

ICT is Excellence → ICT1$3xc3ll3nc3 → BEST
Cms3456ready → Cms#$%^r34dy → Strong
I know I can do it better for PTT → ikicdibfptt → 1k1cD1b4PTT → Strong
I bet Man U must win this season → ibmumwts → 1bMUmwTss → Strong

ตัวอย่าง Password ที่ดีที่สุดซึ่งยากต่อการถูก Crack เช่น Z3br4&H1Pp01$!
Password ตัวอย่างนี้ ยาว 14 ตัว ซึ่ง 7 ตัวแรกมีอักขระทั้ง 4 แบบ และ 7 ตัวหลังก็เช่นกัน ลองเอา Password นี้ ไปทดสอบที่ Password Checker ของ Microsoft ที่
http://www.microsoft.com/protect/yourself/password/checker.mspx
ก็จะได้ผล = BEST
ซึ่งเทคนิคที่ใช้สร้าง password นี้คือ การใช้ Phrase คือ zebra and hippo is ! (panic) และการแทนที่สระด้วยตัวเลขคือ ใช้ 3 แทน E ใช้ 4 แทน A ใช้ 1 แทน i และใช้ 0 (ศูนย์)แทน O

เทคนิคที่ 5 พิมพ์ไทย ได้อังกฤษ

เทคนิคนี้ให้เรานึกคำหรือวลีที่เป็นภาษาไทย แล้วพิมพ์ลงไปบนแป้นพิมพ์เลยโดยไม่ต้องกดเปลี่ยนมาเป็นภาษาไทย

พีทีทีไอซีที	ก็จะกลายเป็น	rumumuwv:umu
อภิวัฒโนกุล	ก็จะกลายเป็น	v4b;y<Fod6]
สู่ความสำเร็จ	ก็จะกลายเป็น	l^j8;k,legiH0

จะเห็นว่าเรากดแป้นพิมพ์ตัว "อ" เราจะได้เป็นตัว "v" ออกมา (lowercase alphabet)
ถ้ากด "ธ" ก็จะได้เป็นตัว "T" ออกมา (uppercase alphabet)
เพราะใช้โหมดแป้นพิมพ์เป็นภาษาอังกฤษ แต่เวลาพิมพ์เรามองที่ตัวภาษาไทยที่เขียนอยู่บนแป้นพิมพ์ เทคนิคนี้ก็อาจสามารถนำไปประยุกต์ใช้ได้ดีเช่นกัน เนื่องจากภาษาไทยจะมีการยกแคร่ (กด Shift) ซึ่งจะทำให้ได้อักษรภาษาอังกฤษตัวใหญ่ อักขระพิเศษและตัวเลขอยู่ใน password ด้วย

ลองนำเทคนิคเหล่านี้ไปลองประยุกต์ใช้กันดูนะครับ

ไชยกร อภิวัฒโนกุล, CISSP
CSO Ext.1126

"Security depends on everyone"
If every single one acts securely, the whole organization might unavoidably be very secure.
*But if one starts to allow ignorance, the organization will soon become very weak. : **CK***