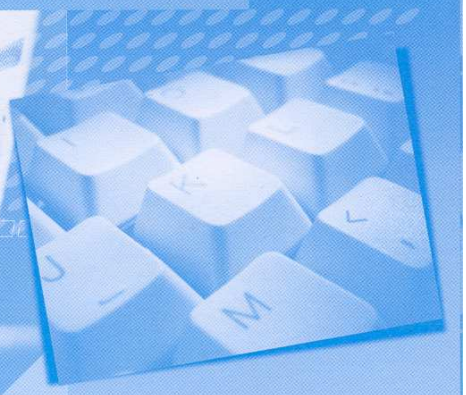


เรื่องของ Password... รหัส (ไม่) ลับ

บทความวิชาการ : คณะวิศวกรรมศาสตร์
อ.เกรียงไกร ลิ่มทอง
อาจารย์ประจำคณะวิศวกรรมศาสตร์

เราคงปฏิเสธไม่ได้ว่าการใช้ชีวิตในปัจจุบันนี้เกี่ยวข้องกับการเข้าไปทำธุรกรรมต่างๆ ที่อยู่ในรูปแบบของธุรกรรมทางอิเล็คโทรนิกส์มากขึ้น เช่น การเช็คอีเมล์ การซื้อขายของผ่านอินเตอร์เน็ต การโอนเงินผ่านธนาคาร เป็นต้น ในการเข้าไปใช้บริการดังกล่าวจำเป็นต้องมีชื่อผู้ใช้ (User Name) และรหัสผ่าน (Password) สำหรับการพิสูจน์ตัวตน (Identication) เพื่อขอเข้าไปใช้บริการ ซึ่งชื่อผู้ใช้และรหัสผ่านอาจถูกกำหนดโดยผู้ให้บริการหรือผู้ใช้งานเป็นคนกำหนดเมื่อลงทะเบียนเพื่อขอใช้งานในครั้งแรก ส่วนใหญ่แล้วชื่อจริงหรือชื่อเล่นของผู้ใช้งานมักจะถูกนำมาตั้งเป็นชื่อผู้ใช้ ปัญหาที่พบมากคือเราจะตั้งรหัสผ่านอย่างไรดี สมมติว่าเราใช้บริการธุรกรรมทางอิเล็คโทรนิกส์ทั้งหมด 20 บริการ ถ้าตั้งรหัสผ่านให้เหมือนกันทั้งหมดเราก็สามารถจำได้ง่าย แต่ถ้าเกิดมีใครรู้รหัสผ่านของเราเขาก็สามารถเข้าไปใช้งานในชื่อของเราได้ทั้งหมด ถ้าตั้งรหัสผ่านให้แตกต่างกันเราก็ต้องหาวิธีตั้งรหัสผ่านให้สามารถจำได้ง่ายและคาดเดาได้ยาก

บทความนี้จึงนำเสนอแนวทางในการตั้งรหัสผ่านที่สามารถจำได้ง่าย คาดเดาได้ยาก และสามารถเปลี่ยนรหัสผ่านได้บ่อยตามที่เราต้องการหลายๆ ท่านคงทราบถึงรหัสผ่านที่ควรหลีกเลี่ยงไม่ควรนำไปใช้ เช่น คำในพจนานุกรม เบอร์โทรศัพท์ วันเดือนปีเกิด เป็นต้น อีกทั้งคงทราบถึงการตั้งรหัสผ่านที่ควรนำไปใช้ เช่น ควรประกอบด้วยตัวอักษร ตัวเลขอักขระพิเศษเป็นต้นเรามาดูกันดีกว่าว่าถ้าต้องการตั้งรหัสผ่านให้ได้อย่างที่ว่านั้นมีขั้นตอนอย่างไร

ขั้นตอนการตั้งรหัสผ่านให้แข็งแกร่ง (Strong Password)

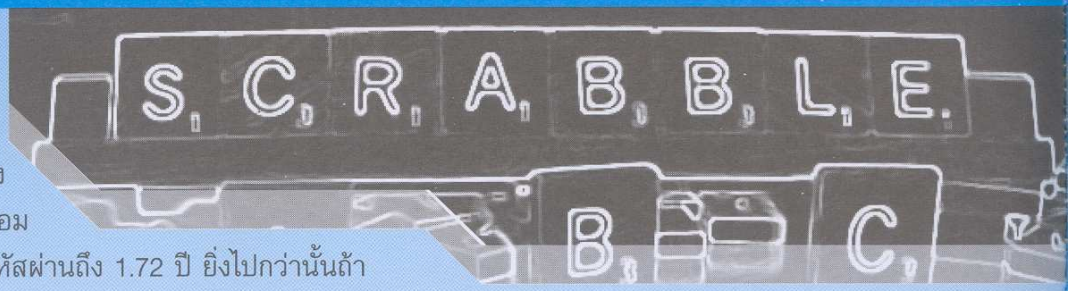
1. สร้างประโยคที่สามารถจำได้ง่าย ควรสร้างประโยคที่มีอย่างน้อย 8 พยางค์ ตัวอย่างเช่น “My favorite website is Google” เห็นได้ว่าประโยคที่สร้างขึ้นมานั้นมี 29 ตัวอักษร (รวมช่องว่าง) มี 9 พยางค์และมีคำทั้งหมด 5 คำ

2. ตรวจสอบว่าเครื่องคอมพิวเตอร์หรือระบบที่จะนำรหัสผ่านไปใช้งานสามารถรองรับรหัสผ่านที่เป็นประโยคโดยมีช่องว่างระหว่างคำได้หรือไม่ ถ้ารองรับได้ก็สามารถนำประโยคดังกล่าวไปใช้เป็นรหัสผ่านได้เลย หลายคนอาจสงสัยว่า “อ้าว... ไหนบอกว่าไม่ควรใช้คำในพจนานุกรมและต้องประกอบด้วยตัวอักษร ตัวเลขและอักขระพิเศษ” ในกรณีนี้เราสามารถนำข้อความที่เป็นประโยคไปใช้เป็นรหัสผ่านได้เพราะว่าประโยคดังกล่าวมีความยากในการเดารหัสผ่านแบบทุกกรณีที่เป็นไปได้ (Brute Force Attack) เนื่องจากประโยคจะมีความยาวของตัวอักษรมากได้มีการทดสอบแล้วว่าเวลาที่ใช้ในการเดารหัสผ่านแบบทุกกรณีที่เป็นไปได้โดยใช้คอมพิวเตอร์คำนวณนั้นใช้เวลาดังแสดงในตารางที่ 1

จำนวนตัวอักษรในรหัสผ่าน	จำนวนตัวอักษรทั้งหมดที่สามารถเลือกนำมาเป็นรหัสผ่านได้		
	26 ตัวอักษร(ตัวพิมพ์เล็กเท่านั้น – abc)	36 ตัวอักษร (ตัวพิมพ์เล็กและตัวเลข – abc123)	52 ตัวอักษร (ตัวพิมพ์เล็กและตัวพิมพ์ใหญ่ AaBbCc)
5	1.98 นาที	10.1 นาที	1.06 ชั่วโมง
6	51.5 นาที	3.74 ชั่วโมง	13.7 วัน
7	22.3 ชั่วโมง	9.07 วัน	3.91 เดือน
8	24.2 วัน	10.7 เดือน	17.0 ปี
9	1.72 ปี	32.2 ปี	8.82 ศตวรรษ
10	44.8 ปี	1.16 สหัสวรรษ	45.8 สหัสวรรษ
11	11.6 ศตวรรษ	41.7 สหัสวรรษ	2,384 สหัสวรรษ
12	30.3 สหัสวรรษ	1,503 สหัสวรรษ	123,946 สหัสวรรษ

ตารางที่ 1 เวลาที่ใช้ในการเดารหัสผ่านทุกกรณีที่เป็นไปได้ด้วยคอมพิวเตอร์

ตารางที่ 1 แสดงให้เห็นว่าถ้าเราใช้ตัวอักษรตัวเล็กเพียงอย่างเดียว 5 ตัวอักษรมาตั้งเป็นรหัสผ่านคอมพิวเตอร์สามารถเดารหัสผ่านได้ภายในเวลา 1.98 นาที



แต่ถ้าใช้ตัวอักษรเล็กเพียงอย่างเดียว 9 ตัวอักษร คอมพิวเตอร์ต้องใช้เวลาเดารหัสผ่านถึง 1.72 ปี ยิ่งไปกว่านั้นถ้าใช้ตัวอักษรตัวเล็กและตัวอักษรตัวใหญ่ปนกัน 9 ตัวอักษร คอมพิวเตอร์ต้องใช้เวลาเดารหัสผ่านมากถึง 8.82 ศตวรรษ ดังนั้นเราสามารถนำเอาประโยคที่มีทั้งตัวอักษรตัวเล็ก ตัวอักษรตัวใหญ่และช่องว่างปนกันมาใช้เป็นรหัสผ่านได้อย่างแน่นอนซึ่งทำให้เราสามารถจำได้ง่ายและยากต่อการเดารหัสผ่าน

3. ถ้าคอมพิวเตอร์หรือระบบไม่รองรับรหัสผ่านที่เป็นประโยค ให้เปลี่ยนประโยคดังกล่าวเป็นรหัสผ่าน โดยใช้อักษรแรกของแต่ละพยางค์ในประโยคมาสร้างเป็นรหัสผ่าน และเปลี่ยนให้ใช้ตัวอักษรตัวเล็กทั้งหมด จากตัวอย่างในข้อแรกเราจะได้ “mfvrwsigg”

4. เพิ่มความซับซ้อนเข้าไปในรหัสผ่านโดยการเปลี่ยนอักษรแรกของคำในประโยคให้เป็นตัวอักษรใหญ่ จากตัวอย่างเราจะได้ “MFvrWsIGg”

5. แทนตัวอักษรบางตัวด้วยอักขระพิเศษหรือตัวเลขที่ดูคล้ายตัวอักษรนั้น โดยเราสามารถดูได้จากตารางที่ 2 ประกอบเพื่อการสร้างรหัสผ่านให้ซับซ้อนมากขึ้นได้ จากตัวอย่างเราจะได้ “MFvrW$!G9”

อักขระพิเศษและตัวเลข	@	4	6	8	(	3	9	!	1	0	$	+	2
ตัวอักษร	a	A	b	B	c,C	e,E	g	i,I	l,L	o,O	s,S	t,T	z,Z

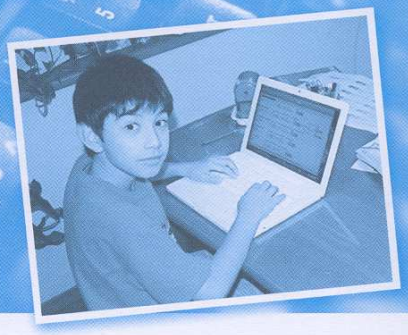
ตารางที่ 2 อักขระพิเศษและตัวเลขที่มีรูปร่างคล้ายตัวอักษร

6. ตรวจสอบความแข็งแกร่งของรหัสผ่าน โดยตรวจสอบผ่านเว็บไซต์ที่ให้บริการการตรวจสอบรหัสผ่าน เช่น http://www.passwordmeter.com เป็นต้น เพื่อให้มั่นใจว่ารหัสผ่านที่เราสร้างขึ้นมานั้นมีความแข็งแกร่งและไม่สามารถเดาได้ง่ายเห็นว่าจากวิธีดังกล่าวเราสามารถสร้างรหัสผ่านที่เราจำได้ง่าย มีความแข็งแกร่งสูงและยากต่อการคาดเดา ซึ่งถ้าต้องการเปลี่ยนรหัสผ่านบ่อยๆ ก็สามารถทำได้โดยเพิ่มคำต่อท้าย (Sufx) เข้าไป เช่นจากตัวอย่างเพิ่มคำต่อท้ายเข้าไปเป็น “MfvrW$!G9__Q305” ซึ่งคำต่อท้ายที่เพิ่มเข้าไปหมายถึง ไตรมาสที่ 3 ปี 2005 หรือจากตัวอย่างเพิ่มคำต่อท้ายเข้าไปเป็น “MfvrW$!G9__J@n05” ซึ่งคำต่อท้ายที่เพิ่มเข้าไปหมายถึงเดือน มกราคม ปี 2005 เป็นต้น

หลายคนคงเคยได้ยินว่าเราสามารถพิมพ์รหัสผ่านภาษาไทยโดยไม่กดแป้นเปลี่ยนภาษา เช่น คำว่า “รหัสผ่าน” ก็กลายเป็น “isylzjko” หรือคำว่า “กูเกิล” ก็จะกลายเป็น “d^gdb]” เป็นต้นแต่สิ่งที่ควรระวังคือปัจจุบันได้มีการเปลี่ยนคำในพจนานุกรมภาษาไทยให้เป็นภาษาอังกฤษแล้ว ดังนั้นจึงไม่เป็นการยากเลยสำหรับการคาดเดารหัสผ่านดังกล่าวด้วยคอมพิวเตอร์ หรือถ้าไม่อยากสร้างรหัสผ่านด้วยตัวเอง ปัจจุบันมีเว็บไซต์บริการสร้างรหัสผ่านให้ เช่น http://strongpasswordgenerator.com เป็นต้น

ขั้นตอนดังกล่าวเป็นเพียงแนวทางที่นำไปใช้ในการสร้างรหัสผ่านซึ่งท่านสามารถดัดแปลงให้เป็นแนวทางของท่านเองได้ ไม่มีการกำหนดตายตัวว่าต้องเป็นตามขั้นตอนที่กล่าวมาแล้วเท่านั้น

หวังว่าท่านคงมีความสุขมากขึ้นกับการสร้างรหัสผ่านใหม่ ๆ ที่สามารถจำได้ง่ายและคาดเดาได้ยาก แต่สิ่งที่สำคัญคือควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 3 เดือนนะครับ



ข้อมูลประกอบ :

http://www.bu.ac.th/hotnews/apr__june46/password/

http://www.cuhk.edu.hk/itsc/security/gpis/guidestrongpw.html

http://www.passwordmeter.com/

http://strongpasswordgenerator.com/