SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 3 ฉบับที่ 19 ประจำเดือน มีนาคม 2554

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

จดหมายข่าวฉบับนี้มาพร้อมกับการเปิดตัว SRAN Comics การ์ตูนเผยแพร่ความรู้ด้าน IT Security ที่ทางทีมงาน SRAN ตั้งใจจัดทำขึ้น ซึ่งสามารถติดตามได้ทาง Facebook อีกช่องทางหนึ่ง ที่ Fan Page : Global Technology Integrated Co., Ltd ค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

In This Issue:

- ฟรีอีเมล์...ภัยแฝงใกล้ตัว หน้า 1-2
- Message from SRAN (PROMOTION) หน้า 1
- SRAN Comics หน้า 3

ฟรีอีเมล์...FREE ภัยแฝงใกล้ตัว

คดีด้านอาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้นบ่อยครั้งในปัจจุบันนั้น คดีหนึ่งที่หลายคนคงเคยประสบเข้ากับตนเองหรือคนใกล้ชิดก็คือถูกมิจฉาชีพแฮกข้อมูลอีเมล์ส่วนตัวแล้วเปลี่ยนรหัสผ่านก่อนนำอีเมล์ดังกล่าวส่งข้อความไปยังคนรู้จักที่อยู่ในรายชื่อผู้ติดต่อในอีเมล์นั้น บรรยายข้อความหลอกลวงสารพัดรูปแบบโดยมีเป้าหมายเพื่อล่อลวงทรัพย์จากผู้หลงเชื่อ หรือบางกรณี...

อ่านต่อหน้า 2

กำหนดการฝึกอบรมการใช้งาน SRAN **ฟรี!** สำหรับลูกค้าและตัวแทนจำหน่าย ประจำปี 2554

2011	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
Red Course : SRAN Security Center	17	21	19	16	21	18	22	20	17	15
Red Course : SRAN Light	18	22	20	17	22	19	23	21	18	16
Advanced SRAN Technique Course	15-16	19-20	26-27	14-15	28-29	16-17	20-21	27-28	15-16	22-23

PROMOTION! "ซอฟต์แวร์ไทย ลุ้นรถ ลุ้นโชค ครั้งที่ 4"

สิทธิพิเศษสำหรับลูกค้า **SRAN**
เมื่อซื้อผลิตภัณฑ์ **SRAN**
รุ่นใดก็ได้ ทุกๆ 2,500 บาท จะได้รับคูปองชิงรางวัล 1 ใบ เพื่อชิงโชคในโครงการซอฟต์แวร์ไทย ลุ้นรถ ลุ้นโชค ครั้งที่ 4 ตั้งแต่วันนี้ ถึง 31 พฤษภาคม 2554

- *รางวัลที่ 1 รถยนต์ Nissan March รุ่น 1.2 E CVT*
- *รางวัลที่ 2 Notebook SVOA รุ่น Cleo 133W*
- *รางวัลที่ 3 Printer EPSON รุ่น TX220*

และของรางวัลอีกมากมาย รวมมูลค่ากว่า 700,000 บาท

พิเศษ ! สำหรับลูกค้าที่ต่อ MA รับคูปองเพิ่ม 2 เท่า !

ฟรีอีเมล์...ภัยแฝงใกล้ตัว

คดีด้านอาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้นบ่อยครั้งในปัจจุบันนั้น คดีหนึ่งที่หลายคนคงเคยประสบเข้ากับตนเองหรือคนใกล้ชิดก็คือ ถูกมิจฉาชีพแฮกข้อมูลอีเมล์ส่วนตัวแล้วเปลี่ยนรหัสผ่าน ก่อนนำอีเมล์ดังกล่าวส่งข้อความไปยังคนรู้จักที่อยู่ในรายชื่อผู้ติดต่อในอีเมล์นั้น บรรยายข้อความหลอกลวงสารพัดรูปแบบโดยมีเป้าหมายเพื่อล่อลวงทรัพย์จากผู้หลงเชื่อ หรือบางกรณีมิจฉาชีพอาจนำอีเมล์ที่แฮกมาไปใช้เพื่อการอื่น เช่น ส่งข้อความว่าร้ายหรือหมิ่นประมาทบุคคลอื่น เป็นต้น ซึ่งการกระทำในลักษณะนี้สามารถอำพรางตัวตนของผู้กระทำความผิดที่แท้จริงได้

คำถามที่ได้ยินบ่อยครั้งคือ ผู้ไม่ประสงค์ดีเหล่านั้นทำได้อย่างไร? ต้องใช้เทคนิคชั้นสูง หรือเครื่องมือพิเศษใดช่วยในการแฮกหรือไม่? คำตอบคือ ใช่หรือไม่ก็ได้ เพราะการจะแฮกอีเมล์ใดอีเมล์หนึ่งนั้นสามารถใช้เทคนิคชั้นสูงในการแฮก เช่น การปล่อยมัลแวร์เข้าเครื่องคอมพิวเตอร์ เพื่อทำการรันโปรแกรมประเภท keylogger แล้วทำการเก็บค่า password ของเหยื่อ หรืออาจสุ่มเลือกอีเมล์ของเหยื่อมาสักรายแล้วทำการรันโปรแกรมแฮกอีเมล์ที่มีแจกกันอย่างแพร่หลายในอินเทอร์เน็ตก็ได้ แต่วิธีการเหล่านี้มักสิ้นเปลืองเวลาและทรัพยากร ดังนั้นแฮกเกอร์ทั่วไปจึงมักจะเลือกใช้วิธีการที่ง่ายกว่า **เพียงมีคอมพิวเตอร์เพียงเครื่องเดียวบวกกับอินเทอร์เน็ต ก็สามารถแฮกได้แล้ว...!!!**

วิธีการง่ายๆ ที่พวกเขาใช้กันคือ เลือกอีเมล์ของเหยื่อ ซึ่งอาจได้มาจาก forward mail ที่ได้รับจากเพื่อนๆ ซึ่งมักมีอีเมล์ของคนอื่นๆ ที่เป็น free e-mail แนบมาด้วยเป็นหางว่าว จากนั้นก็ลองพยายาม login ด้วยอีเมล์นั้นๆ ดู ยกตัวอย่างเช่น xxx.th@hotmail.com เมื่อเปิดเข้าหน้า login แล้ว แทนที่จะคาดเดารหัสผ่านโดยตรง ก็อาจใช้วิธีกดเลือกตรงที่ให้แจ้ง "ลืมรหัสผ่าน" แทน ซึ่งเหยื่อหลายๆ คนมักจะเลือกป้องกันการลืมรหัสผ่านด้วยการตั้งคำถามและคำตอบเพื่อให้ผู้ให้บริการ Free e-mail ทำการ reset รหัสผ่านให้ เมื่อแฮกเกอร์รู้ว่าเหยื่อตั้งคำถามใดในการ reset รหัสผ่านแล้วขั้นตอนต่อไปก็เพียงแค่ใช้ google ในการหาคำตอบให้เท่านั้นเอง ยิ่งเหยื่อนิยมใช้ social network มากเท่าใด ข้อมูลส่วนตัวก็จะยิ่งหลุดไปถึงมือแฮกเกอร์ได้สะดวกและง่ายดายมากเท่านั้น

กรณี xxx.th@hotmail.com สมมุติว่าเจ้าของอีเมล์กำหนดคำถามในการ reset รหัสผ่านว่า "ชื่อสัตว์เลี้ยงของฉัน?" เมื่อแฮกเกอร์ไปลองค้นหาใน google แล้วพบ blog ของนาย xxx.th หรืออาจเป็น social network ต่างๆ เช่น **facebook, twitter** ซึ่งมีการพูดถึงชื่อสัตว์เลี้ยงของนาย xxx.th ไว้ด้วย เพียงเท่านี้แฮกเกอร์ก็จะพบคำตอบและนำไป**ใช้แฮก free-email** ดังกล่าว**ได้อย่างง่ายดาย**

ดังที่กล่าวไว้ข้างต้น ยิ่งเราแชร์ความเป็นตัวตนของเราให้คนอื่นรับรู้ผ่านทาง social network มากเท่าใด โอกาสที่เราจะตกเป็นเหยื่อบนโลกออนไลน์ก็ยิ่งมากขึ้นเป็นเงาตามตัว ไม่เฉพาะเรื่องของอีเมล์เท่านั้น แต่ยังครอบคลุมถึงการทำธุรกรรม e-banking หรือ e-commerce อื่นๆ ด้วยเช่นกัน เพราะการจะตรวจสอบตัวตนของเรานั้นผู้ให้บริการมักอาศัยข้อมูลส่วนบุคคลเป็นตัวยืนยัน หากเราเปิดเผยข้อมูลส่วนตัวของเราให้ผู้อื่นรับทราบทั่วไปแล้ว ภัยร้ายก็อาจมาถึงตัวเราได้โดยไม่คาดคิด

SRAN comics

ตอนที่ 1

ตั้งสติ..ก่อนเปิดเครื่อง