SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 1 ฉบับที่ 1 ประจำเดือน กุมภาพันธ์ 2552

--- EDITOR'S TALK ---

เปิดศักราชใหม่ 2552 ทางทีมงาน บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด ตั้งใจมอบสิ่งดีๆ ให้ทุกท่าน จึงคิดทำ **SRAN e-Newsletter** ขึ้น เพื่อเผยแพร่ความรู้ด้าน IT Security ทั้งในมุมมองด้านเทคโนโลยี ภัยคุกคาม และแนวทางปฏิบัติเพื่อความปลอดภัยของข้อมูลสารสนเทศ โดยตั้งหวังให้ผู้อ่านรู้เท่าทันและสามารถป้องกันภัยร้ายที่แฝงเร้นเข้ามาในโลกไซเบอร์ได้

สำหรับฉบับแรกนี้ เปิดตัวด้วยเรื่องราวเกี่ยวกับ **ธุรกรรมออนไลน์** ที่เข้ามามีบทบาทต่อชีวิตประจำวันของเราๆ ท่านๆ มากขึ้นทุกขณะ นำเสนอด้วยบทความของบริษัทฯ ที่ตีพิมพ์ในหนังสือพิมพ์สยามธุรกิจ ฉบับวันที่ 26-28 พฤศจิกายน 2551 ผนวกข้อมูลเสริมด้านการ **ป้องกันอย่างรู้เท่าทัน** และการรับมือภัยคุกคาม เพื่อมุมมองที่ชัดเจนในการป้องกันปัญหาที่เกิดจากการทำธุรกรรมทางอินเตอร์เน็ต

หากมีข้อเสนอแนะติดต่อได้ที่
info@gbtech.co.th **ค่ะ**

กฤตยา รามโกมุท
บรรณาธิการ

ธุรกรรมออนไลน์ ภัยร้าย! แฝงเงามืด

เมื่อหลายเดือนก่อนได้เกิดคดีที่เกี่ยวข้องกับการทำธุรกรรมทางอินเตอร์เน็ต โดยผู้เสียหายได้ใช้บริการ Internet Banking และตกเป็นเหยื่อโดยไม่รู้ตัว ซึ่งเมื่อตรวจสอบพบว่ามีผู้ดักข้อมูลโดยใช้โปรแกรม Key Logger ซึ่งคอยเก็บข้อมูลจากแป้นคีย์บอร์ดขณะใช้งานและส่งผ่านระบบอินเตอร์เน็ตให้กับแฮกเกอร์ ซึ่งนำข้อมูลที่ได้สวมรอยเป็นผู้ใช้งาน เข้าทำธุรกรรมทางการเงิน สร้างความเสียหายมูลค่าไม่น้อย เหตุการณ์นี้สามารถป้องกันได้ หากผู้ใช้งานและผู้ให้บริการระบบธุรกรรมออนไลน์ตระหนักและรู้เท่าทันภัยคุกคาม ตลอดจนเสริมสร้างเทคโนโลยีให้ปลอดภัยมากยิ่งขึ้น . . . .

อ่านต่อ...หน้า 2

ป้องกัน อย่างรู้เท่าทัน

เมื่อการทำธุรกรรมออนไลน์ ไม่ว่าจะเป็นการซื้อขายสินค้าหรือบริการทางอินเตอร์เน็ต, การทำธุรกรรมทางการเงินผ่านเว็บไซต์ธนาคาร เข้ามามีบทบาทในชีวิตประจำวันของผู้คนมากขึ้น จึงจำเป็นอย่างยิ่งที่ต้องให้ความสำคัญกับการพิสูจน์ตัวตนผู้ใช้งาน ซึ่งถือเป็นด่านแรกของการเข้าใช้งานระบบออนไลน์ เพื่อตรวจสอบให้แน่ชัดว่าเป็นบุคคลผู้นั้นจริง การพิสูจน์ตัวตนสามารถทำได้หลายรูปแบบ เช่น การใช้รหัสผ่าน, PIN Code, ระบบ Token, ลักษณะเฉพาะทางชีวภาพ, การเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-Key Cryptography) เป็นต้น ...

อ่านต่อ...หน้า 3

ในปัจจุบันแฮกเกอร์ไม่ได้มีเป้าหมายเจาะระบบเครือข่ายธนาคารหรือผู้ให้บริการธุรกรรมออนไลน์ เพื่อเข้าถึงชั้นความลับของลูกค้าเพียงอย่างเดียว แต่เปลี่ยนเป้าหมายเป็นผู้ใช้งาน (User) อินเตอร์เน็ต ซึ่งเข้าถึงได้ง่ายกว่าแทนโดยอาศัยความ **รู้เท่าไม่ถึงการณ์**

บทความตีพิมพ์ใน ICT FORUM
หนังสือพิมพ์ สยามธุรกิจ
ฉบับวันที่ 26-28
พฤศจิกายน 2551

ต่อจากหน้า 01

ธุรกรรมออนไลน์... ภัยร้ายแฝงเงามืด

เนื่องจากมีการใช้งานอินเตอร์เน็ตอย่างทั่วถึงมากยิ่งขึ้นบางครั้งผู้ใช้งานอาจพยายามดาวน์โหลดโปรแกรมหรือข้อมูลบางอย่างที่แฮกเกอร์ได้เผยแพร่ไว้ตามเว็บสาธารณะยอดนิยม โดยโปรแกรมดังกล่าวมักมีชื่อที่ดึงดูดให้ดาวน์โหลด เช่น clip ฉาว, โปรแกรมเร่งความเร็ว, โปรแกรม crack serial number, โปรแกรมเกมส์ เป็นต้น เมื่อผู้ใช้งานหลงดาวน์โหลดโปรแกรมดังกล่าวมาติดตั้งในเครื่อง อาจมีมัลแวร์แฝงมากับไฟล์ ทำให้ผู้ใช้ตกเป็นเหยื่อมิจฉาชีพที่จ้องดักข้อมูลได้

ในแง่ผู้ใช้งานทั่วไป : ต้องป้องกันภัยคุกคามที่เกิดขึ้นโดยตระหนักรู้ และควบคุมพฤติกรรมตนเองในการใช้งานอินเตอร์เน็ตบนเครื่องคอมพิวเตอร์ส่วนตัว, ไม่ดาวน์โหลดโปรแกรมที่ไม่มั่นใจในความปลอดภัย, หมั่นดูแลเครื่องคอมพิวเตอร์ให้มีการอัพเดททั้งซอฟต์แวร์ป้องกัน และ Patch, ตั้งรหัสผ่านที่ยากต่อการคาดเดา หากต้องทำธุรกรรมทางอินเตอร์เน็ต เช่น ซื้อสินค้า หรือทำธุรกรรมทางการเงินให้ทำบนเครื่องตนเองที่คิดว่าปลอดภัยแล้ว เลือกช่องทางการใช้งานให้ถูกต้อง เช่น เมื่อมีการ Login ผ่านเว็บไซต์ให้ดูว่าเป็นการผ่าน HTTPS หรือไม่ หากไม่ใช่ก็ไม่ควรใช้ โดยเฉพาะหากอยู่ในวง LAN ไม่ว่าจะเป็นร้านอินเตอร์เน็ตคาเฟ่ หรือบริษัท เพราะอาจมีการดัก User / Password ผ่านระบบเครือข่ายได้ และควรเลือกใช้บริการธุรกรรมอินเตอร์เน็ตจากผู้ให้บริการที่น่าเชื่อถือเท่านั้น

ในแง่ผู้ให้บริการ : ผู้ให้บริการต้องให้ความสำคัญกับเทคโนโลยีในการระบุตัวตน ผู้ใช้งาน, ดูแลความปลอดภัยของข้อมูลและวิธีการใช้งานเมื่อลูกค้าต้องทำธุรกรรมผ่านระบบอินเตอร์เน็ต ตลอดจนให้ความรู้แก่ลูกค้าให้รู้เท่าทันภัยคุกคามในปัจจุบัน

ในที่นี้ผมขอเน้นเรื่องการใช้เทคโนโลยีการพิสูจน์ตัวตนของลูกค้าที่ทำธุรกรรม ผ่านอินเตอร์เน็ต ซึ่งที่ใช้กันอยู่มีสามรูปแบบคือ

- สิ่งที่คุณมี (Something you have) เช่น กุญแจไขประตู, บัตรอิเล็กทรอนิกส์ หรือระบบ Token เป็นต้น
- สิ่งที่คุณรู้ (Something you know) คือ รหัสผ่านหรือชุดตัวเลขเฉพาะ
- สิ่งที่คุณเป็น (Something you are) เป็นการพิสูจน์ตัวตนแบบชีวมาตร เช่น ลายนิ้วมือ ระบบรู้จำเสียง ระบบสแกนม่านตา เป็นต้น

อย่างไรก็ดี ผู้ให้บริการด้านพาณิชย์อิเล็กทรอนิกส์ เช่น สถาบันการเงิน, ผู้ประกอบธุรกิจ E-Commerce ควรนำเทคโนโลยีการพิสูจน์ตัวตนแบบ Two-Factor Authentication มาใช้เป็นอย่างน้อย ตลอดจนให้ความรู้แก่ลูกค้าในการทำธุรกรรมผ่านระบบอินเตอร์เน็ต เพื่อไม่ให้ตกเป็นเหยื่อพวกมิจฉาชีพที่นับวันจะมีวิธีการที่ซับซ้อนแยบยลขึ้นทุกที