ปอท. แจก คาถากันภัยผู้ใช้อีเมล์และเฟสบุ๊ค ป้องหลอกโอนเงิน: ห้ามโง่ ห้ามซื่อ ห้ามขี้เกียจ

พล.ต.ต.ศุภเศรษฐ์ โชคชัย ผู้กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กล่าวถึงภัยออนไลน์ว่าในระยะเวลา3 เดือนผ่านมา คนไทยโดนแฮ็ก เฟสบุ๊คและอีเมล์ และสร้างความเสียหาย โดยถูกหลอกโอนเงินกว่ายี่สิบล้านบาท ส่วนวิธีที่คนร้ายใช้ในการหลอกขโมย PASSWORD สำหรับแฮ็กเฟสบุ๊คนั้นมี 3 วิธี 1.คือเดาจากเลขวันเดือนปีเกิด หรือเบอร์โทรศัพท์ และเหยื่อการเดา PASSWORD จะเป็นผู้สูงอายุหรือผู้ที่มีอายุตั้งแต่ 40 ปี ขึ้นไป เนื่องจากมักตั้ง PASSWORD เป็นวันเดือนปีเกิดและเบอร์โทรศัพท์เพื่อกันลืม ซึ่งเป็นการง่ายที่คนร้ายจะสามารถหาข้อมูลเหล่านี้ได้บนอินเตอร์เน็ต 2. สร้างหน้าเพจปลอมขึ้นมา แล้วแจ้งว่า PASSWORD ของท่านกำลังจะหมดอายุ หรือแจ้งว่ามีคนร้ายกำลังจะแฮ็ก เฟสบุ๊ค เพื่อความปลอดภัยให้คลิกไปตามลิงค์ที่ให้มาเพื่อทำการเปลี่ยน PASSWORD ใหม่ โดยเมื่อหลงกลคลิกไปตามลิงค์หน้าเพจปลอมนั้น ก็จะให้เราใส่ PASSWORD อันใหม่ 3. คนร้ายจะปล่อย SPYWARE เข้าเครื่องคอมพิวเตอร์ โดยที่ SPYWARE นั้นทำลายระบบ และเข้าถึงข้อมูลในคอมพิวเตอร์ ทำให้คนร้ายรู้ PASSWORD ได้ทันที

สำหรับการแฮ็กเฟสบุ๊ค สิ่งที่สร้างความเสียหายคือ โจรจะสวมรอยเป็นเจ้าของเฟสบุ๊ค และส่งข้อความหาเพื่อนๆ ญาติๆว่ากำลังเดือดร้อน หรือต้องการใช้เงินด่วนให้โอนเงินไปให้ตามเลขที่บัญชีที่โจรให้มา ถ้าเกิดหลงเชื่อขึ้นมา พวกเขาต้องมาสูญเสียเงินมากมายให้โจรไป ซึ่งปัจจุบันมีประชาชนตกเป็นเหยื่อจำนวนมาก

จึงขอเตือนประชาชนว่าห้ามตั้ง PASSWORD เป็นหมายเลขดังกล่าวเด็ดขาด งดข้อมูล PASSWORD ในหน้าเพจที่ส่งมาหรือตามลิงค์ต่างๆ หากต้องการเปลี่ยน PASSWORD สิ่งที่ควรทำคือการเข้าไปที่เว็ปไซต์ของเฟสบุ๊กโดยตรง เพื่อเปลี่ยนแปลงข้อมูลคือ และท้ายสุดให้ไปตั้งค่าระบบความปลอดภัยของเฟสบุ๊ค ซึ่งได้มีรองรับ และหากมีเพื่อนเฟสบุ๊คมาหาและบอกให้เราโอนเงินให้ไม่ว่าจะด้วยเหตุผลอะไรก็ตาม ต้องโทรเช็คเจ้าตัวโดยตรงทุกครั้งว่าข้อความที่ส่งมาเป็นของเขาจริงหรือเปล่า

สำหรับการแฮ็กอีเมลล์นั้น ส่วนใหญ่ผู้เสียหายจะเป็นบริษัทที่ต้องติดต่อซื้อขายกับต่างประเทศทางอีเมลล์ เมื่อแฮ็กไปเข้าอีเมล์แล้ว โจรจะเฝ้าดูการโต้ตอบอีเมล์อย่างใจเย็น รอจนถึงเวลาที่สั่งสินค้า และโอนเงินค่าสินค้าไปให้บริษัทนั้น จังหวะนี้โจรจะสวมรอย ส่งอีเมล์มาแจ้งว่าบริษัทได้เปลี่ยนบัญชีรับโอนเงินเป็นบัญชีใหม่ ซึ่งแท้จริงแล้วก็คือบัญชีของโจรนั่นเอง

สิ่งจำเป็นอย่างยิ่งที่ต้องไปตั้งค่าความปลอดภัยเพิ่มเติมในกรณีนี้คือ ต้องใส่รหัสพิเศษอีกตัวที่ทางผู้ให้บริการอีเมล์ เช่น GMAIL, HOTMAIL หรือ YAHOO จะส่งมาให้ทางมือถือทาง SMS เพื่อใส่ควบคู่กับ PASSWORD ไปด้วย โดยรหัสนี้ (รหัส OTP) จะถูกส่งมายังมือถือเท่านั้นทำให้บุคคลอื่นไม่สามารถเข้าอีเมล์ของคุณได้แน่นอน ซึ่งระบบความ

ปลอดภัย 2 ชั้นแบบนี้ ค่ายอีเมล์ต่างๆมีให้ทุกคนได้ใช้ฟรี แค่สละเวลาเพียงสองสามนาที การทำธุรกิจก็จะปลอดภัยขึ้น

หากบริษัทที่เคยซื้อของกันเป็นประจำอยู่แล้ว ส่งอีเมล์มาแจ้งว่าบริษัทได้เปลี่ยนเลขที่บัญชีในการโอนเงินเป็นอีกบัญชีหนึ่ง แล้วบอกให้เราโอนเงินค่าสินค้าที่จะซื้อไปยังบัญชีใหม่แทน ห้ามเชื่อเด็ดขาด ต้องได้รับการยืนยันทางโทรศัพท์เท่านั้นถึงจะมั่นใจได้ว่าจะไม่ถูกหลอก เพราะมีความเป็นไปได้สูงว่าอีเมล์ที่ได้รับไม่ได้มาจากบริษัท แต่มาจากคนร้ายนั่นเอง

ดังนั้นเพื่อป้องกันผู้ประกอบการจากการตกเป็นเหยื่ออีเมล์สแกม กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีจึงได้ร่วมมือทุกธนาคาร โดยส่งวิทยากรเจ้าหน้าที่เข้าไปอบรมพนักงานธนาคารที่เกี่ยวข้อง ทั้งในด้านระบบเทคโนโลยีสารสนเทศ การโอนเงินต่างประเทศ และการบริการลูกค้า เพื่อให้นำความรู้ไปแนะนำลูกค้า โดยเนื้อหาในการอบรมจะครอบคลุมถึงทุกมิติของการหลอกลวงทางอีเมล์ ทั้งนี้เพื่อเป็นการยกระดับการให้บริการของธนาคารในการดูแลลูกค้าต่อไป

หากประชาชนต้องการใช้ชีวิตในโลกออนไลน์ได้อย่างปลอดภัย โดยไม่ตกเป็นเหยื่อหลอกโอนเงินนั้น มีคาถาสั้นๆอยู่เพียง 3 ข้อที่อยากให้จำไว้เสมอ คือ 1. ห้ามมึน คืออย่าเป็นเพียงผู้ใช้เพียงอย่างเดียวโดยไม่สนใจหาความรู้ในการป้องกันตัวเองเลย ประชาชนต้องคอยหาความรู้ใหม่ๆอยู่เสมอทั้งในเรื่องการป้องกัน และอาชญากรรมใหม่ๆที่เกิดขึ้น 2. ห้ามซื่อ เนื่องจากคนร้ายมีวิธีการหลอกลวงต่างๆมากมายเพราะฉะนั้นต้องหัดเป็นคนช่างสังเกตและไม่เชื่ออะไรง่ายๆ เพราะแทบทุกสิ่งในโลกออนไลน์นั้นสามารถปลอมได้หมด และ 3.อย่าขี้เกียจ นั่นคือถ้าหากผู้ให้บริการต่างๆมีระบบความปลอดภัยอะไรมาให้ใช้ ต้องใช้ให้หมด อย่าขี้เกียจไปตั้งค่าความปลอดภัย ทั้งที่จริงแล้วใช้เวลาเพียงไม่เกิน 5 นาที ดีกว่าต้องเสียเงินมากมายให้คนร้ายไป