เฝ้าระวังข้อมูลทางการเงินบนโลก Online

ต่อ จากฉบับที่แล้ว

วิชญ์ฤทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ซึ่งสำหรับประเทศไทยจะแตกต่างกันตรง ยังไม่มีการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเต็มรูปแบบเป็นรูปธรรม ซึ่งพอกฎหมายออกมาผู้ให้บริการก็จะมีการแจ้งข้อความขออนุญาตจากผู้ใช้ ให้ทำการยอมรับในการที่ผู้ให้บริการจะขอจัดเก็บข้อมูลส่วนบุคคล และชี้แจงว่าจะนำข้อมูลไปใช้ในเรื่องใดบ้างอย่างเป็นกิจลักษณะมากขึ้น มีกระบวนการดูแลรักษาความปลอดภัยของข้อมูลเป็นไปตามที่กฎหมายกำหนด โดยจะถือว่าผู้ใช้บริการได้รับทราบ และยอมรับเงื่อนไขดังกล่าวแล้ว ถ้ามีความเสียหายเกิดขึ้นก็ให้พิสูจน์ทราบว่าอยู่ในเงื่อนไขที่ผู้ให้บริการต้องรับผิดชอบหรือไม่ แต่ถ้าไม่อยู่ในเงื่อนไข หรือเกิดจากผู้ใช้บริการละเลยคำแนะนำ ข้อควรปฏิบัติในการใช้บริการ หรือเพิกเฉยต่อการแจ้งเตือนจากผู้ให้บริการแล้ว ก็จะกลายเป็นความรับผิดชอบของผู้ให้บริการเองไปโดยปริยาย อาทิ การดูแลความปลอดภัยของบัญชีผู้ใช้ การเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ การไม่เผยแพร่ข้อมูลอันจะนำไปสู่การถูกลักลอบเข้าใช้งานบัญชี หรือเอาไปใช้เพื่อยืนยันตัวตนสวมรอยเข้าใช้งานบัญชี แม้กระทั่งการดูแลรักษาอุปกรณ์พวก mobile device, laptop, PC ที่อาจจะสูญหาย ถูกเข้าถึง และควบคุมผ่าน malware เป็นต้น

ดังนั้น เมื่อเราเข้าใจบริบทของความรับผิดชอบที่ผู้ให้บริการพึงมีต่อผู้รับบริการ และรับรู้ว่าจริง ๆ แล้วข้อมูลของเราถูกวางไว้บน Internet เพื่อนำไปใช้งาน ให้เราย้อนกลับมาทบทวนดูว่า ปัจจุบันเราได้ใช้บริการ Online อะไรบ้าง โดยเฉพาะบัญชีผู้ใช้ที่มีการใช้งานบ่อยครั้ง และนำไปเชื่อมโยงกับบัญชีบริการอื่น ๆ อาทิ Social Network, e-mail และที่สำคัญได้มีการผูกบัญชีธนาคาร บัตรเครดิต/เดบิต หรือกรอบข้อมูลทางการเงินไว้ในตอนลงทะเบียนหรือไม่ การใช้งานยังเป็นปกติหรือไม่ มีประวัติของธุรกรรมที่ผิดปกติหรือน่าสงสัยบ้างหรือไม่ สิ่งเหล่านี้เราต้องคอยตรวจสอบและเฝ้าระวังอยู่อย่างสม่ำเสมอเพื่อป้องกันกรณีที่ไม่พึงประสงค์ ผู้เขียนจะขอยกตัวอย่างสิ่งที่ได้รับทราบข้อมูลจากที่เคยได้ประสานกับบริษัทบัตรเครดิต

- การผูกบัตรเครดิต/เดบิต กรณีของ Payment Service จากต่างประเทศ ที่ใช้มาตรฐานความปลอดภัยของบัตรประเภทต่าง ๆ ผู้ให้บริการจะขอให้ระบุรหัสรักษาความปลอดภัยสำหรับไว้ใช้อ้างอิงเพื่อขออนุญาตทำธุรกรรม อาทิ
- “CVV” หรือ “ค่าการตรวจสอบบัตร” - บัตรเครดิต Visa
- “CSC” หรือ “รหัสการ์ดรักษาความปลอดภัย” – บัตรเดบิต

• "CAV" หรือ "มูลค่าการตรวจสอบความถูกต้องของบัตร" บัตรเครดิต JCB

• "CID": "รหัสบัตร", "หมายเลขประจำตัวบัตร" หรือ "รหัสประจำตัวบัตร" - บัตรเครดิต Discover, American Express

• "CVC" หรือ "รหัสตรวจสอบบัตร" – บัตรเครดิต Mastercard

• "CVD" หรือ "ข้อมูลการตรวจสอบบัตร" – บัตรเครดิต Discover

• "CVN" หรือ "หมายเลขการตรวจสอบบัตร" - บัตรเครดิต China UnionPay

โดยให้ผู้ใช้ระบุหมายเลขดังกล่าวไว้ และใช้กลไกการยืนยันตัวตน พิสูจน์ความเป็นเจ้าของบัญชีผู้ใช้ในการอนุญาตให้ทำธุรกรรม ซึ่งหากเราถูกเข้าถึง หรือสวมรอยบัญชีผู้ใช้ก็อาจจะโดนนำบัตรไปใช้ทำธุรกรรมได้ และที่สำคัญคือส่วนใหญ่จะไม่ได้มีการเชื่อมโยงข้อมูลหมายเลขโทรศัพท์มือถือของผู้ใช้บริการ หรือไม่เชื่อมโยงกับผู้ให้บริการเครือข่ายโทรศัพท์มือถือในประเทศไทย ทำให้ในกระบวนการชำระเงินจะใช้รหัสความปลอดภัยแทนการให้ผู้ใช้บริการอนุญาตให้ทำธุรกรรม ผ่านการระบุหมายเลข OTP ที่ถูกส่งผ่าน SMS ซึ่งหมายรวมถึงการผูกบัญชีธนาคาร และโอนเงินผ่านบัญชีผู้ใช้ของ Payment Service ด้วย กรณีของการถูกโอนเงินด้วยบัญชีผู้ใช้ของ Payment Service ต่างประเทศก็เกิดขึ้นบ่อยครั้งเช่นกัน

• บัญชี online ต่าง ๆ ทั้ง e-mail, social network หากมีการใช้ร่วมกับ Payment service ของผู้ให้บริการต่าง ๆ ต้องคอยดูแลเรื่องความปลอดภัยของบัญชีอย่างสม่ำเสมอ เพราะกรณีที่โดนมิจฉาชีพเข้าถึง และสวมรอยบัญชีผู้ใช้เป็นเรื่องที่เกิดขึ้นอยู่บ่อย ๆ ทั้งที่เกิดจากความผิดพลาดของผู้ใช้บริการเอง และการถูกเจาะเข้าระบบของผู้ให้บริการ รวมถึงกรณีที่มีข้อมูลบัญชีผู้ใช้รั่วไหลตามที่เป็นข่าวอยู่เป็นระยะ ๆ

ปัจจุบันการสมัคร เพื่อลงทะเบียนใช้บริการ Online ผ่าน website หรือ application ทำได้สะดวกรวดเร็วมากกว่าเดิม โดยเฉพาะที่ผ่านกลไกการขอเข้าถึงบัญชีพวก Social network หรือที่เรียกว่า Social login เป็นการเชื่อมโยงข้อมูลบัญชีผู้ใช้จาก Social network และนำไปสร้างบัญชีผู้ใช้บริการของ website หรือ application เราสามารถตรวจสอบความผิดปกติได้ โดยไปที่เครื่องมือจัดการบัญชีของ Social network ต่าง ๆ ซึ่งมีให้ตรวจสอบการผูกบัญชีกับบริการต่าง ๆ ถ้าตรวจสอบพบว่า ไม่ได้สมัครใช้บริการก็สามารถยกเลิกการเชื่อมโยงบัญชีได้ รวมถึงบาง Social network สามารถตรวจสอบประวัติการเข้าใช้งานระบบว่าเข้าใช้ผ่านอุปกรณ์ใด เมื่อไปและเข้าจะบริเวณใดของโลก เพื่อเป็นข้อมูลให้เราสามารถป้องกันเหตุไม่พึงประสงค์ได้ทันท่วงที

สำหรับ e-mail ต้องคอยตรวจสอบ spam mail, จดหมายขยะ ที่ผิดปกติ ไม่ควรเปิด mail ที่ไม่แน่ใจในความปลอดภัย รวมถึงการเปลี่ยนรหัสผ่านเป็นประจำตามคำแนะนำของผู้ให้บริการโดยรหัสผ่านต้องเป็นไปตามคำแนะนำด้านความปลอดภัยที่กำหนด

• กรณีการผูกบัตรเครดิต/เดบิต กับ Payment service ของบริการพวก marketplace หรือ shopping application ที่ให้บริการภายในประเทศจะต้องคอยตรวจสอบประวัติการทำธุรกรรม ถึงแม้ว่าผู้ให้บริการจะชี้แจงว่าเชื่อมโยงข้อมูล และกลไกการชำระเงินปลอดภัยได้มาตรฐานสากล แต่ก็มีกรณีเกิดขึ้นอยู่เสมอ ดังนั้นในการทำธุรกรรมชำระเงินขั้นตอนของการยืนยันการชำระเงินด้วย OTP จึงมีความสำคัญ และควรจะต้องมีทุกครั้งที่มีการชำระเงิน ตัวผู้เขียนเองเคยเจอกับบางผู้ให้บริการ จะเป็นในลักษณะที่ถ้าเคยชำระผ่านบริการนี้มาแล้วอย่างน้อย 1 ครั้ง โดยครั้งแรกจะได้รับ OTP และดำเนินการตามขั้นตอนปกติครั้งต่อ ๆ มา ถ้าวงเงินที่ชำระไม่มากบางครั้งก็จะข้ามขั้นตอนของ OTP ไป โดยตัดยอดเงินในบัตรเครดิต/เดบิต หรือตัดบัญชีเลย ซึ่งก็รวมถึง application หรือ website จองที่พัก ตั๋วเครื่องบินด้วยเช่นกัน สำหรับในกรณีลักษณะนี้ผู้ให้บริการบางรายก็ออกมาชี้แจงบ้างแล้วว่า ทำไมถึงข้ามขั้นตอนดังกล่าว ซึ่งให้เหตุผลว่ามีการกำหนดยอด verify ขั้นต่ำไว้ ซึ่งแต่ละกรณีที่เกิดขึ้นยอดขั้นต่ำไม่เท่ากัน

เนื่องจากความเสียหายที่เกิดขึ้นส่งผลกระทบโดยตรงกับความเชื่อมั่นในบริการทางด้านการเงิน ของธนาคาร สถาบันการเงิน ผู้ให้บริการ Payment Gateway ทั้งใน และต่างประเทศ ผู้ให้บริการ Market place, Shopping Online platform ทั้งระบบ อย่างไรก็ตามเราก็ยังคงต้องใช้บริการเหล่านี้อยู่ และเหมือนจะกลายเป็นส่วนหนึ่งของการใช้ชีวิตประจำวันไปแล้ว ดังนั้นวิธีที่ดีที่สุดในตอนนี้คือ เราต้องดูแลเรื่องความปลอดภัยข้อมูลการเงินของเราเองอย่างสม่ำเสมออย่าละเลย เพราะแม้ว่าจะสามารถเรียกคืนทรัพย์สินมาได้แต่ความเชื่อมั่น ความไว้วางใจต่าง ๆ เรียกคืนมาได้ยาก ไม่เช่นนั้นเราคงต้องใช้บริการทางด้านการเงินด้วยความหวาดระแวงไปตลอด ซึ่งคงไม่มีใครต้องการให้เป็นอย่างนั้นแน่ ๆ