

เฝ้าระวังข้อมูลทางการเงินบนโลก Online

วิษณุภักดิ์ เมาะพงษ์

ศึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สำนักตลาดทุนวิจัยและให้คำปรึกษา
มหาวิทยาลัยธรรมศาสตร์

ในช่วงเดือนที่ผ่านมา นอกจากข่าวคราวเรื่องการแพร่ระบาดของ Covid-19 ตัวเลขการฉีดวัคซีนที่เพิ่มขึ้นอย่างต่อเนื่อง การเปิดเรียนแบบ Onsite การเปิดประเทศ อยู่ในความสนใจของทุกคน ซึ่งรวมถึงเรื่องของการที่มีกรณีผู้เสียหายจำนวนมากถูกโจรกรรมเงินจากบัญชีธนาคาร บัตรเดบิต บัตรเครดิต ผ่านการโอน การใช้จ่ายซื้อสินค้าในช่องทางต่าง ๆ บนโลก Online โดยที่เจ้าของบัญชีไม่รู้ตัว และไม่สามารถที่จะป้องกันได้ มีมูลค่าความเสียหายรวมกว่า 100 ล้านบาท ซึ่งผู้เสียหายนั้นเป็นลูกค้าจากหลากหลายธนาคาร และสถาบันการเงินต่าง ๆ แบบไม่เฉพาะเจาะจง โดยผู้เสียหายส่วนใหญ่จะมีประวัติการทำธุรกรรม Online ผ่านช่องทางการให้บริการของ Payment Gateway (ผู้ให้บริการชำระเงิน) ทั้งที่เป็นของสถาบันการเงิน ธนาคารให้บริการเอง และส่วนที่เป็นของผู้ให้บริการเฉพาะทาง ทั้งใน และต่างประเทศ ซึ่งตัวผู้เขียนเองก็เคยเป็นหนึ่งในผู้เสียหายจากกรณีในลักษณะดังกล่าว จึงขอมาแชร์ประสบการณ์ให้รับทราบเพื่อเป็นประโยชน์ในการเฝ้าระวังต่อไปครับ

เรื่องมีอยู่ว่า ตัวผู้เขียนเองทำงานในแวดวงของการพัฒนาระบบเทคโนโลยีสารสนเทศ การออกแบบ Solution สำหรับแก้ปัญหาทางบริการ รวมถึงการพัฒนา Product ต่าง ๆ ทำให้มีภาระที่ต้องยุ่งเกี่ยวกับการใช้จ่ายเพื่อชำระค่าบริการของ Application service ค่า Software ค่าบริการ Cloud ค่า Hosting ฯลฯ และเพื่อความสะดวกในการทำธุรกรรม ผู้เขียนจึงทำการสร้างบัญชีผู้ใช้ และผูกบัตรเครดิตสำหรับหักค่าบริการต่าง ๆ ไว้กับผู้ให้บริการ Payment ชื่อของต่างประเทศ เพราะเนื่องจากบริการส่วนใหญ่ที่ใช้เป็นของต่างประเทศเช่นกัน โดยบัตรเครดิตที่ผูกไว้เป็นบัตรประเภท VISA ซึ่งก็มีการใช้งานมาตามปกติในช่วงหลายปีที่ผ่านมา

แต่เมื่อวันปีใหม่ 1 มกราคม พ.ศ. 2564 ที่ผ่านมามี e-mail มาจากผู้ให้บริการ Payment รายดังกล่าว และได้รับ message แจ้งเตือนเรื่องการใช้จ่ายจาก mobile banking application ของสถาบันการเงินที่เป็นผู้ให้บริการบัตรเครดิต โดยเนื้อหาบอกว่ามีการใช้จ่ายบัตรเครดิตสำหรับค่าบริการ games online ของบริษัทแห่งหนึ่งในประเทศเบารุส (ประเทศในแถบยุโรปตะวันออก แยกตัวออกมาจากสหภาพโซเวียต) และเมื่อกดดูรายละเอียดค่าใช้จ่ายก็พบว่ามีการเรียกเก็บเงินเป็นสกุลเงินรัสเซีย กับ USD ซึ่งรวมทุกรายการธุรกรรมแล้วก็เป็นจำนวนเงินหลักหมื่นบาท โดยธุรกรรมเหล่านั้นเกิดขึ้นภายในไม่ถึง 24 ชั่วโมง

และน่าจะเพราะเป็นวันปีใหม่ผู้เขียนเลยเผอเรอ ไม่ได้มาดู e-mail เหมือนวันทำงานปกติ อันนี้ก็น่าจะเป็นเวลาฉวยโอกาสลงมือของมิจฉาชีพ พอรู้ตัวก็เลยรีบเข้าไปยกเลิกการผูกบัตรเครดิตกับบัญชีผู้ให้บริการ Payment และบริหารจัดการเรื่องการรักษาความปลอดภัยของบัญชี e-mail ที่ผู้เขียนใช้ในการลงทะเบียนสร้างบัญชีผู้ใช้งานกับให้บริการ Payment ซึ่งคาดว่าจะโดนแฮกผ่านทาง e-mail นี้ จากนั้นจึงรีบโทรศัพท์ประสานกับทางบัตรเครดิต ซึ่งก็ถือว่าผู้เขียนโชคดี เพราะได้รับคำแนะนำและช่วยเหลือดีมาก ๆ โดยทางบัตรเครดิตรีบทำเรื่องระงับการชำระไปถึงทางผู้ให้บริการ Payment และเจรจาให้โดยดูจากประวัติการใช้จ่ายของผู้เขียน ซึ่งพบว่ากรณีที่เกิดขึ้นมันผิดปกติ



การดำเนินการเพื่อขอระงับการชำระเงินที่เกิดจากรูกรวมดังกล่าว เป็นไปตามขั้นตอน และสามารถจบลงได้ภายใน 3 สัปดาห์โดยผู้เขียนไม่ต้องชำระค่าบริการที่เกิดขึ้นดังกล่าว ซึ่งก็ถือเป็นบทเรียนให้กับผู้เขียนว่าต้องใช้ความระมัดระวังในการทำธุรกรรมทางการเงินบนโลก Online และจากกรณีที่เกิดขึ้น ทำให้มุมมองเรื่องความปลอดภัยในการทำธุรกรรมทางการเงินผ่านช่องทางต่าง ๆ เปิดกว้างขึ้น เพราะทุกอย่างที่เป็นข้อมูลส่วนบุคคลของเราสามารถเชื่อมโยงกันหมด โดยเฉพาะเมื่อเราสร้างข้อมูลกิจกรรมทางการเงินขึ้นไปไว้บน Internet

หลังจากที่เกิดเหตุการณ์ดังกล่าว เมื่อมีเวลาร่างผู้เขียนจะค้นหากรณีศึกษา และก็เข้าร่วมกลุ่ม Social media ต่าง ๆ เพื่อแลกเปลี่ยนประสบการณ์ สอบถามปัญหาเกี่ยวกับแนวทางป้องกันอย่างต่อเนื่อง จนกระทั่งมาเกิดเหตุการณ์ในช่วงที่ผ่านมา ซึ่งจริง ๆ แล้วก็ยังมีความเสี่ยงนี้ที่เกิดขึ้นอยู่ โดยหลายกรณีที่ผู้เสียหาย

ถูกโจรกรรมเงินจำนวนหลักแสนบาทแต่ยังไม่ได้ถูกนำเสนอเป็นข่าวก็มีอยู่อีกหลายกรณี อาจจะเนื่องมาจากยังมีกลุ่มมิจฉาชีพดำเนินการโจรกรรมผ่านช่องทางต่าง ๆ ของบริการธุรกรรมการเงินอย่างต่อเนื่อง และมีจาช็พส่วนใหญ่ทำการโจรกรรมผ่านเครือข่าย Internet จากต่างประเทศ ทำให้การดำเนินการทางกฎหมายเป็นไปได้ด้วยความยุ่งยาก และล่าช้า การติดตามค่อนข้างยากลำบาก ดังนั้นสิ่งที่ภาครัฐ และสถาบันการเงินทำได้ ณ ปัจจุบัน คือการชดเชยตามมูลค่าทรัพย์สินที่ถูกโจรกรรม และออกมาตรการป้องกันเท่าที่จะทำได้ รวมถึงให้คำแนะนำแนวปฏิบัติต่าง ๆ แก่ผู้ให้บริการในเบื้องต้น และให้ช่องทางในการประสานเพื่อติดต่อกรณีเกิดเหตุการณ์ในลักษณะดังกล่าว

เมื่อพิจารณาในภาพรวมแล้ว ส่วนใหญ่เราจะมองไปที่ปลายทาง และมองหาผู้รับผิดชอบ นั่นก็คือผู้ให้บริการด้านการเงิน สถาบันการเงิน ธนาคาร ซึ่งก็เป็นเรื่องที่เหมาะสมผล และเป็นภาระหน้าที่ที่ต้องรับผิดชอบ เพราะว่าผู้ให้บริการได้รับผลประโยชน์จากเม็ดเงินที่หมุนอยู่ในระบบ แต่ในข้อเท็จจริงแล้ว กรณีส่วนใหญ่จะเริ่มมาจากจุดอื่น ซึ่งถูกชี้ไปที่ความรับผิดชอบต่อข้อมูลส่วนบุคคล และข้อมูลทางการเงินของผู้ใช้บริการเอง

ปัจจุบัน โดยทั่วไปหากเคยใช้บริการบนโลก Online เราจะมีข้อมูลส่วนบุคคลที่วิ่งอยู่บน Internet ทั้งนี้หมายรวมถึงข้อมูลที่ผู้ให้บริการทั้งภาครัฐ และเอกชนบอกว่าเป็น Private เป็นข้อมูลที่เป็นส่วนตัว ถูกเก็บไว้อย่างปลอดภัย ซึ่งจริง ๆ แล้ว เป็นเช่นนั้นหรือไม่ จะมีใครสามารถเข้าถึง และนำไปใช้หาผลประโยชน์ได้หรือไม่

จากบทความตอนที่ผ่านมา ผมกล่าวถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่กำลังจะบังคับใช้ ซึ่งไม่ได้หมายความว่าตอนนี้จะยังไม่ได้มีการจัดเก็บข้อมูลส่วนบุคคลจากผู้ให้บริการต่าง ๆ เพราะจริง ๆ แล้ว ข้อมูลส่วนบุคคลของผู้คนจากทั่วทุกมุมโลกนั้นถูกผู้ให้บริการ application หรือ website จัดเก็บแล้วนำไปใช้งานอยู่ตลอดเวลา และส่วนใหญ่ถูกนำไปวางไว้บน Internet ซึ่งก็รวมถึงข้อมูลทางการเงินด้วย ในกรณีที่มีการใช้บริการในด้านดังกล่าว ทั้งนี้ก็ขึ้นอยู่กับว่าจะอนุญาตให้เข้าถึงได้หรือไม่ และด้วยวิธีใด