

“Co(mputer)-Vi(rus)d 19” ทำธุรกรรมออนไลน์อย่างไรให้การ์ดไม่ตก

อนุภาค มาตรฐาน
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้าน IT
ธนาคารแห่งประเทศไทย

“คุณได้รับการอนุมัติเงินเยียวยา ผู้ได้รับผลกระทบจากสถานการณ์โรคระบาดไวรัสโคโรนา 19 กรณารอกข้อมูลและรหัสผ่านของธนาคารท่านในแบบฟอร์ม เพื่อยืนยันตัวตนและรับเงินโอนโดยอัตโนมัติ” หลายท่านคงเคยได้รับข้อความลักษณะนี้ และยังคงได้รับบ่อยขึ้น โดยเฉพาะในยุค new normal ที่คนส่วนมากมีพฤติกรรมใช้บริการธุรกรรมทางการเงินผ่านช่องทางออนไลน์เพิ่มขึ้นมาก ผ่านช่องทางยอดฮิตอย่าง “mobile banking” ที่ช่วยรักษาระยะห่าง สะดวกและรวดเร็ว ไม่ว่าจะเป็นจ่ายค่าอาหาร จ่ายค่าบริการต่าง ๆ บริจาคเงินผ่าน QR code หรือรับเงินช่วยเหลือจากภาครัฐ ทำให้ธุรกรรมออนไลน์เป็นส่วนหนึ่งในการใช้ชีวิตประจำวันของเราเสียแล้ว เมื่อเป็นเช่นนี้แน่นอนว่าเราไม่เพียงต้องดูแลป้องกันตัวเองไม่ให้ติดเชื้อ COVID-19 แต่ไวรัสที่มากับระบบคอมพิวเตอร์ เราก็ต้องการ์ดไม่ตกเช่นเดียวกัน วันนี้จึงขอเสนอแนะวิธีการสร้างภูมิคุ้มกัน เพื่อป้องกันไวรัสคอมพิวเตอร์ที่ทุกคนสามารถทำได้ด้วยตนเองกันดีกว่าครับ

1. ดูแลให้อุปกรณ์ปลอดภัย ไม่นำมือถือไปติดตั้งแอปพลิเคชันให้เกิดจุดอ่อน เช่น ทำ root/jailbreak ไม่ลงแอปพลิเคชันเถื่อนหรือแอปพลิเคชันที่ไม่น่าเชื่อถือ อัปเดตระบบปฏิบัติการ (OS) ของโทรศัพท์มือถือ ให้เป็นปัจจุบันอย่างสม่ำเสมอ ก็จะช่วยลดความเสี่ยงจากช่องโหว่ต่าง ๆ เพราะหากมีช่องโหว่ อาจทำให้คนร้ายสามารถเข้าควบคุมมือถือผ่านการส่งข้อมูล หรือแอบมาทาง Wi-Fi แล้วดักจับข้อมูลที่เราทำธุรกรรม นั่นจึงเป็นที่มาว่า ทำไมปัจจุบันธนาคารไม่อนุญาตให้ลูกค้าใช้มือถือที่ติดตั้ง หรือใช้ OS เวอร์ชันเก่าเข้าใช้บริการ mobile banking ทำธุรกรรมทางการเงิน

2. คอยระวังความผิดปกติ คอยสังเกตว่ามีสิ่งผิดปกติหรือไม่ เช่น คนร้ายอาจสวมรอยสถานการณ์มาหลอกเรา ถ้าสุครึ้น COVID-19 ที่รัฐเปิดให้ลงทะเบียนรับเงินเยียวยา คนร้ายได้สวมรอยโดยส่ง SMS แจ้งว่าให้ลงทะเบียนผ่านเว็บไซต์หรือแอปพลิเคชันปลอมเพื่อรับเงิน แล้วหลอกเอาข้อมูลของเราไปทำทุจริต จึงต้องคอยหมั่นสังเกตความผิดปกติ เช่น ชื่อเว็บไซต์หรือเบอร์โทรศัพท์แปลก ๆ ที่ดูแล้วไม่น่าเชื่อถือ อาจสะกดผิดหรือชื่อแปลกไปจากเดิม จึงควรตรวจสอบให้แน่ใจก่อนดีที่สุด

3. ตั้งรหัสผ่านที่ไม่ธรรมดา ให่ยากต่อการคาดเดา ไม่ควรใช้รหัสผ่านที่เดาได้ง่าย เช่น 123456 password abc1234 iloveyou หรือใช้ข้อมูลใกล้ตัวมากำหนดรหัสผ่าน เช่น เบอร์โทรศัพท์ วันเดือนปีเกิด เลขที่บัตรประชาชน และควรเก็บรหัสผ่านเป็นความลับ ไม่ควรบอกแม้แต่คนใกล้ชิดในครอบครัว เพราะหลายเหตุการณ์การทุจริตเกิดจากคนใกล้ตัวคุณเอง

ธนาคารแห่งประเทศไทย ให้ความสำคัญกับการดูแลความมั่นคงปลอดภัยของบริการทางการเงินออนไลน์ กำกับดูแลให้ระบบของสถาบันการเงินมีความมั่นคงปลอดภัย ควบคู่กับการนำเสนอบริการทางการเงินที่ทันสมัย อย่างไรก็ตาม การดำเนินการรับมือภัยไซเบอร์จากธนาคารเพียงฝ่ายเดียวยังไม่เพียงพอรับมือกับภัยในปัจจุบันที่มีรูปแบบที่หลากหลาย ซับซ้อน แต่ต้องได้ความร่วมมือจากทุกท่านที่จะการ์ดไม่ตก มีสุขอนามัยขั้นพื้นฐานด้านการทำธุรกรรมออนไลน์ (cyber hygiene) เปรียบดังการใส่หน้ากาก ล้างมือ รักษาระยะห่างทางสังคม เพื่อให้เรารอดปลอดภัยเชื้อทั้งเชื้อไวรัส COVID-19 และไวรัส computer

บทความนี้เป็นข้อคิดเห็นส่วนบุคคล ซึ่งไม่จำเป็นต้องสอดคล้องกับข้อคิดเห็นของธนาคารแห่งประเทศไทย