เมื่อข้อมูลส่วนบุคคลของเรารั่วไหล เราจะรับมือแล้วป้องกันอย่างไร?

นำเสนอเมื่อ : 9 เม.ย. 2566

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) หรือ เอ็ตด้า ได้เสนอแนวทางป้องกันกรณีข้อมูลส่วนบุคคลรั่วไหล! ที่คัดพิเศษมาให้สำหรับคนทั่วไป และหน่วยงานที่ทำการพิสูจน์และยืนยันตัวตน ว่าต้องปฏิบัติตัวอย่างไร ? ตามไปดูกันได้เลย

แนวทางป้องกันตัวเองจากผู้ไม่หวังดี ที่อาจจะแอบใช้ข้อมูลส่วนบุคคลของเราที่รั่วไหล

1. หยุด

โอนเงิน ให้ข้อมูลส่วนบุคคล หรือข้อมูลสำคัญ กับบุคคลที่ไม่รู้จัก ที่ติดต่อเรา มาทาง อีเมล SMS หรือโทรศัพท์

เพราะผู้ไม่หวังดีอาจปลอมตัวเป็นเจ้าหน้าที่ของหน่วยงานต่างๆ ติดต่อมาหาเรา และใช้ข้อมูลที่รั่วไหล สร้างความน่าเชื่อในการพูดคุยกับเรา

2. คิดก่อนคลิก

หลีกเลี่ยงการเปิดลิงก์หรือไฟล์แนบ จากอีเมลหรือ SMS ที่ไม่รู้จัก

เพราะผู้ไม่หวังดี อาจส่งลิงก์หรือไฟล์แนบ มายังอีเมลหรือ SMS และหวังให้เราหลงกล กดคลิกติดตั้ง malware เพื่อขโมยข้อมูลสำคัญของเราไปใช้ทำธุรกรรมการเงินต่อได้

ดังนั้น เมื่อได้รับการติดต่อจากคนที่เราไม่รู้จัก หรือ ไม่แน่ใจว่าเป็นตัวจริง

โปรด!!! หยุด โอนเงิน ให้ข้อมูล หรือคลิกลิงก์

แล้วใช้เวลาสักนิด ตรวจเช็คข้อมูลกับหน่วยงานก่อน

(ควรตรวจสอบผ่านช่องทางการติดต่อทางการของหน่วยงานนั้นๆ เช่น เบอร์โทรศัพท์ ที่เผยแพร่บนเว็บไซต์หน่วยงาน เป็นต้น)

แล้วเราจะป้องกันตัวเอง ได้อย่างไรก่อน

1. เปิดใช้ “วิธีการยืนยันตัวแบบหลายปัจจัย” กับบริการสำคัญ (ถ้ามี) นอกเหนือจากการใช้ Password หรือ PIN เพียงอย่างเดียว เช่น OTP เพื่อให้มั่นใจว่าเราที่เป็นตัวจริงเท่านั้น เข้าใช้งานได้
2. เปิดใช้งาน “ระงับบัญชี (Account) ชั่วคราว” (ถ้ามี) เมื่อไม่ได้ใช้งานบัญชีหรือ Account ในขณะนั้น เพื่อป้องกันการเข้ามาทำธุรกรรมของผู้ไม่หวังดี
3. หมั่นตรวจสอบประวัติการเข้าใช้งาน (Log in) บัญชีออนไลน์หรือแอปพลิเคชันต่างๆ หากพบว่ามีการใช้งานจากอุปกรณ์ที่ไม่รู้จัก หรือไม่ใช่ของเรา ควรรีบลงชื่อออก (Log out) และเปลี่ยน

Password ทันที
4. หมั่นตรวจสอบข้อมูลหรือประวัติการทำธุรกรรมทางการเงินว่า มีการโอนเงินเข้าออกที่ผิดปกติหรือไม่ หากผิดปกติให้รีบติดต่อธนาคาร โดยเร็ว
5. เมื่อข้อมูลรั่วไหล ให้แจ้งธนาคารทราบว่าข้อมูลสำคัญของเราได้รั่วไหล เพื่อธนาคารจะได้เพิ่มกลไกตรวจสอบตัวตนของเรา หรือให้คำแนะนำที่เหมาะสมกับเราต่อไป

เมื่อข้อมูลส่วนบุคคลของผู้ใช้บริการของเรารั่วไหล จากหน่วยงานอื่น

และเราเป็นหน่วยงานที่ให้บริการ e-Service และให้ผู้ใช้บริการของเราใช้ Digital ID ที่เราออกให้ (เช่น บัญชีผู้ใช้งาน (User Account)) เข้าถึงบริการออนไลน์ของเราได้

เราจะรับมือแล้วป้องกันอย่างไร?

ETDA ขอเสนอแนวทางป้องกันสำหรับหน่วยงานที่ทำการพิสูจน์และยืนยันตัวตน ดังนี้

การป้องกันในขั้นตอนการพิสูจน์ตัวตน (identity proofing)

เพื่อป้องกันไม่ให้ผู้ไม่หวังดี ใช้ข้อมูลส่วนบุคคลที่รั่วไหล มาสวมรอยเป็นบุคคลอื่น ในขั้นตอนการพิสูจน์ตัวตน ทั้งที่ไม่ใช่ตัวจริง

1. หน่วยงานควรตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลกับหน่วยงานที่ออกหลักฐานแสดงตน เช่น ตรวจสอบข้อมูลโดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบกับข้อมูลจากชิป

2. หน่วยงานควรหลีกเลี่ยงการพิสูจน์ตัวตน โดยใช้แค่การตรวจสอบข้อมูลหน้าบัตรประชาชนและหมายเลขหลังบัตรประจำตัวประชาชน (laser code) เท่านั้น

การป้องกันในขั้นตอนการยืนยันตัวตน (authentication)

เพื่อป้องกันไม่ให้ผู้ไม่หวังดี สวมรอยใช้ Digital ID หรือบัญชีผู้ใช้งาน (User Account) ของเรา เข้าถึงบริการออนไลน์ของเราได้

3. หน่วยงานควรใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) ซึ่งมีการใช้ปัจจัยของการยืนยันตัวตน (authentication factor) ที่แตกต่างกันมากกว่าหนึ่งปัจจัย เช่น

- การกรอกรหัสผ่าน (ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณรู้) ร่วมกับรหัส OTP ที่ส่งมายังโทรศัพท์ของผู้ใช้บริการ (ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณมี) หรือ

- การเปรียบเทียบชีวมิติ (biometrics) ของผู้ใช้บริการ (ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณเป็น) และเรียกใช้กุญแจเข้ารหัสที่อยู่ในแอปพลิเคชัน (ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณมี) เพื่อนำมากุญแจเข้ารหัสมาใช้ยืนยันตัวตน (cryptographic software)

ขอบคุณข้อมูลจาก สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)