6 สิ่งที่ต้องทำ เมื่อข้อมูลส่วนตัวรั่วไหลจากผู้ให้บริการ

TLP: WHITE

เผยแพร่วันที่ 17 มกราคม 2564

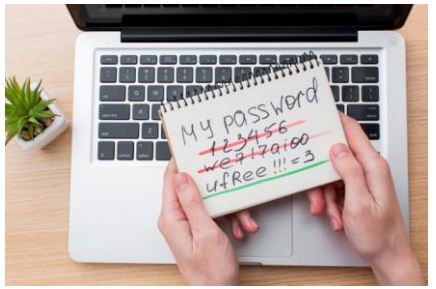
ปัจจุบันมีเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้นมากมาย ทั้งภัยไซเบอร์ที่เกิดขึ้นกับผู้ใช้งานโดยตรงและภัยไซเบอร์ที่เกิดจากผู้ให้บริการแต่ส่งผลกระทบวงกว้างมายังผู้ใช้งาน **โดยจุดมุ่งหมายหลักของกลุ่มแฮกเกอร์คือ การพยายามเข้าถึงระบบและข้อมูลสำคัญ หนึ่งในข้อมูลสำคัญที่แฮกเกอร์ให้ความสนใจคือ การเข้าถึงข้อมูลส่วนตัวหรือการหลอกลวงเอาข้อมูลส่วนตัวของเราเพื่อนำไปใช้งานเสมือนเป็นเจ้าของข้อมูลนั้น ๆ** ด้วยข้อมูลส่วนตัวหรือข้อมูลส่วนบุคคลเป็นข้อมูลที่บ่งบอกถึงลักษณะเฉพาะของบุคคลนั้น เพื่อเข้าใช้งานบริการของหน่วยงานต่าง ๆ ไม่ว่าจะเป็นภาครัฐหรือเอกชน โดยเฉพาะอย่างยิ่งสถาบันการเงิน มักจะใช้ข้อมูลนี้เพื่อประกอบการยืนยันตัวตน ดังนั้นข้อมูลส่วนบุคคลจึงมีความสำคัญ เพราะหากมีผู้ไม่หวังดีล่วงรู้ก็อาจจะใช้สวมรอยในการทำธุรกรรมแทนและสร้างความเสียหายให้แก่เจ้าของข้อมูลได้ หากพบว่ามีข้อมูลส่วนตัวรั่วไหลจากผู้ให้บริการ ควรปฏิบัติดังนี้

1. **<u>ตรวจสอบและประเมินความสำคัญ</u>**ของข้อมูลที่ใช้งานกับผู้ให้บริการรายนั้น

2. **<u>เปลี่ยนรหัสผ่าน</u>**ที่ใช้ในการเข้าระบบของผู้ให้บริการรายนั้น

3. หากมีการใช้รหัสผ่านเดียวกันกับระบบอื่น ๆ เช่น **<u>อีเมล Facebook หรือ LINE</u>** ควรเปลี่ยนรหัสผ่านดังกล่าวด้วย

4. **<u>หลีกเลี่ยงการตั้งรหัสผ่าน</u>**ด้วยข้อมูลส่วนตัว เช่น วันเดือนปีเกิด หรือ หมายเลขโทรศัพท์ เป็นต้น



5. ตรวจสอบความน่าเชื่อถือของผู้ขอข้อมูล **<u>ระมัดระวังการให้ข้อมูลส่วนตัว</u>**ทางช่องทางต่าง ๆ เช่น เว็บไซต์ หรือโทรศัพท์

6. หากสงสัยในการกรอกข้อมูลใด ๆ บนธุรกรรมออนไลน์หรือเว็บไซต์ **<u>ควรติดต่อสอบถามกับเจ้าหน้าที่ที่เกี่ยวข้องโดยตรง</u>**