ข้อควรระวังด้านความเสี่ยงในการใช้บริการ ICBC E-Banking

ในการใช้บริการ ICBC E-Banking ผู้ใช้บริการควรคำนึงถึงข้อควรระวังดังต่อไปนี้

1. เข้าเว็บไซต์หรือแอปพลิเคชั่นที่ถูกต้อง

- ผู้ใช้บริการที่เข้าใช้บริการ ICBC E-Banking ผ่านเครื่องคอมพิวเตอร์ควรเข้าเว็บไซต์ (Website) ของธนาคาร "www.icbcthai.com" โดยตรง ผู้ใช้บริการควรเพิ่มที่อยู่ของเว็บไซต์ (Website) ของธนาคารในบราว์เซอร์ที่ชอบ (favorite browser) และไม่ควรเข้าเว็บไซต์ (Website) ของธนาคารผ่านลิ้งค์อื่นๆ เป็นอันขาด
- ผู้ใช้บริการที่เข้าใช้บริการ ICBC E-Banking ผ่านโทรศัพท์เคลื่อนที่ ควรติดตั้งแอปพลิเคชั่นของธนาคาร ICBC Mobile Banking ผ่านทาง App Store สำหรับระบบ iOS หรือผ่าน Play Store สำหรับระบบ Android
- ผู้ใช้บริการควรตรวจสอบตรวจสอบผู้พัฒนาแอปพลิเคชันของธนาคาร ก่อนทำการดาวน์โหลดเพื่อให้แน่ใจว่าแอปพลิเคชันที่ดาวน์โหลดเพื่อใช้งานนั้นถูกต้อง ไม่ใช่แอปพลิเคชันปลอมจากผู้ทุจริต
- ผู้ใช้บริการควรตรวจสอบและติดตั้งแอปพลิเคชันให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ

2. เก็บรักษา เลขที่บัญชี รหัสประจำตัวผู้ใช้ระบบ (User Name) และรหัสลับให้ปลอดภัย

- เพื่อความปลอดภัยของข้อมูลและเงินฝากของผู้ใช้บริการ ผู้ใช้บริการควรอ่านข้อควรระวังด้านความเสี่ยงนี้ให้ครบถ้วนก่อนการตั้งรหัสลับ ไม่ควรใช้ข้อมูลส่วนตัว หรือข้อมูลที่สามารถคาดเดาได้ง่าย เช่น ชื่อ วันเกิดหรือหมายเลขโทรศัพท์ มาตั้งเป็นรหัสลับ
- ผู้ใช้บริการจะต้องเก็บรหัสประจำตัวผู้ใช้ระบบ (User Name) และรหัสลับ รวมถึงรหัสและข้อมูลอื่นใดที่เกี่ยวข้องกับการเข้าใช้บริการ ICBC E-Banking ไว้เป็นความลับ ไม่แจ้งให้ผู้อื่นทราบ
- ผู้ใช้บริการควรเปลี่ยนรหัสลับอยู่เสมอ อย่างน้อยเปลี่ยนทุกๆ 3 เดือน
- ไม่ควรตั้งรหัสลับสำหรับบริการ ICBC E-Banking เป็นรหัสเดียวกันกับรหัสลับที่ใช้สำหรับบัตรธนาคารหรือรหัสลับของผู้ใช้ระบบที่ใช้สำหรับการเข้าเว็บไซต์ (Website) อื่นๆ
- ไม่ควรเก็บหรือบันทึกรหัสลับไว้ในระบบคอมพิวเตอร์หรือเอกสารอิเล็กทรอนิกส์ หรือห้ามจดบันทึกในกระดาษซึ่งมิได้เก็บรักษาไว้ในสถานที่ปลอดภัย
- ทุกครั้งเมื่อผู้ใช้บริการเข้าสู่บริการ ICBC E-Banking ควรตรวจสอบ "เวลาที่เข้าสู่ระบบล่าสุด" เพื่อยืนยันเวลาที่เข้าสู่ระบบที่แท้จริง

3. วิธีการตั้งค่าใช้งาน ICBC E-Banking ให้ปลอดภัย

- ผู้ใช้บริการสามารถกำหนดการแจ้งเตือนการเข้าใช้งานผ่านทาง E-Mail ได้ที่เมนูตั้งค่า ในกรณีที่ได้รับแจ้งเตือนเข้าสู่ระบบโดยที่ผู้ใช้บริการไม่ได้เป็นผู้ทำรายการ ควรรีบทำการเปลี่ยนรหัสลับ และติดต่อศูนย์บริการลูกค้าสัมพันธ์ (CALL CENTER) ของธนาคารโดยทันที
- ผู้ใช้บริการสามารถกำหนดข้อความยืนยันบริการได้ที่เมนูตั้งค่า และควรตรวจสอบข้อความยืนยันบริการที่ปรากฏบนหน้าหลักเพื่อป้องกันสถานการณ์ผิดปกติ

4. ใช้เครื่องยืนยันตัวตนให้ถูกต้อง

- USB-Shield และ E-Password Token เป็นอุปกรณ์ที่สำคัญอย่างหนึ่งสำหรับการรักษาความปลอดภัยในการใช้บริการ ICBC E-Banking ซึ่งผู้ใช้บริการสามารถขอรับ USB-Shield หรือ E-Password Token (แล้วแต่กรณี) ได้ที่สาขาของธนาคาร
- ผู้ใช้บริการต้องเก็บรักษา USB-Shield หรือ E-Password Token (แล้วแต่กรณี) และรหัสลับยืนยันตัวตนไว้ในสถานที่ที่ปลอดภัย

5. เก็บรักษาบัตรรหัสลับ (Code Card) ในสถานที่ที่ปลอดภัย

- บัตรรหัสลับ (Code Card) ควรถูกเก็บในสถานที่ที่ปลอดภัยเพื่อป้องกันมิให้มีการใช้โดยบุคคลที่ไม่ได้รับอนุญาตและป้องกันการสูญหายหรือถูกขโมย
- แผ่นฟิล์มบนบัตรรหัสลับ (Code Card) สามารถถูกขูดลอกออกได้ เมื่อแผ่นฟิล์มดังกล่าวถูกขูดลอกออกจะทำให้บุคคลอื่นสามารถล่วงรู้รหัสลับทำธุรกรรมได้ง่าย ด้วยเหตุนี้ ผู้ใช้บริการต้องใช้ความระมัดระวังและวิธีการที่จำเป็นในการรักษาความปลอดภัยของรหัสลับทำธุรกรรมที่ถูกขูดลอกออกแล้ว เมื่อแผ่นฟิล์มถูกขูดลอกออกเกินกว่าครึ่ง ผู้ใช้บริการควรใช้ความระมัดระวังมากขึ้นในการป้องกันและรักษาความปลอดภัยของบัตรรหัสลับ (Code Card) และผู้ใช้บริการต้องขอบัตรรหัสลับ (Code Card) ใหม่เมื่อแผ่นฟิล์มบนบัตรรหัสลับ (Code Card) ถูกขูดลอกออกทั้งหมด

6. ป้องกันโทรศัพท์เคลื่อนที่ของผู้ใช้บริการ

- ผู้ใช้บริการไม่ควรดัดแปลง หรือแก้ไขระบบโทรศัพท์เคลื่อนที่ของผู้ใช้บริการที่ใช้เข้าสู่บริการ ICBC E-Banking เช่น การ Jailbreak หรือ Root เป็นต้น
- ผู้ใช้บริการ ซึ่งขอรับข้อความสั้น (SMS) จากธนาคารทางโทรศัพท์เคลื่อนที่ของตน ต้องใช้ความระมัดระวังในการใช้โทรศัพท์เคลื่อนที่ การป้องกันโทรศัพท์เคลื่อนที่ให้ปลอดภัยจากไวรัสและไม่ให้โทรศัพท์เคลื่อนที่อยู่ในความครอบครองของบุคคลที่ไม่ได้รับอนุญาต

7. ควรรักษาอุปกรณ์และระบบคอมพิวเตอร์ของผู้ใช้บริการให้ปลอดภัยเสมอ

- ดาวน์โหลด ติดตั้งและปรับปรุงระบบปฏิบัติการและซอฟต์แวร์บราว์ให้เป็นปัจจุบันอยู่เสมอตามที่ธนาคารกำหนดหรือแนะนำ
- ติดตั้งและปรับปรุงโปรแกรมต่อต้านไวรัสให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ
- ติดตั้งโปรแกรม Firewall
- ไม่ควรเปิด E-Mail ที่ส่งมาจากแหล่งที่ไม่รู้จัก

8. วิธีการป้องกันอื่น ๆ

- ไม่อนุญาตให้บุคคลที่ไม่ได้รับอนุญาตใดๆ ใช้เครื่องคอมพิวเตอร์หรือโทรศัพท์มือถือของผู้ใช้บริการ
- ไม่ควรใช้บริการ ICBC E-Banking จากเครื่องคอมพิวเตอร์ที่ติดตั้งในที่สาธารณะ (เช่น ร้านอินเตอร์เน็ต ห้องสมุดสาธารณะ เป็นต้น)
- ตั้งรหัสลับในการใช้เครื่องคอมพิวเตอร์และโทรศัพท์มือถือเพื่อป้องกันบุคคลอื่นเข้าถึงข้อมูลที่เป็นความลับ
- ไม่ควรทิ้งเครื่องคอมพิวเตอร์และโทรศัพท์มือถือไว้โดยที่ผู้ใช้บริการไม่อยู่ ในขณะเข้าสู่ระบบ ICBC E-Banking
- ในขณะที่ใช้บริการ ICBC E-Banking ห้ามเปิดใช้งานระบบการให้ความช่วยเหลือทางไกล (Remote Assistance)
- กรุณาตรวจสอบรายละเอียด ข้อมูลและจำนวนเงินให้ถูกต้องก่อนจะยืนยันการทำธุรกรรมทุกครั้ง
- กดเมนู “ออกจากระบบ” ที่อยู่มุมบนขวาของหน้าจอ เพื่อออกจากการใช้บริการ ICBC E-Banking ทุกครั้ง เมื่อสิ้นสุดการใช้บริการทุกครั้ง