ข้อแนะนำเบื้องต้นในการใช้อินเทอร์เน็ตแบงก์กิ้งอย่างปลอดภัย

ปัจจุบันเทคโนโลยีมีบทบาทต่อการดำเนินชีวิตประจำวันและการดำเนินธุรกิจมากขึ้น บทบาทของเทคโนโลยีจะไม่ได้จำกัดอยู่ที่ระดับของธุรกิจเท่านั้น แต่ได้แผ่ขยายเข้ามามีบทบาทต่อการดำเนินชีวิตประจำวันของบุคคลทั่วไป ดังจะเห็นได้จากการมีโทรศัพท์มือถือ การใช้เครือข่ายอินเตอร์เน็ตเพื่อการติดต่อสื่อสาร เป็นต้น ธุรกิจหลากหลายประเภทได้เริ่มหันมาเน้นการใช้ประโยชน์จากเทคโนโลยีกันมากขึ้น ไม่เว้นแม้แต่สถาบันการเงินที่กำลังเริ่มขยายช่องทางการให้บริการผ่านเครือข่ายอิเล็กทรอนิกส์ เช่น การให้บริการ Internet Banking การให้บริการ Mobile Bankingsหรือ E-ATM เป็นต้น ลักษณะการให้บริการ E-Banking ในประเทศไทย มี 2 ลักษณะ คือ เพื่อการประชาสัมพันธ์ ข้อมูลข่าวสาร และเพื่อการทำธุรกรรมทางการเงินกับธนาคาร จากการใช้เทคโนโลยีเพื่อการให้บริการตามที่กล่าวนั้น จะทำให้สถาบันการเงินเข้าถึงฐานลูกค้าได้กว้างขวางขึ้น ให้บริการแก่ลูกค้าได้รวดเร็วขึ้น สามารถลดค่าใช้จ่ายในระยะยาวและเป็นการสร้างรายได้ค่าธรรมเนียมได้อีกทางหนึ่ง

อย่างไรก็ตาม ถึงแม้ว่าการทำธุรกรรมทางการเงินผ่านสื่ออิเล็กทรอนิกส์ จะทำให้สถาบันการเงินเข้าถึงฐานลูกค้าได้กว้างขวาง แต่สถาบันการเงินก็เกิดความเสี่ยงรูปแบบแปลกใหม่เกิดขึ้น เนื่องจากการเข้าถึงลูกค้าทำได้อย่างไร้พรมแดน และข้อมูลธุรกรรมทางการเงินของลูกค้าจะถูกส่งผ่านสื่ออิเล็กทรอนิกส์ ซึ่งอาจถูกโจรกรรมข้อมูลลูกค้า ทำให้เพิ่มความเสี่ยงต่อการเสียชื่อเสียง ความเสี่ยงจากการดำเนินงาน และความเสี่ยงด้านกลยุทธ์ ดังนั้นเพื่อให้ลูกค้าเกิดความเชื่อมั่นในการทำธุรกรรมทางการเงินผ่านสื่ออิเล็กทรอนิกส์ นอกจากสถาบันการเงินต้องมีระบบควบคุมภายใน และระบบรักษาความปลอดภัยที่มีประสิทธิภาพแล้ว สถาบันการเงินจะต้องให้ความรู้กับผู้ใช้บริการในการใช้อินเทอร์เน็ตแบงก์กิ้งอย่างปลอดภัยดังต่อไปนี้

1. ควรศึกษารูปแบบธุรกรรมและวิธีการรักษาความปลอดภัยที่ธนาคารเสนอให้บริการอินเทอร์เน็ตแบงก์กิ้ง ก่อนตัดสินใจใช้บริการ ติดตามข่าวสารเกี่ยวกับเทคโนโลยีใหม่ๆ อย่างสม่ำเสมอ

2. หลีกเลี่ยงการตั้ง Password ที่ง่ายต่อการคาดเดา และต้องเก็บรักษา User ID และ Password ให้เป็นความลับส่วนบุคคล พร้อมทั้งเปลี่ยน Password เป็นระยะอย่างต่อเนื่อง

3. หลีกเลี่ยงการคลิ๊กลิงก์ที่แนบมาพร้อมกับ E-mail โดยให้พิมพ์ Address ของ Website (URL) ของธนาคารพาณิชย์ด้วยตนเอง เมื่อต้องการเข้าใช้บริการผ่านเครือข่ายอินเทอร์เน็ต

4. ห้ามตอบหรือให้ข้อมูลส่วนบุคคลและข้อมูลสำคัญทางการเงิน เช่น Username, Password, ATM PIN และหมายเลขบัตรเครดิต เป็นต้น ไม่ว่าในกรณีใด ๆ ก็ตาม ผ่านทาง E-mail โทรศัพท์ โทรสารและจดหมาย

5. ควรตรวจสอบความถูกต้องของรายการธุรกรรมอย่างสม่ำเสมอ เช่น จำนวนเงิน วันที่ทำรายการ เลขที่บัญชี และตรวจสอบยอดเงินในบัญชี เป็นต้น เพื่อป้องกันรายการผิดปกติที่อาจเกิดขึ้น

6. ควรติดตั้งและปรับปรุงโปรแกรมเพื่อการรักษาความปลอดภัยที่เครื่องคอมพิวเตอร์ และ/หรือ อุปกรณ์ต่อพ่วงที่ใช้เป็นช่องทางในการทำธุรกรรมให้ทันสมัย เช่น โปรแกรม Scan Virus และโปรแกรม Personal Firewall เป็นต้น

7. หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์สาธารณะ เช่น Internet Cafe ในการทำธุรกรรมทางการเงิน รวมทั้งไม่ควรดาวน์โหลด ติดตั้งโปรแกรมที่ไม่น่าเชื่อถือ โปรแกรมที่ไม่ทราบแหล่งที่มา และกรณีไม่ได้ใช้งานควรปิด Bluetooth และ Wireless

8. ทุกครั้งที่ใช้บริการเสร็จ ควรคลิก “ออกจากระบบ” (Log off, Log out, Sign off, etc.) ทันที เพื่อป้องกันมิให้ผู้อื่นสามารถทำรายการจากบัญชีของท่านได้

9. หากมีข้อสงสัยหรือไม่แน่ใจ ควรติดต่อธนาคารพาณิชย์ที่ท่านใช้บริการ โดยเร็ว