นโยบายด้านความปลอดภัยในการใช้บริการ

เพื่อให้ลูกค้ามั่นใจได้ว่า ในการให้บริการต่างๆของธนาคาร ไม่ว่าจะผ่านทางช่องทางใดธนาคารได้ใช้ เทคโนโลยีระบบรักษาความปลอดภัยที่มีมาตรฐานสูง ในการป้องกันข้อมูลที่สำคัญและเป็นความลับของลูกค้าธนาคาร นอกจากนี้ธนาคารยังได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยของข้อมูลลูกค้าและมีการพัฒนาอยู่อย่างสม่ำเสมอ

เทคโนโลยีดังกล่าว ได้แก่

- **Secure Socket Layer (SSL)** ระดับ 128 bits (128-bit Encryption) สำหรับบริการทางการเงิน ผ่านใช้ในการเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่าย Internet ทำให้ผู้ที่ดักจับข้อมูลระหว่างทาง ไม่สามารถนำข้อมูลไปใช้ต่อได้ โดยระบบที่ธนาคารใช้ ได้รับการตรวจสอบและรับรองจากบริษัทที่มีชื่อเสียงและมีมาตรฐานในระดับสากล ด้านระบบรักษาความปลอดภัย
- **Data Encryption** ระบบของธนาคารจะนำข้อมูลที่มีความสำคัญมาก เช่น รหัสผ่านส่วนตัว(Password) ผ่านกระบวนการเข้ารหัส โดยใช้ Algorithm ที่ซับซ้อนก่อนเก็บข้อมูลในระบบ โดยเป็นการเข้ารหัสข้อมูลทางเดียว เพื่อใช้เทียบเคียงข้อมูลที่ได้จากลูกค้าเท่านั้น ทั้งนี้ เพื่อป้องกันการนำข้อมูลไปใช้โดยไม่สุจริต
- **Firewall** ธนาคารติดตั้ง Firewall หลายชั้น ซึ่งทำหน้าที่ปกป้องข้อมูล เปรียบได้กับเจ้าหน้าที่รักษาความปลอดภัยหน้าประตูที่ไม่อนุญาตให้คนแปลกหน้าเข้า-ออกจากระบบ
- **Auto Logout** หากลูกค้าที่ใช้บริการ Internet Banking ของธนาคารไม่ได้ออกจากระบบหลังจากใช้งานแล้ว หรือเปิดหน้าจอทิ้งไว้โดยไม่มีพิมพ์หรือการทำรายการใดๆ บนหน้าจอภายในระยะเวลาหนึ่งที่ธนาคารกำหนด ระบบจะทำการออกจากระบบ (Logout) ให้โดยอัตโนมัติ เพื่อความปลอดภัยในการใช้บริการทางอิเล็กทรอนิกส์
- **Intrusion Detection** เป็น Software ที่ใช้เพื่อตรวจสอบและแจ้งข้อความเตือนทันทีที่มีความผิดปกติเกิดขึ้นในระบบ
- **Scan Virus** เครื่องคอมพิวเตอร์รวมทั้งเครื่อง Server ทุกเครื่องของธนาคาร ได้มีการติดตั้งSoftware ป้องกัน Virus ที่มีประสิทธิภาพสูงและได้รับการ Update อย่างสม่ำเสมอ
- **Cookies** คือ File ข้อมูลเข้ารหัสขนาดเล็กที่ธนาคารสร้างขึ้นและส่งผ่าน Web Browser ไปยังเครื่องคอมพิวเตอร์ของท่านเมื่อ ธนาคารอาจใช้เพื่อช่วยในการติดต่อระหว่างธนาคารและเครื่องคอมพิวเตอร์ของท่านให้มีมาตรฐานด้านความปลอดภัยสูงขึ้น โดยค่า Cookies จะไม่สามารถนำกลับมาใช้ได้อีกหลังจากที่ท่านออกจากระบบ (Logout) หรือปิด Browser
- **Lock Password** กรณีที่มีการใส่รหัสผ่านส่วนตัว (Password) ผิด 3 ครั้ง ระบบจะระงับการใช้บริการของท่าน ทั้งนี้เพื่อป้องกันการเข้ามาใช้บัญชีของท่านทำรายการทางการเงินโดยไม่สุจริต

เพื่อให้ท่านมั่นใจในเรื่องของความปลอดภัยมากขึ้น ธนาคารขอแจ้งว่า Website ของธนาคารได้รับใบรับรอง Verisign Certificate ที่ออกโดยบริษัท Verisign Inc. ซึ่งเป็นบริษัทที่มีมาตรฐานด้านระบบรักษาความปลอดภัยในระดับสากล

ธนาคารขอแจ้งให้ทราบว่า

ธนาคารไม่มีนโยบายสอบถามข้อมูลทางการเงิน ข้อมูลส่วนตัว ข้อมูลรหัสประจำตัว (User ID) รหัสผ่านส่วนตัว (Password) หรือรหัส PIN Code กับลูกค้าของธนาคารผ่านทาง E-mail หรือช่องทางใดๆ หากท่านพบการกระทำดังกล่าว กรุณาแจ้งศูนย์ลูกค้าสัมพันธ์ของธนาคาร โทร.1551 หรือติดต่อสาขาของธนาคารที่ท่านใช้บริการอยู่

ธนาคารไม่มีนโยบายแนบ link ไปยัง web site ต่างๆ ใน E-Mail ของธนาคารที่ส่งให้ลูกค้า ทั้งนี้เพื่อให้ลูกค้ามั่นใจว่าจะไม่ถูกลวงไปยัง web site ที่ไม่พึงประสงค์

Website ของธนาคารอาจมีการเชื่อมต่อไปยัง Website ของร้านค้า องค์กร หรือสถาบันอื่น หากท่านเลือกที่จะใช้บริการ Website ที่เชื่อมโยงเหล่านั้น ซึ่งไม่อยู่ในความควบคุมของธนาคาร ธนาคารไม่สามารถรับผิดชอบต่อความปลอดภัยหรือความเป็นส่วนตัวของข้อมูลของท่าน ธนาคารขอแนะนำให้ท่านตรวจสอบนโยบายความเป็นส่วนตัวของ Website นั้นๆ เพื่อทราบและศึกษาถึงวิธีการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านอย่างรอบคอบเสียก่อน

ข้อแนะนำด้านความปลอดภัยในการใช้บริการ

- อย่าเปิดไฟล์แนบที่มากับอีเมล์ที่ไม่รู้ที่มา
- Update โปรแกรม Anti-Virus อย่างสม่ำเสมอ
- เปลี่ยน Password อย่างสม่ำเสมอ และกำหนดรหัสผ่าน โดยใช้คำหรือรหัสที่คาดเดาได้ยาก ซึ่งมีข้อแนะนำในการกำหนดรหัสผ่าน ดังนี้
    - เป็นคำหรือรหัสที่ไม่ปรากฏในเอกสารหรือเครื่องคอมพิวเตอร์ที่ท่านใช้งานอยู่
    - ง่ายต่อการจดจำ เพื่อที่ท่านจะได้ไม่ต้องบันทึกไว้ในเอกสารใดๆ
    - ประกอบด้วยตัวอักษร ตัวเลข และสัญลักษณ์พิเศษ
    - ไม่ควรเป็นคำที่ง่ายต่อการคาดเดา เช่น ชื่อ นามสกุลตนเองหรือสมาชิกในครอบครัว ยี่ห้อรถยนต์ หรือข้อมูลส่วนตัว เช่น หมายเลขบัตรประชาชน เป็นต้น

ข้อควรทราบเกี่ยวกับ Phishing

Phishing เป็นรูปแบบหนึ่งของการปลอมแปลง E-mail (E-mail Spoofing) และสร้าง Website ปลอมเพื่อหลอกลวงผู้ใช้บริการของธนาคาร ให้เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ เช่น หมายเลขบัตรเครดิต ชื่อบัญชีผู้ใช้บริการ (User Name) รหัสประจำตัว (User ID) หรือรหัสผ่านส่วนตัว (Password)วิธีการกระทำธุรกิจที่พบคือการส่ง E-Mail โดยแอบอ้างชื่อสถาบันการเงิน และขอให้ลูกค้ายืนยันข้อมูลทางการเงินหรือข้อมูลสำคัญอื่นๆ ด้วยสาเหตุต่างๆ เช่น เพื่อให้เป็นไปตามมาตรการรักษาความปลอดภัยของข้อมูลหรือถึงรอบระยะเวลาการตรวจสอบข้อมูล หรือบัญชีมีปัญหา จึงขอให้ลูกค้าทำการยืนยันข้อมูล เพื่อให้การทำธุรกรรมทางการเงินสามารถดำเนินได้ต่อไป เป็นต้น ซึ่งใน E-mail ดังกล่าว จะมีการแนบ Link การเชื่อมโยงไปยัง Website ของสถาบันการเงินปลอม เพื่อให้ลูกค้ากรอกข้อมูล และนำข้อมูลที่ได้ไปใช้ในทางมิชอบต่อไป

แนวทางการป้องกัน

- ไม่ตอบกลับ E-Mail ที่เข้าข่ายดังกล่าว และควรลบทิ้งทันที
- ควรตรวจสอบการเคลื่อนไหวในบัญชีของท่านอย่างสม่ำเสมอ หากพบสิ่งผิดปกติ กรุณาแจ้งธนาคารทันทีที่ KTB Contact Center โทร 1551 หรือ Cash Management Call Center โทร 02-208-7799 (8.00-17.00 น.)
- ควรพิมพ์ Address (URL) ของ Website ธนาคารด้วยตัวท่านเองทุกครั้ง หรือใช้ Link ที่เก็บไว้ในเมนู“Favorites” ซึ่งได้ถูกบันทึกด้วยตัวท่านเอง ไม่ควรใช้ Link ที่แนบมากับ E-Mail
- กรณีที่ลูกค้า KTB Corporate Online ไม่ได้เข้าใช้บริการมากกว่า 6 เดือน ธนาคารจะเปลี่ยนสถานะเป็น Inactive เพื่อความปลอดภัยต่อลูกค้าในการถูกแอบอ้างเข้าใช้ระบบและเป็นการเพิ่มประสิทธิภาพในการเข้าใช้ระบบงานธนาคาร ทั้งนี้ หากลูกค้าท่านใดประสงค์จะกลับมาใช้บริการ กรุณาติดต่อสาขาที่ท่านได้สมัครใช้บริการ และกรณีต้องการข้อมูลเพิ่มเติม กรุณาติดต่อ 02-208-7799 (8.00-17.00 น.)