ความปลอดภัยของการทำธุรกรรมผ่านอินเทอร์เน็ต

1. ความหมายการทำธุรกรรมผ่านอินเตอร์เน็ต

นายมีชัย ฤชุพันธ์ ผู้เชี่ยวชาญด้านกฎหมาย ได้ให้ความหมายของธุรกรรม ไว้ว่า กิจกรรมที่เกี่ยวกับการทำนิติกรรม สัญญา หรือการดำเนินการใดกับผู้อื่น ทางการเงิน ทางธุรกิจ หรือการดำเนินการเกี่ยวกับทรัพย์สิน ซึ่งรวมความว่า อะไร ๆ ที่ทำกับคนอื่นเกี่ยวกับการเงิน ธุรกิจ หรือทรัพย์สิน ล้วนเป็นธุรกรรมทั้งสิ้น

กล่าวสรุปได้ว่า**ธุรกรรม** คือ การประกอบกิจกรรมอย่างใดอย่างหนึ่งระหว่างคู่สัญญาสองฝ่าย โดยเฉพาะด้านธุรกิจและการเงิน เช่นการฝากเงินในธนาคารเป็นการทำธุรกรรมอย่างหนึ่ง การจ่ายค่าบริการโดยหักบัญชีจากธนาคาร เป็นธุรกรรมที่นิยมกันมากในปัจจุบัน

การทำธุรกรรมผ่านอินเทอร์เน็ต คือ การประกอบธุรกิจการพาณิชย์อิเล็กทรอนิกส์เกี่ยวกับการให้บริการทำธุรกรรมทางการเงินต่างๆผ่านอุปกรณ์หรือระบบอิเล็กทรอนิกส์เช่นโทรศัพท์มือถือ หรือ อินเตอร์เน็ตมีการให้บริการเช่น การฝากเงิน ถอนเงิน โอนเงิน หรือ สอบถามยอดเงิน เป็นต้นโดยในอนาคตการให้บริการของธนาคารอิเล็กทรอนิกส์ยังสามารถพัฒนาได้อีกเรื่อยๆ เพื่อรองรับความต้องการในการใช้บริการของผู้ใช้บริการธนาคารอิเล็กทรอนิกส์ ที่เพิ่มมากขึ้นอย่างต่อเนื่อง เนื่องจากธนาคารอิเล็กทรอนิกส์ทำให้เกิดความรวดเร็วและสะดวกสบายในการทำธุรกรรมมากขึ้นและประหยัดทรัพยากร

2. รูปแบบการทำธุรกรรมผ่านอินเตอร์เน็ต

รูปแบบการทำธุรกรรมผ่านอินเทอร์เน็ตหลักๆก็คือรูปแบบของธนาคารอินเทอร์เน็ต(Internet Banking)การชำระเงินออนไลน์(Payment Gateway or Bill payment)และธนาคารมือถือ (Mobile Banking) โดยมีรูปแบบการให้บริการที่ต่างกัน

ภาพที่ 1. รูปแบบการทำธุรกรรมผ่าน

2.1 ธนาคารอินเทอร์เน็ต(Internet Banking)

เป็นการให้บริการการทำธุรกรรมทางธนาคารที่ทำได้ทุกที่ ทุกเวลา ผ่านระบบอินเตอร์เน็ต เช่น สอบถามยอดคงเหลือ โอนเงิน ชำระค่าสาธารณูปโภค บริการเช็ค พิมพ์รายการเดินบัญชี ดูรายการใช้จ่ายผ่านบัตรเครดิต ย้อนหลัง ฯลฯ โดยลูกค้าของธนาคารสามารถบริหารการเงินด้วยตนเองทางอินเตอร์เน็ตด้วยเครื่องคอมพิวเตอร์ส่วนบุคคลของลูกค้าแต่ละคน โดยผู้ที่สนใจใช้บริการจะต้องติดต่อกับธนาคารของตน เพื่อขอเปิดใช้บริการ

ลักษณะบริการ

- สอบถามยอดคงเหลือในบัญชี (Account Balance Inquiry)
- สอบถามรายการเคลื่อนไหวในบัญชี (Account Statement Inquiry)
- โอนเงินระหว่างบัญชีตนเองหรือไปยังบุคคลอื่นทั้งในและต่างประเทศ (Inter-Account Funds Transfer to owner or other account)
- สอบถามสถานะเช็ค (Cheque Status Inquiry)
- สอบถามการอายัดเช็ค (Stop-Payment Cheque Inquiry)
- อายัดเช็ค (Stop-Payment of Cheque)
- การโอนเงินเพื่อชาระเป็นค่าเงินกู้ธนาคาร
- บริการสินเชื่อบุคคล

2.2 ชำระเงินออนไลน์(Payment Gateway or Bill payment)ลักษณะการให้บริการลูกค้าสามารถชำระค่าบริการต่างๆได้ทุกวัน ตลอด 24 ชม.โดยไม่ต้องเดินทาง เช่น ค่าโทรศัพท์มือถือ ค่าบัตรเครดิต ค่าใช้บริการอินเทอร์เน็ต การผ่อนชำระค่าบ้าน ค่าบริการเคเบิลทีวี และค่าเล่าเรียนของมหาวิทยาลัยต่างๆ เป็นต้น นอกจากนี้ บางธนาคารยังอำนวยความสะดวกให้โดยการมีระบบตั้งเวลาชาระเงินอัตโนมัติที่ลูกค้าสามารถตั้งเวลาชาระเงินไว้ล่วงหน้าเพื่อตัดบัญชีให้ตรงกับวันที่ครบกำหนดชาระเงิน

ภาพที่ 2. บริษัทผู้ให้บริการชำระเงิน

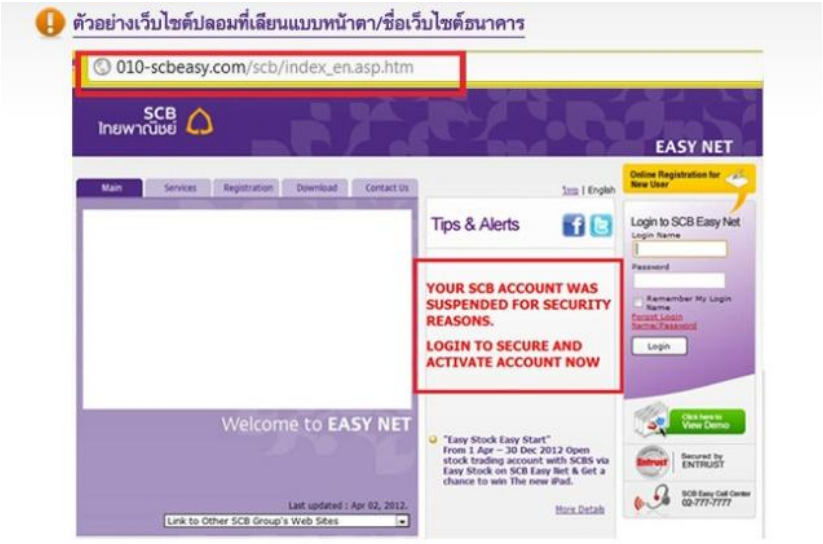
3. ความเสี่ยงจากการทำธุรกรรมผ่านอินเตอร์เน็ต

การทำธุรกรรมการเงินในปัจจุบันไม่ว่าจะเป็นโอนเงิน ฝากเงิน ถอนเงิน เช็คยอดเงินคงเหลือ ฯลฯ ก็สามารถทำออนไลน์ได้ แต่เมื่อสะดวกสบายมากเท่าไหร่ ความปลอดภัยในการใช้งานก็ยิ่งน้อยลง ดังนั้นความเสี่ยงจึงอาจจะเกิดขึ้นกับการทำธุรกรรมทางผ่านอินเทอร์เน็ตได้ในหลายรูปแบบซึ่งรูปแบบการคุกคามความปลอดภัยต่อการทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์ที่เกิดขึ้นเป็นประจำมากที่สุดและก่อให้เกิดความเสียหายมากที่สุด มีดังต่อไปนี้

3.1 การถูกแอบอ้างใช้งานธนาคารออนไลน์หลังจากการใช้งานหากลืมออกจากระบบหรือบอกรหัสผ่านเลขบัญชีการทำธุรกรรมต่างๆแก่บุคคลอื่นซึ่งเสี่ยงถูกสวมรอยหรือแอบอ้างการเข้าใช้งานการทำธุรกรรมได้

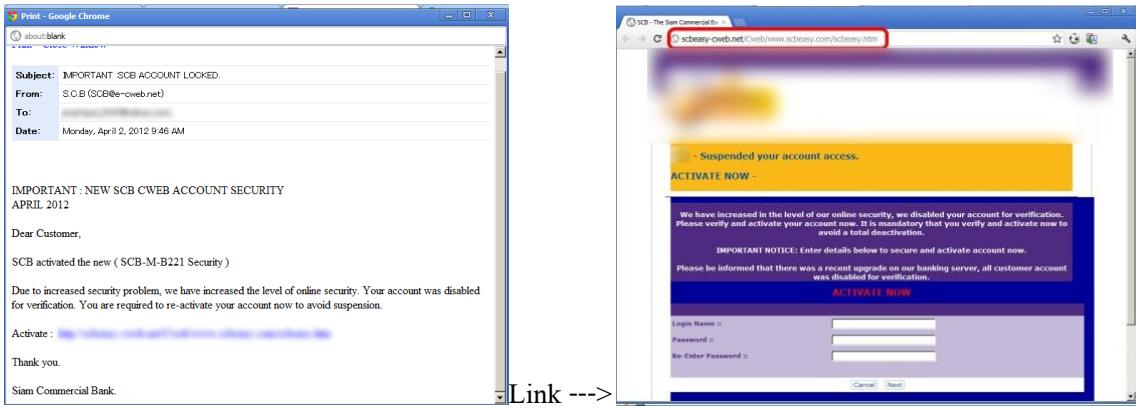
3.2 การหลอกลวงทางอินเทอร์เน็ต (Phishing)เป็นการหลอกลวงในรูปแบบต่างๆ ไม่ว่าจะเป็นเว็บไซต์ปลอม หรือ อีเมล์ปลอม เป็นความพยายามหลอกลวงใดๆก็ตามที่มาจากบุคคลที่สามที่พยายามจะเอาข้อมูลลับข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิตเพื่อผลประโยชน์ทางการเงินของตัวเอง

เว็บไซต์ปลอม: ซึ่งเว็บไซต์จะมีชื่อโดเมนและ Subdirectory เหมือนกับ URL ของสถาบันการเงินนั้น ๆ ซึ่งแท้จริงแล้วเป็น Website ปลอม ซึ่งเสี่ยงต่อการถูกดักจับข้อมูลการใช้งานจากหน้าเว็บ เช่น (Username) และรหัสผ่าน (Password) เพื่อนำไปแอบอ้างการเข้าใช้งาน



ภาพที่ 3. ภาพตัวอย่างเว็บไซต์ปลอมที่เลียนแบบเว็บไซต์

อีเมล์ปลอม: การหลอกให้ลูกค้าหลงเชื่อว่ามี e-mail มาจากสถาบันการเงินและใช้หัวข้อและข้อความที่มีความน่าเชื่อถือ เช่น การแจ้งว่าบัญชีของลูกค้าได้ถูกอายัดไว้ชั่วคราวพร้อมใส่สัญลักษณ์หรือเครื่องหมายของสถาบันการเงินและ Hyperlink ที่ e-mail ไปยังWebsite ปลอม เพื่อให้ลูกค้ากรอกข้อมูลส่วนบุคคล username และ password ยืนยันข้อมูลหากต้องการให้สามารถใช้งานได้ปกติ



ภาพที่ 4. ภาพอีเมล์ปลอมที่มีข้อความน่าเชื่อถือแนบลิงค์เว็บไซต์ปลอมมาให้กรอกข้อมูลส่วนบุคคล

3.3 โปรแกรมอันตรายต่างๆโดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มีหลายประเภท เช่น ไวรัส(Virus)เวิร์ม(Worm) ม้าโทรจัน (Trojan Horses) การแอบดักจับข้อมูล (Spyware) และคีย์ ล็อกเกอร์ (Key Logger)เป็นภัยคุมคามต่อความสมบูรณ์ของระบบ โดยโปรแกรมจะทำการควบคุมการทำงานให้เป็นไปตามความต้องการของผู้ที่ไม่หวังดี เพื่อหลอกล่อเอาข้อมูลสำคัญๆต่างๆ

3.4 การเข้าเว็บไซต์ธนาคารออนไลน์จากสมาร์ทโฟน หรือแท็บเล็ต

3.4.1 การโหลดใช้โปรแกรมธนาคารจากการแชร์โปรแกรมที่ไม่ใช้จากการอัพโหลดจากธนาคารผู้ให้บริการซึ่งเสี่ยงที่อาจจะเป็นโปรแกรมปลอมที่เอาไว้ดักจับข้อมูลของผู้ใช้งาน

3.4.2 สมาร์ทโฟนหรือแท็บเล็ตบางรุ่นอาจมองไม่เห็น URLการเขารหัสของเว็บไซต์ซึ่งเสี่ยงที่เราไม่สามารถทราบได้ว่าเป็นเว็บไซต์จริงหรือปลอม

3.4.3 การใช้ระบบปฏิบัติที่ผ่านการJailbreakหรือการ ดัดแปลงระบบปฏิบัติของ สมาร์ทโฟนซึ่งเสี่ยงต่อการถูกขโมยข้อมูลหากเชื่อมต่อเข้าสู่เว็บไซต์

Jailbreak หรือ Root คือการดัดแปลงระบบปฏิบัติ (Operating System) ของสมาร์ทโฟนหรือแท็บเล็ตที่ใช้ระบบปฏิบัติการของ iOS และ Android ซึ่งระบบปฏิบัติการ iOS และ Android นั่นเป็นระบบปฏิบัติการที่แบ่งแยกการทำงานของ Application ต่างๆออกจากกันโดยสิ้นเชิงจึงทำให้แต่ละ Application ไม่สามารถแทรกแซงหรือมองเห็นการทำงานของกันและกันได้แต่การ Jailbreak และ Root จะทำให้ระบบปฏิบัติการที่เคยแยกกันกลายเป็นระบบปฏิบัติการที่เปิดกว้างให้แต่ละ Application สามารถมองเห็นการทำงานของกันและกันได้จึงกลายเป็นช่องทางให้มิจฉาชีพสร้าง Application ขึ้นมาเพื่อสอดแนมการเข้าใช้ธนาคารออนไลน์

4. แนวทางการจัดการความเสี่ยงการทำธุรกรรมผ่านอินเตอร์เน็ต

การทำธุรกรรมผ่านอินเทอร์เน็ต ถึงระบบจะดีเพียงใดแต่ก็ยังมีจุดอ่อนให้พวกมิจฉาชีพเข้ามาแสวงหาผลประโยชน์อยู่เสมอ ดังนั้นเราจึงควรจัดการกับความเสี่ยงเหล่านี้ โดย

4.1 ป้องกันการถูกแอบอ้างใช้งานธนาคารออนไลน์

4.1.1 ออกสู่ระบบ (log out) ทุกครั้งหลังเลิกใช้งานระบบออนไลน์เพื่อป้องกันการแอบอ้างการใช้งาน

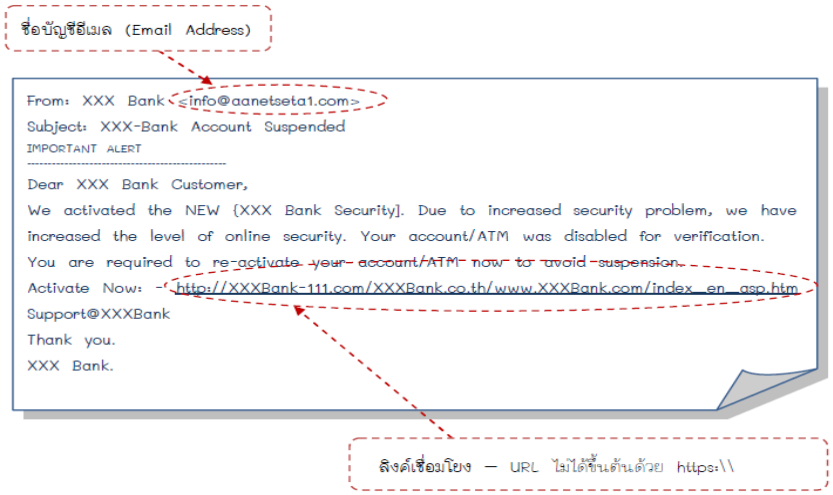
4.1.2 ไม่ให้ข้อมูลส่วนตัวเช่นหมายเลขบัตรเครดิตเลขที่บัญชีเงินฝากรหัสผ่านต่างๆแก่บุคคลอื่นเพราะอาจถูกนาไปใช้แอบอ้างใช้ทำธุรกรรมทางการเงินได้

4.2 ป้องกันการหลอกลวงทางอินเตอร์เน็ต

4.2.1 สังเกตอีเมล์ปลอม

- พิจารณาชื่อบัญชีอีเมล์ (Email Address) ว่าเป็นขององค์กรหรือเจ้าหน้าที่ขององค์กรที่ถูกแอบอ้างจริงหรือไม่หากเป็นองค์กรหรือเจ้าหน้าที่ขององค์กรจริงชื่อบัญชีอีเมล์มักต่อท้ายด้วยชื่อย่อขององค์กรนั้นๆเช่น xxx@bot.or.th เป็นบัญชีอีเมล์ของธนาคารแห่งประเทศไทยโดยย่อมากจาก Bank of Thailand เป็นต้นแต่ควรตรวจสอบควบคู่ไปกับลิงค์เชื่อมโยงที่แนบมากับอีเมล์ด้วย

- ตรวจสอบลิงค์เชื่อมโยงเว็บไซต์ว่า URL ที่ให้เชื่อมโยงไปนั้นเป็นของเว็บไซต์ที่เราเคยใช้บริการอยู่เป็นประจาหรือไม่หากเป็นเว็บไซต์ระบบธนาคารออนไลน์จะต้องมี “s” ต่อท้าย https:\\ ซึ่งหมายถึงการเข้าระบบความปลอดภัยหากไม่มีให้สงสัยว่าเป็นอีเมล์แอบอ้างนอกจากนี้หากเป็นการทำธุรกรรมทางการเงินสถาบันการเงินไม่มีนโยบายในการส่งลิงค์เชื่อมโยงเข้าสู่เว็บไซต์เพื่อทำธุรกรรมการเงินผ่านอีเมล์ที่ส่งถึงผู้ใช้บริการหากมีอีเมล์แอบอ้างแจ้งให้เชื่อมโยงเข้าสู่เว็บไซต์เพื่อทำธุรกรรมการเงินให้สงสัยว่าเป็นอีเมล์จากมิจฉาชีพ



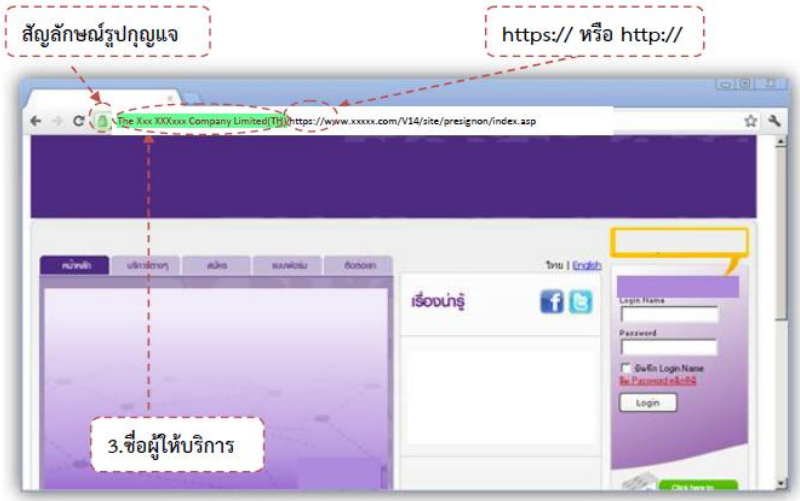
ภาพที่ 5. ภาพตัวอย่างการสังเกตอีเมล์ปลอม

4.2.2 สังเกตเว็บไซต์ปลอม

- สังเกต “**สัญลักษณ์รูปกุญแจ**” เพราะระบบธนาคารออนไลน์จะต้องมีการเข้ารหัสปลอดภัยที่หน้าเว็บไซต์ที่ให้ลงชื่อเข้าใช้ระบบโดยสัญลักษณ์รูปกุญแจแสดงในส่วนของเว็บบราวเซอร์ (Web browser) ซึ่งตำแหน่งของสัญลักษณ์อาจแตกต่างกันไปตามประเภทของเว็บบราวเซอร์

- สังเกต “**URL**” ของเว็บไซต์ระบบธนาคารออนไลน์ว่ามีการเข้ารหัสความปลอดภัยโดยขึ้นต้นด้วย https:// หรือไม่หากพบว่าเว็บไซต์ (หน้าลงชื่อเข้าสู่ระบบ) http:// (ไม่มี s)ให้สงสัยว่าเป็นเว็บปลอม

-สังเกต “**ชื่อผู้ให้บริการ**” ว่าถูกจดทะเบียนภายใต้ชื่อสถาบันการเงินใดโดยสามารถสังเกตได้จากตัวอักษรที่อยู่ถัดจากรูปกุญแจหรือโดยการคลิกที่สัญลักษณ์รูปกุญแจจะเห็นชื่อสถาบันการเงินซึ่งสามารถตรวจสอบดูได้ว่าเป็นชื่อของสถาบันการเงินที่เราใช้บริการหรือไม่



ภาพที่ 6. ภาพตัวอย่างการสังเกตเว็บไซต์ปลอม

4.3 หลีกเลี่ยงเข้าเว็บไซต์ธนาคารออนไลน์จากสมาร์ทโฟนหรือแท็บเล็ต

4.3.1 หากต้องการทำธุรกรรมทางการเงินผ่านสมาร์ทโฟนหรือแท็บเล็ตควรใช้แอพพลิเคชั่น (Application) ของธนาคารโดยตรง

4.3.2 หลีกเลี่ยงการเข้าใช้เว็บไซต์ธนาคารออนไลน์ผ่านสมาร์ทโฟนและแท็บเล็ตบางรุ่นที่ไม่แสดงสัญลักษณ์รูปกุญแจซึ่งเป็นสัญลักษณ์แสดงความปลอดภัยของเว็บไซต์(SSL)

4.3.3 หลีกเลี่ยงการใช้งานธนาคารออนไลน์ผ่านสมาร์ทโฟนและแท็บเล็ตที่ผ่านการ Jailbreakหรือรูท (Root) แล้วเพราะมีความเสี่ยงที่จะถูกขโมยข้อมูลหรืออาจถูกเชื่อมต่อเข้าสู่เว็บไซต์ธนาคารออนไลน์ปลอมโดยไม่รู้ตัว

4.3.4 ล็อคหน้าจอการเข้าใช้สมาร์ทโฟนหรือแท็บเล็ตด้วยรหัสผ่าน (Password) ที่ยากต่อการเดา เพื่อป้องกันการแอบอ้างใช้บริการธนาคารออนไลน์หากสมาร์ทโฟนหรือแท็บเล็ตสูญหายหรือถูกขโมย

4.4 ป้องกันโปรแกรมอันตรายต่างๆ

4.4.1 หลีกเลี่ยงการติดตั้งระบบปฏิบัติการและโปรแกรมที่ไม่มีลิขสิทธิ์เพื่อป้องกันโทรจัน/สปายแวร์ที่อาจแฝงอยู่ในโปรแกรม

4.4.2 ควรติดตั้งโปรแกรมรักษาความปลอดภัยพวก Personal Firewall โปรแกรม Antivirusหมั่นอัพเดตให้เป็นเวอร์ชั่นล่าสุดอยู่เสมอ และหมั่นสแกนตรวจสอบไวรัสคอมพิวเตอร์บ่อยๆ ด้วย

4.4.3 ในกรณีที่ใช้ระบบปฏิบัติการ Windows ควรเปิดใช้งาน Windows Firewalls และควรอัพเดทโปรแกรมความปลอดภัยของระบบปฏิบัติการ (Security Patch) อย่างสม่ำเสมอ

4.4.4 ตรวจหาไวรัส (Scan Virus) ทุกครั้งก่อนใช้บริการธนาคารออนไลน์

4.4.5 หากต้องการทำธุรกรรมทางการเงินให้ใช้คอมพิวเตอร์ของตนเองเพื่อป้องกันการขโมยข้อมูลโดยโทรจัน/สปายแวร์ที่อาจแฝงตัวอยู่ในคอมพิวเตอร์สาธารณะและหลีกเลี่ยงการเชื่อมต่อหรือเข้าสู่ระบบจากอินเตอร์เน็ตสาธารณะรวมไปถึงการเชื่อมต่อกับฟรีWifiเพราะอาจเชื่อมต่อกับwifi ปลอม ที่มิจฉาชีพสร้างขึ้นมา

4.4.6 หากเป็นไปได้ควรแยกเครื่องคอมพิวเตอร์ที่ใช้สำหรับทำธุรกรรมทางการเงินกับเครื่องคอมพิวเตอร์ที่ใช้ท่องโลกออนไลน์หรือทำงานอื่น เพื่อการใช้งานธนาคารออนไลน์ที่ปลอดภัย

4.5 ติดตามข่าวสารกลโกงและภัยทางการเงิน

ติดตามข่าวสารกลโกงและภัยการเงินอย่างสม่ำเสมอทั้งจาก website ของธนาคารแห่งประเทศไทย website ของสถาบันการเงินต่างๆหรือสื่อสิ่งพิมพ์ต่างๆเพื่อป้องกันภัยทางการเงินที่อาจเกิดขึ้น

5. ข้อดี การทำธุรกรรมผ่านอินเทอร์เน็ต

การทำธุรกรรมผ่านอินเตอร์เน็ตเป็นอีกช่องทางหนึ่งที่สะดวกสบายในยุคโลกการสื่อสารไร้พรมแดน เพราะไม่ต้องเสียเวลาในการเดินทาง ซึ่ง

5.1 เราสามารถดูข้อมูลบัญชีต่างๆ ล่าสุดของท่านได้อย่างรวดเร็ว และทันใจ

5.2 ปลอดภัยและใช้งานง่าย เพียงใช้รหัสประจำตัวบริการธนาคารทางอินเทอร์เน็ต (iBanking) ควบคู่กับรหัสผ่าน ก็สามารถทำธุรกรรมต่างๆ ด้วยความมั่นใจในความปลอดภัยในการทำรายการ เพียงใช้แถบเครื่องมือและปุ่มเลือกบนหน้าจอที่ใช้งานง่ายและไม่ซับซ้อน

5.3 รวดเร็ว ใช้เวลาเพียงไม่กี่นาทีในการเรียกดูข้อมูลบัญชีล่าสุด และการทำรายการ ทำให้มีเวลาในการทำสิ่งต่างๆ ได้มากขึ้น

5.4 สะดวกสบาย สามารถทำรายการทางออนไลน์ได้อย่างสะดวกสบายไม่ว่าอยู่ที่บ้านหรือสำนักงาน

5.5 บริการตลอด 24 ชั่วโมง เป็นบริการที่ท่านสามารถทำธุรกรรมต่างๆ จากบัญชีธนาคารเราได้ตลอดเวลาทั้งกลางวันและกลางคืน โดยไม่จำเป็นต้องรอใบแจ้งรายการบัญชีจากธนาคาร

5.6 ใช้บริการได้จากทั่วทุกมุมโลก เพียงใช้อินเทอร์เน็ตได้ ก็จะสามารถทำธุรกรรมจากบัญชีธนาคารแสตนดาร์ดชาร์เตอร์ได้จากทุกสถานที่ทั่วโลก

5.7บริการหลากหลาย ซึ่งช่วยให้จัดการเรื่องการเงิน การธนาคารได้ดียิ่งขึ้น นอกจากนี้ ธนาคารจะพัฒนาการให้บริการ รวมทั้งเพิ่มบริการใหม่ ๆ อยู่เสมอเพื่อเพิ่มความสะดวกสบายในการใช้บริการ

6. ข้อด้อย การทำธุรกรรมผ่านอินเทอร์เน็ต

ถึงแม้การทำธรกรรมผ่านอินเทอร์เน็ตจะมีข้อดีอยู่ไม่น้อย แต่เพราะเป็นการทำธุรกรรมผ่านอินเทอร์เน็ตจึงมีความซับซ่อนอยู่บ้างที่ต้องเรียนรู้ และยังมีข้อจำกัดอยู่เช่นกัน

6.1 ใช้เวลาในการเรียนรู้รูปแบบเว็บ ผู้ที่เข้าใช้เว็บธนาคารออนไลน์ครั้งแรก อาจจะสับสนกับรูปแบบการใช้งาน ซึ่งต้องใช้เวลาศึกษา

6.2 เสียเวลาในการลงทะเบียน อาจต้องเสียเวลาในการลงทะเบียน เช่นกรอกชื่อ ที่อยู่ และข้อมูลส่วนตัว หมายเลขบัญชี และรหัสส่วนตัว เนื่องจากการใช้งานธนาคารออนไลน์ต้องการความปลอดภัยและความเป็นส่วนตัวของผู้ใช้งาน

6.3 อาจขาดความน่าเชื่อถือ บางคนจะไม่ค่อยเชื่อถือการทำธุรกรรมออนไลน์ เนื่องจากไม่มั่นใจว่าระบบป้องกันความปลอดภัย จะมีประสิทธิภาพหรือไม่

6.4 ที่อยู่เว็บอาจเปลี่ยนแปลง แม้แต่ธนาคารขนาดใหญ่ก็อาจมีโอกาสเปลี่ยนที่อยู่เว็บหรือเปลี่ยนรูปแบบทั้งหมดได้บางกรณีผู้ใช้อาจต้องลงทะเบียนสมัครสมาชิกใหม่

6.5 มีความเสี่ยงจากภัยคุกคามในรูปแบบอื่นๆ เช่นการติดไวรัสคอมพิวเตอร์ หรือการแฮกเกอร์เจาะระบบ

6.6อาจเกิดปัญหาเว็บไซต์ปลอมที่มักจะแฝงตัวมากับลิงค์ต่างๆซึ่งเสี่ยงต่อการถูกดักจับข้อมูลการใช้งานจากหน้าเว็บเช่น (Username) และรหัสผ่าน (Password) เพื่อนำไปแอบอ้างการเข้าใช้งาน

6.7 การทำธุรกรรมรูปแบบนี้สามารถ ใช้บริการได้เฉพาะอุปกรณ์ที่รองรับและบริเวณที่มีสัญญาณอินเทอร์เน็ตเท่านั้น

สรุป

ธุรกรรม คือ การประกอบกิจกรรม อย่างใดอย่างหนึ่งระหว่างคู่สัญญาสองฝ่าย โดยเฉพาะด้านธุรกิจและการเงิน ส่วน การทำธุรกรรมผ่านอินเทอร์เน็ต คือ การประกอบธุรกิจการพาณิชย์อิเล็กทรอนิกส์เกี่ยวกับการให้บริการทำธุรกรรมทางการเงินต่างๆผ่านอุปกรณ์หรือระบบอิเล็กทรอนิกส์ เช่น โทรศัพท์มือถือ หรือ อินเตอร์เน็ตมีการให้บริการเช่น การฝากเงิน ถอนเงิน โอนเงิน หรือ สอบถามยอดเงิน

รูปแบบการทำธุรกรรมผ่านอินเทอร์เน็ตหลักๆก็คือ รูปแบบของ ธนาคารอินเทอร์เน็ต(Internet Banking)การชำระเงินออนไลน์(Payment Gateway or Bill payment)แต่การทำธุรกรรมผ่านอินเตอร์เน็ตก็ยังมีความเสี่ยงต่างๆ เช่น Phishing คือ การหลอกลวงทางอินเตอร์เน็ตในรูปแบบของการปลอมแปลง e-mail หรือสร้าง Website ปลอม เพื่อหลอกให้ลูกค้าเปิดเผยข้อมูลทางด้านการเงิน หรือข้อมูลส่วนตัวต่างๆ เช่น ข้อมูลหมายเลขบัตรเครดิตUsername และ Password เป็นต้น ซึ่งสร้างความเสียหายทางการเงินต่อลูกค้าและสถาบันการเงิน รวมทั้งส่งผลกระทบต่อความเชื่อมั่นของลูกค้าในการใช้บริการการเงินทางอิเล็กทรอนิกส์

ซึ่งในปัจจุบันการทำธุรกรรมผ่านอินเตอร์เน็ตได้รับความนิยมมากขึ้น เพราะเป็นอีกช่องทางหนึ่งที่สะดวกสบายในยุคโลกการสื่อสารไร้พรมแดน สามารถทำได้ทุกที่ ทุกเวลา ไม่ต้องเสียเวลาในการเดินทาง และถึงแม้การทำธุรกรรมผ่านอินเทอร์เน็ตจะมีข้อดีอยู่ไม่น้อย แต่อย่างไรก็ตาม ยังมีความซับซ้อน มีข้อจำกัดในการใช้งานอยู่เช่นกัน ต้องกระทำอย่างละเอียดรอบคอบ เพื่อจะได้ไม่ตกเป็นเหยื่อของมิจฉาชีพ

เพราะในการทำธุรกรรมผ่านอินเทอร์เน็ตในปัจจุบัน ยิ่งสะดวกสบายมากเท่าไหร่ ความปลอดภัยในการใช้งานก็ยิ่งน้อยลง ดังนั้นจึงควรติดตามข่าวสารกลโกงและภัยการเงินอย่างสม่ำเสมอ ทั้งจาก website ของธนาคารแห่งประเทศไทย website ของสถาบันการเงินต่างๆหรือสื่อสิ่งพิมพ์ต่างๆ เพื่อป้องกันภัยทางการเงินที่อาจเกิดขึ้น