

"ระวัง!! โจร-ออนไลน์ ล้วงกระเป๋า"

ปัจจุบัน Internet Banking ซึ่งเป็นช่องทางการให้บริการธุรกรรมทางการเงิน พื้นฐานผ่านทางอินเทอร์เน็ตที่ช่วยเพิ่มช่องทางให้สามารถทำธุรกรรมทางการเงิน พื้นฐาน เช่น การเช็คยอดบัญชี การโอนเงินและบริการด้วยตนเองผ่านทาง อินเทอร์เน็ตกำลังนิยมอย่างแพร่หลาย ทำให้ช่องทางนี้เป็นที่สนใจในหมู่โจรไฮเทค ที่มาพร้อมกับกลอุบายที่แยบยลเพื่อหลอกลวงล้วงกระเป๋าตั้งค่อออนไลน์ของเรา เรา จึงจำเป็นที่จะต้องรู้เท่าทันกลลวงเหล่านี้ เพื่อให้ใช้ Internet Banking ได้อย่าง มั่นใจ ไร้กังวล



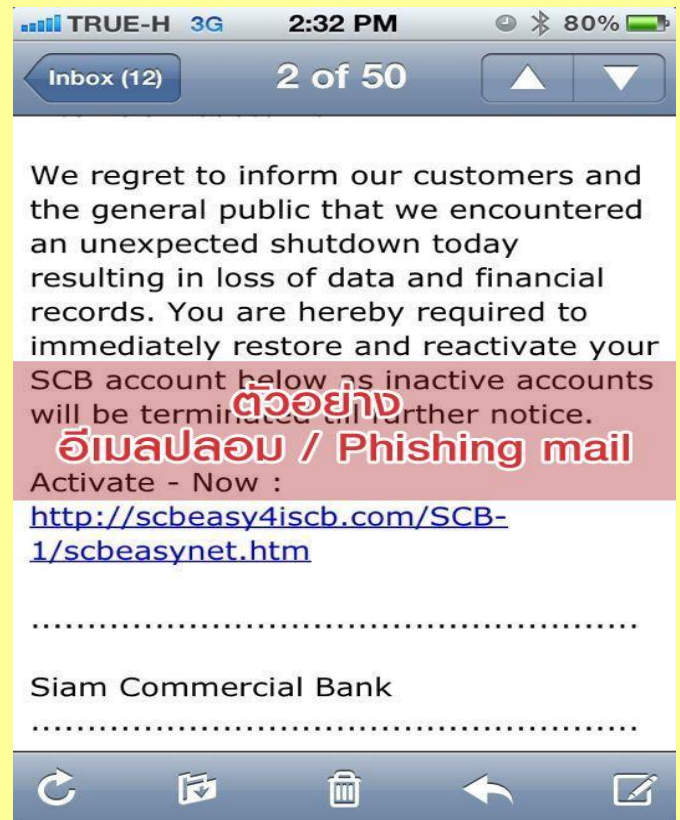
ทำความรู้จักกับ PHISHING



Phishing (ฟิชชิ่ง) คือ กลวิธีในการ หลอกลวงเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล อันจะนำไปสู่การแสวงหาผลประโยชน์ซึ่งอาจก่อให้เกิดความเดือดร้อนแก่ผู้ที่ถูกล่อลวง ข้อมูลส่วนบุคคลที่กล่าวถึงนี้มักจะเป็น รหัสประจำตัวต่าง ๆ , รหัสในการเข้าใช้งานระบบ , รหัสผ่าน , เลขที่บัตรเครดิต , เลขที่บัญชี หรือ เลขที่บัตรประชาชน

กลวิธีในการหลอกลวงแบบต่าง ๆ

ผ่าน **e-Mail** โดยการปลอมแปลงลักษณะของ e-Mail ให้ดูเหมือนถูกส่งมาโดยธนาคาร สถาบันการเงินหรือบริษัทห้างร้านที่มีชื่อเสียง ซึ่งมักมีเครื่องหมายการค้า สี และรูปแบบเหมือนกับถูกส่งมาจากบริษัทดังกล่าวจริง โดยเนื้อหาของ e-Mail จะเป็นการบอกให้ผู้ใช้บริการดำเนินการบางอย่างใดอย่างหนึ่ง ซึ่งที่พบได้มากคือการหลอกลวงให้คลิกลิ้งค์ที่อยู่ใน e-Mail เพื่อทำการกรอกข้อมูลต่าง ๆ ผู้ใช้บริการอาจได้รับข้อความในเชิงเตือน หรือขู่ เช่น "หากไม่ดำเนินการภายใน 15 วัน ทางบริษัทมีความจำเป็นต้องปิดบริการของท่าน"



สร้างเว็บไซต์เลียนแบบ มักใช้กับเว็บไซต์ทางการเงิน เช่น ธนาคารออนไลน์ เป็นช่องทางที่นำไปสู่บัญชีที่เก็บเงินของลูกค้าได้ดีที่สุด ผู้ทำ Phishing จะทำการโอนเงินไปยังบัญชีปลายทาง (ถูกเปิดขึ้นเพื่อรอรับเงินที่ทุจริต) จากนั้นคนร้ายจะไปถอนเงินออกจากบัญชีจนหมดสิ้น



ทางโทรศัพท์ โดยการแอบอ้าง
เป็นพนักงานหรือเจ้าหน้าที่ใน
หน่วยงานราชการ ธนาคาร หรือ
บริษัทต่าง ๆ แล้วทำการติดต่อ
ลูกค้าโดยแจ้งให้โอนเงินทาง
ATM ไปยังบัญชีปลายทางซึ่งถูก
เปิดไว้ หรืออาจใช้วิธีหลอกลวง
ข้อมูลส่วนตัวซึ่งสามารถนำไปใช้
ภายหลังเพื่อย้อนกลับมาโจมตี
บัญชีของลูกค้าเองอีกครั้ง

รู้หรือไม่ : ในประเทศไทยนั้นการ Phishing ทางโทรศัพท์เป็นวิธีที่ถูกพบ
บ่อยที่สุด เนื่องจากประชากรส่วนมากยังไม่มีความรู้ในการใช้งานอินเทอร์เน็ต
หรือธนาคารออนไลน์ แต่มีการใช้บัตร ATM กันอย่างกว้างขวาง เป็นเป้าหมาย
กลุ่มใหญ่ที่โจมตีแล้วได้ผลมากกว่า

TROJAN VIRUS



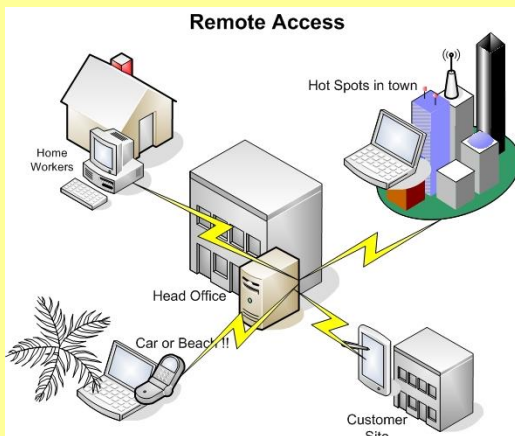
TROJAN VIRUS

มาจาก "ม้าไม้โทรจัน" ในสงครามกรุงทรอย ที่กรีกส่งมาหลอกให้ชาวทรอยคิดว่าเป็นของบรรณาการ แต่กลับซ่อนทหารกรีกที่ซ่อนตัวมาในม้าไม้ เปิดประตูเมืองให้กองทัพกรีกที่เหลือเข้ามาตีกรุงทรอยจนสำเร็จ

ถ้าการรักษาความปลอดภัยของคอมพิวเตอร์ของคุณไม่ดีพอและมีไวรัส TROJAN เข้าไปแฝงอยู่ในคอมพิวเตอร์ ไวรัสจะเชื่อมโยงคอมพิวเตอร์คุณเข้ากับเว็บไซต์ปลอมโดยไม่รู้ตัว เมื่อคุณ Login เข้าเว็บไซต์ Internet Banking จะถูกขโมย Username และ Password ของคุณไปทันที

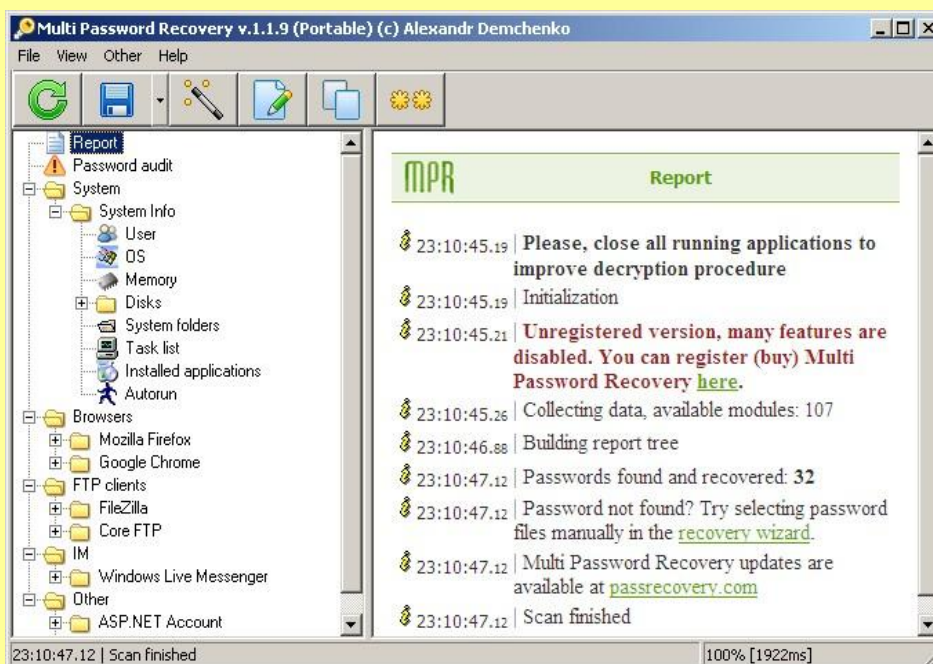


โปรแกรมโทรจัน แบ่งออกเป็น 3 ชนิดหลัก ๆ ดังนี้



โปรแกรมเข้าถึงเครื่องคอมพิวเตอร์จากทางไกล (Remote Access Tools – RATs) โปรแกรมประเภทนี้จะทำให้ผู้บุกรุกระบบจากทางไกล เช่น โดยผ่านทางเครือข่ายเข้ามาสามารถเข้าถึงเครื่องคอมพิวเตอร์ที่ถูกติดตั้งโทรจันลงไป

ตัวจับการพิมพ์แป้นคีย์บอร์ด (Key Loggers) โปรแกรมประเภทนี้ จะบันทึกการพิมพ์จากแป้นคีย์บอร์ดทั้งหมดที่ป้อนเข้าเครื่อง แล้วรวบรวมส่งเป็นไฟล์ให้ผู้บุกรุกต่อไป



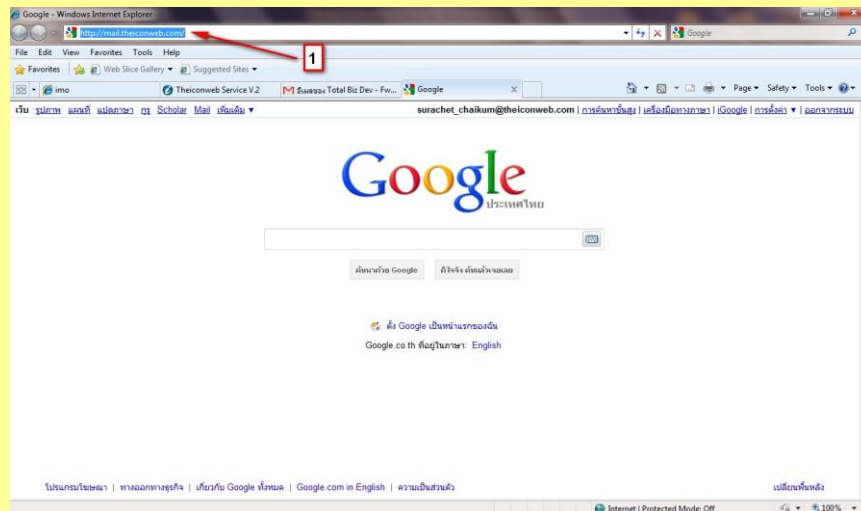
ตัวจับรหัสผ่าน (Password Retrievers) โปรแกรมประเภทนี้จะนำส่งไฟล์รหัสผ่านในเครื่องของผู้ใช้ให้แก่ผู้บุกรุก

คำแนะนำเพิ่มเติมเพื่อป้องกันการทุจริตจากโปรแกรมโทรจัน (Trojan)

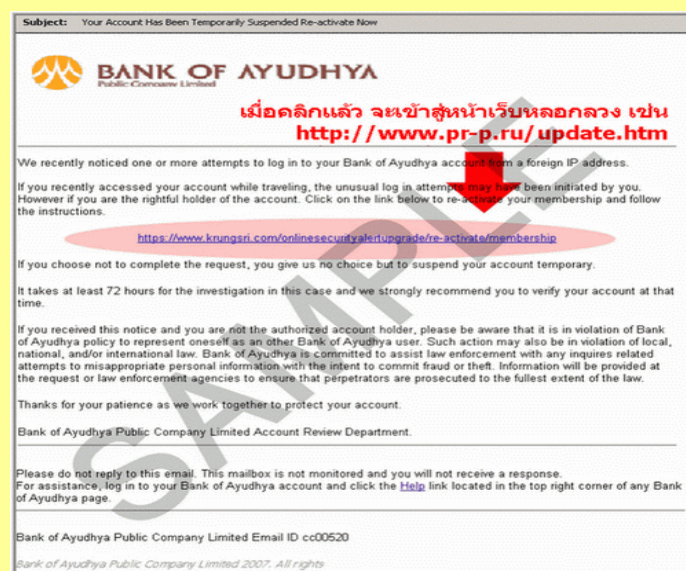
ในการใช้ Internet Banking ทุกครั้งที่ทำการรายการเพิ่มบัญชีบุคคลอื่น จะต้องตรวจสอบ “เลขที่บัญชี” ซึ่งปรากฏใน OTP-SMS (One Time Password) ที่ระบบส่งไปยังโทรศัพท์มือถือรวมทั้ง e-mail ยืนยันการเพิ่มบัญชีในครั้งนั้น เพื่อให้แน่ใจว่าเป็นหมายเลขบัญชีที่ต้องการ ก่อนที่จะนำรหัส OTP มากรอกลงในระบบเพื่อยืนยันการทำการรายการเพิ่มบัญชีและรายการโอนเงินไปยังบัญชีนั้น เนื่องจากหากมีโปรแกรมโทรจัน (Trojan) แอบฝังตัวอยู่บนเครื่องคอมพิวเตอร์ โปรแกรมโทรจันนั้นอาจจะสามารถเปลี่ยนแปลงเลขที่บัญชีก่อนส่งข้อมูล

ปลอดภัยไว้ก่อน

- เข้าสู่หน้าเว็บไซต์ด้วยการพิมพ์ URL โดยตรงด้วยตัวท่านเองทุกครั้งที่ต้องการใช้บริการธนาคารทางอินเทอร์เน็ต และตรวจสอบชื่อเว็บไซต์ในช่อง Address ให้แน่ใจก่อน Login เพื่อให้มั่นใจว่า ได้เข้าสู่เว็บไซต์นั้นอย่างแท้จริง



- เมื่อเสร็จสิ้นการใช้งานในแต่ละครั้ง ควรล้างหน่วยความจำคอมพิวเตอร์ (cache) และล้างบันทึกประวัติการใช้งาน (history settings) ในเว็บเบราว์เซอร์ เพื่อลบข้อมูลบัญชีทั้งหมด ลดโอกาสที่ผู้อื่นจะสามารถเข้าถึงข้อมูลส่วนตัวได้ และให้ทำการ log off ปิดเบราว์เซอร์ทั้งหมดที่เปิดใช้งานทุกครั้ง ห้ามละทิ้งคอมพิวเตอร์ไว้ หากท่านยังทำธุรกรรมทางการเงินไม่เสร็จ
- หลีกเลี่ยงการคลิกลิงค์ (Link) ที่แนบมากับ e-Mail เพื่อการเข้าสู่หน้าเว็บไซต์ เป็นการป้องกันมิให้เฟลอคคลิกเข้าสู่เว็บไซต์ปลอมที่กลุ่มผู้กระทำการทุจริตนั้นเตรียมไว้



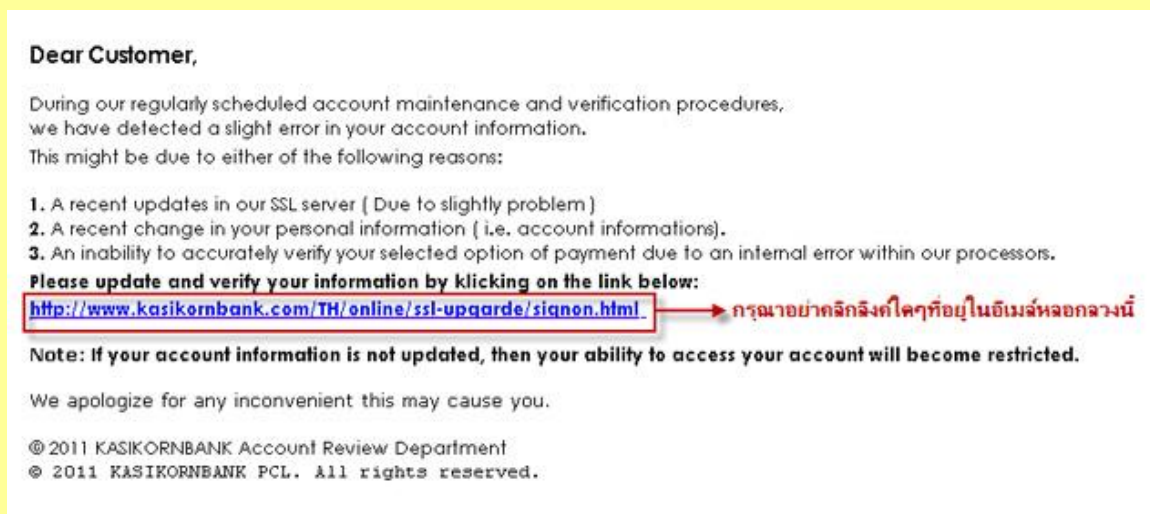
➤ เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

คำแนะนำเกี่ยวกับการตั้งรหัสผ่าน

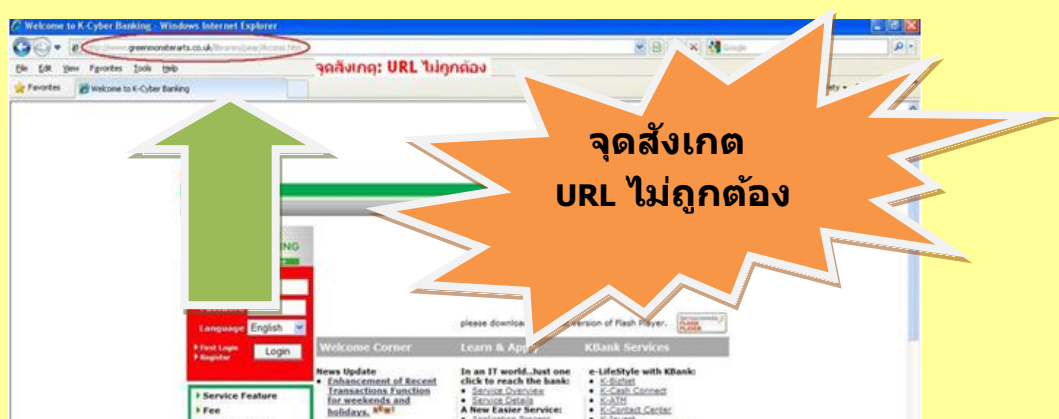
- ❖ ไม่ใช่คำใด ๆ ที่มีอยู่ในพจนานุกรมไม่ว่าจะเป็นพจนานุกรมภาษาใด ๆ ก็ตาม รวมทั้งคำศัพท์ทางวิทยาศาสตร์ด้วย
- ❖ ไม่ใช่คำใด ๆ ที่สะกดกลับทาง ซึ่งเป็นคำที่มาจากพจนานุกรม เช่น flower สะกดกลับเป็น rewolf
- ❖ ไม่ใช่คำใด ๆ ที่เกี่ยวข้องกับตัวเรา เช่น ที่อยู่ หมายเลขโทรศัพท์ วันเกิด ชื่อสัตว์เลี้ยง ชื่อเล่น งานอดิเรก หรือกีฬาที่ชอบ
- ❖ ไม่ใช่ตัวอักษรหรือตัวเลขที่เรียงกัน เช่น "abcdefg" หรือ "1234"
- ❖ ไม่ใช่ตัวอักษรที่เรียงกันตามแป้นพิมพ์ เช่น "qwerty"
- ❖ ให้ใช้ตัวอักษร ตัวเลข และตัวอักษรพิเศษ ร่วมกันแบบสุ่ม
- ❖ ให้ใช้ตัวอักษรทั้งตัวพิมพ์เล็กและตัวพิมพ์ใหญ่ในภาษาอังกฤษและใช้ตัวอักษรพิเศษร่วมด้วย เช่น * @ #
- ❖ ให้ใช้รหัสผ่านที่มีความยาวอย่างน้อย 6 ตัว ยิ่งรหัสผ่านมีความยาวเท่าใดก็ยิ่งมีความยากต่อการเดา เท่านั้น
- ❖ ไม่จดรหัสผ่านเก็บไว้ไม่ว่าจะในที่ใด ๆ ก็ตาม และให้ระมัดระวังคนที่นั่งหรือยืนใกล้ ๆ ซึ่งอาจแอบมองจากด้านหลังเพื่อขโมยบัญชีผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนตัวอื่น ๆ ในขณะที่ผู้ใช้กำลังป้อนข้อมูลเหล่านั้นเข้าเครื่อง
- ❖ ไม่บอกรหัสผ่านกับผู้อื่นไม่ว่าจะด้วยเหตุผลใด ๆ ก็ตาม
- ❖ ไม่ใช่ตัวเลือกให้จำรหัสผ่านที่มีอยู่ในเว็บไซต์บางเว็บหรือโปรแกรมที่ใช้ งานบางโปรแกรม และให้ปิดความสามารถนี้ในโปรแกรมเบราว์เซอร์ที่ใช้งาน โดยคลิกตัวเลือกการจำรหัสผ่านออก
- ❖ ไม่ใช้รหัสผ่านเดียวกันเพื่อเข้าโปรแกรมต่าง ๆ ที่ใช้งาน

- หลีกเลี่ยงการใช้คอมพิวเตอร์สาธารณะ และระมัดระวังการเชื่อมต่อกับเครือข่าย WiFi สาธารณะหรือเครือข่ายที่ไม่ปลอดภัย เช่น ในอินเทอร์เน็ตคาเฟ่ โดยไม่ป้อนข้อมูลลับ หรือส่วนตัวที่เป็นความลับใด ๆ โดยผ่านเครื่องคอมพิวเตอร์สาธารณะ
- หากพบความผิดปกติของหน้าจอขณะทำรายการผ่านบริการธนาคาร โปรดหยุดทำรายการทันที ไม่ต้องปฏิบัติตามคำแนะนำใด ๆ ทั้งสิ้น และกรุณาออกจากเว็บไซต์ที่น่าสงสัยทันที

ตัวอย่างอีเมลหลอกลวง



ตัวอย่างเว็บไซต์ปลอม

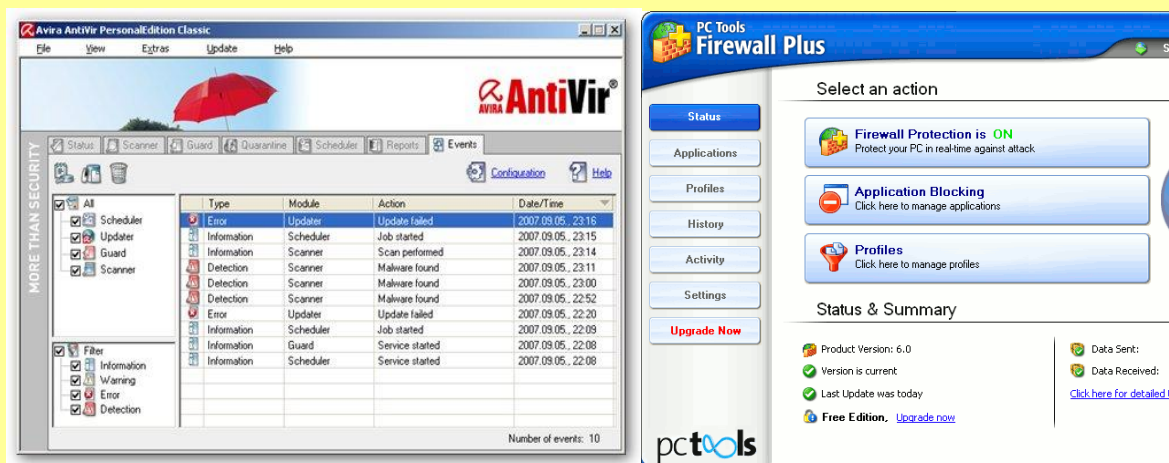


เมื่อได้รับอีเมลหลอกลวงหรือพบเว็บไซต์ปลอม (Phishing Website) หรือได้กรอกข้อมูลไปในเว็บไซต์ปลอม (Phishing Website) แล้ว ควรติดต่อไปยังหน่วยงาน call center ของบริษัท ธนาคาร หรือสถาบันการเงินนั้น ๆ โดยเร็วที่สุด เพื่อทำการเปลี่ยนแปลงรหัสผ่าน (Password) หรืออายัดบัญชี เนื่องจากทางบริษัท ธนาคาร หรือสถาบันการเงินไม่มีนโยบายส่งอีเมลที่มี Link ให้คลิกเพื่อเข้าสู่ระบบใด ๆ ของธนาคาร หรือสอบถามข้อมูลส่วนตัวใด ๆ ผ่านทางอีเมล หากต้องการใช้บริการหรือระบบใด ๆ จะต้องพิมพ์ URL เพื่อเข้าสู่เว็บไซต์ด้วยตัวท่านเอง หรือเข้าจาก Favorite/Bookmark ที่สร้างด้วยตนเองเท่านั้น

- ระมัดระวังไม่หลงเชื่อข้อความใด ๆ ใน e-Mail หรือโทรศัพท์ที่ได้รับ หากมีการอ้างว่าส่งหรือติดต่อมาจากสถาบัน หรือบริษัทใดก็ตาม ควรค้นหาหมายเลขโทรศัพท์ของสถาบันหรือบริษัทนั้น หรือติดต่อไปยังหน่วยงาน Call Center ของบริษัทนั้น ๆ หรือให้ไปติดต่อที่ธนาคารที่ถูกอ้างชื่อสาขาใดก็ได้ (อย่าติดต่อไปตามหมายเลขโทรศัพท์ที่มีอยู่ใน e-Mail ต้องสงสัยฉบับนั้น) เพื่อให้ทำการตรวจสอบว่ามีการส่ง e-Mail ลักษณะดังกล่าวจริงหรือไม่ หรือส่งมาจากหน่วยงานใด หากมีข้อสงสัยสามารถโทรศัพท์สอบถามได้ที่ ศูนย์ประสานงานแก้ไขปัญหาการปล่อยสินเชื่อ (ศปส.) หมายเลขโทรศัพท์ 02-283-5900 ในวันทำการ ตั้งแต่เวลา 8.30 – 16.30 น.



- ติดตั้งโปรแกรม Personal Firewall และซอฟต์แวร์ป้องกันไวรัส (Anti-Virus) ที่ถูกลิขสิทธิ์และเชื่อถือได้ และควรตรวจสอบโปรแกรมป้องกันไวรัส และทำการอัปเดตฐานข้อมูลไวรัสให้เป็นเวอร์ชันล่าสุดอยู่เสมอ รวมทั้งอัปเดตการปรับปรุงด้านความปลอดภัย (Update Microsoft Security Patch) สำหรับซอฟต์แวร์บนคอมพิวเตอร์และอินเทอร์เน็ตอยู่เสมอ เพื่อปิดช่องโหว่ที่ไวรัสและมัลแวร์อาจใช้เป็นช่องทางบุกรุกเข้าสู่ระบบ และหมั่นสแกนตรวจจับไวรัสในคอมพิวเตอร์



- หลีกเลี่ยงการดาวน์โหลดโปรแกรม หรือข้อมูลจากเว็บไซต์ที่ไม่น่าเชื่อถือและไม่มั่นใจในความปลอดภัย



- ควรลบอีเมลที่น่าสงสัยว่ามีไวรัสแนบมา อีเมลขยะ อีเมลลูกโซ่ หรืออีเมลล่อลวงทั้งหมดที่อย่าตอบกลับอีเมลใด ๆ ที่ขอให้เปิดเผยข้อมูลส่วนบุคคล โปรดตั้งข้อสงสัยไว้เมื่อพบว่า มีอีเมลจากธุรกิจหรือบุคคลใดที่พยายามให้ผู้ให้บริการเปิดเผยรหัสผ่าน หมายเลขบัญชี หรือข้อมูลใด ๆ ที่เป็นความลับ หรืออีเมลใดที่ส่งข้อมูลส่วนบุคคลของผู้ใช้บริการมาเพื่อให้ปรับปรุงข้อมูล หรือยืนยันความถูกต้อง และไม่ควรรันไฟล์ที่แนบมากับอีเมลที่ส่งมาจากบุคคลที่ไม่รู้จัก หรือ ไม่ทราบที่มาแน่ชัด ตลอดจนไฟล์ที่ส่งด้วยโปรแกรมแชทต่าง ๆ



- ไม่เปิดเผยข้อมูลส่วนบุคคลใด ๆ ของตนเอง เช่น รหัสประจำตัว (User ID) รหัสผ่าน (Password) รหัสเอทีเอ็ม (ATM PIN) รหัสบัตรเครดิต หมายเลขบัญชี หมายเลขบัตร เลขที่บัตรประชาชน ที่อยู่ เบอร์โทรศัพท์ วันเดือนปีเกิด หรือข้อมูลส่วนบุคคลใด ๆ ผ่านทางอีเมล หรือในระหว่างทำรายการผ่านบริการของธนาคาร เนื่องจากธนาคารไม่มีนโยบายในการดำเนินการสอบถามข้อมูลส่วนบุคคลใด ๆ ของผู้ใช้บริการผ่านช่องทางดังกล่าว

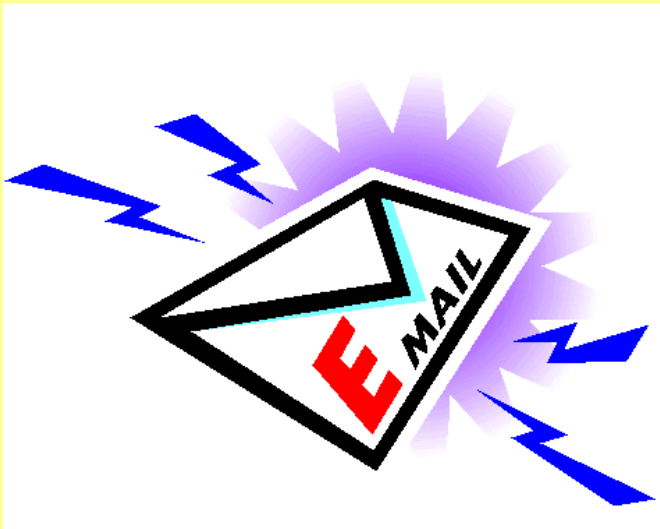


- หมั่นตรวจสอบข้อมูลความถูกต้องของการทำรายการธุรกรรมและบัญชีธนาคารทางอินเตอร์เน็ตอย่างสม่ำเสมอ โดยไม่จำเป็นต้องรอให้ครบ 1 เดือนและตรวจสอบยอดเงินในบัญชีของผู้ใช้บริการอย่างสม่ำเสมอเพื่อป้องกันรายการผิดปกติที่อาจเกิดขึ้น รวมทั้งตรวจสอบใบแจ้งรายการใช้บัตรเครดิตทุกครั้งที่ได้รับ และตรวจสอบให้แน่ใจว่าไม่มีรายการธุรกรรมแปลกปลอม หากพบรายการที่น่าสงสัย ให้ติดต่อธนาคารหรือบริษัทผู้ออกบัตรทันที

เลขที่บัญชี ACCOUNT NUMBER 账户号码					
วันที่ DATE 日期	คำย่อ CODE 代码	ถอน WITHDRAWAL 取款	ฝาก DEPOSIT 存款	ยอดคง BALANCE 余额	รหัสสาขา TELLER NO. 出款点号码
1 01/10/10PC			50.00	20,172.11	23022A
2 05/10/10TRN			500.00	20,572.11	00011A+
3 07/10/10TRN			399.99	21,072.10	00014A*
4 04/12/10PCN			900.00	21,972.10	21429A+
5 04/12/10PCN			300.00	22,272.10	21429A*
6 07/12/10IND		2	24.99	22,297.09	05328A
7 07/12/10TX			0.00	22,297.09	05328A
8 07/12/10CSI			22,297.09	0.00	05328A
9					
10					
11					



- हमันตรวจสอบข้อความแจ้งเตือนต่าง ๆ ที่ธนาคารส่งให้ทั้งทางอีเมลและข้อความทางโทรศัพท์มือถือ (sms) อย่างถี่ถ้วน เพื่อให้ทราบถึงความเคลื่อนไหวในบัญชีและการทำธุรกรรมต่าง ๆ และหากพบความผิดปกติ เช่น หมายเลขบัญชีที่ปรากฏใน SMS ไม่ตรงกับหมายเลขบัญชีที่ต้องการลงทะเบียน , ได้รับความแจ้งเตือนทางอีเมล โดยที่ไม่ได้เข้าใช้งาน เป็นต้น ควรติดต่อธนาคาร สถาบันการเงินนั้นทันที



ด้วยความปรารถนาดีจาก :

ศูนย์บริหารจัดการความเสี่ยง มหาวิทยาลัยมหิดล

ขอขอบคุณแหล่งที่มาของข้อมูล

- ธนาคารทหารไทย จำกัด (มหาชน)
- ธนาคารกรุงเทพ จำกัด (มหาชน)
- ธนาคารกสิกรไทย จำกัด (มหาชน)
- ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)
- คู่มือการใช้งานเครือข่ายอินเทอร์เน็ตอย่างปลอดภัย โดย คณะอนุกรรมการด้านความมั่นคง ภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์

