เดลินิวส์
Daily News
Circulation: 500,000
Ad Rate: 950

Section: First Section/กีฬา - บทความ
วันที่: ศุกร์ 14 เมษายน 2566
ปีที่: - ฉบับที่: 26846 หน้า: 11(กลาง)
Col.Inch: 39 Ad Value: 37,050 PRValue (x3): 111,150 คลิป: ขาว-ดำ
คอลัมน์: จดหมายถึงเดลินิวส์

หงุดหงิดสัญญาณเน็ตไม่ดี อยากให้ปรับปรุงบริการ

เรื่อง สัญญาณโทรศัพท์
เรียน เอก วิภาวดี

ดิฉันใช้โทรศัพท์เครือข่ายหนึ่งอยู่ ตอนแรกก็ปกติสัญญาณชัดเจนดีมาก แต่พอหลังจากมีการรวมตัวของ 2 ค่ายเท่านั้นแหละสัญญาณไม่ดีเลย ทาง 2 ค่ายไม่มีการแจ้งผู้บริโภคเลย อีกอย่างสัญญาณเน็ตก็ไม่ดี มา ๆ หาย ๆ พอไปแจ้งก็ได้รับคำตอบว่ากำลังปรับปรุงการรวมสัญญาณอยู่

ก็เลยอยากรู้ว่า สัญญาณเน็ตจะดีเมื่อไหร่ การรวมกันแล้วทำให้ผู้บริโภคเดือดร้อน ค่าใช้จ่ายแพงเพราะเราต้องการความสะดวกสบายในการทำงาน ในการติดต่อกับลูกค้า ไหนบอกว่ารวมกันแล้วผู้บริโภคจะได้สัญญาณดีขึ้น ไม่เห็นเป็นอย่างที่บอกเลย ใครจะรับผิดชอบเรื่องนี้ เราจ่ายค่าบริการแพงไปเพื่ออะไร ขอถามหน่อย

ผู้ที่เดือดร้อนมาก

ป.ล.ไปติดต่อที่ศูนย์ราชการ ก็ไม่มีอะไรดีขึ้น ก็เลยคิดว่าจะย้ายค่ายดีไหม เพราะค่าใช้จ่ายก็พอ ๆ กัน สัญญาณก็แรงดี ไม่อยากย้ายก็เพราะใช้ค่ายเก่ามานานมาก ตั้งแต่เริ่มมีเงินซื้อโทรศัพท์ใช้เอง แต่หากยังเป็นเช่นนี้คงต้องบอกลา ไปหาค่ายใหม่ดีกว่า

.....

ท่านผู้อ่านที่ปรึ๊ดกับเรื่องสัญญาณเน็ตไม่แรงของค่ายทรูและดีแทค ที่ควบรวมกัน เชื่อว่าเป็นปัญหาอมตะของค่ายมือถือที่พยายามปรับปรุงแก้ไขกันตลอด ปัญหาเรื่องสัญญาณเน็ตไม่แรงนั้นมีปัจจัยร่วมมากมาย เชื่อว่าผู้ให้บริการคงไม่ได้นิ่งนอนใจอย่างแน่นอน ส่วนการจะเลือกใช้ต่อหรือย้ายค่ายนั้นก็แล้วแต่วิจารณญาณและต่อมความอดทนของแต่ละท่านที่จะจัดการกับอารมณ์ตอนหงุดหงิดอย่างไร แต่สิทธิการเลือกใช้อยู่ที่เราตัดสินใจเอาเลยครับ

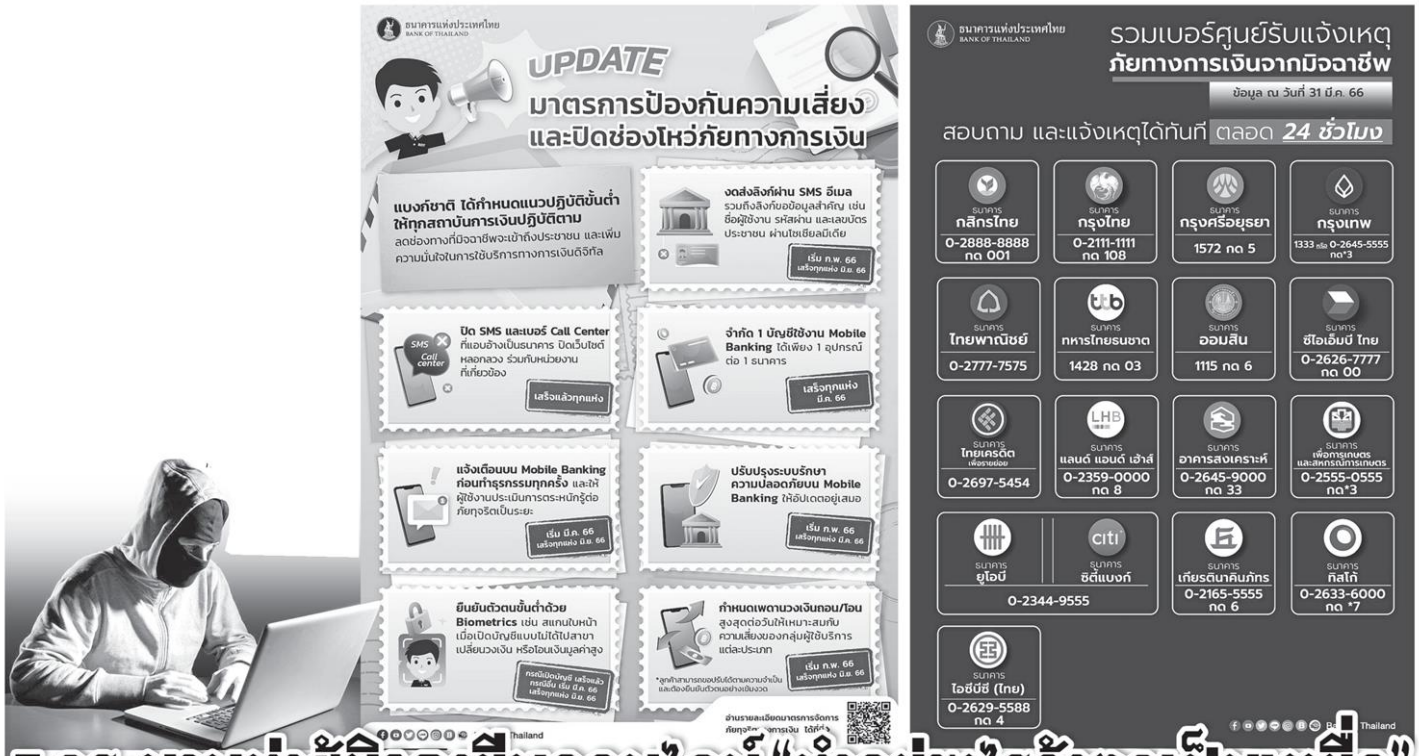
เมื่อพูดถึงดีลการควบรวม 2 ค่ายมือถือเป็นข่าวใหญ่และข่าวดังใช่ย่อย โดย ทรู คอร์ปอเรชั่น มีฐานผู้ใช้บริการทั้งหมดรวมกัน 55 ล้านเลขหมาย แบ่งเป็นจากของค่ายทรู 33.8 ล้านเลขหมาย และค่ายดีแทค 21.2 ล้านเลขหมาย และยังมีคลื่นความถี่จากทั้ง 2 ค่าย ได้แก่ย่านความถี่ระดับต่ำ (Low Band) มีทั้ง 700 MHz, 800 MHz, 900 MHz และย่านความถี่ระดับกลาง (Mid Band) คือ 1800 MHz, 2100 MHz, 2600 MHz รวมถึงเป็นคลื่นความถี่สูง (High band) คือ 25 GHz นอกจากนี้ผู้ใช้บริการยังสามารถเข้าถึงบริการต่าง ๆ ของทั้ง 2 ค่ายได้ทั้งหมดเหมือนกัน

ทางบริษัทได้เริ่มเปิดการ "โรมมิ่ง" หรือเปิดสัญญาณข้ามโครงข่าย เพื่อให้ผู้ใช้บริการทรูและดีแทคสามารถใช้งานคลื่นสัญญาณ 5G และ 4G บนความถี่ 2600 MHz และ 700 MHz ร่วมกันได้โดยลูกค้าจะสามารถสังเกตการเปลี่ยนได้จากสัญลักษณ์เครือข่าย dtac-True และ True-dtac จะอยู่บนหน้าจอมือถือ และบริษัทฯจะเดินหน้าเปิดโรมมิ่งขยายให้ครอบคลุมทั้งประเทศ 77 จังหวัด ซึ่งหมายความว่าลูกค้าของทั้ง 2 ค่าย จะสามารถใช้คลื่นทดแทนกันและกันได้ในทุกพื้นที่

ขณะที่ในประเด็นเรื่องแบรนด์ทรูและดีแทค บริษัทฯ จะยังคงดำเนินงานของทั้ง 2 แบรนด์นี้ต่อไปในช่วงระยะเวลา 3 ปี ตามกฎของ กสทช. นอกจากนี้ ประธานคณะบริหาร TRUE ยืนยันว่า จะไม่มีการปรับลด หรือเพิ่มราคาแพ็กเกจของทั้ง 2 ค่าย โดยจะไม่ทำให้ผู้บริโภคเสียประโยชน์ และได้รับประโยชน์อย่างสูงสุด.

ไทยรัฐ
Thai Rath
Circulation: 500,000
Ad Rate: 1,000

Section: First Section/ข่าวเศรษฐกิจไทยรัฐ
วันที่: ศุกร์ 14 เมษายน 2566
ปีที่: 74 **ฉบับที่:** 23824 **หน้า:** 8(เต็มหน้า)
Col.Inch: 258.50 **Ad Value:** 258,500 **PRValue (x3):** 775,500 **คลิป:** ขาว-ดำ
หัวข้อข่าว: 5 กระบวนท่าสู้มิจฉาชีพออนไลน์ "ทำอย่างไรถ้าตกเป็นเหยื่อ"



5 กระบวนท่าสู้มิจฉาชีพออนไลน์ "ทำอย่างไรถ้าตกเป็นเหยื่อ"

ในช่วง 1-2 ปีที่ผ่านมาความเสียหายจากการถูกหลอกลวงออนไลน์เพิ่มขึ้นสู่หลายพันล้านบาท และกลายเป็น "ปัญหาระดับชาติ" ที่สร้างความอึดอัดไม่สบายและความกังวลใจให้คนไทยทั้งประเทศ

ทั้งนี้ จากสถิติของศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ ช่วงเดือนมีนาคม 2565-กุมภาพันธ์ 2566 พบว่าเป็นคดีหลอกให้ซื้อสินค้าออนไลน์มากที่สุดกว่า 50,000 รายการ อันดับ 2 หลอกลวงให้โอนเงิน 20,000 กว่ารายการ และอันดับ 3 หลอกให้กู้เงินกว่า 18,000 รายการ โดยเฉพาะการหลอกให้โอนเงิน และแก๊งคอลเซ็นเตอร์ มีความเสียหายกว่า 2,600 ล้านบาท ขออายัดบัญชีม้าไป 58,000 บัญชี กว่า 5,500 ล้านบาท

และถ้าจำกันได้ ยังมีคดี BIN attack ซึ่งแอบดูดเงินผ่านบัตรเดบิต และบัตรเครดิต ตามมาด้วยการหลอกลวงผ่าน mobile application โดยเฉพาะแอปพลิเคชันดูดเงิน ซึ่งธนาคารแห่งประเทศไทย (ธปท.) ระบุตัวเลขความเสียหายส่วนนี้กว่า 511 ล้านบาท และล่าสุดการแฮ็กข้อมูลส่วนตัวประชาชน และหน่วยงานราชการของแฮกเกอร์

ดังนั้น หากไม่ต้องการ "ตกเป็นเหยื่อ" หรือ "ต้องใช้วิธีถอนเงินไปฝังดิน" พวกเราก็ต้องเตรียมพร้อมรับมือกับกลโกงออนไลน์เหล่านี้ รวมทั้งมีความรู้ด้วยว่าหากโชคไม่ดีพลาดพลั้ง "เสียเงินเสียทอง" ไปจะแก้ไขอย่างไร

ในช่วงหยุดยาวสงกรานต์นี้ "ทีมเศรษฐกิจ" *ได้คัดบางส่วนของคอลัมน์ Financial Wisdom "5 กระบวนท่าสู้มิจฉาชีพ" และบทสัมภาษณ์ "ภิญโญ ตรีเพชราภรณ์" ผอ.ฝ่ายกำกับและตรวจสอบความเสี่ยงด้าน IT ธปท. จากวารสารพระสยาม BOT Magazine ฉบับที่ 1/2566 รวมทั้งการเตือนภัยของสมาคมธนาคารไทยมาให้อ่านกัน เพื่อป้องกันและรับมือคนร้าย และเสริมวัคซีนทางการเงิน*

●"ปิดจุดอ่อน" ตั้งสติ หยุดคิด ไม่หลงเชื่อ

ทั้งนี้ ตั้งแต่ต้นปีที่ผ่านมา หน่วยงานที่เกี่ยวข้องได้ร่วมกันผลักดัน พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อให้สามารถปราบปรามภัยออนไลน์ได้อย่างครบวงจร รวมทั้งเพิ่มโทษคนที่ใช้ชิมผี-บัญชีม้า ขณะที่ในภาคการเงิน ซึ่งเป็นเป้าหมายหลักของการหลอกลวง ธปท.ได้ออกชุดมาตรการจัดการภัยทุจริตทางการเงิน เพื่อเพิ่มความเข้มข้นการป้องกันภัยจากโลกไซเบอร์และรักษาความปลอดภัยแอปฯธนาคาร

อย่างไรก็ตาม จุดแรกที่ "มิจฉาชีพ" เข้าถึงก็คือ "ตัวเรา" ดังนั้น นอกเหนือจากการเรียนรู้ระบบป้องกันของทางการเราต้องเรียนรู้ที่จะป้องกันตัวเองก่อน

โดย ธปท.ได้แนะนำ "5 กระบวนท่าสู้มิจฉาชีพ" ที่สามารถนำไปปฏิบัติได้ง่ายๆ เริ่มจาก **กระบวนท่าที่ 1 คือ การตั้งสติ หยุดคิด ไม่หลงเชื่อใครง่ายๆ** *เพราะมิจฉาชีพจะพยายามหาจุดอ่อนของเรามาหลอกล่อให้หลงเชื่อและโอนเงินให้ เช่น หลอกให้รัก ให้เห็นใจ หลอกให้ลงทุนโดยให้ผลตอบแทนสูงๆ หรือขู่ว่ามีการทำผิดกฎหมาย*

ไทยรัฐ
Thai Rath
Circulation: 500,000
Ad Rate: 1,000
Section: First Section/ข่าวเศรษฐกิจไทยรัฐ
วันที่: ศุกร์ 14 เมษายน 2566
ปีที่: 74 ฉบับที่: 23824 หน้า: 8(เต็มหน้า)
Col.Inch: 258.50 Ad Value: 258,500 PRValue (x3): 775,500 คลิป: ขาว-ดำ
หัวข้อข่าว: 5 กระบวนท่าสู้มิจฉาชีพออนไลน์ "ทำอย่างไรถ้าตกเป็นเหยื่อ"

ทั้งนี้ ธปท.แนะนำว่า ไม่ว่าจะมาจากไหน เราต้องตั้งสติ หยุดคิดก่อนว่า "จริงหรือมั่ว" เราเคยขอสินเชื่อ หรือกระทำใดๆ ตามที่เขาหลอกหรือไม่ และยิ่งถ้ามาบอกให้เราโอนเงินไปให้ก่อน ปล่อยกู้ ส่งเงินส่งของมาให้ ให้โอนเงินมาเพื่อเคลียร์คดี หรือให้ผลตอบแทนก้อนเล็กๆมาล่อก่อนชวนลงทุนเพิ่ม ให้มั่นใจได้ว่า "เราเจอมิจฉาชีพเข้าให้แล้ว"

และอีกจุดหนึ่งที่ต้อง "ตั้งสติ หยุดคิด" คือ เวลาที่เราได้ SMS ข้อความทางไลน์ หรืออีเมลที่มีลิงก์แนบมาพร้อมข้อความ ชวนให้คลิก เช่น คลิกเพื่อรับเงินกู้หรือรางวัล คลิกเพื่อตรวจสอบข้อมูล ฯลฯ หาก "ไม่แน่ใจ" อย่าคลิก !!! เพราะอาจเป็นช่องทางให้มัลแวร์ หรือแอปฯแปลกปลอมจากมิจฉาชีพเข้ามาแฝงตัวเพื่อดูดข้อมูลสำคัญจากโทรศัพท์มือถือหรืออุปกรณ์ของเรา หรือร้ายแรงกว่านั้นคือ ดูดเงินออกจากบัญชีธนาคาร

● อย่ารีบโอน-คลิก "เช็กก่อนชัวร์กว่า"

จากกระบวนท่าที่ 1 เมื่อตั้งสติได้แล้ว หากยังกังวลว่าเป็นเรื่องจริงหรือหลอก เพราะมิจฉาชีพมักแอบอ้างชื่อหน่วยงานหรือคนที่เรารู้จักให้ดูน่าเชื่อถือ ให้ไปต่อที่กระบวนท่าที่ 2 คือเช็กก่อนชัวร์กว่า

ให้ถือคติว่า "เสียเวลาเช็กสักนิด ดีกว่าเสียเงินทั้งชีวิตที่หามา" ด้วยการโทร.กลับไปสอบถามหน่วยงานหรือบุคคลที่ SMS มาโดยตรงด้วยเบอร์โทร.จากเว็บไซต์หรือเบอร์ที่เราเคยติดต่อ หรือเช็กจากแหล่งข้อมูลที่ทางการรวบรวมไว้ เช่น หากต้องการตรวจสอบว่าเป็นผู้ให้บริการสินเชื่อ และผู้ให้บริการทางการเงินภายใต้การกำกับของ ธปท. จริงหรือไม่ ตรวจสอบได้ที่เว็บไซต์แบงก์ชาติ www.bot.or.th หัวข้อ เช็กแอปเงินกู้ และ BOT License Check

หรือจะตรวจสอบผู้ประกอบธุรกิจสินเชื่อพิโกไฟแนนซ์ ที่ได้รับอนุญาตจากคลัง ก็ทำได้จากเว็บไซต์กองนโยบายพัฒนาระบบการเงินภาคประชาชน สำนักงานเศรษฐกิจการคลัง https://1359.go.th/picodoc/ หรือหากอยากตรวจสอบผู้ให้บริการภายใต้การกำกับของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) เพื่อเช็กว่าถูกหลอกให้ลงทุนหรือไม่ ที่เว็บไซต์ www.sec.or.th หัวข้อ SEC Check First ส่วนการตรวจสอบผู้จดทะเบียนนิติบุคคล ไปที่เว็บไซต์กรมพัฒนาธุรกิจการค้า (www.dbd.go.th) หัวข้อ DBD DataWarehouse+

ขณะที่วิธีสังเกตเว็บไซต์หรือลิงก์ที่แฝงตัวมา หรือจำเป็นต้องกรอกข้อมูลส่วนตัวหรือรหัสผ่านเว็บไซต์ อย่างแรกควรพิมพ์ URL ของเว็บไซต์เอง หรือหากค้นหาด้วย search engine ควรตรวจสอบตัวสะกด URL ให้ถูกต้อง (ระวังอักษรที่คล้ายกัน เช่น O (อักษรโอ) กับ o (เลขศูนย์) หรืออีกกลุ่มหนึ่งคือ a (อักษรเอ) @ และ o (อักษรโอเล็ก) หรือตัว .com.org เพราะมิจฉาชีพมักใช้ชื่อเว็บไซต์ที่ใกล้เคียงของจริงมากๆ แต่ถ้าสังเกตให้ดีจะมีข้อแตกต่างเล็กน้อย รวมทั้งให้สังเกตสัญลักษณ์แม่กุญแจและตัว "s" ที่ https ซึ่งแสดงว่าเว็บไซต์นี้มีการเข้ารหัสเพื่อปกป้องข้อมูล

นอกจากนั้น สมาคมธนาคารไทยยังได้ชี้เป้าแอปพลิเคชันอันตรายว่ามักจะลงท้าย .apk ซึ่งเมื่อติดตั้งแล้วจอมือถือของเหยื่อจะค้าง มิจฉาชีพจะรีโมตมาควบคุมมือถือและโอนเงินออกทันที และที่พบมาก เช่น แอปฯปลอมของ DSI, สรรพากร, Lion-Air, ไทยประกันชีวิต, กระทรวงพาณิชย์ รวมทั้งแอปฯหาคู่ Bumble, Snapchat

● ใช้อุปกรณ์ปลอดภัยโอน-จ่ายเงิน

ต่อมาที่กระบวนท่าที่ 3 ส่วนนี้เป็นการรักษาความปลอดภัยของอุปกรณ์เพื่อไม่ให้ถูกเจาะระบบง่ายๆ โดยไม่ jailbreak หรือ root ระบบปฏิบัติการโทรศัพท์มือถือและอุปกรณ์ต่างๆ

ไม่ว่าการแก้ไขการตั้งค่า ติดตั้งโปรแกรมที่ปกติไม่สามารถติดตั้งได้ เพราะอาจถูกโจมตีด้วยไวรัส ถูกติดตั้งมัลแวร์ลงบนอุปกรณ์เพื่อส่งข้อมูลสำคัญให้มิจฉาชีพ นอกจากนี้ การใช้ Wi-Fi สาธารณะก็เป็นอีกช่องทางหนึ่งที่อาจถูกดักขโมยข้อมูล เช่น รหัสผ่าน จึงไม่ควรใช้ Wi-Fi สาธารณะทำธุรกรรมทางการเงินหรือกรอกข้อมูลสำคัญ

การติดตั้งแอปฯ ควรทำจากแหล่งที่น่าเชื่อถือ เช่น App store หรือ Google play store รวมถึงไม่ควร Add LINE หรือ Chat อื่นๆ คุยกับคนแปลกหน้า และถ้าเกิดพบว่าแอปฯของมิจฉาชีพมาอยู่ในมือถือหรืออุปกรณ์เราแล้วให้ทำ factory reset ล้างข้อมูลทั้งหมด แต่หากไม่สามารถทำได้ให้ปิดเครื่อง และรีบไปที่ศูนย์บริการมือถือเพื่อแก้ไข

ขณะที่สมาคมธนาคารไทยแนะผู้ที่หลงกลตกเป็นเหยื่อของมิจฉาชีพแล้ว ให้รีบดำเนินการปิดเครื่องทันทีด้วยวิธีกด Force-Reset คือ การกดปุ่ม Power และปุ่มลดเสียง พร้อมกันค้างไว้ 10-20 วินาที แต่ถ้าทำวิธีนี้ไม่สำเร็จ ให้ตัดการเชื่อมต่อของโทรศัพท์ด้วยการถอดซิมการ์ด ปิด Wi-Fi หลังจากนั้น ให้ติดต่อธนาคารแจ้งความทันที

● ไม่เชื่อ ไม่กรอก ไม่บอก ไม่โพสต์

มาถึงกระบวนท่าที่ 4 ซึ่งเป็นการเตือนใจตัวเองและป้องกันมิจฉาชีพเข้าถึง "ข้อมูลส่วนตัว" โดยให้ยึดหลัก 4 ไม่ "ไม่เชื่อ ไม่กรอก ไม่บอก ไม่โพสต์ข้อมูลสำคัญ"

ไม่เปิดเผยข้อมูลส่วนตัวในสื่อสาธารณะเกินความจำเป็น ไม่ให้ข้อมูลส่วนตัวกับคนแปลกหน้า และเวลารับโทรศัพท์ไม่แสดงตัวก่อน หากถูกถามให้ตรวจสอบคู่สนทนาให้แน่ชัดว่ารู้จักกันจริงหรือเป็นคนที่เรารู้จักจริงหรือไม่ รักษาความลับข้อมูลสำคัญ โดยเฉพาะอย่างยิ่ง เลขประจำตัวประชาชน วันเดือนปีเกิด เลขบัญชีธนาคาร เลขบัตรเครดิต OTP ซึ่งหากมิจฉาชีพได้ข้อมูลไปแล้ว อาจจะสวมรอยเป็นเราเข้าไปทำธุรกรรมเพื่อเอาเงินไป แถมยังปลอมตัวไปหลอกคนรู้จักของเรา ขอให้โอนเงินมาช่วยหรือให้ยืม กลายเป็นเหยื่ออีกทอดหนึ่ง

สุดท้าย **กระบวนท่าที่ 5 คือการติดตามข่าวสารและหาความรู้ใหม่ๆ** เพื่อให้เรารู้ทันกลโกง กลลวงใหม่ๆ นอกจากนั้น ยังจะช่วยให้ไม่ส่งข้อมูลที่ผิดพลาด หรือหลอกลวงไปยังคนอื่น รวมทั้งยังช่วยให้รู้กฎหมาย ขั้นตอนการป้องกันและแก้ไขปัญหาที่ถูกต้องเมื่อเราประสบภัยทางการเงิน และหากสงสัยให้ตรวจสอบข้อเท็จจริงจากแหล่งที่น่าเชื่อถือ เช่น ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.) โทร.1213 ศูนย์ปราบปรามอาชญากรรมเทคโนโลยีสารสนเทศ และศูนย์

ไทยรัฐ
Thai Rath
Circulation: 500,000
Ad Rate: 1,000
Section: First Section/ข่าวเศรษฐกิจไทยรัฐ
วันที่: ศุกร์ 14 เมษายน 2566
ปีที่: 74 ฉบับที่: 23824 หน้า: 8(เต็มหน้า)
Col.Inch: 258.50 Ad Value: 258,500 PRValue (x3): 775,500 คลิป: ขาว-ดำ
หัวข้อข่าว: 5 กระบวนท่าสู้มิจฉาชีพออนไลน์ "ทำอย่างไรถ้าตกเป็นเหยื่อ"

ต่อต้านข่าวปลอมประเทศไทย กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี โทร. 1441

● จะทำอย่างไรถ้าตกเป็นเหยื่อ!!

"ภิญโญ ตรีเพชรภรณ์" ผู้อำนวยการฝ่ายกำกับและตรวจสอบความเสี่ยงด้าน IT ธปท. กล่าวว่า สาเหตุที่ประชาชนตกเป็นเหยื่อได้ง่ายมาจากรัก โลภ กลัว หลง เช่น ถูกหลอกให้สนับสนุนเงินโดยอาศัยความรัก หลอกให้กลัวหรือตกใจ โดยอ้างเป็นหน่วยงานราชการ หรือใช้ความหลงหลอกให้เรารีบโอนเงินโดยไม่ทันได้ฉุกคิด

"หากยังไม่ตกเป็นเหยื่อ ทันทีที่ได้รับโทรศัพท์หรือ SMS ผิดปกติให้บล็อกเบอร์หรือ SMS ที่ติดต่อมาแล้วแจ้งผู้ให้บริการเครือข่ายโทรศัพท์ หรือติดต่อสายด่วน 1200 ของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ให้บล็อกเบอร์และ SMS ของคนร้ายเพื่อไม่ให้คนอื่นๆถูกหลอก"

"แต่เมื่อรู้ตัวว่าเป็นเหยื่อโอนเงินไปแล้ว สิ่งแรกคือ ต้องรีบติดต่อธนาคารเพื่อแจ้งเหตุ โดยแจ้งศูนย์ฮอตไลน์ภัยการเงิน 24 ชม. ของแต่ละธนาคารพาณิชย์เพื่อส่งข้อมูล และอายัดบัญชีโดยรวดเร็วที่สุด"

ซึ่งแต่ก่อนการโทร.ไปคอลเซ็นเตอร์ธนาคารมักใช้เวลานานกว่าเจ้าหน้าที่จะรับสาย แต่ปัจจุบัน ธปท.ได้ออกมาตรการให้ทุกธนาคารต้องมีสายด่วนหรือมีเบอร์เฉพาะให้ประชาชนแจ้งเรื่องภัยการเงินตลอด 24 ชั่วโมง และหลังจากนั้นให้แจ้งความออนไลน์กับตำรวจไซเบอร์ที่ www.thaipoliceonline.com หรือแจ้งความได้ที่สถานีตำรวจทั่วประเทศ

ที่สำคัญขอให้พยายามเก็บหลักฐานต่างๆ ไว้ให้มากที่สุดเพื่อให้กระบวนการติดตามคนร้ายง่ายขึ้น ขณะที่ พ.ร.บ.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่เพิ่งมีผลบังคับใช้ จะช่วยให้ธนาคารดูแลช่วยเหลือประชาชนที่ตกเป็นเหยื่อได้รวดเร็วขึ้น ระงับความเสียหายได้อย่างทันท่วงที สามารถบล็อกบัญชีต้องสงสัยได้ 72 ชม. ขณะรอแจ้งความ ขณะที่คนที่ขายซิมม้าหรือประกาศขายซิมม้า รวมทั้งบัญชีม้าจะมีบทลงโทษตามกฎหมาย

● อัปเดตมาตรการสู้ภัยการเงิน

นายภิญโญกล่าวต่อว่า "การออกมาตรการสู้ภัยทุจริตการเงิน ธปท.เน้นดูแลต้นจนจบ ตั้งแต่ป้องกัน ตรวจจับ ตอบสนองและรับมือ และในเบื้องต้นโมบาย แบงกิ้ง mobile banking ของทุกธนาคารมีความปลอดภัยตามมาตรฐานสากล ซึ่ง ธปท.ได้เข้าไปดูแลให้มั่นใจว่าพร้อมรับมือภัยต่างๆ แต่เนื่องจากคนร้ายปฏิบัติการในที่มืดปรับรูปแบบตลอดเวลา แต่ธนาคารอยู่ในที่สว่างทำให้อาจมีช่องโหว่ในบางช่วง จึงอยากให้คนไทยรู้จักป้องกันตัวเองเป็นอันดับแรก"

โดยในส่วนของธนาคารได้พัฒนาแอปพลิเคชันป้องกันไม่ให้แอปฯ ดูดเงินทำงานได้ ซึ่งล่าสุดระบบแอปพลิเคชันของธนาคารสามารถตรวจสอบได้ว่ามีการ "รีโมตหรือเปิดสิทธิ์" การใช้งานผิดปกติบนโทรศัพท์มือถือของลูกค้าหรือไม่ หากตรวจพบจะหยุดให้บริการ mobile banking ทันที ซึ่งวิธีการนี้จะช่วยลดการโจมตีของคนร้ายไปได้

นอกจากนั้น ธนาคารจะขึ้น pop-up message เตือนผ่านแอปฯในมือถือขณะที่กำลังโอนเงินทุกครั้งเพื่อให้เกิดความระมัดระวัง ปรับปรุงระบบรักษาความปลอดภัย mobile banking ให้เท่าทันภัยการเงินใหม่ๆ และในช่วงต่อไปจะมีเพิ่มมาตรการยืนยันตัวตนด้วย biometrics หรือการสแกนใบหน้า ในกรณีที่มีการโอนเงินตามจำนวนที่กำหนด

ขณะที่การป้องกันกรณีการแอบใช้หรือโอนเงินจากบัตรเดบิต บัตรเครดิต ขอให้ลูกค้าหมั่นดู SMS แจ้งเตือนจากธนาคาร เมื่อพบความผิดปกติให้รีบติดต่อธนาคารเพื่อระงับธุรกรรมทันที ส่วนการรับลิงก์ผ่าน SMS นั้น มาตรการล่าสุดธนาคารจะไม่แนบลิงก์ใน SMS หรือส่งอีเมลแนบลิงก์ให้ลูกค้าเด็ดขาด และท้ายสุดกรณีแก๊งคอลเซนเตอร์ ซึ่งส่วนใหญ่ติดต่อมาจากต่างประเทศ จึงไม่ควรรับสายที่มีเครื่องหมายบวก เช่น +697 +698

● "ถูกหลอก" มีโอกาสได้เงินคืนหรือไม่

ท้ายที่สุด อีกหนึ่งคำถามที่คนส่วนใหญ่อยากรู้ คือ โอกาสที่จะได้ตัวคนร้ายและได้เงินคืน สำหรับการดำเนินคดีและการช่วยเหลือเยียวยา นายภิญโญกล่าวว่า *นอกจากธนาคารจะต้องมีหน้าที่ช่วยติดตามเงินคืน ประสานงาน และช่วยหาตัวคนร้ายแล้ว ธนาคารยังมีหน้าที่ต้องรับผิดชอบลูกค้าของธนาคารในกรณีที่สืบสวนข้อเท็จจริงแล้วพบว่าความเสียหายเกิดจากข้อบกพร่องของธนาคารจะต้องคืนเงินที่เสียหายให้กับลูกค้า*

นอกจากนั้น จากเดิมที่การบล็อกเส้นทางเงินทำได้ล่าช้าเพราะต้องรอใบแจ้งความจากตำรวจ ตามกฎหมายใหม่ธนาคารจะสามารถเพิ่มการตรวจจับธุรกรรมที่ผิดปกติ และมีสิทธิระงับธุรกรรมได้ชั่วคราว เมื่อตรวจพบว่าบัญชีเงินฝากถูกใช้ทำธุรกรรมต้องสงสัย หรือได้รับแจ้งจากผู้เสียหายและยังระงับธุรกรรมที่ดำเนินการเป็นทอดๆ จนถึงทอดสุดท้ายได้ ซึ่งจะช่วยลดโอกาสสูญเสียเงินได้มากขึ้น.