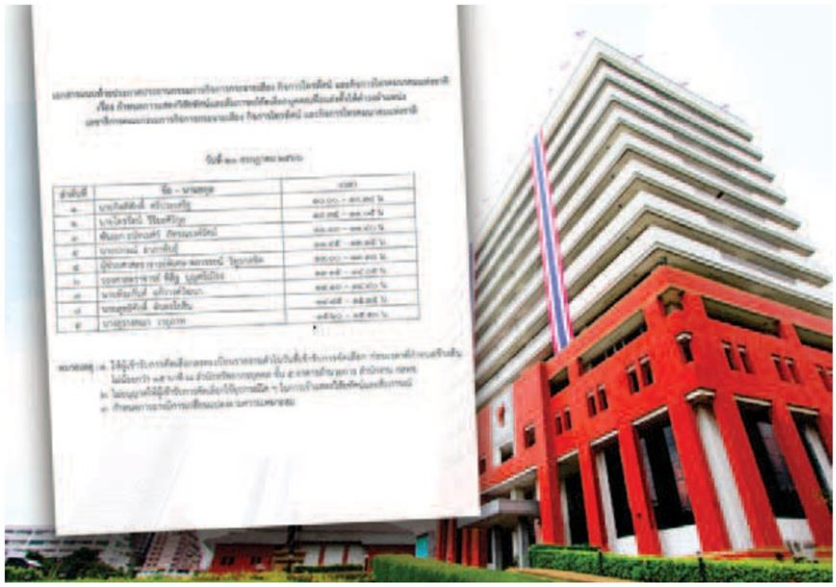
กรุงเทพธุรกิจ
Krungthep Turakij
Circulation: 150,000
Ad Rate: 1,250

Section: First Section/new norm is now
วันที่: พฤหัสบดี 20 กรกฎาคม 2566
ปีที่: 36 **ฉบับที่:** 12427 **หน้า:** 1(บนซ้าย), 3
Col.Inch: 69.65 **Ad Value:** 87,062.50 **PRValue (x3):** 261,187.50 **คลิป:** สีสี
หัวข้อข่าว: เลือก'เลขาธิการ กสทช.'วันนี้

เลือก'เลขาธิการ กสทช.'วันนี้
คาด'ไตรรัตน์'ตัวเต็งมีลุ้น
> 3

เลือก'เลขาธิการ กสทช.'วันนี้ คาด'ไตรรัตน์'ตัวเต็งมีลุ้น

ปานฉัตร สินสุข
กรุงเทพธุรกิจ



การสรรหาเลขาธิการ กสทช.คนใหม่อยู่ในช่วงโค้งสุดท้าย หลังเชิญผู้สมัคร 9 ราย เข้าแสดงวิสัยทัศน์วันนี้ (20 ก.ค.) คาดมีการเคาะผลทันที หลังจบการแสดงวิสัยทัศน์ งานนี้ตัวเต็งยังคงเป็นรักษาการเลขาธิการ กสทช. คนปัจจุบัน **"ไตรรัตน์ วิริยะศิริกุล"** ทั้งที่ถูกหลายฝ่ายกังขาในคุณสมบัติ อีกทั้งถูกตั้งคณะกรรมการสอบวินัย กรณีอนุมัติงบสนับสนุนการจัดซื้อลิขสิทธิ์บอลโลก 2022 ให้แก่การกีฬาแห่งประเทศไทย (กกท.) ในช่วงที่ผ่านมา

แหล่งข่าวจากสำนักงานกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ให้ข้อมูลว่า **ในวันนี้ 20 ก.ค. 2566 คณะทำงานสรรหาเลขาธิการ กสทช.ได้เชิญผู้สมัครที่ผ่านคุณสมบัติเข้ารับการสรรหาเป็นเลขาธิการ กสทช. จำนวน 9 ราย เข้าแสดงวิสัยทัศน์ เพื่อเข้าเป็นว่าที่เลขาธิการ กสทช.คนใหม่ ประกอบด้วย**

1.นายไตรรัตน์ วิริยะศิริกุล รองเลขาฯ และรักษาการเลขาธิการ กสทช.ในปัจจุบัน 2. พ.อ.ดร.ธนัทเทศร์ ภัทรณรงค์รัศม์ กรรมการติดตามและประเมินผลการปฏิบัติงาน กสทช. 3. รศ.พิสิฐ บุญศรีเมือง อาจารย์สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง 4.นายปกรณ์ อาภาพันธ์ ผู้อำนวยการสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (GISTDA) 5.นายกิตติศักดิ์ ศรีประเสริฐ อดีตกรรมการผู้จัดการใหญ่บริษัท กสท.โทรคมนาคมจำกัด (มหาชน)

6.ผศ.(พิเศษ) ดร.นพ.พลวรรธน์ วิทูรกลชิต อดีตผู้ตรวจราชการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 7.นางสุรางคณา วายุภาพ อดีตผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) 8. ดร.พีระกันต์ แก้ววัฒนา อดีตกรรมการผู้อำนวยการใหญ่ บริษัทรถไฟฟ้า รฟท.จำกัด 9. นายสุทธิศักดิ์ ตันตะโยธิน รองเลขาธิการ กสทช.สายงานโทรคมนาคม

ทั้งนี้ การแสดงวิสัยทัศน์และสัมภาษณ์ให้ผู้เข้ารับการคัดเลือก นำเสนอวิสัยทัศน์ต่อคณะกรรมการ กสทช.ใช้เวลาประมาณ 10 นาที จากนั้นคณะกรรมการ กสทช. จะดำเนินการสัมภาษณ์ผู้เข้ารับการคัดเลือก โดยใช้เวลารวมแต่ละคนประมาณ 30 นาที ขณะที่การประกาศผลการคัดเลือก ประธาน กสทช.จะประกาศรายชื่อบุคคลผู้ที่ได้รับความเห็นชอบจากคณะกรรมการ กสทช. ให้ดำรงตำแหน่งเลขาธิการ กสทช.ณ สำนักงาน กสทช. และทางเว็บไซต์ กสทช.ในทันที

ไตรรัตน์ ตัวเต็งท่ามกลางข้อกังขา

มีรายงานว่า ตัวเต็งบุคคลที่ได้รับการคาดหมายว่าจะเป็นเลขาธิการ กสทช.คนใหม่ยังคงเป็น "นายไตรรัตน์" เช่นเดิม แม้จะเผชิญกับแรงต่อต้านจากบอร์ด กสทช.ที่ก่อนหน้านี้มีมติให้ยุติการปฏิบัติหน้าที่รักษาการเลขาธิการ กสทช.และตั้งคณะกรรมการสอบวินัย กรณี รักษาการ เลขาธิการ กสทช.อนุมัติงบสนับสนุนการจัดซื้อลิขสิทธิ์บอลโลก 2022 ให้แก่การกีฬาแห่งประเทศไทย (กกท.)

แต่ท้ายที่สุดกลับไม่มีการปฏิบัติตามประกาศหลักเกณฑ์การเผยแพร่รายการโทรทัศน์เป็นการทั่วไปที่ต้องดูได้ในทุก

กรุงเทพธุรกิจ
Krungthep Turakij
Circulation: 150,000
Ad Rate: 1,250

Section: First Section/new norm is now
วันที่: พฤหัสบดี 20 กรกฎาคม 2566
ปีที่: 36 **ฉบับที่:** 12427 **หน้า:** 1(บนซ้าย), 3
Col.Inch: 69.65 **Ad Value:** 87,062.50 **PRValue (x3):** 261,187.50 **คลิป:** สีสี
หัวข้อข่าว: เลือก'เลขาธิการ กสทช.'วันนี้

แพลตฟอร์ม ซึ่งขัดประกาศ "มัสต์แคร์รี่" ของกสทช.เอง แต่นายไตรรัตน์ ได้ยกเลิกคำสั่งสอบวินัยตนเองไป จนกลายเป็นข้อถกเถียงในบอร์ด กสทช.ว่า ทำได้หรือไม่ เพราะเป็นมติบอร์ด กสทช.เอง และเรื่องดังกล่าว แม้จะมีการนำเข้าหารือในที่ประชุมบอร์ด กสทช.แต่ก็ยังไม่มีข้อยุติ

นอกจากนี้ นายไตรรัตน์ ยังถูกสภาองค์กรเพื่อผู้บริโภคออกโรงคัดค้านต่อการที่รักษาการ เลขาธิการ กสทช. ใช้อำนาจมิชอบสั่งปลด นพ.ประวิทย์ ลี่สถาพรวงศา ที่ปรึกษาประธานกสทช. โดยทั้งสองกรณีก็ดูจะไม่มีผลต่อการตัดสินใจใดๆ ของประธานกสทช.ที่อิงตามประกาศการรับสมัครว่าเป็นอำนาจของตนเองแต่ผู้เดียวตามมาตรา 60 และ 61 ที่ระบุว่าประธาน มีอำนาจแต่งตั้งและปลดเลขาธิการ กสทช.ได้ และตนเองได้ตัดสินใจใช้อำนาจประธาน กสทช.ในการสรรหาและแต่งตั้งเลขาธิการ กสทช.เอง เพราะเป็นตำแหน่งที่ต้องทำงานใกล้ชิดกับประธาน กสทช.

นอกจากนี้ ยังปรากฏว่า นายไตรรัตน์ และ ประธานกสทช.ควงกันออกงานที่สวิตเซอร์แลนด์ ในการประชุมสภาบริหารของสหภาพโทรคมนาคมระหว่างประเทศ (ไอทียู) ประจำปี 2023 (2023 Session of the Council) ในระหว่างวันที่ 8-23 ก.ค. 2566 ด้วย โดยประธานกสทช.เดินทางระหว่างวันที่ 8-14 ก.ค. 2566 ขณะที่นายไตรรัตน์เดินทางระหว่างวันที่ 8-16 ก.ค.2566

ฉะนั้น วันนี้ สิ่งที่ต้องจับตาการคัดเลือกเลขาฯกสทช.คนใหม่ ว่าประธานจะเลือกคนสนิทอย่าง "ไตรรัตน์" เข้าป้ายตามข่าวสะพัดที่ว่ามาหรือไม่

ผู้จัดการรายวัน 360°
Poo Jadkarn Daily 360 Degree
Circulation: 850,000
Ad Rate: 1,500

Section: iBusiness/-
วันที่: พฤหัสบดี 20 กรกฎาคม 2566
ปีที่: 15 ฉบับที่: 4000 หน้า: 2(กลาง)
Col.Inch: 225.64 Ad Value: 338,460 PRValue (x3): 1,015,380 คลิป: สีสี
หัวข้อข่าว: ธปท.เข้มมาตรการภัยการเงินปิดช่องโหว่รูปแบบใหม่

ธปท.เข้มมาตรการภัยการเงินปิดช่องโหว่รูปแบบใหม่ รับมือให้ปลอดภัยจากกลโกงทางการเงินและโจรไซเบอร์

ตลาดเงิน-ตลาดทุน

"อะไรที่มีคุณประโยชน์ก็อาจมีอันตรายแฝงอยู่ อย่างเทคโนโลยีทางการเงินที่ทำให้การใช้ชีวิตของเราสะดวกสบายก็มาพร้อมกับมิจฉาชีพออนไลน์ที่มากขึ้นทุกวัน แล้วโจรพวกนี้ก็ขยันสรรหาสารพัดวิธีที่จะมาขโมยเงิน หลอกลวง และต้มตุ๋นจนหลายๆ คนตกเป็นเหยื่อ จากการขโมยเงินออนไลน์ผ่านบัตรเดบิต/เครดิต (BIN attack) มาสู่การใช้คอลเซ็นเตอร์และการส่ง SMS หรือการเพิ่มเพื่อนทาง Line ลวงให้กดลิงก์ไปยังเว็บไซต์ และติดตั้งแอปพลิเคชันปลอมเพื่อดูดข้อมูลส่วนตัว ภัยการเงินเหล่านี้มักปรับเปลี่ยนให้ทันสมัย และใช้จุดอ่อนของความเป็นมนุษย์เข้ามาหลอกล่อ ทำให้เราโดนฉกเงินไปโดยไม่รู้ตัว"

ภัยทางการเงินในยุคดิจิทัลที่พบบ่อยๆ มีอะไรบ้าง รับมือ Phishing ของปลอมก๊อบเกรดเอ

Phishing คือ การแอบอ้างว่าตนเองเป็นผู้ให้บริการ เพื่อหลอกให้เรากรอกข้อมูลส่วนตัว เช่น ข้อมูลบัตรเครดิต เลขที่บัญชีธนาคาร ชื่อผู้ใช้งาน หรือรหัสผ่าน เพื่อให้มิจฉาชีพสามารถนำข้อมูลเหล่านั้นไปสวมรอยทำธุรกรรมต่อไป

โดยทั่วไป มิจฉาชีพจะวางเหยื่อล่อโดยการส่ง SMS หรืออีเมลปลอมที่ออกแบบให้ดูคล้ายกับอีเมลของผู้ให้บริการที่เราใช้บริการอยู่ โดยมิจฉาชีพมักใช้ความตกใจของเราเป็นเครื่องมือ เช่น อ้างว่าเราถูกอายัดบัญชี หรือข้อมูลถูกแฮก และขอให้เราเข้าไปกรอกข้อมูลที่เว็บไซต์ที่มิจฉาชีพสร้างขึ้นให้ดูคล้ายกับเว็บไซต์จริงของผู้ให้บริการ เมื่อเราหลงเชื่อกรอกข้อมูลไป ข้อมูลดังกล่าวจะถูกส่งต่อไปยังมิจฉาชีพทันที

การรับมือภัย Phishing ง่ายมาก แค่เพิ่มความระมัดระวังให้มากขึ้น เช่น เมื่อได้รับอีเมลหรือ SMS ที่อ้างว่าเป็นผู้ให้บริการ ควรดูว่ามาจากผู้ให้บริการจริงหรือไม่ และไม่คลิกลิงก์ที่แนบมากับอีเมลหรือ SMS ที่เราไม่รู้จัก เก็บข้อมูลส่วนตัวไว้เป็นความลับ หรือหากไม่แน่ใจให้โทรศัพท์สอบถามผู้ให้บริการโดยตรง

BIN attack เป็นอีกหนึ่งวิธีที่มิจฉาชีพใช้หลอกลวง BIN attack คืออะไร

BIN attack ก็คือการที่มิจฉาชีพใช้โปรแกรมสุ่มเลขบัตรไปเรื่อยๆ แล้วลองกดซื้อของดู ถ้าไม่ได้ก็ลองเลขใหม่ ถ้าได้ก็เก็บข้อมูลบัตรนั้นไว้ เพราะสามารถเอาไปใช้ได้อีกหลายรอบจนกว่าเจ้าของหรือสถาบันการเงินจะรู้ตัว

ผู้จัดการรายวัน 360°
Poo Jadkarn Daily 360 Degree
Circulation: 850,000
Ad Rate: 1,500

Section: iBusiness/-
วันที่: พฤหัสบดี 20 กรกฎาคม 2566
ปีที่: 15 ฉบับที่: 4000 หน้า: 2(กลาง)
Col.Inch: 225.64 Ad Value: 338,460 PRValue (x3): 1,015,380 คลิป: สีสี
หัวข้อข่าว: ธปท.เข้มมาตรการภัยการเงินปิดช่องโหว่รูปแบบใหม่

การทำ BIN attack นี้ ไม่ซับซ้อนเหมือนที่หลายคนเข้าใจ (ว่าต้องทราบทั้งเลขบัตร ชื่อผู้ถือบัตร วันหมดอายุ รหัสหลังบัตร และมี OTP) เพราะข้อมูลที่จำเป็นจริงๆ คือเลขบัตรและวันหมดอายุเท่านั้น ข้อมูลเพื่อตรวจสอบอื่นๆ เป็นส่วนที่ร้านค้าสามารถเลือกได้เองว่าจะใช้หรือไม่ (เพราะร้านค้าเป็นคนรับความเสี่ยงในกรณีที่เกิดการสวมรอยใช้บัตร) ร้านค้าส่วนหนึ่งไม่ได้ให้ลูกค้ากรอกข้อมูลอื่นๆ โดยเฉพาะกรณีที่ธุรกรรมมีมูลค่าไม่มากเพื่อความสะดวกของลูกค้า เมื่อมิจฉาชีพพบร้านค้าออนไลน์ที่ระบบการตรวจสอบไม่เข้มงวดมากนัก ก็สามารถลองสุ่มเลขบัตรเพื่อใช้งานได้ หากสำเร็จก็จะทำต่อไปเรื่อยๆ

การป้องกัน BIN attack

หลายธนาคารมีการป้องกัน BIN attack คือเมื่อพบรายการชำระเงินที่ถูกปฏิเสธหลายครั้งติดต่อกันจากร้านค้า (เพราะมิจฉาชีพสุ่มเลขแล้วผิด) ระบบเตือนจะทำงาน และอาจจะหยุดการให้บริการร้านค้านั้นชั่วคราวเพื่อตรวจสอบเพิ่มเติม โดยสถาบันการเงินหรือผู้ให้บริการแต่ละรายสามารถปรับการตั้งค่าได้ เช่น ตั้งค่าจำนวนการกรอกข้อมูลของบัตรผิด หากเกินกี่ครั้งต่อนาทีจะหยุดให้บริการร้านค้านั้นชั่วคราว หรือถ้ามีการใช้บัตรซ้ำๆ ถี่ๆ เกินกี่ครั้ง จะระงับการใช้บัตรนั้นไปก่อน

สำหรับประชาชนก็สามารถดูแลความปลอดภัยให้ตัวเองเพิ่มขึ้นได้อีก โดยหมั่นตรวจสอบความเคลื่อนไหวของรายการในบัตร เพื่อดูว่ามีรายการผิดปกติบ้างหรือไม่ และอาจกำหนดวงเงินของบัตรให้ไม่สูงมาก หากต้องใช้จ่ายรายการใหญ่ๆ ก็สามารถโทร.ไปหาธนาคารเจ้าของบัตรเพื่อขอเพิ่มวงเงินชั่วคราวได้ รวมถึงอาจกำหนดให้บัตรบางใบใช้จ่ายออนไลน์ไม่ได้ นอกจากนี้ ไม่ควรผูกบัญชีบัตรกับร้านค้าออนไลน์ เพื่อลดความเสี่ยงที่ข้อมูลบัตรจะรั่วไหลผ่านร้านค้าเหล่านั้น

แอปฯ เงินกู้ปลอม

การกู้เงินในยุคปัจจุบันทำได้ง่ายและรวดเร็วผ่านสมาร์ทโฟน โดยไม่ต้องออกจากบ้านให้ยุ่งยาก แต่สิ่งที่ยากสำหรับผู้กู้คือ จะรู้ได้อย่างไรว่าใครคือผู้ให้กู้ที่ไม่คิดดอกเบี้ยหรือทวงถามหนี้โหด หรือไม่ใช่มิจฉาชีพที่จะมาหลอกเอาเงินเราไป ยิ่งหากได้รับ SMS หรือมีคนโทรศัพท์ หรือแอดไลน์มาแล้วอ้างว่าเป็นเจ้าหน้าที่ธนาคาร หรือหน่วยงานภาครัฐ หรือบริษัทที่จะให้เงินกู้หรือให้เงินช่วยเหลือ อย่ารีบกดลิงก์หรือกรอกข้อมูลเด็ดขาด ควรเช็กให้แน่ใจก่อน จะได้ไม่ถูกเอาเปรียบหรือหลอกลวง สิ่งที่ทำให้เรารู้ทันและไม่หลงเชื่อมีง่ายๆ 4 ข้อ ดังนี้

1. **แยกแยะผู้ให้เงินกู้** แอปฯ เงินกู้ปลอมจะใช้วิธีการต่างๆ เช่น โฆษณาบนเว็บไซต์ โซเชียลมีเดีย ส่ง SMS หรือแม้แต่โทร.หาโดยตรง หากผู้ที่ได้รับการติดต่อสนใจ มิจฉาชีพก็จะส่ง SMS มาให้คลิกลิงก์เพื่อดาวน์โหลดแอปฯ หรือให้แอดไลน์คุยกัน จากนั้นจะสอบถามข้อมูลส่วนตัว ให้ทำสัญญาเงินกู้ และขอเอกสารต่างๆ

ผู้จัดการรายวัน 360°
Poo Jadkarn Daily 360 Degree
Circulation: 850,000
Ad Rate: 1,500
Section: iBusiness/-
วันที่: พฤหัสบดี 20 กรกฎาคม 2566
ปีที่: 15 ฉบับที่: 4000 หน้า: 2(กลาง)
Col.Inch: 225.64 Ad Value: 338,460 PRValue (x3): 1,015,380 คลิป: สีสี
หัวข้อข่าว: ธปท.เข้มมาตรการภัยการเงินปิดช่องโหว่รูปแบบใหม่

คล้ายกับการขอกู้ที่ธนาคาร ทำให้เหยื่อเริ่มเชื่อใจ จากนั้นจะโน้มน้าวให้โอนเงินเป็นค่าค้ำประกัน โดยบอกว่าจะคืนให้พร้อมกับเงินกู้ หากหลงกลก็จะหลอกล่อให้โอนเพิ่มอีกเรื่อยๆ เช่น อ้างว่าโอนเงินไม่ได้เพราะเหยื่อกรอกเลขที่บัญชีผิด มีค่าใช้จ่ายในการแก้ไขเอกสารเพื่อปลดล็อก หรือต้องจ่ายค่าลัดคิวจึงจะได้เงินเร็วขึ้น

2. ไม่แน่ใจ อย่าเพิ่งคลิก ควรตรวจสอบรายชื่อแอปฯ และชื่อผู้ให้บริการก่อนตัดสินใจ โดยสามารถหาข้อมูลได้จากเว็บไซต์ ธปท. ในหัวข้อ "เช็กแอปเงินกู้" ที่รวบรวมรายชื่อผู้ให้บริการที่ได้รับอนุญาตในส่วนที่ ธปท. กำกับดูแล และมีลิงก์ไปยังเว็บไซต์กระทรวงการคลัง ซึ่งรวบรวมรายชื่อผู้ให้บริการสินเชื่อพิโกไฟแนนซ์ไว้ในที่เดียว หรือควรสอบถามหรือหาข้อมูลด้วยตัวเองจากแหล่งข้อมูลที่น่าเชื่อถือว่าเป็นแอปฯ ของผู้ให้บริการจริงหรือไม่

3. เลือกแหล่งดาวน์โหลดแอปฯ ดาวน์โหลดจากแหล่งที่ปลอดภัย เชื่อถือได้

4. อย่าลืมอ่านเงื่อนไขก่อนกู้ ไม่ต้องรีบกู้จนลืมดูรายละเอียดที่จำเป็น เช่น อัตราดอกเบี้ย ระยะเวลา และจำนวนเงินที่ต้องจ่ายคืน ที่สำคัญ ต้องคำนึงถึงความสามารถในการผ่อนชำระของเราโดยควรกู้เท่าที่จำเป็น

ธปท.แนะรับมือให้ปลอดภัย จากกลโกงทางการเงิน และโจรไซเบอร์

จากการขโมยเงินออนไลน์ผ่านบัตรเดบิต/เครดิต (BIN attack) มาสู่การใช้คอลเซ็นเตอร์และการส่ง SMS หรือการเพิ่มเพื่อนทาง Line ลวงให้กดลิงก์ไปยังเว็บไซต์และติดตั้งแอปพลิเคชันปลอมเพื่อดูดข้อมูลส่วนตัว ภัยการเงินเหล่านี้มักปรับเปลี่ยนให้ทันสมัย และใช้จุดอ่อนของความเป็นมนุษย์เข้ามาหลอกล่อ ทำให้เราโดนฉกเงินไปโดยไม่รู้ตัวยิ่งเทคโนโลยีมีการพัฒนาก็ยิ่งเสี่ยงต่อการตกเป็นเหยื่อมิจฉาชีพมากขึ้น โดยเฉพาะช่วงบูมของธนาคารดิจิทัล ผู้คนมักทำธุรกรรมผ่าน mobile application ทำให้มิจฉาชีพนำมาใช้เป็นช่องทางหลอกลวงประชาชน

"สาเหตุที่ประชาชนตกเป็นเหยื่อได้ง่ายก็มาจาก รัก โลภ กลัว หลง เช่น ถูกหลอกล่อให้เราสนับสนุนเงิน โดยอาศัยความรัก (romance scam) หลอกให้กลัวหรือตกใจโดยอ้างว่าเป็นหน่วยงานราชการ หรือใช้ความหลงหลอกให้เรารีบโอนเงินโดยไม่ทันได้ฉุกคิด พฤติกรรมตามธรรมชาติของมนุษย์ที่มิจฉาชีพนำมาใช้จนทำให้ต้องสูญเสียเงินจากกลโกงต่างๆ"

แจ้งเหตุทันทีที่ตกเป็นเหยื่อ

เมื่อรู้ตัวว่าตกเป็นเหยื่อโอนเงินให้มิจฉาชีพไปแล้ว สิ่งแรกที่ต้องทำคือรีบติดต่อธนาคารเพื่อแจ้งเหตุ ปัจจุบัน ธปท. ได้ออกมาตรการให้ทุกธนาคารต้องมีสายด่วนหรือมีเบอร์เฉพาะให้ประชาชนเข้ามาแจ้งเรื่องภัยการเงิน และต้องพร้อมให้บริการตลอด 24 ชั่วโมง จากนั้นติดต่อไปยังสถานีตำรวจของแต่ละท้องที่ เพื่อให้ความช่วยเหลือในการระงับธุรกรรมหรืออายัดเงินและดำเนินคดี แต่ถ้าจะให้เร็วขึ้นก็สามารถแจ้งความออนไลน์ได้ที่ www.thaipoliceonline.com โดยเก็บหลักฐานต่างๆ ไว้เพื่อให้กระบวนการติดตามคนร้ายง่ายขึ้น หากยังขาดความราบรื่นแนะนำให้ติดต่อมายังศูนย์คุ้มครองผู้ใช้บริการทางการเงิน สายด่วน 1213 ของ ธปท. ที่จะคอยให้คำแนะนำเกี่ยวกับแนวปฏิบัติต่างๆ และรับเรื่องร้องเรียน

ป้องกันตัวจากกลลวงหลอก

จากสถิติของศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ ทางเว็บไซต์ www.thaipoliceonline.com ในช่วงเดือนมีนาคม 2565-กุมภาพันธ์ 2566 พบว่า 22.77% ของเรื่องที่รับแจ้งเป็นคดีการหลอกลวงให้โอนเงินเพื่อหารายได้จากการทำกิจกรรมและหลอกลวงผ่านแก๊งคอลเซ็นเตอร์ซึ่งอยู่อันดับสองรองจากการหลอกลวงซื้อขายสินค้าออนไลน์

จากข้อมูลของธนาคารแห่งประเทศไทย กรณี BIN attack พุ่งสูงในช่วงปี 2564 เมื่อถึงปี 2565 สถิติความเสียหายในเรื่องนี้ก็ลดลงอย่างมาก โดยความเสียหายจากช่องทางให้บริการผ่านบัตรเดบิตลดลง 47.62% และบัตรเครดิตลดลง 66.58% แต่กลับพบความเสียหายจาก mobile application โดยเฉพาะแอปฯ ดูดเงินเพิ่มขึ้นแทน โดยมีตัวเลขความเสียหายรวมกว่า 511 ล้านบาท เป็นการสะท้อนว่าคนร้ายได้พัฒนาการโจมตีโดยปรับรูปแบบการหลอกลวงอย่างต่อเนื่อง ขณะที่ฝั่งสถาบันการเงินเองก็พยายามพัฒนาแอปพลิเคชันเพื่อป้องกันไม่ให้แอปฯ ดูดเงินทำงานได้ ซึ่งล่าสุดระบบแอปพลิเคชันของธนาคารสามารถตรวจสอบได้ว่ามีการรีโมตหรือเปิดสิทธิ์การใช้งานผิดปกติบนโทรศัพท์มือถือของลูกค้าหรือไม่ หากตรวจพบก็จะหยุดให้บริการ mobile banking ทันที ซึ่งวิธีการนี้จะช่วยลดการโจมตีของคนร้ายไปได้

ทั้งนี้วิธีป้องกันตัวเองอย่างง่ายๆ เช่น กรณีบัตรเดบิต/เครดิต ให้หมั่นดู SMS แจ้งเตือนจากธนาคาร เมื่อพบความผิดปกติก็รีบติดต่อธนาคารเพื่อระงับธุรกรรมนั้น กรณีได้รับลิงก์ผ่าน SMS ให้พิจารณาถึงความน่าเชื่อถือทั้งตัวผู้ส่งและเนื้อหาที่ส่งมา มาตรการล่าสุดของ ธปท. ที่ธนาคารได้ดำเนินการแล้วคือไม่แนบลิงก์ใน SMS สำหรับกรณีแก๊งคอลเซ็นเตอร์ส่วนใหญ่ติดต่อมาจากต่างประเทศ จึงไม่ควรรับสายที่มีเครื่องหมายบวกขึ้นมา เช่น +697 +698 ก็จะช่วยสกัดกั้นไม่ให้เกิดการพูดคุยที่นำไปสู่การหลอกลวงได้ และในกรณีแอปฯ เงินกู้ ให้สังเกตดูว่าเป็นแอปพลิเคชันของบริษัทที่ได้รับอนุญาตประกอบธุรกิจอย่างถูกต้องหรือไม่ **โดยสามารถตรวจสอบรายชื่อได้ที่เว็บไซต์ของ ธปท.(https://www.bot.or.th/Thai/ConsumerInfo/Fraud/Pages/BOTLicensedLoan.aspx) และสุดท้าย กรณีแอปฯ ดูดเงิน ให้สังเกตถึงแหล่งที่มาในการกดลิงก์เพื่อดาวน์โหลดแอปพลิเคชัน หากอยู่นอก official store ซึ่งเป็นแหล่งที่ได้รับการควบคุมและรับรองความปลอดภัยจากผู้พัฒนาระบบปฏิบัติการ เช่น Play Store หรือ App Store ก็ควรระมัดระวังตัวไว้**

ยกระดับเกณฑ์การกำกับดูแล ธนาคารพาณิชย์ให้สามารถรับมือภัยการเงิน

สิริธิดา พนมวัน ณ อยุธยา ผู้ช่วยผู้ว่าการ สายกำกับระบบการชำระเงินและคุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย(ธปท.) กล่าวว่า ธปท.ร่วมกับหน่วยงานที่เกี่ยวข้อง ปปง. กสทช. TB-CERT สมาคมธนาคารไทย พยายามผลักดันมาตรการ และแนวปฏิบัติต่างๆ อย่างต่อเนื่องเพื่อยกระดับการป้องกัน ตรวจจับ และตอบสนองรับมือ เพื่อความมั่นใจในระบบสถาบันการเงิน การกำหนดแนวนโยบายที่จะช่วยลดความเสี่ยงหรือนำไปสู่การลงโทษผู้กระทำผิดใน 4 ขั้นตอน โดยมี พ.ร.ก.มาตรการป้องกัน และปราบปรามอาชญากรรมทางเทคโนโลยีเข้ามามีบทบาทสำคัญในการคุ้มครองประชาชนจากมิจฉาชีพที่หลอกลวง ประกอบด้วย

1. การติดต่อของคนร้ายผ่านโทรศัพท์มือถือ เป้าหมายของมาตรการในกลุ่มนี้คือ ลดโอกาสในการติดต่อเหยื่อได้สำเร็จ ได้แก่ การปิดกั้น SMS โดย ธปท. และศูนย์ประสานงานด้านความมั่นคง

ผู้จัดการรายวัน 360°
Poo Jadkarn Daily 360 Degree
Circulation: 850,000
Ad Rate: 1,500

Section: iBusiness/-
วันที่: พฤหัสบดี 20 กรกฎาคม 2566
ปีที่: 15 ฉบับที่: 4000 หน้า: 2(กลาง)
Col.Inch: 225.64 Ad Value: 338,460 PRValue (x3): 1,015,380 คลิป: สีสี
หัวข้อข่าว: ธปท.เข้มมาตรการภัยการเงินปิดช่องโหว่รูปแบบใหม่

ปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) ทำงานร่วมกับ กสทช. ในการลด SMS หลอกลวงที่แอบอ้างชื่อธนาคาร และการปิดกั้นเว็บไซต์ปลอมที่จะเป็นช่องทางของคนร้ายหลอกให้ติดตั้งแอปพลิเคชัน โดยทำงานร่วมกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) เพื่อให้เกิดกระบวนการที่รวดเร็วขึ้นในการปิดกั้นเว็บไซต์

2. การทำธุรกรรมโอนเงินให้คนร้าย มาตรการที่จะช่วยป้องกันในขั้นตอนนี้คือ การแจ้งเตือนผ่าน pop-up message บนโทรศัพท์มือถือในขณะที่ผู้โอนกำลังทำธุรกรรมทาง mobile banking ซึ่งจะช่วยเพิ่มความระมัดระวังในการทำธุรกรรมมากยิ่งขึ้น การปรับปรุงระบบรักษาความปลอดภัยบน mobile banking ให้ทันสมัย เท่าทันภัยการเงินรูปแบบใหม่อยู่เสมอ และยังมีการเพิ่มมาตรการยืนยันตัวตนด้วย biometrics หรือการสแกนใบหน้าในกรณีที่มีการโอนเงินตามจำนวนที่กำหนดเงื่อนไขไว้ ซึ่งจะช่วยสร้างภูมิคุ้มกันและป้องกันภัยใหม่ๆ

3. การโอนเงินเป็นทอดๆ ของบัญชีม้า ในส่วนนี้มีการพัฒนาระบบเฝ้าระวัง และการตรวจจับธุรกรรมที่ผิดปกติ ซึ่งเดิมธนาคารไม่มีอำนาจระงับธุรกรรมได้ แต่ พ.ร.ก.ฯได้กำหนดให้ธนาคารสามารถระงับธุรกรรมได้ชั่วคราว เมื่อตรวจพบว่าบัญชีเงินฝากถูกใช้ทำธุรกรรมต้องสงสัยหรือได้รับแจ้งจากผู้เสียหาย และยังสามารถระงับธุรกรรมที่ดำเนินการเป็นทอดๆ จนถึงทอดสุดท้ายได้อีกด้วย

4. การดำเนินคดีและการช่วยเหลือเยียวยา เพื่ออำนวยความสะดวกให้กับประชาชนในการติดต่อธนาคาร นอกจากที่ ธปท. ได้ออกมาตรการให้ธนาคารมีสายด่วนที่ประชาชนสามารถติดต่อได้ตลอด 24 ชั่วโมง และการติดตามให้การดูแลรับผิดชอบลูกค้าของธนาคารในกรณีพิสูจน์ข้อเท็จจริงพบว่าความเสียหายเกิดจากข้อบกพร่องของธนาคารแล้ว พ.ร.ก.ฯก็ได้ให้สิทธิประชาชนสามารถไปแจ้งความได้ทั่วราชอาณาจักร ทำให้การติดต่อเจ้าหน้าที่ตำรวจเพื่อดำเนินคดีกับผู้ร้ายเป็นเรื่องที่ง่ายขึ้น นอกจากนี้ พ.ร.ก.ฯดังกล่าวก็ยังกำหนดบทลงโทษผู้รับจ้างเปิดบัญชีม้า หรือผู้ที่ประกาศขายบัญชีม้าและหมายเลขโทรศัพท์ที่จะนำไปใช้กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอีกด้วย

คาถาระวังภัย 'มีสติ อย่าเชื่อ อย่ากด อย่าโอน'

"ธปท. ได้พยายามสื่อสารให้ประชาชนทราบถึงภัยทางการเงินต่างๆ อย่างทันท่วงที เพื่อไม่ให้ใครต้องตกเป็นเหยื่อรายถัดไป โดยช่องทางหลักของ ธปท. ที่ประชาชนสามารถติดตามข้อมูลข่าวสาร แจ้งเหตุ รวมถึงร้องทุกข์ด้านการเงินเข้ามาได้ นอกจากสายด่วน 1213 ของศูนย์คุ้มครองผู้ใช้บริการทางการเงินแล้ว ยังมีบริการผ่านเพลตเว็บไซต์ (https://www.1213.or.th) เฟซบุ๊ก (ศคง. 1213) รวมถึงสื่อสังคมออนไลน์อื่นๆ และยังร่วมมือกับพันธมิตร อาทิ ธนาคารพาณิชย์ สำนักงานตำรวจแห่งชาติ กระทรวงดิจิทัลฯ กสทช. รวมทั้งหน่วยงานผู้ให้บริการเครือข่ายโทรศัพท์ ในการยกระดับการเตือนภัยให้เข้าถึงประชาชนได้มากที่สุด ขณะเดียวกันก็ต้องขอความร่วมมือประชาชนในการระมัดระวังตัวเอง รู้เท่าทันมิจฉาชีพ เข้าใจทริกที่คนร้ายพยายามเข้ามาหลอกลวง โดยระลึกไว้เสมอว่าต้อง 'มีสติ อย่าเชื่อ อย่ากด อย่าโอน' อันจะเป็นคาถาง่ายๆ ที่จะทำให้ชีวิตเราปลอดภัยจากภัยการเงินหรือจากมิจฉาชีพต่างๆ ได้" .