

อันตราย-ดูดเงิน 203 แอป เดือนให้รับลบทิ้ง

ปธ.สมาคมธนาคารยืนยันเอง แบงก์เสียหายแล้วถึงหมื่นล้าน ธปท.เตือน-สั่งเฝ้าระวังลูกก้าว่น

‘203 แอปพลิเคชัน’ อันตรายดูดเงินออนไลน์
กระทรวงดีอีเอสเปิดรายชื่อ □ อ่านต่อหน้า 12

● 203 แอป □ ต่อจากหน้า 1

ขึ้นบัญชีดำ เตือนอย่าหลงเชื่อโหลดไว้ในมือถือ เพราะอาจถูกดูดทั้งเงินฝากและข้อมูลส่วนตัวได้ กระทรวงคลังยังไม่นิ่งนอนใจ เร่งแก้ไขถูกดูดเงินในบัญชีแบงก์ แต่ขอให้ผู้มีบัญชีระมัดระวังมากขึ้น ด้านแบงก์ชาติเตรียมออกมาตรการเสริม กำชับธนาคารตอบสนองลูกค้าด่วนจี๋ ส่วนสมาคมธนาคารเผยเกณฑ์แจ้งไว-ได้เงินคืน เดือนคนในชื่อยักคลึงก็ชี้ชัดว่าระบบปลอดภัย ล้วงข้อมูลไม่ได้แน่ เผยตัวเลขเสียหายแล้วหลักหมื่นล้าน ‘บิ๊กตู’ สั่งฟันอาชญากรรมออนไลน์ลบใช้เน็ตข้าม

ประเทศ-ชมผิ-บัญชีม้า ป้องประชาชนไม่ให้

เป็นเหยื่อ เมื่อวันที่ 20 ม.ค. นายอนุชา นूरพชัยศรี รองเลขาธิการนายกรัฐมนตรีฝ่ายการเมือง ปฏิบัติหน้าที่โฆษกประจำสำนักนายกรัฐมนตรี เปิดเผยความคืบหน้าการปราบปรามอาชญากรรมออนไลน์ ตามข้อสั่งการของ พล.อ.ประยุทธ์ จันทร์โอชา นายกฯ และรมว.กลาโหม โดยกำชับทุกหน่วยงานที่เกี่ยวข้องบูรณาการความร่วมมือปราบปรามอาชญากรรมออนไลน์อย่างจริงจังและเด็ดขาด

นายอนุชากล่าวว่าหน่วยงานที่เกี่ยวข้อง

เดินหน้าปราบปรามการลักลอบใช้อินเตอร์เน็ตข้ามประเทศผิดกฎหมาย แก้ปัญหาชมผิและบัญชีม้า โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอีเอส) สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) และสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ร่วมกันเดินหน้าปราบปรามมีความคืบหน้า ดังนี้ แก้ปัญหาการลักลอบใช้อินเตอร์เน็ตข้ามประเทศผิดกฎหมาย กสทช.ได้กำชับผู้ให้บริการโทรคมนาคมตรวจสอบการใช้บริการอินเตอร์เน็ตข้ามประเทศ และได้ตรวจสอบหาบริเวณที่มีการกระทำความผิดรวมถึงตัวผู้กระทำความผิด

นอกจากนี้ ยังแก้ปัญหาชมผิ กสทช. ให้ผู้ให้บริการโทรคมนาคมแจ้งเจ้าของชมโทรศัพท์มือถือขึ้นยันตัวตนให้ถูกต้อง กรณีผู้มี 100 ชมขึ้นไปประมาณ 8,000 ราย ให้ขึ้นยันตัวตนภายในเดือนม.ค. 2566 กรณีผู้มี 30 ชมขึ้นไปประมาณ 22,000 ราย ให้ขึ้นยันตัวตนภายในเดือนมีนาคม 2566 และกรณีผู้มี 5 ชมขึ้นไปประมาณ 380,000 ราย ให้ขึ้นยันตัวตนภายในเดือนมิ.ย. 2566 และแก้ปัญหาบัญชีม้า

และบัญชีต้องส่งสายนำไปใช้กระทำผิดกฎหมาย สำนักงาน ปปง. ได้จัดทำประกาศหลักเกณฑ์ในการพิจารณากำหนดหรือทบทวนรายชื่อบุคคลที่มีความเสี่ยงสูง ซึ่งควรได้รับการเฝ้าระวังอย่างใกล้ชิด และได้แจ้งรายชื่อผู้กระทำผิดกฎหมาย ให้สถาบันการเงินดำเนินมาตรการที่เกี่ยวข้องต่อไป

ด้านนายชัชวาลย์ ธนาทิมพิทักษ์ รองอธิบดีเพื่อเศรษฐกิจและสังคม (คีโอเอส) เปิดเผยว่า ขณะนี้มีการแพร่ระบาดของมัลแวร์อันตรายที่มาในรูปแบบของแอปพลิเคชัน ซึ่งคีโอเอสและสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ตรวจสอบมาโดยตลอด โดยพบปัญหาสำคัญที่ส่งผลกระทบต่อประชาชน โดยเฉพาะผู้ใช้งานโทรศัพท์ที่ติดตั้งแอปพลิเคชันที่ถูกระบุว่าสามารถขโมยข้อมูล หรือควบคุมเครื่องโทรศัพท์ได้ โดยในปี 2022 มีการเผยแพร่รายชื่อแอปพลิเคชันอันตรายเหล่านี้ ซึ่งมีมากกว่า 200 รายการ ทั้งในระบบ iOS และ Android ตามที่ปรากฏใน Facebook ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ Facebook ของสกมช. (NCSA THAILAND) จึงขอให้ผู้ใช้งานตรวจสอบ หากพบแอปพลิเคชันดังกล่าว ให้ถอนการติดตั้งโดยทันที และควรอัปเดตระบบของเครื่องโทรศัพท์ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

ทั้งนี้ คีโอเอสขอแจ้งเตือนพี่น้องประชาชนให้ระมัดระวังในการดาวน์โหลดแอปพลิเคชันต่างๆ ลงบนโทรศัพท์มือถือ เพราะอาจจะไปเจอมัลแวร์อันตรายได้ เพราะหากโหลดเข้าไปในเครื่องก็จะมีโอกาสที่จะถูกดูดข้อมูลส่วนบุคคล หรือถูกรีโมตเข้ามาควบคุมมือถือ ซึ่งถ้าเกี่ยวกับการเงินก็อาจจะถูกโอนเงินออกไปที่เรียกว่าใช้แอปดูดเงิน และถ้าพบแอปฯ เหล่านี้ อยู่ในมือถือให้รีบลบออก ซึ่งขณะนี้ กระทรวงได้ประสานกับทาง Play Store หรือ App Store ทั้งหมดแล้วไม่ให้มีแอปฯ เหล่านี้ในระบบเพื่อป้องกันไม่ให้ประชาชนหลงกลแล้วโหลดเข้าไป

นอกจากนี้ ยังพบปัญหาการสร้าง SMS โดยใช้ชื่อเดียวกับผู้ส่ง (Sender Name) ที่เป็นธนาคาร แพลตฟอร์มอีคอมเมิร์ซ และสื่อสังคมออนไลน์ ทำให้ผู้รับ SMS เข้าใจผิดและหลงเชื่อมาจากหน่วยงานจริง ซึ่งโดยทั่วไปหน่วยงานส่วนใหญ่ได้ออกประกาศว่าจะไม่มีการส่งลิงก์ผ่าน SMS ให้กับผู้ใช้บริการ ดังนั้นจึงขอเตือนให้ประชาชน อย่าหลงเชื่อคลิก

ที่มากับ SMS หรือเพิ่มเพื่อนจากไลน์ไอดี โดยให้สังเกตรูปแบบ เนื้อหาที่อาจเป็นสิ่งที่เกิดขึ้นจริงหรือทำให้หวาดกลัว เช่น “คุณได้รับอนุมัติวงเงินกู้ 50,000 บาท คลิกลิงก์...” หรือ “โปรดยืนยันรหัสผ่าน มิฉะนั้นบัญชีของท่านจะถูกระงับการใช้งาน คิดต่อไลน์ไอดี...” โดยอาจจะตรวจสอบข้อมูลกับหน่วยงานที่ถูกระบุว่าส่ง SMS มาอีกครั้ง

ทั้งนี้ สกมช. ได้รวบรวมรายชื่อบริษัทที่ทำการส่ง SMS ปลอมเหล่านี้ เพื่อหยุดการทำการธุรกรรมต่างๆ ซึ่งกระทรวงและหน่วยงานที่เกี่ยวข้อง จะดำเนินการประสานงานกับสกมช. เพื่อขอให้ผู้ให้บริการมือถือทุกค่ายและธุรกิจที่ทำ SMS แล้วปล่อยให้มีการปลอมชื่อออกมา ซึ่งหากทำสำเร็จก็จะไม่มี SMS ปลอมอีก นอกจากนี้ เรื่องการแอดไลน์ก็เช่นเดียวกัน บางทีส่งไลน์มาก็เป็นไลน์ปลอมให้เข้าไปแอด เห็นชื่อเห็นรูปอาจจะเป็นคนที่เรารู้จัก หรือเป็นบริษัท หน่วยงานที่เรารู้จัก เพราะฉะนั้นขอให้ระวังเช่นเดียวกัน

“อย่าไปแอดไลน์ อย่าไปคุยกับคนเหล่านี้ เพราะว่าถ้าเขาพูดคุยเข้ามา ส่งข้อความมาที่เป็นของที่ดีเกินจริง ได้ประโยชน์มากเกินไป เช่น อาจจะให้กู้เงินห้าหมื่นบาท ให้ขายสินค้าในราคาพิเศษถูกมากๆ หรือหลอกว่าจะมีรายได้พิเศษให้เรา ถ้าเราไปทำงานกับเขา ไปลงทุนกับเขา พวกนี้มันดีเกินจริง คิดไว้เลยว่า เป็นมิจฉาชีพ ผ่านช่องทางไลน์ปลอม หรือ SMS ปลอม ก็อย่าไปยุ่ง อย่าไปคลิก อย่าไปให้ข้อมูลเด็ดขาด” นายชัชวาลย์กล่าว

วันเดียวกัน นายอคม เดิมพิทยไพสิฐ รมว.คลัง เปิดเผยมติการหลอกลวงทางออนไลน์ ขอให้ประชาชนระมัดระวัง โดยเฉพาะโลกดิจิทัล อาจจะถูกหลอกลวงมาให้กดปุ่ม กดลิงก์ต่างๆ แล้วเงินก็ถูกดูดไปหมด ซึ่งรวมถึงหน่วยงานรัฐต่างๆ ก็ถูกนำไปอ้างหลอกลวงเงินด้วย ซึ่งล่าสุด มีจำนวนมากที่มีปัญหา รัฐบาลไม่ได้นั่งนอนใจ ก็ขอให้ตรวจสอบ ทางธนาคารแห่งประเทศไทย (ธปท.) ก็สื่อสารออกไปแล้วขอให้ระมัดระวังให้มาก โดยเฉพาะเด็กและเยาวชน

นายธนากร นุ่มนนท์ รองผู้ว่าการ ด้านเสถียรภาพสถาบันการเงิน ธนาคารแห่งประเทศไทย (ธปท.) เปิดเผยว่า การแก้ปัญหาการถูกหลอกลวงเงินในบัญชี มีมาตรการที่ ธปท.กำลังหารือกันอยู่ โดยเฉพาะแนวทางการให้ความรู้แก่ผู้ใช้บริการทางการเงิน ให้มีความตระหนัก ให้ความสำคัญ กรณีที่มีการกดลิงก์

ในระบบออนไลน์ต่างๆ เหล่านั้นมีความเสี่ยง แปรปรวน ไม่อยากให้ประชาชนเข้าไปคลิก ขณะเดียวกัน ต้องประสานกับหน่วยงานที่เกี่ยวข้อง ให้ช่วยสกัดกันเว็บปลอม ให้ทันการมากขึ้น ในกรณีผู้เสียหายถูกดูดเงินออกจากบัญชีไปแล้วนั้น ได้เน้นย้ำให้สถาบันการเงินมีมาตรการดูแลลูกค้าทุกรายอย่างเต็มที่ ต้องดูเป็นรายกรณีไป ถ้าเป็นความผิดพลาดจากสถาบันการเงินก็รับผิดชอบเต็มร้อย รับพิจารณาช่วยเหลือและดูแลความเสียหายของผู้เสียหาย แต่ถ้าเกิดจากสาเหตุตัวผู้ใช้เองก็ต้องดูเป็นรายกรณีไป โดยกำหนดให้สถาบันการเงินมีขั้นตอนปฏิบัติที่กำหนดร่วมกัน เมื่อมีเหตุการณ์เกิดขึ้น ก็ต้องมีการตอบสนองเร็วกว่าที่ผ่านมา

ด้านนายพย ศรีวัชร กรรมการผู้จัดการใหญ่ ธนาคารกรุงไทย ในฐานะประธานสมาคมธนาคารไทย เปิดเผยว่า แนวทางภาครัฐในการเร่งแก้ไขแก้ปัญหาอาชญากรรมออนไลน์ กรณีที่กำกับให้สถาบันการเงินตรวจสอบ เฝ้าติดตาม ขอมรับว่ายังมีข้อจำกัดสามารถเร่งได้ แต่ก็ทำได้ถึงจุดเดียว เพราะเมื่อไหร่ที่ไปคาบเกี่ยวกับบุคคลที่สาม หรือธนาคารอื่น เช่น การอายัดบัญชีทันทีที่พบว่ามี ความผิดปกติ ก็ไม่สามารถก้าวล่วงได้ตามพร.บ.ข้อมูลส่วนบุคคล หรือพีดีพีเอ ซึ่งเรื่องนี้ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อยู่ระหว่างเร่งปรับข้อกฎหมาย เพื่อให้ธนาคารสามารถแก้ไขปัญหาได้เร็วขึ้น

ทั้งนี้ ขอเน้นย้ำให้ผู้ใช้บริการทุกรายระมัดระวังในการให้ข้อมูล เช่น ให้ USER-NAME PASSWORD โดยเฉพาะการกดลิงก์ต่างๆ ที่ส่งผ่านกันในระบบออนไลน์ โดยเฉพาะในรายการที่มีการชักชวนแปลกๆ เช่น เงินกู้ อนุมัติ ชวนชิม ปลูกอง บัตรลดต่างๆ เพราะต้องยอมรับว่าอาชญากร มีระบบ เวลาที่ดูดเงินได้ ก็โอนต่อไปอีกหลายบัญชี ทั้งบัญชีม้า บัญชีข้ามแบงก์ บัญชีเปลี่ยนชื่อเปลี่ยนมือเงินของท่านจะถูกส่งต่อไปไว้มาก

“เพราะฉะนั้น อย่ากด เพราะการกดมันจะมีหลายเรื่อง คือ ต้องเข้าใจโทรศัพท์ตนเอง เช่น มีระบบอัตโนมัติ หรือเปิดรับอนุญาตทำให้ล่วงข้อมูลต่างๆ ได้ ที่สุดผู้ใช้คือ กล้อง ต้องรู้ว่ากดอะไร เหมือนท่านไปเซ็นสัญญา ท่านก็ต้องรู้ว่ากำลังเซ็นอะไร ซึ่งเรื่องนี้ทางสมาคมธนาคารก็มีการสื่อสารออกมาตลอดให้ระมัดระวังการใช้งาน ถ้าจะเชื่อมบัญชีจริงๆ ควรเชื่อมกับบัญชีที่มีวงเงินนิดเดียว อย่าไป

เปิดบัญชีหลายอย่าง ถ้าขยันกด ก็ต้องรู้ พฤติกรรมการใช้ของตัวเอง”

นายผยงกล่าวว่า ขึ้นชื่อว่าตามระบบของ ธนาคารจะไม่สามารถถูกล้วงข้อมูลจาก อาชญากรได้ หากผู้ใช้ไม่ได้ไปกดยินยอม อะไรให้ระบบเอง ส่วนในกรณีผู้เสียหายที่ ธนาคารสามารถรับผิดชอบได้ ก็ต้องดูเป็น กรณีๆ เช่น การแจ้งของผู้ใช้งานเกี่ยวกับความ ผิดปกติ มีการแจ้งสายไปแล้วหรือไม่ หรือเมื่อ อาจจะแจ้งเร็วแต่ถ้าเป็นหน่วยงานที่เป็นบุคคล ที่สาม มีหมายจับตำรวจหรือไม่ มีหมายแจ้ง ความจากตำรวจหรือไม่ ที่จะให้ธนาคารมี สิทธิ์ในการไปประสานกับหน่วยงานที่เกี่ยวข้อง เพราะฉะนั้น มีเรื่องกฎหมายข้อมูล ส่วนบุคคล ซึ่งเป็นข้อจำกัดอยู่

นายผยงกล่าวว่า การตรวจจับระบบหลอกลวง ทำได้เฉพาะตรวจจับในกลไกของแต่ละ ธนาคารเอง เช่น จับผู้รัย ก็จะรู้รัยใน ธนาคาร แต่ไม่รู้ผู้รัยข้ามธนาคาร อาชญากร ข้ามธนาคาร ต้องยึดกรณีนี้เป็นขบวนการ ก็ สลับหมุนไปได้เรื่อยๆ ที่ผ่านแต่ละธนาคาร ก็ได้เตือนกันบ่อย แต่ผู้ใช้ยังไม่สนใจเท่าที่ควร ผู้สื่อข่าวถามว่า ทางสถาบันการเงินได้ ประเมินตัวเลขความเสียหายจากภัยหลอกลวง มีสัดส่วนเพิ่มขึ้นหรือไม่ นายผยงกล่าวว่า ไม่ได้ดูตัวเลข แต่รู้ว่าตัวเลขมันเยอะ และถามว่า ถึงหลักหมื่นล้านบาทหรือไม่ นายผยงกล่าวว่า ถึงหลักหมื่นล้านบาท

สำหรับแอปพลิเคชัน ที่กระทรวงคือเอส ประภาสให้เป็นแอปพลิเคชันอันตราย ไม่ ปลดออกได้แก่ 1. 4K Pro Camera 2. 4K Wattpapers Aout Changer 3. Advanced SMS 4.apic-magic Photo Editor 5. All Good PDF Scanner 6. All Language Transtate 7. All Photo Translator 8. Art Filters 9. Astrom+Horoscope & Astrology 10. Astroline The Daily Horoscope 11. Auto Sticker Maker Studio 12. Avatat Maket character creatca 13. Baby Sticker-Track Miletones 14. Bass Boosyer Volume Power Amp 15. Battery Charging Animations Battery Wallpaper 16. Battery Charging Animations Bubbic-Effects 17. Beat.ty Music Viedo Maker 18. Beat maker pro 19. Beauty Filer 20. Blood Pressure Checker

21. Blood Pressure Diary 22. Blue Scanner 23. Blur Image 24. Caller Theme 25. CallMe Phone Themes 26. Call Skins 27. Camera Translator 28. Care Message 29. Cartoons Me

30. Cashe Cleaner 31. Chat Ontine 32. Chat SMS 33. Chat Text SMS 34. Ctassie Emoji Keyboard 35. Ctassie Game Messenger 36. Coco camera v1.1 37. Come Messages 38. Contact Background 39. Cool Keyboard 40. Cool Messages

41. Creative 3D Launcher 42. Creative Emoji Keyboard 43. Cusstom Themed Keyboard 44. Cut, Paste 45. Dazz Cam- D3D Photo Effect 46. Dazz-insta stories editor 47. Dazzling Keyboard 48. Design Maker 49. Desire Translate 50. Direct Messenger 51. Dizzi 52. DJ itl 53. Drink Water 54. Drums Play Beats & Drum Games 55. Easy PDF Scanner 56. edjing Mix 57. edjing Pro 58. EmojiOne Keyboard 59. Emoji Theme Keyboard 60. Equalizer+HD music player

61. Equalizer Fx Bass Booster App 62. Facelad 63. FaceMe 64. Factory Face Yoga & Exercise 65. Fancy Charging 66. Fancy SMS 67. Flashlight Flash Alert On Call 68. FLMX 69. Fonts Emoji Keyboard 70. Frame 71. Frames 72. Freeglom Camera 1.0.0 73. Funny Caller 74. Funny Camera 75. Funny Emoji Message 76. Funny Keyboard 77. Funny Wallpapers-Live Scree 78. Gif Emoji Keydoard 79. Girl Games Unicom Slime 80. Guitar Play-Games & Songs

81. Guitar - real games & lessons 82. Guitar Tuner - Ukulele & Bass 83. Halloween Coloring 84. Handset - Second Phone Number 85. Heart Emoji Stickers 86. Hightiht Story Cover Makerl 87. Hi Text SMS 88. Horoscope 2019 and patm Peadar 89. Hub - Story Temptates Maker 90. Hummingbird PDF Converter - photo to PDF 91. Hyper Cleaner Clean Phone 92. icons - Icon Changer App+ 93. iMessenger 94. impresso 95. instant Messenger 96. iWidget pro 97. JambL DJ Band & Beat Maker 98. Jigsaw Puzzle 99. Karaoke Songs 100. Life Patmistry

101. LiFl Story Messenger 102. Light Messages 103. Live Wallpaper Maker 4K Theme 104. Loop Maker Pro 105. Lucky Life 106. MagicFX -Magic Video Effects 107. Magic Photo EDitor 108. Memoristo BrainTest, IO Game 109. Memory Sitent Camera 110. Menu Makerl 111. Meticulous Scanner 112. Metronome Pro - Beat & Tempo 113.

Metronome - Tap Tempo & Rhythm 114. Mimi PDF Scanner 115. Mint Leaf Message Your Private Message 116. Mood Balance Self Care Tareker 117. Music Zen -Relaxing Sounds 118. MyCall - Call Personalization 119. Nebula: Horoscope & Astrolgy 120. Neon Theme Keyboar

121. NewScrean: 4D Wallpapers 122. Notes - reminders and lists 123. Now QR code Scan 124. One Sentence Translator - Multifunctional Tarnslator 125. Painting Photo Editor 126.Paper Doc Scanner 127. Part Message 128. Password Manager 129. Path - horoscope & Astrology 130. PDF Scanner: Document Scan 131. Personal Message 132. Photo Collage 133. Photo Editor & Background Eraser 134. Photo Editor -Filters Effects 135. Photo & Exif Editor 136. Photo Filters & Effects 137. Photoly Remove Object & Editor 138. Photo To Sketch 139. Piano Crush 140. Piamo

141. Pista 142. Pixomatic 143. Poco Launcher 144. Premium SMS 145. Preseis for Lightroom 146. Private Garne Messages 147. Private Messenger 148. Private SMS 149. Professional Messenger 150. Quick Talk Message 151. Razer Keyboard & Theme 152. RECOLLECT 153. Retouch & Cutout 154. Rich Theme Message 155. Ringtones HD 156. ScanGuru 157. Scanner App 158. Send SMS 159. Simple Note Scanner 160. SlidePic 161. Slimy 162. Smart Messages 163. Smart SMS Messages 164. Smnrt TV remote 165. Smite Emoji 166. Social Message 167. SpeedPro Slow speed video edit 168. Stickerfy: Sticker Maker 169. Sticker Maker 170. Stickers & GIF

171. Stock wallpapers & Backgrounds 172. Sty Message 173. Style Photo Collage 174. Super Hero - Effect 175. Sweet Pics - Baby Photo Editio 176. Talent Photo Editor - Blur fous 177. Tangram App Lock 178. TeasEar : ASMR Slime Antistress 179. Text Emoji SMS 180. Text SMS 181. Themes Chat Messenger 182. Themes Photo Keyboard 183. Timestamp Camera 184. ToonApp Cartoon Photo Editor 185. Yranslate Camera - Speak On 186. Translator Guru: Voice & Text 187. Ultar FX - Effect Video Maker 188. Unice QR Scanner 189. Unipue Keyboard 190. Univers

ข่าวสด

Khao Sod
Circulation: 950,000
Ad Rate: 1,650

Section: First Section/หน้าแรก

วันที่: เสาร์ 21 มกราคม 2566

ปีที่: 32

ฉบับที่: 11742

หน้า: 1 (บนซ้าย), 12

Col.Inch: 177.10 Ad Value: 292,215

PRValue (x3): 876,645

คลิป: สีสี่

หัวข้อข่าว: อินเทอร์เน็ต-ดูเงิน203แอปเตือนให้รับลบทิ้ง

PDF Scanner

191. Vanitla Snap Camera 192. Video
Puzzles - Puzzle 193. Ringtones HD Ringtone
Maker 194. VOCHI Video Effects Editor 195.
Volume Booster Hearing Aid 196. Volume
Booster Louder Sound Equalizer 197. Water
Reminder 198. Wedrum: Drums, Real Drum
Games 199. Widget PLUS+ - Photo & Weather
200. WowBeautyCamera 201. Wow Translator
202. Yoga - For Beginner to Advanced 203.
YouToon - AI Cartoo

แอปฯ ดูดเงิน มัลแวร์ล้วงข้อมูล “ยอดเหยื่อพุ่ง” ติดกับ “โจรไซเบอร์”

เป็นปัญหาหลุมกลามขยายวงกว้างไปเรื่อยๆ สำหรับกรณี “ถูกดูดเงิน” ในบัญชีธนาคารผ่านแอปฯ บนโทรศัพท์มือถือ ติดกับ “โจรไซเบอร์” ออกอุบายล่อลวงเหยื่อผ่าน SMS ลวงให้กดลิงก์ปลอม ลวงให้โหลดแอปฯ แอปฯ ปลอม “แฝงมัลแวร์” ใช้ Remote app ควบคุมการทำการธุรกรรมต่างๆ บนมือถือ ถอนเงินจากบัญชีธนาคาร รู้ตัวอีกทีก็ตอนเงินที่ผูกในบัญชี mobile banking ถูกดูดออกไปเกลี้ยง

สัปดาห์ที่ผ่านมา เกิดประเด็นสายชาร์จมือถือดูดเงินเกลี้ยงบัญชีผู้เสียหายรายหนึ่ง ซึ่งหน่วยงานที่เกี่ยวข้องอย่างธนาคารแห่งประเทศไทย (ธปท.) ได้หารือสมาคมธนาคารไทย ตรวจสอบการนี้ดังกล่าวพบว่ากรณีนี้ไม่ได้เกิดจากการใช้งานสายชาร์จปลอม แต่เกิดจากผู้เสียหายถูกมิจฉาชีพหลอกลวงให้ติดตั้งแอปพลิเคชันหาข้อมูลการทำการธุรกรรมของลูกค้า และควบคุมเครื่องโทรศัพท์เพื่อสวมรอยทำการธุรกรรมแทนจากระยะไกล เพื่อโอนเงินออกจากบัญชีโดยอาจเลือกทำการธุรกรรมในช่วงเวลาที่ผู้เสียหายไม่ได้ใช้งานโทรศัพท์

อีกกรณีที่ต้องจับตา นายเอกภพ เหลืองประเสริฐ ผู้ก่อตั้งเพจสายไหมต้องรอด และทีมงานพากลุ่มผู้เสียหาย 20 คน หากนับรวมผู้เสียหายที่มีการร้องเรียนผ่านเพจฯ ยังมีอีกนับร้อยราย ซึ่งถูกแฮกเกอร์ดูดเงินในบัญชีธนาคารผ่านแอปฯ มูลค่าความเสียหายกว่า 1 ล้านบาท ไปร้องทุกข์กับ พล.ต.ต.กาน

ตพงศ์ ชัยรุ่งเรือง ผู้บังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี (ผบก.ตอท.) จากการณีถูกดูดเงินเกลี้ยงบัญชี อยู่ๆ เงินที่อยู่ในแอปธนาคารซึ่งอยู่ในโทรศัพท์มือถือถูกโอนย้ายไปบัญชีของมิจฉาชีพโดยที่ไม่ทราบสาเหตุ และทุกคนยืนยันว่าไม่ได้กดลิงก์แปลกๆ ไม่ได้โหลดแอปฯ เกือบใด ซึ่งอยู่ระหว่างการตรวจสอบต่อไป

ขณะที่ พล.ต.ต.กานตพงศ์ แนะนำว่าบัญชีเงินฝากไม่ควรไปผูกกับ e-banking ไว้โดยเฉพาะเงินที่ไม่ได้ใช้ประจำต้องแจ้งธนาคารว่าจะไม่ผูกทาง อินเทอร์เน็ตแบงก์กิ้งทุกกรณี อย่างไรก็ตาม ต้องยอมรับว่าพฤติกรรมของคนร้ายจะมีพัฒนาการไปเรื่อยๆ

ทั้งนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) เปิดเผยว่า ปัจจุบันเกิดปัญหาปลอม SMS หรือ Line เป็นหน่วยงานรัฐ เช่น ดีเอสไอ กรมสรรพากร หรือ สถาบันการเงิน เพื่อหลอกให้ประชาชนหลงเชื่อและคลิกลิงก์เว็บปลอมที่แนบมาจนนำไปสู่การถูกติดตั้งมัลแวร์ในเครื่องเพื่อติดตั้งแอปพลิเคชันและดูดเงินจากบัญชีธนาคารออนไลน์ของประชาชนจนเกลี้ยงบัญชี ด้วยการใช้คอมพิวเตอร์ระยะไกล เป็นปัญหาที่เพิ่มขึ้นอย่างต่อเนื่อง

วิธีสังเกต

แอปฯ ดูดเงินแฝงในมือถือ

- 1 แอปฯ ค้าง หรือหยุดทำงานแบบไม่มีเหตุผล
- 2 เครื่องช้า และอืดกว่าเดิมมาก
- 3 แบตเตอรี่หมดเร็วกว่าปกติ

ตัวอย่างแอปฯ อันตราย

- Smat TV remote
- Super Hero-Effect
- Volume Booster Louder Sound Equalizer
- Flashlight Flash Alert On Call
- Now QRcode Scan
- Volume Booster Hearing Aid

ที่มา : Kaspersky US ปรึกษาความปลอดภัยกับไอที

ที่ผ่านมา สกมช.ดำเนินการปิดเว็บมิจฉาชีพไปแล้ว 70 เว็บ ขณะที่ภาครัฐเองก็ประกาศนโยบายชัดเจนว่า ไม่มีการส่งเอสเอ็มเอส หรือติดต่อประชาชนผ่านทางไลน์เด็ดขาด

อย่างไรก็ตาม สถานการณ์ดังกล่าวเป็นเรื่องปัญหาหลุมกลามขยายวงกว้าง แนวโน้มมีผู้เสียหายเพิ่มขึ้นต่อเนื่อง ซึ่ง พลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงกลาโหม ได้เน้นย้ำให้ทุกหน่วยงานที่เกี่ยวข้องทั้งในส่วนกลางและส่วนภูมิภาค ธนาคารแห่งประเทศไทย (ธปท.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงาน กสทช. สำนักงาน ปปง. และสำนักงานตำรวจแห่งชาติ ดำเนินการเพื่อป้องกันและแก้ไขปัญหที่เกิดขึ้น

ขณะเดียวกัน ทาง ธปท. ก็ออกมาตรการต่างๆ ให้สถาบันการเงินต้องปฏิบัติ พร้อมร่วมมือกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) และสำนักงานตำรวจแห่งชาติ เพื่อดำเนินการต่างๆ ดังนี้

1) ปรับปรุงพัฒนาระบบรักษาความปลอดภัยบน Mobile Banking อย่างต่อเนื่อง 2) ปิดกั้นเว็บไซต์หลอกลวง และตัดการเชื่อมต่อกับเครื่องคอมพิวเตอร์ที่มีมัลแวร์ใช้ควบคุมเครื่องผู้เสียหายจากระยะไกล และ 3) แก้ไขปัญหา SMS หลอกลวง ที่แอบอ้างชื่อเป็นสถาบันการเงิน 4) จัดให้มีช่องทางในการรับแจ้งความออนไลน์เพื่อให้ประชาชนแจ้งความได้สะดวกและอายุคดีบัญชีได้รวดเร็วขึ้น 5) ประชาสัมพันธ์สร้างการตระหนักรู้ แจ้งเตือนภัย และให้คำแนะนำประชาชนอย่างต่อเนื่อง

รวมทั้งประชาสัมพันธ์ขอความร่วมมือพี่น้องประชาชนให้เพิ่มความระมัดระวัง โดยสามารถป้องกันภัยในเบื้องต้น เพื่อไม่ให้ตกเป็นเหยื่อมัลแวร์ ดังนี้ 1. ไม่คลิกลิงก์จาก SMS LINE และ อีเมลที่มีแหล่งที่มาที่ไม่รู้จักหรือไม่น่าเชื่อถือ 2. ไม่ดาวน์โหลดโปรแกรม นอกเหนือจากแหล่งที่ได้รับการควบคุมและรับรองความปลอดภัยจากผู้พัฒนาระบบปฏิบัติการที่เป็น Official Store อาทิ Play Store หรือ App Store เท่านั้น 3. อัปเดต Mobile Banking ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ หรือตั้งค่าให้มีการอัปเดตแบบอัตโนมัติ ซึ่งจะมีมาตรการป้องกันการควบคุมเครื่องทางไกลรวมถึงมีการปรับปรุงพัฒนาระบบรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ 4. ไม่ใช้เครื่องโทรศัพท์มือถือที่ไม่ปลอดภัยมาทำธุรกรรมทางการเงิน อาทิ เครื่องที่ปลดล็อก (root/jailbreak) เพื่อให้สามารถติดตั้งแอปพลิเคชันใดๆ ก็ได้ หรือใช้เครื่องที่มีระบบปฏิบัติการล้าสมัย เป็นต้น และ 5. ร่วมมือกับหน่วยงานที่เกี่ยวข้องในการให้ข้อมูลที่ถูกต้อง เพื่อให้การติดตามแก้ไขปัญหาเป็นไปอย่างรวดเร็ว และหากลูกค้าธนาคารพบธุรกรรมผิดปกติ สามารถติดต่อคอลเซ็นเตอร์หรือสาขาของธนาคารที่ลูกค้าใช้งาน เพื่อแจ้งตรวจสอบและยืนยันความถูกต้องของธุรกรรมในทันที โดยธนาคารจะดูแลแก้ไขปัญหาที่เกิดขึ้นโดยเร็วที่สุด

ทั้งนี้ ธปท. ได้ขอให้สถาบันการเงินทุกแห่ง มีมาตรการดูแลลูกค้าทุกรายตามขั้นตอนปฏิบัติที่กำหนด หากตรวจสอบและพิสูจน์พบว่า ลูกค้ามีส่วนเกี่ยวข้องในการให้ข้อมูลส่วนตัว สถาบันการเงินนั้น ต้องรีบช่วยเหลือและดูแลความเสียหายของลูกค้า โดยเร็วภายใน 5 วัน

พ.ต.อ.กฤษณะ พัฒนเจริญ โฆษกกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) เปิดเผยถึง

กรณีการหลอกลวงประชาชนผ่านสื่อสังคมออนไลน์ ซึ่งเป็นหนึ่งในแผนประทุษกรรมใหม่ๆ ของมัลแวร์ที่นำมาใช้ในการหลอกลวง เช่น ช่วงเทศกาล มัลแวร์จะฉวยโอกาสดังกล่าวส่งลิงก์ที่แนบมากับข้อความสั้น (SMS) อ้างว่าท่านได้รับอั่งเปาฟรี ได้รับสิทธิพิเศษ หรือได้รับเงินรางวัลต่างๆ

มัลแวร์จะหลอกลวงให้คลิกลิงก์เข้าไปในเว็บไซต์ปลอม หลอกลวงให้กรอกข้อมูลส่วนบุคคล และข้อมูลทางการเงิน เช่น ชื่อ นามสกุล วันเดือนปีเกิด เบอร์โทรศัพท์ หมายเลขบัตรประชาชน เลขบัญชีธนาคาร เลขบัตรเดบิตหรือเครดิต รหัสหลังบัตร 3 หลัก รหัส OTP เป็นต้น เพื่อนำไปใช้ประโยชน์ในทางมิชอบ ไม่ว่าจะเป็นการนำข้อมูลไปเข้าถึงบัญชีสื่อสังคมออนไลน์แล้วไปหลอกลวงผู้อื่น ใช้บัตรเดบิตหรือเครดิตรูดชำระค่าสินค้า

หรือถูกโอนเงินจากบัญชีธนาคาร หรือนำไปแอบอ้างทำเรื่องที่เกิดกฎหมาย

กรณีแอปดูเงินฯ ที่เกิดขึ้น ส่วนใหญ่เกิดจากผู้เสียหายถูกมัลแวร์สร้างกลอุบายหลอกลวงให้คลิกลิงก์ ดาวน์โหลด หรือติดตั้งแอปพลิเคชันปลอม โดยเฉพาะอย่างยิ่งแอปพลิเคชันที่มีไว้สำหรับการทำธุรกรรม แอปพลิเคชันดูเงินสด ดูภาพลามกอนาจาร และแอปพลิเคชันพูดคุยยอดนิยม เช่น Viber, Sweet meet, Bumble, Snapchat, Kakao Talk และ Flower Dating เป็นต้น โดยเมื่อติดตั้งแอปพลิเคชันดังกล่าวขอสิทธิการเข้าถึงข้อมูลที่มีความอ่อนไหว (permission) หลาก

รายการ ทำให้มัลแวร์สามารถเชื่อมต่อกับระบบธนาคาร และควบคุมหน้าจอโทรศัพท์ของเหยื่อเมื่อใดก็ได้ โดยจะทิ้งระยะเวลาให้เหยื่อตายใจระหว่างนั้นมัลแวร์จะส่งเกิดพฤติกรรมของเหยื่อ เช่น ใช้ธนาคารใด มีเงินในบัญชีเท่าไร และจดจำรหัสผ่านจากที่เหยื่อกดเข้าระบบของแอปพลิเคชันธนาคาร กระทั่งเวลาผ่านไปจนเหยื่อเผลอ เมื่อได้โอกาสมัลแวร์จะเชื่อมต่อแล้วโอนเงินออกจากบัญชีไป

ขณะที่ "พล.อ.ต.อมร ชมเชย" เลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กล่าวถึงกรณีสาย USB ที่สามารถดูดเงินตามที่ปรากฏเป็นข่าวอยู่ในขณะนี้ ว่า สาย USB ที่สามารถดึงข้อมูลสำคัญได้นั้นมีขายอยู่ และมีต้นทุนต่อเส้นอยู่ที่เส้นละ 4,000 บาท ผลิตโดยบริษัท Haks ซึ่งเป็นสายที่เหล่าแฮกเกอร์ใช้เพื่อดึงข้อมูลเหล่านั้นได้โดยตรงซึ่งต้นทุนต่อเส้นค่อนข้างสูง ทั้งนี้ การเข้าถึงข้อมูลด้วยสาย USB หรือสายชนิดอื่นๆ จะต้องทำงานผ่าน wifi และแฮกเกอร์จะต้องอยู่ใกล้กับมือถือจึงจะใช้สายชาร์จดูดข้อมูลได้ ดังนั้น ตามที่มีการแชร์ข่าวออกมาว่า เงินในบัญชีจะหายไปหากเสียบสายชาร์จแบตเตอรี่และไม่ควรซื้อสายชาร์จราคาถูกอาจจะไม่ปลอดภัยต่อข้อมูลในโทรศัพท์มือถือ ถือว่ามีโอกาสน้อยมากที่จะเกิดขึ้น

สำหรับหน่วยงานที่กำกับดูแลโดยตรง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอีเอส) ที่ผ่านมามีประชุมกับสถาบันการเงินผ่านสมาคมธนาคารไทยและธนาคารแห่งประเทศไทย เพื่อเร่งรัดแก้ปัญหาให้แอปธนาคารให้มีระบบป้องกันการถูกควบคุมหรือโจรกรรมข้อมูลอย่างรวดเร็วที่สุด ได้ตกลงให้ทุกธนาคารมีระบบ Cybersecurity ป้องกันแอปพลิเคชันธนาคาร ซึ่งได้รับการตรวจสอบแล้วว่าสามารถป้องกันได้จริง ซึ่งหลายธนาคารก็ได้ปรับปรุงไปแล้ว

ยังคงต้องติดตามว่า การแก้ปัญหา Remote app โดยเฉพาะสถานการณ์แอปฯ ดูเงิน ซึ่งทาง ธปท. และสมาคมธนาคารไทย ได้จัดทำระบบป้องกันมัลแวร์ เพื่อป้องกันการใช้ Remote Application ควบคุมการทำ Mobile Banking สวมรอยโอนเงินออกจากบัญชีผู้เสียหาย

และปฏิเสธไม่ได้ว่า เป็นโจทย์ข้อใหญ่ของธนาคารพาณิชย์ต่างๆ ในการจัดทำระบบป้องกันและปรับปรุงระบบ เพื่อกอบกู้ความเชื่อมั่นทางการเงินการใช้จ่าย Mobile Banking ในยุคดิจิทัล ■

เดือนภัยไซเบอร์



ความเคลื่อนไหวอย่างจริงจังและเป็นระบบมากขึ้นของหน่วยงานรัฐ ที่บูรณาการร่วมกันเพื่อการปราบปรามอาชญากรรมทางไซเบอร์ทุกรูปแบบ สะท้อนภาพว่าพฤติกรรมดังกล่าวในเมืองไทยรุนแรงมากขึ้น และสร้างความเสียหายในวงกว้างอย่างมีนัยสำคัญ ซึ่งไม่เพียงแต่การดูดเงินจากบัญชี หรือข้อมูลสำคัญของเหยื่อเท่านั้น แต่หมายรวมถึงการต้มตุ๋นออนไลน์ ล่อลวงให้ลงทุนรูปแบบต่าง ๆ ซึ่งนับวันยิ่งซับซ้อนมากขึ้น

ก่อนหน้านี้ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอีเอส) สนับสนุนกำลังกับสำนักงานตำรวจแห่งชาติ สำนักงานคณะกรรมการกฤษฎีกากระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ธนาคารแห่งประเทศไทย (ธปท.) สมาคมธนาคารไทย สำนักงาน ปปง. และหน่วยงานอื่น ๆ จัดทำระบบป้องกันมิฉะนั้นใช้ remote application ควบคุมการทำ mobile banking และสวมรอยโอนเงินออกจากบัญชีผู้เสียหาย

สำหรับ remote application เป็นแอปประเภท remote access ที่หากติดตั้งแล้วจะทำให้มีจวินสามารถเข้าถึงข้อมูลและควบคุมโทรศัพท์มือถือของเหยื่อ เพื่อทำธุรกรรมและโอนเงินออกจากบัญชีได้ โดยจะหลอกให้เหยื่อกรอกตัวเลข หรือรหัสผ่าน แล้วจึงนำรหัสเหล่านั้นไปใช้ทำธุรกรรมและโอนเงินออกจากบัญชี

ขณะที่ ธปท. ร่วมกับหน่วยงานภาครัฐ และภาคการเงินวางมาตรการป้องกันปัญหาดังกล่าว ประชาสัมพันธ์เสริมสร้างความตระหนักรู้ และแจ้งเตือนภัยแก่ประชาชน อีกทั้งยังอยู่ระหว่างร่วมมือกับสมาคมธนาคารไทย แลกเปลี่ยนข้อมูลการทุจริต และบัญชีม้า เพื่อลดจำนวนบัญชีม้า และลดความเสียหายจากการถูกทำทุจริตด้วย

ที่น่าสนใจไม่พ้นข้อมูลการรับแจ้งความออนไลน์ www.ThaiPoliceOnline.com ตั้งแต่วันที่ระบบเริ่มใช้งาน 1 มี.ค. 2565 ถึง 31 ธ.ค. 2565 รวม 10 เดือน มีผู้เข้ามาแจ้งความ 163,091 คดี มูลค่าความเสียหายประมาณ 27,305 ล้านบาท

แบ่งเป็นคดีที่ผู้กระทำความผิดอยู่ในประเทศไทย อาทิ การซื้อขายสินค้าหรือบริการผ่านทางออนไลน์แต่ไม่รับสินค้า การปล่อยกู้ผ่านแอป การลงทุนแชร์ลูกโซ่ เป็นต้น ความเสียหายประมาณ 1,230 ล้านบาท และคดีที่ผู้กระทำความผิดอยู่ต่างประเทศ-มีคนไทยร่วมขบวนการ หลอกหลวงคนไทยผ่านทางออนไลน์ ความเสียหายประมาณ 15,800 ล้านบาท

นอกจากหน่วยงานรัฐที่เร่งปราบปรามแล้ว ข้อสำคัญคือประชาชนต้องพึงระวังในการทำธุรกรรมออนไลน์ที่น่าสงสัย รวมถึงตั้งสติและคิดให้รอบด้านก่อนทำธุรกรรมใด ๆ โดยเฉพาะการชวนเชื่อผ่านโซเชียลมีเดีย ให้ร่วมลงทุนหรือทำธุรกิจที่ได้กำไรมากผิดปกติ เพราะคดีลักษณะนี้เมื่อสูญเสียเงินไปแล้วยากที่จะตามคืนมาได้

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 203แอปโจร ดูดเงินในบช.

เปิดรายชื่อทั้งหมด
ฝังมัลแวร์คุนมือถือ
ห้ามโหลด-หมดตัว
สั่งล้างบางแก๊งค์
เอสเอ็มเอสปลอม

“ดีเอส” จับมือ “ไซเบอร์แห่งชาติ” ★ มีต่อหน้า 6

กระทรวงดิจิทัล ☆ ต่อจากหน้า 1
เปิดรายชื่อ 203 แอปอันตราย หรือแอปดูดเงิน โหลดปั๊บ
ฝังมัลแวร์คุนข้อมูลส่วนบุคคล หรือถูกรีโมตเข้ามา
ควบคุมมือถือ ดูดเงินออกจากแอปบัญชีธนาคารได้
เตือนอย่าหลงเชื่อคลิกลิงก์ที่มาจากเอสเอ็มเอส หรือ
เพิ่มเพื่อนจากไลน์ไอดี โดยให้สังเกตรูปแบบเนื้อหา
ที่อาจผิดเพี้ยนจริง หรือทำให้หวาดกลัว เร่งประสาน
เพลย์สโตร์ และแอปสโตร์ไม่ให้ขึ้นแอปเหล่านี้ใน
ระบบเพื่อป้องกันไม่ให้ประชาชนหลงกลดาวน์โหลด
พร้อมรวบรวมรายชื่อบริษัทที่เอสเอ็มเอสปลอมระบาด

ให้หยุดการทำธุรกรรมต่างๆที่เป็นช่องทางของมิจฉาชีพ
ส่งไปหลอกลวงประชาชนด้วย

ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
(ดีเอส) เมื่อเวลา 09.00 น. วันที่ 20 ม.ค. นายชัยวุฒิ
ธนานานุสรณ์ รมว.ดิจิทัลเพื่อเศรษฐกิจและสังคม
เผยว่า ขณะนี้มีการแพร่ระบาดของมัลแวร์อันตราย
ในรูปแบบแอปพลิเคชันดีเอสและสำนักงานคณะกรรมการ
การกักกันโรคความมั่นคงปลอดภัยไซเบอร์
แห่งชาติ (สกมช.) ตรวจสอบพบปัญหาสำคัญส่งผล
ต่อประชาชน โดยเฉพาะผู้ใช้โทรศัพท์ที่ติดตั้งแอป

พลิเคชันที่ถูกระบุว่า โมยข้อมูลหรือควบคุมเครื่อง
โทรศัพท์ได้ปี 2565 มีการเผยแพร่รายชื่อแอปพลิเคชัน
อันตรายกว่า 200 รายการ ทั้งระบบไอโอเอส(iOS)
และแอนดรอยด์(Android) ตามที่ปรากฏในเฟซบุ๊ก
ของกระทรวงดีเอส และ สกมช. (NCSA THAILAND)
ขอให้ผู้ใช้งานตรวจสอบหากพบแอปพลิเคชัน
ดังกล่าวให้ถอนการติดตั้งทันที และอัปเดตระบบ
โทรศัพท์ตัวเองให้เป็นเวอร์ชันล่าสุดเสมอ

“ทั้งนี้ ดีเอสขอแจ้งเตือนพี่น้องประชาชน
ให้ระมัดระวังการดาวน์โหลดแอปพลิเคชันต่างๆลง
บนโทรศัพท์มือถือเพราะอาจไปเจอมัลแวร์อันตราย
ได้ หากโหลดเข้าไปในเครื่องมีโอกาสถูกดูดข้อมูล
ส่วนบุคคล หรือถูกรีโมตเข้ามาควบคุมมือถือ ถ้า
เกี่ยวกับการเงินอาจถูกโอนเงินออกไปเรียกว่าใช้
แอปดูดเงิน ขณะนี้ดีเอสประสานทางเพลย์สโตร์
(Play Store) หรือแอปสโตร์ (App Store) แล้ว
ไม่ให้ขึ้นแอปเหล่านี้ในระบบ เพื่อป้องกันไม่ให้
ประชาชนหลงกลโหลด” รมว.ดีเอสกล่าว

นายชัยวุฒิกล่าวต่อไปว่า นอกจากนี้ยังพบ
ปัญหาการส่งเอสเอ็มเอส(SMS) โดยใช้ชื่อเดียวกับ
ผู้ส่ง(Sender Name) ที่เป็นธนาคาร แพลตฟอร์ม
อีคอมเมิร์ซและสื่อสังคมออนไลน์ ทำให้ได้รับเอส
เอ็มเอสเข้าใจผิดหลงเชื่อว่าเป็นจากหน่วยงานจริง
โดยทั่วไปหน่วยงานส่วนใหญ่ออกประกาศว่า ไม่มี
การส่งลิงก์ผ่านเอสเอ็มเอสให้ผู้รับบริการ ดังนั้น ขอ
เตือนให้ประชาชนอย่าหลงเชื่อคลิกลิงก์ที่มาจาก
เอสเอ็มเอสหรือเพิ่มเพื่อนจากไลน์ไอดี ให้สังเกต
รูปแบบเนื้อหาที่อาจเป็นสิ่งที่ไม่ดีจริงหรือทำให้

หาวดกลัว เช่น “คุณได้รับอนุมัติวงเงินกู้ 50,000 บาท คลิ๊กลิ้ง...” หรือ “โปรดยืนยันรหัสผ่าน มิฉะนั้นบัญชีของท่านจะถูกระงับการใช้งาน จิตต่อไลน์ไอดี...” อาจตรวจสอบข้อมูลกับหน่วยงานที่ระบุว่าส่งเอสเอ็มเอสมาอีกครึ่ง

รณว.ดีเอสไอกล่าวต่อว่าสมท.รวบรวมรายชื่อบริษัทที่ส่งเอสเอ็มเอสปลอมเหล่านี้เพื่อหยุดการทำธุรกรรมต่างๆ ดีเอสไอและหน่วยงานที่เกี่ยวข้องจะดำเนินการประสานงานกับสำนักงานคณะกรรมการกฤษฎีกากระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) เพื่อขอให้ผู้ให้บริการมือถือทุกค่าย และธุรกิจที่ทำเอสเอ็มเอสแล้ว หากทำสำเร็จจะไม่มีเอสเอ็มเอสปลอมอีก นอกจากนี้เรื่องการแอดไลน์ก็เช่นเดียวกัน บางทีส่งไลน์มาเป็นไลน์ปลอมให้เข้าไปแอด เห็นชื่อเห็นรูปอาจเป็นคนที่เรารู้จัก หรือเป็นบริษัท หน่วยงานที่เรารู้จัก เพราะฉะนั้นขอให้ระวังให้ดี

“อย่างไรก็ตาม หากจะติดต่อกับหน่วยงานใดก็ตามผ่านช่องทางออนไลน์ ควรติดต่อผ่านแอปพลิเคชันที่ได้ตรวจสอบแล้วว่าเป็นแอปพลิเคชันจริง หรือไปที่เว็บไซต์ของเขาและต้องเป็นเว็บไซต์จริง วิธีการสังเกตคือเป็นเว็บที่ลงท้ายด้วยคอตไทย (.th) ที่เขาคือไทยแลนด์เป็นเว็บไซต์ที่จดทะเบียนในประเทศไทย อันนี้มีการตรวจสอบยืนยันตัวตนอย่างถูกต้องและเชื่อถือได้ ดังนั้น ขอให้ประชาชนดูที่แอปพลิเคชันที่คุ้นเคยและใช้งานอยู่เป็นประจำ ตรวจสอบอย่างถี่ถ้วนแล้วเพื่อความปลอดภัยในการใช้งานและไม่ถูกหลอกให้สูญเงินด้วย” นายชัยวุฒิกล่าว

ผู้สื่อข่าวรายงานว่าเพิ่มเติมว่า 203 แอปพลิเคชันที่กระทรวงดีเอสไอประกาศเตือนมีดังนี้ 4K Pro Camera, 4K Wallpapers Auto Changer, Advanced SMS, aipic-Magic Photo Editor, All Good PDF Scanner, All Language Translate, All Photo Translator, Art Filters, Astro + Horoscope & Astrology, Astroline: The Daily Horoscope, Auto Sticker Maker Studio, Avatar Maker Character Creator, Baby Sticker-Track Milestones, Bass Booster Volume Power Amp, Battery Charging Animations Battery Wallpaper, Battery Charging Animations Bubble-Effects, Beat.ly Music Video Maker, Beat maker pro, Beauty Filter, Blood Pressure Checker, Blood Pressure Diary, Blue Scanner, Blur Image

Caller Theme, Call Me Phone Themes Call Skins, Camera Translator, Care

Message, Cartoons Me, Cashe Cleaner, Chat Online, Chat SMS, Chat Text SMS, Classic Emoji Keyboard, Classic Game Messenger, Coco camera vll, Come Messages, Contact Background, Cool Keyboard, Cool Messages, Creative 3D Launcher, Creative Emoji Keyboard, Custom Themed Keyboard, Cut, Paste, Dazz Cam-D3D Photo Effect, Dazzle-Instastories editor, Dazzling Keyboard, Design Maker, Desire Translate, Direct Messenger, Dizzi, DJ it!, Drink Water, Drums: Play Beats & Drum Games, Easy PDF Scanner, edjing Mix, edjing Pro, EmojiOne Keyboard, Emoji Theme Keyboard, Equalizer+ HD music player, Equalizer Fx: Bass Booster App

Facelab, FaceMe, Facetory: Face Yoga & Exercise, Fancy Charging, Fancy SMS, Flashlight Flash Alert On Call, FLMX, Fonts Emoji Keyboard, Frame, Frames, Freeglow Camera 1.0.0, Funny Caller, Funny Camera, Funny Emoji Message, Funny Keyboard, Funny Wallpapers-Live Scree, Gif Emoji Keyboard, Girl Games: Unicorn Slime, Guitar Play-Games & Songs, Guitar-real games & lessons, Guitar Tuner-Ukulele & Bass, Halloween Coloring, Handset-Second Phone Number, Heart Emoji Stickers, Highlight Story Cover Maker!, Hi Text SMS, Horoscope 2019 and Palm Reader, Hub-Story Templates Maker, Hummingbird PDF Converter-Photo to PDF, Hyper Cleaner: Clean Phone, iCons-Icon Changer App+, iMessenger, Impresso, Instant Messenger, iWidget Pro, Jambl: DJ Band & Beat Maker, Jigsaw Puzzle, Karaoke Songs

Life Palmistry, Lift: Story Maker, Light Messages, Live Wallpaper Maker: 4K Theme, Loop Maker Pro, Lucky Life, MagicFX-Magic Video Effects, Magic Photo Editor, Memoristo: Brain Test, IQ Game, Memory Silent Camera, Menu Maker!, Meticulous Scanner, Metronome Pro-Beat & Tempo, Metronome-Tap Tempo & Rhythm, Mini PDF Scanner, Mint Leaf Message-Your Private Message, Mood Balance: Self Care Tracker, Music Zen-

Relaxing Sounds, MyCall-Call Personalization, Nebula: Horoscope & Astrology, Neon Theme Keyboard, NewScreen: 4D Wallpapers, Notes-reminders and lists, Now QRcode Scan, One Sentence Translator-Multifunctional Translator, Painting Photo Editor, Paper Doc Scanner, Part

☆ มีต่อหน้า 7

กระทรวงดิจิทัล ☆ ต่อจากหน้า 6

Message, Password Manager, Path-Horoscope & Astrology, PDFScanner: Document Scan, Personal Message, Photo Collage, Photo Editor & Background Eraser, Photo Editor-Filters Effects, Photo & Exif Editor, Photo Filters & Effects, Photoly Remove Object & Editor, Photo To Sketch, Piano Crush, Piano, Pista, Pixomatic, Poco Launcher, Premium SMS, Presets for Lightroom, Private Game Messages, Private Messenger, Private SMS, Professional Messenger, Quick Talk Message

Razer Keyboard & Theme, RECOLLECT, Retouch & Cutout, Rich Theme Message, Ringtones HD, ScanGuru, Scanner App, Send SMS, Simple Note Scanner, SlidePic, Slimy, Smart Messages, Smart SMS Messages, Smart TV remote, Smile Emoji, Social Message, SpeedPro Slow speed video edit, Stickerfy: Sticker Maker, Sticker Maker, Stickers & GIF, Stock Wallpapers & Backgrounds, Style Message, Style Photo Collage, Super Hero-Effect, Sweet Pics-Baby Photo Edit, Talent Photo Editor-Blur focus, Tangram App Lock, TeasEar: ASMR Slime Antistress, Text Emoji SMS, Text SMS, Themes Chat Messenger, Themes Photo Keyboard, Timestamp Camera, ToonApp Cartoon Photo Editor, Translate Camera-Speak On, Translator Guru: Voice & Text

UltraFX-Effect Video Maker, Unicc QR Scanner, Unique Keyboard, Universal PDF Scanner, Vanilla Snap Camera, Video Puzzles-Magic Puzzle, Ringtones HD* Ringtone Maker, VOCHI Video Effects Editor, Volume Booster Hearing Aid, Volume Booster Louder Sound Equalizer, Water Reminder, WeDrum: Drums, Real Drum Games, Widget PLUS+ Photo & Weather, Wow Beauty Camera, Wow Translator, Yoga-For Beginner to Advanced, YouToon-AI Cartoon Effect

จากการที่นายอนุชา บูรพชัยศรี รองเลขาธิการนายกรัฐมนตรีปฏิบัติหน้าที่โฆษกประจำสำนักนายกรัฐมนตรีกล่าวว่า นายกกฯกำชับให้ทุกหน่วยงานที่เกี่ยวข้องบูรณาการความร่วมมือปราบปรามอาชญากรรมออนไลน์อย่างจริงจังเด็ดขาด

ที่ผ่านมา การทำงานร่วมกันของหน่วยงานที่เกี่ยวข้องปราบปรามการลักลอบใช้อินเตอร์เน็ตข้ามประเทศผิดกฎหมาย แก้ปัญหาขโมยบัตรและบัญชีม้า โดยกระทรวงดิจิทัลฯ ปปง. และ กสทช.

การลักลอบใช้อินเตอร์เน็ตข้ามประเทศผิดกฎหมายกสทช.ได้กำชับผู้ให้บริการโทร



คมนาคมเข้าตรวจสอบการใช้บริการอินเทอร์เน็ตข้ามประเทศตรวจสอบบริเวณที่กระทำความผิด รวมถึงตัวผู้กระทำความผิด

การแก้ปัญหาขโมยบัตรและบัญชีม้าให้ผู้ให้บริการโทรคมนาคมแจ้งเจ้าของซิมโทรศัพท์ที่มายืนยันตัวตนให้ถูกต้อง

และแก้ปัญหาบัญชีม้าและบัญชีต้องสงสัยนำไปใช้กระทำความผิดกฎหมาย สำนักงาน ปปง.

ได้จัดทำประกาศหลักเกณฑ์พิจารณา กำหนดหรือทบทวนรายชื่อบุคคลที่มีความเสี่ยงสูง และแจ้งรายชื่อผู้กระทำความผิดให้สถาบันการเงิน

นอกจากนี้ดีอีเอสอยู่ระหว่างเสนอร่าง พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีต่อครม.เพื่อเร่งแก้ปัญหาอาชญากรรมออนไลน์ให้เป็นรูปธรรม

วันนี้ภัยด้านเทคโนโลยีกำลังเป็นปัญหาใหญ่ การส่งสัญญาณให้หน่วยงานต่างๆร่วมมือถือเป็นเรื่องดี

และควรมีมาตรการเชิงรุกเร่งปรับแก้กฎหมายให้เท่าทันปัญหา.

CYBERCRIME

Phone users warned over malicious apps

POST REPORTERS

The Ministry of Digital Economy and Society (DES) has urged iOS and Android phone users to look out for some 200 malicious applications and delete them from their devices if found.

DES Minister Chaiwut Thanakamanusorn said the ministry and the National Cyber Security Agency (NCSA) have found more than 200 apps infected with malware and published them on their Facebook page at <https://www.facebook.com/prmdes.official>.

These malicious apps include Chat Text SMS, Classic Game Messenger, Care Message, Cartoons Me, Creative Emoji Keyboard, Flashlight Flash Alert On Call, Password Manager and YouToon-All Cartoon Effect.

Anyone who has these apps installed on their devices is urged to delete them immediately as well as update their software to ensure that security is up to date, Mr Chaiwut said, adding that the ministry has already asked Google and Apple to remove these apps from app stores.

"The public is being asked to look out for malicious apps. If they are downloaded, hackers can steal your personal data or take control of your phones," he said.

Mr Chaiwut also warned about phishing, where scammers send a text message

that appears to be from well-known establishments, including banks, asking the phone user to click on a link or enter personal data such as passwords.

NCSA Thailand is gathering information about companies that send out fake texts and will ask the National Broadcasting and Telecommunications Commission (NBTC) and mobile phone operators to block these text messages, he said.

The DES minister said scammers also use the Line chat application while disguised as legitimate companies to steal personal information. He asked the public to double-check when contacting businesses or state agencies via Line.

Chayawadee Chai-Anant, Bank of Thailand's assistant governor, said the central bank had instructed commercial banks to improve security for mobile banking security services.

One measure for cyber safety is that a mobile banking app or an e-wallet must only be used on one device to reduce risks, she said.

Ms Chayawadee said phone users need to be aware that banks will not include a link in their text messages or emails asking users to enter personal information. She said the central bank is also working with agencies concerned to raise public awareness about fraudulent activities and to prevent the use of mule accounts.

15 “เอ็นที” เร่งเกม
ปรับองค์กร

ลดคน-ปั้นธุรกิจใหม่
หนีเส้นตายปี'68

“เอ็นที”
เร่งเกมปรับองค์กร

15 ลดคน-ปั้นธุรกิจใหม่
หนีเส้นตายปี'68

‘เอ็นที’ เร่งเกมปรับองค์กร ลดคน-ปั้นธุรกิจใหม่หนีเส้นตายปี'68

“ที” โอที และแคท” ควบรวม
เป็นหนึ่งในเดียวกัน ภายใต้
บริษัท ไทคอมเนคแห่งชาติ
หรือ “เอ็นที” ตั้งแต่ 7 ม.ค. 2564 ที่ผ่านมา
แม้จะไม่ได้เป็นดิลที่โด่งดัง และเป็น
ที่จับตาเท่ากรณี “ทรู-ดีแทค” แต่เส้นทาง
กว่าจะรวมกันได้ก็ผ่านมาแล้วไม่รู้ว่ารัฐบาล
มาสำเร็จจบกันได้ที่รัฐบาลนี้

อย่างไรก็ตาม การควบรวมเป็นแค่
สเต็ปแรก ยังมีงานยากรออยู่อีกไม่น้อย
ทั้งการปรับโครงสร้างองค์กร และ
กระบวนการทำงานภายใน ก็ไม่ใช่ว่า
ปรับครั้งเดียวแล้วจบเลย

เดินหน้าปรับองค์กรต่อเนื่อง

ในโอกาสครบรอบ 2 ปี พันเอก
สรรพชัย หุวะนันทน์ กรรมการ
ผู้จัดการใหญ่ บริษัท ไทคอมเนคแห่งชาติ
จำกัด (มหาชน) หรือ NT ยอมรับว่าแม้จะมี
การปรับโครงสร้างองค์กรล่าสุดไปเมื่อ ต.ค.
ปีที่แล้ว ลดความซ้ำซ้อน และลดค่าใช้จ่ายใน
การบริหารงานลงได้ระดับหนึ่ง แต่ก็ยัง
จะมีแผนการปรับโครงสร้างครั้งใหญ่
อีกรอบในปีหน้า เพื่อเพิ่มประสิทธิภาพใน



พันเอก สรรพชัย หุวะนันทน์

ประชาชาติ ธุรกิจ

Prachachat Turakij
Circulation: 120,000
Ad Rate: 1,350

Section: การตลาด/ไอซีที

วันที่: จันทร์ 23 - พุธ 25 มกราคม 2566

ปีที่: 45

ฉบับที่: 5534

หน้า: 1 (ขวา), 13, 15

Col.Inch: 117.43

Ad Value: 158,530.50

PRValue (x3): 475,591.50

คลิป: สีสี่

หัวข้อข่าว: 'เอ็นที' เร่งเกมรับรององค์กร ลดคน-ปั้นธุรกิจใหม่หนีเส้นตายปี'68

การทำงาน และลดต้นทุนลงต่อเนื่องให้ได้มากกว่านี้อีก 10-15% รวมถึงมุ่งหน้าไปสู่ธุรกิจดิจิทัลแบบใหม่ เพื่อสร้างรายได้ทดแทนธุรกิจดั้งเดิม ทั้งการบริหารทรัพยากรไตรมาสแรก ทั้งคลื่นความถี่ และโครงสร้างพื้นฐานที่จะหายไปในอนาคต กับเป้าหมายในการรับรององค์กรจากผู้ให้บริการโทรคมนาคมสู่ Tech Company ภายใต้แนวคิด Neutral Operator เพิ่มมูลค่าธุรกิจโครงสร้างพื้นฐาน

“เราเป็นองค์กรขนาดใหญ่จึงต้องควบคุมต้นทุนการดำเนินงานอย่างจริงจัง เพื่อลดรายจ่ายในองค์กรให้ได้ต่อเนื่อง เน้นการจัดการเพื่อลดต้นทุนโครงข่าย และระบบเครือข่ายการสื่อสารที่ซับซ้อน ร่วมกับการเร่งกระบวนการจัดการภายในทั้งระบบ IT และข้อมูลภายในที่มีจำนวนมาก เพื่อบูรณาการฐานข้อมูลเป็นหนึ่งเดียว ส่วนด้านบุคลากร ได้มีโครงการเกษียณก่อนอายุ เพื่อลดค่าใช้จ่ายด้านบุคลากรต่อเนื่อง”

แจงผลประกอบการปี'65

สำหรับผลประกอบการ 11 เดือน/2565 มีรายได้รวม 84,013 ล้านบาท ค่าใช้จ่าย 82,369 ล้านบาท กำไรสุทธิ 1,644 ล้านบาท และประมาณการสิ้นปี 2565 มีรายได้รวม 91,528 ล้านบาท ค่าใช้จ่ายรวม 90,209 ล้านบาท กำไรสุทธิ 1,319 ล้านบาท โดยมีรายได้จาก 5 กลุ่มธุรกิจ ได้แก่ ธุรกิจ mobile 50,820 ล้านบาท หรือ 55% ของรายได้, ธุรกิจ fixed line & broadband และ satellite รวม 19,930 ล้านบาท หรือ 22% ของรายได้, ธุรกิจโครงสร้างพื้นฐานและเสาโทรคมนาคม 9,486 ล้านบาท หรือ 10% ของรายได้, ธุรกิจ international 2,178 ล้านบาท หรือ 3% ของรายได้, ธุรกิจ digital และ IDC & Cloud รวม 3,902 ล้านบาท หรือ 4% ของรายได้ และรายได้อื่น ๆ

5,212 ล้านบาท หรือ 6%

“ส่วนหนึ่งที่ยังทำได้ ทั้งที่วางแผนประจำปีแบบขาดทุนไว้ ก็เพราะโครงการเกษียณก่อนอายุ (early retirement) เดิมตั้งเป้าไว้ 1,800 คน แต่ทำมา 600 คน จึงนำค่าใช้จ่ายส่วนนี้คอนเวิร์ตกลับมาจนเป็นกำไร”

ทำไมต้องเป็นปี 2568

“สรรพชัย” กล่าวว่า รายได้ที่เอ็นทีเคยได้จากสัญญาของเอไอเอส ในคลื่น 2100 Mhz ของทรูในคลื่น 2300 MHz และดีแทค 850 Mhz จะหายไปในปี 2568 รวมแล้วกว่า 60,000 ล้านบาท ซึ่งมีสัดส่วนมากกว่า 50% ของรายได้รวมในปัจจุบัน รวมถึงรายได้อื่น ๆ ที่เกิดจากพันธมิตรก็จะลดลงตาม ทำให้ธุรกิจโครงสร้างพื้นฐานด้านโทรคมนาคมอยู่ในขาหล่ง หรือเรียกได้ว่าเป็น “sunset” จึงจะต้องเร่งบริหารจัดการ เพื่อหารายได้ส่วนอื่นมาทดแทน

แบ่งเป็น **1.เร่งสร้างรายได้กลุ่มดิจิทัลใหม่ ๆ** โดยร่วมมือกับพันธมิตรทางธุรกิจเพื่อสร้างรายได้ เช่น 5G แพลตฟอร์ม, คลาวด์ หรือบริการดิจิทัลต่าง ๆ และ **2.ปรับลดคนต้องเป็นไปตามแผนให้เหลือ 9,000 คน** (ปัจจุบัน 1.4 หมื่นคน) เพื่อลดการทำงานซ้ำซ้อน และทำให้รายได้เฉลี่ยต่อพนักงานสูงขึ้น

“การพัฒนาธุรกิจใหม่ ๆ ไม่น่ากังวล แต่ความเสี่ยงเดียวของเราจนถึงปี 2568 คือการลดจำนวนคนไม่เข้าเป้า ซึ่งเป็นเรื่องยากที่จะบอกให้พนักงานลาออกไป ผมก็คงทำได้แค่บอกเขาว่า นี่เป็นความจำเป็น และเป็นการทำเพื่อองค์กร”

อัปเดตคลื่น 700 MHz-26 GHz

การสร้างธุรกิจดาวรุ่งที่จะเห็นในปีนี้ คือ บริการ 5G โดยจะเสนอ ครม. ในไตรมาส 1/2566 นี้ ก่อนให้บริการลูกค้าได้จริงในปลายไตรมาส 2 หรือ 3/2566

เพื่อพัฒนาคลื่นความถี่ 700 MHz และ 26 GHz

“คลื่น 700 MHz เป็นการลงทุนติดตั้งโครงข่าย 4G ใช้ทดแทนคลื่น 850 MHz เพื่อดูแลลูกค้าที่มีในระบบเดิมกว่า 2 ล้านเลขหมาย และอาจเพิ่มเป็น 4 ล้านเลขหมายในแง่ธุรกิจมือถือ เราแทบจะแข่งขันกับเอกชนไม่ได้เลย เราจึงจะไปโฟกัสที่อุปกรณ์ IOT ที่กำลังเติบโตอย่างมาก ทั้งในภาคครัวเรือน และอุตสาหกรรม ทำให้รองรับการใช้งานในพื้นที่ห่างไกล ทั้งยังเชื่อมต่อกับคลื่นความถี่ 26 GHz ที่ใช้ในการพัฒนา 5G สำหรับพื้นที่เฉพาะ โดยเสริมด้วยสายใยแก้วนำแสงที่เชื่อมโยงครอบคลุมพื้นที่ทั่วประเทศ”

อีกบริการที่คาดว่าจะมีความต้องการเพิ่มขึ้นคือ โครงการเคเบิลใต้น้ำเส้นใหม่ ASIA DIRECT CABLE ที่จะเปิดใช้ในปี

“กรณีสายเคเบิลใต้น้ำ บริษัทต่างชาติให้ความสนใจ เพราะช่วงนี้เขามาลงทุนมาก โดยเฉพาะ data center ทั้งแอมะซอนหรือหัวเว่ย ที่ต้องการเช่าใช้สายเคเบิล แต่เมื่อเวลาผ่านไป บริษัทต่างชาติเหล่านี้จะมีอำนาจต่อรองมากขึ้น เพราะมีฐานลูกค้า และในที่สุดก็จะลงทุนทำเอง เราจึงต้องมองเผื่ออนาคตไว้ด้วย”

สปินออฟธุรกิจ-ต่อยอดของเดิม

และในปีนี้จะมีความร่วมมือกับเอกชนหลายรูปแบบ รวมถึงแยก (spin off) ธุรกิจกลุ่มบริการดิจิทัลออกมาตั้งเป็นบริษัท 1-2 บริษัท ด้าน Cloud และ IT security รวมถึงลงทุนหรือมีส่วนร่วมในธุรกิจใหม่ ๆ ที่มีโอกาสเติบโต เช่น smart city, data management service, environment, health care, EV, gaming, big data รวมถึงเทรนด์เทคโนโลยีอย่าง AI AR/VR robotic/automation และ green energy เพื่อให้ดำเนินธุรกิจที่แข่งขันได้

ประชาชาติ ธุรกิจ

Prachachat Turakij
Circulation: 120,000
Ad Rate: 1,350

Section: การตลาด/ไอซีที

วันที่: จันทร์ 23 - พุธ 25 มกราคม 2566

ปีที่: 45

ฉบับที่: 5534

หน้า: 1(ขวา), 13, 15

Col.Inch: 117.43 Ad Value: 158,530.50

PRValue (x3): 475,591.50

คลิ๊ป: สีสี่

หัวข้อข่าว: 'เอ็นที' เร่งเกมปรับปรุงโครง ลดคน-ปั้นธุรกิจใหม่หนีเส้นตายปี'68

และสร้างผลกำไรมากกว่าโครงสร้างพื้นฐานแบบเดิม

อย่างไรก็ตาม จุดแข็งของเอ็นทีปัจจุบันคือ โครงสร้างพื้นฐาน และทรัพย์สินเดิมที่มี จึงต้องมุ่งต่อยอดและสร้างโอกาสใหม่ ๆ เช่น รักษารายได้จากการให้เช่าพื้นที่เสาโทรคมนาคมกว่า 30,000 ต้น และยุบรวมเสาในบริเวณเดียวกัน เพื่อลดต้นทุนในการให้บริการ รวมถึงขยายเพิ่มพื้นที่เฉพาะ เช่น อุทยาน, ป่าไม้ เป็นต้น ส่วนท่อร้อยสายใต้ดิน มีแผนร่วมกับการไฟฟ้าตามนโยบาย กสทช. พร้อมกับมีแนวทางพัฒนาบทบาทเป็น neutral operator และ neutral last mile provider เพื่อให้ผู้ใช้บริการใช้โครงสร้างร่วมกันได้ทั้งเสาโทรคมนาคม และสายสื่อสาร core fiber โดยไม่ต้องลงทุนเพิ่ม เช่น บริการบรอดแบนด์ ผู้ให้บริการไม่ต้องลงทุนสายทั้งหมด แต่ใช้โครงข่ายกลาง และลากเฉพาะสาย last mile เข้าสู่บ้าน เพื่อให้บริการลูกค้าได้

ย้ายบทบาทรัฐวิสาหกิจ

นอกจากต้องปรับตัวเพื่อแข่งขัน และหารายได้เลี้ยงองค์กรแล้ว ชัดเจนว่าอีกภารกิจสำคัญของ “เอ็นที” คือการดำเนินงานตามนโยบายของรัฐบาล ล่าสุดกับการเข้าร่วมประมูลสิทธิในการเข้าใช้วงโคจรดาวเทียม และได้รับสิทธิ 1 วงโคจรชุดที่ 4 (126E) ให้บริการครอบคลุมภูมิภาคเอเชีย-แปซิฟิก และทะเลจีนใต้ ที่ราคา 9.076 ล้านบาท ทั้งคงสิทธิความจุ 400 Mbps

และสิทธิในการบริหารจัดการช่องสัญญาณดาวเทียมในวงโคจร 119.5E ของภาครัฐไว้ด้วย

สำหรับวงโคจร 126E ที่ประมูลได้ จะทำให้ NT เพิ่มศักยภาพธุรกิจบริการดาวเทียมได้เต็มรูปแบบทั้งทางเทคโนโลยีและบุคลากร เป็นการส่งเสริมกิจการอวกาศ และรักษาวงโคจรของประเทศสอดคล้องกับการปรับโครงสร้างองค์กรล่าสุดที่มีเพิ่มการจัดตั้งสายงานดาวเทียมและโครงข่าย เพื่อดำเนินภารกิจด้านดาวเทียม ทั้งบริหารจัดการ และการสนับสนุนการขาย บริการสื่อสารผ่านดาวเทียม เกตเวย์ และสถานีภาคพื้นดินรองรับการก้าวสู่ธุรกิจดาวเทียมวงโคจรระดับต่ำ low earth orbit (LEO) และดาวเทียมวงโคจรค้างฟ้า (GEO)

“วงโคจรที่ กสทช. นำมาใช้ในการประมูล เป็นวงโคจรเชิงพาณิชย์ ส่วนการใช้งานด้านความมั่นคง เอ็นที จะประสานกับ กสทช. ให้ได้มา ซึ่งวงโคจรสำหรับวัตถุประสงค์ดังกล่าว โดยบริษัทตระหนักดีถึงความสำคัญของการพัฒนากิจการดาวเทียมสื่อสารของประเทศ และพิจารณาความเป็นไปได้ทางธุรกิจ และความคุ้มค่าในการลงทุนประกอบกัน เพื่อให้เกิดประโยชน์สูงสุดในภาพรวมของประเทศในหลากหลายมิติ ทั้งด้านการพัฒนาเทคโนโลยีและการสื่อสาร สาธารณสุข การพัฒนาเชิงเศรษฐกิจ และสังคม”