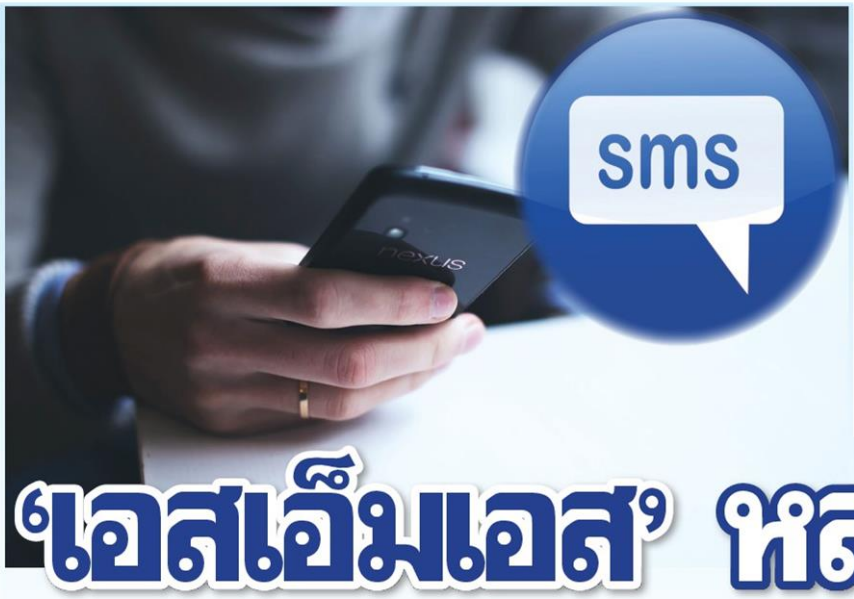
เดลินิวส์
Daily News
Circulation: 500,000
Ad Rate: 2,100

Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: - **ฉบับที่:** 26288 **หน้า:** 7(บน)
Col.Inch: 73.74 **Ad Value:** 154,854 **PRValue (x3):** 464,562 **คลิป:** สี่สี
หัวข้อข่าว: 'เอสเอ็มเอส' หลอกลวง ภัยใกล้ตัวถ้าไม่โลภก็รอด!



'เอสเอ็มเอส' หลอกลวง ภัยใกล้ตัวถ้าไม่โลภก็รอด!

กลายเป็นปัญหากวนใจของผู้ใช้โทรศัพท์มือถือหรือสมาร์ทโฟนกันแทบทุกคนที่ช่วงนี้โดนข้อความสั้นหรือเอสเอ็มเอส หลอกลวง กระหน่ำส่งเข้ามายังมือถือไม่เว้นวัน!!

นอกจากจะ **"กวนใจ"** แล้ว สำหรับคนที่ไม่รู้เท่าทันหลงไปกดหรือคลิกเข้าไปดู แล้วกรอกข้อมูลตามคำเชิญชวนหว่านล้อมต่าง ๆ บ้างก็ว่า คุณเป็นผู้โชคดีถูกรางวัลได้รับเงิน, คุณได้รับเงินกู้ดอกเบี้ยต่ำ หรือคุณมีเงินเข้าบัญชีจำนวนเท่านั้นเท่านี้ ฯลฯ อาจมีปัญหาปวดหัวตามมาเพราะอาจถูกแฮก หรือขโมยข้อมูล ทำให้สูญเสียทรัพย์สินเงินในบัญชีได้ **โดยเฉพาะชาวบ้าน "ตาสีตาสา" ที่อาจไม่ได้ติดตามข่าวสารในเรื่องนี้ที่เกิดขึ้น เรียกว่าอุตส่าห์ "เก็บหอมรอมริบ" มาทั้งชีวิตอาจหมดตัวได้ง่าย ๆ**

เอสเอ็มเอสหลอกลวงเหล่านี้ ส่วนใหญ่เป็นมิจฉาชีพที่ส่งมาหลอกลวงล้วงข้อมูลแล้วไปสวมรอยเพื่อนำไปทำธุรกรรมออนไลน์ และเป็นเว็บพนันออนไลน์ที่ส่งลิงก์เชิญชวนให้เป็นลูกค้า หรือเป็นลิงก์แอพเงินกู้ออนไลน์ เรียกดอกเบี้ยโหดถือว่าผิดกฎหมาย ฯลฯ

เสียงบ่นถึงปัญหาเหล่านี้ของ "ประชาชน" ในสังคมดังขึ้นเรื่อย ๆ หน่วยงานรัฐไม่ทำอะไรที่ช่วยคุ้มครองประชาชนเลยหรือ??

สำนักงานคณะกรรมการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (สำนักงานฯกสทช.) ในฐานะที่เป็นหน่วยงานกำกับดูแล ต้องออกมาสั่งกำชับให้ **"ค่ายมือถือ"** เร่งแก้ไขปัญหาเรื่องนี้โดยให้ตรวจสอบและทำการบล็อกเอสเอ็มเอสหลอกลวงเหล่านี้ และให้ประสานแชร์ข้อมูลระหว่างกันเพื่อแบล็กลิสต์ หรือขึ้นบัญชีดำให้ทุกค่ายบล็อกเอสเอ็มเอสจากผู้ส่งรายเดียวกัน

นอกจากนี้ทาง กสทช. จะนำข้อมูลเกี่ยวกับเอสเอ็มเอสหลอกลวงไปเผยแพร่บนเว็บไซต์ของสำนักงาน กสทช. (www.nbtc.go.th) เพื่อให้ประชาชนสามารถตรวจสอบชื่อผู้ส่งข้อความที่น่าสงสัย เพื่อเป็นการป้องกันไม่ให้ตกเป็นเหยื่อได้

อย่างไรก็ตามปัญหาเอสเอ็มเอสหลอกลวงเหล่านี้ส่วนใหญ่จะถูกส่งจาก **ผู้ให้บริการด้านเนื้อหา** ที่ได้ซื้อบริการส่งเอสเอ็มเอสจากโอปเรเตอร์หรือผู้ให้บริการมือถือและบางครั้งผู้ให้บริการเนื้อหา ก็นำไปขายต่อกับบริษัทหรือธุรกิจทำให้การตรวจสอบได้ยากว่านำไปส่งข้อความเกี่ยวกับอะไร

กสทช.ได้ออกมาคาดโทษกับผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมที่ให้บริการขายต่อเอสเอ็มเอส และผู้ให้บริการด้านเนื้อหา หากทางสำนักงาน กสทช. ได้รับแจ้งว่าบริษัทใดเป็นผู้ส่งเอสเอ็มเอสที่มีลักษณะเนื้อหาเป็นการหลอกลวงจะตรวจสอบและพิจารณาลงโทษทางปกครอง ตั้งแต่เตือน ปรับ พักใช้ใบอนุญาต และโทษสูงสุด คือเพิกถอนใบอนุญาตประกอบกิจการและจะดำเนินคดีตามกฎหมายควบคู่ไปด้วย

การออกมา **"เขียนเสือให้วัวกลัว"** ก็ได้ผลระดับหนึ่งเมื่อทางค่ายมือถือออกมาประสานเสียงพร้อมดำเนินการตาม กสทช. และพร้อมร่วมมือกับทุกฝ่ายที่เกี่ยวข้อง พร้อมทั้งมีการแลกเปลี่ยนข้อมูลเอสเอ็มเอสกันเพื่อทำการบล็อก โดย "ค่ายทรู" ได้เปิด **ศูนย์เฉพาะกิจรับแจ้งปัญหาเอสเอ็มเอส ที่มีข้อความไม่เหมาะสมผ่านหมายเลขพิเศษ โทร. 0-2700-8085** เพื่อตรวจสอบและดำเนินการปิดกั้น พร้อมแจ้งเตือนบริษัทคู่สัญญา ที่ใช้บริการส่งเอสเอ็มเอส หากตรวจพบมีการส่งข้อความที่ไม่เหมาะสมจะดำเนินการทาง

เดลินิวส์
Daily News
Circulation: 500,000
Ad Rate: 2,100

Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: - ฉบับที่: 26288 หน้า: 7(บน)
Col.Inch: 73.74 Ad Value: 154,854 PRValue (x3): 464,562 คลิป: สี่สี
หัวข้อข่าว: 'เอสเอ็มเอส' หลอกลวง ภัยใกล้ตัวถ้าไม่โลภก็รอด!

กฎหมายทันที

ด้าน **"ดีแทค"** พร้อมยกระดับมาตรการการจัดการกับสแปม และเอสเอ็มเอส หลอกลวง พร้อมทั้งให้ความรู้กับสังคมและประชาชนเกี่ยวกับภัยออนไลน์ที่มาในรูปแบบต่าง ๆ ผ่าน **dtac Safe Internet** ซึ่งเป็นโครงการที่มุ่งสร้างเสริมทักษะการรับมือภัยเสี่ยงบนโลกออนไลน์

ขณะที่ **"ค่ายเอไอเอส"** ยืนยันว่าจะทำการคัดกรองผู้ประกอบการที่ซื้อบริการแพ็กเกจเอสเอ็มเอสอย่างเข้มงวด หากพบว่ามีการส่งเอสเอ็มเอสที่สร้างการรบกวน หรือหลอกลวง จะทำการบล็อก และขึ้นทะเบียนต้องห้าม หรือแบล็กลิสต์ ผู้ประกอบการรายดังกล่าวทันที!! พร้อมสื่อสารให้ข้อมูลกับประชาชน เพื่อให้รู้เท่าทันกลุ่มมิจฉาชีพด้วยเช่นกัน โดยลูกค้าที่ได้รับเอสเอ็มเอสเหล่านี้สามารถแจ้งเข้ามาได้ที่ **AIS Call Center หรือ กด *137 โทรฯ ออกฟรี เพื่อบล็อก การได้รับเอสเอ็มเอสทันที** หรือหากมีโทรศัพท์ที่โทรฯ เข้ามาสร้างความรำคาญใจ หรือก่อให้เกิดความเสี่ยงก็สามารถโทรฯ แจ้งที่ AIS Call Center เพื่อรับคำแนะนำในการบล็อกการรับสายได้ด้วยตนเอง

อย่างไรก็ตามขึ้นชื่อว่า "มิจฉาชีพ" ยังไงก็ต้องหาวิธีหลอกลวงเหยื่อให้ได้ แม้ช่องทางการส่งเอสเอ็มเอสจะไม่สะดวกเหมือนก่อนก็ได้เปลี่ยนวิธีมาใช้โทรศัพท์ตรงเข้าหาเหยื่อเพื่อหลอกลวง อ้างว่าโทรฯ มาจากหน่วยงานภาครัฐบอกเจ้าของเลขหมายว่าได้รับความช่วยเหลือจากรัฐบาลเป็นเงิน 2,000 บาท หรือมีสิทธิได้รับเงินกู้ 200,000 บาทบ้างแล้วหลอกถามข้อมูลส่วนตัว

จึงเป็นสิ่งที่ต้องระวังเช่นกันซึ่งทางสำนักงาน กสทช.ได้ขอความร่วมมือจากประชาชนให้โทรฯ แจ้ง **ร้องเรียนที่คอลเซ็นเตอร์ โทรศัพท์ 1200 (โทรฯ ฟรีไม่มีค่าใช้จ่าย) หรือโทรฯ แจ้งคอลเซ็นเตอร์ของมือถือที่ใช้อยู่** หากมีหลักฐานเป็นคลิปเสียงของมิจฉาชีพที่โทรฯ เข้ามาหลอกลวงก็ยิ่งดี เพราะสามารถตรวจสอบได้ว่าเบอร์ที่โทรฯ เข้ามาใครเป็นผู้ลงทะเบียนเป็นเจ้าของเบอร์ เพื่อประสานงานกับตำรวจให้ดำเนินคดีกับมิจฉาชีพเหล่านี้

สุดท้ายแล้ว!! เกราะป้องกันตัวเองที่ดีที่สุด คือต้องตั้งสติ อย่าโลภ ไม่คลิกลิงก์ในข้อความน่าสงสัยและกรอกข้อมูลส่วนตัว ให้กับผู้ส่งที่ไม่รู้จักเพื่อจะได้ไม่เป็นเหยื่อ!!.

จิราวัฒน์ จารุพันธ์

มติชน
Matichon
Circulation: 950,000
Ad Rate: 1,100

Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: 44 ฉบับที่: 15911 หน้า: 9(ล่าง)
Col.Inch: 67.92 Ad Value: 74,712 PRValue (x3): 224,136 คลิป: ขาว-ดำ
คอลัมน์: คิดเห็นShare: แนวนโยบายแห่งรัฐ ต่อการหยุดยั้งภัยพิบัติไซเบอร์ยุค 5G การใช้เล่ห์...

แนวนโยบายแห่งรัฐ ต่อการหยุดยั้งภัยพิบัติไซเบอร์ยุค5G การใช้เล่ห์หลอกลวงดิจิทัล

หัวหน้าฝ่ายรัฐกิจและธุรกิจสัมพันธ์ บริษัทอิริคสันประเทศไทย

ท่ามกลางภัยพิบัติโควิดสร้างความยากลำบากหนักหนาสาหัสกับประชาชนอยู่มากโข

ชีวิตที่ไม่ได้ติดออนไลน์มากมาย ก็ถูกบังคับให้เข้าสู่ยุคดิจิทัลทั้งๆ ที่ไม่พร้อม ถ้าไม่มีสมาร์โฟนก็ยากมากที่จะเข้าถึง ต้องขวนขวายหามาใช้ทั้งที่รู้เรื่องบ้างไม่รู้เรื่องบ้างเพื่อจะได้รับการศึกษาออนไลน์, การขอรับความช่วยเหลือจากภาครัฐ ไม่ว่าจะเป็นโครงการคนละครึ่ง โครงการเราชนะ รวมถึงการจองฉีดวัคซีนในระยะแรกที่ต้องจองผ่านแอพพลิเคชั่นต่างๆ และด้วยไม่มีความชำนาญ และรอบรู้ ย่อมง่ายต่อการเป็นเป้าหมายในการถูกหลอกลวงผ่านช่องทางออนไลน์ ของกระบวนการพนันออนไลน์ การกู้ยืมเงินออนไลน์ การทำแชร์ลูกโซ่ หรืออะไรอีกมากมายที่จะเกิดขึ้นอีก

การพลาดพลั้งเสียท่าให้กับมิจฉาชีพเหล่านี้ ก็ไม่ใช่ความผิดของเขาเหล่านี้ที่รู้ไม่ทัน ไม่ใช่เหตุที่จะถูกถากถางว่าทำไมไม่ระวัง ทำไมไม่ติดตามข่าว

การใช้เครื่องมือทันสมัยในการหลอกลวง ไม่ได้มีเพียง SMS หรือ Call center เท่านั้น ยังปรากฏว่ามีการสื่อโซเชียลต่างๆ เช่น Line, TikTok, Facebook และอื่นๆ การป้องกันโดยการปิดกั้นก็ยากที่จะทำได้สมบูรณ์ เพราะเหล่ามิจฉาชีพจะสามารถเปิดบัญชีใหม่ได้เกือบจะทันทีที่ถูกปิดลง การให้ความรู้การรู้เท่าทันมิจฉาชีพเหล่านี้ยังคงต้องใช้เวลาพอสมควร แต่สมควรจะต้องดำเนินการต่อไปควบคู่การปิดกั้น

นอกจากนี้การดำเนินการเพื่อจับตัวผู้กระทำผิด การหาหลักฐานเพื่อเข้าสู่กระบวนการยุติธรรม เพื่อดำเนินการฟ้องร้องเพื่อให้ได้ทรัพย์สินกลับคืนถึงแม้จะทำได้แต่ก็ต้องใช้เวลาและทรัพยากรเป็นอย่างมาก

การดำเนินการเรื่องนี้นอกเหนือจากตำรวจแล้ว ยังต้องได้รับความร่วมมือผู้ประกอบการโทรคมนาคม เพราะอาชญากรส่วนมากจะใช้ระบบออนไลน์ผ่านเครือข่ายโทรศัพท์มือถือ เพราะโยกย้ายได้สะดวก ใช้ Sim แบบชั่วคราว

เพราะการตามสะกดรอยผู้กระทำผิด จำเป็นจะได้ข้อมูลการโทร การใช้ Line ในการหลอกลวงเหยื่อ วัน เวลา พร้อมทั้งข้อมูล GPS สถานที่ที่ผู้ต้องหาอยู่ เพื่อทางเจ้าหน้าที่จะทำการสะกดรอยได้

โดยที่ผ่านมาทางเจ้าหน้าที่ตำรวจจะมีปัญหาที่จะหาเครื่องมือในการวิเคราะห์ข้อมูลเหล่านี้ ถึงแม้จะได้ข้อมูลจากผู้ประกอบการโทรคมนาคม ซึ่งกว่าจะได้ข้อมูลใช้เวลานานมาก

ทั้งนี้ ด้วยข้อบังคับ กสทช. มีนโยบายคุ้มครองข้อมูลส่วนบุคคล จะดำเนินการเอาข้อมูลให้บุคคลที่สามได้ บางครั้งผู้ประกอบการต้องสอบถามไปยัง กสทช.ก่อน รวมทั้งการวิเคราะห์ข้อมูลยังอาจต้องพึ่งพาเครื่องมือและบุคลากรจากผู้ประกอบการ ที่จะต้องให้พนักงานมาทำงานให้และรวมไปถึงเป็นพยานในชั้นการดำเนินการในชั้นศาล โดยในแต่ละกรณีเสียเวลาและทรัพยากรเป็นอย่างมาก

ดังนั้น การสร้างกลไกและเครื่องมือในการทำให้เกิดความร่วมมือจากผู้ประกอบการโดยไม่เป็นภาระเกินสมควร เป็นสิ่งที่จำเป็นต้องทำ มากกว่าการใช้อำนาจบังคับสั่งการจากเจ้าหน้าที่ภาครัฐ

ปัญหาที่สำคัญที่สุดของการดำเนินการอันดับแรก ไม่ใช่เรื่องการปิดกั้นหรือ การเอาผิดจับตัวคนผิดเป็นอันดับแรก แต่สิ่งที่ต้องทำก่อนและต้องใช้เวลาน้อยที่สุดคือการลดความสูญเสียของผู้เสียหาย รวมทั้งการระงับยับยั้งไม่ให้มิจฉาชีพใช้หมายเลขโทรศัพท์ หรือหมายเลขบัญชีธนาคารในการล่อลวงเหยื่อรายต่อไป ท่ามกลางการตั้งโต๊ะแถลงข่าวของหน่วยงานภาครัฐต่างๆ การตั้งเบอร์สายด่วนสี่หลัก

ตราบใดที่มิจฉาชีพยังสามารถใช้สิ่งเหล่านี้ในการประกอบอาชญากรรมได้อย่างต่อเนื่องย่อมก่อให้เกิดความ

มติชน
Matichon
Circulation: 950,000
Ad Rate: 1,100
Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: 44 ฉบับที่: 15911 หน้า: 9(ล่าง)
Col.Inch: 67.92 Ad Value: 74,712 PRValue (x3): 224,136 คลิป: ขาว-ดำ
คอลัมน์: คิดเห็นShare: แนวนโยบายแห่งรัฐ ต่อการหยุดยั้งภัยพิบัติไซเบอร์ยุค 5G การใช้เล่ห์...

ลำพองในการทำผิดได้อย่างต่อเนื่องต่อไป เช่น การดำเนินการในการระงับธุรกรรมของผู้ร้ายใช้เวลาเป็นสัปดาห์ เป็นเดือน ในขณะที่ผู้ร้ายใช้เวลาแค่ไม่กี่ชั่วโมง หรือเพียงไม่กี่วันในการยักย้ายถ่ายเททรัพย์สินของเหยื่อผู้เคราะห์ร้าย การบรรเทาเยียวยาแก่ผู้เสียหายจะไม่สามารถบรรลุมรรคผลได้

ถอดกรณีศึกษาคดีกลุ่มมิจฉาชีพ Fraud-2-Phone(F2P) ใน18 รัฐของอินเดีย

คดี F2P ที่คิดว่าเป็นเพียงความเสียหายส่วนบุคคลของการถูกหลอกลวงผ่านโทรศัพท์มือถือ ด้วยเหยื่อชายชราด้วยความเสียหายราวสามแสนบาท แต่จากการขยายผลด้วยการทำงานที่ใช้เวลาเพียงห้าวันจากศูนย์ประสานงานธุรกรรมการเงิน (Financing Coordination Centre: FCORD) ภายใต้กระทรวงมหาดไทยของอินเดีย (Ministry of Home Affair) ทำให้รู้ว่า F2P ไม่ได้มีเพียงชายชรา แต่มีพื้นที่ทำงานครอบคลุม 18 รัฐของอินเดียและมีความเสียหายมากกว่าหลายสิบล้านบาท

ขั้นตอนในการหลอกลวงของกลุ่มนี้เริ่มต้นเมื่อเย็นวันที่ 8 มิถุนายนที่ผ่านมา ชายชราอายุ 78 ปี ขณะกำลังจะรับประทานอาหารมื้อค่ำได้รับข้อความ SMS ที่มีใจความแจ้งว่า SIM card ของเขาถูกระงับการใช้งานและต้องการการยืนยันตัวตนในการแก้ปัญหานี้

ในเวลาไม่กี่อึดใจมีสายโทรศัพท์เข้ามาแจ้งว่าต้องการข้อมูลของบัตรเดบิตรวมทั้งข้อมูลส่วนบุคคลของเขาเพื่อใช้ในการชำระค่าบริการราวห้าสิบบาท ในตอนแรกชายชราจะขอชำระผ่านบัตรเครดิตแต่มิจฉาชีพแจ้งว่าต้องการการชำระผ่านบัตรเดบิตของธนาคารเท่านั้น และเมื่อได้ข้อมูลตามที่ต้องการไปได้แล้ว ภายในเวลาไม่กี่นาทีเงินจำนวนสามแสนบาทที่ถูกถอนออกจาก 4 บัญชีธนาคารของเหยื่อไม่ใช่ห้าสิบบาทตามที่แจ้งไว้

ดังนั้นในอีกสิบนาทีต่อมาเหยื่อได้โทรไปที่ศูนย์ดูแลลูกค้าของธนาคารซึ่งทำได้เพียงแต่ทำการระงับการธุรกรรมออนไลน์ทุกอย่างและทุกบัญชีของเหยื่อไว้ทันที และสามวันต่อมาในวันที่ 11 มิถุนายน เจ้าหน้าที่ของรัฐอุทัยปุระเข้าพบชายชราที่บ้านพักเพื่อจำลองสถานการณ์วันเกิดเหตุโดยทันที แอพพลิเคชั่น “CyberSafe” ของกระทรวงมหาดไทยอินเดียได้เข้ามาเป็นเครื่องมือหลักในการช่วยเหลือชายชรา

หลังการสืบสวนพบว่าจำนวนผู้เกี่ยวข้องมากกว่า 800 รายในประกอบอาชญากรรมใน 18 รัฐของอินเดีย และสามารถจับกุมผู้ร้ายจากรัฐฌาร์ขันธ์ซึ่งอยู่ห่างจากเหยื่อมากกว่าหนึ่งพันห้าร้อยกิโลเมตรที่โทรศัพท์เข้าไปหลอกลวงชายชราได้ในทันที

โดยเงินที่ได้จากเหยื่อถูกนำไปซื้อสมาร์ทโฟนราคาแพงยี่ห้อยอดนิยมจากตลาดออนไลน์ และนำไปขายในตลาดขายปลีกด้วยราคาต่ำกว่าท้องตลาด 10% โดยเงินที่ได้จากการขายจะนำเข้าไปฝากในอีกบัญชีธนาคาร การขยายผลการจับกุมพบมีเครื่องโทรศัพท์มากกว่า 900 เครื่อง บัญชีธนาคารมากกว่าพันบัญชี บัญชีผู้ใช้ของกลุ่มมิจฉาชีพในตลาดออนไลน์ รวมทั้งหลายร้อยบัญชีการทำธุรกรรมออนไลน์

ทั้งนี้การจำกัดความเสียหายได้มีการดำเนินการระงับการทำธุรกรรมหลายร้อยบัญชีของธนาคารต่างๆ บัตรเดบิตและบัตรเครดิตภายในระยะเวลาน้อยกว่าห้าวันเมื่อมีการแจ้งเหตุจากเหยื่อ โดยมีการประมาณการว่าความเสียหายจากมิจฉาชีพ F2P มีราวแปดสิบถึงร้อยล้านบาทและมีผู้อยู่ในข่ายผู้ต้องสงสัยราวแปดร้อยรายที่กำลังถูกตรวจสอบขยายผลต่อไป

แอพพลิเคชั่น “CyberSafe” ได้มีการพัฒนาและนำมาใช้ตั้งแต่เดือนสิงหาคม 2562 ที่ทำหน้าที่เชื่อมโยงประสานงานหน่วยงานมากกว่าสามพันแห่งทั้งหน่วยงานตำรวจใน 19 รัฐ และหน่วยงานทางเทคโนยีด้านการเงิน 18 แห่ง เจ้าหน้าที่ตำรวจสามารถล็อกอินเข้าสู่ CyberSafe ได้ ทำการป้อนหมายเลขโทรศัพท์และหมายเลขบัญชีของมิจฉาชีพ ข้อมูลจะถูกนำไปตรวจสอบ

ถ้าพบว่าข้อมูลเหล่านี้เคยมีการแจ้งไว้ในระบบก่อนหน้านี้แล้ว รายละเอียดจะถูกส่งมาให้เจ้าหน้าที่พร้อมดำเนินการปิดกั้นและระงับการธุรกรรมล่อลวงต่อเหยื่อรายอื่นๆ ต่อไป

จากกรณีศึกษาของอินเดีย การดำเนินการหยุดยั้งภัยพิบัติไซเบอร์ของภาคส่วนต่างๆ ควรจะต้องมีการพิจารณาสร้างกลไกและพัฒนาเครื่องมือต่างๆ เพื่อใช้ดำเนินการร่วมกันเพื่อลดความสูญเสียให้ได้ในระยะเวลาอันสั้น

เพราะประชาชนผู้ตกเป็นเหยื่อก็ไม่รู้จะหันหน้าไปพึ่งใครได้ ทุกวันนี้เมื่อโชคร้ายตกเป็นเหยื่อก็ทำได้แต่ต้องไปแจ้งความที่หน่วยงานต่างๆ ที่มีอยู่มากมาย และติดตามการดำเนินการด้วยตัวเองทั้งสิ้น

นอกจากสูญเสียจากการถูกหลอกลวง ยังจะต้องมีค่าใช้จ่ายและสูญเสียเวลาในการร้องขอความช่วยเหลือจากหน่วยงานรัฐต่างๆ ด้วยความหวังอันริบหรี่ที่จะได้ทรัพย์สินกลับคืนมา!!

ข่าวสด
Khao Sod
Circulation: 950,000
Ad Rate: 1,100

Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: 31 ฉบับที่: 11267 หน้า: 12(ขวา)
Col.Inch: 21.02 Ad Value: 23,122 PRValue (x3): 69,366 คลิป: ขาว-ดำ
หัวข้อข่าว: 'ในหลวง-พระราชินี'เสด็จออก

'ในหลวง-พระราชินี'เสด็จออก

เมื่อเวลา 18.23 น. วันที่ 2 ต.ค. พระบาทสมเด็จพระเจ้าอยู่หัว และสมเด็จพระนางเจ้าฯ พระบรมราชินี เสด็จออกพร้อมด้วยเจ้าคุณพระสินีนาฏ พิลาสกัลยาณี ณ พระที่นั่งอัมพรสถาน พระราชวังดุสิต พระราชทานพระบรมราชวโรกาสให้ คณะบุคคลต่างๆ เฝ้าทูลละอองธุลีพระบาท ตามลำดับดังนี้ พล.อ.ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี และรมว.กลาโหม พร้อมคณะ เฝ้าทูลละอองธุลีพระบาท ทูลเกล้าทูลกระหม่อมถวายเงิน เพื่อสมทบทุนมูลนิธิทุนการศึกษาพระราชทานสมเด็จพระบรมโอรสาธิราชฯ สยามมกุฎราชกุมาร (ม.ท.ศ)

มูลนิธิทุนการศึกษาพระราชทานฯ เป็นมูลนิธิที่พระบาทสมเด็จพระเจ้าอยู่หัว ทรงมีพระราชปณิธานที่จะสร้างโอกาสแก่เยาวชนที่จะเติบโตเป็นกำลังสำคัญของชาติ และทรงมีพระราชดำริพระราชทานพระราชทรัพย์ส่วนพระองค์ และเงินที่มีผู้ทูลเกล้าทูลกระหม่อมถวายโดยเสด็จพระราชกุศล มาใช้ให้เกิดประโยชน์ในการเสริมสร้างโอกาสทางการศึกษาแก่เยาวชนที่ยากจนให้ได้รับการศึกษาอย่างต่อเนื่อง โดยทรงพระกรุณาโปรดเกล้าโปรดกระหม่อมให้จัดทำ "โครงการทุนการศึกษา สมเด็จพระบรมโอรสาธิราชฯ สยามมกุฎราชกุมาร" เมื่อพุทธศักราช 2552

ต่อมาเมื่อวันที่ 4 กุมภาพันธ์ 2553 ทรงมีพระราชดำริให้จัดตั้งมูลนิธิทุนการศึกษาพระราชทานสมเด็จพระบรมโอรสาธิราชฯ สยามมกุฎราชกุมาร (ม.ท.ศ.) เพื่อดำเนินการส่งเสริมเยาวชนที่เรียนดี ขยันหมั่นเพียร ประพฤติดี มีคุณธรรม มีฐานะยากจน สามารถศึกษาต่อในชั้นมัธยมศึกษาตอนปลาย ถึงระดับปริญญาตรี หรือเทียบเท่าในสาขาวิชาตามความต้องการ โดยทรงวางหลักการกระจายทุนให้ครอบคลุมทุกจังหวัด อันเป็นการพัฒนาความรู้ความสามารถ และศักยภาพแก่เยาวชนไทย

พล.อ.สุกิจ ขมะสุนทร กรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ทำหน้าที่ประธานกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ พร้อมคณะกรรมการกิจการฯ ผู้บริหารระดับสูง และพนักงานสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เฝ้าทูลละอองธุลีพระบาท ทูลเกล้าทูลกระหม่อมถวายเงิน โดยเสด็จพระราชกุศลตามพระราชอัธยาศัย เนื่องในโอกาสวันเฉลิมพระชนมพรรษา วันที่ 28 กรกฎาคม 2564

มติชน
Matichon
Circulation: 950,000
Ad Rate: 1,100

Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: 44 **ฉบับที่:** 15911 **หน้า:** 15(บนซ้าย)
Col.Inch: 19.55 **Ad Value:** 21,505 **PRValue (x3):** 64,515 **คลิป:** ขาว-ดำ
หัวข้อข่าว: ในหลวงพระราชทานพระบรมราชวโรกาส นายกฯเข้าเฝ้าฯถวายเงินสมทบทุน ม.ท.ศ.

ในหลวงพระราชทานพระบรมราชวโรกาส นายกฯเข้าเฝ้าฯถวายเงินสมทบทุน ม.ท.ศ.

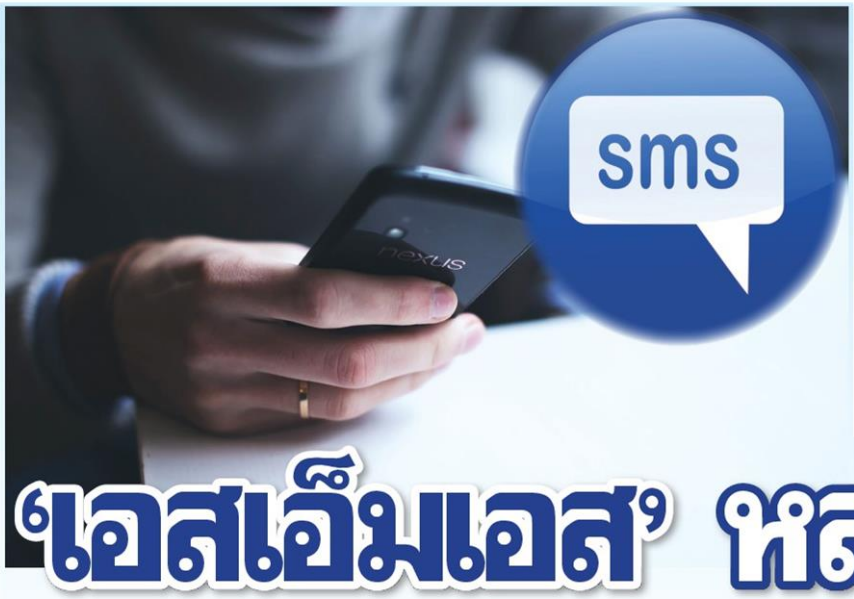
เมื่อเวลา 18.23 น. วันที่ 2 ตุลาคม พระบาทสมเด็จพระเจ้าอยู่หัว และสมเด็จพระนางเจ้าฯ พระบรมราชินี เสด็จออกพร้อมด้วย เจ้าคุณพระสินีนาฏ พิลาสกัลยาณี ณ พระที่นั่งอัมพรสถาน พระราชวังดุสิต พระราชทานพระบรมราชวโรกาสให้ คณะบุคคลต่างๆ เฝ้าฯ ตามลำดับดังนี้ พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี และรัฐมนตรีว่าการกระทรวงกลาโหม พร้อมคณะ เฝ้าฯทูลเกล้าฯถวายเงิน เพื่อสมทบทุนมูลนิธิทุนการศึกษาพระราชทานสมเด็จพระบรมโอรสาธิราชฯ สยามมกุฎราชกุมาร (ม.ท.ศ.)

มูลนิธิทุนการศึกษาพระราชทานฯ เป็นมูลนิธิที่พระบาทสมเด็จพระเจ้าอยู่หัว ทรงมีพระราชปณิธานที่จะสร้างโอกาสแก่เยาวชนที่จะเติบโตเป็นกำลังสำคัญของชาติ และทรงมีพระราชดำริพระราชทานพระราชทรัพย์ส่วนพระองค์ และเงินที่มีผู้ทูลเกล้าทูลกระหม่อมถวายโดยเสด็จพระราชกุศล มาใช้ให้เกิดประโยชน์ ในการเสริมสร้างโอกาสทางการศึกษาแก่เยาวชนที่ยากจน ให้ได้รับการศึกษาอย่างต่อเนื่อง โดยทรงพระกรุณาโปรดเกล้าฯ ให้จัดทำโครงการทุนการศึกษาสมเด็จพระบรมโอรสาธิราชฯ สยามมกุฎราชกุมาร เมื่อพุทธศักราช 2552 และต่อมาเมื่อวันที่ 4 กุมภาพันธ์ 2553 ทรงมีพระราชดำริให้จัดตั้งมูลนิธิทุนการศึกษาพระราชทานสมเด็จพระบรมโอรสาธิราชฯ สยามมกุฎราชกุมาร (ม.ท.ศ.) เพื่อดำเนินการส่งเสริมเยาวชนที่เรียนดี ขยันหมั่นเพียร ประพฤติดี มีคุณธรรม มีฐานะยากจน สามารถศึกษาต่อในชั้นมัธยมศึกษาตอนปลาย ถึงระดับปริญญาตรี หรือเทียบเท่าในสาขาวิชาตามความต้องการ โดยทรงวางหลักการกระจายทุนให้ครอบคลุมทุกจังหวัด อันเป็นการพัฒนาความรู้ความสามารถ และศักยภาพแก่เยาวชนไทย

ต่อมาพลเอกสุกิจ ขมะสุนทร กรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ทำหน้าที่ประธานกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ พร้อมคณะกรรมการกิจการฯ ผู้บริหารระดับสูง และพนักงาน สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เฝ้าฯทูลเกล้าฯถวายเงิน โดยเสด็จพระราชกุศลตามพระราชอัธยาศัย เนื่องในโอกาสวันเฉลิมพระชนมพรรษา วันที่ 28 กรกฎาคม 2564

เดลินิวส์ กรอบบ่าย
Daily News (Mid-Day)
Circulation: 500,000
Ad Rate: 2,100

Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: - **ฉบับที่:** 26288 **หน้า:** 7(บน)
Col.Inch: 73.74 **Ad Value:** 154,854 **PRValue (x3):** 464,562 **คลิป:** สี่สี
หัวข้อข่าว: 'เอสเอ็มเอส' หลอกลวง ภัยใกล้ตัวถ้าไม่โลภก็รอด!



'เอสเอ็มเอส' หลอกลวง ภัยใกล้ตัวถ้าไม่โลภก็รอด!

กลายเป็นปัญหากวนใจของผู้ใช้โทรศัพท์มือถือหรือสมาร์ทโฟนกันแทบทุกคนที่ช่วงนี้โดนข้อความสั้นหรือเอสเอ็มเอส หลอกลวง กระหน่ำส่งเข้ามายังมือถือไม่เว้นวัน!!

นอกจากจะ **"กวนใจ"** แล้ว สำหรับคนที่ไม่รู้เท่าทันหลงไปกดหรือคลิกเข้าไปดู แล้วกรอกข้อมูลตามคำเชิญชวนหว่านล้อมต่าง ๆ บ้างก็ว่า คุณเป็นผู้โชคดีถูกรางวัลได้รับเงิน, คุณได้รับเงินกู้ดอกเบี้ยต่ำ หรือคุณมีเงินเข้าบัญชีจำนวนเท่านั้นเท่านี้ ฯลฯ อาจมีปัญหาปวดหัวตามมาเพราะอาจถูกแฮก หรือขโมยข้อมูล ทำให้สูญเสียทรัพย์สินเงินในบัญชีได้ **โดยเฉพาะชาวบ้าน "ตาสีตาสา" ที่อาจไม่ได้ติดตามข่าวสารในเรื่องนี้ที่เกิดขึ้น เรียกว่าอุตส่าห์ "เก็บหอมรอมริบ" มาทั้งชีวิตอาจหมดตัวได้ง่าย ๆ**

เอสเอ็มเอสหลอกลวงเหล่านี้ ส่วนใหญ่เป็นมิจฉาชีพที่ส่งมาหลอกลวงล้วงข้อมูลแล้วไปสวมรอยเพื่อนำไปทำธุรกรรมออนไลน์ และเป็นเว็บพนันออนไลน์ที่ส่งลิงก์เชิญชวนให้เป็นลูกค้า หรือเป็นลิงก์แอพเงินกู้ออนไลน์ เรียกดอกเบี้ยโหดถือว่าผิดกฎหมาย ฯลฯ

เสียงบ่นถึงปัญหาเหล่านี้ของ "ประชาชน" ในสังคมดังขึ้นเรื่อย ๆ หน่วยงานรัฐไม่ทำอะไรที่ช่วยคุ้มครองประชาชนเลยหรือ??

สำนักงานคณะกรรมการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (สำนักงานฯกสทช.) ในฐานะที่เป็นหน่วยงานกำกับดูแล ต้องออกมาสั่งกำชับให้ **"ค่ายมือถือ"** เร่งแก้ไขปัญหาเรื่องนี้โดยให้ตรวจสอบและทำการบล็อกเอสเอ็มเอสหลอกลวงเหล่านี้ และให้ประสานแชร์ข้อมูลระหว่างกันเพื่อแบล็กลิสต์ หรือขึ้นบัญชีดำให้ทุกค่ายบล็อกเอสเอ็มเอสจากผู้ส่งรายเดียวกัน

นอกจากนี้ทาง กสทช. จะนำข้อมูลเกี่ยวกับเอสเอ็มเอสหลอกลวงไปเผยแพร่บนเว็บไซต์ของสำนักงาน กสทช. (www.nbtc.go.th) เพื่อให้ประชาชนสามารถตรวจสอบชื่อผู้ส่งข้อความที่น่าสงสัย เพื่อเป็นการป้องกันไม่ให้ตกเป็นเหยื่อได้

อย่างไรก็ตามปัญหาเอสเอ็มเอสหลอกลวงเหล่านี้ส่วนใหญ่จะถูกส่งจาก **ผู้ให้บริการด้านเนื้อหา** ที่ได้ซื้อบริการส่งเอสเอ็มเอสจากโอปเรเตอร์หรือผู้ให้บริการมือถือและบางครั้งผู้ให้บริการเนื้อหา ก็นำไปขายต่อกับบริษัทหรือธุรกิจทำให้การตรวจสอบได้ยากว่านำไปส่งข้อความเกี่ยวกับอะไร

กสทช.ได้ออกมาคาดโทษกับผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมที่ให้บริการขายต่อเอสเอ็มเอส และผู้ให้บริการด้านเนื้อหา หากทางสำนักงาน กสทช. ได้รับแจ้งว่าบริษัทใดเป็นผู้ส่งเอสเอ็มเอสที่มีลักษณะเนื้อหาเป็นการหลอกลวงจะตรวจสอบและพิจารณาลงโทษทางปกครอง ตั้งแต่เตือน ปรับ พักใช้ใบอนุญาต และโทษสูงสุด คือเพิกถอนใบอนุญาตประกอบกิจการและจะดำเนินคดีตามกฎหมายควบคู่ไปด้วย

การออกมา **"เขียนเสือให้วัวกลัว"** ก็ได้ผลระดับหนึ่งเมื่อทางค่ายมือถือออกมาประสานเสียงพร้อมดำเนินการตาม กสทช. และพร้อมร่วมมือกับทุกฝ่ายที่เกี่ยวข้อง พร้อมทั้งมีการแลกเปลี่ยนข้อมูลเอสเอ็มเอสกันเพื่อทำการบล็อก โดย "ค่ายทรู" ได้เปิด **ศูนย์เฉพาะกิจรับแจ้งปัญหาเอสเอ็มเอส ที่มีข้อความไม่เหมาะสมผ่านหมายเลขพิเศษ โทร. 0-2700-8085** เพื่อตรวจสอบและดำเนินการปิดกั้น พร้อมแจ้งเตือนบริษัทคู่สัญญา ที่ใช้บริการส่งเอสเอ็มเอส หากตรวจพบมีการส่งข้อความที่ไม่เหมาะสมจะดำเนินการทาง

เดลินิวส์ กรอบบ่าย
Daily News (Mid-Day)
Circulation: 500,000
Ad Rate: 2,100

Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: - **ฉบับที่:** 26288 **หน้า:** 7(บน)
Col.Inch: 73.74 **Ad Value:** 154,854 **PRValue (x3):** 464,562 **คลิป:** สี่สี
หัวข้อข่าว: 'เอสเอ็มเอส' หลอกลวง ภัยใกล้ตัวถ้าไม่โลภก็รอด!

กฎหมายทันที

ด้าน **"ดีแทค"** พร้อมยกระดับมาตรการการจัดการกับสแปม และเอสเอ็มเอส หลอกลวง พร้อมทั้งให้ความรู้กับสังคมและประชาชนเกี่ยวกับภัยออนไลน์ที่มาในรูปแบบต่าง ๆ ผ่าน **dtac Safe Internet** ซึ่งเป็นโครงการที่มุ่งสร้างเสริมทักษะการรับมือภัยเสี่ยงบนโลกออนไลน์

ขณะที่ **"ค่ายเอไอเอส"** ยืนยันว่าจะทำการคัดกรองผู้ประกอบการที่ซื้อบริการแพ็กเกจเอสเอ็มเอสอย่างเข้มงวด หากพบว่ามีการส่งเอสเอ็มเอสที่สร้างการรบกวน หรือหลอกลวง จะทำการบล็อก และขึ้นทะเบียนต้องห้าม หรือแบล็กลิสต์ ผู้ประกอบการรายดังกล่าวทันที!! พร้อมสื่อสารให้ข้อมูลกับประชาชน เพื่อให้รู้เท่าทันกลุ่มมิจฉาชีพด้วยเช่นกัน โดยลูกค้าที่ได้รับเอสเอ็มเอสเหล่านี้สามารถแจ้งเข้ามาได้ที่ **AIS Call Center หรือ กด *137 โทรฯ ออกฟรี เพื่อบล็อก การได้รับเอสเอ็มเอสทันที** หรือหากมีโทรศัพท์ที่โทรฯ เข้ามาสร้างความรำคาญใจ หรือก่อให้เกิดความเสี่ยงก็สามารถโทรฯ แจ้งที่ AIS Call Center เพื่อรับคำแนะนำในการบล็อกการรับสายได้ด้วยตนเอง

อย่างไรก็ตามขึ้นชื่อว่า "มิจฉาชีพ" ยังไงก็ต้องหาวิธีหลอกลวงเหยื่อให้ได้ แม้ช่องทางการส่งเอสเอ็มเอสจะไม่สะดวกเหมือนก่อน ก็ได้เปลี่ยนวิธีมาใช้โทรศัทท์ตรงเข้าหาเหยื่อเพื่อหลอกลวง อ้างว่าโทรฯ มาจากหน่วยงานภาครัฐ บอกเจ้าของเลขหมายว่าได้รับความช่วยเหลือจากรัฐบาลเป็นเงิน 2,000 บาท หรือมีสิทธิได้รับเงินกู้ 200,000 บาทบ้างแล้วหลอกถามข้อมูลส่วนตัว

จึงเป็นสิ่งที่ต้องระวังเช่นกันซึ่งทางสำนักงาน กสทช.ได้ขอความร่วมมือจากประชาชนให้โทรฯ แจ้ง **ร้องเรียนที่คอลเซ็นเตอร์ โทรศัพท์ 1200 (โทรฯ ฟรีไม่มีค่าใช้จ่าย) หรือโทรฯ แจ้งคอลเซ็นเตอร์ของมือถือที่ใช้อยู่** หากมีหลักฐานเป็นคลิปเสียงของมิจฉาชีพที่โทรฯ เข้ามาหลอกลวงก็ยิ่งดี เพราะสามารถตรวจสอบได้ว่าเบอร์ที่โทรฯ เข้ามาใครเป็นผู้ลงทะเบียนเป็นเจ้าของเบอร์ เพื่อประสานงานกับตำรวจให้ดำเนินคดีกับมิจฉาชีพเหล่านี้

สุดท้ายแล้ว!! เกราะป้องกันตัวเองที่ดีที่สุด คือต้องตั้งสติ อย่าโลภ ไม่คลิกลิงก์ในข้อความน่าสงสัยและกรอกข้อมูลส่วนตัว ให้กับผู้ส่งที่ไม่รู้จักเพื่อจะได้ไม่เป็นเหยื่อ!!.

จิราวัฒน์ จารุพันธ์

มติชน กรอบบ่าย
Matichon (Mid-Day)
Circulation: 950,000
Ad Rate: 1,100

Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: 44 ฉบับที่: 15911 หน้า: 9(ล่าง)
Col.Inch: 67.92 Ad Value: 74,712 PRValue (x3): 224,136 คลิป: ขาว-ดำ
คอลัมน์: คิดเห็นShare: แนวนโยบายแห่งรัฐ ต่อการหยุดยั้งภัยพิบัติไซเบอร์ยุค 5G การใช้เล่ห์...

แนวนโยบายแห่งรัฐ ต่อการหยุดยั้งภัยพิบัติไซเบอร์ยุค5G การใช้เล่ห์หลอกลวงดิจิทัล

หัวหน้าฝ่ายรัฐกิจและธุรกิจสัมพันธ์ บริษัทอิริคสันประเทศไทย

ท่ามกลางภัยพิบัติโควิดสร้างความยากลำบากหนักหนาสาหัสกับประชาชนอยู่มากโข

ชีวิตที่ไม่ได้ติดออนไลน์มากมาย ก็ถูกบังคับให้เข้าสู่ยุคดิจิทัลทั้งๆ ที่ไม่พร้อม ถ้าไม่มีสมาร์โฟนก็ยากมากที่จะเข้าถึง ต้องขวนขวายหามาใช้ทั้งที่รู้เรื่องบ้างไม่รู้เรื่องบ้างเพื่อจะได้รับการศึกษาออนไลน์, การขอรับความช่วยเหลือจากภาครัฐ ไม่ว่าจะเป็นโครงการคนละครึ่ง โครงการเราชนะ รวมถึงการจองฉีดวัคซีนในระยะแรกที่ต้องจองผ่านแอพพลิเคชั่นต่างๆ และด้วยไม่มีความชำนาญ และรอบรู้ ย่อมง่ายต่อการเป็นเป้าหมายในการถูกหลอกลวงผ่านช่องทางออนไลน์ ของกระบวนการพนันออนไลน์ การกู้ยืมเงินออนไลน์ การทำแชร์ลูกโซ่ หรืออะไรอีกมากมายที่จะเกิดขึ้นอีก

การพลาดพลั้งเสียท่าให้กับมิจฉาชีพเหล่านี้ ก็ไม่ใช่ความผิดของเขาเหล่านี้ที่รู้ไม่ทัน ไม่ใช่เหตุที่จะถูกถากถางว่าทำไมไม่ระวัง ทำไมไม่ติดตามข่าว

การใช้เครื่องมือทันสมัยในการหลอกลวง ไม่ได้มีเพียง SMS หรือ Call center เท่านั้น ยังปรากฏว่ามีการสื่อโซเชียลต่างๆ เช่น Line, TikTok, Facebook และอื่นๆ การป้องกันโดยการปิดกั้นก็ยากที่จะทำได้สมบูรณ์ เพราะเหล่ามิจฉาชีพจะสามารถเปิดบัญชีใหม่ได้เกือบจะทันทีที่ถูกปิดลง การให้ความรู้การรู้เท่าทันมิจฉาชีพเหล่านี้ยังคงต้องใช้เวลาพอสมควร แต่สมควรจะต้องดำเนินการต่อไปควบคู่การปิดกั้น

นอกจากนี้การดำเนินการเพื่อจับตัวผู้กระทำผิด การหาหลักฐานเพื่อเข้าสู่กระบวนการยุติธรรม เพื่อดำเนินการฟ้องร้องเพื่อให้ได้ทรัพย์สินกลับคืนถึงแม้จะทำได้แต่ก็ต้องใช้เวลาและทรัพยากรเป็นอย่างมาก

การดำเนินการเรื่องนี้นอกเหนือจากตำรวจแล้ว ยังต้องได้รับความร่วมมือผู้ประกอบการโทรคมนาคม เพราะอาชญากรส่วนมากจะใช้ระบบออนไลน์ผ่านเครือข่ายโทรศัพท์มือถือ เพราะโยกย้ายได้สะดวก ใช้ Sim แบบชั่วคราว

เพราะการตามสะกดรอยผู้กระทำผิด จำเป็นจะได้ข้อมูลการโทร การใช้ Line ในการหลอกลวงเหยื่อ วัน เวลา พร้อมทั้งข้อมูล GPS สถานที่ที่ผู้ต้องหาอยู่ เพื่อทางเจ้าหน้าที่จะทำการสะกดรอยได้

โดยที่ผ่านมาทางเจ้าหน้าที่ตำรวจจะมีปัญหาที่จะหาเครื่องมือในการวิเคราะห์ข้อมูลเหล่านี้ ถึงแม้จะได้ข้อมูลจากผู้ประกอบการโทรคมนาคม ซึ่งกว่าจะได้ข้อมูลใช้เวลานานมาก

ทั้งนี้ ด้วยข้อบังคับ กสทช. มีนโยบายคุ้มครองข้อมูลส่วนบุคคล จะดำเนินการเอาข้อมูลให้บุคคลที่สามได้ บางครั้งผู้ประกอบการต้องสอบถามไปยัง กสทช.ก่อน รวมทั้งการวิเคราะห์ข้อมูลยังอาจต้องพึ่งพาเครื่องมือและบุคลากรจากผู้ประกอบการ ที่จะต้องให้พนักงานมาทำงานให้และรวมไปถึงเป็นพยานในชั้นการดำเนินการในชั้นศาล โดยในแต่ละกรณีเสียเวลาและทรัพยากรเป็นอย่างมาก

ดังนั้น การสร้างกลไกและเครื่องมือในการทำให้เกิดความร่วมมือจากผู้ประกอบการโดยไม่เป็นภาระเกินสมควร เป็นสิ่งที่จำเป็นต้องทำ มากกว่าการใช้อำนาจบังคับสั่งการจากเจ้าหน้าที่ภาครัฐ

ปัญหาที่สำคัญที่สุดของการดำเนินการอันดับแรก ไม่ใช่เรื่องการปิดกั้นหรือ การเอาผิดจับตัวคนผิดเป็นอันดับแรก แต่สิ่งที่ต้องทำก่อนและต้องใช้เวลาน้อยที่สุดคือการลดความสูญเสียของผู้เสียหาย รวมทั้งการระงับยับยั้งไม่ให้มิจฉาชีพใช้หมายเลขโทรศัพท์ หรือหมายเลขบัญชีธนาคารในการล่อลวงเหยื่อรายต่อไป ท่ามกลางการตั้งโต๊ะแถลงข่าวของหน่วยงานภาครัฐต่างๆ การตั้งเบอร์สายด่วนสี่หลัก

ตราบใดที่มิจฉาชีพยังสามารถใช้สิ่งเหล่านี้ในการประกอบอาชญากรรมได้อย่างต่อเนื่องย่อมก่อให้เกิดความ

มติชน กรอบบ่าย
Matichon (Mid-Day)
Circulation: 950,000
Ad Rate: 1,100
Section: First Section/-
วันที่: อาทิตย์ 3 ตุลาคม 2564
ปีที่: 44 ฉบับที่: 15911 หน้า: 9(ล่าง)
Col.Inch: 67.92 Ad Value: 74,712 PRValue (x3): 224,136 คลิป: ขาว-ดำ
คอลัมน์: คิดเห็นShare: แนวนโยบายแห่งรัฐ ต่อการหยุดยั้งภัยพิบัติไซเบอร์ยุค 5G การใช้เล่ห์...

ลำพองในการทำผิดได้อย่างต่อเนื่องต่อไป เช่น การดำเนินการในการระงับธุรกรรมของผู้ร้ายใช้เวลาเป็นสัปดาห์ เป็นเดือน ในขณะที่ผู้ร้ายใช้เวลาแค่ไม่กี่ชั่วโมง หรือเพียงไม่กี่วันในการยักย้ายถ่ายเททรัพย์สินของเหยื่อผู้เคราะห์ร้าย การบรรเทาเยียวยาแก่ผู้เสียหายจะไม่สามารถบรรลุมรรคผลได้

ถอดกรณีศึกษาคดีกลุ่มมิจฉาชีพ Fraud-2-Phone(F2P) ใน18 รัฐของอินเดีย

คดี F2P ที่คิดว่าเป็นเพียงความเสียหายส่วนบุคคลของการถูกหลอกลวงผ่านโทรศัพท์มือถือ ด้วยเหยื่อชายชราด้วยความเสียหายราวสามแสนบาท แต่จากการขยายผลด้วยการทำงานที่ใช้เวลาเพียงห้าวันจากศูนย์ประสานงานธุรกรรมการเงิน (Financing Coordination Centre: FCORD) ภายใต้กระทรวงมหาดไทยของอินเดีย (Ministry of Home Affair) ทำให้รู้ว่า F2P ไม่ได้มีเพียงชายชรา แต่มีพื้นที่ทำงานครอบคลุม 18 รัฐของอินเดียและมีความเสียหายมากกว่าหลายสิบล้านบาท

ขั้นตอนในการหลอกลวงของกลุ่มนี้เริ่มต้นเมื่อเย็นวันที่ 8 มิถุนายนที่ผ่านมา ชายชราอายุ 78 ปี ขณะกำลังจะรับประทานอาหารมื้อค่ำได้รับข้อความ SMS ที่มีใจความแจ้งว่า SIM card ของเขาถูกระงับการใช้งานและต้องการการยืนยันตัวตนในการแก้ปัญหานี้

ในเวลาไม่กี่อึดใจมีสายโทรศัพท์เข้ามาแจ้งว่าต้องการข้อมูลของบัตรเดบิตรวมทั้งข้อมูลส่วนบุคคลของเขาเพื่อใช้ในการชำระค่าบริการราวห้าสิบบาท ในตอนแรกชายชราจะขอชำระผ่านบัตรเครดิตแต่มิจฉาชีพแจ้งว่าต้องการการชำระผ่านบัตรเดบิตของธนาคารเท่านั้น และเมื่อได้ข้อมูลตามที่ต้องการไปได้แล้ว ภายในเวลาไม่กี่นาทีเงินจำนวนสามแสนบาทที่ถูกถอนออกจาก 4 บัญชีธนาคารของเหยื่อไม่ใช่ห้าสิบบาทตามที่แจ้งไว้

ดังนั้นในอีกสิบนาทีต่อมาเหยื่อได้โทรไปที่ศูนย์ดูแลลูกค้าของธนาคารซึ่งทำได้เพียงแต่ทำการระงับการธุรกรรมออนไลน์ทุกอย่างและทุกบัญชีของเหยื่อไว้ทันที และสามวันต่อมาในวันที่ 11 มิถุนายน เจ้าหน้าที่ของรัฐอุทัยปุระเข้าพบชายชราที่บ้านพักเพื่อจำลองสถานการณ์วันเกิดเหตุโดยทันที แอพพลิเคชั่น “CyberSafe” ของกระทรวงมหาดไทยอินเดียได้เข้ามาเป็นเครื่องมือหลักในการช่วยเหลือชายชรา

หลังการสืบสวนพบว่าจำนวนผู้เกี่ยวข้องมากกว่า 800 รายในประกอบอาชญากรรมใน 18 รัฐของอินเดีย และสามารถจับกุมผู้ร้ายจากรัฐฌาร์ขันธ์ซึ่งอยู่ห่างจากเหยื่อมากกว่าหนึ่งพันห้าร้อยกิโลเมตรที่โทรศัพท์เข้าไปหลอกลวงชายชราได้ในทันที

โดยเงินที่ได้จากเหยื่อถูกนำไปซื้อสมาร์ทโฟนราคาแพงยี่ห้อยอดนิยมจากตลาดออนไลน์ และนำไปขายในตลาดขายปลีกด้วยราคาต่ำกว่าท้องตลาด 10% โดยเงินที่ได้จากการขายจะนำเข้าไปฝากในอีกบัญชีธนาคาร การขยายผลการจับกุมพบมีเครื่องโทรศัพท์มากกว่า 900 เครื่อง บัญชีธนาคารมากกว่าพันบัญชี บัญชีผู้ใช้ของกลุ่มมิจฉาชีพในตลาดออนไลน์ รวมทั้งหลายร้อยบัญชีการทำธุรกรรมออนไลน์

ทั้งนี้การจำกัดความเสียหายได้มีการดำเนินการระงับการทำธุรกรรมหลายร้อยบัญชีของธนาคารต่างๆ บัตรเดบิตและบัตรเครดิตภายในระยะเวลาน้อยกว่าห้าวันเมื่อมีการแจ้งเหตุจากเหยื่อ โดยมีการประมาณการว่าความเสียหายจากมิจฉาชีพ F2P มีราวแปดสิบถึงร้อยล้านบาทและมีผู้อยู่ในข่ายผู้ต้องสงสัยราวแปดร้อยรายที่กำลังถูกตรวจสอบขยายผลต่อไป

แอพพลิเคชั่น “CyberSafe” ได้มีการพัฒนาและนำมาใช้ตั้งแต่เดือนสิงหาคม 2562 ที่ทำหน้าที่เชื่อมโยงประสานงานหน่วยงานมากกว่าสามพันแห่งทั้งหน่วยงานตำรวจใน 19 รัฐ และหน่วยงานทางเทคโนยีด้านการเงิน 18 แห่ง เจ้าหน้าที่ตำรวจสามารถล็อกอินเข้าสู่ CyberSafe ได้ ทำการป้อนหมายเลขโทรศัพท์และหมายเลขบัญชีของมิจฉาชีพ ข้อมูลจะถูกนำไปตรวจสอบ

ถ้าพบว่าข้อมูลเหล่านี้เคยมีการแจ้งไว้ในระบบก่อนหน้านี้แล้ว รายละเอียดจะถูกส่งมาให้เจ้าหน้าที่พร้อมดำเนินการปิดกั้นและระงับการธุรกรรมล่อลวงต่อเหยื่อรายอื่นๆ ต่อไป

จากกรณีศึกษาของอินเดีย การดำเนินการหยุดยั้งภัยพิบัติไซเบอร์ของภาคส่วนต่างๆ ควรจะต้องมีการพิจารณาสร้างกลไกและพัฒนาเครื่องมือต่างๆ เพื่อใช้ดำเนินการร่วมกันเพื่อลดความสูญเสียให้ได้ในระยะเวลาอันสั้น

เพราะประชาชนผู้ตกเป็นเหยื่อก็ไม่รู้จะหันหน้าไปพึ่งใครได้ ทุกวันนี้เมื่อโชคร้ายตกเป็นเหยื่อก็ทำได้แต่ต้องไปแจ้งความที่หน่วยงานต่างๆ ที่มีอยู่มากมาย และติดตามการดำเนินการด้วยตัวเองทั้งสิ้น

นอกจากสูญเสียจากการถูกหลอกลวง ยังจะต้องมีค่าใช้จ่ายและสูญเสียเวลาในการร้องขอความช่วยเหลือจากหน่วยงานรัฐต่างๆ ด้วยความหวังอันริบหรี่ที่จะได้ทรัพย์สินกลับคืนมา!!