บทความ

เกราะป้องกันภัยไซเบอร์สำหรับเยาวชนไทย

ในทศวรรษที่ผ่านมาประเทศไทยได้ก้าวเข้าสู่การเป็นสังคมดิจิทัลอย่างรวดเร็ว การเข้าถึงอินเทอร์เน็ตกลายเป็นสิทธิขั้นพื้นฐานที่เด็กและเยาวชนในปัจจุบันสามารถเข้าถึงได้อย่างง่ายดาย อย่างไรก็ตาม ท่ามกลางความสะดวกสบายของโลกออนไลน์ กลับมีภัยมืดที่แฝงตัวมาในรูปแบบของอาชญากรรมทางไซเบอร์ ซึ่งปัจจุบันได้ทวีความรุนแรงและซับซ้อนขึ้นอย่างน่าตกใจ โดยมีเป้าหมายหลัก คือ **กลุ่มเด็กและเยาวชน** ซึ่งถือเป็นกลุ่มเปราะบางที่สุดในระบบนิเวศดิจิทัล

หน้าจอมือถือเปรียบเสมือนประตูบานใหญ่ที่เปิดออกสู่โลกกว้าง แต่ขณะเดียวกันก็เป็นช่องโหว่ให้มิจฉาชีพก้าวเข้าถึงตัวเด็กได้ถึงในห้องนอน ความอันตรายออนไลน์ที่เกิดขึ้นกับเด็กนั้นมีมิติความรุนแรงที่ซับซ้อนและยาวนานกว่าวัยผู้ใหญ่ เนื่องจากกระบวนการคิดและวุฒิภาวะทางอารมณ์ที่ยังพัฒนาไม่เต็มที่ ทำให้เด็กมักจะตกเป็นเหยื่อของการปั่นหัวทางจิตวิทยาโดยอาชญากรทางไซเบอร์ได้อย่างง่ายดาย

นอกจากนี้ ความน่ากลัวของอาชญากรรมไซเบอร์ในวัยเด็ก ไม่ได้จำกัดอยู่เพียงแค่การสูญเสียทรัพย์สินของพ่อแม่ผู้ปกครองเท่านั้น แต่สิ่งที่ร้ายแรงกว่า คือการโจมตีไปที่สภาพจิตใจ และอนาคตของเยาวชน มิจฉาชีพยุคใหม่ใช้เครื่องมือทางจิตวิทยาที่ซับซ้อนในการล่อลวง ข่มขู่ และบงการเหยื่อ บทความฉบับนี้จึงมุ่งเน้นการวิเคราะห์ความน่ากลัวของภัยจากอาชญากรทางไซเบอร์ในวัยเด็ก ผ่านกรณีศึกษาที่เกิดขึ้นจริงพร้อมนำเสนอแนวทางการป้องกันและแก้ไข เพื่อสร้างความปลอดภัยให้แก่บุคลากรที่สำคัญที่สุดของชาติ

๑. ความอันตรายสามารถจำแนกออกเป็น ๓ ด้านหลัก ดังนี้

๑.๑ การสูญเสียข้อมูลส่วนบุคคลที่ย้อนกลับมาทำร้าย

การสูญเสียข้อมูลส่วนบุคคลในวัยเด็กหรือเยาวชนไม่ได้หยุดอยู่แค่การถูกนำเอาชื่อไปแอบอ้าง แต่คือการถูกลอกคราบตัวตน เพื่อเป้าหมายที่อันตรายกว่าเดิม เด็กมักจะขาดความตระหนักว่าข้อมูลเพียงเล็กน้อย เช่น ชื่อเล่น ชื่อโรงเรียน ภาพถ่ายในชุดนักเรียน หรือการเช็คอินสถานที่ ที่ไปเป็นประจำ สามารถนำมาประกอบเป็นฐานข้อมูลขนาดใหญ่ที่มิจฉาชีพใช้ เพื่อทำการตีสนิทอย่างเป็นระบบ มิจฉาชีพจะใช้ข้อมูลเหล่านี้ สร้างเรื่องราวให้เด็กเชื่อใจว่าเรารู้จักกัน เพื่อหลอกล่อเอาข้อมูลที่สำคัญกว่าเดิม เช่น เลขบัตรประชาชนของพ่อแม่ หรือเลขบัตรเครดิตที่ผูกไว้กับแอปพลิเคชันเกม ข้อมูลเหล่านี้เมื่อหลุดออกไปสู่ตลาดมืดจะถูกนำไปใช้ในการโจรกรรมทางการเงิน หรือซ้ำร้ายกว่านั้น คือ การใช้ติดตามตำแหน่งของเด็กในโลกความเป็นจริงเพื่อทำการลักพาตัวหรือล่วงละเมิด ซึ่งถือเป็นการละเมิดสิทธิความเป็นส่วนตัวที่ส่งผลกระทบต่อความปลอดภัยของทั้งตัวเด็กและครอบครัวอย่างรุนแรง

๑.๒ ผลกระทบต่อสภาพจิตใจ บาดแผลที่ไม่มีเลือดออก แต่กลับเยียวยายากที่สุด

ความอันตรายทางออนไลน์มักมาในรูปแบบของการกดขี่ข่มเหงทางไซเบอร์ และการข่มขู่กรรโชกซึ่งสร้างบาดแผลลึกในใจเด็กอย่างที่ประเมินค่าไม่ได้ เมื่อเด็กพลาดพลั้งส่งรูปภาพที่ไม่เหมาะสม หรือกระทำสิ่งที่ผิดพลาดไป มิจฉาชีพจะใช้สิ่งนั้นเป็นโซ่ล่ามทางจิตวิทยา โดยข่มขู่ว่าจะนำสิ่งนั้นไปประจานในกลุ่มเพื่อนหรือส่งให้คุณครูผู้สอนดูความกดดันมหาศาลนี้ ทำให้เด็กตกอยู่ในสภาวะจำยอมและหวาดระแวงตลอดเวลาผลกระทบที่ตามมา คือ การสูญเสียความมั่นใจในตัวเองอย่างรุนแรง โดยที่เด็กจะเริ่มปลีกตัวออกจากสังคม มีผลการเรียนที่แย่ลงและเข้าสู่สภาวะซึมเศร้าขั้นรุนแรง เนื่องจากในสายตาของเด็ก โลกออนไลน์คือ โลกทั้งใบของพวกเขา การถูกประจานออนไลน์จึงเท่ากับศาลเตี้ยที่ตัดสินชีวิตเขาให้พังทลายลง บาดแผลเหล่านี้มักฝังลึกและกลายเป็นปมด้อยที่ขัดขวางการเติบโตเป็นผู้ใหญ่ที่มีคุณภาพ และในกรณีที่ร้ายแรงที่สุด คือ ความสิ้นหวังจากการถูกกดดันทางออนไลน์มักจะนำไปสู่การตัดสินใจที่ผิดพลาดอย่างการพยายามจบชีวิตตนเองของเด็ก

/๑.๓ ภัยต่อความปลอดภัย...

๑.๓ ภัยต่อความปลอดภัยในชีวิตจากโลกเสมือนสู่การล่วงละเมิดในโลกจริง

ขั้นสุดของความอันตรายออนไลน์ที่พัฒนาไปสู่คดีอาชญากรรมในโลกจริง มิจฉาชีพที่เชี่ยวชาญจะใช้เวลาหลายเดือนในการสร้างความสัมพันธ์เสมือน เพื่อให้เด็กเกิดความรัก ความผูกพัน หรือความเชื่อใจ โดยใช้เทคนิคการล่อลวงให้เด็กรู้สึกว่า มีแต่พี่เท่านั้นที่เข้าใจหนู จนกระทั่งเด็กยอมออกมานัดเจอในโลกความจริง โดยที่ไม่ได้บอกให้ผู้ปกครองรับทราบก่อน เมื่อเด็กออกมาสู่โลกภายนอกที่ไร้การป้องกันมักจะถูกล่อลวงไปสู่การล่วงละเมิดทางเพศ การถูกกักขังหน่วงเหนี่ยว หรือถูกบังคับให้เข้าสู่ขบวนการค้ามนุษย์และการผลิตสื่อลามกอนาจารเด็ก ซึ่งเป็นเรื่องที่ยากจะแก้ไขได้ทันท่วงที ความอันตรายนี้จึงไม่ใช่แค่เรื่องของข้อมูลหรือเงินทอง แต่คือการสูญเสียอิสรภาพร่างกาย และจิตวิญญาณ ซึ่งเป็นการทำลายอนาคตของเด็กไทย และมักจะเป็นจุดเริ่มต้นของวงจรอาชญากรรมที่ซับซ้อนยิ่งขึ้นไป

๒. มิติความน่ากลัวของอาชญากรรมไซเบอร์ต่อเด็ก

ความน่ากลัวของอาชญากรรมที่มุ่งเป้าไปยังเยาวชนมีความแตกต่างจากวัยผู้ใหญ่ มิจฉาชีพไม่ได้มองหาเพียงแค่ตัวเงินในบัญชี แต่พวกเขากำลังมองหาอำนาจในการควบคุม ซึ่งส่งผลกระทบโดยตรงที่รุนแรงกว่าในทั้ง ๓ ด้านหลัก ดังนี้

๒.๑ การทำลายความไว้วางใจพื้นฐาน เมื่อเด็กถูกหลอกโดยคนที่เขาเชื่อว่าเป็นเพื่อนหรือไอดอล เด็กจะสูญเสียความเชื่อใจในสังคมออนไลน์และคนรอบข้าง จึงส่งผลให้เด็กกลายเป็นบุคคลที่เก็บตัวและมีปัญหาในการสร้างปฏิสัมพันธ์ในโลกจริง

๒.๒ การตกเป็นเหยื่อซ้ำซ้อน เนื่องจากข้อมูลหรือภาพลักษณ์ที่ผิดพลาดของเด็กในโลกออนไลน์จะคงอยู่ตลอดไป มิจฉาชีพมักจะนำข้อมูลเดิมมาวนเวียนข่มขู่เด็กในระยะเวลาที่ยาวนาน ทำให้เด็กตกอยู่ในความหวาดระแวงตลอดเวลา

๒.๓ การถูกหล่อหลอมค่านิยมที่ผิด เนื่องจากอาชญากรบางกลุ่มไม่ได้หลอกเงิน แต่กลับหลอกลวงทางความคิด ชักจูงเด็กให้ทำเรื่องอันตราย พนันออนไลน์ หรือการส่งต่อข้อมูลบิดเบือน ซึ่งเป็นการทำลายทรัพยากรมนุษย์ในระดับรากฐาน

๓. เหตุการณ์หรือกรณีศึกษาเกี่ยวกับอาชญากรรมทางไซเบอร์ต่อวัยเด็ก

บทความนี้ได้จัดจำแนกวิธีการและกลลวงต่างๆ ที่สามารถพบเห็นและมีแนวโน้มที่จะเกิดขึ้นได้สูงในสังคมไทยปัจจุบันเกี่ยวกับเหตุการณ์ การถูกหลอกลวงและการตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ผ่านกลวิธีต่าง ๆ ของอาชญากรทางไซเบอร์ ซึ่งมุ่งเน้นโจมตีเป้าหมายในช่วงวัยเด็กโดยเฉพาะ ดังต่อไปนี้

เหตุการณ์ ที่ ๑ การล่าเหยื่อในโลกเสมือน มิจฉาชีพยุคใหม่ฉลาดพอที่จะไม่เริ่มต้นด้วยการขอเงิน แต่จะเริ่มต้นด้วยการให้ เช่น การแจกเงินหรืออุปกรณ์หายากในเกม โดยใช้ช่องทางการสื่อสารในเกมเป็นช่องทางหลัก มิจฉาชีพจะส่งลิงก์ที่อ้างว่าเป็นโปรแกรมช่วยเล่นหรือกิจกรรมแจกของฟรีไปให้เด็ก แต่ความจริงคือหน้าเว็บเพื่อดึงรหัสบัญชี เมื่อเด็กกรอกข้อมูล มิจฉาชีพจะเข้าถึงบัญชีธนาคารหรือบัตรเครดิตของผู้ปกครองที่ผูกบัญชีไว้ และทำการโอนเงินออกผ่านช่องทางการชำระเงินออนไลน์ที่ตรวจสอบได้ยาก นอกจากนี้ เด็กมักจะไม่กล้าบอกความจริงกับผู้ปกครอง เนื่องจากกลัวความผิด เรื่อง การเล่นเกมหรือการนำเงินไปใช้ ส่งผลให้มิจฉาชีพมีเวลาในการโอนเงินออกจากบัญชีผู้ปกครองไปจนหมด

เหตุการณ์ที่ ๒ การข่มขู่และการแสวงหาประโยชน์ทางเพศ มักเกิดขึ้นผ่านแอปพลิเคชันหาคู่สำหรับวัยรุ่นหรือแอปโซเชียลทั่วไป โดยมิจฉาชีพจะสร้างตัวตนปลอมที่ตรงกับความชอบของเด็ก โดยเริ่มต้นจากการชวนคุยสร้างความสนิทสนมจนเกิดความผูกพันทางอารมณ์ จากนั้นจะขอให้เด็กถ่ายภาพหรือวิดีโอในลักษณะที่ไม่เหมาะสม เมื่อได้คลิปไปแล้ว มิจฉาชีพจะเปลี่ยนท่าทีทันที โดยใช้การประจาน เป็นเครื่องมือในการข่มขู่เรียกเงิน หรือบังคับให้เด็กโอนเงินจากบัญชีผู้ปกครองมาให้ ผลกระทบในกรณีนี้ มักจะนำไปสู่สาเหตุของการเลือกที่จะจบชีวิตตนเอง เนื่องจากเด็กไม่มีทางออกและแบกรับความกดดันจากสังคมไม่ไหว

/เหตุการณ์ที่ ๓...

เหตุการณ์ที่ ๓ การขยายตัวของธุรกิจบัญชีปลอมเยาวชน เนื่องจากการเปิดบัญชีธนาคารออนไลน์สามารถทำได้ง่ายมากขึ้นในยุคปัจจุบัน โดยที่มิจฉาชีพมักจะใช้โฆษณาว่ารับสมัครเด็กนักเรียนมาทำงานด้วย เพียงแค่รับโอนเงินหรือถอนเงินให้ ก็รับเงินตอบแทนไปได้เลย หรือหลอกลวงให้เด็กเปิดบัญชีธนาคาร เพื่อรับส่วนลดสินค้า เมื่อเด็กถูกใช้เป็นเครื่องมือในการฟอกเงินผิดกฎหมาย เมื่อมีคดีความเกิดขึ้น เด็กจะถูกออกหมายเรียกและเสียประวัติ ซึ่งถือเป็นอุปสรรคต่อการศึกษาและการทำงานในอนาคตอย่างถาวร

เหตุการณ์ที่ ๔ การหลอกลวงผ่านภารกิจออนไลน์ ที่มุ่งเน้นเป้าหมายไปหาเด็กที่มีนิสัยชอบมีความต้องการที่จะช่วยเหลือพ่อแม่ในการประหยัดค่าใช้จ่าย โดยมิจฉาชีพมักจะอ้างว่า เป็นงานตอบกลับหรือการนำเสนอสินค้าผ่านช่องทางออนไลน์ โดยให้เด็กทำภารกิจ เช่น กดถูกใจสินค้า แล้วเด็กก็จะได้รับเงินตอบแทน เมื่อเด็กเริ่มเกิดความไว้วางใจ มิจฉาชีพจะเริ่มให้เด็กทำภารกิจที่จะต้องใช้เงินส่วนตัวจ่ายไปก่อนเป็นจำนวนหลักพันถึงหลักหมื่น ซึ่งเด็กมักจะนำเงินค่าเทอมหรือเงินเก็บทั้งปีมาลงกับภารกิจสุดท้าย เนื่องจากความหวังว่าจะได้กำไรก้อนใหญ่ แต่สุดท้ายหลังจากที่โอนเงินไปแล้ว มิจฉาชีพก็จะตัดช่องทางการติดต่อสื่อสารและหนีหายไปพร้อมเงินทั้งหมด

อาชญากรรมออนไลน์จึงเป็นสงครามทางจิตวิทยาที่มุ่งเน้นทำลายเยาวชน การป้องกันที่ดีที่สุดคือการยึดถือคาถาป้องกันตัว **ไม่เชื่อ ไม่รีบ ไม่โอน** ของรัฐบาล ที่มุ่งเน้นต้องการให้ประชาชนทุกคน มีสติก่อนการทำธุรกรรมใดๆ ซึ่งสามารถนำมาประยุกต์ใช้กับวัยเด็กหรือเยาวชนได้อย่างมีประสิทธิภาพ โดยที่สามารถทำความเข้าใจส่วนสำคัญของนโยบาย ได้ดังนี้

ไม่เชื่อ หมายถึง การสร้างหลักสูตรการสอนที่จะช่วยพัฒนาเด็กให้ฉลาดสงสัยและตั้งคำถามเกี่ยวกับทุกสิ่งอย่างที่เด็กได้รับมาโดยไม่เสียค่าใช่จ่ายใดๆ หรือคำชมจากคนแปลกหน้าในอินเทอร์เน็ตว่าเป็นสัญญาณอันตราย ต้องมีการตรวจสอบความถูกต้องของสิ่งเหล่านั้นก่อนเสมอ

ไม่รีบ เนื่องจากหัวใจของอาชญากรไซเบอร์ คือ การสร้างสถานการณ์เร่งด่วน นโยบายนี้สอนให้เด็กเรียนรู้ที่จะนิ่ง เมื่อถูกข่มขู่หรือถูกกระตุ้นความโลภ หากถูกเร่งรัดให้ทำธุรกรรมให้หยุดใช้งานเครื่องมือสื่อสารและกล้าที่จะปรึกษากับผู้ใหญ่อย่างเปิดเผย

ไม่โอน ถือเป็นด่านสุดท้ายที่สำคัญที่สุด ต้องย้ำเตือนให้เป็นค่านิยมในชุมชนว่า เงินและข้อมูลส่วนตัว คือ ทรัพย์สินที่ห้ามมอบให้ใครผ่านโลกออนไลน์โดยเด็ดขาด หากไม่มีการยืนยันตัวตนที่ศูนย์ราชการหรือพนักงานธนาคาร ที่สำนักงานจริง

๔. วิธีการป้องกันและการสร้างเกราะคุ้มกันเชิงรุก

การป้องกันที่ดีที่สุดคือการทำให้มิจฉาชีพ เข้าถึงตัวเด็กได้ยากที่สุด และทำให้เด็กมีไหวพริบสูงที่สุด ผ่าน ๓ กลไกสำคัญ ดังนี้

๔.๑ การตั้งค่าความปลอดภัยทางเทคโนโลยี พ่อแม่และผู้ปกครองต้องทำหน้าที่ เป็นเหมือนด่านคัดกรองโดยการใช้เครื่องมือบนอุปกรณ์สื่อสาร เพื่อทำหน้าที่ตรวจสอบประเภทของแอปพลิเคชันที่เด็กดาวน์โหลดจำกัดเวลาการใช้งานไม่ให้เกิดการเสพติดจนขาดการยับยั้งชั่งใจ รวมถึงการตรวจสอบและสอนให้เด็ก ตั้งค่าบัญชีโซเชียลมีเดียให้เป็นบัญชีส่วนตัวเสมอ สิ่งนี้จะช่วยจำกัดวงของคนที่จะเข้ามาปฏิสัมพันธ์กับเด็ก ให้เหลือเพียงคนใกล้ชิด และลดโอกาสที่มิจฉาชีพจะแฝงตัวเข้ามาส่งข้อความหรือเข้าถึงข้อมูลส่วนตัวของเด็กได้โดยตรง

๔.๒ การสร้างเกราะความรู้และทัศนคติ การสอนให้เด็กมีทักษะการคิดเชิงวิพากษ์ในโลกออนไลน์เป็นเรื่องสำคัญอย่างยิ่ง เด็กต้องเข้าใจกฎเหล็กที่ว่า ของฟรีไม่มีในโลก ไม่ว่าจะเป็นไอเทมเกมสุดหายาก เพชรฟรีหรือเงินรางวัลมหาศาล ทุกอย่างคือเหยื่อล่อที่ มิจฉาชีพ ใช้เพื่อดึงเด็กเข้าสู่กับดัก นอกจากนี้ต้องย้ำเตือนว่าคนหน้าตาดีหรือใจดีในรูปโปรไฟล์ อาจเป็นมิจฉาชีพที่ใช้เทคโนโลยีปัญญาประดิษฐ์หรือภาพปลอมมาสร้างความเชื่อใจ ดังนั้น การปฏิเสธคนแปลกหน้าทางออนไลน์ จึงไม่ใช่เรื่องเสียมารยาท แต่เป็นเรื่องของความปลอดภัยที่วัยเด็กควรที่จะต้องเข้าใจและให้ความสำคัญเป็นอย่างมากในยุคปัจจุบันนี้

/๔.๓ การสร้างพื้นที่...

๔.๓ การสร้างพื้นที่ปลอดภัยทางความรู้สึก หัวใจสำคัญของการป้องกันไม่ใช่แค่เรื่องของเครื่องมือบนอุปกรณ์สื่อสารหรือเทคโนโลยี แต่คือความสัมพันธ์ในบ้านพ่อและแม่ต้องสร้างบรรยากาศที่เด็กไม่รู้สึกกดดัน ถ้าหากเด็กเผลอทำผิดพลาด เช่น เผลอกดลิงก์แปลกปลอม หรือแอบนำเงินไปเติมเกม ผู้ปกครองจะต้องไม่เริ่มด้วยการดุด่ารุนแรง เนื่องจากความกลัวจะทำให้เด็กเลือกที่จะปิดบังปัญหา และตกเป็นเหยื่อของการถูกมิจฉาชีพขมขู่ต่อไปได้การสร้างความมั่นใจให้ลูกรู้ว่าไม่ว่าเกิดอะไรขึ้นพ่อและแม่พร้อมที่จะอยู่เคียงข้างกับลูกเสมอจะทำให้เด็กมีความกล้าที่จะเดินเข้ามาบอกเล่าถึงปัญหาทันที หลังจากที่เริ่มรู้สึกถึงความผิดปกติ

๕. วิธีการแก้ไข ยุทธศาสตร์การยับยั้งความเสียหายทันที

เมื่อเด็กเกิดพลาดพลั้งและตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ ผู้ปกครองหรือเด็กจะต้องดำเนินการแก้ไขทันทีอย่างฉับไวและมีสติ เพื่อตัดวงจรของมิจฉาชีพให้เร็วที่สุด ดังนี้

๕.๑ มาตรการ หยุด บล็อก แจ้ง ทันทีที่พบร่องรอยการหลอกลวงหรือการข่มขู่ ต้องสั่งให้เด็กหยุดการสื่อสารทุกรูปแบบทันที ห้ามตอบโต้ ห้ามโอนเงินเพิ่ม และห้ามพยายามต่อรอง หลังจากนั้นให้ทำการบล็อกหรือตัดช่องทางการติดต่อของบัญชีดังกล่าว ในทุกช่องทางเพื่อป้องกันการคุกคามต่อเนื่อง ขั้นตอนถัดไปคือเด็กต้องรีบแจ้งผู้ปกครองหรือครูในทันทีเพื่อเปลี่ยนหน้าที่การรับผิดชอบและการตัดสินใจจากเด็กมาสู่ผู้ใหญ่ที่มีวุฒิภาวะมากกว่า

๕.๒ การปฏิบัติการเก็บหลักฐานดิจิทัล ในโลกไซเบอร์ พยานหลักฐานสามารถที่จะถูกลบเลือนได้ง่าย ดังนั้น ผู้ปกครองต้องทำหน้าที่รวบรวมหลักฐานอย่างละเอียด ตั้งแต่การบันทึกภาพหน้าจอแชทสนทนาที่เห็นลำดับเหตุการณ์ชัดเจน บัญชีที่คนร้ายใช้งาน ไปจนถึงสลิปการโอนเงินและเลขบัญชีปลายทาง หลักฐานเหล่านี้ห้ามทำการแก้ไขหรือดัดแปลงเด็ดขาด เพราะจะเป็นกุญแจสำคัญในการนำตัวมิจฉาชีพมาลงโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๕.๓ การใช้กลไกทางกฎหมายและสายด่วน เมื่อรวบรวมหลักฐานได้แล้ว ต้องรีบดำเนินการตามขั้นตอนของกฎหมายอย่างรวดเร็วที่สุด โดยเฉพาะถ้าหากมีการสูญเสียทรัพย์สิน ให้โทรแจ้งสายด่วน **๑๔๑๑** เพื่อทำการระงับบัญชีม้าที่รับโอนเงินภายใน ๑๕ ถึง ๓๐ นาทีแรก เพื่อเพิ่มโอกาสในการอายัดเงินคืน หลังจากนั้น ให้ดำเนินการแจ้งความที่สถานีตำรวจ หรือผ่านช่องทางที่เป็นทางการเพียงช่องทางเดียว คือ www.thaipoliceonline.go.th ซึ่งเป็นศูนย์รวมคดีไซเบอร์โดยตรง เพื่อให้เจ้าหน้าที่ตำรวจที่มีความชำนาญการพิเศษเข้ามาดูแลจัดการเรื่องคดีความ เพื่อดำเนินการจับกุม มิจฉาชีพและผู้สมรู้ร่วมคิดมาลงโทษและดำเนินคดี ตามกระบวนการทางกฎหมายต่อไป

บทสรุปของอาชญากรรมทางไซเบอร์ ที่จ้องเล่นงานเด็กและเยาวชนในปัจจุบัน สะท้อนให้เห็นว่าความเสียหายไม่ได้หยุดอยู่เพียงแค่ตัวเงิน แต่แผ่ขยายไปถึงการสูญเสียตัวตน สภาพจิตใจที่บอบช้ำ และความปลอดภัยในชีวิต ซึ่งยากที่จะกอบกู้เอาคืนมาได้ ดังนั้น การป้องกันเชิงรุกผ่านยุทธศาสตร์ **ไม่เชื่อ ไม่รีบ ไม่โอน** ต้องถูกปลูกฝังให้เป็นสัญชาตญาณดิจิทัลของเด็กทุกคน เพื่อให้พวกเขามีสติในการคัดกรองข้อมูล ไม่ตื่นตระหนกต่อการข่มขู่ และเด็ดขาดในการปฏิเสธการโอนเงิน หรือส่งมอบข้อมูลส่วนตัวให้แก่คนแปลกหน้า ซึ่งถือเป็นเกราะคุ้มกันที่แข็งแกร่งที่สุดในการปกป้องลูกหลานไทย ให้เติบโตอย่างปลอดภัยและมั่นคง ท่ามกลางกระแสการเปลี่ยนแปลงของโลกออนไลน์ที่เต็มไปด้วยเล่ห์เหลี่ยมของอาชญากรทางไซเบอร์อย่างยั่งยืน

บรรณานุกรม

กรมกิจการผู้สูงอายุ. (2567). คู่มือรับมือภัยไซเบอร์สำหรับผู้สูงอายุ. สืบค้นจาก https://www.dop.go.th/th/news/1/5035

ธนาคารไทยพาณิชย์. (2567). ภัยหลอกลวงผู้สูงอายุที่ควรระวัง. สืบค้นจาก https://www.scb.co.th/th/personal-banking/fraud-fighter/update-fraud/scams-elderly

ธัญพิชชา สามารถ. (2565). การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ (วิทยานิพนธ์ปริญญามหาบัณฑิต). จุฬาลงกรณ์มหาวิทยาลัย, กรุงเทพฯ. สืบค้นจาก https://digital.car.chula.ac.th/chulaetd/6716

The Reporter. (2567). ภัยไซเบอร์กับผู้สูงอายุ: ทำไมผู้สูงวัยจึงตกเป็นเป้าหมายของมิจฉาชีพออนไลน์. สืบค้นจาก https://today.line.me/th/v3/article/XY8g5GZ

องค์การบริหารส่วนตำบลบุรีรัมย์. (2567). ประชาสัมพันธ์ภัยไซเบอร์และแนวทางป้องกันภัยออนไลน์. สืบค้นจาก https://www.buriramlocal.go.th/public/list/data/detail/id/16291/menu/1554/page/1

บทความ

คู่มือวัยเก๋ารู้ทันภัยไซเบอร์ รู้ทันกลโกงออนไลน์ ปลอดภัย ไม่ตกเป็นเหยื่อมิจฉาชีพ

ทุกวันนี้ เพียงเสียงโทรศัพท์หนึ่งสาย หรือข้อความหนึ่งข้อความ อาจกลายเป็นจุดเริ่มต้นของการสูญเสียเงินเก็บทั้งชีวิตได้โดยไม่รู้ตัว มิจฉาชีพในยุคดิจิทัลไม่ได้ใช้เพียงการข่มขู่หรือหลอกลวงแบบเดิมอีกต่อไป แต่มีการปรับเปลี่ยนวิธีการให้แนบเนียนและสมจริงมากขึ้น ทั้งการแอบอ้างเป็นเจ้าหน้าที่รัฐ ตำรวจ ธนาคาร คนรู้จัก หรือแม้แต่การเข้ามาพูดคุยสร้างความสัมพันธ์ผ่านโลกออนไลน์ เพื่อหลอกเอาเงิน ข้อมูลส่วนตัว หรือทรัพย์สินจากผู้เสียหาย

ปัจจุบันผู้สูงอายุจำนวนมากเริ่มใช้สมาร์ตโฟนและสื่อออนไลน์ในชีวิตประจำวันมากขึ้น ไม่ว่าจะเป็นการพูดคุยกับลูกหลาน ซื้อสินค้าออนไลน์ ติดตามข่าวสาร หรือทำธุรกรรมทางการเงิน แม้เทคโนโลยีจะช่วยเพิ่มความสะดวกสบายในการใช้ชีวิต แต่ในขณะเดียวกันก็ทำให้ผู้สูงอายุกลายเป็นหนึ่งในกลุ่มเป้าหมายสำคัญของอาชญากรรมทางไซเบอร์

อาชญากรรมไซเบอร์ (Cyber Threat) คือ การกระทำหรือความพยายามเข้าถึงข้อมูล ระบบ หรือทรัพย์สินของผู้อื่นผ่านช่องทางออนไลน์โดยมิชอบ เพื่อหลอกลวงหรือสร้างความเสียหาย ซึ่งในปัจจุบันมีหลากหลายรูปแบบ ตั้งแต่แก๊งคอลเซ็นเตอร์ การหลอกลงทุน หลอกขายสินค้าออนไลน์ ไปจนถึงการใช้ความสัมพันธ์และความสงสารเป็นเครื่องมือในการหลอกเอาเงิน สิ่งสำคัญคือ มิจฉาชีพมักไม่ได้อาศัยเพียง เทคโนโลยี ในการหลอกลวง แต่อาศัย จิตวิทยา เข้ามาเป็นเครื่องมือสำคัญ ทั้งการสร้างความกลัว ความรีบเร่ง ความไว้ใจ หรือความหวัง เพื่อให้เหยื่อตัดสินใจผิดพลาดโดยไม่ทันตั้งตัว

ดังนั้น การรู้เท่าทันกลวิธีของมิจฉาชีพ จึงถือเป็นเกราะป้องกันสำคัญที่จะช่วยลดความเสี่ยงจากภัยออนไลน์ และช่วยให้ผู้สูงอายุสามารถใช้เทคโนโลยีได้อย่างมั่นใจและปลอดภัยมากยิ่งขึ้น

อาชญากรรมไซเบอร์ ๖ รูปแบบ ที่มิจฉาชีพนิยมใช้หลอกลวงผู้สูงอายุ

๑. หลอกซื้อขายสินค้าออนไลน์

มิจฉาชีพมักสร้างเพจปลอมบนแพลตฟอร์มออนไลน์ โดยนำภาพสินค้าจากร้านค้าจริงมาใช้ แล้วตั้งราคาถูกกว่าท้องตลาด เพื่อดึงดูดความสนใจของผู้สูงอายุ นอกจากนี้ยังใช้ข้อความเร่งรัด เช่น โปรโมชั่นวันสุดท้าย หรือ สินค้าเหลือจำนวนจำกัด เพื่อให้รีบตัดสินใจซื้อโดยไม่ทันตรวจสอบ เมื่อผู้เสียหายหลงเชื่อและโอนเงินเข้าบัญชีส่วนตัว มิจฉาชีพจะปิดเพจหรือปิดช่องทางการติดต่อทันที ทำให้ไม่ได้รับสินค้าและไม่สามารถติดตามตัวได้ ตัวอย่างเช่น

(๑) ใช้ของราคาถูกล่อใจ
(๒) สร้างความเร่งรีบให้รีบตัดสินใจ
(๓) ตอบแชทสุภาพ สร้างความน่าเชื่อถือ
(๔) หลอกให้โอนเงินก่อนตรวจสอบร้านค้า

๒. หลอกลงทุน

มิจฉาชีพมักอ้างตัวเป็นผู้เชี่ยวชาญด้านการเงิน ชักชวนลงทุนผ่านไลน์หรือเฟซบุ๊ก พร้อมโชว์ภาพกำไร รีวิว หรือบัญชีปลอมเพื่อสร้างความน่าเชื่อถือในช่วงแรกอาจให้ถอนกำไรได้จริง เพื่อสร้างความไว้ใจก่อนชักชวนให้ลงทุนเพิ่มทีละมาก ๆ โดยอ้างว่าเป็น โอกาสพิเศษ หรือ ลงทุนรอบสุดท้าย และสุดท้ายเมื่อเหยื่อโอนเงินจำนวนมาก มิจฉาชีพจะเริ่มติดต่อไม่ได้ และปิดช่องทางหนีทันที ตัวอย่างเช่น

(๑) สร้างภาพเป็นผู้เชี่ยวชาญ
(๒) ใช้รีวิวและกำไรปลอม
(๓) ให้ได้ผลตอบแทนจริงในช่วงแรก
(๔) หลอกให้ลงทุนเพิ่มเรื่อย ๆ

/๓. หลอกให้รัก...

๓. หลอกให้รัก (Romance Scam)

มิจฉาชีพมักใช้รูปโปรไฟล์ปลอม เช่น ทหาร แพทย์ นักธุรกิจ หรือชาวต่างชาติ เข้ามาพูดคุยตีสนิทผ่านแอปพลิเคชันแชทในช่วงแรกจะพูดจาเอาใจ ใส่ใจ และติดต่อสม่ำเสมอ เพื่อสร้างความผูกพันทางจิตใจ เมื่อเหยื่อเริ่มไว้ใจ จึงเริ่มอ้างปัญหาต่าง ๆ เช่น ป่วย อุบัติเหตุ เงินไม่พอ หรือส่งของมาให้แต่ติดค่าศุลกากร พร้อมขอให้โอนเงินช่วยเหลือ หลายคนสูญเงินจำนวนมาก เพราะเชื่อว่ากำลังช่วยเหลือคนที่รักและไว้ใจ ตัวอย่างเช่น

(๑) สร้างตัวตนปลอมให้น่าเชื่อถือ
(๒) ใช้เวลาสร้างความสัมพันธ์
(๓) ทำให้เหยื่อรู้สึกสำคัญ
(๔) ใช้อารมณ์และความสงสารหลอกเงิน

๔. หลอกให้กลัว หรือแก๊งคอลเซ็นเตอร์

หนึ่งในภัยไซเบอร์ที่สร้างความเสียหายมากที่สุด คือ การแอบอ้างเป็นเจ้าหน้าที่รัฐ ตำรวจ ธนาคาร หรือหน่วยงานราชการ มิจฉาชีพมักโทรศัพท์มาแจ้งว่า ผู้เสียหายมีส่วนเกี่ยวข้องกับคดีฟอกเงิน บัญชีผิดกฎหมาย หรือทุจริตเงินสวัสดิการ พร้อมใช้ข้อมูลส่วนตัวจริง เช่น ชื่อ–นามสกุล หรือเลขบัตรประชาชน เพื่อสร้างความน่าเชื่อถือจากนั้นจะเร่งให้โอนเงินเพื่อตรวจสอบบัญชี หรือส่งเอกสารปลอมที่มีตราครุฑผ่านไลน์ เพื่อให้เกิดความกลัวจนรีบทำตามโดยไม่ทันตรวจสอบ ตัวอย่างเช่น

(๑) แอบอ้างหน่วยงานรัฐ
(๒) ใช้ข้อมูลจริงสร้างความน่าเชื่อถือ
(๓) ใช้ความกลัวและความกดดัน
(๔) เร่งให้รีบตัดสินใจทันที

๕. หลอกขายยา อาหารเสริม และประกันสุขภาพ

มิจฉาชีพมักโฆษณาอาหารเสริมหรือยารักษาโรคผ่านเฟซบุ๊ก ยูทูบ หรือไลน์ โดยกล่าวอ้างว่าสามารถรักษาโรคเรื้อรังได้ พร้อมใช้ภาพบุคคลแต่งกายคล้ายแพทย์ หรืออ้างผลวิจัยทางการแพทย์ปลอม บางกรณียังใช้รีวิวปลอมจากผู้สูงอายุ และโปรโมชั่นจำกัดเวลา เพื่อเร่งให้รีบซื้อทันที เมื่อได้รับสินค้า อาจเป็นสินค้าที่ไม่มีคุณภาพ ไม่มีเลข อย. หรืออาจเป็นอันตรายต่อสุขภาพ ตัวอย่างเช่น

(๑) ใช้ความกังวลเรื่องสุขภาพเป็นจุดอ่อน
(๒) แอบอ้างบุคลากรทางการแพทย์
(๓) ใช้รีวิวปลอมสร้างความน่าเชื่อถือ
(๔) เร่งให้รีบซื้อผ่านโปรโมชั่นพิเศษ

๖. หลอกรับสวัสดิการผู้สูงอายุ

มิจฉาชีพมักส่ง SMS หรือข้อความไลน์แอบอ้างเป็นหน่วยงานราชการ แจ้งว่าผู้สูงอายุมีสิทธิได้รับเงินช่วยเหลือเพิ่มเติม หรือได้รับสิทธิเบี้ยยังชีพเพิ่ม ในข้อความจะมีลิงก์ปลอมให้กด ยืนยันสิทธิ หรืออัปเดตข้อมูล เมื่อกดเข้าไปจะให้กรอกข้อมูลส่วนตัว เลขบัญชี หรือรหัส OTP บางกรณีอาจอ้างว่าต้องโอนค่าธรรมเนียมก่อนรับเงิน สุดท้ายผู้เสียหายอาจสูญเสียเงินในบัญชี หรือข้อมูลส่วนตัวถูกนำไปใช้ในทางทุจริต ตัวอย่างเช่น

(๑) แอบอ้างโครงการช่วยเหลือจากภาครัฐ
(๒) ใช้เรื่องเงินสวัสดิการล่อใจ
(๓) ส่งลิงก์ปลอมเพื่อขโมยข้อมูล
(๔) หลอกขอ OTP หรือข้อมูลธนาคาร

/จากตัวอย่าง...

จากตัวอย่างภัยไซเบอร์ที่เกิดขึ้นในปัจจุบัน จะเห็นได้ว่ามิจฉาชีพมีการพัฒนาวิธีการหลอกลวงให้แนบเนียน ซับซ้อน และเข้าถึงผู้คนได้ง่ายมากยิ่งขึ้น ทั้งการแอบอ้างเป็นเจ้าหน้าที่รัฐ การสร้างเรื่องเร่งด่วนให้เกิดความตกใจ หรือแม้แต่การใช้ความไว้ใจและความสงสารเป็นเครื่องมือในการหลอกเอาเงินและข้อมูลส่วนตัวจากผู้เสียหายหลายครั้ง ความเสียหายอาจเริ่มต้นจากเพียง "การรีบเชื่อ" หรือ "การด่วนตัดสินใจโดยไม่ทันตรวจสอบ" การรู้เท่าทันกลโกงของมิจฉาชีพ และการมีสติก่อนดำเนินการทุกครั้ง จึงเป็นเกราะป้องกันสำคัญที่จะช่วยลดความเสี่ยงจากภัยออนไลน์ได้อย่างมีประสิทธิภาพ

กรมส่งเสริมการปกครองท้องถิ่นจึงขอแนะนำ "คาถาป้องกันภัยไซเบอร์" หลักคิดง่าย ๆ ที่ประชาชนทุกวัย โดยเฉพาะผู้สูงอายุ สามารถจดจำและนำไปใช้ได้จริงในชีวิตประจำวัน เพื่อสร้างภูมิคุ้มกันทางดิจิทัลและป้องกันตนเองจากมิจฉาชีพออนไลน์ ภายใต้หลักสำคัญ ๓ คำสั้น ๆ คือ "ไม่เชื่อ ไม่รีบ ไม่โอน"

"ไม่เชื่อ" อย่าหลงเชื่อทันที เมื่อมีผู้ติดต่อมาแจ้งข่าวที่ทำให้ตกใจ กลัว หรือดีใจเกินจริง ควรตรวจสอบข้อมูลกับหน่วยงานที่เกี่ยวข้องโดยตรงทุกครั้ง

"ไม่รีบ" มิจฉาชีพมักสร้างสถานการณ์เร่งด่วนเพื่อไม่ให้มีเวลาคิด ควรตั้งสติ หยุดคิด และปรึกษาคนในครอบครัวก่อนดำเนินการใด ๆ

"ไม่โอน" ไม่โอนเงินให้บุคคลที่ยังไม่ได้รับการยืนยันตัวตน และไม่เปิดเผยข้อมูลสำคัญ เช่น รหัส OTP เลขบัตรประชาชน หรือข้อมูลบัญชีธนาคารแก่ผู้อื่นเด็ดขาด

กรมส่งเสริมการปกครองท้องถิ่นมุ่งมั่นส่งเสริมความรู้ด้านการป้องกันภัยไซเบอร์แก่ประชาชน เพื่อสร้างภูมิคุ้มกันทางดิจิทัล ลดความสูญเสียจากภัยออนไลน์ และร่วมสร้างสังคมไทยให้ปลอดภัยจากอาชญากรรมทางไซเบอร์ โดยเฉพาะในกลุ่มผู้สูงอายุที่ควรได้รับการดูแลและเข้าถึงข้อมูลอย่างเท่าทัน

บรรณานุกรม

กรมกิจการผู้สูงอายุ. (2567). คู่มือรับมือภัยไซเบอร์สำหรับผู้สูงอายุ. สืบค้นจาก https://www.dop.go.th/th/news/1/5035

ธนาคารไทยพาณิชย์. (2567). ภัยหลอกลวงผู้สูงอายุที่ควรระวัง. สืบค้นจาก https://www.scb.co.th/th/personal-banking/fraud-fighter/update-fraud/scams-elderly

ธัญพิชชา สามารถ. (2565). การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ (วิทยานิพนธ์ปริญญามหาบัณฑิต). จุฬาลงกรณ์มหาวิทยาลัย, กรุงเทพฯ. สืบค้นจาก https://digital.car.chula.ac.th/chulaetd/6716

The Reporter. (2567). ภัยไซเบอร์กับผู้สูงอายุ: ทำไมผู้สูงวัยจึงตกเป็นเป้าหมายของมิจฉาชีพออนไลน์. สืบค้นจาก https://today.line.me/th/v3/article/XY8g5GZ

องค์การบริหารส่วนตำบลบุรีรัมย์. (2567). ประชาสัมพันธ์ภัยไซเบอร์และแนวทางป้องกันภัยออนไลน์. สืบค้นจาก https://www.buriramlocal.go.th/public/list/data/detail/id/16291/menu/1554/page/1

บทความ

คู่มือเอาตัวรอดของวัยทำงาน บริหารความเสี่ยงแบบมืออาชีพ รู้ทันกลลวง ของอาชญากรทางไซเบอร์

ในยุคปัจจุบันที่เทคโนโลยีสารสนเทศและการสื่อสารก้าวเข้ามาเป็นส่วนหนึ่งในชีวิตประจำวันอย่างหลีกเลี่ยงไม่ได้ นวัตกรรมและเทคโนโลยีต่างๆ ได้เข้ามาช่วยอำนวยความสะดวกในการขับเคลื่อนทางเศรษฐกิจและการดำเนินชีวิตของประชาชนเป็นอย่างมาก แต่อย่างไรก็ตาม เมื่อความสะดวกสบายทางดิจิทัลเพิ่มมากขึ้นสิ่งที่เกิดขึ้นตามมา คือ อาชญากรรมทางไซเบอร์ ซึ่งมีวิวัฒนาการรูปแบบกลโกงที่ซับซ้อนและยากต่อการตรวจจับ

คนส่วนใหญ่มักเข้าใจว่า ผู้ที่ตกเป็นเหยื่อของมิจฉาชีพทางออนไลน์ส่วนใหญ่ คือ กลุ่มเด็กและเยาวชนที่ยังขาดประสบการณ์ชีวิต หรือกลุ่มผู้สูงอายุที่ตามไม่ทันเทคโนโลยี แต่จากสถิติของศูนย์รับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ และรายงานสถานการณ์ภัยไซเบอร์ในประเทศไทย ปรากฏข้อเท็จจริงว่า กลุ่มประชากรที่ตกเป็นเหยื่อและสร้างมูลค่าความเสียหายทางเศรษฐกิจสูงที่สุด คือ กลุ่มคนวัยทำงานหรือวัยผู้ใหญ่ที่มีช่วงอายุระหว่าง ๓๐ ถึง ๔๔ ปี เป็นกลุ่มที่มีจำนวนผู้เสียหายมากที่สุด เนื่องจากเป็นช่วงวัยที่มีรายได้และทรัพย์สินมั่นคง

คนวัยทำงาน คือ ฟันเฟืองชิ้นสำคัญที่สุดในการขับเคลื่อนเศรษฐกิจ เป็นผู้ที่มีรายได้ มีเงินเก็บ มีเครดิตทางธุรกรรมและที่สำคัญที่สุดคือเป็นเสาหลักของครอบครัว การที่คนกลุ่มนี้ตกเป็นเป้าหมายหลักของอาชญากรไซเบอร์จึงมิใช่เรื่องบังเอิญ แต่เกิดจากการที่มิจฉาชีพเล็งเห็นถึงผลประโยชน์มหาศาลที่สามารถดึงเอาไปจากเหยื่อกลุ่มนี้ได้ บทความนี้มุ่งวิเคราะห์เจาะลึกถึงภัยเงียบที่คุกคามคนวัยทำงาน เหตุผลทางจิตวิทยาและสังคมที่ทำให้คนกลุ่มนี้เปราะบางที่สุด ตลอดจนถอดบทเรียนจากคดีที่เคยเกิดขึ้นจริงในประเทศไทย เพื่อเป็นแนวทางในการสร้างภูมิคุ้มกันและตระหนักรู้เท่าทันภัยไซเบอร์อย่างยั่งยืน

๑. สาเหตุที่วัยทำงาน เป็นกลุ่มเป้าหมายที่น่ากลัวและน่าเป็นห่วงที่สุดสามารถวิเคราะห์สาเหตุและปัจจัยความเสี่ยงได้ดังนี้

๑.๑ มิติทางเศรษฐกิจ ที่เสียหายสูงที่สุดและอาจนำไปสู่สภาวะหนี้สินท่วมหัว

วัยเด็กอาจสูญเสียเพียงเงินค่าขนมหลักร้อยหรือหลักพัน ขณะที่วัยผู้สูงอายุอาจสูญเสียเงินเก็บก้อนสุดท้าย แต่วัยทำงานมีความน่ากลัวที่แตกต่างออกไป เนื่องจากเป็นกลุ่มคนที่มีเครดิตทางการเงินสูงที่สุด มีวงเงินบัตรเครดิต มีแอปพลิเคชันธนาคารที่ผูกกับบัญชีเงินเดือน และมีความสามารถในการอนุมัติสินเชื่อ มิจฉาชีพยุคปัจจุบันจึงไม่ได้หยุดอยู่แค่การหลอกเอาเงินในบัญชีจนเหลือศูนย์บาท แต่จะใช้จิตวิทยาบีบคั้น หรือล่อลวงให้เหยื่อ ไปกู้หนี้ยืมสินมาโอนเพิ่ม เช่น การหลอกให้ทำภารกิจหรือลงทุนเพิ่มเพื่อถอนเงินก้อนเก่าออก เหยื่อวัยทำงานจำนวนมากจึงยอมรูดบัตรเครดิตจนเต็มวงเงิน นำรถยนต์เข้าไฟแนนซ์ หรือแม้กระทั่งนำโฉนดบ้านไปจำนอง ผลกระทบของกลุ่มวัยนี้ จึงไม่ใช่เพียงแค่การหมดตัว แต่คือการติดลบและทำให้มีหนี้สินผูกพันระยะยาว

๑.๒ มิติทางสังคม ผลกระทบลูกโซ่ต่อผู้พึ่งพิง

คนวัยทำงาน คือ ประชากรกลุ่มที่เป็นเหมือนศูนย์กลางของครอบครัว ซึ่งต้องรับผิดชอบค่าใช้จ่ายของกลุ่มคนถึง ๓ ช่วงวัย ได้แก่ การเลี้ยงดูบุตร ซึ่งเป็นวัยเด็ก และการดูแลพ่อแม่ ซึ่งเป็นวัยสูงอายุ รวมไปถึงค่าใช้จ่ายส่วนตัว เช่น ค่าผ่อนที่อยู่อาศัย และค่าผ่อนรถยนต์ เมื่อเสาหลักของบ้านถูกมิจฉาชีพปล้นเงินไปทางอากาศ ระบบการเงินของครอบครัวจะพังทลายลงทันที บุตรอาจจะต้องออกจากระบบการศึกษา เนื่องจากผู้ปกครองไม่มีเงินจ่ายค่าเทอม พ่อแม่ในวัยชราอาจจะขาดแคลนยารักษาโรค และทรัพย์สินที่สร้างมาด้วยน้ำพักน้ำแรงอาจถูกยึด ความเสียหายที่เกิดขึ้นกับคนวัยทำงานเพียงแค่หนึ่งคน จึงส่งผลกระทบโดยตรงต่อคุณภาพชีวิตของสมาชิกในครอบครัวหรือกลุ่มวัยอื่นๆ อย่างหลีกเลี่ยงไม่ได้

/๑.๓ มิติทางจิตวิทยา...

๑.๓ มิติทางจิตวิทยากับดักเรื่องศักดิ์ศรี และความลับ

คนวัยทำงานมักมีความมั่นใจในตัวเองสูง เนื่องจากเชื่อว่าตนเองมีความรู้ความเข้าใจในเทคโนโลยีและข่าวสารบ้านเมืองเป็นอย่างดี ความมั่นใจนี้บางครั้งทำให้ขาดความระมัดระวัง อีกทั้งเมื่อตกเป็นเหยื่อแล้วสิ่งที่ตามมา คือ ความอับอายและกลัวเสียชื่อเสียง ไม่ว่าจะเป็นกลัวเพื่อนร่วมงานดูถูก กลัวผู้บังคับบัญชามองว่าขาดวุฒิภาวะอันอาจส่งผลต่อความก้าวหน้าในหน้าที่การงาน หรือกลัวครอบครัวผิดหวังกับดักทางจิตวิทยานี้ทำให้เหยื่อวัยทำงานเลือกที่จะปิดบังความจริง และพยายามแก้ปัญหาเพียงลำพัง ซึ่งเข้าทางของมิจฉาชีพ ที่มักจะใช้ความลับนี้ในการข่มขู่เพื่อเรียกร้องเอาเงินเพิ่ม หรือล่อลวงให้โอนเงินเพิ่มเพื่อเคลียร์คดี กว่าที่เหยื่อจะยอมเปิดเผยความจริงหรือเข้าแจ้งความ เงินก็ถูกโอนย้ายผ่านบัญชีม้าออกไปนอกประเทศจนยากเกินจะเยียวยา

๑.๔ มิติทางวิถีชีวิต ความเร่งรีบ และความเหนื่อยล้า

วิถีชีวิตของคนทำงานในปัจจุบันเต็มไปด้วยความเร่งรีบและความเครียดจากการทำงานในแต่ละวันต้องจัดการกับอีเมล ข้อความ และธุรกรรมจำนวนมาก มิจฉาชีพจึงอาศัยช่องว่างนี้ในการส่งลิงก์ปลอมหรือโทรศัพท์เข้ามาหาเหยื่อในช่วงเวลาที่กำลังยุ่งล้นมือ หรือช่วงเวลาที่ร่างกายและสมองเกิดความเหนื่อยล้า เช่น ช่วงบ่ายของการทำงานหรือช่วงค่ำหลังเลิกงาน ส่งผลให้ความสามารถในการคิดวิเคราะห์และคัดกรองหรือกลั่นกรองข้อมูลลดลงอย่างมาก

๒. กลวิธี ที่อาชญากรทางไซเบอร์ มักจะใช้เพื่อโจมตีคนวัยทำงาน

มิจฉาชีพมีการออกแบบสคริปต์และวิธีการหลอกลวงที่สอดคล้องกับพฤติกรรมและความต้องการของคนวัยทำงานอย่างเป็นระบบ โดยมีรูปแบบที่พบบ่อยและสร้างความเสียหายรุนแรง ดังนี้

๒.๑ กลโกงแอปพลิเคชันดูดเงิน มิจฉาชีพจะส่งข้อความปลอม โดยอ้างว่าเป็นหน่วยงานของรัฐหรือองค์กรใหญ่ ชวนเชื่อเรื่องสิทธิประโยชน์หรือการตรวจสอบข้อมูล เมื่อเหยื่อหลงเชื่อกดลิงก์และติดตั้งไฟล์แปลกปลอม โทรศัพท์มือถือจะถูกควบคุมจากระยะไกลโดยมิจฉาชีพ หลังจากนั้น หน้าจอโทรศัพท์มือถือจะขึ้นแสดงผลว่า โทรศัพท์มือถือกำลังอัปเดตห้ามปิดเครื่องเด็ดขาด ระหว่างนั้น มิจฉาชีพจะเจาะรหัสเข้าไปในบัญชีธนาคารบนมือถือของเหยื่อ และโอนเงินออกไปจนหมดสิ้น

๒.๒ แก๊งคอลเซ็นเตอร์อ้างหน่วยงานบังคับใช้กฎหมาย การโทรศัพท์สวมรอยเป็นเจ้าหน้าที่กรมสอบสวนคดีพิเศษ หรือ สำนักงานป้องกันและปราบปรามการฟอกเงิน แจ้งว่าบัญชีธนาคารของเหยื่อพัวพันกับการฟอกเงินหรือยาเสพติด โดยเน้นที่การข่มขู่ให้เกิดความกลัวและบังคับให้โอนเงินมาตรวจสอบ

๒.๓ หลอกลงทุนและทำงานออนไลน์ การหลอกให้ทำภารกิจเสริม เช่น ถูกใจบทความ รีวิวสินค้า หรือการหลอกให้รักแล้วชวนลงทุนในแอปพลิเคชันเทรดสินทรัพย์ดิจิทัลปลอม โดยใช้ผลตอบแทนสูงในช่วงแรกเป็นเหยื่อล่อ เพื่อให้เหยื่อหลงกลและลงทุนเพิ่มเป็นจำนวนมากก่อนที่จะปิดช่องทางการติดต่อไป

๒.๔ ภัยแบล็กเมล์ทางเพศและการข่มขู่กรรโชกทรัพย์ การใช้โปรไฟล์ปลอมเข้ามาตีสนิทเชิงชู้สาว นำไปสู่การวิดีโอคอลแบบลับเฉพาะ จากนั้นแอบบันทึกภาพและวิดีโอมาข่มขู่กรรโชกทรัพย์เหยื่อ เพื่อแลกเปลี่ยนเงินกับการที่จะไม่ส่งคลิปไปให้คนในที่ทำงานหรือคนในครอบครัวของเหยื่อ

๒.๕ เพจขื้อสินค้าและบริการท่องเที่ยวปลอม การสร้างเพจเฟซบุ๊กปลอมเลียนแบบโรงแรมหรูแล้วลงโฆษณาลดราคาสูง ภายในช่วงระยะเวลาที่จำกัดเพื่อกดดันให้ เหยื่อ รีบทำการจองหรือโอนเงินมัดจำ

๓. เหตุการณ์จริงที่เกิดขึ้นในประเทศไทย ซึ่งแสดงให้เห็นถึงกลยุทธ์ของมิจฉาชีพและมูลค่าความเสียหายที่เกิดขึ้นจริงกับกลุ่มวัยทำงาน ดังนี้

เหตุการณ์ที่ ๑ มหันตภัยแอปพลิเคชันดูดเงินสายการบินชื่อดัง

เหยื่อซึ่งเป็นนักธุรกิจและคนทำงานกลุ่มหนึ่ง ได้รับข้อความ แอบอ้าง ชื่อสายการบินแห่งหนึ่ง ที่มีเนื้อหาแจ้งว่า เหยื่อ ได้รับมอบตั๋วเครื่องบินฟรี เนื่องในโอกาสพิเศษ โดยให้กดลิงก์เพื่อดาวน์โหลดแอปพลิเคชันมาลงทะเบียนรับสิทธิ์ โดย เมื่อเหยื่อกดลิงก์ ระบบจะหลอกให้ติดตั้งไฟล์ที่สามารถควบคุมหน้าจอโทรศัพท์มือถือจากระยะไกลได้ หน้าจอโทรศัพท์ของเหยื่อจะเกิดอาการค้างหรือขึ้นข้อความว่า กำลังอัปเดตระบบ ห้ามปิดเครื่อง ในระหว่างนั้น มิจฉาชีพได้ทำการเจาะรหัสเข้าแอปพลิเคชันธนาคารและโอนเงินออกจากบัญชีจนหมดเกลี้ยง[๓]

เหตุการณ์ที่ ๒ แก๊งคอลเซ็นเตอร์แอบอ้างเป็นเจ้าหน้าที่ ข่มขู่ข้าราชการและบุคลากรทางการแพทย์

มิจฉาชีพโทรศัพท์หาแพทย์หญิงและข้าราชการระดับสูงรายหนึ่ง แอบอ้างเป็นเจ้าหน้าที่ไปรษณีย์แจ้งว่า พบกล่องพัสดุตกค้าง ที่ภายในบรรจุพาสปอร์ตปลอมและสมุดบัญชีธนาคารผิดกฎหมาย โดย คนร้ายส่งภาพหมายจับปลอมที่มีชื่อและนามสกุลจริงของเหยื่อ มาให้ดูทางแอปพลิเคชันไลน์ พร้อมข่มขู่ว่าหากต้องการพิสูจน์ความบริสุทธิ์ เหยื่อ จะต้องโอนเงินจากทุกบัญชีที่มีมารวมกันไว้ที่บัญชีกลางของเจ้าหน้าที่ ด้วยความตระหนกตกใจและกลัวกระทบต่อตำแหน่งหน้าที่การงาน เหยื่อจึงยินยอมโอนเงินไปรวมกว่า ๒๐ ครั้ง รวมมูลค่ากว่า ๖๐ ล้านบาท[๒]

เหตุการณ์ที่ ๓ คดีหลอกลวงลงทุนฟาร์มเห็ด

บริษัทเอกชนแห่งหนึ่งได้ทำการโฆษณาผ่านสื่อมวลชนและผู้ที่มีชื่อเสียงโด่งดัง เชิญชวนผู้ที่มีเงินเก็บมาร่วมลงทุนในโครงการเกษตรกรรมยุคใหม่ เช่น การปลูกเห็ดนางฟ้า การเลี้ยงผึ้ง และการปลูกกัญชา โดยที่ผู้ลงทุนไม่จำเป็นต้องมีความรู้ ความเชี่ยวชาญหรือลงแรงเอง เนื่องจากมีทีมงานบริหารจัดการให้ทั้งหมด ขบวนการนี้สัญญาว่าจะให้เงินปันผลที่สูง ในช่วงแรกเหยื่อได้รับเงินปันผลจริงตามกำหนด ทำให้หลงเชื่อ จึงนำเงินเก็บทั้งหมดที่มีไปลงทุนเพิ่ม พร้อมทั้งชักชวนคนรู้จักมาร่วมลงทุนด้วย สุดท้ายเมื่อระดมทุนได้จำนวนมาก บริษัทก็ได้ประกาศปิดตัวและทีมผู้บริหารได้เดินทางหลบหนีออกนอกประเทศไปมูลค่าความเสียหายที่เกิดจากคดีนี้รวมแล้วมากกว่า ๒,๐๐๐ ล้านบาท [๓]

เหตุการณ์ที่ ๔ ขบวนการหลอกให้รักแล้วชวนลงทุนสินทรัพย์ดิจิทัล

ผู้หญิงวัย ๔๐ ปี ได้รับข้อความทักทาย จากนักธุรกิจชาวต่างชาติ ผ่านทางแอปพลิเคชันหาคู่ โดยได้ใช้เวลาพูดคุยสร้างความสัมพันธ์ห่วงใยในชีวิตประจำวันนานนับเดือน จนเกิดความไว้วางใจและพัฒนาความสัมพันธ์เป็นความรักออนไลน์ เมื่อผู้หญิงคนดังกล่าว เริ่มปักใจเชื่อ คนร้ายได้ชักชวนให้ลงทุนในแพลตฟอร์มการเทรดเหรียญดิจิทัล ปลอมที่คนร้ายสร้างขึ้น โดยอ้างว่า เป็นช่องทางสร้างความมั่นคงเพื่อสร้างอนาคตและเตรียมพร้อมสำหรับใช้ในการแต่งงานร่วมกัน เหยื่อหลงเชื่อโอนเงินไปลงทุนเพิ่มทีละน้อย และเห็นตัวเลขกำไรพุ่งสูงขึ้นบนหน้าจอ จึงยอมนำเงินเก็บทั้งหมดรวมถึงการนำบ้านและรถยนต์ไปจำนองเพื่อหาเงินมาเติมในระบบสุดท้ายเมื่อต้องการถอนเงิน ระบบแจ้งว่าต้องจ่ายภาษีเพิ่ม และคนร้ายได้ปิดช่องทางการติดต่อหนีไป[๔]

/เหตุการณ์ที่ ๕...

---

[๑] ข้อมูลจาก กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กรณีจับกุมเครือข่ายแอปพลิเคชันดูดเงินแอบอ้าง สายการบิน เมื่อวันที่ ๘ กรกฎาคม พ.ศ. ๒๕๖๖

[๒] ข้อมูลจาก กรมสอบสวนคดีพิเศษ และสำนักงานตำรวจแห่งชาติ เมื่อวันที่ ๓๑ มีนาคม พ.ศ. ๒๕๖๕

[๓] ข้อมูลจาก ศาลอาญา คดีหมายเลขแดง ที่ อ.๓๘๕๗/๒๕๖๖ พิพากษาเมื่อวันที่ ๑๙ ธันวาคม พ.ศ. ๒๕๖๖

[๔] ข้อมูลจาก กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี และสมาคมธนาคารไทย ได้เปิดเผยรายละเอียดคดีนี้เพื่อเป็นอุทาหรณ์เตือนภัยรูปแบบกลโกงแบบหลอกให้อ้วนแล้วเชือด เมื่อวันที่ ๑๖ พฤศจิกายน พ.ศ. ๒๕๖๖

เหตุการณ์ที่ ๕ ขบวนการขู่กรรโชกทรัพย์พนักงานออฟฟิศและวิศวกร

มิจฉาชีพ ใช้บัญชีผู้ใช้ปลอม เป็นหญิงสาวหน้าตาดี ส่งข้อความเข้ามาเพื่อพูดคุยในเชิงชู้สาว เมื่อความสัมพันธ์เริ่มสนิทสนม คนร้ายได้ชวนเปิดกล้องวิดีโอคอลเพื่อทำกิจกรรมทางเพศออนไลน์ โดยคนร้ายได้ทำการบันทึกหน้าจอ ที่เห็นใบหน้าของเหยื่อและพฤติกรรมส่วนตัวอย่างชัดเจน จากนั้นได้เปลี่ยนท่าทีเป็นข่มขู่ทันที โดย ยื่นคำขาดว่าถ้าหากไม่โอนเงินให้จะส่งคลิปดังกล่าว ไปให้ภรรยาและบริษัทของเหยื่อ ดูข้อมูลจากแหล่งข่าวของกองบัญชาการสอบสวนกลาง เมื่อวันที่ ๑๕ กุมภาพันธ์ พ.ศ. ๒๕๖๗ ยืนยันสถิติคดีกรรโชกทรัพย์ในลักษณะนี้ว่ามีแนวโน้มที่จะเพิ่มสูงขึ้นในกลุ่มของคนวัยทำงานที่ต้องการความเป็นส่วนตัว แต่ยังขาดความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์

๔. มาตรการป้องกันและแนวทางการแก้ไขปัญหา

การรับมือกับภัยไซเบอร์สำหรับคนวัยทำงานหรือวัยผู้ใหญ่ จำเป็นต้องใช้มาตรการ สร้างภูมิคุ้มกันทางดิจิทัล ผสานเข้ากับการบังคับใช้กลยุทธ์เตือนใจเพื่อระงับและยับยั้งพฤติกรรมที่มีความเสี่ยง โดยแนวทาง ที่มีประสิทธิภาพสูงมากที่สุด คือ การบังคับใช้คาถาป้องกันภัย **ไม่เชื่อ ไม่รีบ ไม่โอน** ซึ่งถือเป็นเกราะป้องกันด่านแรกที่สั้น กระชับ และสามารถตัดวงจรอัตโนมัติทางจิตวิทยาที่มิจฉาชีพพยายามสร้างขึ้นได้อย่างทันที

ไม่เชื่อ คือ การวางรากฐานทางความคิดที่ไม่เชื่อหรือไม่ไว้วางใจสิ่งใดในโลกออนไลน์เอาไว้ก่อน ไม่ว่าจะเป็นสายโทรศัพท์ลึกลับ ข้อความ ลิงก์แนบ หรือโปรไฟล์คนหน้าตาดี ให้ตระหนักเสมอว่าหน่วยงานรัฐและสถาบันการเงินที่ถูกต้องตามกฎหมาย ไม่มีนโยบายการติดต่อประชาชนผ่านทางข้อความโทรศัพท์มือถือเพื่อให้กดลิงก์ดาวน์โหลดแอปพลิเคชัน และไม่มีนโยบายการให้โอนเงินมาตรวจสอบ ในทุกกรณี

ไม่รีบ เนื่องจาก มิจฉาชีพเกลียดการรอคอยและการมีสติของเหยื่อ ทุกวิธีการของคนร้ายมักจะถูกออกแบบมา ให้เหยื่อเกิดความตื่นตระหนกและเร่งรัดให้ทำธุรกรรมในทันที ดังนั้น เมื่อไหร่ก็ตามที่รู้สึกว่ากำลังถูกเร่งรัด ให้ใช้วิธีการ ตัดบท วางสายชั่วคราว เพื่อขอเวลาหายใจและทบทวนข้อมูลอีกครั้ง โดยที่การหยุดคิดจะช่วยให้สมองส่วนหน้ากลับมาทำงานอย่างมีเหตุผลอีกครั้ง

ไม่โอน คือ กฎเหล็กข้อสุดท้ายและสำคัญที่สุด เนื่องจาก เป็นการรักษาอำนาจการควบคุมเงินไว้ในมือของตนเอง ตราบใดที่เงินยังอยู่ในบัญชีธนาคาร มิจฉาชีพ จะไม่สามารถทำอันตรายใดๆ ต่อตัวเราได้ โดยที่จะต้องห้ามโอนเงิน ห้ามบอกรหัสผ่าน ห้ามบอกรหัสพิน ๖ หลักให้กับผู้อื่นเด็ดขาด

จึงสรุปได้ว่า อาชญากรรมทางไซเบอร์ในยุคปัจจุบันมิใช่เพียงแค่ปัญหาภัยส่วนบุคคลอีกต่อไป แต่ได้ยกระดับขึ้นเป็น ภัยความมั่นคงระดับชาติ ที่ทำลายเสถียรภาพทางเศรษฐกิจและโครงสร้างสถาบันครอบครัวอย่างรุนแรง จากข้อมูลทั้งหมดจะเห็นได้ชัดเจนว่า กลุ่มคนวัยทำงานหรือวัยผู้ใหญ่เป็นกลุ่มคนที่ต้องเผชิญหน้ากับความน่ากลัวและความอันตรายจากภัยเงียบนี้มากที่สุด เนื่องจาก เป็นมนุษย์กลุ่มเดียวในสังคมที่มีแรงขับเคลื่อนทางทรัพย์สิน มีเครดิตทางการเงิน และแบกรับภาระความกดดัน ในฐานะเสาหลักของครอบครัวเอาไว้ มิจฉาชีพจึงพุ่งเป้าโจมตีไปที่จุดอ่อนทางจิตวิทยา ทั้งความโลภ ความกลัว และความอาย เพื่อสั่นคลอนสติสัมปชัญญะของคนวัยนี้

การแก้ไขปัญหาที่ยั่งยืน จึงต้องอาศัยกลไกการร่วมมือกันของสังคมทุกภาคส่วน ได้แก่ ภาครัฐ ภาคเอกชน และภาคประชาชน โดย การกระจายองค์ความรู้และสร้างความตระหนักรู้ให้เข้าถึงประชาชนในทุกชุมชน และสิ่งที่สำคัญที่สุด คือ การเปลี่ยนผ่านจาก ความตื่นตระหนก ไปสู่ ความตระหนักรู้ โดยที่คนวัยทำงานทุกคนจำเป็นต้องพึงระลึกอยู่เสมอว่า ในโลกดิจิทัลที่ทุกสิ่งขับเคลื่อนด้วยความเร็วสูง การหยุดคิดและหยั่งรากอยู่บนความไม่ประมาทผ่านคาถา **"ไม่เชื่อ ไม่รีบ ไม่โอน"** จะเป็นเกราะกำบังทางไซเบอร์ที่มีประสิทธิภาพสูงสุดในการปกป้องเงินทอง หน้าที่การงาน และความสุขของคนที่เรารักหรือคนในครอบครัวให้รอดพ้นจากอาชญากรทางไซเบอร์ได้อย่างปลอดภัยอย่างแท้จริง

บรรณานุกรม

ไทยรัฐออนไลน์. (2566). อ้างไลอ้อนแอร์ หลอกดูดเงินในบัญชี ทำลิงก์ปลอมให้กด เหยื่อสูญกว่า 150 ล้านบาท. สืบค้นจาก https://www.thairath.co.th/news/crime/2650801

ข่าวสดออนไลน์. (2566). ตร.ไซเบอร์ แจงอ้างเป็นจนท.ไทยไลอ้อนแอร์ หลอกกดลิ้งก์ดูดเงิน-แจกตั๋วฟรี เสียหาย 150 ล้าน. สืบค้นจาก https://www.khaosod.co.th/around-thailand/news_7756291

เดลินิวส์. (2566). จับผัวเมียรับจ้างเปิดบัญชีม้าให้แก๊งคอลเซ็นเตอร์ ใช้ตุ่น 'หมอ-นักธุรกิจ' สูญ 143 ล้าน. สืบค้นจาก https://www.dailynews.co.th/news/2229100/

สำนักข่าวอิศรา. (2565). แฉกลโกงคอลเซ็นเตอร์อ้าง DSI หลอกแพทย์หญิงโอนเงินอ้างพัวพันคดีฟอกเงิน สูญนับ 100 ล้าน.สืบค้นจาก https://www.isranews.org/article/isranews-short-news/107851-isranews-354.html

มติชนออนไลน์. (2566). ศาลสั่งคุก 5,585 ปี 5 จำเลย คดีฟาร์มเห็ด Turtle Farm ชดใช้เหยื่อ 1.1 พันคน กว่า 614 ล้าน. สืบค้นจาก https://www.matichon.co.th/local/news_4342328

Thai PBS News. (2566). ปิดฉากแชร์ลูกโซ่ฟาร์มเห็ด ศาลสั่งคุกกรรมการ-พวก สั่งคืนเงินผู้เสียหาย. สืบค้นจาก https://www.thaipbs.or.th/news/content/335124

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.). (2566). เตือนภัย Hybrid Scam (Pig Butchering) โรแมนซ์สแคมรูปแบบใหม่ หลอกรักชวนลงทุนคริปโทฯ. สืบค้นจาก https://tcsd.go.th/hybrid-scam-warning

กองบัญชาการสอบสวนกลาง (CIB). (2567). ภัยเงียบคนทำงาน ตำรวจสอบสวนกลางเตือนภัย Sextortion วิดีโอคอลแบล็กเมล์ ขู่ประจานที่ทำงาน. สืบค้นจาก https://cib.go.th/news/sextortion-cyber-blackmail

ฐานเศรษฐกิจ. (2566). สถิติพุ่ง! มิจฉาชีพใช้ร่างอวตารสาวสวย ลวงวิศวกร-หนุ่มออฟฟิศอัดคลิป Cybersex ขูรีดเงิน. สืบค้นจาก https://www.thansettakij.com/technology/technology/581240

สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.) | Thai Health Promotion Foundation (ThaiHealth).(2568).สถิติชี้ชัด คนวัย 30-44 ปี โดนตกทรัพย์จากอาชญากรรมไซเบอร์พุ่งสูงมากที่สุด. สืบค้นจาก https://resourcecenter.thaihealth.or.th/content/5731-content-

ไทยรัฐ Money. (2566). สมาคมธนาคารไทย ร่วมมือตำรวจไซเบอร์ แถลงกลโกง "หลอกให้อ้วนแล้วเชือด" เสียหายจำนองบ้าน-รถเทรดเหรียญปลอม.
สืบค้นจาก https://www.thairath.co.th/money/economics/thailand_econ/2741105

บทความ

ภัยไซเบอร์ใกล้ตัววัยเริ่มทำงาน: รู้ทันกลโกง สังเกตให้เป็น ป้องกันได้

ในยุคที่การทำธุรกรรมทางการเงินและการสื่อสารเกิดขึ้นผ่านช่องทางดิจิทัลเป็นหลัก กลุ่มวัยเริ่มทำงาน ซึ่งมีอายุระหว่าง ๒๒ – ๒๙ ปี ถือหนึ่งในกลุ่มเสี่ยงที่มีความเสี่ยงสูงต่อการตกเป็นเหยื่อของมิจฉาชีพออนไลน์ เนื่องจากกลุ่มนี้มีทั้งรายได้ประจำ บัญชีธนาคาร และความคุ้นเคยกับเทคโนโลยีที่ทำให้เชื่อมั่นในการทำธุรกรรมออนไลน์มากจนเกินไป จากข้อมูลของสำนักงานตำรวจแห่งชาติและสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พบว่ามูลค่าความเสียหายจากภัยไซเบอร์ในประเทศไทยเพิ่มสูงขึ้นอย่างต่อเนื่องทุกปี บทความนี้จึงมุ่งนำเสนอความรู้เชิงปฏิบัติเพื่อให้ผู้อ่านสามารถรับมือกับภัยได้อย่างยั่งยืนและมีประสิทธิภาพ

๑. รูปแบบการหลอกลวงที่วัยเริ่มทำงานมักตกเป็นเหยื่อ มิจฉาชีพออนไลน์มีการพัฒนารูปแบบการหลอกลวงอย่างต่อเนื่องเพื่อให้สอดคล้องกับพฤติกรรมของกลุ่มเป้าหมาย รูปแบบที่พบบ่อยในกลุ่มวัยเริ่มทำงาน มีดังต่อไปนี้

๑.๑ การหลอกลวงผ่านงานออนไลน์รายได้ดี

มิจฉาชีพจะใช้โฆษณาชักชวนให้ทำงานออนไลน์ที่มีลักษณะเรียบง่าย เช่น การกดไลก์โพสต์ การรีวิวสินค้าหรือการกดซื้อสินค้าเพื่อรับค่าตอบแทน โดยอ้างว่าสามารถทำได้จากที่บ้าน และมีรายได้ ๕๐๐ - ๒,๐๐๐ บาทต่อวัน กระบวนการหลอกลวงมักดำเนินการดังนี้ เริ่มต้นให้เหยื่อทำงานและได้รับเงินในระยะแรก เพื่อสร้างความน่าเชื่อถือ หลังจากนั้นมักจะให้เหยื่อโอนเงินค้ำประกันหรือทำออเดอร์และรอเงินคืน โดยอ้างว่าจะโอนคืนในภายหลัง ท้ายสุดเมื่อเหยื่อโอนเงินก้อนใหญ่มิจฉาชีพจะหายตัวไปโดยไม่สามารถติดต่อได้

๑.๒ การโจมตีแบบฟิชชิ่ง

ฟิชชิ่งเป็นการส่งอีเมลหรือข้อความแจ้งเตือนปลอมที่แอบอ้างเป็นหน่วยงานที่น่าเชื่อถือ เช่น ธนาคารหรือบริษัทขนส่งพัสดุ เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัวหรือรหัสผ่าน นอกจากนี้มิจฉาชีพยังสร้างเว็บไซต์ปลอมที่ใช้ในการหลอกลวงมักออกแบบให้มีหน้าตาคล้ายกับเว็บจริง จึงจำเป็นที่จะต้องตรวจสอบลิงก์ URL อย่างละเอียดทุกครั้ง รูปแบบที่พบบ่อย ได้แก่ อีเมลแจ้งเตือนว่าบัญชีธนาคารจะถูกระงับ พร้อมลิงก์ให้ยืนยันตัวตน ข้อความแจ้งเตือนมีเนื้อหาว่ามีพัสดุรอรับ ให้กดลิ้งก์เพื่อชำระค่าธรรมเนียมหรือค่าปรับ และอีเมลที่อ้างว่ามีเงินคืนภาษีมักจะให้กรอกข้อมูลบัญชีธนาคารเพื่อรับเงิน

๑.๓ การแอบอ้างเป็นบุคคลที่รู้จัก

มิจฉาชีพจะเจาะเข้าบัญชี LINE หรือ Facebook ของบุคคลที่เหยื่อรู้จัก จากนั้นส่งข้อความขอยืมเงินโดยอ้างเหตุฉุกเฉิน วัยเริ่มทำงานมักตกเป็นเหยื่อของรูปแบบนี้เนื่องจากความไว้วางใจที่มีต่อบุคคลที่รู้จักและไม่ต้องการเสียน้ำใจด้วยการให้ยืมเงินโดยขาดการไตร่ตรองและพิจารณาอย่างรอบคอบ

๑.๔ การหลอกลวงด้านการลงทุน

มิจฉาชีพมักจะชักชวนให้ลงทุนในสินทรัพย์ดิจิทัล หุ้น หรือสินทรัพย์อื่นๆ โดยสัญญาว่าจะได้รับผลตอบแทนสูงผิดปกติ เช่น ๒๐ – ๓๐% ต่อเดือน กลโกงประเภทนี้มีความซับซ้อนสูงขึ้น โดยสร้างแอปพลิเคชัน หรือเว็บไซต์ปลอมที่มีหน้าแดชบอร์ดแสดงผลกำไรที่สมจริง เพื่อสร้างความน่าเชื่อถือในระยะแรกก่อนที่เหยื่อจะโอนเงินก้อนใหญ่

๑.๕ การหลอกลวงทางอารมณ์

มิจฉาชีพมักจะสร้างโปรไฟล์ปลอมของบุคคลที่มีรูปลักษณ์ดีในแพลตฟอร์มสังคมออนไลน์หรือในแอปพลิเคชันหาคู่ จากนั้นสร้างความสัมพันธ์อย่างค่อยเป็นค่อยไป เป็นระยะเวลาประมาณ ๑ - ๓ เดือน ก่อนจะขอให้โอนเงินด้วยเหตุผลต่างๆ หรือชักชวนให้ลงทุนร่วมกัน กลุ่มวัยเริ่มทำงานที่ต้องการสร้างความสัมพันธ์ใหม่มักตกเป็นเป้าหมายของกลโกงประเภทนี้

/๒. ข้อสังเกต...

๒. ข้อสังเกตและสัญญาณเตือนภัย

การรู้จักสังเกตสัญญาณเตือนเป็นหลักสำคัญในการป้องกันตนเองจากภัยไซเบอร์ข้อสังเกตที่ควรระวังมีดังต่อไปนี้

๒.๑ การสร้างความเร่งด่วน

มิจฉาชีพมักใช้กลยุทธ์กดดันให้เหยื่อตัดสินใจอย่างรวดเร็ว โดยใช้ภาษาที่แสดงความเร่งด่วน เช่น ด่วนมาก หมดเวลาภายใน ๒๔ ชั่วโมง หรือโอกาสสุดท้าย วัตถุประสงค์หลักคือการป้องกันไม่ให้เหยื่อมีเวลาคิดพิจารณาอย่างรอบคอบ

๒.๒ ผลตอบแทนที่สูงผิดปกติ

ข้อเสนอใดก็ตามที่สัญญาผลตอบแทนสูงกว่าความเป็นจริงอย่างมีนัยสำคัญ ควรได้รับการพิจารณาอย่างระมัดระวัง โดยอัตราดอกเบี้ยของธนาคารพาณิชย์อยู่ที่ประมาณ ๑ – ๒% ต่อปี และกองทุนรวมส่วนใหญ่มักให้ผลตอบแทนเฉลี่ย ๑๐ – ๑๕% ต่อปี ดังนั้นข้อเสนอที่อ้างผลตอบแทน ๒๐% ขึ้นไปต่อเดือนจึงเป็นสัญญาณเตือนที่ชัดเจนว่ามีความเป็นไปได้ว่าอาจเป็นมิจฉาชีพ

๒.๓ ลิงก์และที่อยู่เว็บไซต์ที่ผิดปกติ

เว็บไซต์ปลอมมักใช้ชื่อโดเมนที่คล้ายกับเว็บจริงแต่มีความแตกต่างเล็กน้อย ตัวอย่างเช่น เว็บไซต์จริงของกรมคือ www.dla.go.th ในทางกลับกันเว็บไซต์ปลอมที่อาจพบเห็นจะมีลักษณะดังนี้ www.dla.go.th-secure.com โดยมีการใส่คำว่า -secure เพิ่มเติมทำให้น่าเชื่อถือมากยิ่งขึ้น ดังนั้น ผู้ใช้งานควรตรวจสอบลิงก์ URL อย่างละเอียดทุกครั้งก่อนกรอกข้อมูล

๒.๔ การขอข้อมูลที่เป็นความลับ

สถาบันการเงินและหน่วยงานภาครัฐที่ถูกกฎหมายจะไม่มีการขอรหัสผ่าน หมายเลข PIN รหัส OTP หรือข้อมูลส่วนตัวที่ละเอียดอ่อนผ่านทางโทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือข้อความแจ้งเตือน การร้องขอข้อมูลเหล่านี้ผ่านช่องทางดังกล่าวถือเป็นข้อความจากมิจฉาชีพที่ชัดเจน

๒.๕ โปรไฟล์ออนไลน์ที่ผิดสังเกต

บัญชีออนไลน์ที่มีรูปโปรไฟล์สวยงามเกินจริง มีจำนวนเพื่อนหรือผู้ติดตามน้อยมีประวัติการโพสต์น้อย หรือเพิ่งสร้างบัญชีใหม่ ควรได้รับการตรวจสอบเพิ่มเติมและพิจารณาอย่างรอบคอบว่าเป็นมิจฉาชีพหรือไม่

๓. แนวทางการป้องกันตนเองจากภัยไซเบอร์

การป้องกันภัยไซเบอร์อย่างมีประสิทธิภาพ ต้องอาศัยทั้งความรู้ความเข้าใจและการปฏิบัติอย่างสม่ำเสมอ แนวทางที่แนะนำมีดังต่อไปนี้

๓.๑ เปิดใช้งานการยืนยันตัวตนสองขั้นตอน

การยืนยันตัวตนสองขั้นตอนเป็นมาตรการรักษาความปลอดภัย ที่กำหนดให้ผู้ใช้ต้องยืนยันตัวตนด้วยวิธีสองวิธีที่แตกต่างกัน เช่น รหัสผ่านร่วมกับรหัส OTP จาก Application บนโทรศัพท์มือถือ แม้มิจฉาชีพจะทราบรหัสผ่าน แต่ไม่สามารถเข้าถึงบัญชีได้หากไม่มีโทรศัพท์ของเจ้าของบัญชี

๓.๒ การจัดการรหัสผ่านอย่างปลอดภัย

การจัดการรหัสผ่านที่ดีเป็นพื้นฐานสำคัญของความปลอดภัยทางไซเบอร์ โดยมีหลักการดังต่อไปนี้ ใช้รหัสผ่านที่มีความยาวอย่างน้อย ๑๒ ตัวอักษร ประกอบด้วยตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษ ไม่ใช้รหัสผ่านเดิมซ้ำกันในหลายแพลตฟอร์ม และไม่ใช้ข้อมูลส่วนตัวที่คาดเดาได้ง่าย เช่น วันเกิด ชื่อ หรือหมายเลขโทรศัพท์

/๓.๓ การตรวจสอบ...

๓.๓ การตรวจสอบก่อนคลิกลิงก์

ก่อนกดลิงก์ที่ได้รับทางไปรษณีย์อิเล็กทรอนิกส์ ข้อความแจ้งเตือน หรือแพลตฟอร์มโซเชียลมีเดีย ควรตั้งคำถามดังต่อไปนี้

(๑) ตรวจสอบว่าเราได้สมัครใช้บริการหรือสั่งซื้อสินค้าที่เกี่ยวข้องกับข้อความนี้หรือไม่ และลิงก์ URL ปลายทางตรงกับลิงก์ของหน่วยงานจริงหรือไม่

(๒) กรณีตรวจสอบตามข้อ (๑) แล้วยังไม่ชัดเจนให้เปิดเว็บเบราว์เซอร์ และพิมพ์ที่อยู่เว็บไซต์โดยตรงแทนการกดลิงก์

๓.๔ การอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ

การอัปเดตซอฟต์แวร์เป็นการปิดช่องโหว่ด้านความปลอดภัยที่อาจถูกมิจฉาชีพนำไปใช้โจมตีระบบ แนะนำให้ตั้งค่าการอัปเดตอัตโนมัติสำหรับระบบปฏิบัติการ แอปพลิเคชันธนาคาร และซอฟต์แวร์ที่ใช้งานประจำ

๓.๕ การตรวจสอบธุรกรรมทางการเงินก่อนดำเนินการ

เมื่อได้รับคำขอให้โอนเงินหรือดำเนินธุรกรรมทางการเงิน ไม่ว่าจะเป็นบุคคลที่รู้จักหรือหน่วยงานใดก็ตาม ควรดำเนินการตามขั้นตอนดังต่อไปนี้

(๑) ติดต่อผู้ส่งข้อความโดยตรงผ่านหมายเลขโทรศัพท์ที่ทราบอยู่แล้ว ไม่ใช่หมายเลขที่ระบุในข้อความ

(๒) ในกรณีที่เป็นธุรกรรมกับสถาบันการเงิน ให้ติดต่อสอบถามโดยตรงผ่านหมายเลขที่ระบุไว้ด้านหลังบัตรเดบิตหรือเครดิต และสำหรับธุรกรรมที่มีมูลค่าสูง ควรพิจารณาดำเนินการที่สาขาธนาคารโดยตรง

๓.๖ ความระมัดระวังในการใช้เครือข่ายสาธารณะ

เครือข่าย Wi-Fi สาธารณะมีความเสี่ยงสูงต่อการถูกดักจับข้อมูล ควรหลีกเลี่ยงการทำธุรกรรมทางการเงินหรือการกรอกข้อมูลส่วนตัวที่ละเอียดอ่อนบนเครือข่ายดังกล่าว หากจำเป็นต้องใช้เครือข่ายสาธารณะ ควรเปลี่ยนไปใช้เครือข่ายโทรศัพท์มือถือแทน

โดยสรุป ภัยไซเบอร์เป็นปัญหาที่มีความซับซ้อนและพัฒนาอย่างต่อเนื่อง การป้องกันตนเองอย่างมีประสิทธิภาพต้องอาศัยความรู้ความเข้าใจเกี่ยวกับรูปแบบการหลอกลวง ความสามารถในการสังเกตสัญญาณเตือน และการปฏิบัติตามมาตรการรักษาความปลอดภัยอย่างสม่ำเสมอ วัยเริ่มทำงานควรตระหนักว่า การหยุดคิดวิเคราะห์ก่อนดำเนินการทางดิจิทัล โดยเฉพาะอย่างยิ่งในกรณีที่เกี่ยวข้องกับการเงิน เป็นกลยุทธ์ที่มีประสิทธิภาพสูงสุดในการป้องกันภัยไซเบอร์ การรู้เท่าทันมิจฉาชีพเป็นทักษะที่ทุกคนสามารถพัฒนาได้ และการแบ่งปันความรู้ดังกล่าวให้แก่คนรอบข้าง จะช่วยลดความเสียหายที่เกิดจากภัยไซเบอร์ในสังคมโดยรวมได้อย่างยั่งยืน คาถาป้องกันมิจฉาชีพยุคดิจิทัลที่ดีที่สุดคือ **"ไม่เชื่อ – ไม่รีบ – ไม่โอน"** **การไม่เชื่อ** คือการพิจารณาอย่างถี่ถ้วนก่อนกระทำการสิ่งใดสิ่งหนึ่ง แม้จะอ้างตัวเป็นเจ้าหน้าที่รัฐขู่ว่ามีพัวพันคดี หรือแจ้งว่าได้รับสิทธิพิเศษ **การไม่รีบ** มักมาพร้อมความกลัวและความโลภ ให้เวลาในการตรวจสอบข้อเท็จจริง อย่ากดลิงก์หรือโอนเงินในทันที **การไม่โอน** คือการตรวจสอบชื่อบัญชีปลายทางทุกครั้ง และปฏิเสธการโอนเงินให้บัญชีบุคคลธรรมดาในการซื้อสินค้าหรือติดต่อราชการ การตรวจสอบให้มั่นใจคือการโทรกลับไปสอบถามหน่วยงานต้นสังกัดด้วยเบอร์ทางการ หรือติดต่อสถานีตำรวจใกล้บ้าน เพื่อสร้างภูมิคุ้มกันภัยหลอกลวงทางออนไลน์อย่างยั่งยืนและมีประสิทธิภาพ

บรรณานุกรม

กรมส่งเสริมการปกครองท้องถิ่น. (2569). รู้ทันกลโกงมิจฉาชีพ ป้องกันภัยไซเบอร์ เริ่มต้นที่ตัวเรา: รูปแบบมิจฉาชีพที่พบบ่อยตามช่วงวัย พร้อมแนวทางการป้องกันภัย. เผยแพร่โดยเทศบาลตำบลหลุบ. สืบค้นจาก https://www.lub.go.th/news-6-5-2569-1/

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.). (2566). ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.). สำนักงานตำรวจแห่งชาติ. สืบค้นจาก https://thaipoliceonline.com

ไทยพีบีเอส. (2567, 29 กรกฎาคม). เผยสถิติอาชญากรรมไซเบอร์ ผู้เสียหายส่วนใหญ่เป็นหญิงวัยทำงาน. สืบค้นจาก https://www.thaipbs.or.th/news/content/342472

ธนาคารแห่งประเทศไทย. (2566). อัตราดอกเบี้ยเงินฝากและเงินให้สินเชื่อของธนาคารพาณิชย์. สืบค้นจาก https://www.bot.or.th/th/statistics/interest-rate.html

สำนักงานตำรวจแห่งชาติ. (2566, 9 กรกฎาคม). หลอกลงทุนระบาดหนัก! ตร. เตือนต้องมีสติ "ไม่เชื่อ ไม่รีบ ไม่โอน". อินโฟเควสท์. สืบค้นจาก https://www.infoquest.co.th/2023/316436

สำนักงานปลัดกระทรวงกลาโหม. (2568, 26 ธันวาคม). 5 กลโกงมิจฉาชีพยอดฮิต และวิธีป้องกัน. กรมประชาสัมพันธ์. สืบค้นจาhttps://www.prd.go.th/th/content/category/detail/id/39/iid/459323

เดลินิวส์. (2568, 31 พฤษภาคม). อย่าโอนก่อนเด็ดขาด! ระวัง 6 กลโกงยอดฮิตจากมิจฉาชีพออนไลน์. สืบค้นจาก https://www.dailynews.co.th/news/4765954/