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