Vol.2 No.1 (January-June 2020)

ภัยคุกคามทางไซเบอร์ในสังคมสูงวัยของไทย

สุณิสา รื่นมาลี[1] และธีรวุฒิ นิลเพ็ชร์[2]

วันได้รับบทความ: 1 พฤษภาคม 2563 วันแก้ไข: 27 พฤษภาคม 2563 วันยอมรับเผยแพร่: 31 พฤษภาคม 2563

บทคัดย่อ

ประเทศไทยกำลังก้าวเข้าสู่สังคมสูงวัยอย่างสมบูรณ์ โดยเมื่อเข้าสู่สังคมสูงวัย ปัญหาสำคัญที่ต้องเผชิญไม่เพียงแต่ปัญหาความเสื่อมถอยตามวัยด้านร่างกายความเปราะบางทางธรรมชาติที่หลีกเลี่ยงไม่ได้ รวมไปถึงปัญหาอาชญากรรมต่างๆ ที่ผู้สูงอายุมีความเสี่ยงต่อการตกเป็นเหยื่อ โดยรูปแบบการก่ออาชญากรรรมมีหลากหลายรูปแบบเปลี่ยนแปลงตามสถานการณ์ ซึ่งปัจจุบันมีเทคโนโลยีเข้ามาเกี่ยวข้องกับการดำเนินชีวิตและผู้สูงอายุส่วนใหญ่หันมาใช้อินเทอร์เน็ตมากขึ้น ทำให้เกิดอาชญากรรมรูปแบบใหม่ที่เรียกว่าอาชญากรรมไซเบอร์ และในปัจจุบันมือถือถูกพัฒนาให้มีระบบต่างๆ ที่อำนวยความสะดวกให้มากขึ้น หรือที่เรียกว่าสมาร์ทโฟน ทำให้ผู้สูงอายุที่ใช้งานมือถือสื่อสารแทนการพูดคุย ทั้งการส่งรูปภาพ วิดีโอทำให้ช่องทางการสื่อสารกว้างมากขึ้น นำไปพบกับเพื่อนใหม่และผู้สูงอายุเองที่ใช้งานก็ไม่ทราบได้เลยว่าเพื่อนใหม่นั้นมีพื้นเพเป็นอย่างไร เป็นข้อมูลจริงดังที่แสดงเอาไว้หรือไม่ ซึ่งมิจฉาชีพใช้การสร้างโปรไฟล์ส่วนตัวที่ปลอมแปลงขึ้นมาเพื่อต้มตุ๋นหลอกลวงเหยื่อ และผู้สูงอายุจำนวนไม่น้อยที่ต้องสูญเสียเงินทองผ่านการหลอกลวงในสื่อสังคมออนไลน์ ดังนั้น การให้ความรู้กับผู้สูงอายุเกี่ยวกับการใช้เทคโนโลยีที่เหมาะสมนับว่าเป็นเรื่องสำคัญอย่างมาก ทั้งภาครัฐและภาคเอกชน หรือแม้แต่ครอบครัวควรจะต้องเข้ามามีบทบาทในการถ่ายทอดความรู้ตรงนี้สู่ผู้สูงอายุในสังคมสูงวัยไม่เช่นนั้นผู้สูงอายุจะเป็นกลุ่มเสี่ยงอย่างมากต่อภัยทางไซเบอร์ที่มีอยู่ในโลกที่มีการเปลี่ยนไปอย่างรวดเร็วในปัจจุบัน

คำสำคัญ : สังคมสูงวัย ภัยคุกคามทางไซเบอร์ สื่อสังคมออนไลน์

[1] นักศึกษาหลักสูตรศิลปศาสตรมหาบัณฑิต สาขาวิชาอาชญาวิทยาและการบังคับใช้กฎหมาย คณะสังคมศาสตร์ โรงเรียนนายร้อยตำรวจ (ผู้ประพันธ์บรรณกิจ)

[2] อาจารย์ประจำคณะสังคมศาสตร์ โรงเรียนนายร้อยตำรวจ

Vol.2 No.1 (January-June 2020)

Cyber threats in Ageing Society of Thailand

Sunisa Ruenmalee[1] & Theeravut Ninphet[2]

Received: May 1, 2020 Revised: May 27, 2020 Accepted: May 31, 2020

Abstract

Thailand has almost completely entered the aged society. The problems that the elderly persons will face are the health problem and also the risk of being a victim of crimes including cybercrimes. Recently, crimes have evolved according to the advancement of technology and more elderly persons have used the internet and smartphones in their daily life such as chatting, sending pictures and videos, contacting new friends, and transferring money. This makes them more vulnerable to the cyber threats including online scams. A number of elderly persons being a victim of online scams have lost a large amount of their money saved for the post retirement life. Therefore, providing information and knowledge to prevent elderly persons from being a victim of cybercrime is vital in the ageing society.

Keywords: Ageing society, Cyber threats, Online social media

[1] Graduate student in Master of Arts Program (Criminology and Law Enforcement) Faculty of Social Sciences, Royal Police Cadet Academy (Corresponding author)

[2] Lecturer at Faculty of Social Sciences, Royal Police Cadet Academy

บทนำ (Introduction)

จากการที่ประเทศไทยได้เข้าสู่ “สังคมสูงอายุ” (Ageing society) ซึ่งหมายถึงสังคมที่โครงสร้างประชากรที่มีสัดส่วนของผู้สูงอายุ หรือผู้ที่มีอายุตั้งแต่ 60 ปีขึ้นไป มากกว่าร้อยละ 10 ของประชากรทั้งหมด ทั้งนี้ การเปลี่ยนแปลงโครงสร้างประชากรดังกล่าวนี้นับเป็นความท้าทายของประเทศ ที่ต้องเตรียมพร้อมรับมือกับสถานการณ์ดังกล่าว ดังที่ทราบกันเป็นอย่างดีว่าในอุบัติการณ์การเกิดอาชญากรรม เด็ก ผู้หญิง และผู้สูงอายุเป็นกลุ่มคนที่มีความเสี่ยงเป็นเหยื่ออาชญากรรม โดยเฉพาะผู้สูงอายุนับว่ามีความเสี่ยงต่อการตกเป็นเหยื่ออาชญากรรม หรือการเกิดอาชญากรรม กับการอยู่บ้านปิดประตูรั้วล้อมมิดชิดก็ใช่ว่าจะปลอดภัย โดยเฉพาะผู้สูงอายุที่ต้องอยู่บ้านอย่างโดดเดี่ยวเพียงตามลำพังส่งผลให้ “ผู้สูงอายุ” เป็นหนึ่งในกลุ่มของประชากรที่มีความเสี่ยงมากที่สุด (ไกรวุฒิ วัฒนสิน, 2561) ซึ่งผลการวิจัยของมูลนิธิสถาบันวิจัยและพัฒนาผู้สูงอายุไทย (มส.ผส.) และสำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.) โดยข้อมูลสถิติจากสำนักงานตำรวจแห่งชาติ พบว่า คดีอาญาที่ผู้เสียหายเป็นผู้ที่มีอายุ 60 ปีขึ้นไป มีแนวโน้มสูงขึ้นอย่างต่อเนื่องการตกเป็นเหยื่ออาชญากรรมของผู้สูงอายุ 3 ลำดับแรกคือ ด้านอารมณ์ และจิตใจ รองลงมาคือการทอดทิ้งในกลุ่มผู้สูงอายุที่มีภาวะพึ่งพิง และตามด้วยการเอาประโยชน์ด้านทรัพย์สิน ขณะเดียวกันผู้สูงอายุที่ตกเป็นเหยื่ออาชญากรรมส่วนใหญ่ถูกกระทำโดยคนใกล้ชิดหรือคนในครอบครัว จากข้อมูลสภาพปัญหาดังกล่าวแสดงให้เห็นว่าการตกเป็นเหยื่ออาชญากรรม ในสังคมผู้สูงอายุมีแนวโน้มเพิ่มสูงขึ้นทั้งด้านความถี่ ความรุนแรง และมีความหลากหลายที่สลับซับซ้อนมากยิ่งขึ้นตามสภาพการพัฒนาของประเทศและสังคมโลก แม้หน่วยงานต่าง ๆ ที่เกี่ยวข้องได้พยายามเข้ามามีส่วนร่วมในการป้องกันและแก้ไขปัญหาอาชญากรรม อย่างต่อเนื่องแต่ยังคงประสบกับปัญหากับการขาดความพร้อมที่จะจัดการกับปัญหาดังกล่าว ซึ่งหมายถึงการขาดข้อมูลการตกเป็นเหยื่ออาชญากรรมที่เกิดขึ้นกับผู้สูงอายุ อย่างแท้จริงเห็นได้จากข้อมูลการสำรวจคดีอาชญากรรมภาคประชาชนหลายครั้งที่ผ่านมาพบว่า ผู้ประสบเหตุส่วนใหญ่ไม่ได้แจ้งเหตุต่อเจ้าหน้าที่ตำรวจหรือผู้เกี่ยวข้อง มากกว่าร้อยละ 60 (พิสิฐ ระฆังวงษ์ และประพนธ์ สหพัฒนา, 2561)

การเข้าสู่สังคมผู้สูงอายุของประเทศไทยนั้นภาครัฐและเอกชนได้รับรู้และตระหนักถึงสถานการณ์พอสมควร และได้มีการเตรียมการพอสมควร อาทิ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ได้มีการจัดตั้งหน่วยงานระดับกรมขึ้นมาดูแลกิจการของผู้สูงอายุเป็นการเฉพาะ มีการตราพระราชบัญญัติผู้สูงอายุ พ.ศ. 2546 เพื่อส่งเสริมผู้สูงอายุให้มีคุณภาพชีวิตที่ดีเพื่อส่งเสริมผู้สูงอายุให้มีคุณภาพชีวิตที่ดี และนอกจากนี้การศึกษาวิจัยในประเด็นเกี่ยวกับผู้สูงอายุเป็นประเด็นที่ได้รับความสนใจอย่างมาก ซึ่งเป็นประโยชน์ในการเตรียมความพร้อมทั้งทางร่างกายและจิตใจของผู้สูงอายุเองที่มีจำนวนมากขึ้นเรื่อย ๆ และเป็นประโยชน์ในการเตรียมความพร้อมทางเศรษฐกิจและสังคมของประเทศในภาพรวม การดำเนินงานที่ผ่านมารัฐบาลได้ให้ความสำคัญและมีนโยบายในการสนับสนุนส่งเสริมคุณภาพชีวิตของผู้สูงอายุมาอย่างต่อเนื่อง ทั้งในประเด็นเรื่องสุขภาพและคุณภาพชีวิตความเป็นอยู่ แต่อย่างไรก็ตามจากการศึกษาเบื้องต้น ในปัญหาอาชญากรรมความรุนแรงที่เกิดกับผู้สูงอายุซึ่งในทางอาชญาวิทยาถือว่าเป็นกลุ่มเสี่ยงที่จะเป็นเหยื่ออาชญากรรมในประเทศไทยยังมีการศึกษาน้อยมาก พบว่ามี เพียงการศึกษาสถานการณ์ความรุนแรงที่เกิดขึ้นกับผู้สูงอายุ ในปี พ.ศ. 2552 พบว่าความรุนแรงที่กระทำต่อผู้สูงอายุ ที่พบได้แก่ 1) การกระทำรุนแรงด้านร่างกาย 2) การกระทำรุนแรงด้านอารมณ์และจิตใจ

3) การหาประโยชน์ในทรัพย์สินและการเอาเปรียบทางกฎหมาย รวมทั้งการลักขโมย การล่อลวงเอาทรัพย์สินหรือนำทรัพย์สินไปใช้ในทางที่ไม่ถูกต้อง 4) การคุกคาม และการถูกล่วงละเมิดทางเพศ 5) การละเลยทอดทิ้ง ปฏิเสธการดูแล โดยสถิติการกระทำรุนแรงต่อผู้สูงอายุดังกล่าว ไม่ปรากฏว่ามีระบบการรายงานอย่างเป็นรูปธรรมมากนัก อาจเนื่องด้วยการเข้าถึงข้อมูล และเป็นปัญหาดังกล่าวมักซ่อนเร้น หรือปกปิดเพราะสิ่งที่เกิดขึ้นกับผู้สูงอายุมักเป็นเหตุการณ์ที่เกิดขึ้นภายในครอบครัว อีกทั้งรายงานสถิติคดีที่เกิดขึ้นของสำนักงานตำรวจแห่งชาติก็ยังไม่มีการรายงานเป็นการเฉพาะ แต่ทั้งนี้จากการศึกษาที่ผ่านมาและการรายงานข่าวสารเกี่ยวกับความรุนแรงต่อผู้สูงอายุในสื่อต่าง ๆ ทั้งหนังสือพิมพ์ ข่าวสารออนไลน์ โทรทัศน์ วิทยุที่ปรากฏเป็นระยะ ๆ ก็อาจเป็นภาพสะท้อนของความรุนแรงที่เกิดขึ้นได้เป็นอย่างดีว่ามีแนวโน้มของอุบัติการณ์ของการกระทำรุนแรงต่อผู้สูงอายุสูงขึ้น (ไกรวุฒิ วัฒนสิน, 2561)

อย่างไรก็ตามเริ่มมีอาชญากรรมยุคใหม่ที่เกิดขึ้นกับผู้สูงอายุ เป็นสิ่งที่ต้องระมัดระวังและร่วมกันหาแนวทางการช่วยเหลือ โดยเฉพาะกลุ่มผู้สูงอายุเป็นเป้าหมายของการทุจริต ฉ้อโกงจากกลุ่มมิจฉาชีพในประเทศสหรัฐอเมริกา มีการประมาณการความเสียหายถึง 3.6 หมื่นล้านดอลลาร์สหรัฐฯ โดยกลุ่มผู้สูงอายุมีความกังวลกับการใช้งานเทคโนโลยีใหม่ที่ซับซ้อน เข้าใจยาก และกลัวการถูกทุจริต ฉ้อโกง ปัจจุบันอินเทอร์เน็ตเป็นส่วนสำคัญในการดำรงชีวิต ไม่ว่าจะในมิติต่าง ๆ ของการดำเนินการทางเศรษฐกิจและสังคม การรักษาความมั่นคงและการป้องกันประเทศ การสื่อสารโทรคมนาคมและการควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญและจะทวีความสำคัญยิ่งขึ้นในอนาคต ความก้าวหน้าของเทคโนโลยีในยุคดิจิทัลที่ช่วยเชื่อมต่อแลกเปลี่ยนข้อมูลระหว่างกันได้ตลอดเวลาผ่านเครือข่ายอินเทอร์เน็ตบนโลกของเราทุกวันนี้ ทำให้การติดต่อสื่อสารและการทำธุรกรรมอิเล็กทรอนิกส์ในโลกเป็นเรื่องที่สะดวกรวดเร็วที่ช่วยเพิ่มความสะดวกสบายในการดำเนินชีวิตประจำวันให้เห็นกันบ้างแล้วทั้งทางตรงและทางอ้อม ยกตัวอย่างเช่น การค้าออนไลน์ (E-Commerce) หรือ การทำธุรกรรมออนไลน์ (E-Payment) (มณีรัตน์ อนุโลมสมบัติ, 2560) พ.ต.ต.ปฐมพงษ์ ศิลปสุข สารวัตรกองกำกับการ 1 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บอท.) ยอมรับว่า ปัจจุบันคดีหลอกลวงให้โอนเงินบนอินเทอร์เน็ตเริ่มมีมากขึ้นเรื่อย ๆ โดยมิจฉาชีพอาจจะเป็นคนร้ายกลุ่มเดียวกันซึ่งเปลี่ยนเหยื่อไปเรื่อย ๆ ซึ่งมีวิธีการหลากหลายรูปแบบ เช่น การหลอกว่ากำลังเดือดร้อนต้องการขอยืมเงินด่วน โดยจำเป็นต้องให้หมายเลขบัญชีของญาติ หรือการขอให้เพื่อนเติมเงินมือถือให้ ซึ่งมีตั้งแต่จำนวนเงินน้อย ๆ ไปจนถึงหลักพัน ผู้สูงอายุที่อยู่บ้านคนเดียว หากมีหมายเลขโทรศัพท์บ้านโทรมาแล้วอ้างเป็นเจ้าหน้าที่ตำรวจหรือเจ้าหน้าที่ของหน่วยงานรัฐ ขอให้รีบวางสาย อย่าคุยเด็ดขาด แล้วให้รีบแจ้งที่สถานีตำรวจใกล้บ้านให้เจ้าหน้าที่ตำรวจใกล้บ้านเพื่อประสานงานกับหน่วยงานรัฐที่ถูกแอบอ้างเพื่อมิให้ถูกหลอกลวง หรือให้รีบแจ้งบุตรหลานหรือบุคคลใกล้ชิด อย่าคุยคนเดียวเด็ดขาด เพราะเป็นจุดอ่อนให้มิจฉาชีพใช้ข่มขู่เหยื่อให้กลัวแล้วทำตามที่มิจฉาชีพทุกอย่างแล้วสูญเสียเงินจำนวนมาก

การเข้าสู่สังคมผู้สูงวัยเป็นพลวัตสำคัญที่ส่งผลกระทบในวงกว้าง ทั้งต่อสังคมโลกและประเทศไทย โดยเฉพาะประเทศไทยก้าวเข้าสู่สังคมผู้สูงวัยตั้งแต่ปี 2548 ขณะที่สัดส่วนประชากรผู้สูงวัยเพิ่มขึ้นอย่างรวดเร็วและต่อเนื่อง ส่งผลให้ปี 2562 ประชากรผู้สูงวัยมีมากกว่าประชากรวัยเด็ก สะท้อนได้จากตัวเลขของกรมกิจการผู้สูงอายุ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (พม.) ข้อมูล ณ วันที่ 31 ธ.ค.

2561พบว่า ประเทศไทยมีประชากรทั้งหมด 66.4 ล้านคน เฉพาะผู้สูงอายุ 10,670,000 คน หรือร้อยละ 16.06 แบ่งเป็นผู้สูงอายุชาย 4,720,000 คน และผู้สูงอายุหญิง 5,950,000 คน โดยจังหวัดที่มีประชากรผู้สูงอายุมากที่สุดคือ กรุงเทพฯ มากกว่า 1 ล้านคน (ร้อยละ 17.98) รองลงมา นครราชสีมา เชียงใหม่ ขอนแก่น และอุบลราชธานีในปี 2564 ประเทศไทยจะเข้าสู่สังคมผู้สูงวัยอย่างสมบูรณ์ เป็นประเทศที่สองของอาเซียน รองจากสิงคโปร์โดยประชากรที่มีอายุ 60 ปีขึ้นไป จะมีจำนวนไม่น้อยกว่า 13 ล้านคน หรือร้อยละ 20 ของประชากรทั้งหมดและอีก 20 ปีข้างหน้า ในปี 2583 ประเทศไทยจะมีผู้สูงวัยจำนวน 20 ล้านคน หรือ 1 ใน 3 ของคนไทยจะเป็นผู้สูงวัย และผู้สูงวัยอายุมากกว่า 80 ปีขึ้นไป จะมีมากถึง 3,500,000 คน สังคมผู้สูงวัยกลายเป็นเรื่องใกล้ตัวคนไทยซึ่งต่อไปประเทศไทยต้องให้ความสำคัญกับเรื่องนี้ โดยตัวเลขระบุว่าในอนาคตคนไทย 1 ใน 3 จะเป็นผู้สูงวัยนั้นถือว่าเป็นเรื่องน่าตกใจ เพราะเป็นตัวเลขสูงมาก รองจากสิงคโปร์ ในประเทศไทยเป็นสังคมผู้สูงอายุมาสักพักใหญ่แล้วการเป็นสังคมผู้สูงอายุไม่ได้น่ากลัว แต่สิ่งที่น่ากลัวคือการบริหารจัดการสังคมผู้สูงอายุว่าเราจะทำอย่างไรให้สังคมผู้สูงอายุเป็นสังคมที่มีคุณภาพและมีความพร้อมอุบัติการณ์การเกิดอาชญากรรม เด็ก ผู้หญิงและผู้สูงอายุ เป็นกลุ่มคนที่มีความเสี่ยงเป็นเหยื่ออาชญากรรม สังคมผู้สูงอายุเพิ่มขึ้นเรื่อย ๆ ทั่วโลก โดยเริ่มจากประเทศที่พัฒนาแล้วมีความก้าวหน้าทางเศรษฐกิจและเทคโนโลยีและตามมาด้วยประเทศกำลังพัฒนา (Thaireform, 2562)

สำนักงานตำรวจแห่งชาติ (ตร.) ร่วมกันสรุปผลงานสำนักงานตำรวจแห่งชาติ ประจำปี 2561 ภาพรวมอาชญากรรมพื้นฐานลดลง เช่นคดีความผิดเกี่ยวกับชีวิต ร่างกาย เพศ มีคดีเกิด 18,923 ราย จับได้ 15,879 ราย คิดเป็น 83.91 เปอร์เซ็นต์ มีสถิติลดลงกว่า 1,000 ราย คดีความผิดเกี่ยวกับทรัพย์ มีคดีเกิด 57,671 ราย จับได้ 38,696 ราย คิดเป็น 67.10 เปอร์เซ็นต์ มีสถิติลดลงกว่า 4,000 ราย เมื่อเปรียบเทียบกับปี 2560 แต่ขอแจ้งเตือนประชาชนอาชญากรรมทางไซเบอร์จะเพิ่มสูงขึ้นในปี พ.ศ.2562 “ปัจจุบันเทคโนโลยีต่าง ๆ พัฒนาขึ้นอย่างรวดเร็ว โดยเฉพาะเทคโนโลยีเกี่ยวกับคอมพิวเตอร์และอินเตอร์เน็ตมิจฉาชีพนำมาใช้ทำผิด ทำให้เกิดอาชญากรรมรูปแบบใหม่ ที่เรียกว่า “อาชญากรรมไซเบอร์” หรือ “อาชญากรรมคอมพิวเตอร์” เช่น คดีฉ้อโกงออนไลน์แก๊งคอลเซ็นเตอร์ แก๊งรักหลอกออนไลน์ การละเมิดทรัพย์สินทางปัญญา คดีค้ามนุษย์ หรือคดีเรียกดอกเบี้ยเกินอัตราในรอบปี 2561 มีสถิติสูงขึ้นอย่างมากรับแจ้ง 26,659 ราย ศปอส.ตร.จับได้ 16,086 ราย ทั้งนี้ คดีแก๊งคอลเซ็นเตอร์ คดีเกิดขึ้น 508 ราย จับกุมทั้งหมดเรียกว่าหมดไปจากประเทศแล้ว รวมความผิดคดีอาชญากรรมไซเบอร์ ระดมกวาดล้างมีมูลค่า 428,494,744 บาท ส่งเรื่องให้สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงินยึดทรัพย์แล้ว 16 เรื่อง มูลค่าทรัพย์สินที่อายัดและรออายัด 397,635,520 บาท ส่วนคดียาเสพติดมีผลจับกุมเพิ่มมากขึ้นกว่าปี 2560 จับกุม 556,502 ราย ผู้ต้องหากว่า 615,134 คน มีคดีเพิ่มขึ้นกว่า 93,140 ราย สรุปภาพรวมอาชญากรรมทั้งประเทศ ในปี 2561 รับคำร้องทุกข์ 762,890 คดีจับกุม 699,043 คดี คิดเป็น 91.63 เปอร์เซ็นต์ (ไทยรัฐออนไลน์, 2562)

จากสภาพปัญหาที่เปลี่ยนแปลงไป ภัยคุกคามทางไซเบอร์ซึ่งทวีความรุนแรงขึ้นตามจำนวนผู้ใช้งานอินเทอร์เน็ต มีความซับซ้อน ที่ส่งผลกระทบต่อปัญหาทางสังคมและเศรษฐกิจมากขึ้นทุก ๆ ปี รวมถึงจำนวนผู้สูงวัยที่เพิ่มขึ้นที่มีความเสี่ยงต่อการตกเป็นเหยื่ออาชญากรรม หรือการเกิดอาชญากรรม เช่น การละเมิดทรัพย์สินทางปัญญา การลักลอบเข้าถึงข้อมูล ระบบการเงินการธนาคาร เป็นต้น ทำไมผู้สูงอายุผู้ตกเป็นเหยื่ออาชญากรรม

จำนวนมาก เพราะผู้สูงอายุบางท่านยังขาดความรู้ความเข้าใจในการในอินเทอร์เน็ต เสี่ยงต่อการโดนหลอกได้ง่าย และที่ไม่แจ้งความต่อเจ้าหน้าที่ตำรวจเพราะไม่รู้จะต้องแจ้งที่ไหนหรือต้องทำอย่างไรบ้าง ถึงเวลาแล้วที่ผู้สูงอายุจะต้องทำความเข้าใจ และปรับตัวให้ทันต่อสถานการณ์ สภาพปัญหาที่กำลังเกิดขึ้น ดังนั้น เพื่อศึกษาสภาพปัญหารูปแบบ และผลกระทบจากอาชญากรรมยุคใหม่ที่ผู้สูงอายุมีความเสี่ยงต่อการตกเป็นเหยื่ออาชญากรรม หรือการเกิดอาชญากรรมเป็นอย่างไร รวมถึงแนวทางการป้องกันปัญหาที่เป็นประโยชน์กับผู้สูงอายุ เจ้าหน้าที่ที่เกี่ยวข้องให้ความช่วยเหลือและสนับสนุน ร่วมกันแก้ไขปัญหาการตกเป็นเหยื่ออาชญากรรมที่เกิดขึ้นกับผู้สูงอายุต่อไป ในปัจจุบันที่เป็นเหตุให้ก่อเกิดปัญหา ทั้งปัญหาอาชญากรรมและปัญหาสังคมอีกมากมายตามมา รวมถึงเทคโนโลยีได้มีการพัฒนาขึ้นเรื่อย ๆ หลากหลายรูปแบบ ทำให้บางทีผู้สูงอายุก็ไม่ทันต่อรูปแบบที่เกิดขึ้น เพราะฉะนั้นอาชญากรรมทางคอมพิวเตอร์จึงเป็น “ภัยใกล้ตัวกว่าที่คุณคิด” ที่กำลังเกิดขึ้นในขณะนี้

คำนิยามของผู้สูงอายุ (Definitions of Elderly Person)

“ผู้สูงอายุ” (Older/Elderly person) ตามนิยามขององค์การสหประชาชาติ (United Nations) คือผู้ที่มีอายุ 60 ปีขึ้นไป ประเทศที่พัฒนาแล้วส่วนใหญ่ใช้อายุ 65 ปีขึ้นไป เป็นเกณฑ์ในการเรียก “ผู้สูงอายุ” (สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ, ม.ป.ป.)

สำหรับประเทศไทยกำหนดนิยาม “ผู้สูงอายุ” ไว้ในพระราชบัญญัติผู้สูงอายุ พ.ศ. 2546 มาตรา 3 หมายถึง บุคคลซึ่งมีอายุเกิน 60 ปีบริบูรณ์ขึ้นไปและมีสัญชาติไทย

สังคมสูงวัย (Aged Society) หมายถึงสังคมที่มีประชากรอายุ 60 ปีขึ้นไป มากกว่าร้อยละ 10 ของประชากรทั้งหมด(หรือมีประชากรอายุ 65 ปีขึ้นไป มากกว่าร้อยละ 7)

สังคมสูงวัยอย่างสมบูรณ์ (Complete Aged Society) หมายถึง สังคมที่มีประชากรอายุ 60 ปีขึ้นไป มากกว่าร้อยละ 20 ของ ประชากรทั้งหมด (หรือมีประชากรอายุ 65 ปีขึ้นไป มากกว่าร้อยละ 14)

สังคมสูงวัยระดับสุดยอด (Super Aged Society) หมายถึง สังคมที่มีประชากรอายุ 60 ปีขึ้นไป มากกว่าร้อยละ 28 ของ ประชากรทั้งหมด (หรือประชากรอายุ 65 ปีขึ้น มากกว่าร้อยละ 20)

สภาพปัญหาอาชญากรรมของผู้สูงอายุ (Situation of Crimes Related to Elderly Person)

ประเทศไทยมีการเปลี่ยนแปลงทั้งทางด้านการเมือง เศรษฐกิจและสังคมอย่างรวดเร็ว ส่งผลให้เกิดปัญหาอาชญากรรมขึ้น ซึ่งปัญหาอาชญากรรมเป็นปัญหาที่สำคัญของสังคมที่มีแนวโน้มและความรุนแรงเพิ่มมากขึ้น ส่งผลให้คนในสังคมมีความรู้สึกไม่ปลอดภัยในชีวิต ซึ่งการแก้ไขปัญหาดังกล่าวภาครัฐจะต้องมีความตระหนักต่อความเสี่ยงของการเกิดอาชญากรรมและหาทางการป้องกันการก่ออาชญากรรมแก่ประชาชน รัฐจะต้องจัดการลงโทษอาชญากรหรือผู้ที่กระทำความผิดขั้นเด็ดขาดเพื่อลดจำนานวนของอาชญากรรมที่เกิดขึ้น

จากการศึกษาเกี่ยวกับสภาพปัญหาอาชญากรรมของผู้สูงอายุ พบว่า การตกเป็นเหยื่ออาชญากรรมของผู้สูงอายุส่วนใหญ่มักเกิดขึ้นในเขตที่อยู่อาศัย และผู้กระทำผิดมักเป็นบุคคลใกล้ชิดในครอบครัวของผู้สูงอายุ

โดยนักวิชาการที่ศึกษาในบริบทของสังคมไทยได้แบ่งลักษณะของการตกเป็นเหยื่ออาชญากรรมของผู้สูงอายุ ซึ่งส่วนใหญ่เกิดจากการถูกละเมิดและการใช้ความรุนแรงต่อผู้สูงอายุ ทั้งนี้ เกิดจากการกระทำของบุคคลโดยสมาชิกในครอบครัว กล่าวคือ เป็นพฤติกรรมของสมาชิกในครอบครัวทั้งที่เจตนาหรือไม่เจตนาที่เป็นการคุกคามหรือทำร้ายผู้สูงอายุ แบ่งออกเป็น 5 ประเภท ดังต่อไปนี้

(1) ด้านร่างกาย เป็นการถูกคุกคามหรือทำร้ายด้านร่างกายต่อผู้สูงอายุ เป็นการใช้พละกำลังทางกายอาจเป็นพฤติกรรมของสมาชิกในครอบครัว เพื่อน หรือบุคคลอื่น ที่ไม่รู้จักต่อผู้สูงอายุ ส่งผลให้ผู้สูงอายุได้รับความเจ็บปวดจากการถูกทำร้ายทางด้านร่างกาย รวมถึงการขัดขวางการรับประทานยาและการให้ยาที่เกินขนาดกับผู้สูงอายุ

(2) ด้านอารมณ์และจิตใจ เป็นการถูกคุกคามหรือทำร้ายผู้สูงอายุให้ได้รับความรู้สึกเสียใจ โดยการใช้คำพูด ท่าทาง สีหน้า ส่งผลให้ผู้สูงอายุได้รับความทุกข์ทรมาน ทางด้านจิตใจ หรือความเจ็บปวดทางอารมณ์ รวมถึงการละเมิดความเป็นส่วนตัว เป็นสาเหตุที่ทำให้ผู้สูงอายุเกิดภาวะความเครียดต่อสุขภาพ และอาจตัดสินใจกระทำความผิดโดยไม่รู้ตัว เช่น การใช้คำพูดก้าวร้าว การดูถูก รังเกียจ ท่าทาง สีหน้า การถูก แบ่งแยกจากสังคม การไม่เห็นคุณค่าของผู้สูงอายุ เป็นต้น

(3) ด้านเพศ เป็นการถูกคุกคามหรือลวนลามทางเพศกับผู้สูงอายุ การข่มขืน ทำอนาจาร เป็นการกระทำของบุคคลสมาชิกในครอบครัว เพื่อน หรือบุคคลอื่นที่ไม่รู้จัก ที่มีพฤติกรรมคุกคาม เช่น การดูภาพโป๊สื่อลามก โดยไม่คำนึงถึงความรู้สึกของผู้สูงอายุ ข่มขู่ บีบบังคับ เป็นเหตุให้ผู้สูงอายุถูกคุกคามทางเพศ

(4) ด้านทรัพย์สิน เป็นการถูกคุกคามหรือการเอาเปรียบผู้สูงอายุโดยการใช้ แรงงาน หรือการเอาประโยชน์จากทรัพย์สมบัติของผู้สูงอายุ การแอบอ้างใช้ข้อมูลส่วนตัว เช่น การขโมยเลขบัตรเครดิตหรือรหัสบัตรกดเงินสด บัตรประชาชน เป็นต้น รวมถึง การเอาผลประโยชน์จากผู้สูงอายุเมื่อเสียชีวิต เช่น การแอบอ้างเอาชื่อสมัครสมาชิก ชมรมผู้สูงอายุ กล่าวคือ เมื่อผู้สูงอายุเสียชีวิต ก็จะได้เงินจากชมรมในการปลงศพ โดยส่วนใหญ่มักเป็นการกระทำของสมาชิกในครอบครัว เพื่อน หรือบุคคลอื่นที่ไม่รู้จักเพื่อเอาผลประโยชน์จากส่วนต่างหลังหักค่าใช้จ่ายในการปลงศพ

(5) ด้านการถูกทอดทิ้ง เป็นการละเลยหรือการไม่ให้ความช่วยเหลือกิจวัตรประจำวันต่อการดำรงชีวิตของผู้สูงอายุ ด้วยความตั้งใจหรือไม่ตั้งใจ การปล่อยให้ ผู้สูงอายุอยู่เพียงลำพัง ซึ่งเป็นสาเหตุที่ทำให้อาชญากรเล็งเห็นผู้สูงอายุเป็นเหยื่อที่ไม่สามารถตอบโต้หรือต่อสู้ได้ ส่งผลให้ผู้สูงอายุไม่ได้รับการดูแลที่จำเป็นเกิดความทุกข์ลำบากจากการถูกทอดทิ้ง การไม่ได้รับอาหาร เสื้อผ้า ยารักษาโรค การดูแลความสะอาด รวมถึงการจำกัดหรือปฏิเสธสิทธิส่วนบุคคลของผู้สูงอายุในการปฏิบัติกิจกรรมต่าง ๆ ภายในครอบครัว หรือการเข้าร่วมสังคมของผู้สูงอายุในชุมชน (พิสิฐ ระฆังวงษ์ และประพนธ์ สหพัฒนา, 2561)

อาชญากรรมทางคอมพิวเตอร์ (Computer Crime)

อาชญากรรมทางคอมพิวเตอร์ หรือ อาชญากรรมไซเบอร์ หมายถึงอาชญากรรมใด ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ อาชญากรรม(บน)อินเทอร์เน็ตก็เป็นอีกคำหนึ่งซึ่งหมายถึงการแสวงหาผลประโยชน์อย่างผิดกฎหมายบนอินเทอร์เน็ต คอมพิวเตอร์นั้นอาจถูกใช้เป็นเครื่องมือก่ออาชญากรรมหรืออาจตกเป็นเป้าหมายของการกระทำก็ได้ Dr. Debarati Halder และ Dr. K. Jaishankar ได้นิยาม

อาชญากรรมไซเบอร์ไว้ว่าเป็น ความผิดที่กระทำขึ้นต่อปัจเจกบุคคลหรือกลุ่มของปัจเจกบุคคล ด้วยเหตุจูงใจทางอาญา ที่เจตนาทำให้เหยื่อเสื่อมเสียชื่อเสียง หรือทำร้ายร่างกายหรือจิตใจของเหยื่อ โดยทางตรงหรือทางอ้อม โดยใช้เครือข่ายโทรคมนาคมสมัยใหม่ อาทิ อินเทอร์เน็ต (ห้องแชท อีเมล กระดานประกาศ และกลุ่มข่าว) และโทรศัพท์เคลื่อนที่ (เอสเอ็มเอส/เอ็มเอ็มเอส) อาชญากรรมเช่นนั้นอาจคุกคามความมั่นคงและสภาวะทางการคลังของรัฐ ปัญหาต่าง ๆ ที่เกี่ยวข้องกับอาชญากรรมชนิดนี้ได้กลายมาเป็นปัญหาสำคัญ โดยเฉพาะที่เกี่ยวข้องกับการเจาะระบบเครือข่าย การละเมิดลิขสิทธิ์ สื่อลามกอนาจารเด็ก และการล่อลวงเด็ก นอกจากนี้ยังมีปัญหาเรื่องความเป็นส่วนตัวเมื่อสารสนเทศที่เป็นความลับถูกสกัดกั้นหรือถูกเปิดเผยโดยทางกฎหมาย (อาชญากรรมคอมพิวเตอร์, 2562)

ประเภทของอาชญากรรมคอมพิวเตอร์ ได้ 9 ประเภท (บัณฑิต อาณาจักรานนท์, ม.ป.ป.)

1. การขโมยข้อมูลทางอินเตอร์เน็ต รวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ
2. การปกปิดความผิดของตัวเอง โดยใช้ระบบการสื่อสาร
3. การละเมิดลิขสิทธิ์ ปลอมแปลงรูปแบบเลียนแบระบบซอฟแวร์โดยมิชอบ
4. การเผยแพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่เหมาะสม
5. การฟอกเงิน
6. การก่อกวน ระบบคอมพิวเตอร์ เช่น ทำลายระบบสาธารณูปโภค เช่น ระบบจ่ายน้ำ จ่ายไฟ จราจร
7. การหลอกลวงให้ร่วมค้าขาย หรือ ลงทุนปลอม (การทำธุรกิจที่ไม่ชอบด้วยกฎหมาย)
8. การลักลอบใช้ข้อมูลเพื่อแสวงหาผลประโยชน์ในทางมิชอบ เช่น การขโมยรหัสบัตรเครดิต
9. การใช้คอมพิวเตอร์ในการโอนบัญชีผู้อื่นเป็นของตัวเอง

ความเสี่ยงของผู้สูงอายุต่อภัยคุกคามทางไซเบอร์ (Risks of Elderly Person for Cyber Threats)

"อินเทอร์เน็ต" ถือเป็นสื่อออนไลน์ที่ได้รับความนิยมเป็นอย่างมากในทุกเพศทุกวัย โดยไม่จำกัดแค่เฉพาะวัยรุ่น หรือวัยทำงานเท่านั้น ในวัยผู้สูงอายุก็สามารถเปิดโลกทัศน์ในโลกออนไลน์ได้เช่นกัน ความก้าวหน้าของระบบเทคโนโลยีสารสนเทศที่ทันสมัยส่งผลทั้งเชิงบวกและเชิงลบเนื่องจากปัจจัยบวกของกระแสโลกาภิวัตน์ ที่มีการเปิดเสรี การค้า การเงิน การลงทุน ส่งผลให้การติดต่อสื่อสารระหว่างกันเป็นไปได้อย่างสะดวกรวดเร็ว ซึ่งแม้จะมีมาตรการในการป้องกัน แต่ยังคงพบช่องโหว่ทำให้ถูกกลุ่มผู้ไม่หวังดีนำไปใช้ประโยชน์ในทางที่ผิดจนกลายเป็นภัยคุกคามทางไซเบอร์ และอาจส่งผลกระทบต่อความมั่นคง โดยเฉพาะในด้านการก่อการร้ายที่อำนวยให้การประกอบอาชญากรรมข้ามชาติสะดวกและซับซ้อนมากขึ้น นอกจากนี้ยังมีโอกาสที่กลุ่มก่อการร้ายและกลุ่มอาชญากรรมข้ามชาติจะร่วมมือหรือแสวงประโยชน์ซึ่งกันและกัน ถึงแม้ว่า "อินเทอร์เน็ต" จะช่วยให้ผู้สูงอายุมีสังคม ส่งเสริมการเรียนรู้อย่างต่อเนื่อง และช่วยลดความเหลื่อมล้ำทางเทคโนโลยีสารสนเทศก็ตาม บางครั้งอาจเกิดการรู้ไม่เท่าทันภัยในโลกออนไลน์ที่อาจจะส่งผลกระทบต่อตัวผู้สูงอายุ ผู้สูงอายุต้องระวังการฉ้อโกงทางอินเทอร์เน็ต ไม่ว่าจะเป็นการฉ้อโกงในเรื่องการประกันสุขภาพ

ยาปลอม ผลิตภัณฑ์ชะลอความแก่ การค้าออนไลน์ หรืออื่น ๆ ด้วย เพราะพวกมิจฉาชีพมักคิดว่าผู้สูงอายุเป็นเหยื่อที่หลอกง่าย เชื่อง่าย (ศิริชัย ทรัพย์ศิริ, 2552)

อาชญากรไซเบอร์เริ่มหันไปโจมตีผู้สูงอายุมากขึ้นจนกำลังเป็นปัญหาใหญ่ไปทั่วโลก เนื่องจากหลายประเทศเริ่มเข้าสู่สังคมผู้สูงอายุ วัยเกษียณหลายคนเป็นโสด เป็นปู่ย่าตายายขาดการดูแลเอาใจใส่ สถานภาพเหล่านี้ทำให้เข้าถึงได้ง่ายและตกเป้าหมายของเหล่าอาชญากร ปัจจัยอื่น ๆ ที่ผลักดันให้ผู้สูงวัยตกเป็นเหยื่อ อย่างเช่น ผู้สูงอายุจำนวนมากเพิ่งเข้าถึงเทคโนโลยี ใช้รหัสผ่านง่ายๆ ไม่เรียนรู้วิธีป้องกันตัวเองจากภัยไซเบอร์ใหม่ๆ ที่สำคัญ ผู้คนในช่วงอายุนี้โดยทั่วไปมีความสุภาพกับคนแปลกหน้า อาชญากรไซเบอร์จะใช้กลวิธีหลอกลวงที่เหมาะกับพวกเขาและตกเป็นเหยื่อในท้ายที่สุด (เห็นได้จากคดีหลอกลวงผู้สูงวัยดังๆ ในประเทศไทย) แต่วิธีการลักษณะนี้ ถ้าผู้สูงอายุมีความ "ตระหนักรู้" เพียงเล็กน้อย พวกเขาก็จะรอดพ้นจากการตกเป็นเหยื่อจากภัยคุกคามทางไซเบอร์ มีจำนวนผู้ใหญ่ที่ใช้งานโซเชียลมีเดียสูงถึง 72% เลยทีเดียว นับเป็นตัวเลขที่สูงมาก และช่วงอายุเฉลี่ยที่ใช้งานนั้นคือ 30-49 ปี (78%) 50-64 ปี (60%) และ 65 ปีขึ้นไป (43%) นั่นหมายความว่าแม้แต่คนอายุ 65 ปี หรือมากกว่า ก็ยังใช้งานโซเชียลมีเดียแทบจะเป็นหลัก อันตรายที่แฝงมากับการติดโซเชียลของผู้สูงอายุ สิ่งที่มีประโยชน์มากแค่ไหนถ้าใช้งานอย่างผิดวิธีหรือมากเกินไปก็จะให้โทษได้อยู่ดี การเล่นโซเชียลมีเดียของผู้สูงอายุก็เช่นกัน เพราะมันเสี่ยงต่อการเกิดอันตรายหรือภัยร้ายได้มากกว่าที่คิด และรูปแบบที่ผู้สูงอายุมักเสี่ยงโดนหลอกได้ง่ายจากการใช้การเล่นโซเชียลมีเดีย (Bangkokbanksme, (2562)

1. การติดกับดัก Fake News บนโลกออนไลน์นี้มีข่าวสารปลอมๆ เกิดขึ้นมากมายทุกวัน ซึ่งมีทั้งภาพตัดต่อการนำคำพูดคนนั้นมาใส่คนนี้ การปลุกปั่นต่าง ๆ ทั้งทางการเมือง เชื้อชาติ และศาสนา ซึ่งผู้ใหญ่จะขาดภูมิต้านทานเรื่องนี้ ทำให้เห็นภาพอะไรที่น่าสนใจ ก็จะแชร์ต่อไปทันที โดยไม่วิเคราะห์หรือไตร่ตรอง โดยเชื่อฝังหัวสนิทใจว่า นี่คือสิ่งที่ถูกต้อง จึงอาจทำให้เกิดความเข้าใจผิดที่รุนแรงและเกิดผลเสียได้

2. การโดนหลอกลวงง่ายนอกจากเรื่องข่าวปลอมแล้ว พวกข่าวสารการหลอกลวงต่าง ๆ กลุ่มผู้ใหญ่เองก็จะไม่ค่อยทันกับสื่อปลอมๆ เหล่านี้ เช่น การหลอกให้โอนเงินช่วยเหลือผู้เจ็บป่วย ผ่านทางสื่อสังคมออนไลน์ (Social Media) เพิ่มมากขึ้นเรื่อย ๆ เพราะเทคโนโลยีที่มีการพัฒนา ช่วยให้การโอนเงินสะดวกสบายเพียงแค่ปลายนิ้วมือ หรือการยกเอาบุคคลที่ดูน่าเชื่อถือมาอ้างอิง ให้เกิดน้ำหนักเพื่อหลอกขายสินค้า ซึ่งนี่ไม่ใช่ความผิดของผู้สูงอายุที่เขารู้ไม่เท่าทัน มันเป็นเพราะเขาเกิดมาในยุคที่มีแค่การสื่อสารทางเดียว สื่อต่าง ๆ ที่จะออกมาได้จะต้องกรองแล้ว และมีความน่าเชื่อถือ พอยุคสมัยเปลี่ยนไปจนใคร ๆ ก็ทำหน้าที่เป็นสื่อได้ จึงทำให้คนที่ปรับตัวไม่ทันหลงเชื่อข้อมูลผิดๆ เหล่านี้ไป

3. การแชร์ของผู้สูงอายุ ซึ่งจะขาดซึ่งการไตร่ตรอง ทำให้แม้จะเป็นข่าวปลอมแค่ไหน ถ้ามันสะเทือนใจหรือทัชกับอารมณ์ของเขา ก็มีโอกาสที่จะถูกแชร์ต่อไปอย่างรวดเร็ว

4. เป็นเหยื่อการตลาดออนไลน์ เรื่องของการสั่งของออนไลน์ เพราะความเข้าถึงง่ายของเทคโนโลยี ความสะดวกสบาย รวมเร็วและบางร้านก็ไม่มีจำหน่ายในประเทศไทย การเติบโตทางธุรกิจออนไลน์ก็ทำให้เกิดปัญหาหลายอย่างตามมา เช่น ได้รับสินค้าที่ไม่มีคุณภาพ การโฆษณาเกินจริง การหลอกให้โอนเงินและไม่ได้รับสินค้าที่สั่ง หรือบางครั้งถูกยกเลิกบริการและไม่สามารถติดตามขอเงินคืนได้ เนื่องจากไม่ทราบชื่อที่แท้จริงและที่อยู่ของผู้ประกอบธุรกิจ

วิธีรับมือกับความเสี่ยงของผู้สูงอายุต่อภัยคุกคามทางไซเบอร์ (Guilines to Deal with Risks of Elderly Person for Cyber Threats)

1.วิธีรับมือ เมื่อติดกับดัก Fake News 10 วิธี (ทสพร ฐานะตระกูล, 2563)

1.1 สังเกตหัวข้อข่าว ซึ่งข่าวปลอมมักจะมีพาดหัวข่าวที่สะดุดตา หรือหวา ดูไม่น่าเป็นไปได้ และมักจะใช้อักษรตัวหนา หรือเครื่องหมายอัศเจรีย์ (!)

1.2 สังเกตลิงก์ข่าว มักจะเป็นลิงก์ข่าวที่ใช้ URL คล้ายกับของสำนักข่าว จนบางทีแทบแยกไม่ออก อาจปรับเปลี่ยนเล็กน้อยและเลียนแบบแหล่งข่าวจริง

1.3 สังเกตชื่อแหล่งข่าวว่ามีความน่าเชื่อถือหรือไม่ หรือเป็นที่รู้จักหรือไม่

1.4 สังเกตสิ่งผิดปกติอื่น ๆ เนื่องจากเว็บไซต์ข่าวปลอมมักสะกดคำผิด หรือวางเลย์เอาท์ไม่เป็นมืออาชีพ

1.5 สังเกตรูปภาพหรือวิดีโอในข่าว มักบิดเบือนจากข่าวจริง หรือไม่เกี่ยวข้องกับกับเรื่องนั้น ๆ เลย

1.6 สังเกตวันที่ ลำดับเหตุการณ์ต่าง ๆ ว่ามีความสมเหตุสมผลหรือไม่ หรือเป็นการนำข่าวเก่าแล้วมาเปลี่ยนวันที่ใหม่หรือไม่

1.7 สังเกตแหล่งข้อมูลที่มาในข่าว โดยตรวจสอบหลักฐานมีอ้างอิงหรือไม่

1.8 สังเกตจากแหล่งที่มาอื่น ๆ โดยดูรายงานข่าวจากที่อื่น ๆ ประกอบ

1.9 สังเกตจากบริบทของเนื้อหา เนื่องจากข่าวปลอมบางครั้งอาจมาในรูปแบบของการล้อเลียน เสียดสี หรือตลกขบขัน

1.10 ระมัดระวังเรื่องที่จงใจให้เป็นข่าว

2. วิธีการรับมือเมื่อโดนหลอกให้โอนเงิน

2.1 การป้องกันมิจฉาชีพทาง Social Media

2.1.1 ไม่เปิดเผยข้อมูลส่วนบุคคล เช่น เลขบัตรประชาชน เลขที่บัญชี บน Social Media เพราะอาจเป็นช่องทางให้มิจฉาชีพนำข้อมูลดังกล่าวไปปลอมแปลง หรือสวมตัวตนของเราได้

2.1.2 ตรวจสอบความสัมพันธ์ทุกครั้งก่อนรับบุคคลอื่น ๆ มาเป็นเพื่อนกับเราใน Social Media เพื่อป้องกันการแฝงตัวของมิจฉาชีพ

2.1.3 ตั้งสติและตรวจสอบธุรกรรมทุกครั้งหากต้องทำธุรกรรมทางการเงินกับบุคคลหรือองค์กรใน Social Media เช่น การสอบถามจากช่องทาง Call Center ของหน่วยงานที่ถูกอ้างถึง เป็นต้น และควรเช็กรายละเอียดก่อนโอนว่าเลขที่บัญชี ชื่อบัญชี และจำนวนเงินถูกต้องหรือไม่

2.2 ขั้นตอนรับมือหากตกเป็นเหยื่อจากมิจฉาชีพทาง Social Media

2.2.1 แจ้งธนาคารเจ้าของบัญชีของเราถึงเหตุการณ์ที่เกิดขึ้นพร้อมวิธีแก้ไข

2.2.2 รีบรายงานข้อมูลแก่ศูนย์ให้ความช่วยเหลือ และแจ้งแก่บุคคลต่าง ๆ ที่เรามีความสัมพันธ์ด้วยให้เร็วที่สุด

2.2.3 รวบรวมหลักฐานที่เกี่ยวข้องกับการกระทำความผิดทั้งหมด เช่น หน้าโปรไฟล์ที่ถูกปลอมขึ้น หน้าจอการสนทนา หลักฐานการโอนเงิน แล้วนำหลักฐานทั้งหมดไปแจ้งความ ณ สถานีตำรวจ ดังนั้น เราจึงควรเก็บข้อมูลต่าง ๆ ทุกครั้งเมื่อมีการทำธุรกรรมทางออนไลน์

2.3 ข้อเตือนใจกับ 5 สิ่งที่คุณไม่ควรโพสต์ลงใน Social Media เพื่อป้องกันไม่ให้มิจฉาชีพนำไปปลอมแปลงข้อมูล

2.3.1 บัตรประชาชน ไม่ควรถ่ายรูปบัตร หรือโพสต์เลขบัตรประชาชนโดยเด็ดขาด เพราะอาจถูกนำไปทำธุรกรรมทางการเงิน

2.3.2 บัตรเครดิต ไม่ควรถ่ายรูปบัตรทั้งด้านหน้า และด้านหลังบัตรที่มีเลข CVV เพราะข้อมูลเหล่านี้สามารถถูกนำไปใช้ในการทำธุรกรรมออนไลน์ได้

2.3.3 การ Check-in ตามสถานที่ต่าง ๆ ไม่ควร Check-in ตลอดเวลา เพราะจากการสำรวจพบว่า กว่า 75% มิจฉาชีพจะใช้ข้อมูลการ Check-in ในการค้นหาตำแหน่งที่อยู่ในปัจจุบันของเหยื่อได้

2.3.4 ลายนิ้วมือ ข้อนี้อาจจะตรงกับใครหลาย ๆ คนที่ชอบถ่ายรูป เพราะการโพสต์ภาพที่มีการโชว์สองนิ้ว ด้วยเทคโนโลยีสมัยใหม่การถ่ายรูปเห็นปลายนิ้วภายใน 3 เมตร อาจทำให้ถูกสวมรอยลายนิ้วมือ และขโมยข้อมูลสำคัญได้

2.3.5 ตั๋วเครื่องบินหรือบอร์ดดิ้งพาส ไม่ควรโพสต์โชว์ เพราะมิจฉาชีพอาจนำไปใช้ในการค้นหาข้อมูลสู่บ้านของเราได้ หรือข้อมูลบนบัตร เช่น ชื่อ-นามสกุล จุดเริ่มต้น จุดหมายปลายทาง และบาร์โค้ด ทำให้สามารถเปลี่ยนแปลงการเดินทางของเราได้อีกด้วย (kapookonline, 2562)

3. การคิดก่อนที่จะแชร์ข้อมูล ข้อมูลที่เผยแพร่ในสื่อสังคมออนไลน์ต่าง ๆ ส่วนใหญ่ไม่ได้มาจากแหล่งอ้างอิงที่เชื่อถือได้ แต่มักจะมาจากเพื่อนฝูง คนรู้จัก หรือบุคคลมีชื่อเสียงที่อาจจะไม่ได้มีความรู้เท่าทันสื่อ

3.1 'ไม่มีลิงก์' อย่าเพิ่งแชร์ ข้อมูลที่ไม่มีลิงก์กลับไปยังต้นตอ มักจะเป็น 'ข่าวปลอม' แต่ข้อมูลที่มีลิงก์แนบมาด้วย ก็ใช่ว่าจะจริงร้อยเปอร์เซ็นต์ แต่ต้องกลับไปดูยังลิงก์ข่าวต้นตอว่ามีความน่าเชื่อถือหรือไม่ เพราะปัจจุบันนี้มีเว็บไซต์เลียนแบบสำนักข่าวหรือมีการแอบอ้างตัวเป็นบุคคลอื่น ๆ อยู่เต็มไปหมด

ข้อสังเกตง่ายๆ ว่าเว็บไซต์เป็นของแท้หรือเทียม อาจดูได้จากข้อมูลที่เผยแพร่ว่ามีลักษณะชวนให้กดเข้าไปดูข้อมูลเพิ่มเติมแบบ 'คลิกเบท' หรือไม่ และแม้เว็บไซต์จะดูน่าเชื่อถือก็ต้องดูไปถึงข้อมูลอื่น ๆ ที่เผยแพร่ก่อนหน้านั้นด้วย รวมถึงเปรียบเทียบกับข้อมูลในเว็บไซต์อื่น ๆ ว่ามีผู้รายงานเรื่องดังกล่าวไว้บ้างหรือไม่

3.2 สิ่งที่เราชอบ อาจไม่ใช่สิ่งที่ 'ควรเชื่อ' ระบบจัดการข้อมูลในสื่อออนไลน์ ทั้ง Facebook, twitter, Instagram, line, google จะเรียงลำดับข้อมูลตามความนิยม สิ่งที่ผู้ใช้สื่อมองเห็นเป็นอันดับแรก จึงมักเป็นสิ่งที่เราแสดงความรู้สึกเชิงบวกหรือข้อมูลที่ค้นหาบ่อย แต่ไม่ได้หมายความว่าข้อมูลที่ชอบจะเป็นความจริงเสมอไป เพราะคนส่วนใหญ่ไม่ตั้งคำถามกับข้อมูลที่ตัวเอง 'ถูกใจ' โดยเฉพาะการแชร์สิ่งที่ตัวเอง 'ถูกใจ' ในสื่อออนไลน์ แต่เมื่อแชร์ข่าวหรือข้อมูลไปแล้ว กลับส่งผลกระทบต่อชื่อเสียงและความน่าเชื่อถือ เพราะสิ่งที่แชร์เป็นข่าวปลอมหรือข้อมูลลวงโลก

3.3 คิดก่อนแชร์ ปลอดภัยกว่า สื่อออนไลน์อยู่ได้ด้วยการมีปฏิสัมพันธ์กับผู้ใช้ ยิ่งมีคนกดไลค์หรือตอบโต้มากเท่าไหร่ ยิ่งกระตุ้นให้ข้อมูลเหล่านั้นถูกแชร์ไปไกลขึ้น ผู้ที่ต้องการหาผลประโยชน์

จากสื่อออนไลน์จึงมักจะใช้พฤติกรรมเช่นนี้ของผู้ใช้สื่อเป็นเครื่องมือ เพราะการเผยแพร่ข้อมูลปลอมเพื่อกระตุ้นเร้าอารมณ์ความรู้สึก ทั้งเรื่องอื้อฉาวหรือประเด็นที่เป็นข้อขัดแย้งในสังคม รวมถึงข้อความสร้างแรงบันดาลใจที่อ้างอิงมาแบบผิดๆ จะช่วยปั่นกระแสให้มีการแชร์ต่อไปมากขึ้น "ก่อนจะแชร์ ควรหยุดคิดสักนิด" แล้วถามตัวเองอีกครั้งว่า "แชร์ข้อมูลนี้แล้วได้อะไร และถ้าไม่แชร์แล้วจะเป็นยังไง" ถ้าข้อมูลที่อยากแชร์ไม่มีที่มาที่น่าเชื่อถือก็ไม่ควรแชร์ โดยเฉพาะข้อมูลที่ถูกใจแต่ตรวจสอบไม่ได้ หรือข้อมูลที่เพื่อนในสื่อออนไลน์แชร์กันเป็นจำนวนมาก (กองบรรณาธิการวอยซ์ออนไลน์, 2561)

4. วิธีรับมือเมื่อเป็นเหยื่อการตลาดออนไลน์

4.1 ขอรหัสประจำตัวประชาชน เป็นหลักฐานยืนยันตัวบุคคล เมื่อถูกหลอกลวง ID ประจำตัวประชาชนจะสามารถนำเราไปสู่ผู้หลอกลวงได้ แม้ว่ารหัสจะปลอมแปลงเรายังคงสามารถยื่นรายงานตำรวจเพื่อค้นหาได้

4.2 เลขที่บัญชีธนาคาร ทุกคนที่ซื้อสินค้าออนไลน์เป็นประจำจะทราบว่าหมายเลขบัญชีธนาคารเป็นข้อมูลที่สำคัญในการทำธุรกรรมออนไลน์ ดังนั้นนักต้มตุ๋นจะรีบร้อนที่จะส่งหมายเลขบัญชีธนาคารไปให้เหยื่อเพื่อพยายามให้เหยื่อโอนเงินมาให้เร็วที่สุด แน่นอนว่าหมายเลขบัญชีเป็นอีกหลักฐานหนึ่งในการค้นหาข้อมูลของนักต้มตุ๋น

4.3 ชื่อผู้ขาย พร้อมชื่อเจ้าของบัญชีก่อนโอนเงิน เทคโนโลยีในปัจจุบันเราสามารถหาค้นหาบุคคลออนไลน์โดยรู้เพียงชื่อของพวกเขาผ่านวิธีการต่าง ๆ เช่น Facebook, Instagram, line อย่างไรก็ตามเราสามารถใช้ข้อมูลเหล่านี้เพื่อค้นหานักต้มตุ๋นด้วยรหัสประจำตัวประชาชนหรือหมายเลขบัญชีธนาคารในกรณีส่วนใหญ่ สิ่งที่เกิดขึ้นในโลกอินเตอร์เน็ตจะทำให้มีข้อมูลและร่องรอยต่าง ๆ ยังคงอยู่ ดังนั้นเราอาจสามารถหาข้อมูลเพิ่มเติมเกี่ยวกับความผิดทางอาญาได้ ตัวอย่างเช่น สิ่งที่ถูกขายความคิดเห็นของลูกค้าโพสต์เกี่ยวกับความผิดทางอาญาหากมีการหลอกลวงบุคคลอื่น ๆ ด้วย (กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, 2562)

ขั้นตอนการแจ้งความ

1. ให้ผู้เสียหาย เตรียมเอกสารส่วนตัว และสำเนาบัตรประจำตัวประชาชน

2. กรณีที่เสียหายต่อชื่อเสียง ให้เตรียมหลักฐาน ที่พบว่ามีการกระทำความผิด เช่น ปรินส์เอกสารหน้าจอ หน้าเว็บไซต์ หน้าโปรแกรมไลน์ โปรแกรม Facebook หรือหน้าเพจที่พบการกระทำความผิด

3. กรณีที่เสียหายต่อทรัพย์ ให้เตรียมหลักฐานที่พบการกระทำความผิด การหลอกลวง ปรินส์เอกสารออกมาจากระบบคอมพิวเตอร์ให้เรียบร้อย หลักฐานการโอนเงิน เป็นต้น

4. ให้ไปแจ้งความ ณ สถานีตำรวจท้องที่เกิดเหตุ สถานีตำรวจนครบาล หรือสถานีตำรวจภูธร หรือท่านสามารถเดินทางมา ร้องทุกข์ที่กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ได้เช่นกัน

แนวทางในการป้องกันภัยทางไซเบอร์ (Guidelines for Cyber Threats Prevention)

แนวทางทั่วไปในการรับมือกับอาชญากรรมทางไซเบอร์ในสังคมไทย ประกอบด้วยวิธีการ ดังต่อไปนี้ (Techsauce Team, 2560)

1. เลือกใช้งาน web browser ที่ทันสมัย ตัวอย่างเช่น Google Chrome มีการแจ้งเตือนผู้ใช้ เมื่อเข้าเว็บไซต์ต่าง ๆ อยู่ 3 ระดับ ได้แก่ Secure (เว็บไซต์ที่ใช้ protocol https) Info (เว็บไซต์ที่ใช้ protocol httpsทั่วไปและมีความน่าเชื่อถือ) และ Not Secure หรือ Dangerous (เว็บไซต์ที่ไม่ปลอดภัยให้ระวังการใช้งาน เนื่องจากทาง Google อาจจะตรวจสอบมัลแวร์)

2. ทดสอบ link ที่ไม่มั่นใจ ถ้าต้องการเปิด link ที่ไม่แน่ใจเรื่องความปลอดภัย ให้ลอง copy link URL นั้นไปวางที่ search engine เช่น Google หรือ Bing ถ้าพบผลลัพธ์จากการค้นหา อย่างน้อยก็มั่นใจได้ระดับหนึ่งว่าเป็นเว็บไซต์ที่ปลอดภัย เนื่องจากระบบแสดงผลลัพธ์การค้นหาของ search engine มักจะป้องกันผู้ใช้งานจากเว็บไซต์ที่มีมัลแวร์ (เช่น แจ้งว่า this site may harm your computer)

3. การใช้งานเว็บไซต์ธุรกรรมทางการเงิน การใช้งานเว็บไซต์ธนาคาร หรือการทำธุรกรรมทางการเงินต้องตรวจสอบให้มั่นใจก่อนการ Login เข้าใช้งานระบบ หรือการกรอกข้อมูลบัตรเครดิต ตรวจสอบ URL ของเว็บไซต์ว่าเป็นเว็บไซต์ของธนาคารที่กำลังใช้งานอยู่จริงหรือเป็น เว็บไซต์ของผู้ให้บริการรับชำระเงินผ่านบัตรเครดิต ตรวจสอบว่าเว็บไซต์ที่กำลังใช้งานเป็น https://

4. การใช้จ่ายบัตรเครดิต การใช้งานบัตรเครดิต เพื่อชำระค่าสินค้าหรือบริการ ถ้าเป็นบัตร VISA ควรสมัครใช้บริการ Verified by VISA สำหรับบัตร Mastercard ควรสมัครใช้บริการ MasterCard Secure Code หรือสมัครบริการแจ้งเตือนเมื่อมีการใช้จ่ายบัตรเครดิต และควรตรวจสอบรายการใช้จ่ายอยู่ เสมอ

5. การใช้งานอินเทอร์เน็ตผ่านเครื่องคอมพิวเตอร์สาธารณะ การใช้งานอินเทอร์เน็ตผ่านเครื่องคอมพิวเตอร์สาธารณะ ควรใช้งานโหมด Private windows เพื่อรักษาความปลอดภัยของข้อมูล เนื่องจากการใช้งานโหมดนี้ เมื่อผู้ใช้เลิกใช้งาน และปิด โปรแกรม browser ข้อมูลต่าง ๆ เช่น cookies จะถูกลบทิ้ง ซึ่ง browser แต่ละตัวจะมีชื่อเรียกที่แตกต่างกัน

Internet Explorer ใช้ชื่อ InPrivate Browsing

Mozilla Firefox ใช้ชื่อ Private Browsing

Google Chrome ใช้ชื่อ Incognito mode

Opera ใช้ชื่อ Private Browsing Safari ใช้ชื่อ Private Browsing

6. หมั่น sign out หลังจากใช้งานเว็บไซต์ที่มีระบบการ Login เรียบร้อยแล้ว ควรจะ Sign out หรือ Log out ออกจากระบบทุกครั้ง

7. หลีกเลี่ยงการดาวน์โหลดโปรแกรม หรือเกมฟรีจากแหล่งที่ไม่น่าเชื่อถือ

8. หลีกเลี่ยงการใช้งานผ่านฟรี Wi-Fi สาธารณะที่ไม่รู้จัก เนื่องจากอาจจะโดนโจรกรรมข้อมูลได้

9. หลีกเลี่ยงการชาร์จโทรศัพท์มือถือฟรีจากที่สาธารณะ ซึ่งอาจจะโดนขโมยข้อมูล หรือที่เรียกว่า “Juice Jacking”

10. ติดตั้ง Antivirus และอัพเดตให้ทันสมัยอยู่เสมอ

ประเทศไทยได้ให้ความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์มาอย่างต่อเนื่อง ในปี 2562 มีการประกาศใช้กฎหมายให้หน่วยงานตระหนักถึงความสำคัญกับการดูแลข้อมูลและตระหนักถึงภัยไซเบอร์มากขึ้น ประกอบด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยกฎหมายหลายฉบับได้กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เอาไว้ แบ่งออกได้เป็น 3 กลุ่ม คือ

1) กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งได้กำหนดมาตรการสำคัญด้านความมั่นคงปลอดภัยเอาไว้เพื่อลดความเสี่ยงและทำให้เกิดความน่าเชื่อถือเมื่อมีการใช้ระบบคอมพิวเตอร์หรือระบบอินเทอร์เน็ตในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งครอบคลุมทั้งในการพาณิชย์อิเล็กทรอนิกส์ รวมไปจนถึงการให้บริการทางอิเล็กทรอนิกส์ของรัฐ หรือในงานรัฐบาลอิเล็กทรอนิกส์นั้นมีความมั่นคงปลอดภัย ตลอดจนกำหนดให้หน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Information Infrastructure Protection) ต้องปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัย และต่อมาก็ได้มีการตรากฎหมายจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ซึ่งได้กำหนดอำนาจหน้าที่สำคัญเพิ่มเติมอีกประการ คือการยกระดับทักษะผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งทำหน้าที่ดูแลศูนย์ประสานความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)

2) กฎหมายระดับอนุบัญญัติหรือกฎหมายลูกที่กำหนดมาตรการในการกำกับดูแลตลาดเงินโดยธนาคารแห่งประเทศไทย และตลาดทุนโดยสำนักงานคณะกรรมการหลักทรัพย์และตลาดหลักทรัพย์ แห่งประเทศไทย รวมทั้งในการกำกับดูแลธุรกิจประกันภัยโดยกำนักงานคณะกรรมการกำกับและส่งเสริมการ ประกอบธรุกิจประกันภัยเพื่อให้บริการของผู้ประกอบการในภาคเศรษฐกิจที่มีการกำกับดูแลนั้นมีความมั่นคงปลอดภัย

3) กฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งกำหนดฐานความผิดและบทลงโทษสำหรับการก่ออาชญากรรมทางคอมพิวเตอร์ โดยมีกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีภายใต้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีภายใต้สำนักงานตำรวจแห่งชาติ

อย่างไรก็ตาม การกำหนดมาตรการด้านความมั่นคงปลอดภัยเอาไว้ในกฎหมายที่เกี่ยวข้องได้เน้นให้ความสำคัญในด้านมาตรการป้องกันหรือลดความเสี่ยงการสร้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยและการกำหนดฐานความผิดและบทลงโทษ ซึ่งอาจครอบคลุมเพียงบางมิติของการรักษาความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น จึงยังจำเป็นต้องยกระดับความเข้มแข็งเพื่อเตรียมความพร้อมของประเทศด้านดังกล่าวให้ครอบคลุมถึงมิติของการเฝ้าระวังภัยคุกคาม หรือการดำเนินการใด ๆ ที่จำเป็นเมื่อมีการโจมตี หรือเมื่อเกิดวิกฤติต่อความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนการกำหนดมาตรการในการทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง เมื่อต้องเผชิญกับการโจมตี หรือภาวะวิกฤติดังกล่าว ที่อาจส่งผลกระทบอย่างมีนัยสำคัญและรุนแรง อันส่งผลกระทบต่อความมั่นคงของประเทศในภาพรวม นอกจากนั้นยังขาดแนวทางปฏิบัติและบรรทัดฐานในการบริหารจัดการไซเบอร์สเปซ (Cyberspace) ที่ชัดเจนในระดับภูมิภาคและระดับระหว่างประเทศ ซึ่งไทยเองก็ควรให้ความสำคัญกับการสนับสนุนให้มีบรรทัดฐาน และแนวทางปฏิบัติระหว่างประเทศที่เป็นที่ยอมรับ เพื่อส่งเสริมความร่วมอื่นระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์และการป้องกัน

ความขัดแย้งทางไซเบอร์ระหว่างรัฐอันอาจเกิดขึ้นได้ในอนาคต จึงจำเป็นต้องมีการผลักดันการจัดทำกรอบนโยบายหรือยุทธศาสตร์การรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติและกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร่งด่วนต่อไป (ไซเบอร์สเปซ (Cyberspace) คือเครือข่ายอินเตอร์เน็ต (Internet) ซึ่งทำให้การเคลื่อนย้ายและส่งผ่านข้อมูลข่าวสารจากที่หนึ่งไปอีกที่หนึ่งนั้นกระทำได้โดยง่าย ไม่จำกัดเรื่องระยะทางและเวลา อีกทั้งสามารถส่งข้อมูลได้หลากหลายรูปแบบ เช่น ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง โดยใช้เครือข่ายโทรคมนาคมเป็นตัวเชื่อมนั้นเอง ไซเบอร์สเปซ นั้นมีความสามารถในการยืนยันตัวตน ซึ่งสามารถตรวจสอบและนำพาไปยังผู้ใช้จริง ๆ ในโลกแห่งความจริงที่มิใช่ไซเบอร์สเปซได้ด้วย เช่น การใช้ Line, Facebook, Twitter เป็นต้น) (สำนักงานสภาความมั่นคงแห่งชาติ, ม.ป.ป.)

สังคมไทยเริ่มเป็นสังคมดิจิทัลอย่างเต็มรูปแบบรวมถึงนโยบายของรัฐบาลที่เสนอให้ทุกภาคส่วนร่วมกันขับเคลื่อนนโยบายไทยแลนด์ 4.0 จากข้อมูลการสำรวจโดยสำนักงานสถิติแห่งชาติ ในปี 2560 พบว่ามีผู้สูงอายุเพียงร้อยละ 4.2 ที่ได้รับข้อมูลข่าวสารที่เป็นประโยชน์จากอินเทอร์เน็ตหรือโซเชียลมีเดีย ผู้สูงอายุไทยในอนาคตจึงต้องรู้เท่าทันและสามารถใช้ประโยชน์จากอินเทอร์เน็ต โซเชียลมีเดีย และสมาร์ทโฟน ในการรับรู้ข้อมูลข่าวสาร โปรแกรมการดูแลสุขภาพต่าง ๆ ตลอดจนการทำธุรกรรมทางการเงิน ไม่ตกเป็นผู้เสียหายโดนหลอกจากการเผยแพร่ข่าวสารปลอม นำไปสู่การละเมิดสิทธิ การฉ้อโกงทรัพย์สิน ในปัจจุบันเทคโนโลยีมีความสำคัญกับผู้สูงอายุเพราะจะช่วยให้ผู้สูงอายุก้าวทันโลกสามารถค้นหาข้อมูลต่าง ๆ ได้ และเป็นเครื่องมือในการติดต่อกับลูกหลาน แต่ในปัจจุบันเทคโนโลยีก็มีฟังก์ชันหลากหลายมากยิ่งขึ้น ผู้สูงอายุก็ยังเป็นบุคคลที่น่าห่วงใยในเรื่องของการถูกหลอกลวง โดยเฉพาะถูกหลอกลวงจากการถูกโฆษณาสินค้าสุขภาพต่าง ๆ มากที่สุด รวมไปถึงการส่งต่อข้อความหรือรูปภาพที่ไม่เป็นความจริง เนื่องจากยังรู้ไม่เท่าทันการใช้สื่อเหล่านี้

ภัยคุกคามทางไซเบอร์ หรือ อาชญากรรมไซเบอร์ ถือเป็นกิจกรรมที่เป็นความผิดทางอาญาที่ดำเนินการโดยใช้คอมพิวเตอร์ หรือ อินเทอร์เน็ตเป็นเครื่องมือ ปัจจุบันตัวเลขการคุกคามมีโนวโน้มเพิ่มสูงขึ้นมาก โดยเฉพาะในสหรัฐอเมริกาอย่างเดียวก็เสียหายเป็นมูลค่ารวมกว่า 6,000 ล้านเหรียญสหรัฐ ในขณะที่ผู้บริโภคเริ่มหันมาพึ่งพาเทคโนโลยีในชีวิตส่วนตัวของพวกเขามากขึ้น เทคโนโลยีนี้เหล่านี้เป็นแหล่งเก็บข้อมูลสำคัญของผู้คน ไม่ว่าจะเป็นข้อมูลส่วนตัว ความลับทางธุรกิจ รหัสผ่านบัญชี หลายสิ่งที่กล่าวมานี้ล้วนเก็บอยู่ในรูปแบบดิจิตอลอาจถูกแฮ็กจากผู้ที่ไม่ประสงค์ดีจากภายนอก อินเทอร์เน็ตเป็นแหล่งความรู้ขนาดใหญ่ที่เข้ามาเป็นส่วนหนึ่งของเราได้อย่างกลมกลืน ทั้งในด้านการเรียน การทำงาน และการดำเนินชีวิตประจำวัน เช่น การค้นหาข้อมูลเพื่อมาทำรายงาน ส่งอาจารย์หรือหัวหน้า, การค้นหาเส้นทางของสถานที่ที่ต้องการ, การค้นหาข้อมูลเพื่อประกอบการตัดสินใจในการซื้อสินค้าหรือบริการตั้งแต่สินค้าขนาดเล็กไปจนถึงสินค้าขนาดใหญ่ เช่น รถยนต์หรือที่อยู่อาศัย รวมไปถึงการทำธุรกรรมทางการเงินต่าง ๆ อีกด้วย รัฐบาลควรจัดให้มีเครือข่ายในการช่วยสอนให้ผู้สูงอายุใช้เทคโนโลยีและสื่อดิจิทัลเป็น รวมถึงสอนการรู้เท่าทันสื่อออนไลน์ด้วย

เชื่อว่าอนาคตผู้สูงอายุจะก้าวทันยุคดิจิทัลดีขึ้น เพราะผู้สูงอายุในอนาคตก็คือคนสมัยใหม่ในปัจจุบันที่จะชราไปในวันข้างหน้า ซึ่งไม่น่าห่วงเท่าปัจจุบัน เพราะอาชญากรรมไซเบอร์ พุ่งสูงขึ้นทุกปี สวนทางปัญหาอาชญากรรมลดลงต่อเนื่องเหตุการณ์ ชก ชิง วิ่งราว ทำร้ายร่างกาย และอีกหลายเหตุการณ์ที่ส่งผลกระทบกับ

การใช้ชีวิตของประชาชน ถือเป็นภัยร้ายใกล้ตัวที่เกิดขึ้นได้ทุกที่ ทุกเวลา ขณะที่ผู้ก่อเหตุเองมีตั้งแต่เด็กเยาวชนไปจนถึงผู้สูงอายุ เพราะยิ่งสังคมมีปัญหามากขึ้นเท่าใด ก็จะส่งผลให้ปัญหาเหล่านี้ เจริญเติบโตมากขึ้นเป็นเท่าตัว ทั้งนี้หากประชาชนมีข้อมูลเบาะแสเกี่ยวกับการกระทำความผิดในลักษณะข้างต้น สามารถติดต่อผ่าน 5 ช่องทาง ดังนี้ 1.การติดต่อด้วยตนเองที่ดีเอสไอ 2.ติดต่อผ่านเว็บไซต์ www.dsi.go.th 3.การยื่นหนังสือที่กรมสอบสวนคดีพิเศษ 4.ติดต่อผ่านสายด่วนหรือ Call Center 1202 (โทรฟรีทั่วประเทศ) และ 5.การติดต่อผ่านศูนย์ปฏิบัติการคดีพิเศษทั้ง 10 เขต โดยข้อมูลเบาะแสที่ประชาชนแจ้งเข้ามาจะถูกเก็บข้อมูลเป็นความลับ แม้จะมีการจับกุมมากมาย แต่ยังมีผู้เสียหายตกเป็นเหยื่ออยู่ตลอด โดยเฉพาะคดีคอลเซ็นเตอร์ แสร้งรักออนไลน์ แชร์ออนไลน์ แชทหลอกยืมเงิน ฯลฯ ฉะนั้นการระมัดระวังตัวเองไม่หลงเชื่อง่ายๆ น่าจะดีกว่ารอให้เจ้าหน้าที่กวาดล้างอาชญากรไซเบอร์ให้หมด

เอกสารอ้างอิง (References)

กองบรรณาธิการวอยซ์ออนไลน์. (2561). *กฎ 3 ข้อ ป้องกันแชร์ข้อมูลพลาดในโลกออนไลน์*. สืบค้นจาก http://www.voicetv.co.th/read/ryFd7rDcG.

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. (2562). *วิธีป้องกันโดนหลอกซื้อของออนไลน์*. สืบค้นจาก https://tcsd.go.th/วิธีป้องกันโดนหลอกซื้อ/.

ไกรวุฒิ วัฒนสิน. (2561). *รูปแบบการป้องกันอาชญากรรมที่กระทำต่อผู้สูงอายุ*. สืบค้นจาก https://research.police.go.th/index.php/datacenter/research/2558/-2560/286–33/file.

ทสพร ฐานะตระกูล. (2563). *เปิดวิธีป้องกัน 'ข่าวปลอม' ลวงลึกหลอกแชร์*. สืบค้นจาก https://www.bangkokbiznews.com/news/detail/861198.

ไทยรัฐออนไลน์. (2561). *ดีเอสไอ รับมือโจรไซเบอร์ ชี้อาชญากรรมปี 62 แนวโน้มก่อคดีสูง*. สืบค้นจาก https://www.thairath.co.th/news/local/bangkok/1457208.

บัณฑิต อาณาจักรานนท์. (ม.ป.ป.). *รูปแบบและตัวอย่าง ของอาชญากรรมทางคอมพิวเตอร์*. สืบค้นจาก https://www.gotoknow.org/posts/374163.

พิสิฐ ระฆังวงษ์ และ ประพนธ์ สหพัฒนา. (2561). *ปัจจัยที่มีผลต่อการตกเป็นเหยื่ออาชญากรรมที่เกิดขึ้นกับผู้สูงอายุ ในเขตกรุงเทพมหานคร*,วารสารรัฐประศาสนศาสตร์ ปีที่ 10 (ฉบับที่ 2) https://www.tci-thaijo.org/index.php/polscicmujournal/article//download /141378/158105/.

มณีรัตน์ อนุโลมสมบัติ. (2560).*สังคมผู้สูงวัยรับมือได้ด้วยเทคโนโลยี*. สืบค้นจาก https://www.bangkokbiznews.com/blog/detail/642056.

ศิริชัย ทรัพย์ศิริ. (2552). *ภัยออนไลน์...ผู้สูงอายุต้องระวัง*. สืบค้นจาก http://www.apdi2002.com/index.php?lay=boardshow&ac=webboard_show&WBntype=1&No=1260313.

สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ. (ม.ป.ป.).*สังคมสูงวัย60+*. สืบค้นจาก https://vulnerablegroup.in.th/wp-content/uploads/2018/08/สังคมสูงวัย.pdf.

สำนักงานสภาความมั่นคงแห่งชาติ. (ม.ป.ป.). ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564.

Bangkokbanksme. (2562). *สูงวัยติดโซเชียลเรื่องใกล้ตัวที่ต้องใส่ใจ*. สืบค้นจาก https://www.bangkokbanksme.com/en/ageingsociety-social-media.

Kapookonline. (2562). *ใช้สติป้องกันสตางค์ ก่อนโอนเงินผ่าน Social Media*. (2562). สืบค้นจาก https://money.kapook.com/view207616.html.

Techsauce Team. (2560). *สรุปความรู้ และคำแนะนำเรื่องความปลอดภัยบนอินเทอร์เน็ต*. สืบค้นจาก https://techsauce.co/tech-and-biz/internet-security-guidelines-cat-allsecure.

Thaireform. (2562). *ปี 64 ไทยมีคนชรา 13 ล้าน เข้าสู่สังคมสูงวัยสมบูรณ์*. สืบค้นจาก https://www.isranews.org/isranews-news/77916-news-779161.html.