เอกสารรายงานสรุป

การฝึกปฏิบัติ

วันอังคารที่ ๒๖ ธันวาคม ๒๕๖๖

หัวข้อ

การฝึกปฏิบัติด้านการวิเคราะห์อาชญากรรมในรูปแบบใหม่

ณ วิทยาลัยการยุติธรรม สำนักงานกิจการยุติธรรม

จัดทำโดย กลุ่มที่ ๑ การเวก

เอกสารรายงานนี้ เป็นส่วนหนึ่งของการฝึกอบรม

หลักสูตรการป้องกันอาชญากรรมกับการอำนวยความยุติธรรมในสังคม

Crime Prevention รุ่นที่ ๗ (CP๗)

วิทยาลัยกิจการยุติธรรม สำนักงานกิจการยุติธรรม

รายชื่อสมาชิก
กลุ่มที่ ๑ การเวก

ชื่อ - สกุล	ตำแหน่ง – สังกัด
๑. นางสาวกนกวรรณ แม้นเมฆ	นิติกรชำนาญการ กลุ่มงานเสนอแนะการแก้ไขปรับปรุงกฎหมาย ๒ สำนักกฎหมาย สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ
๒. นางสาวกมลวรรณ วิรุฬห์รัตน์	นักตรวจสอบภาษีชำนาญการ กองตรวจสอบภาษีกลาง กรมสรรพากร
๓. นางสาวชนิกา มหาวีระพจน์	นักสืบสวนสอบสวนชำนาญการ กองคดี ๒ สำนักงานป้องกันและปราบปรามการฟอกเงิน
๔. นาวาอากาศตรี ชุติวุฒิ สุขโกมล	รักษาราชการ หัวหน้าแผนกงานพิเศษ กองนิติธรรมทหาร กรมพระธรรมนูญ
๕. นางสาวณัฐพิมล สมเจษ	ผู้ช่วยเลขานุการนายกสภาทนายความ สภาทนายความ ในพระบรมราชูปถัมภ์
๖. นายณัฐวุฒิ อินทร์เนตร	นักวิชาการยุติธรรมชำนาญการ สำนักงานเลขานุการกรม สำนักงานกิจการยุติธรรม
๗. นางสาววีรวรรณ คำนุชนารถ	นักสืบสวนสอบสวนชำนาญการ สำนักงานคุ้มครองพยาน กรมคุ้มครองสิทธิและเสรีภาพ
๘. นายสุทธิธรรม สุทธิรักษ์	นิติกรชำนาญการ กองพัฒนาระบบการบังคับคดี กรมบังคับคดี
๙. นายสุรเดช ฉัตรเชิดเจริญกุล	ผู้ชำนาญงานอาวุโส กลุ่มคุ้มครองสิทธิประโยชน์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

การสรุปการฝึกปฏิบัติด้านการวิเคราะห์อาชญากรรมในรูปแบบใหม่

๑. <u>ชื่อหน่วยงาน/วันเดือนปี/ที่ทำกิจกรรม</u>

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) โดย พล.ต.ต.นิเวศน์ อาภาวศิน พ.ต.ท. ธนธัส กังรวมบุตร และคณะ/เมื่อวันอังคารที่ ๒๖ ธันวาคม ๒๕๖๖/การฝึกปฏิบัติด้านการวิเคราะห์อาชญากรรมในรูปแบบใหม่

๒. <u>ข้อมูลทั่วไปของหน่วยงาน</u>

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) เป็นหน่วยงานที่จัดตั้งขึ้นเมื่อวันที่ ๙ กันยายน ๒๕๖๓ ตามพระราชกฤษฎีกาแบ่งส่วนราชการสสำนักงานตำรวจแห่งชาติ (ฉบับที่ ๕) พ.ศ. ๒๕๖๓ กฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการอย่างอื่นในสำนักงานตำรวจแห่งชาติ (ฉบับที่ ๑๗) พ.ศ. ๒๕๖๓ ระเบียบสำนักงานตำรวจแห่งชาติ ว่าด้วยการกำหนดอำนาจหน้าที่ของส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ ๒๔) พ.ศ. ๒๕๖๓ ทั้งนี้ กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี มีหน้าที่และอำนาจ ดังต่อไปนี้

๒.๑ เป็นฝ่ายอำนวยการด้านยุทธศาสตร์ให้สำนักงานตำรวจแห่งชาติ ในการวางแผน ควบคุม ตรวจสอบ ให้คำแนะนำ และเสนอแนะการปฏิบัติงาน ตามหน้าที่และอำนาจของกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีและหน่วยงานในสังกัด

๒.๒ ดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร

๒.๓ ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่น อันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยีและความผิดอื่นที่เกี่ยวเนื่อง

๒.๔ ดำเนินการเกี่ยวกับการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยีโดยการใช้เทคโนโลยีสารสนเทศและเครื่องมือพิเศษ สนับสนุนส่วนราชการ หรือหน่วยงานอื่นในการสืบสวนสอบสวน รวมทั้งสนับสนุนการพัฒนาบุคลากรด้านการสืบสวนสอบสวนของสำนักงานตำรวจแห่งชาติ ให้มีความรู้ ความสามารถในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี

๒.๕ ดำเนินการเกี่ยวกับการรวบรวมข้อมูล ตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี

๒.๖ ดำเนินการเกี่ยวกับการพิสูจน์หลักฐานดิจิทัล การตรวจสถานที่เกิดเหตุและเก็บรวบรวมพยานหลักฐานดิจิทัลเพื่อสนับสนุนการปฏิบัติงานสืบสวนสอบสวนของหน่วยงานต่าง ๆ

๒.๗ ส่งเสริมและสนับสนุนให้ท้องถิ่น ชุมชน และประชาชนมีส่วนร่วมในกิจกรรมของตำรวจเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี รวมทั้งประสานความร่วมมือกับหน่วยงานของรัฐหรือองค์กรอื่นที่เกี่ยวข้องกับงานป้องกันและปราบปราม และงานสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ทั้งในประเทศและต่างประเทศ

๒.๘ ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ผู้บัญชาการตำรวจแห่งชาติมอบหมาย

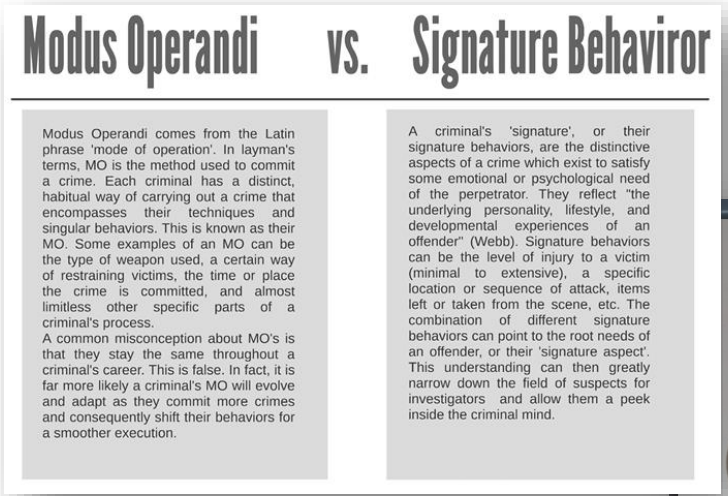
๓. <u>สรุปผลการบรรยายของวิทยากรตามหัวข้อที่กำหนด</u>

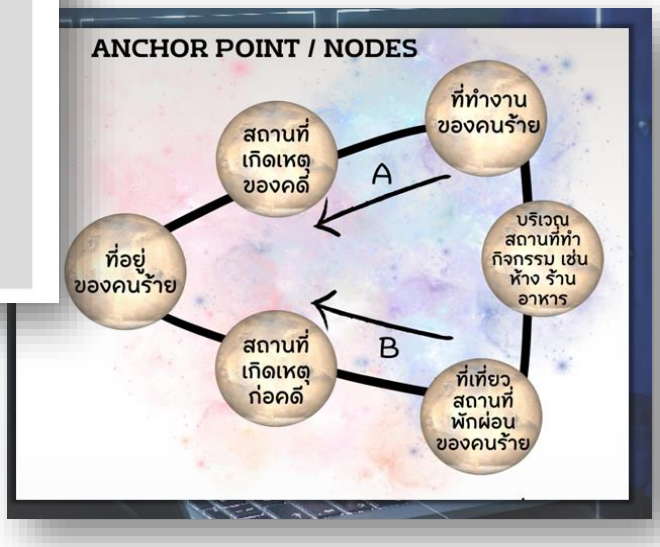
การบรรยายของวิทยากร (พ.ต.ท.ธนธัส กังรวมบุตร และคณะ) ในหัวข้อเรื่อง การฝึกปฏิบัติด้านการวิเคราะห์อาชญากรรมในรูปแบบใหม่ สามารถสรุปโดยสังเขป ดังต่อไปนี้

๓.๑ <u>การวิเคราะห์พฤติกรรมศาสตร์</u> (Behavioral Analysis) เพื่อประโยชน์ในศึกษาพฤติกรรมของอาชญากร ซึ่งจะทำให้เข้าใจกระบวนการทางความคิดของอาชญากร (Criminal Mind) จนกระทั่งทราบว่าอาชญากรมีการวางแผนเพื่อประกอบอาชญากรรมอย่างไร อันจะนำไปสู่การคาดเดา (Prediction) แผนการของอาชญากรได้ซึ่งจะนำไปสู่การจับกุมตัวผู้กระทำความผิดมาดำเนินคดีหรือป้องกันอาชญากรรมที่จะเกิดขึ้น ทั้งนี้ แบ่งออกเป็น ๒ ลักษณะ ดังนี้

๓.๑.๑ แผนประทุษกรรม (Modus Operandi) คือ อาชญากรรมที่เกิดการกระทำเป็นประจำทำเหมือนเดิมซ้ำๆ เป็นปกติจนเป็นผล เช่น อาชญากรกระทำโดยเจตนาในขณะที่กระทำผิด, เหยื่อวิทยา (เหยื่อ/การเลือกสถานที่/จุดมุ่งหมายการเลือกใช้อาวุธ/การวางแผนหลบหนี), มีการพัฒนารูปแบบวิธีการการกระทำผิดเพื่อให้อาชญากรรมนั้นสำเร็จ โดยหลักแล้วมีการลงมือก่อเหตุเท่าที่จำเป็นเพื่อให้อาชญากรรมนั้นสำเร็จหรือทรัพย์สินมีค่าที่ถูกประทุษร้ายไป เป็นต้น

๓.๑.๒ ลายเซ็นอาชญากร (Signature Behavior) คือ การกระทำของอาชญากรที่มีลักษณะเฉพาะตัวบุคคลไม่เหมือนผู้อื่น เช่น เป็นเอกลักษณ์และเป็นส่วนที่สำคัญของพฤติกรรมอาชญากร, มีการกระทำนอกเหนือจากการลงมือกระทำผิดทั่วไป (อาจพบคนร้ายมีการกระทำที่ไม่จำเป็นในสถานที่เกิดเหตุ), เป็นการแสดงออกส่วนบุคคลหรือพิธีการบนพื้นฐาน, ความเชื่อของอาชญากร การแสดงออกนี้จะคงอยู่ตลอดชีวิตไม่มีการเปลี่ยนแปลง, ลักษณะบาดแผล, การแสดงออกทางเพศ, วิธีการในการควบคุม, พิธีกรรมความเชื่อ หรือการหยิบของเป็นที่ระลึกกลับไปภายหลังก่อเหตุ เป็นต้น





๓.๒ ความสำคัญของการวิเคราะห์พฤติกรรมศาสตร์และตัวอย่าง

การป้องกันอาชญากรรมจำเป็นต้องใช้องค์ความรู้ในเรื่องการวิเคราะห์พฤติกรรม (Behavioral Analysis) เข้ามาใช้ในการสืบสวนเพื่อความรวดเร็วและถูกต้องแม่นยำมากขึ้น รวมถึงการนำข้อมูลมาใช้ในการป้องกันและระงับยับยั้งบุคคลที่มีแนวโน้มจะกระทำความผิดลักษณะนี้ นอกจากนั้นยังเป็นข้อมูลสำหรับการตั้งข้อสังเกตให้ประชาชนโดยทั่วไปในการเรียนรู้ หากคนในสังคมมีแนวโน้มจะก่อคดี ซึ่งการวิเคราะห์เรื่องสภาวะทางอารมณ์ แรงกระตุ้น แรงจูงใจ จะมีส่วนสำคัญในการช่วยป้องกันก่อนเกิดเหตุ ประกอบกับเจ้าหน้าที่ของรัฐก็ต้องปรับเปลี่ยนวิธีการทำงาน ตั้งแต่กระบวนการเข้าที่เกิดเหตุและกระบวนการซักถามผู้กระทำความผิด ซึ่งถือเป็นเรื่องละเอียดอ่อนและเชื่อมโยงกัน ไม่ว่าจะเป็นคดีของนายสมคิดหรือคดีของจิตรลดา รวมทั้งยังมีอีกหลายคดีที่มีลักษณะคล้าย ๆ กัน เช่น คดีผู้กระทำความผิดที่วางแผนฆาตกรรมสามีของตนเอง โดยใช้วิธีวางยาพิษทีละน้อย และจัดฉากอำพรางคดีให้มองว่าเป็นอุบัติเหตุและหวังเงินประกัน อย่างไรก็ตาม หากเป็นทำคดีแบบปกติการจับคนร้ายได้แล้วถือว่าสิ้นสุด เพราะผู้กระทำความผิดได้ถูกลงโทษตามกฎหมาย หากแต่ในความเป็นจริงการวิเคราะห์ตามหลักวิชาการจะพบว่าผู้ก่อเหตุเหล่านี้มักมีความผิดปกติทางจิต การลงโทษโดยการคุมขังหรือแม้กระทั่งความตายก็ไม่สามารถยับยั้งคนเหล่านี้ไม่ให้กระทำผิดได้ และในประการที่สำคัญคือทุกครั้งที่ฆาตกรลงมือสำเร็จก็จะมีความมั่นใจเพิ่มมากขึ้น ผู้เสียหายคนต่อไปจะวางแผนละเอียดมากขึ้นและมีความผิดพลาดน้อยลง ฉะนั้น จึงจำเป็นจะต้องศึกษาทำความเข้าใจกับผู้ก่อเหตุและนำมาวิเคราะห์ในการสืบสวนจับกุมอย่างแม่นยำ และสร้างจุดสังเกตให้ประชาชนมีความระมัดระวังบุคคลที่มีแนวโน้มเข้าข่ายเป็นฆาตกร เพื่อป้องกันไม่ให้เกิดความสูญเสียในอนาคต

๓.๓ อาชญากรและแรงจูงใจ ประกอบไปด้วย

๓.๓.๑ เป้าหมายด้านการเงิน (Financial Gain) ทำไปเพื่อมุ่งประสงค์ต่อเงินหรือทรัพย์สินของเหยื่อ

๓.๓.๒ เรียกร้องความสนใจให้เป็นที่จดจำ (Recognition & Achievement) ทำไปเพื่อเรียกร้องความสนใจ หรือต้องการเป็นที่จับจ้องหรืออยู่ในกระแสสังคมที่กำลังได้รับความนิยม จนทำให้ได้รับการยอมรับในสังคม

๓.๓.๓ แรงจูงใจด้านการเมือง (Political Motivation) ทำไปเพื่อหวังผลทางการเมือง

๓.๔ ประเภทอาชญากรทางเทคโนโลยีหรือไซเบอร์ (Hacker)

๓.๔.๑ Black Hacker เป็นนักโจรกรรมข้อมูลทางคอมพิวเตอร์ของผู้อื่นเพื่อนำไปขาย เรียกค่าไถ่หรืออื่น ๆ โดยมีลักษณะการทำที่ประสงค์ต่อทรัพย์หรือค่าตอบแทนโดยชัดเจน ทำเป็นอาชีพ ทำเป็นประจำ

๓.๔.๒ Grey Hacker เป็นนักโจรกรรมข้อมูลที่จะทำการโจรกรรมทางคอมพิวเตอร์ของผู้อื่นเป็นครั้งคราว ทำเมื่อจำเป็นหรือเมื่อได้รับคำสั่งเท่านั้น

๓.๔.๓ White Hacker เป็นนักโจรกรรมข้อมูลที่ไม่ได้มีพฤติกรรมหรือวัตถุประสงค์ที่จะเอาข้อมูลทางคอมพิวเตอร์ของผู้ไปทำการใด แต่จะทำการดูข้อมูลหรือจับตาเฝ้าดูความเคลื่อนไหวของกลุ่มเป้าหมายเท่านั้น

๓.๕ รูปแบบของอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์

๓.๕.๑ หลอกขายของออนไลน์ เช่น เพจซื้อขายสินค้าแบรนด์เนมปลอม โอนเงินแล้วไม่ส่งของ เป็นต้น

๓.๕.๒ หลอกเป็นคนสนิทแล้วขอยืมเงิน เช่น การโทรไปหลอกว่าเป็นเพื่อนหรือญาติกำลังเดือนร้อนต้องการความช่วยเหลือด้านการเงิน เป็นต้น

๓.๕.๓ หลอกให้ทำงานหรือกู้เงิน เช่น เพจจ้างทำงานออนไลน์ ต้องมีการโอนเงินค่าสมาชิก ค่าอุปกรณ์ ไปก่อนแต่ไม่ได้ทำงาน หรือได้รับงานตามที่โฆษณา เป็นต้น

๓.๕.๔ หลอกให้รักแล้วลงทุน เช่น เข้าไปตีสนิท ทำความคุ้นเคย จนหลงรักและเชื่อในสิ่งที่อาชญากรพูดจนให้ความช่วยเหลือด้านการเงินหรือชวนลงทุน เป็นต้น

๓.๕.๕ หลอกให้กลัวแล้วโอนเงิน เช่น หลอกว่าเป็นเจ้าหน้าที่สรรพากร เจ้าหน้าที่กรมที่ดิน เจ้าหน้าที่ตำรวจแล้วบอกว่ามีการกระทำความผิดตามกฎหมายนั้น ๆ เป็นต้น

๓.๕.๖ หลอกติดตั้งแอปดูดเงิน/ขโมยรหัสผ่าน เช่น ส่งข้อความหลอกลวงในนามหน่วยงานของรัฐ พร้อมกับแนบลิงค์ให้ติดตั้งแอปหรือเข้าไปดูข้อมูล จากนั้นอาชญากรจะทำใช้วิธีการทางเทคนิคเข้าไปขโมยข้อมูลในมือถือของเหยื่อ

๓.๖ <u>สถานการณ์คดีอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์</u>

จากสถิติศูนย์บริหารรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ สถิติสะสมตั้งแต่วันที่ ๑ มิถุนายน ๒๕๖๕ ถึงวันที่ ๒๕ ตุลาคม ๒๕๖๖ พบว่า มีการแจ้งความผ่านระบบ www.thaipoliceonline.com ทั้งสิ้นจำนวน ๓๘๐,๕๑๙ เรื่อง แบ่งเป็นคดีออนไลน์ จำนวน ๓๕๑,๓๑๑ เรื่อง คดีอาญาอื่น ๆ จำนวน ๑๐,๖๐๗ เรื่อง และจำหน่ายออกจากระบบ จำนวน ๑๘,๕๗๖ เรื่อง ซึ่งในจำนวนคดีออนไลน์ ๓๕๑,๓๑๑ เรื่อง เป็นคดีที่มีความเชื่อมโยงกัน จำนวน ๑๗๒,๑๘๘ เรื่องไม่เชื่อมโยงกัน จำนวน ๑๗๙,๑๒๓ เรื่อง โดยรวมมูลค่าความเสียหายทั้งสิ้น จำนวน ๔๗,๕๖๕,๘๗๗,๓๔๑.๐๐ บาท ทั้งนี้ มีการขออายัดบัญชี ๑๑๙,๙๔๐ Case ID หรือ ๑๘๒,๗๓๑ บัญชี ยอดเงินที่ต้องอายัด จำนวน ๒,๑๒๐,๒๖๔,๘๖๒ บาท อายัดได้ทัน จำนวน ๑,๓๑๖,๐๐๐,๘๙๔.๐๐ บาท โดยประเภทคดีออนไลน์ที่มีการแจ้งความมากที่สุด ๕ อันดับ คือ

อันดับที่ ๑ หลอกลวงซื้อขายสินค้าหรือบริการไม่เป็นขบวนการ จำนวน ๑๔๐,๘๓๖ เรื่อง คิดเป็นร้อยละ ๔๐.๒๗ ของทั้งหมด โดยมีมูลค่าความเสียหาย ๒,๐๔๑,๓๐๖,๒๑๐.๐๐ บาท

อันดับที่ ๒ หลอกให้โอนเงินเพื่อทำงาน จำนวน ๔๖,๐๔๕ เรื่อง คิดเป็นร้อยละ ๑๓.๑๗ ของทั้งหมด โดยมีมูลค่าความเสียหาย ๕,๖๘๙.๒๕๓.๙๒๒.๐๐ บาท

อันดับที่ ๓ หลอกให้กู้เงิน จำนวน ๓๙,๒๑๓ เรื่อง คิดเป็นร้อยละ ๑๑.๒๑ ของทั้งหมด โดยมีมูลค่าความเสียหาย ๑,๗๓๑,๒๙๑,๕๒๖.๐๐ บาท

อันดับที่ ๔ หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ จำนวน ๒๘,๘๖๑ เรื่อง คิดเป็นร้อยละ ๘.๒๕ ของทั้งหมด โดยมีมูลค่าความเสียหาย ๑๔,๗๒๓,๕๗๘,๖๘๕.๐๐ บาท

อันดับที่ ๕ ข่มขู่ทางโทรศัพท์ (Call Center) จำนวน ๒๕,๓๙๑ เรื่อง คิดเป็น ๗.๒๖% ของทั้งหมด โดยมีมูลค่าความเสียหาย ๕,๖๔๗,๒๕,๓๑๒.๐๐ บาท

๓.๗ <u>แนวโน้มของอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ที่ควรต้องระวัง</u>

๓.๗.๑ AI หรือเทคโนโลยี Deepfake จะเข้ามามีบทบาทของอาชญากรมากขึ้น เทคโนโลยีที่ใช้สร้างสื่อสังเคราะห์เพื่อปลอมแปลงทั้งหน้าตา หรือเสียงสังเคราะห์ให้เราเชื่อว่านี่คือคนที่รู้จัก ฝั่งอาชญากรมีเงินทุนเป็นจำนวนมาก ติดตามข่าวสารตลอด ดังนั้น เรื่องของการมีสติจึงสำคัญมาก อย่าเผลอไปคลิกลิงก์ที่อาชญากรส่งให้เด็ดขาด

๓.๗.๒ มิจฉาชีพจะหลอกลวงเป็นซีซั่น อาทิ ในช่วงของการยื่นภาษีประจำปี อาชญากรมักจะมีการปลอมแปลงเป็นเจ้าหน้าที่สรรพากรนติดต่อในเรื่องของการขอคืนภาษี อาชญากร ในช่วงเทศกาลต่าง ๆ เช่น ปีใหม่ สงกรานต์ เรื่องของเพจท่องเที่ยวปลอม จองที่พักปลอม ก็เริ่มระบาด เพราะอาชญากรรู้ว่าเป็นช่วงเวลาที่คนเริ่มจับจ่ายใช้สอย ท่องเที่ยวต่างจังหวัด ต่างประเทศ อาชญากรก็จะจับจุดความต้องการของคนในแต่ละช่วงเวลา ในการหลอกขายสินค้า ฉะนั้น จุดสังเกตง่าย ๆ คือ หากเว็บไซต์นั้นจะไม่ให้เราติดต่อทางโทรศัพท์ แต่อาชญากรจะบอกให้ inbox ไปหา หรือแอดไลน์เท่านั้น หรือให้โอนเงินค่าจองสถานที่พักทริปทัวร์ ในบัญชีของบุคคลธรรมดาแทนที่จะเป็นในนามของบริษัท หรือในต้นปีหน้าเรื่องของเงินดิจิทัล ๑๐,๐๐๐ บาท ก็เป็นมหกรรมครั้งใหญ่ที่น่าเป็นห่วง อาชญากรจะอาศัยโอกาสส่งแอปปลอม ลิงก์ปลอมหรือไม่ ซึ่งเป็นเรื่องที่หน่วยงานกำลังระวังภัย แต่เหนือสิ่งอื่นใดตัวเราก็สำคัญ เช็กให้ดีก่อนกดเสมอ อย่ามือไวเด็ดขาด

๓.๗.๓ คนสูงอายุวัยเกษียณจะโดนหลอกมากขึ้น อาจจะแอบอ้างว่ามาจากกองทุนบำเหน็จบำนาญข้าราชการ, แอบอ้างเป็นประกันสังคม, แอบอ้างเป็นกองทุนเงินออม ว่ามีเงินออมตกค้างไว้อยู่ให้เหยื่อแอดไลน์หรือติดตั้งโปรแกรมเพื่อเบิกเงินออกส่วนนี้มา หลายคนก็หลงเชื่อกรอกข้อมูล ติดตั้งแอปและถูกดูดเงินในที่สุด เพราะผู้สูงวัยคนกลุ่มนี้มีกำลังจ่ายที่สูง ดังนั้น สิ่งที่สำคัญมาก ๆ คือ คนในครอบครัว การเตือนภัยให้ผู้สูงอายุที่ใช้โซเชียลสำคัญมาก อย่าหลงเชื่อกดลิงก์หรือให้ข้อมูลเด็ดขาด

๓.๗.๔ การส่งลิงก์ หรือแก๊ง Call Center อาชญากรจะศึกษาข้อมูลเหยื่อมากขึ้น มีการล็อกเป้ารู้ว่าคน ๆ นี้มีเงินและมีโอกาสโดนหลอกสูง แกล้งทักเข้ามาคุย สิ่งเหล่านี้จะมากขึ้น เพราะอาชญากรรู้แล้วว่าจะสามารถหาประโยชน์จากสิ่งนี้และจะทำให้เหยื่อเชื่อได้ สร้างความไว้เนื้อเชื่อใจให้กับเหยื่อ

๓.๗.๕ การหลอกเพื่อการลงทุนจะเพิ่มขึ้น อาชญากรจะใช้หลักจิตวิทยาที่ว่ามนุษย์จะกลัวการสูญเสียเงินต้นที่ลงทุนไป โดยการหลอกว่าต้องเสียภาษี ต้องวางเงินมัดจำก่อน ซึ่งคนเราจะกลัวเพื่อให้ได้เงินต้นคืนมา การสร้างความไว้วางใจของอาชญากรคือการคืนให้มากที่สุดก่อน เพื่อให้เกิดความไว้ใจ และนำไปสู่การเสียที่มากขึ้น ทุกเพศ ทุกวัย ทุกอาชีพมีสิทธิ์โดนหลอกได้ทั้งสิ้น หรือแม้กระทั่งใช้วิธีทำให้เหยื่อ Lost Focus หรือทำให้เราตายใจ ชวนเราคุยและทำให้เหยื่อเผลอตัว ไม่ได้โฟกัส พลาดกดลิงก์ และพลาดให้ข้อมูลไปในที่สุด

๓.๗.๖ ปัจจุบันไม่ว่าจะเป็นโทรศัพท์ Android หรือ iOS ก็มีโอกาสถูกแฮคได้ทั้งสิ้น คนที่คิดว่า iOS ปลอดภัย หากแต่ล่าสุดมีผู้เสียหายที่ใช้ iPhone แล้ว ซึ่งส่วนใหญ่มักจะมาจากการกดลิงก์ และกดยืนยันอะไรบางอย่างจนทำให้อาชญากรสามารถควบคุมเครื่องของเราได้ด้วยวิธีการ Remote Control หรือการแฝงเข้ามาควบคุมมือถือของเราจากระยะไกล

๓.๘ <u>การฝึกปฏิบัติด้านการวิเคราะห์อาชญากรรมในรูปแบบใหม่ตามแนวทางในการป้องกันอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์</u> ผ่านกิจกรรมการให้หาเพจหลอกลวง พร้อมอธิบายเหตุและนำหลักฐานมาประกอบว่าเพราะเหตุใดจึงคิดเห็นเช่นนั้น

๓.๘.๑ อย่าหลงเชื่อ อย่ากดลิงก์ อย่าให้ข้อมูลส่วนตัวกับใครเด็ดขาด คิดให้ช้าลง คิดให้ถี่ถ้วน พิจารณาให้ดีว่าใช่คนที่เรารู้จักจริง ๆ หรือไม่

๓.๘.๒ ถ้าเป็นรูปแบบเพจตรวจสอบให้ดีว่ามีการทำ Verified Page เป็นรูปเครื่องหมายติ๊กถูกแล้วหรือไม่

๓.๘.๓ ถ้าเป็น Facebook เราสามารถตรวจสอบความโปร่งใสของเพจ เช่น ตรวจสอบประวัติของเพจเบื้องต้น หรือประเทศที่แอดมินอยู่ได้

๓.๘.๔ กรณีโอนเงิน ก่อนจะโอนควรตรวจสอบก่อนโอน เพราะอำนาจสูงสุดเป็นของเรา โดยเบื้องต้นสามารถตรวจสอบได้จาก https://www.chaladohn.com/ ฉลาดโอนดอทคอม

๓.๘.๕ สังเกต URL เว็บที่เข้าให้ดี หรือถ้าเจอลิงก์แปลก ๆ อย่ากดเด็ดขาดทำ ๒FA (two-factor authentication) หรือการยืนยันรหัสเข้า ๒ ชั้น ซึ่งจะเพิ่มความปลอดภัยได้มากขึ้น

๓.๘.๖ ปัจจุบันเราสามารถระงับบัญชีได้ผ่านธนาคาร ในกรณีถ้าเรารู้ว่าบัญชีเราไม่ปลอดภัย โดยไม่ต้องแจ้งตำรวจก่อน (โทรสายด่วน ๑๔๔๑) เพื่อความปลอดภัย แล้วค่อยไปแจ้งความที่หลังได้ โดยสามารถแจ้งความออนไลน์ได้ที่ www.thaipoliceonline.com

๓.๘.๗ เราไม่สามารถรู้ได้ทั้งหมดว่าคนร้ายมาในรูปแบบใด หากแต่ Mindset ที่สำคัญคือข้อมูลประเภท Sensitive Data เช่น ข้อมูลเชิงบุคคลประวัติของเราหรือบัญชีธนาคาร เป็นต้น เราจะต้องทำการยืนยันตัวตนที่เพิ่มความปลอดภัยทางการเงินทุกครั้ง หรือต้องยืนยันตัวตนให้ได้ว่า คนที่เราคุยด้วยใช่เขาจริง ๆ หรือไม่ หรือเขาแอบอ้าง และไม่ควรส่งต่อข้อมูลให้ใครง่าย ๆ โดยเด็ดขาด

๔. <u>ประโยชน์ที่ได้รับและข้อเสนอแนะเพื่อการพัฒนางานยุติธรรม</u>

การฝึกปฏิบัติด้านการวิเคราะห์อาชญากรรมในรูปแบบใหม่ ซึ่งประกอบไปด้วย การวิเคราะห์พฤติกรรมศาสตร์ ความสำคัญของการวิเคราะห์พฤติกรรมศาสตร์และตัวอย่าง อาชญากรและแรงจูงใจ รูปแบบของอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ สถานการณ์คดีอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ แนวโน้มของอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ที่ควรต้องระวัง และแนวทางในการป้องกันอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ ดังที่กล่าวมาแล้วข้างต้น ก่อให้เกิดประโยชน์ที่ได้รับและข้อเสนอแนะเพื่อการพัฒนางานยุติธรรม ทั้งในมิติต่อตนเองและหน่วยงาน ดังนี้

๔.๑ มิติต่อตนเอง กล่าวคือ ทำให้ทราบถึงอาชญากรรมและกลโกงในรูปแบบใหม่ของอาชญากรในปัจจุบัน พร้อมทั้งวิธีการป้องกันมิให้ตนเองตกเป็นเหยื่อของอาชญกรทางเทคโนโลยี นอกจากนั้น ยังทำให้ทราบถึงแนวทางในการแก้ไขปัญหากรณีที่ตนเองตกเป็นผู้เสียหายจากการหลอกลวง เช่น หากถูกหลอกให้โอนเงินต้องโทรไปที่สายด่วน หมายเลข ๑๔๔๑ ทันที เพื่อดำเนินการอายัดบัญชีก่อนการแจ้งความออนไลน์ รวมทั้งวิธีการรวบรวมหลักฐานที่สำคัญเพื่อใช้ในประกอบการแจ้งความดำเนินคดี

๔.๒ มิติต่อหน่วยงาน กล่าวคือ สามารถนำความรู้ที่ได้ปรับใช้ในการติดตามและวิเคราะห์รูปแบบการก่ออาชญากรรมในรูปแบบใหม่ เพื่อประโยชน์ในการกำหนดรูปแบบ วิธีการ ในการป้องกันและปราบปรามอาชญากรรมในรูปแบบใหม่ที่อาจจะเกิดขึ้นทั้งในปัจจุบันและอนาคต รวมถึงการติดตามผู้กระทำผิดมาลงโทษตามหน้าที่และอำนาจของแต่ละหน่วยงาน อย่างไรก็ตาม การพัฒนางานยุติธรรมจำเป็นจักต้องบูรณาการการทำงานร่วมกันระหว่างหลายหน่วยงานเพื่อให้เท่าทันกับอาชญากรรมในรูปแบบใหม่ รวมทั้งจำเป็นที่จักต้องเร่งสร้างความตระหนักรู้ให้แก่ประชาชนถึงกลโกงในรูปแบบต่าง ๆ รวมทั้งแนวทางในการแก้ไขหยุดยั้งความเสียหายกรณีที่ตกเป็นเหยื่อ โดยเฉพาะอาชญากรรมทางเทคโนโลยี ผ่านสื่อประชาสัมพันธ์ที่เข้าใจได้ง่ายและเข้าถึงได้สะดวก ย่อมจักเป็นประโยชน์ในเชิงการป้องกันอาชญากรรมทั้งต่อตนเอง ประชาชน และสังคมโดยรวม
