“โครงการฝึกอบรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘” ขององค์การบริหารส่วนจังหวัดสระบุรี

****

๑.ชื่อโครงการ

“โครงการฝึกอบรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘” ขององค์การบริหารส่วนจังหวัดสระบุรี

๒. กลุ่มเป้าหมาย

ประกอบด้วย บุคลากรองค์การบริหารส่วนจังหวัดสระบุรี จำนวน ๑๕๐ คน

๓. ระยะเวลาดำเนินโครงการ : วันที่ ๓๐ มิถุนายน ๒๕๖๘

๔. วัตถุประสงค์

๔.๑ เพื่อให้เกิดความตระหนักรู้ในความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

๔.๒ เพื่อให้เกิดความรู้ความเข้าใจและตระหนักถึงความเสี่ยงจากการใช้งานข้อมูลส่วนบุคคลของประชาชนผู้ที่มาติดต่อราชการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๔.๓ เพื่อให้สามารถประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นกับหน่วยงานโดยมีแนวทางการปฏิบัติที่ถูกต้องเหมาะสม

๔.๔ เพื่อให้สามารถรับมือกับภัยคุกคามทางเทคโนโลยีสารสนเทศที่จะเกิดขึ้นได้อย่างปลอดภัยและแก้ปัญหาเบื้องต้นได้อย่างถูกต้อง

๕. เหตุผล/ความสำคัญของการจัดโครงการฝึกอบรม

ปัจจุบันการให้บริการงานขององค์การบริหารส่วนจังหวัดสระบุรี การติดต่อสื่อสาร การรายงานผลการดำเนินงาน การสืบค้นข้อมูลต่าง ๆ ได้ก้าวเข้าสู่ยุคดิจิทัล เจ้าหน้าที่ขององค์การบริหารส่วนจังหวัดสระบุรีมีการปฏิบัติงานตามกฎหมาย ระเบียบ ที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งกำหนดเหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคล เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อมีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจนการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพสอดคล้องตามที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย และพระราชบัญญัติปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ กำหนดให้หน่วยงานและเจ้าหน้าที่ของรัฐให้สามารถรับเรื่อง และให้บริการประชาชนด้วยวิธีการทางอิเล็กทรอนิกส์ได้อย่างมั่นใจว่าถูกต้องตามกฎหมายและระเบียบที่เกี่ยวข้อง เจ้าหน้าที่ผู้ปฏิบัติงานจึงจำเป็นต้องมีความตระหนักรู้ในด้านความมั่นคงความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศและความเสี่ยงที่เกิดจากภัยคุกคามในรูปแบบต่างๆ รวมถึงแนวทางการปฏิบัติเพื่อหลีกเลี่ยงภัยคุกคามดังกล่าว ตลอดจนมีความรู้ความเข้าใจในบทบาทและความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศในหน่วยงานเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง และมีความปลอดภัยจากการโจมตีทางเทคโนโลยีสารสนเทศในอนาคตด้วย โดยมุ่งเน้นสร้างความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยด้านทางเทคโนโลยีสารสนเทศและป้องกันผลกระทบด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของหน่วยงาน และการใช้งานข้อมูลส่วนบุคคลของประชาชนผู้มาติดต่อราชการให้ปลอดภัยและถูกต้อง กองยุทธศาสตร์และงบประมาณจึงได้จัดโครงการฝึกอบรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางเทคโนโลยีสารสนเทศขึ้น เพื่อให้ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเกี่ยวกับการป้องกันภัยทางเทคโนโลยีสารสนเทศ และความเสี่ยงที่อาจจะก่อให้เกิดความเสียหายต่อระบบสารสนเทศขององค์กรจากการใช้งาน

เกิดความตระหนักถึงภัยคุกคามเทคโนโลยีสารสนเทศที่เกิดขึ้นในปัจจุบัน แนวทางการป้องกัน แก้ไข และสามารถนำความรู้ไปประยุกต์ใช้ ในการทำงานและชีวิตประจำวัน รวมถึงเกิดความรู้ความเข้าใจและตระหนักถึงความเสี่ยงจากการใช้งานข้อมูลส่วนบุคคลของประชาชนผู้ที่มาติดต่อราชการได้อย่างถูกต้องตามกฎหมาย และระเบียบที่เกี่ยวข้อง

๖. การบริหารงบประมาณ

เบิกจ่ายตามข้อบัญญัติองค์การบริหารส่วนจังหวัด เรื่อง งบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๘ ขององค์การบริหารส่วนจังหวัดสระบุรี แผนงานบริหารงานทั่วไป งานสารสนเทศ งบดำเนินงาน ค่าใช้สอย ประเภทรายจ่ายเกี่ยวเนื่องกับการปฏิบัติราชการที่ไม่เข้าลักษณะรายจ่ายงบรายจ่ายอื่น ๆ หน้า ๑๒๗ โครงการฝึกอบรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ จำนวน ๒๐๐,๐๐๐.- บาท เพื่อเป็นค่าใช้จ่ายในการจัดฝึกอบรมด้านความปลอดภัยทางด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรผู้ปฏิบัติงานภายในองค์การบริหารส่วนจังหวัดสระบุรี ตามโครงการขององค์การบริหารส่วนจังหวัดสระบุรี เช่น ค่าอาหารว่างและเครื่องดื่ม ค่าอาหารกลางวัน ค่ากระเป๋าเอกสาร ค่าสมนาคุณวิทยากร และค่าใช้จ่ายอื่นที่เกี่ยวข้อง ทุกรายการสามารถถัวเฉลี่ยได้

๗. ผลที่คาดว่าจะได้รับ

๗.๑ ผู้เข้ารับการฝึกอบรมเกิดความตระหนักรู้ในความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

๗.๒ ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจและตระหนักถึงความเสี่ยงจากการใช้งานข้อมูลส่วนบุคคลของประชาชนผู้มาติดต่อราชการ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

๗.๓ ผู้เข้ารับการฝึกอบรมสามารถประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในหน่วยงานได้มีแนวทางการดำเนินการที่ถูกต้องและเหมาะสม

๗.๔ ผู้เข้ารับการฝึกอบรมสามารถรับมือกับภัยคุกคามและแก้ปัญหาเบื้องต้นได้อย่างถูกต้อง

๘. การประเมินผล

๘.๑ เชิงปริมาณ : ผู้เข้ารับการฝึกอบรมตามโครงการตอบแบบประเมินความพึงพอใจผลการประเมินไม่น้อยกว่าร้อยละ ๘๐

๘.๒ เชิงคุณภาพ : ผู้เข้ารับการฝึกอบรมตามโครงการ มีความรู้ความเข้าใจการปฏิบัติงานถูกต้องตามกฎหมาย และระเบียบที่เกี่ยวข้อง

๙. สรุปเนื้อหาที่ได้รับจากการเข้าร่วมโครงการฝึกอบรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘” ขององค์การบริหารส่วนจังหวัดสระบุรี

๙.๑ สถานที่ฝึกอบรม : ลีลาวดี รีสอร์ท สระบุรี อำเภอเมืองสระบุรี จังหวัดสระบุรี

๙.๒ รายละเอียดเนื้อหาการฝึกอบรม

เนื้อหาการบรรยาย จากวิทยากร นายบุญญวุฒิ บุญญาธิการ อัยการจังหวัดประจำสำนักงานอัยการสูงสุด

“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕”

"ความรู้เบื้องต้นเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายการปฏิบัติราชการทางอิเล็กทรอนิกส์”

“พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕”

เป็นกฎหมายกลางเพื่ออำนวยความสะดวกในการติดต่อราชการ ยกระดับรัฐบาลดิจิทัล ลดภาระประชาชน เพิ่มประสิทธิภาพภาครัฐ

<u>วัตถุประสงค์</u>

๑. เพื่อขจัดอุปสรรคทางกฎหมายในการให้บริการแบบอิเล็กทรอนิกส์

๒. เพื่อส่งเสริมการใช้เทคโนโลยีดิจิทัลของหน่วยงานรัฐและประชาชน

<u>ที่มาและความสำคัญของ พ.ร.บ.</u>

๑. พัฒนาขึ้นเพื่ออำนวยความสะดวกให้ประชาชนในยุคดิจิทัล

๒. ปัจจุบันประชาชนคุ้นเคยกับบริการอิเล็กทรอนิกส์จากภาคเอกชน เช่น ธนาคาร แอปพลิเคชันจัดส่งอาหาร การจองคิวออนไลน์ ฯลฯ

๓. ภาครัฐจึงต้องปรับตัวให้บริการผ่านระบบอิเล็กทรอนิกส์เช่นกัน

๔. เพื่อให้ประชาชนสามารถติดต่อราชการได้สะดวก รวดเร็ว และโปร่งใส

<u>ขอบเขตการบังคับใช้</u>

๑. ครอบคลุมราชการส่วนกลาง ภูมิภาค ท้องถิ่น และหน่วยงานรัฐ

๒. ยกเว้นฝ่ายนิติบัญญัติ ตุลาการ องค์กรอิสระ อัยการ ฯลฯ

๓. ประชาชนทุกคนมีสิทธิติดต่อทางอิเล็กทรอนิกส์ได้อย่างเสมอภาค

<u>สิทธิของประชาชน</u>

๑. ยื่นคำขอ ส่งข้อมูล ติดต่อ จ่ายเงิน ผ่านช่องทางอิเล็กทรอนิกส์ได้

๒. ขอใบอนุญาตและเอกสารราชการในรูปแบบอิเล็กทรอนิกส์

๓. ตรวจสอบข้อมูลทางออนไลน์โดยไม่เสียค่าใช้จ่าย

<u>หน้าที่ของรัฐ</u>

๑. ช่องทางอิเล็กทรอนิกส์และรับเรื่องจากประชาชน

๒. ออกเอกสารราชการและติดต่อกลับในรูปแบบดิจิทัล

๓. พัฒนาฐานข้อมูลและยกระดับระบบราชการให้รองรับ e-Gov

<u>สภาพบังคับของกฎหมาย</u>

๑. ไม่มีบทกำหนดโทษเฉพาะ แต่ยังมีผลผูกพันตามกฎหมายอื่น

๒. เจ้าหน้าที่ละเว้นหน้าที่อาจมีความผิดทางวินัยหรืออาญา

๓. ความเสียหายต่อประชาชนอาจนำไปสู่ความรับผิดทางแพ่ง

ประโยชน์ที่ได้รับ

๑. เพิ่มความสะดวก ลดค่าใช้จ่ายแก่ประชาชน

๒. เพิ่มประสิทธิภาพและความโปร่งใสของภาครัฐ

๓. ลดการทุจริต ส่งเสริมการแข่งขันของประเทศ

<u>คำจำกัดความ: ขออนุญาต/อนุญาต</u>

๑. ครอบคลุมการยื่นคำขอ/รับบริการทุกรูปแบบ เช่น ขอรับใบอนุญาต / ขออนุมัติ / ขอจดทะเบียน ขอขึ้นทะเบียน / ขอแจ้ง / ขออาชญาบัตร / ขอรับรอง/ ร้องทุกข์ / ขอรับเงิน/ขอรับสวัสดิการ / ขอรับบริการอื่นใด

๒. หน่วยงานของรัฐมีหน้าที่พิจารณาและ "อนุญาต" ตามรูปแบบต่าง ๆ

<u>การแบ่งระดับ “หน่วยงานของรัฐ” เพื่อรองรับการให้บริการทางอิเล็กทรอนิกส์</u>

๑. เพื่อให้การนำระบบอิเล็กทรอนิกส์ไปใช้เป็นไปอย่างเหมาะสมกับขีดความสามารถของแต่ละหน่วยงาน

๒. เพื่อไม่สร้างภาระเกินความจำเป็นกับหน่วยงานขนาดเล็ก

๓. ช่วยวางแผนการลงทุนและการสนับสนุนระบบจากภาครัฐได้อย่างมีประสิทธิภาพ หน่วยงานต้องประเมินตนเอง และกำหนดระดับความพร้อมในการให้บริการ

<u>ระดับเริ่มต้น: (Basic)</u>

<u>ลักษณะ :</u> หน่วยงานขนาดเล็ก ทรัพยากรจำกัด

<u>แนวทาง</u> : ใช้ระบบที่มีอยู่เดิมของรัฐ เช่น ระบบกลางของหน่วยงานที่จัดให้ (เช่น ระบบ e-Service หรือ DGA Platform)

- มุ่งเน้นการเปิดช่องทางติดต่อราชการทางอิเล็กทรอนิกส์ให้ได้ก่อน
- ไม่จำเป็นต้องพัฒนาระบบเอง ตัวอย่าง: องค์การบริหารส่วนตำบล, หน่วยงานท้องถิ่นขนาดเล็ก

<u>ระดับกลาง: (Intermediate)</u>

<u>ลักษณะ</u> : หน่วยงานที่มีการดำเนินการด้านไอทีอยู่บ้าง มีเจ้าหน้าที่ด้านเทคโนโลยีประจำ

<u>แนวทาง</u> : • สามารถพัฒนาระบบบริการประชาชนในบางเรื่องเองได้
- เชื่อมโยงกับระบบกลางของรัฐได้
- มีการจัดการเอกสารหรือข้อมูลในรูปแบบอิเล็กทรอนิกส์ภายในหน่วยงานได้บางส่วน

ตัวอย่าง: เทศบาลเมือง, สำนักงานเขต, หน่วยงานภูมิภาคระดับจังหวัด

ระดับสูง: (Advance)

<u>ลักษณะ:</u> หน่วยงานขนาดใหญ่ มีโครงสร้างพื้นฐานดิจิทัลและบุคลากรด้านไอทีพร้อม

<u>แนวทาง:</u> • พัฒนาระบบบริการประชาชนครบวงจรด้วยตนเอง
- เชื่อมโยงข้อมูลระหว่างหน่วยงานได้ (interoperability)
- สนับสนุนระบบลายเซ็นอิเล็กทรอนิกส์ e-Payment, e-License, e-Tracking
- เป็นแบบอย่างหรือศูนย์กลางในการพัฒนาระบบให้กับหน่วยงานอื่น

ตัวอย่าง : หน่วยราชการขนาดใหญ่ เช่น กรมสรรพากร, สำนักงานตำรวจแห่งชาติ, กรุงเทพมหานครฯ

หน่วยงานของรัฐต้องเตรียมความพร้อมรับการปรับตัว พระราชบัญญัติการบริการงาน และการใช้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ไม่ต้องเดินทางไปสำนักงานเขต สามารถดำเนินการผ่านเว็บไซต์ของหน่วยงาน เช่น การยื่นขออนุญาตก่อสร้างออนไลน์ , การขอใบอนุญาตพกพา , การขออนุญาตขายสุรา ยาสูบ ขายไพ่ , การขออนุญาตจุดพุออนไลน์ , การยื่นภาษีออนไลน์ , การต่อทะเบียนรถยนต์ออนไลน์ การต่อภาษีออนไลน์ , การย้ายทะเบียนบ้านออนไลน์ , การขอ อย. ออนไลน์ , การขอใบรับรองแพทย์ดิจิทัล , การยื่นฟ้องทางอิเล็กทรอนิกส์ เป็นต้น

หมายเหตุ : กรณียื่นฟ้องคดีออนไลน์ ทำผ่านระบบศาลยุติธรรมเท่านั้น ซึ่งทำได้เฉพาะคดีแพ่งหรือคดีฝ่ายเดียว ส่วนคดีอาญาทำไม่ได้ยังต้องยื่นที่ศาล

- ➢ คดีแพ่ง (บอกเลิกสัญญาเรียก ค่าเสียหาย , ผิดสัญญา , ทำละเมิด , ฟ้องขับไล่ , ขอให้ส่งมอบทรัพย์สิน)
- ➢ ดีผู้บริโภค
- ➢ คดีร้องขอตั้งผู้จัดการมรดก
- ➢ คดีขอศาลสั่งเป็นคนสาบสูญ

๑. ยื่นขออนุญาตออนไลน์

- ✓ ก่อสร้าง ดัดแปลง รื้อถอน เคลื่อนย้ายอาคาร (สำหรับบ้านพักอาศัย ที่มีขนาดต่ำกว่า ๓๐๐ ตร.ม. รับใบอนุญาตภายใน ๓๐ วัน)
- ✓ ขออนุญาตเพื่อประกอบธุรกิจ ร้านอาหาร ร้านค้าปลีก โรงแรม ตลาด
- ✓ ขึ้นทะเบียนรับเงินช่วยเหลือ เบี้ยผู้พิการ เบี้ยผู้สูงอายุ เบี้ยเงินจัดการศพ

ข้อมูลส่วนบุคคลทั่วไป หมายถึง

- ○ ข้อมูลส่วนบุคคลทั่วไป (General หรือ PLL)
- ○ ชื่อ-นามสกุล
- ○ เบอร์โทรศัพท์
- ○ ที่อยู่
- ○ วันเดือนปีเกิด
- ○ น้ำหนักส่วนสูง
- ○ เลขที่บัญชีธนาคาร
- ○ รหัสประจำตัวหรือID รหัสพนักงาน
- ○ E-mail Facebook Line

หลักการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยการเก็บข้อมูล ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องมีการดำเนินการ ดังนี้

๑. เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอม
๒. ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
๓. Consent ต้องแยกจากส่วนอื่นชัดเจน
๔. มีแบบหรือข้อความที่อ่านแล้วเข้าใจโดยง่ายและต้องไม่เป็นการหลอกลวง
๕. เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้

การเก็บข้อมูลส่วนบุคคล

๑.การเก็บรวบรวมข้อมูลส่วนบุคคล ต้องขอความยินยอมก่อนหรือขณะดำเนินการ

๒.การเก็บข้อมูลส่วนบุคคล ต้องแจ้งรายละเอียดให้เจ้าของข้อมูลทราบ ดังนี้

- วัตถุประสงค์ของการเก็บรวบรวม
- แจ้งให้ทราบกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลเพื่อปฏิบัติตามกฎหมายหรือสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จาการไม่ให้ข้อมูลส่วนบุคคล
- ระยะในการเก็บรวบรวม
- บุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อ
- สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิของเจ้าของข้อมูลส่วนบุคคล

๑. สิทธิได้รับแจ้งรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล(Right to be informed)

๒. สิทธิขอเข้าถึงข้อมูลส่วนบุคคล(Right of access)

๓. สิทธิขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)

๔. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)

๕. สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวบุคคลได้ (Right to erasure/right to be forgotten)

๖. สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล(Right to restrict porcessing)

๗. สิทธิขอให้แก้ไขข้อมูลส่วนบุคคล (Right to rectification)

๘. สิทธิในการร้องเรียนกรณีที่ผู้ควบคุมหรือประมวลผลไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองส่วนบุคคล

ข้อมูลส่วนบบุคคลที่มีความอ่อนไหว (Sensitive Pll)

๑. ข้อมูลสหภาพแรงงาน

๒. ข้อมูลพันธุกรรม/ชีวภาพ

๓. ศาสนา

๔. ข้อมูลสุขภาพความพิการ

๕. เชื้อชาติเผ่าพันธุ์

๖. ประวัติอาชญากรรม

๗. ความเห็นทางการเมือง

๘. พฤติกรรมทางเพศ

ข้อยกเว้นการบังคับใช้พระราชบัญญัติคุ้มครองของมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองของมูลส่วนบุคคลฯ จะไม่สามารถใช้กับกรณี ดังต่อไปนี้

๑.การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัว

๒.การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่รักษาความมั่นคงของรัฐ

๓.การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บข้อมูลไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรม

๔.การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา และคณะกรรมาธิการ

๕.การพิจารณาพิพากษาคดีของศาลหรือการดำเนิดงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี

๖.การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและชอบด้วยกฎหมาย เมื่อทำตามหลักการหนึ่งหลักการใด ดังนี้

๑. ต้องได้รับความยินยอมโดยชัดแจ้ง

๒. ทำไปเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขาพของบุคคล ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้

๓. การดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงกำไร

๔. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

๕. จำเป็นเพื่อการก่อสร้างตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย

๖. จำเป็นในการปฏิบัติตามกฎหมาย ที่กำหนดไว้เฉพาะ

เจ้าของข้อมูลส่วนบุคคลมีสิทธิ์ขอให้ลบข้อมูลส่วนบุคคลได้ (Right Erasure) เมื่ออยู่ในกรณีดังต่อไปนี้

๑. เมื่อเก็บข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้

๒. เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมเป็นการเก็บรวบรวมได้หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายก็จะเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ต่อไป

๓. เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล

๔. เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวมใช้หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้

เว้นแต่กรณี

๑. การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น

๒. การเก็บรักษาเพื่อวัตถุประสงค์เฉพาะ เอกสารประวัติศาสตร์/ประโยชน์สาธารณะ/วิชาชีพทางการแพทย์/การสาธารณสุข

๓. การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมายหรือเพื่อการปฏิบัติตามกฎหมาย

ความรับผิดและบทลงโทษ

ความรับผิดทางแพ่ง

๑. ผู้กระทำละเมิดข้อมูลส่วนบุคคลต้องชดใช้สินไหมทดแทนให้กับเจ้าของข้อมูลส่วนบุคคลไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม

๒. ศาลมีอำนาจสั่งให้ชดใช้ค่าสินไหมทดแทนเพิ่มเติมได้ ๒ เท่าของสินไหมทดแทนที่แท้จริง

ความผิดทางแพ่ง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ นอกจากค่าสินไหมทดแทนที่แท้จริงแล้วศาลมีอำนาจสั่งให้จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นได้ แต่ไม่เกิน ๒ เท่าของค่าสินไหมทดแทนที่แท้จริง โดยมีอายุความฟ้องคดี ๓ ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิดหรือ ๑๐ ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลต้องชดใช้สินไหมค่าทดแทน ว่าจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่จะพิสูจน์ได้ว่า

- เหตุสุดวิสัย หรือเกิดจากกระกระทำหรือละเว้นการกระทำโดยเจ้าของข้อมูลส่วนบุคคล
- เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

โทษอาญา

ผู้ควบคุมข้อมูลส่วนบุคคล ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย

ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย จำคุก ๖ เดือน หรือปรับ ๕๐๐,๐๐๐ บาท

เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จำคุก ๑ ปี หรือปรับ ๑,๐๐๐,๐๐๐ บาท

๑. กำหนดบทลงโทษทางอาญาไว้สำหรับความผิดร้ายแรงเช่นการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนโดยมิชอบ ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นแล้วนำไปเปิดเผยให้แก่ผู้อื่นโดยมิชอบ

๒. ระหว่างโทษสูงสุดจำคุกไม่เกิน ๑ ปีหรือปรับไม่เกิน ๑ ล้านบาทหรือทั้งจำทั้งปรับ

๓. ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคลกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้นอาจจะต้องร่วมรับผิดชอบในความผิดอาญาที่เกิดขึ้น

โทษทางปกครอง

๑. กำหนดโทษปรับทางปกครองสำหรับการกระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนดเช่นไม่แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ ขอความยินยอมโดยหลอกลวงเจ้าของข้อมูลส่วนบุคคลไม่แต่งตั้ง Dpo เป็นต้น

๒. โทษปรับทางปกครองสูงสุด ๕,๐๐๐,๐๐๐ บาท

การกระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนด เช่น

- ไม่แจ้งวัตถุประสงค์ในการเก็บรวมรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ
- ขอความยินยอมโดยหลอกลวงเจ้าของข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งลงโทษปรับทางปกครอง

บทลงโทษตาม PDPA

โทษอาญา มาตรา ๗๙-๘๑ ผู้ควบคุมข้อมูลส่วนบุคคล ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย

ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย จำคุก ๖ เดือน หรือปรับ ๕๐๐,๐๐๐ บาท

เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จำคุก ๑ ปี หรือปรับ ๑,๐๐๐,๐๐๐ บาท

ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากปฏิบัติหน้าที่ตามพรบ. นี้ห้ามนำไปเปิดเผยแก่ผู้อื่นเว้นแต่เปิดเผยตามหน้าที่เพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดีหรือได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนตัวหรือเปิดเผยให้หน่วยงานที่มีอำนาจหน้าที่ตามกฎหมายหรือข้อมูลคดีต่างๆที่เปิดเผยต่อสถานะ **จำคุก ๖ เดือนหรือปรับ ๕๐๐,๐๐๐ บาท**

ผู้กระทำความผิดที่เป็นนิติบุคคลหากกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้นสั่งการหรือกระทำหรือละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิดต้องรับโทษในส่วนที่กำหนดโทษอาญาไว้ด้วย

ผู้ที่เกี่ยวข้องใน PDPA

- เจ้าของข้อมูลส่วนบุคคล บุคคลที่ข้อมูลส่วนบุคคลนั้นระบุไปถึง
- ผู้ควบคุมข้อมูลส่วนบุคคล บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลส่วนบุคคล บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล

DPO (Data Protection Officer)

คือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา ๔๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยมีหน้าที่ ดังนี้

๑. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับการปฏิบัติตามพระราชบัญญัติ

๒. ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลขอมูลส่วนบุคคล

๓. ประสานงานและให้ความร่วมมือกับสำนักงาน ในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

๔. รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

เนื้อหาการบรรยาย จากวิทยากร โดย พันตำรวจโท ประวิทย์ วงษ์เกษม รองผู้กำกับการ ๑ และทีมงานวิทยากรจาก กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ๒

<u>รู้ทันกลลวง มิจฉาชีพแก๊งคอลเซ็นเตอร์</u>

ในยุคดิจิทัลที่มิจฉาชีพมีกลยุทธ์ใหม่ๆ หลอกลวงผู้คนอยู่เสมอเอกสารฉบับนี้จึงรวบรวม ประเภทกลโกงมิจฉาชีพแก๊งคอลเซ็นเตอร์ ที่พบได้บ่อย เพื่อให้หน่วยงานราชการ เอกชน และประชาชนทั่วไป สามารถรู้เท่าทัน เข้าใจกลวิธี และป้องกันตัวได้อย่างมีประสิทธิภาพ

ในปัจจุบัน แก๊งคอลเซ็นเตอร์ได้พัฒนาเทคนิคในการโกงให้แนบเนียนขึ้นเรื่อย ๆ จากการอาศัยช่องโหว่ของความไม่รู้และความกลัวของเหยื่อ มาหลอกลวงเพื่อหวังผลประโยชน์ แม้ว่าจะมีข่าวเตือนภัยมากมาย แต่ก็ยังคงมีผู้เสียหายออกมาให้เห็นจำนวนมาก รูปแบบของ แก๊งคอลเซ็นเตอร์ ซึ่งวิธีการของกลุ่มนี้ มักทำเป็นขบวนการ และจะหลอกเหยื่อผ่านทางโทรศัพท์ โดยใช้การแอบอ้าง เป็นเจ้าหน้าที่จากหน่วยงานต่าง ๆเช่น เจ้าหน้าที่ธนาคาร บริษัทขนส่ง หรือหน่วยงานรัฐ ด้วยการใช้ข้อมูลส่วนตัวของเหยื่อมาอ้างอิง เพื่อให้ดูมีความน่าเชื่อถือ พร้อมกับหว่านล้อมให้เกิดความกลัว วิตกกังวล หรือลังเลในการตัดสินใจ จนบางครั้งอาจเผลอ โอนเงินไปโดยไม่ทันตั้งตัว

วิธี หรือ กลโกงของแก๊งคอลเซ็นเตอร์ ที่หลอกให้โอนเงิน

- **อ้างว่าเป็นเจ้าหน้าที่ธนาคาร:** มิจฉาชีพมักอ้างว่าตนเองเป็นเจ้าหน้าที่ธนาคารและตรวจสอบพบความปกติบนบัญชีของคุณ เช่น บัญชีเงินฝากคุณถูกอายัด มีหนี้บัตรเครดิตค้างชำระให้รีบไปที่ตู้ ATM ทำตามขั้นตอนที่บอกจะแก้ปัญหาได้แต่แท้จริงแล้วเป็นการหลอกลวงเพื่อโอนเงินไปยังบัญชีของโจร หรือแจ้งว่าข้อมูลของคุณหายไปจากธนาคาร รบกวนขอข้อมูลส่วนตัวอีกครั้ง เพื่อหลอกเอาข้อมูลส่วนตัวของคุณไปใช้ทำธุรกรรมทางการเงิน
- **อ้างว่าเป็นเจ้าหน้าที่ขนส่งและโอนสายให้ตำรวจ:** เนื่องจากในปัจจุบันผู้คนนิยมใช้การสั่งซื้อสินค้าทางออนไลน์จึงมีการใช้บริการขนส่งเป็นจำนวนมาก มิจฉาชีพจึงอาศัยช่องโหว่ตรงนี้ในการแอบอ้างเป็นเจ้าหน้าที่ขนส่ง แล้วหลอกว่ามีพัสดุตกค้าง หรือตรวจพบพัสดุที่มีของผิดกฎหมายหรือเกี่ยวข้องกับการฟอกเงินที่อยู่ภายใต้ชื่อของคุณ และจะทำการโอนสายไปให้กับตำรวจเพื่อหลอกให้คุณโอนเงินเพื่อยืนยันความบริสุทธิ์
- **อ้างว่าเป็นเจ้าหน้าที่ตำรวจ:** มิจฉาชีพจะอ้างตนเป็นเจ้าหน้าที่ตำรวจ และหลอกลวงว่าคุณเป็นผู้ต้องสงสัยว่าพัวพันกับคดีค้ายาหรือฟอกเงิน จึงต้องโอนเงินทั้งหมดมาให้เราตรวจสอบ
- **อ้างว่าเป็นเจ้าหน้าที่สรรพากร:** มิจฉาชีพจะอ้างตนเป็นเจ้าหน้าที่สรรพากร และหลอกลวงให้คุณเชื่อว่าคุณได้รับสิทธิ์ขอคืนภาษี ให้รีบไปทำรายการขอรับคืนที่ตู้เอทีเอ็ม แต่เมื่อทำตามขั้นตอนกลับกลายเป็นการโอนเงินให้กับโจร
- **อ้างว่าเป็นเจ้าหนี้นอกระบบ:** มิจฉาชีพอาศัยการหลอกลวงว่าเป็นเจ้าหนี้นอกระบบของบุคคลในครอบครัวหรือคนรอบตัว และข่มขู่ต่อไปว่าหากไม่อยากให้คนในครอบครัวหรือคนที่รู้จักโดนทำร้ายจะต้องโอนเงินให้เพื่อชำระหนี้นั้นแทน
- **อ้างว่าเป็นผู้โชคดีหรือได้รับรางวัล:** มิจฉาชีพอาจหลอกลวงว่าคุณคือ ผู้โชคดีที่ได้รับเงินรางวัลจำนวนมาก แต่ก่อนที่จะรับรางวัลได้ต้องโอนจ่ายภาษีให้กับพวกเขาก่อน แต่สุดท้ายเมื่อโอนเงินไปแล้วกลับไม่ได้ทั้งเงินรางวัลและโดนเชิดเงินที่โอนไปหนีหายไปด้วย

- **อ้างว่ามีรูปหรือคลิปวิดีโอหลุด:** มิจฉาชีพแอบอ้างว่ามีรูปหรือคลิปวิดีโอที่อาจทำให้คุณต้องอับอาย หรือคลิปการกระทำของคุณที่ผิดกฎหมาย ให้คุณคลิกลิงก์เข้าไป หากหลงเชื่อกดดูอาจโดนแฮ็กข้อมูลและเงินในบัญชี
- **อ้างว่าเป็นนักลงทุนเพื่อหลอกให้ลงทุน:** มิจฉาชีพหลอกให้โอนเงินไปร่วมลงทุน หลังจากนั้นหลอกต่อไปอีกว่าได้กำไรมหาศาลให้โอนค่าธรรมเนียมมาจะได้เบิกเงินไปใช้ได้
- **อ้างว่าโอนเงินผิดบัญชี:** มิจฉาชีพโทรมาและอ้างว่า “เมื่อกี้โอนเงินไปผิดบัญชี รบกวนโอนคืนมาให้หน่อย” ซึ่งอาจเกิดจากเหยื่อถูกขโมยข้อมูลส่วนตัวเอาไปขอสินเชื่อ เมื่อเงินเข้าบัญชีโจรจึงโทรมาหลอกให้เราโอนเงินให้ หรือเราอาจถูกหลอกให้เป็นเหยื่อการทำธุรกรรมที่ผิดกฎหมายโดยใช้บัญชีของเราเป็นตัวกลาง ดังนั้นหากมีใครโอนเงินมาผิดบัญชีไม่ควรโอนกลับไปให้แต่ให้อีกฝ่ายการติดต่อธนาคารเพื่อดึงเงินกลับไปด้วยตนเอง
- **อ้างว่าจะถูกตัดไฟฟ้าและประปา:** มิจฉาชีพอาจโทรมาแอบอ้างในลักษณะเป็นเจ้าหน้าที่จากการไฟฟ้าหรือการประปา มาแอบอ้างเก็บค่าไฟ เก็บค่าน้ำ แจ้งตัดไฟฟ้า แจ้งตัดน้ำประปา เปลี่ยนมิเตอร์ และตรวจซ่อมอุปกรณ์ไฟฟ้า และเหยื่อจะรีบโอนเงินให้โดยทันทีเพราะไม่อยากถูกตัดน้ำ ตัดไฟ หรือเสียค่าปรับ
- **อ้างว่าเป็นพนักงานจากเครือข่ายโทรศัพท์:** มิจฉาชีพใช้เบอร์มือถือ ๐XX-XXXXXXX โทรหาลูกค้าแจ้งว่า มีข้อมูลส่วนบุคคลของลูกค้า อาทิ ชื่อ ที่อยู่ เลขบัตรประชาชน ไปเปิดเบอร์และดำเนินการผิดกฎหมาย โดยมิจฉาชีพบางรายบอกชื่อ ที่อยู่ เลขบัตรประชาชนของเหยื่อได้อย่างถูกต้อง จนอาจทำให้เหยื่อหลงเชื่อ จากนั้นมิจฉาชีพจะหลอกว่า ต้องโอนสายไปยังเจ้าหน้าที่ตำรวจ เพื่อให้ดำเนินการเกี่ยวกับข้อมูลของลูกค้า เป็นต้น ซึ่งถือเป็นจุดที่จะทำให้เกิดความเสี่ยงที่เหยื่อเปิดเผยข้อมูลส่วนบุคคลและสูญเสียทรัพย์สินหากคุณเป็นลูกค้าของ AIS และพบความผิดปกติของเบอร์โทร หรือ SMS ข้อความ ที่ติดต่อเข้ามา สามารถแจ้งผ่านสายด่วน ๑๑๘๕ AIS Spam Report Center ได้ฟรีตลอด ๒๔ ชั่วโมง โดย AIS จะตรวจสอบร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อดำเนินการทางกฎหมายต่อไป
- **หลอกให้ทำงานออนไลน์:** มิจฉาชีพจะโทรเข้ามาเพื่อนำเสนองานง่าย ๆ แต่รายได้ดีมาก ทำให้ดูน่าสนใจ แต่จะมีเงื่อนไขในการสมัคร คือ จะต้องโอนเงินเพื่อเป็นค่าธรรมเนียมในการเข้าทำงานหรือค่าอื่น ๆ แต่ปรากฏว่าเมื่อโอนเงินแล้วจะถูกบล็อกช่องทางการติดต่อและพบว่างานนั้นไม่มีอยู่จริง

โดยแก๊งคอลเซ็นเตอร์สามารถเข้าถึงข้อมูลส่วนตัวของได้ด้วยวิธีการ เช่น

๑. การคลิกลิงก์ : การคลิกลิงก์ที่มาจากแหล่งที่ไม่น่าเชื่อถือ อาจทำให้มิจฉาชีพแฝงมัลแวร์หรือโปรแกรมดักจับข้อมูลไว้ในอุปกรณ์ของคุณ

๒. การกรอกแบบฟอร์ม : ข้อมูลส่วนตัวที่คุณกรอกลงในแบบฟอร์มออนไลน์ โดยเฉพาะข้อมูลที่ไม่ได้อยู่ในเว็บไซต์ที่น่าเชื่อถือ อาจถูกนำไปใช้ในทางที่ผิด

๓. การยินยอมสมัครใช้บริการ : บางครั้งคุณอาจเผลอให้ข้อมูลส่วนตัวกับมิจฉาชีพ โดยการสมัครใช้บริการหรือเข้าร่วมกิจกรรมบางอย่าง โดยไม่ทันอ่านรายละเอียดให้ละเอียด

๔. ข้อมูลรั่วไหลจากบริษัท : ข้อมูลส่วนตัวของคุณอาจถูกขโมยจากบริษัทที่คุณใช้บริการ โดยฝีมือของแฮกเกอร์

๕. การซื้อข้อมูลส่วนตัว : ข้อมูลส่วนตัวของคุณอาจถูกแฮกและนำไปซื้อขายในตลาดมืด

วิธีรับมือกับแก๊งคอลเซ็นเตอร์

<u>ก่อนรับสาย</u> - ให้ระวังการรับสายจากเบอร์โทรศัพท์ที่ไม่รู้จัก
- ตรวจสอบเบอร์โทรศัพท์ก่อนรับสาย
- ตั้งสติและคำนึงไว้เสมอว่าสถาบันการเงิน และภาคราชการไม่มีนโยบายสอบถามข้อมูลส่วนบุคคลทางโทรศัพท์ จะได้ไม่โอนอ่อนไปตามสิ่งที่ปลายสายกำลังจะพูด

<u>ระหว่างรับสาย</u> - ห้ามให้ข้อมูลส่วนตัว โดยเฉพาะหากมีการถามถึงข้อมูลส่วนตัวที่อาจนำไปสู่การทำธุรกรรมทางการเงินได้
- ตั้งคำถาม เพื่อจับพิรุธของคนร้ายที่อยู่ปลายสาย และตรวจสอบให้แน่ใจว่าผู้ที่เราคุยด้วยเป็นคนร้ายหรือเปล่า
- รีบวางสายหากรู้สึกถึงความไม่ปลอดภัย เพราะปลายสายอาจใช้ช่วงเวลาในระหว่างการคุยโทรศัพท์เพื่อถ่วงเวลาเข้าควบคุมหน้าจอโทรศัพท์ของคุณจากทางไกล

<u>หลังรับสาย</u> - หลังจากวางสายจากผู้ที่คิดว่าเป็นแก๊งคอลเซ็นเตอร์ ให้รีบตรวจสอบธุรกรรมทางการเงินว่ามีอะไรเปลี่ยนแปลงไปหรือไม่
- รีบแจ้งความทันทีหากพบความเปลี่ยนแปลงในบัญชีหรือการทำธุรกรรมของคุณ
- และรีบแจ้งไปยังหน่วยงานที่เกี่ยวข้อง เช่น ธนาคาร หรือผู้ให้บริการทางการเงินเพื่อยุติและตรวจสอบการทำธุรกรรมที่ผิดปกตินั้น
- หากยังไม่แน่ใจว่าปลายสายที่คุยด้วยก่อนหน้านี้เป็นคนร้ายหรือเจ้าหน้าที่ตัวจริง ให้สอบถามข้อมูลจากหน่วยงานหรือธนาคารโดยตรง โดยไม่ใช้ข้อมูลที่ได้มาจากคนร้ายแต่อาจใช้การค้นหาบนอินเตอร์เน็ตเพื่อค้นหาเบอร์โทรและช่องทางติดต่อที่แท้จริงของหน่วยงาน

<u>ข้อควรระวัง</u>

๑. หากมีการส่งลิงก์หรือไฟล์แนบมาให้ระหว่างการสนทนา อย่ากดลิงก์หรือเปิดข้อมูลไฟล์ที่แนบมานั้นเด็ดขาด

๒. ห้ามโอนเงินไปให้คนอื่นผ่านช่องทางออนไลน์

ในกรณีที่พลาดไปแล้วอย่าเพิ่งตกใจและลนลาน เพราะอาจทำให้เผลอตกเป็นเหยื่อซ้ำ ๆ จากความตื่นตระหนก ดังนั้นหากโอนเงินไปให้แก๊งคอลเซ็นเตอร์ไปแล้ว ให้รีบรวบรวมข้อมูล หลักฐาน และเอกสารที่เกี่ยวข้องติดต่อสถาบันการเงินเพื่อระงับการโอนเงินดังกล่าวทันที และไปแจ้งความกับเจ้าหน้าที่ตำรวจเพื่อขอดำเนินคดีกับผู้กระทำผิด รวมไปถึงการแจ้งเบาะแสกับกรมสอบสวนคดีพิเศษ (DSI) หรือแจ้งเบาะแสไปยังสำนักงานตำรวจแห่งชาติ เพื่อเป็นประโยชน์แก่เจ้าหน้าที่ในการสืบหาตัวคนร้ายต่อไป

ผลกระทบจากแก๊งคอลเซ็นเตอร์จากแก๊งคอลเซ็นเตอร์ไม่เพียงแต่จะก่อให้เกิดความเสียหายทางเศรษฐกิจต่อเหยื่อจำนวนมากแล้ว ยังก่อให้เกิดความเสียหายต่อเศรษฐกิจในภาพรวมระดับประเทศอีกด้วย ดังนั้นกรณีแก๊งคอลเซ็นเตอร์นี้ จึงถือได้ว่าเป็นอาชญากรรมทางเศรษฐกิจข้ามชาติที่เป็นภัยร้ายแรงอีกประการหนึ่งของประเทศ ที่ผ่านมาศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) หรือตำรวจไซเบอร์ รายงานว่าแก๊งคอลเซ็นเตอร์สร้างความเสียหายโดยส่งผลกระทบถึงเศรษฐกิจและสังคมถึง ๑,๖๐๐ ล้านบาท

ปัจจุบัน ตำรวจไซเบอร์ ได้มีการจัดทำแพพลิเคชั่น Cyber Check เป็นแอพพลิเคชั่นที่ใช้ป้องกันมิจฉาชีพ แก๊งคอลเซ็นเตอร์ โดยการเช็กก่อนรับ-โอน ได้เพียงกดโทรออก ซึ่งเป็นแอปพลิเคชันที่จะช่วยคัดกรองมิจฉาชีพจากเบอร์โทรปริศนาที่โทรเข้ามา รวมทั้งใช้ตรวจสอบเลขบัญชีธนาคารก่อนจะโอนเงิน เพียงแค่นำเลขบัญชีไปกดโทรออก โดยใช้ฐานข้อมูลโดยตรงจากระบบรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ

การทำงานของแอปพลิเคชัน Cyber Check

๑. เมื่อติดตั้งแอปพลิเคชันครั้งแรกแล้ว สามารถปิดแอปได้ โดยแอปจะทำงานเมื่อมีสายโทรเข้าหรือ โทรออก และจะช่วยตรวจสอบเบอร์โทรศัพท์ หรือ หมายเลขบัญชีธนาคารที่มีการแจ้งความดำเนินคดี(สีแดง) ร้องเรียน(สีเหลือง) และผู้ที่ลงทะเบียนยืนยันตัวตนกับ บช.สอท หรือ หน่วยงานรัฐอื่น (สีเขียว)

๒. ในระบบ Android ยังสามารถนำหมายเลขบัญชีธนาคารมากดโทรออก เพื่อตรวจสอบข้อมูลในลักษณะเดียวกันกับหมายเลขโทรศัพท์ได้ โดยไม่เสียค่าบริการ

๓. สามารถตั้งค่ากดเลือกบล็อคเบอร์สีเหลือง และ สีแดง ได้อัตโนมัติ

๔. ระบบคัดกรอง SMS และ ลิงก์ที่มีความเสี่ยง

๕. แอปพลิเคชันยังรวมลิงก์สำหรับดำเนินการเกี่ยวกับอาชญากรรมทางเทคโนโลยีต่างๆ เช่น ระบบรับแจ้งความออนไลน์ thaipoliceonline.go.th, เช็กก่อน.com, chaladohn.com, ไซเบอร์วัคซีน

๖. ฟังก์ชันสายด่วน ๑๔๔๑

๗. ฟังก์ชัน การค้นหาในแอปดังกล่าว เพื่อตรวจสอบหมายเลขบัญชี และ หมายเลขโทรศัพท์ในลักษณะเดียวกับ ข้อ ๑ และ ข้อ ๒

ข้อดีของแอปพลิเคชันดังกล่าว คือ ระบบไม่มีการดึงข้อมูลของผู้ใช้งานเหมือนแอปพลิเคชันอื่นๆ แต่ใช้ฐานข้อมูลจากระบบรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติที่มีการร้องเรียนและดำเนินคดีจริง โดยในอนาคตจะเป็นการสร้างความมั่นใจในการตัดสินใจซื้อสินค้า เพราะทางแอปพลิเคชันมีแผนในการลงทะเบียนรวบรวมข้อมูลผู้ทำการค้าออนไลน์จริง เพื่อกระตุ้นการไหลเวียนทางเศรษฐกิจอีกด้วย

ในกรณีหน่วยงานราชการ หรือ หน่วยงานเอกชน ที่โดนมิจฉาชีพนำข้อมูลไปแอบอ้าง สามารถติดต่อเพื่อขอลงข้อมูลให้ประชาชนทราบว่า ผู้ที่แอบอ้างไม่ได้เป็นเจ้าหน้าที่รัฐหรือเอกชนที่มีหน้าที่ติดต่อประชาชนอย่างแท้จริง ซึ่งหน่วยงานต่างๆ สามารถติดต่อขอลงทะเบียนข้อมูลได้ที่ บช.สอท. ทั้งนี้ สามารถใช้ได้แล้วทั้งในระบบ Androidและ IOS โดยสามารถดาวน์โหลดได้ทั้งบน Google Play และ App Store

ผู้เข้าร่วมรับการอบรมมีการทำแบบทดสอบก่อนและหลังจากการรับฟังการบรรยายจากวิทยากร เพื่อสร้างความเข้าใจและตระหนักถึงความร้ายแรงของแก๊งคอลเซ็นเตอร์ โดยการติดตั้งแอปพลิเคชัน Cyber Check เป็นอีกทางเลือกหนึ่งที่ช่วยให้สามารถตรวจสอบข้อมูลที่สงสัยว่าอาจจะเป็นแก๊งคอลเซนเตอร์ ก่อนที่จะตกเป็นเหยื่อของแก๊งมิจฉาชีพ

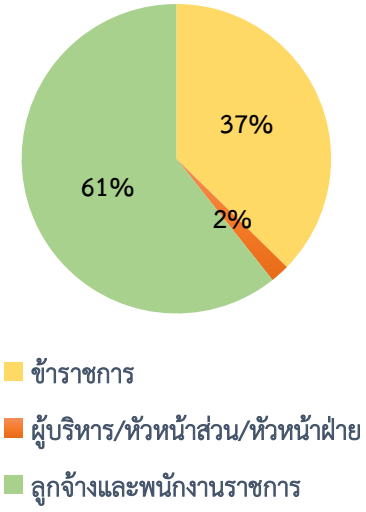
สรุปแบบประเมินความพึงพอใจ โครงการฝึกอบรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ.2568
วันที่ 30 มิถุนายน 2568 ณ ลีลาวดี รีสอร์ท อำเภอเมืองสระบุรี จังหวัดสระบุรี
จำนวนผู้เข้าร่วมโครงการ 150 คน

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบประเมิน

1.1 ตำแหน่งผู้เข้าร่วมโครงการ

ตำแหน่ง	จำนวน(คน)
ผู้บริหาร/หัวหน้าส่วน/หัวหน้าฝ่าย	3
ข้าราชการ	56
ลูกจ้างและพนักงานราชการ	91

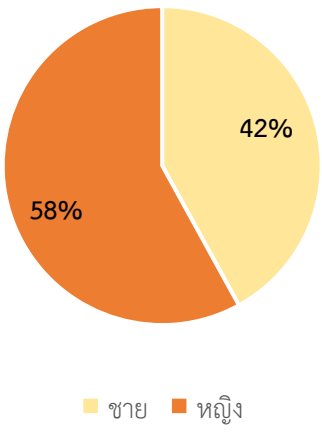
ข้อมูลทั่วไปของผู้ตอบแบบประเมินพบว่า ผู้เข้าร่วมโครงการเป็น ลูกจ้างและพนักงานราชการ มากที่สุด คิดเป็นร้อยละ 61 รองลงมาคือ ข้าราชการ คิดเป็นร้อยละ 37 และ ผู้บริหาร/หัวหน้าส่วน/หัวหน้าฝ่าย คิดเป็นร้อยละ 2 ของผู้เข้าร่วมโครงการทั้งหมด



1.2 เพศผู้เข้าร่วมโครงการ

เพศ	จำนวน(คน)
ชาย	63
หญิง	87

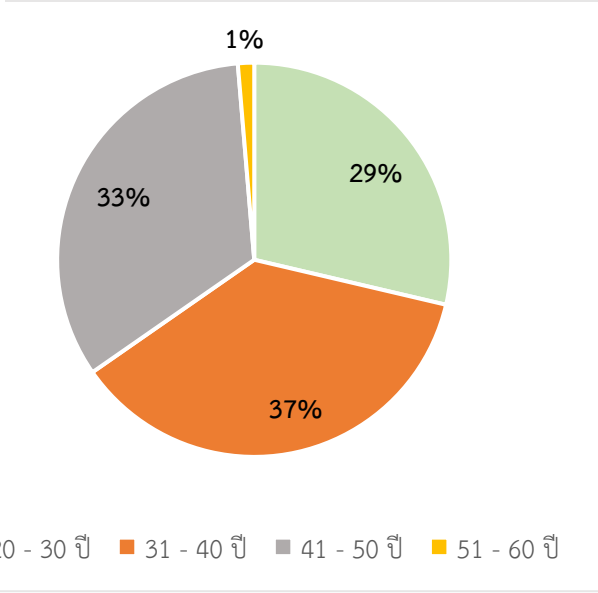
ข้อมูลทั่วไปของผู้ตอบแบบประเมิน พบว่า ผู้เข้าร่วมโครงการเป็น เพศหญิง มากที่สุด คิดเป็นร้อยละ 87 และเพศหญิง คิดเป็นร้อยละ 42 ของผู้เข้าร่วมโครงการทั้งหมด



1.3 ช่วงอายุผู้เข้าร่วมโครงการ

ช่วงอายุ	จำนวน(คน)
20 - 30 ปี	43
31 - 40 ปี	55
41 - 50 ปี	50
51 - 60 ปี	2

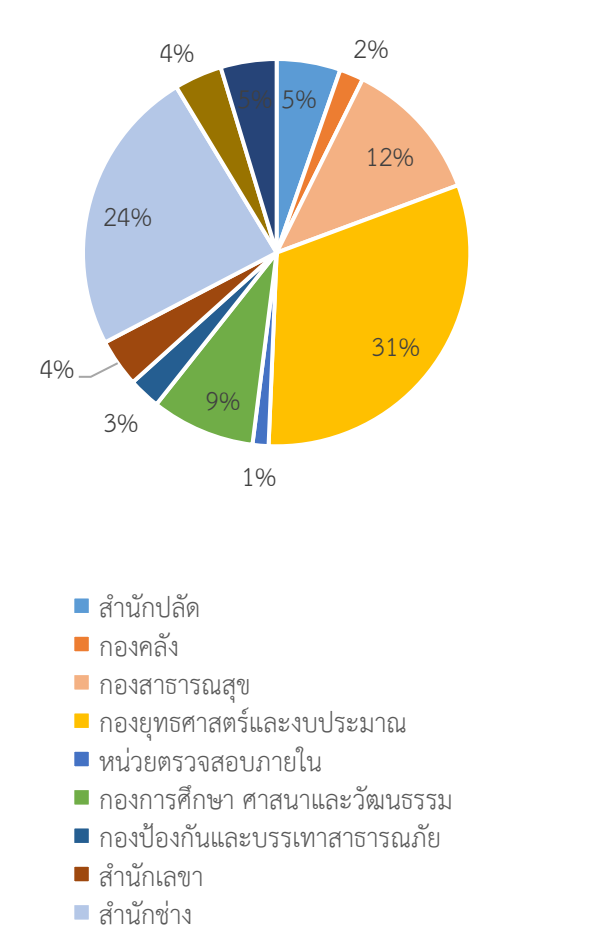
ข้อมูลทั่วไปของผู้ตอบแบบประเมิน พบว่า ผู้เข้าร่วมโครงการมีช่วงอายุเป็น 31 – 40 ปี มากที่สุด คิดเป็นร้อยละ 37 รองลงมาคือช่วงอายุ 41 - 50 ปี คิดเป็นร้อยละ 33 และ ช่วงอายุ 20 - 30 ปี คิดเป็นร้อยละ 29 ของผู้เข้าร่วมโครงการทั้งหมด



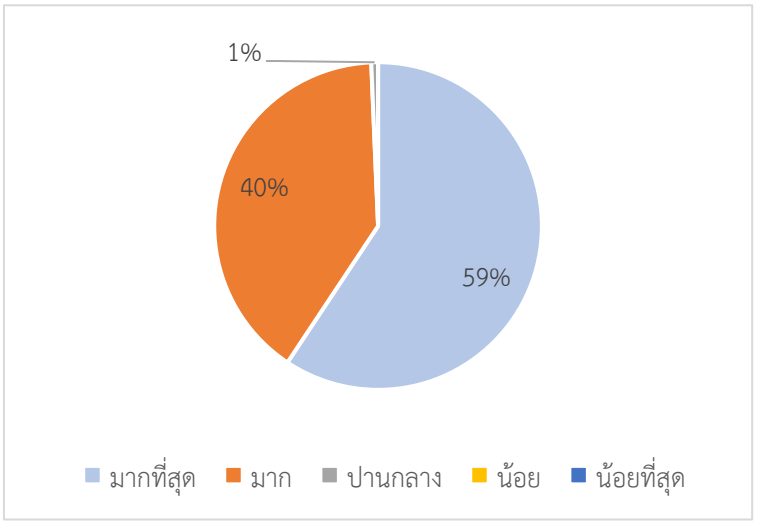
1.4 สังกัดหน่วยงานผู้เข้าร่วมโครงการ

หน่วยงาน	จำนวน(คน)
สำนักปลัดฯ	8
กองคลัง	3
กองสาธารณสุข	18
กองยุทธศาสตร์และงบประมาณ	47
หน่วยตรวจสอบภายใน	2
กองการศึกษา ศาสนาและวัฒนธรรม	13
กองป้องกันและบรรเทาสาธารณภัย	4
สำนักเลขาฯ	6
สำนักช่าง	36
กองการเจ้าหน้าที่	6
กองพัสดุและทรัพย์สิน	7

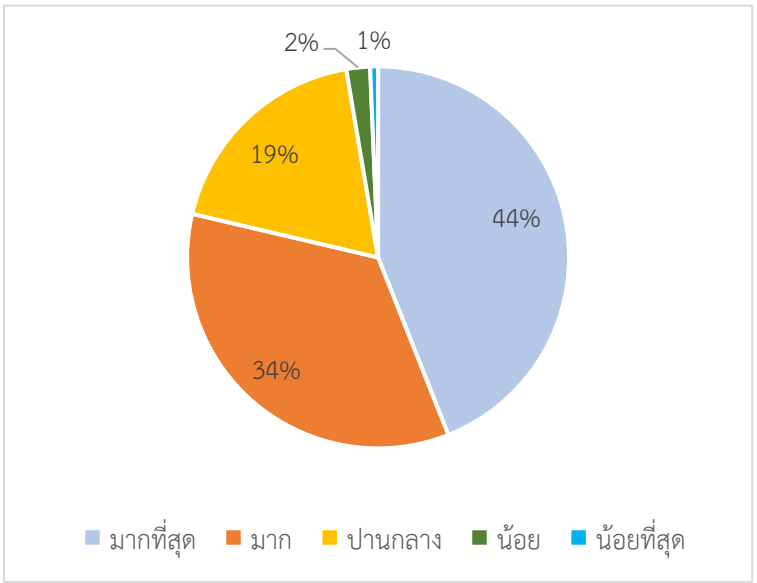
ข้อมูลทั่วไปของผู้ตอบแบบประเมิน พบว่า ผู้เข้าร่วมโครงการเป็นเจ้าหน้าที่กองยุทธศาสตร์และงบประมาณมากที่สุด คิดเป็นร้อยละ 31 รองลงมาคือสำนักช่าง คิดเป็นร้อยละ 24 และ กองสาธารณสุข คิดเป็นร้อยละ 12 ของผู้เข้าร่วมโครงการทั้งหมด



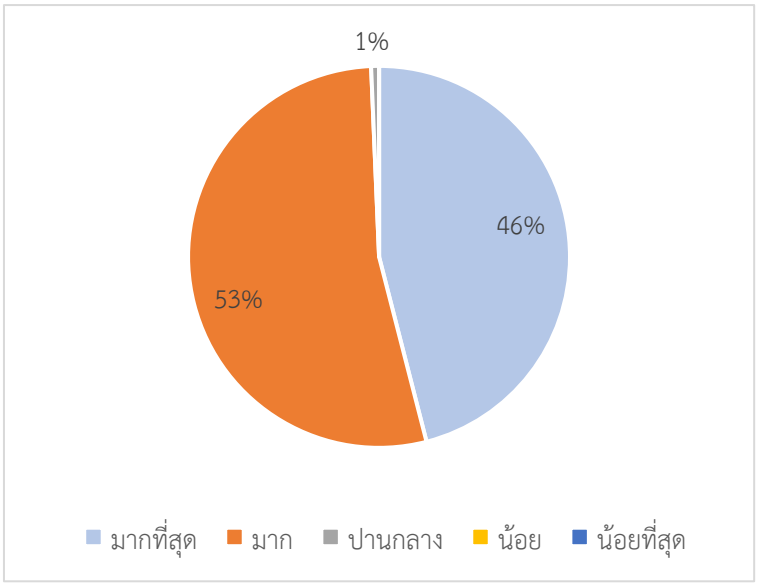
2.1 สถานที่จัดโครงการมีความเหมาะสม ผู้ตอบแบบประเมินพอใจมากที่สุด จำนวน 89 คน คิดเป็นร้อยละ 59 พอใจมาก จำนวน 60 คน คิดเป็นร้อยละ 40 พอใจปานกลางจำนวน 1 คน คิดเป็นร้อยละ 1



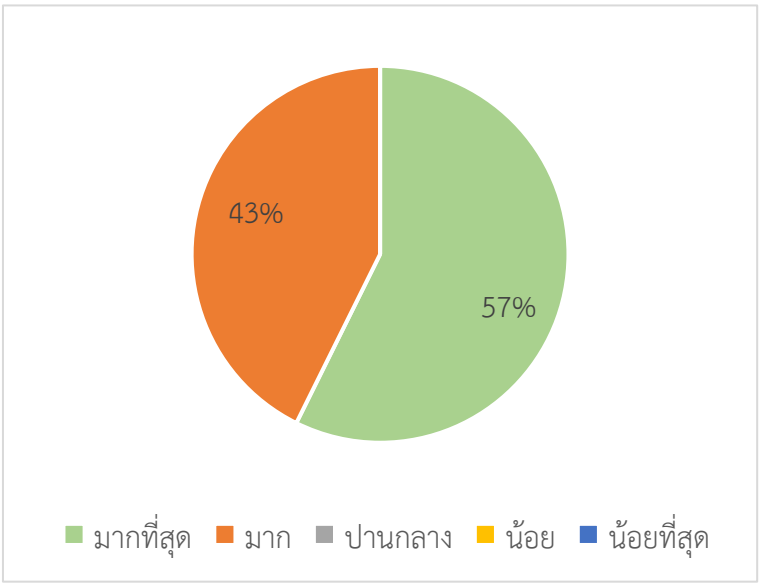
2.2 อาหารและเครื่องดื่มมีความเหมาะสม ผู้ตอบแบบประเมินพอใจมากที่สุด จำนวน 66 คน คิดเป็นร้อยละ 44 พอใจมาก จำนวน 52 คน คิดเป็นร้อยละ 34 พอใจปานกลางจำนวน 28 คน คิดเป็นร้อยละ 19 ตามลำดับ



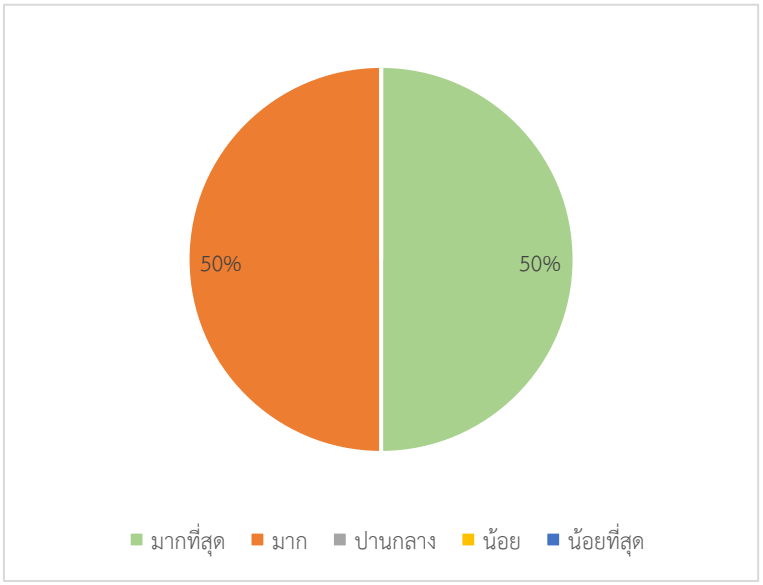
2.3 วันและระยะเวลาในการจัดโครงการอบรมมีความเหมาะสม ผู้ตอบแบบประเมินพอใจมากที่สุด จำนวน 69 คน คิดเป็นร้อยละ 46 พอใจมาก จำนวน 80 คน คิดเป็นร้อยละ 53 พอใจปานกลางจำนวน 1 คน คิดเป็นร้อยละ 1 ตามลำดับ



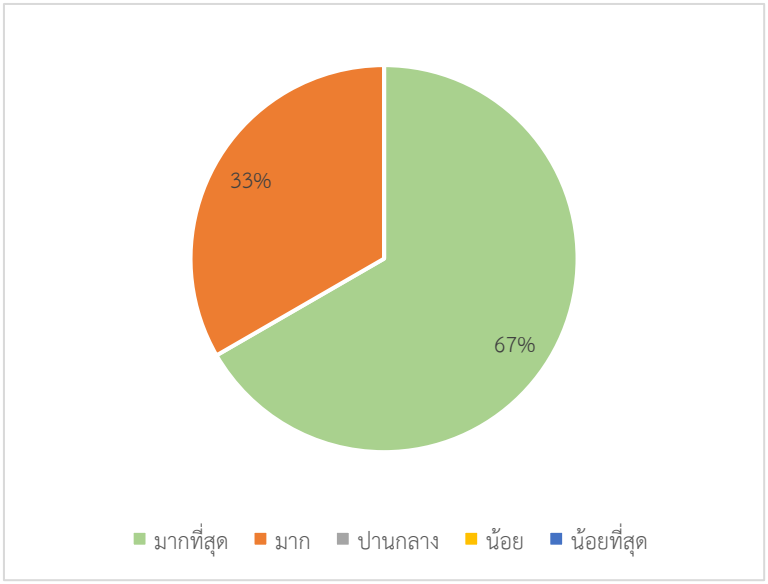
2.4 หลักสูตร เนื้อหา มีความครบถ้วน เป็นประโยชน์ต่อผู้ปฏิบัติงาน ผู้ตอบแบบประเมินพอใจมากที่สุด จำนวน 86 คน คิดเป็นร้อยละ 57 พอใจมาก จำนวน 64 คน คิดเป็นร้อยละ 33 ตามลำดับ



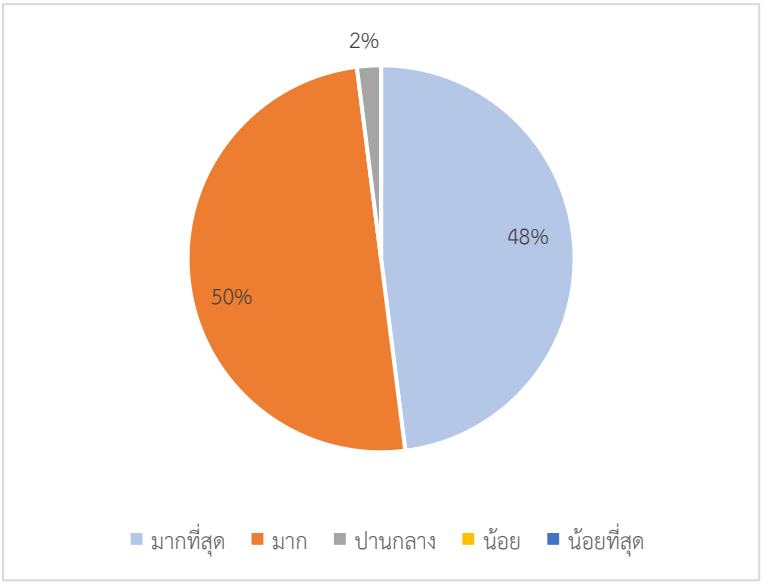
2.5 วิทยากรสามารถถ่ายทอดความรู้ได้อย่างชัดเจน (อัยการจังหวัด) ผู้ตอบแบบประเมินพอใจมากที่สุด จำนวน 75 คน คิดเป็นร้อยละ 50 พอใจมาก จำนวน 75 คน คิดเป็นร้อยละ 50 ตามลำดับ



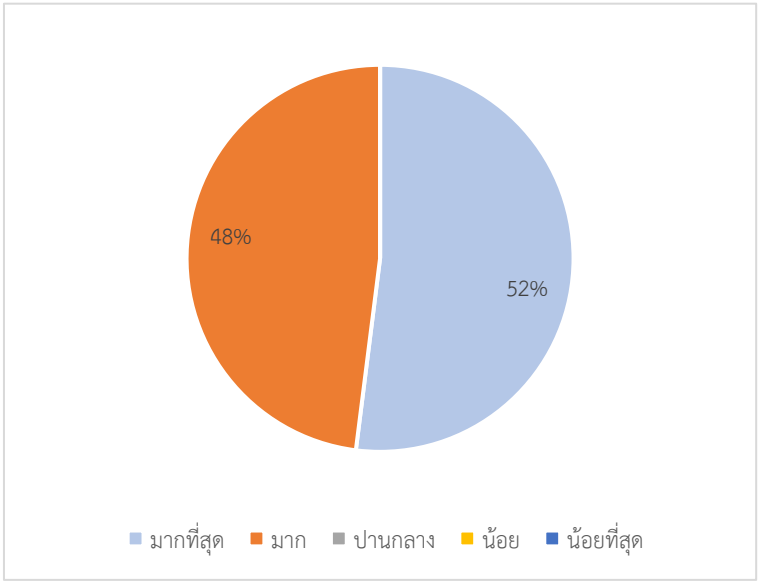
2.6 วิทยากรสามารถถ่ายทอดความรู้ได้อย่างชัดเจน (ตำรวจไซเบอร์) ผู้ตอบแบบประเมินพอใจมากที่สุด จำนวน 100 คน คิดเป็นร้อยละ 67 พอใจมาก จำนวน 50 คน คิดเป็นร้อยละ 33 ตามลำดับ



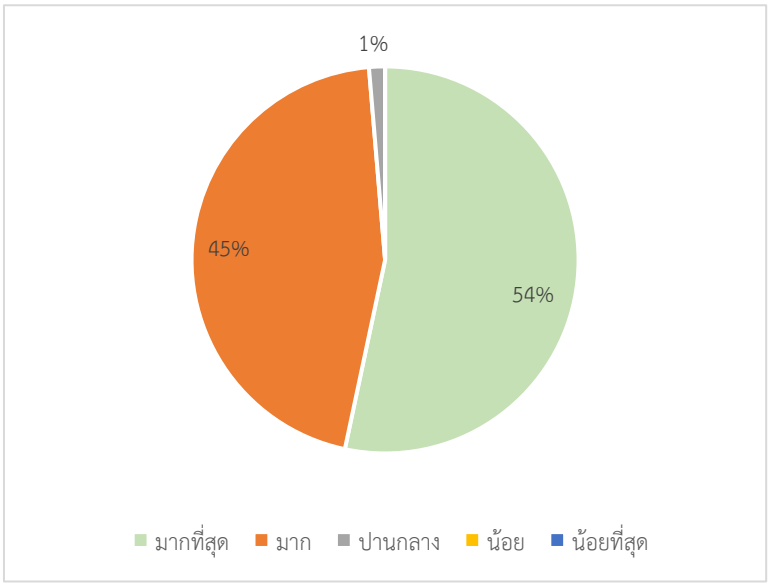
2.7 เอกสาร คู่มือ และสื่อประกอบการอบรมมีความเหมาะสม ผู้ตอบแบบประเมินตอบมากที่สุด จำนวน 72 คน คิดเป็นร้อยละ 48 ตอบมาก จำนวน 75 คน คิดเป็นร้อยละ 50 ตอบปานกลาง จำนวน 3 คน คิดเป็นร้อยละ 2 ตามลำดับ



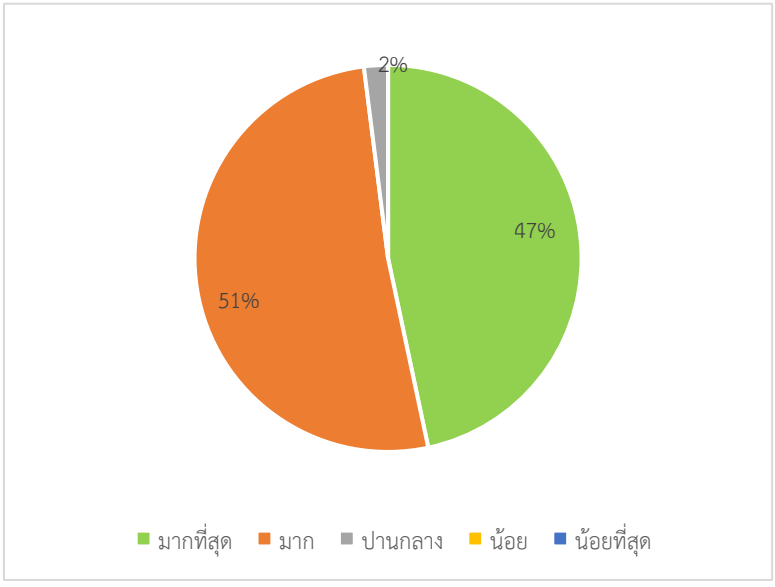
2.8 ความรู้ที่ได้รับสามารถนำไปใช้ปฏิบัติได้จริง ผู้ตอบแบบประเมินตอบมากที่สุด จำนวน 78 คน คิดเป็นร้อยละ 52 ตอบมาก จำนวน 72 คน คิดเป็นร้อยละ 48 ตามลำดับ ตามลำดับ



2.9 ระดับความรู้หลังเข้ารับการฝึกอบรม ผู้ตอบแบบประเมินตอบมากที่สุด จำนวน 80 คน คิดเป็นร้อยละ 54 ตอบมาก จำนวน 68 คน คิดเป็นร้อยละ 45 ตอบปานกลาง จำนวน 2 คน คิดเป็นร้อยละ 1 ตามลำดับ

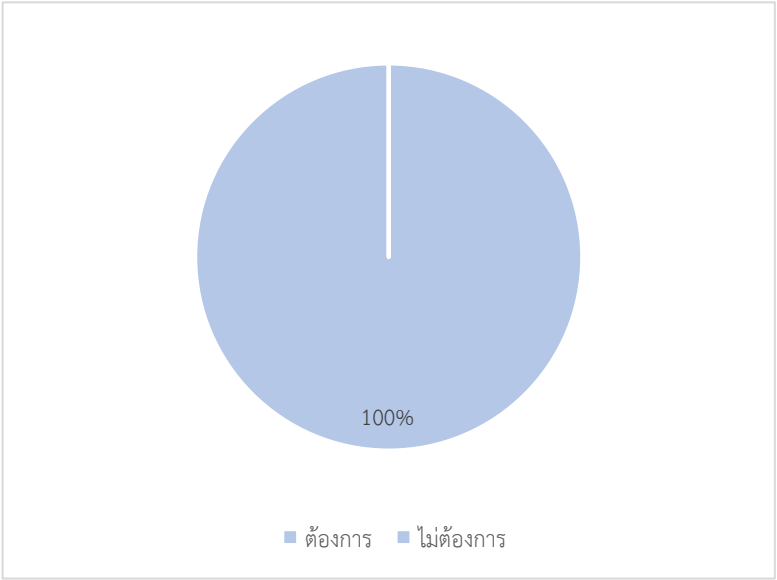


2.10 ความพึงพอใจโดยภาพรวมของโครงการอบรม ผู้ตอบแบบประเมินตอบมากที่สุด จำนวน 70 คน คิดเป็นร้อยละ 47 ตอบมาก จำนวน 77 คน คิดเป็นร้อยละ 51 ตอบปานกลาง จำนวน 3 คน คิดเป็นร้อยละ 2 ตามลำดับ



ส่วนที่ 3 ปัญหาข้อบกพร่อง และข้อเสนอแนะ

3.1 ความต้องการต่อการจัดโครงการ ผู้ตอบแบบประเมินมีความต้องการให้มีการจัดโครงการเป็นประจำ จำนวน 150 คน คิดเป็นร้อยละ 100 และไม่มีผู้ไม่ต้องการให้มีการจัดอบรมเป็นประจำ



3.2 ปัญหาข้อบกพร่อง และข้อเสนอแนะ ผู้ตอบแบบประเมินได้ ให้ข้อเสนอแนะดังนี้

1. ในการจัดอบรมขอให้มีการจัดรถรับส่งผู้เข้าร่วมอบรม เนื่องจากมีปัญหาเรื่องจากเดินทางและค่าใช้จ่าย กรณีที่ใช้รถส่วนตัวเดินทางมาร่วมอบรมควรมีงบประมาณสนับสนุนในเรื่องค่าใช้จ่ายในการเดินทาง เพื่อเป็นการกระตุ้นในผู้เข้าร่วมอบรมมีความกระตือรือร้นในการเดินทางเข้าร่วมมากยิ่งขึ้น

2. ห้องน้ำไม่สะอาด

3. ระยะเวลาการจัดโครงการน้อยเกินไป

ภาคผนวก

“โครงการฝึกอบรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘” ขององค์การบริหารส่วนจังหวัดสระบุรี
วันที่ ๓๐ มิถุนายน พ.ศ. ๒๕๖๘
ณ ลีลาวดี รีสอร์ท สระบุรี อำเภอเมืองสระบุรี จังหวัดสระบุรี

“โครงการฝึกอบรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘” ขององค์การบริหารส่วนจังหวัดสระบุรี
วันที่ ๓๐ มิถุนายน พ.ศ. ๒๕๖๘
ณ ลีลาวดี รีสอร์ท สระบุรี อำเภอเมืองสระบุรี จังหวัดสระบุรี

“โครงการฝึกอบรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘” ขององค์การบริหารส่วนจังหวัดสระบุรี
วันที่ ๓๐ มิถุนายน พ.ศ. ๒๕๖๘
ณ ลีลาวดี รีสอร์ท สระบุรี อำเภอเมืองสระบุรี จังหวัดสระบุรี