การสร้างความมั่นคงปลอดภัยทางไซเบอร์

นางสาวฎานุภา อยู่อุ่นพะเนา นักวิชาการเกษตรชำนาญการพิเศษ กองเทคโนโลยีชีวภาพทางดิน
ที่มา : โครงการพัฒนาบุคลากรด้านคอมพิวเตอร์และสารสนเทศ หลักสูตร “การสร้างความมั่นคงปลอดภัยทางไซเบอร์” รุ่นที่ 1 ระหว่างวันที่ 16 – 17 พฤษภาคม 2567 ณ ห้องปฏิบัติการฝึกอบรมคอมพิวเตอร์และสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

ปัจจุบันการให้บริการของกรมพัฒนาที่ดิน การติดต่อสื่อสาร การรายงานผลการดำเนินงานการสืบค้นข้อมูลต่างๆ ได้ก้าวเข้าสู่ยุคดิจิทัล เจ้าหน้าที่ของกรมฯ จึงต้องใช้งานคอมพิวเตอร์ ระบบเครือข่ายและเทคโนโลยีสารสนเทศของกรมฯ จึงจำเป็นต้องมีความตระหนักรู้ในด้านความมั่นคง ความปลอดภัยการใช้งานเทคโนโลยีสารสนเทศ และความเสี่ยงภัยในรูปแบบต่างๆ และแนวทางปฏิบัติเพื่อหลีกเลี่ยงภัยคุกคามดังกล่าว ในการอบรมเป็นการนำเสนอเกี่ยวกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act - PDPA) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และการฟิชชิงผ่านแอปพลิเคชันมือถือ (Phishing Mobile Apps) โดยมีเนื้อหาสาระสำคัญ ดังนี้

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act - PDPA) ซึ่งถูกบังคับใช้เพื่อปกป้องข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิและเสรีภาพ โดยเนื้อหาครอบคลุมหัวข้อสำคัญต่าง ๆ ดังนี้

1.1 องค์ประกอบของพระราชบัญญัติ มีการอธิบายถึงหมวดหมู่ต่าง ๆ ของกฎหมาย รวมถึงสิทธิของเจ้าของข้อมูลส่วนบุคคล การคุ้มครองข้อมูล การร้องเรียน และบทลงโทษ

1.2 ขอบเขตการบังคับใช้ กฎหมายนี้ครอบคลุมถึงการเก็บรวบรวม การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล ทั้งในและนอกประเทศไทย โดยผู้ควบคุมหรือประมวลผลข้อมูลส่วนบุคคล

1.3 ข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลหมายถึงข้อมูลที่สามารถระบุตัวตนได้ เช่น ชื่อ เลขบัตรประชาชน อีเมล์ รวมถึงข้อมูลชีวมิติ เช่น ลายนิ้วมือ รูปภาพใบหน้า ข้อมูลสุขภาพ และข้อมูลการจ้างงาน

1.4 บทบาทและหน้าที่ของผู้ควบคุมข้อมูล ผู้ควบคุมข้อมูลต้องดำเนินการตามกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

1.5 สิทธิของเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิต่าง ๆ เช่น สิทธิในการเข้าถึงข้อมูล การคัดค้าน การแก้ไข และการลบข้อมูลส่วนบุคคล รวมถึงสิทธิในการยื่นเรื่องร้องเรียนต่อคณะกรรมการ

1.6 ข้อยกเว้น มีบางกรณีที่สามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล เช่น ในกรณีที่เป็นการปฏิบัติตามกฎหมาย หรือเพื่อประโยชน์สาธารณะ

1.7 มาตรการรักษาความมั่นคงปลอดภัย ต้องมีการจัดการมาตรการด้านความปลอดภัยเพื่อป้องกันการละเมิดข้อมูล รวมถึงการแจ้งเหตุเมื่อมีการละเมิดข้อมูลเกิดขึ้น

1.8 การละเมิดข้อมูลส่วนบุคคล มีการอธิบายถึงการละเมิดข้อมูลส่วนบุคคลในลักษณะต่าง ๆ และการดำเนินการเมื่อเกิดเหตุการณ์ละเมิดขึ้น

2. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

โดยความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะในส่วนของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ซึ่งครอบคลุมหลายด้าน เช่น ด้านความมั่นคงของรัฐ บริการภาครัฐที่สำคัญ การเงินและธนาคาร เทคโนโลยีสารสนเทศ การสาธารณสุข และรับมือกับภัยคุกคามทางไซเบอร์ โดยระดับของภัยคุกคามทางไซเบอร์ที่แบ่งออกเป็น 3 ระดับ ได้แก่ ไม่ร้ายแรง ร้ายแรง และวิกฤต พร้อมทั้งบทบาทหน้าที่ของคณะกรรมการต่าง ๆ ที่เกี่ยวข้องกับการกำกับดูแลและรับมือกับภัยคุกคามทางไซเบอร์ นอกจากนี้ยังรวมถึงกฎหมายลำดับรองที่ออกตามพระราชบัญญัติ ซึ่งมีการจัดทำเพื่อสนับสนุนการดำเนินงานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัยตามมาตรฐานที่กำหนด

3. การฟิชชิงผ่านแอปพลิเคชันมือถือ (Phishing Mobile Apps)

โดยฟิชชิงเป็นการโจมตีทางไซเบอร์ที่มีการหลอกลวงเหยื่อเพื่อให้เปิดเผยข้อมูลสำคัญ เช่น ข้อมูลส่วนตัว รหัสผ่าน หรือข้อมูลบัตรเครดิต โดยเฉพาะผ่านแอปพลิเคชันมือถือซึ่งเป็นเป้าหมายสำคัญในปัจจุบันมีหลากหลาย เช่น แอปปลอมที่ออกแบบให้ดูเหมือนกับแอปพลิเคชันจริง หรือการส่งลิงก์ที่เป็นอันตรายผ่านแอปพลิเคชันส่งข้อความ การโจมตีในลักษณะนี้ทำให้ผู้ใช้หลงเชื่อและกรอกข้อมูลสำคัญลงไปโดยไม่รู้ตัว

การป้องกันการฟิชชิงผ่านแอปพลิเคชันมือถือประกอบด้วยหลายวิธี เช่น การตรวจสอบความถูกต้องของแอปพลิเคชันก่อนติดตั้ง การหลีกเลี่ยงการคลิกลิงก์ที่น่าสงสัย การใช้โปรแกรมป้องกันไวรัสและมัลแวร์ การตั้งค่าความปลอดภัยที่เข้มงวดในอุปกรณ์มือถือ และการระมัดระวังในการให้ข้อมูลส่วนตัวออนไลน์

นอกจากนี้ยังมีการ ตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์ และการสร้างความมั่นคงปลอดภัยไซเบอร์ ซึ่งนำเสนอโดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีพันธกิจในการกำหนดนโยบาย ยุทธศาสตร์ และมาตรการที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเป็นศูนย์กลางในการประสานงานระหว่างหน่วยงานภาครัฐและเอกชน ทั้งในและต่างประเทศ