หัวข้อการพัฒนา :
ความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล (Cyber Security and Digital Awareness)

สรุปสาระสำคัญ

การพัฒนาความรู้ในหลักสูตร "ความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล (Cyber Security and Digital Awareness)" มีวัตถุประสงค์สำคัญเพื่อให้ข้าราชการมีความเข้าใจและรู้เท่าทันภัยเงียบในโลกออนไลน์ เพื่อร่วมกันปกป้องข้อมูลของทางราชการไม่ให้เกิดการรั่วไหล สาระสำคัญจากการเรียนรู้ชี้ให้เห็นว่า ความเสี่ยงสูงสุดที่คุกคามหน่วยงานภาครัฐมักมีสาเหตุหลักมาจากความไม่รู้หรือความประมาทของตัวบุคคล (Human Error) เป็นสำคัญ โดยภัยคุกคามที่พบได้บ่อยในปัจจุบันมีทั้งการทำ Phishing หรือการหลอกให้กรอกข้อมูลสำคัญผ่านลิงก์หรืออีเมลปลอม การใช้ Malware ประเภทต่าง ๆ เช่น Ransomware ที่เข้ามาล็อกไฟล์เพื่อเรียกค่าไถ่ซึ่งเป็นอันตรายต่อข้อมูลราชการอย่างมาก รวมถึง Trojan Horse ที่เปิดทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องคอมพิวเตอร์ นอกจากนี้ยังมีกระบวนการ Social Engineering หรือวิศวกรรมสังคมที่ใช้จิตวิทยาในการหลอกลวงผ่านการแอบอ้างเป็นเจ้าหน้าที่ระดับสูงเพื่อขอข้อมูลลับหรือให้โอนเงิน

ในการรับมือกับภัยคุกคามเหล่านี้ ข้าราชการจำเป็นต้องยึดถือหลักการ CIA Triad ซึ่งเป็นหัวใจสำคัญของความมั่นคงปลอดภัยสารสนเทศ อันประกอบด้วย การรักษาความลับ (Confidentiality) เพื่อให้เฉพาะผู้มีสิทธิ์เท่านั้นที่เข้าถึงข้อมูลได้ การรักษาความถูกต้องครบถ้วน (Integrity) เพื่อป้องกันการแก้ไขข้อมูลโดยมิชอบ และ การพร้อมใช้งาน (Availability) เพื่อให้ระบบปฏิบัติงานและข้อมูลต่าง ๆ พร้อมให้บริการประชาชนได้อย่างต่อเนื่อง โดยแนวทางปฏิบัติเพื่อสร้างสุขอนามัยทางไซเบอร์ (Cyber Hygiene) ที่ดีนั้น เริ่มต้นจากการตั้งรหัสผ่านที่คาดเดายากและมีความยาว 8 - 12 ตัวอักษร การใช้ระบบยืนยันตัวตนสองชั้น (2FA) ด้วยรหัส OTP อัปเดตระบบปฏิบัติการและโปรแกรมแอนตี้ไวรัสเพื่ออุดช่องโหว่ของระบบ ตลอดจนความระมัดระวังในการใช้งาน Wi-Fi สาธารณะซึ่งควรเชื่อมต่อผ่านระบบ VPN ของหน่วยงานทุกครั้งเมื่อต้องส่งข้อมูลราชการ ทั้งนี้ ข้าราชการในฐานะเจ้าหน้าที่รัฐต้องมีความตระหนักและปฏิบัติตามกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด ทั้ง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลของประชาชน

การนำความรู้ไปใช้ประโยชน์

สำหรับการนำความรู้ไปใช้ประโยชน์นั้น ในระดับบุคคลจะช่วยสร้างภูมิคุ้มกันให้รอดพ้นจากการเป็นเหยื่อมิจฉาชีพ ปกป้องทรัพย์สินส่วนตัว และยังเป็นการพัฒนาทักษะดิจิทัล (Digital Literacy) ซึ่งเป็นสมรรถนะหลักในการความก้าวหน้าในอาชีพราชการ ในระดับหน่วยงาน ความรู้ดังกล่าวจะช่วยรักษาความลับขององค์กร ทำให้ระบบงานมีความต่อเนื่องลดความเสี่ยงจากการถูกโจมตีด้วยมัลแวร์ และช่วยประหยัดงบประมาณรวมถึงทรัพยากรในการกู้คืนระบบที่เสียหาย และในระดับประเทศชาติ การปฏิบัติงานที่ถูกต้องและปลอดภัยจะช่วยสร้างความเชื่อมั่นให้กับประชาชนในการใช้บริการดิจิทัลของรัฐ