สรุปผลการดำเนินงาน

โครงการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์พื้นฐาน

เมื่อวันพุธที่ 18 มีนาคม 2569 ณ ตึกแดง 1 ห้องประชุมผ่านฟ้า

วัตถุประสงค์

1. เพื่อเสริมสร้างความรู้ความเข้าใจและความตระหนักรู้: ให้แก่บุคลากรของสำนักเลขาธิการนายกรัฐมนตรี (สลน.) เกี่ยวกับภัยคุกคามทางไซเบอร์ รูปแบบการโจมตี และแนวทางการป้องกันที่เหมาะสมกับการปฏิบัติงานและการใช้งานในชีวิตประจำวัน
2. เพื่อยกระดับความมั่นคงปลอดภัยด้านสารสนเทศ: ของ สลน. ให้สอดคล้องกับนโยบายรัฐบาลดิจิทัล แผนปฏิบัติราชการ และแผนปฏิบัติการด้านดิจิทัลประจำปีของ สลน.
3. เพื่อสนับสนุนการพัฒนาระบบการจัดการความรู้: ของ สลน. สู่การเป็นองค์กรแห่งการเรียนรู้ (Learning Organization: LO) ผ่านการแลกเปลี่ยนความรู้และการถอดบทเรียน
4. เพื่อลดความเสี่ยงจากการใช้งานระบบดิจิทัล: ป้องกันการโจมตีทางระบบเครือข่าย การหลอกลวงทางอิเล็กทรอนิกส์ (Phishing) และการรั่วไหลของข้อมูล เพื่อให้การดำเนินงานของหน่วยงานมีความต่อเนื่องและปลอดภัย

สาระสำคัญของความรู้

1. การสร้างความตระหนักรู้ด้านภัยคุกคามไซเบอร์: ให้ความรู้เกี่ยวกับรูปแบบการโจมตีที่หน่วยงานภาครัฐมักตกเป็นเป้าหมาย เช่น การหลอกลวงทางอิเล็กทรอนิกส์ (Phishing), การโจมตีระบบเครือข่าย, และมัลแวร์เรียกค่าไถ่ (Ransomware)
2. แนวทางการป้องกันและใช้งานดิจิทัลอย่างปลอดภัย: ทักษะการคัดแยกอีเมลปลอม การตั้งรหัสผ่านที่มั่นคงปลอดภัย และการใช้มาตรการยืนยันตัวตนหลายชั้น (MFA) เพื่อป้องกันการรั่วไหลของข้อมูล
3. การปฏิบัติตามมาตรฐานและกฎหมาย: เนื้อหาที่สอดคล้องกับนโยบายรัฐบาลดิจิทัล และแผนปฏิบัติการด้านดิจิทัลของสำนักเลขาธิการนายกรัฐมนตรี เพื่อให้การปฏิบัติงานมีความต่อเนื่องและมั่นคง
4. กระบวนการแลกเปลี่ยนเรียนรู้: การใช้วิธีถอดบทเรียน (Lesson Learned) จากการปฏิบัติงานจริง เพื่อสร้างเป็นคลังความรู้ที่บุคลากรสามารถเข้าถึงและนำไปพัฒนาตนเองได้

จำนวนบุคลากรที่เข้าร่วม

70 คน

ผลการอบรม

คะแนนเฉลี่ยหลังการอบรม เพิ่มขึ้นประมาณ 30.7% เมื่อเทียบกับก่อนการอบรม

องค์ความรู้

แนวปฏิบัติที่ดีในการปฏิบัติงาน

1. การเฝ้าระวังและคัดกรองการสื่อสารอิเล็กทรอนิกส์: ตรวจสอบความถูกต้องของชื่อผู้ส่งและลิงก์แนบในอีเมลหรือข้อความทุกครั้งก่อนคลิก เพื่อป้องกันการตกเป็นเหยื่อของการหลอกลวงทางอิเล็กทรอนิกส์ (Phishing)
2. การบริหารจัดการรหัสผ่านและระบบยืนยันตัวตน: กำหนดรหัสผ่านที่มีความซับซ้อนและคาดเดายาก พร้อมทั้งใช้งานระบบยืนยันตัวตนหลายชั้น (Multi-factor Authentication) เพื่อเพิ่มระดับความปลอดภัยในการเข้าถึงระบบสารสนเทศของหน่วยงาน
3. เพื่อสนับสนุนการพัฒนาระบบการจัดการความรู้: ของ สลน. สู่การเป็นองค์กรแห่งการเรียนรู้ (Learning Organization: LO) ผ่านการแลกเปลี่ยนความรู้และการถอดบทเรียน
4. การรักษาความลับและความปลอดภัยของข้อมูล: ตระหนักถึงความสำคัญของข้อมูลดิจิทัลและอิเล็กทรอนิกส์ โดยจัดเก็บและรับส่งข้อมูลตามมาตรฐานที่กำหนดเพื่อป้องกันการรั่วไหลของข้อมูล (Data Leakage)
5. การเรียนรู้และแลกเปลี่ยนประสบการณ์อย่างสม่ำเสมอ: เข้าร่วมกิจกรรมถอดบทเรียน (Lesson Learned) จากสถานการณ์ภัยคุกคามที่เกิดขึ้นจริง เพื่อนำมาสร้างเป็นคลังความรู้และแนวทางป้องกันร่วมกันภายในองค์กร