

สรุปบทเรียนการพัฒนาความรู้

หลักสูตร

การสร้างความรู้ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ชื่อ-สกุล (ภาษาไทย) นางสาวศิริกร ณ ลำปาง ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ

สังกัด กลุ่มวิจัยและพัฒนาการจัดการดินเปรี้ยว กองวิจัยและพัฒนาการจัดการที่ดิน

วันที่อบรม 30 เมษายน 2569

วัตถุประสงค์ของหลักสูตร

เรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

สรุปบทเรียน

ความหมายของความมั่นคงปลอดภัยไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง การปกป้องระบบคอมพิวเตอร์ เครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึง การโจมตี การทำลาย หรือการรั่วไหลโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อบุคคล องค์กร และประเทศชาติ โดยเฉพาะในยุคดิจิทัลที่ภาครัฐและประชาชนใช้เทคโนโลยีสารสนเทศและอินเทอร์เน็ตเป็นส่วนสำคัญในการดำเนินชีวิตและการทำงาน

การสร้างความรู้ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์จึงเป็นสิ่งจำเป็น เพื่อให้ผู้ใช้งานสามารถใช้งานเทคโนโลยีได้อย่างปลอดภัย ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และป้องกันความเสียหายที่อาจเกิดขึ้น

ความสำคัญของการสร้างความรู้ความตระหนักรู้ด้าน Cybersecurity

ภัยคุกคามทางไซเบอร์ในปัจจุบันมีความซับซ้อนและเพิ่มจำนวนมากขึ้น เช่น การหลอกลวงทางออนไลน์ การโจมตีด้วยมัลแวร์ การโจรกรรมข้อมูลส่วนบุคคล และการแฮกกระบบสารสนเทศ ซึ่งสาเหตุสำคัญส่วนหนึ่งมาจากความไม่รู้หรือความประมาทของผู้ใช้งาน

การสร้างความรู้ความตระหนักรู้ช่วยให้

- ผู้ใช้งานมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์
- ลดความเสี่ยงจากความผิดพลาดของมนุษย์ (Human Error)
- เสริมสร้างวัฒนธรรมความปลอดภัยด้านข้อมูลในองค์กร
- สนับสนุนการดำเนินงานของภาครัฐอย่างมั่นคงและน่าเชื่อถือ

ประเภทของภัยคุกคามทางไซเบอร์ที่พบบ่อย

บทเรียนได้กล่าวถึงภัยคุกคามทางไซเบอร์ที่สำคัญ ได้แก่

1. มัลแวร์ (Malware) เช่น ไวรัส โทรจัน แรนซัมแวร์ ซึ่งอาจทำลายระบบหรือเรียกค่าไถ่ข้อมูล

2. ฟิชซิง (Phishing) การหลอกลวงให้เปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน เลขบัตรประชาชน ผ่านอีเมลหรือเว็บไซต์ปลอม

3. การโจมตีทางรหัสผ่าน (Password Attack) เช่น การเดารหัสผ่าน หรือใช้รหัสผ่านที่รั่วไหลจากแหล่งอื่น

4. การรั่วไหลของข้อมูล (Data Breach) เกิดจากการป้องกันข้อมูลไม่เพียงพอ หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

แนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ใช้งาน

เพื่อป้องกันภัยคุกคามทางไซเบอร์ ผู้ใช้งานควรปฏิบัติดังนี้

- ใช้รหัสผ่านที่คาดเดายาก และไม่ใช้รหัสผ่านเดียวกันในหลายระบบ
- ไม่คลิกลิงก์หรือดาวน์โหลดไฟล์จากแหล่งที่น่าเชื่อถือ
- ระมัดระวังการเปิดเผยข้อมูลส่วนบุคคลบนสื่อออนไลน์
- อัปเดตระบบปฏิบัติการและโปรแกรมอย่างสม่ำเสมอ
- ใช้โปรแกรมป้องกันไวรัสและระบบรักษาความปลอดภัยที่เหมาะสม
- ออกจากระบบทุกครั้งเมื่อใช้งานคอมพิวเตอร์สาธารณะ

บทบาทของบุคลากรภาครัฐด้าน Cybersecurity

บุคลากรภาครัฐมีบทบาทสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ เนื่องจากต้องดูแลข้อมูลของประชาชนและข้อมูลสำคัญของประเทศ ดังนั้น บุคลากรทุกระดับต้องมีความรู้ ความเข้าใจ และปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด รวมถึงต้องมีจิตสำนึกในการใช้งานระบบดิจิทัลอย่างปลอดภัยและมีความรับผิดชอบ

ความเชื่อมโยงกับการพัฒนารัฐบาลดิจิทัล

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์เป็นพื้นฐานสำคัญของการพัฒนารัฐบาลดิจิทัล (Digital Government) หากบุคลากรและประชาชนสามารถใช้เทคโนโลยีได้อย่างปลอดภัย จะช่วยเพิ่มความเชื่อมั่นในการใช้บริการภาครัฐออนไลน์ และสนับสนุนการบริหารงานภาครัฐที่มีประสิทธิภาพ โปร่งใส และยั่งยืน

ประโยชน์ที่ได้รับต่อตนเอง

1. เสริมสร้างความรู้ความเข้าใจเกี่ยวกับหลักการและแนวปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์
2. พัฒนาทักษะการรู้เท่าทันภัยคุกคามและสามารถจำแนกรูปแบบกลโกงทางออนไลน์ในชีวิตประจำวันได้อย่างมีประสิทธิภาพ
3. เพิ่มขีดความสามารถในการปกป้องข้อมูลส่วนบุคคลตลอดจนทรัพย์สินดิจิทัลของตนเองให้พ้นจากการถูกโจรกรรม
4. ตระหนักถึงความสำคัญและผลกระทบของภัยคุกคามทางไซเบอร์ที่มีต่อตนเองและองค์กร
5. สามารถนำองค์ความรู้ไปประยุกต์ใช้ในการปฏิบัติงานและการดำเนินชีวิตได้อย่างปลอดภัยและถูกวิธีตามมาตรฐานสากล

ประโยชน์ที่ได้รับต่อหน่วยงาน

1. ยกระดับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานให้อยู่ในเกณฑ์มาตรฐานและมีความรัดกุมยิ่งขึ้น
2. ลดความเสี่ยงและโอกาสเกิดผลกระทบจากภัยคุกคามทางไซเบอร์ที่อาจสร้างความเสียหายต่อระบบปฏิบัติการหลัก
3. ปกป้องข้อมูลส่วนบุคคลและข้อมูลอันเป็นความลับของทางราชการมิให้รั่วไหลสู่ภายนอก
4. เสริมสร้างวัฒนธรรมความตระหนักรู้ด้านความปลอดภัย (Security Culture) ให้เกิดขึ้นภายในองค์กรอย่างยั่งยืน
5. สนับสนุนการขับเคลื่อนนโยบายรัฐบาลดิจิทัล โดยมีบุคลากรที่มีความพร้อมทางทักษะดิจิทัลในการปฏิบัติงานอย่างปลอดภัย
6. ประหยัดงบประมาณและทรัพยากรของหน่วยงานในการแก้ไขหรือฟื้นฟูระบบสารสนเทศหากถูกโจมตีทางไซเบอร์