แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินเลย

ด้วยข้าพเจ้า นางสาวกนกวรรณ แก้วนวล ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ สังกัด สถานีพัฒนาที่ดินเลย สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ ด้านดิจิทัล หลักสูตร การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) ระหว่างวันที่ ๔ สิงหาคม ๒๕๖๘ ถึงวันที่ ๕ สิงหาคม ๒๕๖๘ เป็นเวลารวมทั้งสิ้น ๒ วัน โดยเป็นการฝึกอบรมออนไลน์ ผ่านระบบ e - Learning ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

บัดนี้ ข้าพเจ้าได้เข้าพัฒนาความรู้ฯ หลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการพัฒนาความรู้ฯ เพื่อโปรดพิจารณา ดังนี้

๑. การพัฒนาความรู้ฯ ดังกล่าวมีวัตถุประสงค์เพื่อ

๑.๑ เพื่อเรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงาน และมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่างๆ

๑.๒ เพื่อนำความรู้เกี่ยวกับภัยคุกคามไซเบอร์และวิธีการป้องกันไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

๒. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้ฯ มีดังนี้

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) ประกอบไปด้วย ๔ หัวข้อ ดังนี้

๑. Cybersecurity คืออะไร
๒. ความรู้พื้นฐานของ Cybersecurity
๓. รูปแบบภัยคุกคามของ Cybersecurity
๔. ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

หัวข้อที่ ๑ Cybersecurity คืออะไร

Cybersecurity

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐและภาคเอกชนให้ความสำคัญในเรื่องความปลอดภัยมั่นคงทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีด้านไซเบอร์มีความหลากหลายมากขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มขึ้น

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

หัวข้อที่ ๒ ความรู้พื้นฐานของ Cybersecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (CIA Triad) ประกอบด้วย

๑. Confidentiality

๒. Integrity

๓. Availability

Confidentiality

Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิ์ในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่าง เช่น

- ข้อมูลเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานบริษัทจัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้คือพนักงานบริษัททุกคน

Integrity

Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิ์ของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability

Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่าง เช่น

- ข้อมูลธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

หัวข้อที่ ๓ รูปแบบภัยคุกคามของ Cybersecurity

Malware

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้เข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจจะแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงซอฟต์แวร์ต่างๆ ได้โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

- ไวรัส (virus)
- เวิร์ม (worms)
- โทรจัน (Trojans)

Web-based attack

Web-based attack คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการที่ใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าว จากนั้นจะนำเหยื่อไปที่ปลายทางเป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware เว็บส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

Phishing

Phishing คือ วิธีการโจมตีเหยื่อผ่านช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attacks

Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL Injection
- Path Traversal

สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

Spam

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

DDoS

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องมือโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data breach

Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูล ของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

ผลกระทบที่เกิดขึ้น

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

Insider threat

Insider threat คือ ภัยที่เกิดจากบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโพน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภานในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีป้องกัน Insider threat คือ นำหลักการ Zero Trust มาใช้ภายในองค์กร

Botnets

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware

Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน Ransomware

๑. สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
๒. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
๓. ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมาควรมีความตระหนักก่อนที่จะทำการเปิด

Cryptojacking

Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

หัวข้อที่ ๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

ความตระหนักรู้ด้าน Cybersecurity สามารถนำมาใช้ได้ในชีวิตประจำวัน ทั้งวันทำงานและวันพักผ่อน สิ่งที่สามารถเจอได้ เช่น คอมพิวเตอร์, E-mail, Website, Messaging, Conference, Cloud Storage เป็นต้น

Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗. มีการตั้ง Password ที่ดี และไม่ควรบอก Password แก่ผู้อื่น

Password

การใช้ Password ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)

๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์

๔. มีการเปลี่ยน password อย่างสม่ำเสมอ

๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

๖. ไม่ควรใช้ password ซ้ำกันในแต่ละระบบ

๗. ไม่ควรบอก password แก่ผู้อื่น

E-Mail

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด E-Mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๒. ไม่เปิดไฟล์แนบจาก E-Mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๓. ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

<u>เพิ่มเติม</u> เมื่อนำเมาส์ไปวางที่ลิงค์ของเว็บไซต์ต่างๆ ใน E-Mail มุมล่างด้านซ้ายมือจะแสดงเว็บไซต์ปลายทางให้ตรวจสอบ นอกจากนี้ยังสามารถกด Report spam ได้

Website

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ

๒. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser

๓. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้ เช่น Google Chrome แนะนำใช้โหมด incognito mode หรือ โหมดแบบไม่ระบุตัวตน, Firefox ควรใช้ Private Windows, Mozilla

๕. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ

๖. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัว ควรใช้งาน Browser ในโหมด Safe Web Browser

๗. ควรติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ

Messaging

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรทำการบันทึก Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างไว้บนเครื่อง

๓. มีความตระหนักก่อนเปิด Link หรือไฟล์ต่างๆที่ได้รับมา

๔. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

<u>เพิ่มเติม</u>ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

Fake News

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อสามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น Line, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากขึ้น

วิธีสังเกตุข่าวปลอม

๑. มีการพาดหัวข่าว หรือข้อความเกินจริง เพื่อสร้างความน่าสนใจ

๒. ระบุที่มาของข่าวไม่ได้

๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔. สำนวนการเขียนออกแนวการโฆษณา

Conference

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ใช้สถานที่เหมาะสมกับการ Conference

๒. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓. แชร์เอกสารต่างๆ อย่างระมัดระวัง

๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

<u>เพิ่มเติม</u> ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

Cloud Storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. แยก User ในการใช้งานแต่ละบุคคล

๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

๔. ควรติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๖. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗. มีการใช้ password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

Free WIFI

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรใช้งาน WIFI ที่เปิดใช้บริการแบบไม่มีรหัสผ่าน

๒. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

Mobile

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์

๒. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา

๓. กำหนด Application permission ให้เหมาะสม

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

Internet Connection

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน

๒. เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ

๓. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

IoT Devices

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพื่อใช้ในการทำงานร่วมกับระบบต่างๆ หรือแอปพลิเคชันต่างๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อต่อกับเครือข่ายได้มันจำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับคอมพิวเตอร์ขนาดจิ๋ว

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์นั้นควรจะถ่วงน้ำหนักระหว่างความปลอดภัยกับความสะดวกสบาย หากสะดวกสบายมากเกินไปความปลอดภัยจะลดลง ถ้าลดความสะดวกสบายลงความปลอดภัยจะเพิ่มมากขึ้น

๓.ประโยชน์ที่ได้รับจากการพัฒนาความรู้ฯ ต่อตนเอง ได้แก่

๓.๑ ได้เข้าใจเกี่ยวกับหลักปฏิบัติเพื่อความมั่นคงทางไซเบอร์

๓.๒ ได้ความรู้เรื่องรูปแบบภัยคุกคามต่างๆ รวมทั้งวิธีป้องกันและแก้ไขเมื่อเจอภัยคุกคามแต่ละรูปแบบ

๓.๓ เพิ่มการตระหนักรู้ด้าน Cybersecurity ในการทำงานและชีวิตประจำวัน

๔. แนวทางในการนำความรู้ ทักษะที่ได้จากการพัฒนาความรู้ฯ ครั้งนี้ไปปรับให้เกิดประโยชน์แก่หน่วยงาน มีดังนี้

๔.๑ นำหลักปฏิบัติเพื่อความมั่นคงทางไซเบอร์ และการตระหนักรู้ด้าน Cybersecurity มาปรับใช้กับหน่วยงานเพื่อความมั่นคงปลอดภัยเพิ่มขึ้น

๔.๒ นำความรู้เรื่องรูปแบบภัยคุกคามต่างๆ วิธีการสังเกตุ ป้องกัน และแก้ไข มาใช้กับหน่วยงานเพื่อลดการเกิดภัยคุกคามทางไซเบอร์ และเมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้นสามารถรับมือได้อย่างเท่าทันและเหมาะสม

๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้ไปปรับใช้ในการปฏิบัติงาน

ตัวผู้เข้ารับการพัฒนาความรู้เองยังขาดความชำนาญในการใช้งานเครื่องมือทางเทคโนโลยีบางชนิด ซึ่งส่งผลต่อความปลอดภัยทางไซเบอร์

๖. ความต้องการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้ และทักษะที่ได้ไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล ได้แก่

อยากให้ผู้บังคับบัญชาสนันสนุนให้มีการอบรมเพิ่มเติมแก่บุคลากรในที่ทำงานเพื่อให้เข้าใจถึงภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ และตระหนักถึงความปลอดภัยทางไซเบอร์

จึงเรียนมาเพื่อโปรดพิจารณา

กนกวรรณ แก้วนวล

(นางสาวกนกวรรณ แก้วนวล)
นักวิชาการเกษตรปฏิบัติการ
ผู้เข้ารับการพัฒนาความรู้