แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๒/๒๕๖๗ ตั้งแต่วันที่ ๑ เมษายน ๒๕๖๗ – ๓๐ กันยายน ๒๕๖๗
ประจำปีงบประมาณ พ.ศ.๒๕๖๗

ชื่อ-นามสกุล นางสาวเนตรณพิศ นาคอ่วมค้า **ตำแหน่ง** นักวิชาการเกษตรปฏิบัติการ
หน่วยงาน กลุ่ม/ฝ่าย/สพด./ศูนย์ฯ สถานีพัฒนาที่ดินชลบุรี สำนักงานพัฒนาที่ดินเขต ๒ กรมพัฒนาที่ดิน
หัวข้อการพัฒนา การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness)
สถานที่ อบรมผ่านสื่อการเรียนการสอน TDGA E-Learning สถานีพัฒนาที่ดินชลบุรี
วันที่พัฒนา ๒๐ สิงหาคม ๒๕๖๗ **วิทยากร/ผู้ให้ความรู้** สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
หน่วยงานที่จัดอบรม สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วัตถุประสงค์
๑.เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒.เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข
๓.เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

สรุปสาระสำคัญ
๑.Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

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

๒.ความรู้พื้นฐานของ Cybersecurity
C : Confdentialty หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

✦ ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น

✦ เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

I : Integity หรือ การรักษาความถูกต้องของข้อมูลมูล การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

✦ ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร

✦ ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

A : Avallablity หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๓.รูปแบบภัยคุกคามของ Cybersecurity

- **Malware** คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึงไวรัส(Virus) เวิร์ม(Worms) และโทรจัน(Trojans)

- **Web-based attacks** คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ทำการวางMalware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

- **Phishing** คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Socialโดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

- **Web application attacks** คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ CMS, Web Server หรือ Database Server วิธีการโจมตีที่นิยมใช้ Cross-Site Scripting, SQL Injection, Path Traversal สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

- **Spam** คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

- **DDoS** คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

- **Data breach** คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชันหรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้ใจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

- **Insider threat** คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัทหรือสมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง วิธีการป้องกัน นำหลักการ Zero Trust มาใช้งานภายในองค์กร

- **Botnets** หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการ

บางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

- **Ransomware** คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสให้ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานให้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของร้องของผ่าน ที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง วิธีการป้องกัน สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล, ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ และก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

- **Cryptojacking** คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cyptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hackec

๔.ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

คอมพิวเตอร์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ควรมีการแยก User ใช้งานกันของแต่ละบุคคล, ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์, ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ, มีการ Update Patch ระบบบปฏิบัติการ (OS) อย่างสม่ำเสมอ, มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ, ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ, ไม่ควรบอก Password แก่ผู้อื่น การใช้ Password ควรมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (๑ @ ๕ #) มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่ายและไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน, ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน, ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค และเรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ, ไม่ควรทำการบันทึก Password ต่างๆ บน Browser, เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น, ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น, ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ไม่ควรบันทึก Password ไว้ที่โปรแกรม, กรณีไม่ใช้เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง, มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา, มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประประเหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปรอมที่นำนานานแพร่นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น Facebook ทำให้มีการ

กระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น วิธีการสังเกตข่าวปลอม มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ ระบุที่มาของข่าวไม่ได้ มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์ สำนวนการเขียนออกแนวการโฆษณา

Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ใช้สถานที่เหมาะสมกับการ Conference ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง แชร์เอกสารต่างๆ อย่างระมัดระวัง ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน มีการ Update Version ของโปรแกรม Conference ควรมีการขออนุญาตผู้เข้าร่วมประชุม conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย แยก User ในการใช้งานของแต่ละบุคคล ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

Free WIFI สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

Mobile สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์ ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา กำหนด Application permission ให้เหมาะสม มีการ Update Patch ระบบปฏิบัติการ (OS) Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่างๆ หรือแอปพลิเคชันต่างๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๑. มีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน

๒. มีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข

๓. สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

(ลงนาม).....เนตรณพิศ นาคอ่วมค้า.....

(นางสาวเนตรณพิศ นาคอ่วมค้า)

ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ

(ลงนาม).....

(นางจุฬาลักษณ์ แก้วอ่อน)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินชลบุรี