บันทึกข้อความ

ส่วนราชการ กลุ่มวิเคราะห์สภาพการใช้ที่ดิน กองนโยบายและแผนการใช้ที่ดิน โทร. ๒๒๐๓

ที่ กษ ๐๘๓๗.๐๒/๑๕๔ **วันที่** ๖ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอส่งสรุปรายงานการอบรม (e-Training) ปีงบประมาณ ๒๕๖๙ ครั้งที่ ๑

เรียน ผู้อำนวยการกลุ่มวิเคราะห์สภาพการใช้ที่ดิน

ตามที่ข้าพเจ้า นางสาววาสินี ศิริโภค ได้เข้าเรียนหลักสูตรด้านดิจิทัลสำหรับบุคลากรภาครัฐ (TDGA E-learning) จำนวน ๒ เรื่อง คือ หลักสูตร ความเข้าใจและการใช้เทคโนโลยีดิจิดัล ทักษะที่จำเป็นสำหรับการปฏิบัติงานแบบออนไลน์ และหลักสูตร การสร้างความตระหนักรู้ด้านความมั่งคงทางไซเบอร์

ในการนี้ ได้ดำเนินการสรุปรายงานการอบรมหลักสูตรออนไลน์เสร็จเรียบร้อยแล้ว จำนวน ๑ เรื่อง จึงขอส่งสรุปรายงานการพัฒนาความรู้และใบประกาศนียบัตรมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ

๗ ส.ค ๖๙

(นางสาววาสินี ศิริโภค)
นักวิชาการเกษตรปฏิบัติการ

เรียน ผอ.นผ.

เพื่อโปรดทราบและลงนามในเอกสารแนบ

(นางสาวอมรรัตน์ สระเพ็ชร)
นักวิชาการเกษตรชำนาญการพิเศษ
ผู้อำนวยการกลุ่มวิเคราะห์สภาพการใช้ที่ดิน

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

ส่วนที่ 1 ข้อมูลทั่วไป

ชื่อ นางสาววาสินี นามสกุล ศิริโภค

ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ กลุ่ม/ฝ่าย กลุ่มวิเคราะห์สภาพการใช้ที่ดิน

หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้
อบรมหลักสูตรออนไลน์ "การสร้างความตระหนักรู้ด้านความมั่งคงทางไซเบอร์ "

สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ
กรมพัฒนาที่ดิน

หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ
สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)

ตั้งแต่วันที่ ๓ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙ ถึงวันที่ ๔ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙

เพื่อ ☑ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ.....

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

๒.๑ รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/ สัมมนา/พัฒนาความรู้ฯ

สรุปเนื้อหา อบรมหลักสูตรออนไลน์ " การสร้างความตระหนักรู้ด้านความมั่งคงทางไซเบอร์ "

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐและภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

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

CIA Triad หรือ CIA Model ประกอบด้วย ตัวซี (C) ตัวไอ (I) และตัวเอ (A)

C : Confidentiality หรือ การรักษาความลับของข้อมูล คือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้

I : Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบบสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง

A : Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลารักษาความต่อเนื่องในการให้บริการข้อมูล

รูปแบบภัยคุกคามของ Cybersecurity

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆเช่น E-Mail,SMS,เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attack คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขอนุญาตไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

DDos (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ ระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data Breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ แอปพลิเคชั่น หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

Inside threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร

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

Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้

Cryptocurrency คือเหรียญดิจิตอล ซึ่งเหรียญดิจิตอลจะมีการประมวลผลตลอดเวลา ซึ่งในการประมวลผลจำเป็นที่จะต้องใช้ในส่วนของ CPU หรือ GPU หรือการ์ดจอบนเครื่องคอมพิวเตอร์ทำการประมวลผล และหลังจากประมวลผลเสร็จแล้วเรียบร้อยก็จะส่งกลับไปที่ส่วนกองส่วนกลางของเหรียญนั้นๆ เพื่อที่จะได้รับค่าตอบแทน

ความตระหนักรู้ด้าน Cyber security ในชีวิตประจำวัน

Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก user ใช้งานกันของแต่ละบุคคล
๒. ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
๔. มีการอัพเดท Patch ระบบปฏิบัติการ (OS)
๕. มีการ Update Version ของโปรแกรมบนเครื่อง
๖. ไม่ควรจด password และติด password ไว้ที่หน้าจอ
๗. มีการใช้ password ที่มีความซับซ้อนและไม่ควรบอก 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
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 ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
๓. ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค
๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง social ต่างๆ
๒. ไม่ควรทำการบันทึก Password ต่างๆบน Browser
๓. เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS
๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น google chrome mozilla firefox เป็นต้น
๕. ควรมีการอัพเดทเวอร์ชั่นของ Browser อย่างสม่ำเสมอ
๖. ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing
๗. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรบันทึก password ไว้ที่โปรแกรม
๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
๓. มีความตระหนักก่อนเปิดลิงค์หรือไฟล์ต่างๆที่ได้รับมา
๔. มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ

Fake News

ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวปลอมที่นำมาเผยแพร่ดูมีความน่าเชื่อถือจึงทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ

Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. แยก User ในการใช้งานของแต่ละบุคคล
๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
๔. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ
5. มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ
6. มีการตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น

แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับตัวเอง

- พิจารณาข้อมูลก่อนการแชร์ข้อมูลต่อเพื่อป้องกันการแพร่กระจายข่าวสารที่ไม่เป็นความจริง คอยติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย
- ระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าไปยังเว็บไซต์ที่ไม่เหมาะสม ไม่เปิดไฟล์ที่ไม่มีการตรวจสอบแน่ชัดหรือเปิดไฟล์จากบุคคลที่ไม่รู้จัก
- ไม่ใช้รหัสผ่านเป็นรหัสชุดเดียวกันในทุกระบบ

๒.๒ประสบการณ์/ประโยชน์ที่ได้รับ /การประยุกต์ใช้กับหน่วยงาน

☑ ต่อตนเอง

- มีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์รูปแบบต่าง ๆ ปกป้องทรัพย์สิน และข้อมูลของตนเองให้ปลอดภัยไม่ให้ตกเป็นเหยื่อของมิจฉาชีพ
- สามารถนำความรู้ไปประยุกต์ใช้ในการทำงาน และชีวิตประจำวัน

และชีวิตประจำวัน

☑ ต่อหน่วยงาน / การนำมาประยุกต์ใช้กับหน่วยงาน

- สามารถใช้งานทรัพยากรสารสนเทศขององค์กรได้ถูกต้อง ปลอดภัย
- สามารถป้องกันภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

๒.๓ ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ฯ

-

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

- ควรประชาสัมพันธ์หลักสูตรที่มีประโยชน์และมีความน่าสนใจ ในด้านดิจิทัลให้บุคลากรในหน่วยงานเข้ารับการฝึกอบรมเพิ่มขึ้น

ลงชื่อ.....วาสินี ศิริโภค.....
(นางสาววาสินี ศิริโภค)
ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ
ผู้รายงาน
วันที่...๖...เดือน...กุมภาพันธ์...พ.ศ.๒๕๖๙

ส่วนที่ ๓ ความเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....
.....
.....
.....

ลงชื่อ.....
(นายนันทพล หนองหารพิทักษ์)
ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน
ตำแหน่ง.....
วันที่.....๖ ก.พ. ๒๕๖๙.....เดือน.....พ.ศ. .....

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ วาสินี ศิริโภค

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 4 กุมภาพันธ์ 2569

สำเนาถูกต้อง
วาสินี ศิริโภค

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
Date: 2026-02-04T14:00:28.378+07:00
t6065bab

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ วาสินี ศิริโภค

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

ความเข้าใจและใช้เทคโนโลยีดิจิทัล ทักษะที่จำเป็นสำหรับการปฏิบัติงานแบบออนไลน์

(Digital Literacy : Essential Skills for Working Online)

จำนวนชั่วโมงการเรียนรู้ 2:00 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 4 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

สำเนาถูกต้อง
วาสินี ศิริโภค

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
Date: 2026-02-04T11:42:58.429+07:00
bb777d6c