บันทึกข้อความ

ส่วนราชการ กลุ่มวางแผนการจัดการที่ดินในพื้นที่เสี่ยงภัยทางการเกษตร กนผ. โทร. ๑๓๒๐

ที่ กษ ๐๘๓๗.๐๖/๑๖ **วันที่** ๑๙ มกราคม ๒๕๖๖

เรื่อง ขอส่งสรุปรายงานการอบรม สัมมนา และการพัฒนาความรู้

เรียน ผู้อำนวยการกลุ่มวางแผนการจัดการที่ดินในพื้นที่เสี่ยงภัยทางการเกษตร

ตามที่ กรมพัฒนาที่ดิน ได้กำหนดตัวชี้วัดรายบุคคลด้านการพัฒนาบุคลากร รอบการประเมินที่ ๑ (๑ ตุลาคม ๒๕๖๕ – ๓๑ มีนาคม ๒๕๖๖) ระดับความสำเร็จของการพัฒนาความรู้ โดยมีการพัฒนาทักษะด้านดิจิทัล ๑ เรื่อง นั้น

ในการนี้ข้าพเจ้าได้เข้ารับการฝึกอบรม และพัฒนาความรู้ พร้อมสรุปบทเรียนการพัฒนาความรู้ จำนวน ๑ เรื่อง หลักสูตร “การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness” ผ่านสื่อสารเรียนการสอน สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล TDGA เรียบร้อยแล้ว ตามแบบฟอร์มที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ

(นายเมธาสิทธิ์ ดีพลา)
นักสำรวจดินปฏิบัติการ

เรียน ผอ.กนผ.

เพื่อโปรดพิจารณาลงนามในแบบสรุปรายงานการฝึกอบรมฯ

(นางสาวพิมพิลัย นวลละออง)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
ผู้อำนวยการกลุ่มวางแผนการจัดการที่ดิน
ในพื้นที่เสี่ยงภัยทางการเกษตร

ลงนามแล้ว
- วภก. ศก. รวบรวม

(นายเชฏฐรุจ จันทร์แปลง)
ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน
๑๙ ม.ค. ๒๕๖๖

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

****

ส่วนที่ ๑ ข้อมูลทั่วไป

ชื่อ.....นายเมธาสิทธิ์..... **นามสกุล**.....ดีพลา.....

ตำแหน่ง นักสำรวจดินปฏิบัติการ..... ..... **กลุ่ม/ฝ่าย** ...วภก. กนผ.....

หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ หลักสูตร "การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness".....

สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ) ...วภก. กนผ.....

หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ ...สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน).....

ตั้งแต่วันที่ ....๑... เดือน ตุลาคม พ.ศ. ....๒๕๖๕...

ถึงวันที่ ...๓๑. เดือน มีนาคม. พ.ศ. ...๒๕๖๖....

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

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

๒.๑ รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/ สัมมนา/พัฒนาความรู้ฯ

Cybersecurity คือ ความมั่นคงปลอดภัยทางไซเบอร์ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการ วิธีการปฏิบัติที่ถูกออกแบบไว้แล้ว เพื่อป้องกัน รับมือ การโจมตีอุปกรณ์เครือข่าย โครงสร้างพื้นฐาน ทางสารสนเทศ ระบบ หรือโปรแกรม จากบุคคลที่สามโดยไม่ได้รับอนุญาต

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงทาง Cybersecurity ประกอบด้วย CIA Triad

๑. Confidentiality การรักษาความลับของข้อมูล คือ การระบุสิทธิ์ในการเข้าถึงข้อมูล ตามแต่ละระดับชั้นที่กำหนดไว้ เช่น พนักงานบริษัทเข้าถึงข้อมูลได้แค่ระดับที่หนึ่ง ส่วนผู้จัดการเข้าถึงข้อมูลได้ถึงระดับที่สาม

๒. Integrity การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องต่อเนื่อง เช่น ข้อมูลบัญชีธนาคาร

๓. Availability หรือ ความพร้อมใช้งานของข้อมูล คือ ข้อมูลต้องสามารถเข้าถึงได้ตลอดเวลา

รูปแบบภัยคุกคามทางไซเบอร์

๑. Malware คือ ซอร์ฟแวร์หรือ Code ประเภทหนึ่ง ถูกเขียนโปรแกรมให้เข้าถึงในส่วนที่ต้องการ โดยการคลิกติดตั้งหรือแค่ดาวโหลดลงบนอุปกรณ์ ตัวโปรแกรมก็สามารถทำงานได้เลยทันที สามารถติดต่อเป็นวงกว้างได้ คล้ายเชื้อไวรัสในมนุษย์ ขึ้นอยู่กับการออกแบบโปรแกรมของผู้ไม่ประสงค์ดี

ชื่อเรียก Malware ครอบคลุมถึง

๑.๑) ไวรัส(Virus)

๑.๒) เวิร์ม(Worms)
๑.๓) โทรจัน(Trojans)

๒. Web-based attacks คือ การโจมตีเหยื่อผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ปลอม หรือ Hack เว็บไซต์ที่มีช่องโหว่ แล้วทำการเขียน Code ใหม่ลงไป เพื่อให้ Link เข้าไปสู่เว็บไซต์ที่เขียน Malware ไว้

๓. Phishing คือ การโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-mail, Sms, เว็บไซต์ เป็นต้น โดยหลอกให้คลิกหรือกรอกรหัสผ่าน แล้วนำข้อมูลต่างๆไปทำธุรกรรม

๔. Web application attacks คือ การโจมตีเว็บไซต์โดยอาศัยช่องโหว่ต่างๆ หรือเว็บไซต์ที่ขาดการ Update แล้วมีช่องโหว่ให้สามารถ Hack เข้ามาเปลี่ยนแปลงข้อมูลบางอย่างได้

๕. Spam คือ ผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่างๆ จำนวนมาก ผ่านช่องทางต่างๆ เช่น Sms, E-mail, เว็บไซต์ โดยที่ผู้รับไม่ได้อนุญาต เพื่อก่อกวนหรือสร้างความรำคาญ

๖. DDoS (Distributed Denial of Service) เป็นวิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ หรือระบบให้บริการโดยใช้เครื่องมือจำนวนมาก ยิงเข้าไปที่ระบบพร้อมกัน เพื่อให้ระบบใช้งานไม่ได้

๗. Data breach เกิดจากการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์หรือแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ เพื่อนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของข้อมูลชุดนั้นๆ

๘. Insider threat คือ หรือเรียกว่า “เกลือเป็นหนอน” เกิดจากบุคลากรภายในองค์กร อาจเกิดจากความตั้งใจหรือไม่ตั้งใจ เนื่องจากรู้ระบบภายในเป็นอย่างดี สามารถทำลายระบบได้โดยตรง ก่อให้เกิดความเสียหายอย่างร้ายแรง

๙. Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนโดยผู้ไม่ประสงค์ดี ทำการแฝงตัวและติดตั้งอยู่ในคอมพิวเตอร์หรืออุปกรณ์ต่างๆ รอรับคำสั่งจากผู้ไม่ประสงค์ดี ส่วนมากเจ้าของเครื่องจะไม่ทราบว่าโดน Botnets แฝงตัว เนื่องจากตัวโปรแกรมไม่ได้ทำงานตลอดเวลา

๑๐. Ransomware หรือ Malware ประเภทหนึ่ง มีจุดประสงค์คือการล็อคไฟล์ไม่ให้เจ้าของเครื่องใช้งานได้ เพื่อเรียกค่าไถ่ในการปลดล็อคไฟล์นั้นๆ

๑๑. Cryptojacking แฝงตัวมาจากเว็บหรือโปรแกรมที่หลีกเลี่ยงลิขสิทธิ์ ตัวโปรแกรมจะทำการขุดเหรียญ Crytocurrency โดยจะใช้ CPU และ GPU ของเป้าหมายในการทำงาน และสร้างรายได้คืนไปให้ผู้ไม่ประสงค์ดี

<u>Cybersecurity ในชีวิตประจำวัน</u> สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย
๑. ควรแยก User ของแต่ละบุคคล
๒. ควร Logout เมื่อไม่ใช้งานคอมพิวเตอร์
๓. ควรติดตั้ง Anti-Malware และ Update สม่ำเสมอ
๔. Update ระบบปฏิบัติการสม่ำเสมอ
๕. โปรแกรมต่างๆในเครื่อง ควร Update อย่างสม่ำเสมอ
๖. ไม่ควรจด Password และติด Password ไว้ที่จอ
๗. มีการใช้ Password ที่ดี และไม่ควรบอก Password แก่ผู้อื่น

การใช้ Password ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ใหญ่ ตัวเลข และอักขระพิเศษ

๒. ความยาวอย่างน้อย ๘ อักษร

๓. ควรเลี่ยงการใช้ Common password หรือ Default password หรือคาดเดาง่าย เช่น ๑๒๓๔

๔. เปลี่ยน Password อย่างสม่ำเสมอ

๕. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

๖. ไม่บอก Password แก่ผู้อื่น

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยในการใช้ E-mail

๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๒. ไม่ควรเปิดไฟล์แนบจาก E-mail ที่น่าสงสัย

๓. ไม่คลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญทางธุรกรรม ให้เช็คผ่านช่องทางอื่นๆเพิ่มเติม

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางไม่แน่ชัด

๒. ไม่บันทึก Password บน Browser

๓. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ ต้องมี SSL (เป็นรูปกุญแจ การเข้ารหัสระหว่างต้นทางและปลายทาง) และใช้งานผ่าน HTTPS เท่านั้น

๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google chrome

๕. Update Version Browser อย่างสม่ำเสมอ

๖. ในกรณีใช้งานเครื่องคอมพิวเตอร์ที่ไม่ใช่ของตนเอง ให้ใช้งาน Browser ในโหมด Safe Web Browsing

๗. ติดตั้ง Anti-Malware และ Update สม่ำเสมอ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรบันทึก Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช่คอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆไว้บนเครื่อง

๓. Update โปรแกรมอย่างสม่ำเสมอ

๔. ไม่กด Link หรือไฟล์แปลกๆ

Fake News

ปัจจุบันข่าวปลอมถูกแพร่หลายเป็นอย่างมาก สามารถทำให้เกิดความเสียหายเป็นวงกว้างได้ โดยเฉพาะข่าวที่เผยแพร่ทาง Social วิธีสังเกต Fake News มีดังนี้

๑. มีการพาดหัวเกินจริง

๒. ระบุที่มาของข่าวไม่ได้

๓. ไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔. สำนวนการเขียนออกแนวโฆษณา

Conference

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ใช้สถานที่เหมาะสมกับการ Conference

๒. ควรมีแต่ผู้ที่เกี่ยวข้องในการประชุม
๓. แชร์เอกสารต่างๆอย่างระมัดระวัง
๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
๕. มีการ Update โปรแกรมอย่างสม่ำเสมอ

Cloud Storage
๑. แยก User ในการใช้งานของแต่ละบุคคล
๒. กำหนดผู้เข้าถึงไฟล์เฉพาะผู้เกี่ยวข้อง
๓. มีการตั้ง Password ที่ดี

Free wifi
๑. ไม่ควรใช้ Wifi ที่เปิดให้ใช้งานแบบไม่มีรหัสผ่าน
๒. หลีกเลี่ยงการใช้งาน Wifi ที่ไม่รู้ที่มา

๒ ประสบการณ์/ประโยชน์ที่ได้รับ /การประยุกต์ใช้กับหน่วยงาน

☑ **ต่อตนเอง / การนำมาประยุกต์ใช้กับหน่วยงาน**

การรู้เท่ากันและป้องกันไม่ให้เกิดเรื่องร้ายแรงทางไซเบอร์นั้น ถือเป็นเรื่องที่ดีต่อตนเองและองค์กร เนื่องจากยุคนี้ เป็นยุคดิจิทัล เทคโนโลยีเข้ามามีบทบาทในการทำงานและการใช้ชีวิตประจำมากขึ้น จึงต้องเรียนรู้การป้องกัน การก่อเหตุทางโลกไซเบอร์ให้เท่าทันต่อยุคสมัยที่เปลี่ยนไป นำมาปรับใช้กับงานที่ได้รับมอบหมาย ให้มีความมั่นคงและปลอดภัย

๒.๓ ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ฯ

-

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

-

ลงชื่อ.....

(.....นายเมธาสิทธิ์ ดีพลา.....)

ตำแหน่ง.....นักสำรวจดินปฏิบัติการ.....

ผู้รายงาน

วันที่..๑๘...เดือน....มกราคม.....พ.ศ. ๒๕๖๖..

ส่วนที่ ๓ ความเห็นของผู้บังคับบัญชา

( ) ทราบ

.....

.....

.....

ลงชื่อ.....

(นายเชฎฐรุจ จันทร์แปลง)

ตำแหน่ง ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่ ๑๙ เดือน มกราคม พ.ศ. ๒๕๖๖

DGA
Digital Government Development Agency

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

เมธาสิทธิ์ ดีพลา

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์
Cybersecurity Awareness

รวมระยะเวลาทั้งสิ้น 1 : 30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 16 ม.ค. 2566

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

05a301c3
Signed by สำนักงานพัฒนารัฐบาลดิจิทัล(องค์การมหาชน) (สพร.) - Digital Government Development Agency (Public Organization) (DGA)
Date: 2023-01-16T18:03:03.836+07:00

กรมพัฒนาที่ดิน

ขอมอบประกาศนียบัตรฉบับนี้ไว้เพื่อแสดงว่า

นายเมธาสิทธิ์ ดีพลา

ได้ผ่านการฝึกอบรมการเรียนรู้ผ่านสื่อออนไลน์ ระบบ LDD e-Training

หลักสูตร **"ความรู้พื้นฐานด้านแผนที่เพื่อการพัฒนาที่ดิน"**

รุ่นที่ 1/2566 : ตุลาคม 2565 - มีนาคม 2566

(นายปราโมทย์ ยาใจ)

อธิบดีกรมพัฒนาที่ดิน