บันทึกข้อความ

ส่วนราชการ สถานีพัฒนาที่ดินนนทบุรี โทรศัพท์ ๐ ๒๕๙๕ ๐๖๒๖

ที่ กษ ๐๘๐๘.๑๖/ ๔๕ **วันที่** ๑๖ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอส่งแบบรายงานผลการพัฒนาความรู้ของข้าราชการผ่านสื่อการเรียนการสอน

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินนนทบุรี

ตามที่ กรมพัฒนาที่ดิน อนุมัติให้ข้าราชการ พนักงานราชการ ภายในหน่วยงานของกรมพัฒนาที่ดินทั้งส่วนกลาง และส่วนภูมิภาค ฝึกอบรมพัฒนาความรู้ของข้าราชการรอบที่ ๑ ปีงบประมาณ พ.ศ. ๒๕๖๙ (ตุลาคม ๒๕๖๘ – มีนาคม ๒๕๖๙) นั้น

บัดนี้ ข้าพเจ้า ได้ทำการเรียนรู้ผ่านสื่อการเรียนการสอน เรื่อง หลักการสร้างภาพข้อมูลและการออกแบบแดชบอร์ดอย่างมีประสิทธิภาพ และหลักสูตรการสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ จัดอบรมโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล เสร็จเรียบร้อยแล้ว จึงขอส่งแบบรายงานผลการพัฒนาความรู้ของข้าราชการ หลักสูตรการสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ พร้อมแนบประกาศนียบัตรที่ผ่านการเรียนทั้ง ๒ หลักสูตรมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา

(นายพัสกร ทะสานนท์)

นักวิชาการเกษตรปฏิบัติการ

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ
สถานีพัฒนาที่ดินนนทบุรี สำนักงานพัฒนาที่ดินเขต ๑
รอบการประเมินที่.....๑/๒๕๖๙.....ตั้งแต่วันที่... ๑ ตุลาคม ๒๕๖๘ – ๓๐ มีนาคม ๒๕๖๙.....
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ-นามสกุล นายพัสกร ทะสานนท์ **ตำแหน่ง** นักวิชาการเกษตรปฏิบัติการ
กลุ่ม/ฝ่าย สถานีพัฒนาที่ดินนนทบุรี สำนักงานพัฒนาที่ดินเขต ๑
หัวข้อการพัฒนา การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)
สถานที่ สถานีพัฒนาที่ดินนนทบุรี **วันที่** ๑๔ กุมภาพันธ์ ๒๕๖๙
วิทยากร/ผู้ให้ความรู้ คุณพลากร ลาภอลงกรณ์
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

คำอธิบาย

เรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

วัตถุประสงค์

๑. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข
๓. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

เนื้อหารายวิชา ประกอบด้วย ๔ ตอน ดังนี้

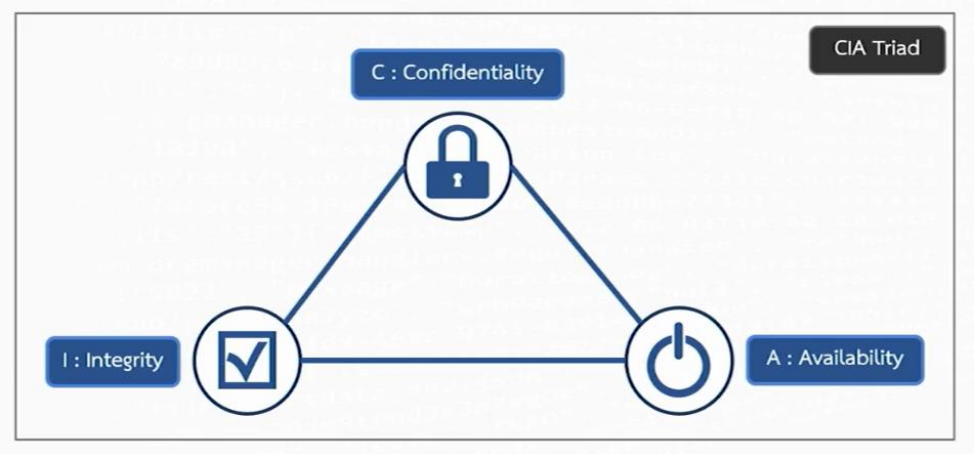
ตอนที่ ๑ Cybersecurity คืออะไร

Cybersecurity หรือ **ความมั่นคงปลอดภัยไซเบอร์** คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกัน และรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

๑. พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ ๒๕๖๒
๒. พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ ๒๕๖๐
๓. พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
๔. มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ ระบบบริหารจัดการความปลอดภัยของข้อมูล

ตอนที่ ๒ ความรู้พื้นฐานของ Cybersecurity



พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ CIA Triad หรือ CIA Model ซึ่งประกอบด้วยตัวซี(C) ตัวไอ(I) และตัวเอ(A)

Confidentiality (C) หรือ **การรักษาความลับของข้อมูล** คือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

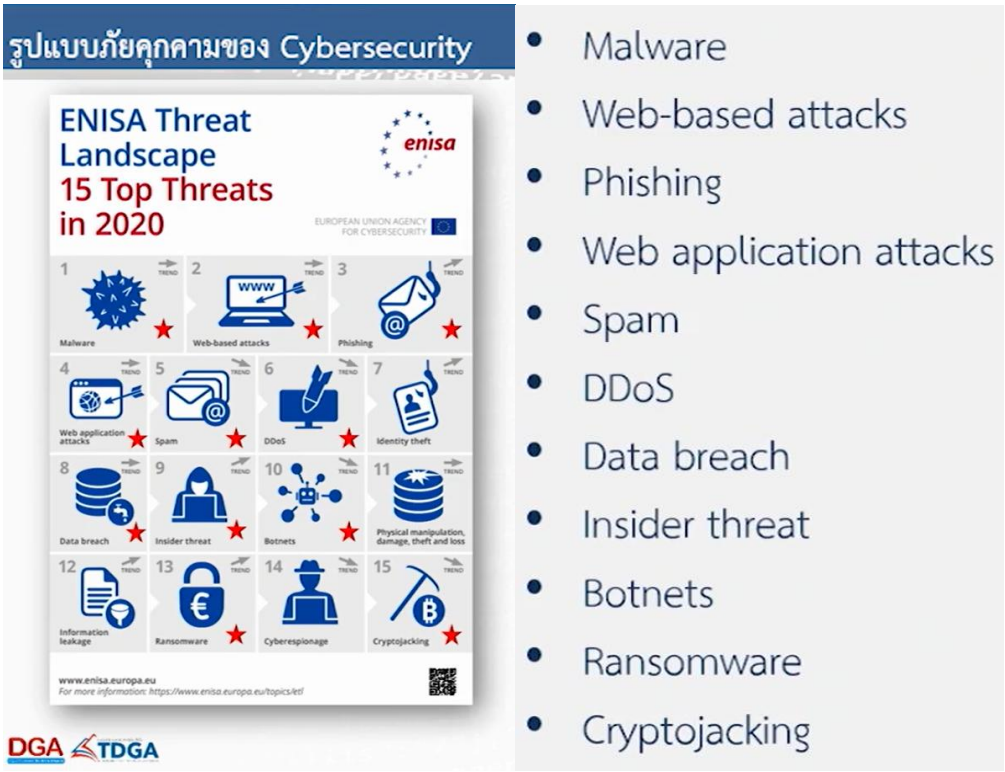
Intergrity (I) หรือ **การรักษาความถูกต้องของข้อมูล** คือ การระบุสิทธิการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability (A) หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น

- มูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

ตอนที่ ๓ รูปแบบภัยคุกคามของ Cybersecurity



ในภาพคือตัวอย่างจาก ENISA คือ องค์กรของฝั่งยุโรปที่ดูแลเรื่องภัยคุกคามทางไซเบอร์ สรุป ๑๕ ภัยคุกคามที่เกิดขึ้นในปี ๒๐๒๐

รูปแบบภัยคุกคามของ Cybersecurity

๑. Malware คือ ซอฟต์แวร์ หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอ่านแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่ายรวมถึง Server ต่างๆ ได้โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา เช่น

ไวรัส (Virus)

เวิร์ม (Worms)

โทรจัน (Trojans)

๒. Wed-based attacks คือ วิธีการโจมตีเหยื่อผ่านช่องทางเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่โค้ดเมื่อเหยื่อเข้ามาเว็บไซต์ดังกล่าว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

เพิ่มเติม : เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

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

๔. Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL injection
- Path Traversal

๕. Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูลข้อความหรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

๖. DDos คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการหรือระบบเครือข่ายโดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๗. Data breach คือ เกิดการรั่วไหลของข้อมูล ที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของ Application หรือระบบที่ทำให้บริการต่างๆโดยที่เจ้าของข้อมูลหรือผู้ให้บริการ Application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัวหรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๘. Insider Threat คือ ภัยที่เกิดจากภายในบุคลากรในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจหากช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้นซึ่งเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้องกัน นำหลักการ Zero Trust มาใช้ภายในองค์กร Zero Trust เป็นคอนเซปต์การจัดการซิเคียวริตี้สมัยใหม่ ที่หลายองค์กรได้นำมาปรับใช้ ตั้งแต่การตรวจสอบผู้เข้าระบบทุกครั้ง การให้สิทธิ์ที่น้อยที่สุดหรือเท่าที่จำเป็นกับผู้ใช้งาน

๙. Botnet หรือ **Robot Network** คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการอย่างที่ถูกโปรแกรมไว้ ส่วนมากจะแฝงตัวบเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets ที่ไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

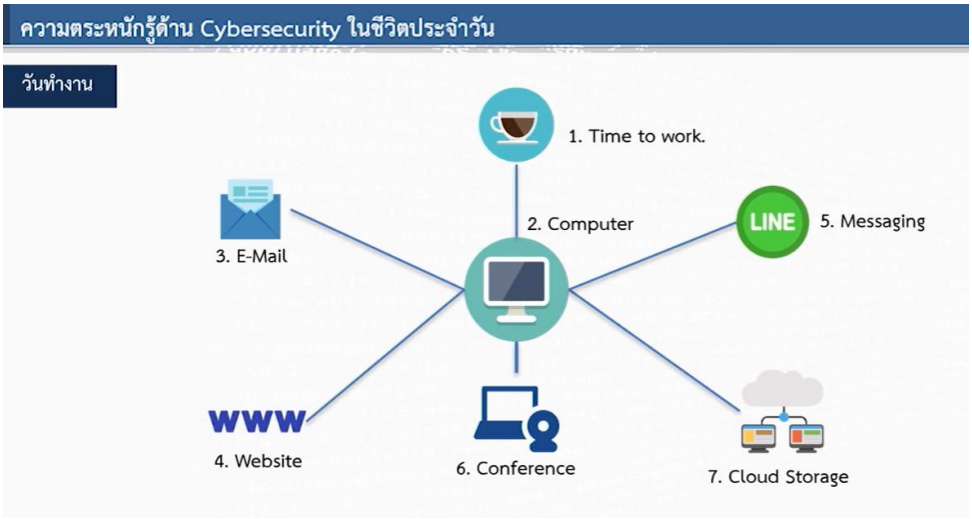
๑๐. Ransomware คือ **Walware** ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าถ่ายของรหัสผ่านที่ใช้ในการปลด ล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำโดยทำการแยกที่เก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการอัพเดทอย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมาควรมีการตระหนักก่อนที่จะทำการเปิด

๑๑. Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้ในการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อตามประเมินผลเพื่อสร้างรายได้กลับไปที่ Hacker

ตอนที่ ๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน



คอมพิวเตอร์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

๑. ควรมีการแยก User ใช้งานการของแต่ละบุคคล

๒. ควรออกจากระบบเมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร

๓. ควรติดตั้ง Anti Malware และมีการอัพเดทอย่างสม่ำเสมอ

๔. มีการอัพเดทระบบปฏิบัติการ OS อย่างสม่ำเสมอ

๕. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗. มีการใช้ Password ที่ดี และไม่บอก Password แก่ผู้อื่น

Password การใช้ Password ที่ดี คือ

๑. การใช้ Password ที่ดีคือหนึ่งมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ

๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๓. ความหลีกเลี่ยงการใช้ Common Password หรือ Default Password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น Password ๑,๒,๓,๔,๕,๖ วันเกิด และหมายเลขโทรศัพท์

๔. มีการเปลี่ยน password อย่างสม่ำเสมอ

๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

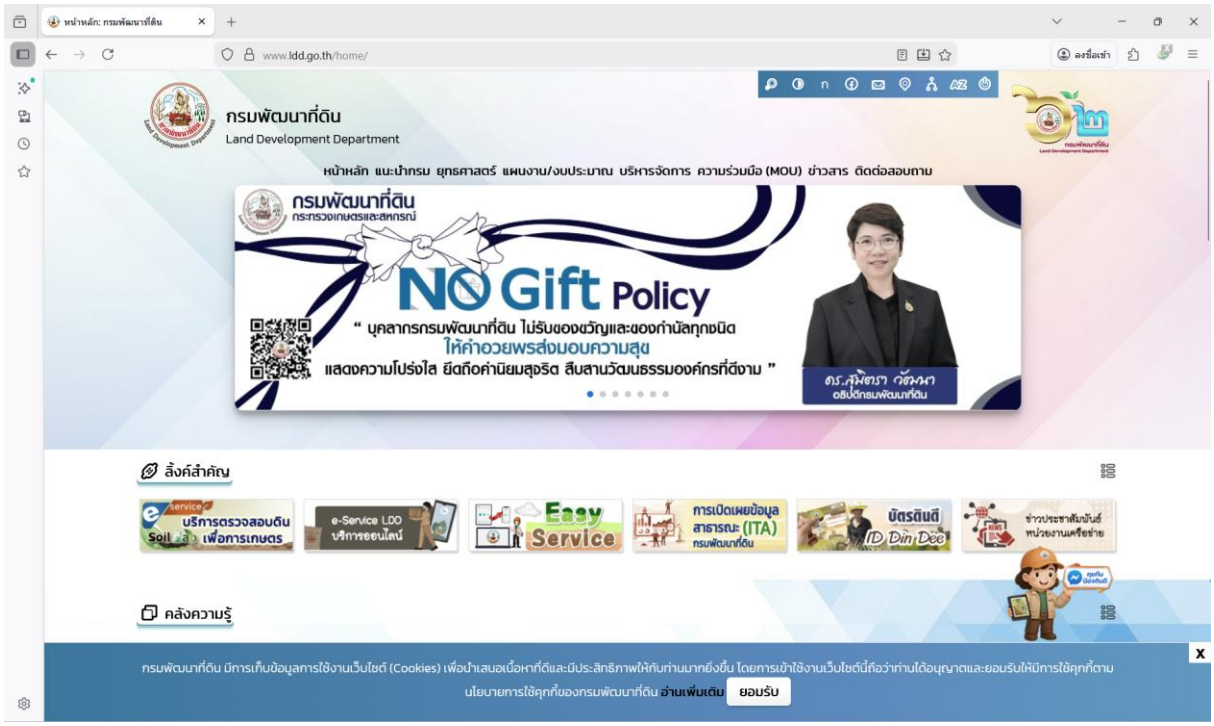
๗. ไม่ควรบอก Password แก่ผู้อื่น

E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

๑. ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
๓. ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค
๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง social ต่างๆ
๒. ไม่ควรทำการบันทึก Password ต่างๆบน Browser
๓. เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
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



ตัวอย่าง Website ของ กรมพัฒนาที่ดิน ที่มีความน่าเชื่อถือ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

๑. ไม่ควรให้ระบบจำ Password ไว้ที่โปรแกรม
๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆไว้บนเครื่อง
๓. มีความตระหนักก่อนเปิดลิงค์หรือไฟล์ต่างๆที่ได้รับมา
๔. มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ
เพิ่มเติม : ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆโดยไม่ทราบที่มาของข้อมูล

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือจึงทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ทางช่องทางออนไลน์ เช่น LINE,Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

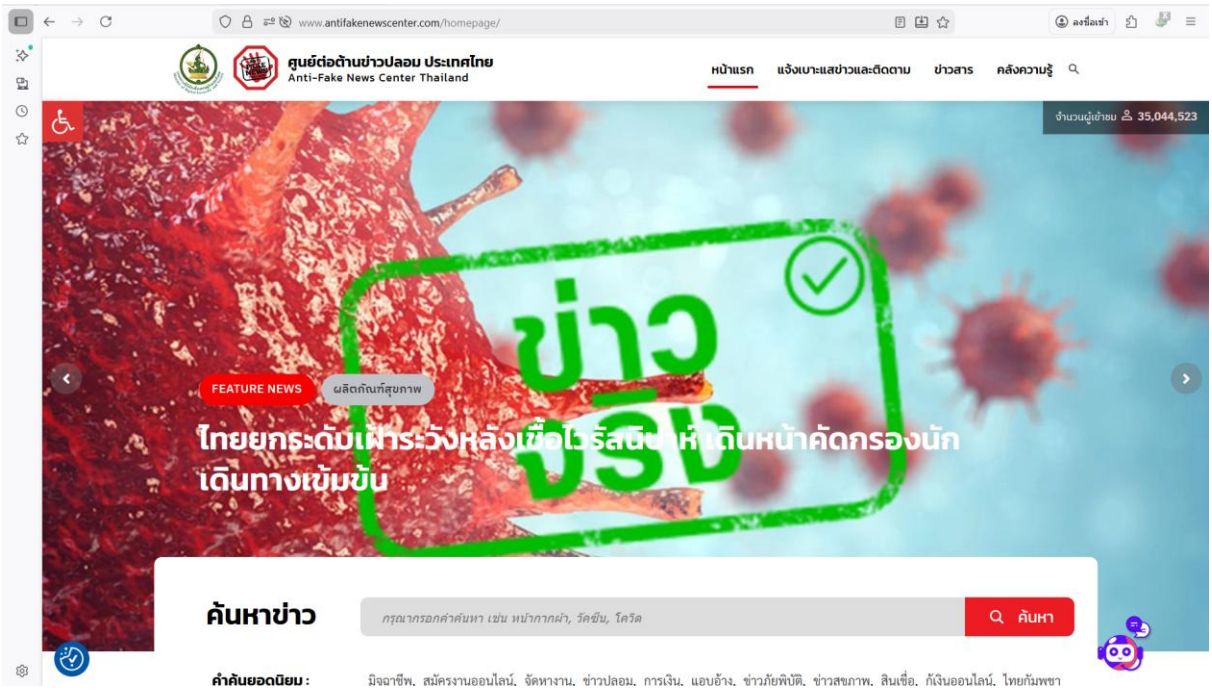
วิธีการสังเกตข่าวปลอม

๑. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ

๒. ระบุที่มาของข่าวไม่ได้

๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔. สำนวนการเขียนออกแนวการโฆษณา



ภาพ Website ศูนย์ต่อต้านข่าวปลอมแห่งประเทศไทย

Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

๑. แยก User ในการใช้งานของแต่ละบุคคล

๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

๔. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ

๕. มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ

๖. มีการตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น

ประโยชน์ที่ได้รับจากการพัฒนาความรู้ต่อตนเอง

การสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ในส่วนของความปลอดภัยกับความสะดวกสบาย ตัวอย่างในรูปจะให้เห็นว่าสิ่งที่เราต้องทำคือเราต้องพยายามถ่วงน้ำหนักให้เท่ากันในส่วนของเรื่องความปลอดภัยทางด้านไซเบอร์ซีเคียวริตี้และความสะดวกสบาย หลักสูตรนี้น่าจะสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ให้ทุกท่านได้เห็นภาพมากยิ่งขึ้นและในหลายๆ ส่วนอยากจะให้ทุกท่านนำไปปฏิบัติตามเพื่อความปลอดภัยในชีวิตประจำวัน

แนวทางในการนำความรู้ ทักษะที่ได้รับจากการพัฒนาความรู้ฯ ครั้งนี้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน มีดังนี้

๑. นำความรู้ที่ได้รับมาใช้ภายในหน่วยงาน เพื่อประโยชน์ของตนเองและองค์กร เพื่อให้หน่วยงานมีความปลอดภัยทางด้านไซเบอร์

๒. สามารถนำมาปรับพื้นฐานของตัวเอง รู้ทัน และป้องกันภัยคุกคามในรูปแบบต่างๆได้

ความเห็นของผู้บังคับบัญชา

( ) ทราบ

.....

.....

.....

(ลงนาม).....

(นายพัสกร ทะสานนท์)

ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ

(ลงนาม).....

(นายพินิจ งาเนียม)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินนนทบุรี

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ พัสกร ทะสานนท์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 14 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-14T14:48:27.779+07:00

7b60b189

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ พัสกร ทะสานนท์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

หลักการสร้างภาพข้อมูลและการออกแบบแดชบอร์ดอย่างมีประสิทธิภาพ

(The Principle of Data Visualization and Dashboard Design)

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 14 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

fbb4f046
Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-14T12:36:47.339+07:00