**แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๓**
**รอบการประเมินที่ ๑**
**ประจำปีงบประมาณ พ.ศ. ๒๕๖๙**

ชื่อ-สกุล นายพชร เสมียนรัมย์ ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ
กลุ่ม/ฝ่าย/สพด. สถานีพัฒนาที่ดินบุรีรัมย์
หัวข้อการพัฒนา การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)
สถานที่ การฝึกอบรมการเรียนรู้ผ่านสื่อออนไลน์ e-learning ของสถาบัน TDGA
วิทยากร/ผู้ให้ความรู้ คุณพลากร ลาภอลงกรณ์ ผู้จัดการส่วนบริการลูกค้า ฝ่ายปฏิบัติการ
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (Thailand Digital Government Academy)

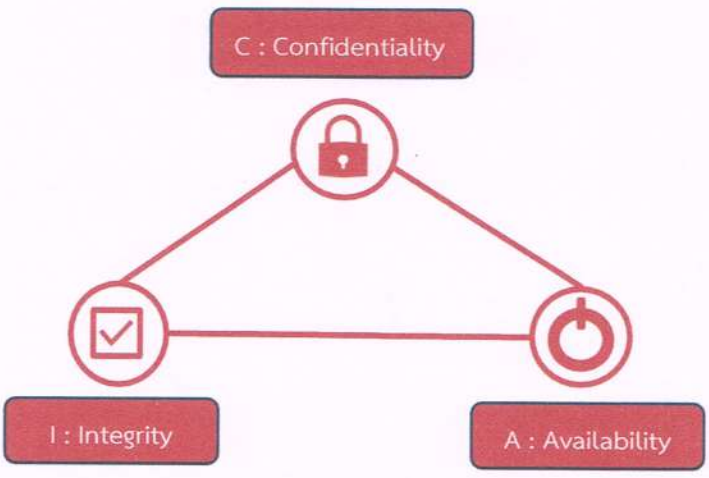
**Cybersecurity คืออะไร**

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาตในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

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

**ความรู้พื้นฐานของ Cybersecurity**



พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ มีดังนี้

**Confidentiality** หรือการรักษาความลับของข้อมูล คือ การที่ระบุสิทธิ์ในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัท

**Integrity** หรือการรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

**Availability** หรือความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

**รูปแบบภัยคุกคามของ Cybersecurity**

**Malware** คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ซึ่ง Malware นั้นครอบคลุมถึง ไวรัส (Virus) เวิร์ม (Worms) และโทรจัน (Trojans)

**Web-based attacks** คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้เว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อ เมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware โดยเว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

**Phishing** คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

**Web application attacks** คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์ เช่น CMS Web Server หรือ Database Server ซึ่งวิธีการโจมตีที่นิยมใช้ คือ Cross-Site Scripting SQL Injection, Path Traversal

**Spam** คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail SMS เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

**DDoS (Distributed Denial of Service)** คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการหรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

**Data breach** คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชันหรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเพื่อเรียกค่าไถ่ของชุดนั้น ๆ ทำให้ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปไปเผยแพร่ ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือถือขององค์กร

**Insider threat** คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรง เนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง ป้องกันโดยการนำหลักการ Zero Trust มาใช้งานภายในองค์กร

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

**Ransomware** คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน ที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง สามารถป้องกันได้โดยการสำรองข้อมูลเป็นประจำโดยทำการแยกเก็บก็บไฟล์สำรองข้อมูล ควรติดตั้ง Anti-Malware และมีการอัปเดตอย่างสม่ำเสมอ และก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

**Cryptojacking** คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacker

**ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน**

**สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ในวันทำงาน มีดังนี้**

**Computer** เน้นการสร้างสภาพแวดล้อมที่ปลอดภัยด้วยการแยกบัญชีผู้ใช้งาน (User) ของแต่ละบุคคลอย่างชัดเจน และต้อง Logout หรือล็อกหน้าจอทุกครั้ง เมื่อไม่อยู่ที่เครื่อง สิ่งสำคัญคือการติดตั้งและอัปเดต Anti-Malware รวมถึง Patch ของระบบปฏิบัติการ (OS) และโปรแกรมต่าง ๆ ให้เป็นเวอร์ชันล่าสุดเสมอเพื่อปิดช่องโหว่ทางเทคนิค

**Password** รหัสผ่านที่ดีต้องมีความยาวอย่างน้อย ๘ ตัวอักษร และมีความซับซ้อนโดยผสมตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ ๕ #) ควรหลีกเลี่ยงรหัสที่เดาง่าย เช่น วันเกิดหรือหมายเลขโทรศัพท์ ห้ามจดรหัสแปะไว้ที่หน้าจอ หรือใช้รหัสซ้ำกันในหลายระบบ ควรเปิดใช้งานการยืนยันตัวตนแบบหลายชั้น (Multi Factor Authentication) ทุกครั้งที่ทำได้ และไม่ควรบอก Password แก่ผู้อื่น

**E-mail** สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ไม่เปิด ไม่คลิก หากไม่มั่นใจ โดยหลีกเลี่ยงการเปิดอีเมล ไฟล์แนบหรือคลิกลิงก์จากผู้ส่งที่ไม่ชัดเจนหรือไม่น่าสงสัย หากต้องทำธุรกรรมสำคัญหรือมีการร้องขอข้อมูลผ่านอีเมล ควรตรวจสอบซ้ำผ่านช่องทางอื่นก่อนดำเนินการเสมอ

**Website** ควรเข้าเว็บไซต์ผ่านทางช่องทางที่น่าเชื่อถือเท่านั้น และต้องตรวจสอบว่าเว็บไซต์ที่ทำธุรกรรมสำคัญมี SSL และใช้งานผ่าน HTTPS ทุกครั้ง ไม่ควรบันทึกรหัสผ่านไว้บน Browser หากต้องใช้เครื่องคอมพิวเตอร์ที่ไม่ใช่ส่วนตัว ให้ใช้งานผ่านโหมด Safe Web Browsing เช่น Incognito ตลอดเวลา

**Messaging** ไม่ควรบันทึก Password ไว้ที่โปรแกรมกรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา มีการอัปเดตเวอร์ชันของโปรแกรมอย่างสม่ำเสมอ ไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล

**Fake News** หรือข่าวปลอม ควรระวังข่าวที่มีการพาดหัวเกินจริง ระบุที่มาไม่ได้ หรือไม่ระบุวันที่ชัดเจน โดยต้องไม่แชร์ข้อมูลใด ๆ ต่อหากยังไม่ทราบที่มาที่แน่นอน

**Conference** ควรใช้สถานที่ที่เหมาะสมและเป็นส่วนตัวในการประชุม โดยจำกัดให้มีเฉพาะผู้ที่เกี่ยวข้องเข้าร่วมเท่านั้น ระมัดระวังการแชร์เอกสารหน้าจอ และควร ขออนุญาตผู้เข้าร่วมประชุมก่อน ทุกครั้งที่จะมีการบันทึกภาพหรือเสียงในการประชุม

**Cloud Storage** ต้องมีการแยกบัญชีผู้ใช้งานและ กำหนดสิทธิ์การเข้าถึงไฟล์ เท่าที่จำเป็นเท่านั้น (Least Privilege) ควรปิดการแชร์ไฟล์ทันทีเมื่อหมดความจำเป็น และหมั่นตรวจสอบความปลอดภัยของไฟล์ด้วย Anti-Malware พร้อมทั้งตั้งรหัสผ่านที่แข็งแรงในการเข้าถึงข้อมูล

**สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ในวันพักผ่อน**

**Computer ส่วนตัว** เน้นการจัดการสิทธิ์และป้องกันการเข้าถึง ข้อมูลควรแยกบัญชีผู้ใช้งานชัดเจนเพื่อไม่ให้ปนกัน ต้อง Logout ทุกครั้ง เมื่อไม่ได้อยู่หน้าจอ และห้ามจดรหัสผ่านแปะไว้ที่ตัวเครื่อง นอกจากนี้ต้องทำให้อุปกรณ์ทันสมัยอยู่เสมอด้วยการอัปเดตทั้ง Anti-Malware, Patch ของระบบปฏิบัติการ (OS) และเวอร์ชันของโปรแกรมต่าง ๆ อย่างสม่ำเสมอ

**Free WIFI** สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ เพราะเสี่ยงต่อการถูกดักจับข้อมูลระหว่างการใช้งาน

**Mobile** ต้องตั้งค่าล็อกเครื่องเสมอไม่ว่าจะเป็น PIN, Password, Face scan หรือ Fingerprint สิ่งสำคัญคือ ห้ามติดตั้งแอปพลิเคชันที่น่าสงสัยหรือนอกเหนือจาก Store มาตรฐาน เช่น App Store/Play Store และต้องหมั่นตรวจสอบการอนุญาตเข้าถึงข้อมูลของแอป (Permission) รวมถึงอัปเดตระบบและแอปให้เป็นปัจจุบันอยู่ตลอด

**Internet Connection** เพื่อป้องกันคนนอกลักลอบใช้งานหรือเจาะระบบ ควรเปลี่ยนรหัสผ่านเริ่มต้น (Default Password) ของ Router และเปลี่ยนชื่อ SSID (ชื่อ Wi-Fi) พร้อมรหัสผ่านใหม่ทันทีหลังจากติดตั้งจากผู้ให้บริการ รวมถึงจำกัดจำนวนผู้ใช้งานเท่าที่จำเป็น

**IoT Devices** คือ อุปกรณ์อีเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือแอปพลิเคชันต่าง ๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้อง มีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

(นายพชร เสมียนรัมย์)
นักวิชาการเกษตรปฏิบัติการ

DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY

TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

# ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

## คุณ พชร เสมียนรัมย์

**ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน**

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

**จำนวนชั่วโมงการเรียนรู้** 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 11 กุมภาพันธ์ 2569

**( นางไอรดา เหลืองวิไล )**

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

2be15306

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (DGA)
Date: 2026-02-24T22:16:46.225+07:00