**แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต 2**
**รอบการประเมินที่ 2/2567 ตั้งแต่วันที่ 1 เมษายน 2567 – 30 กันยายน 2567**
**ประจำปีงบประมาณ พ.ศ. 2567**

**ชื่อ-นามสกุล** นางสาวทัชชา จันทกลม **ตำแหน่ง** นักวิชาการเกษตรปฏิบัติการ
**หน่วยงาน กลุ่ม/ฝ่าย/สพด./ศูนย์** วิชาการเพื่อการพัฒนาที่ดิน สถานีพัฒนาที่ดินจันทบุรี
**หัวข้อการพัฒนา** การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness)
**วิธีการพัฒนา** อบรมทางไกลด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ TDGA E-LEARNING
**วันที่พัฒนา** 27 สิงหาคม 2567 **สถานที่** สถานีพัฒนาที่ดินจันทบุรี
**หน่วยงานที่จัดอบรม** สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy
**สอนโดย** คุณพลากร ลาภอลงกรณ์ ผู้จัดการส่วนบริการลูกค้า ฝ่ายปฏิบัติการ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**วัตถุประสงค์**

1. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
2. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข
3. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

**สรุปสาระสำคัญ**

**การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness)**

**หัวข้อการเรียนรู้**

1. **Cybersecurity คืออะไร**
2. **ความรู้พื้นฐานของ Cybersecurity**
3. **รูปแบบภัยคุกคามของ Cybersecurity**
4. **ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน**

**Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์**

Cybersecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ คือ การใช้เทคโนโลยี เครื่องมือ และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบมาเพื่อป้องกันและรับมือกับการโจมตีที่อาจเกิดขึ้นกับอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบ หรือโปรแกรม เพื่อป้องกันความเสียหายจากการเข้าถึงโดยบุคคลที่สามโดยไม่ได้รับอนุญาต

ในปัจจุบัน หน่วยงานทั้งภาครัฐและภาคเอกชนได้เริ่มให้ความสำคัญกับความมั่นคงปลอดภัยทางไซเบอร์มากขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์ก็มีความหลากหลายมากยิ่งขึ้นและสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

**กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์**

**ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้อง:**

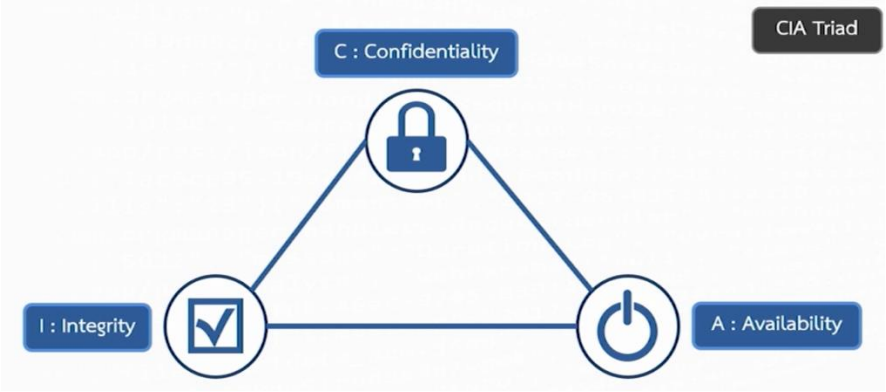
1. **พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

- กฎหมายนี้กำหนดมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมถึงการสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนในการป้องกันและรับมือกับการโจมตีทางไซเบอร์

2. **พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560**
   - กฎหมายนี้ควบคุมการกระทำผิดทางคอมพิวเตอร์ เช่น การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การทำลายข้อมูล และการกระทำผิดอื่นๆ ที่เกี่ยวข้องกับการใช้คอมพิวเตอร์
3. **พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล**
   - กฎหมายนี้มีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลของประชาชน โดยกำหนดสิทธิและหน้าที่ของเจ้าของข้อมูลและผู้ที่ใช้ข้อมูลนั้น รวมถึงการจัดการและการป้องกันข้อมูลส่วนบุคคล
4. **มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)**
   - มาตรฐานนี้เป็นแนวทางในการจัดการความปลอดภัยของข้อมูลในองค์กร โดยเน้นการประเมินความเสี่ยงและการจัดการความเสี่ยงที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล

**ความรู้พื้นฐานของ Cybersecurity**

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

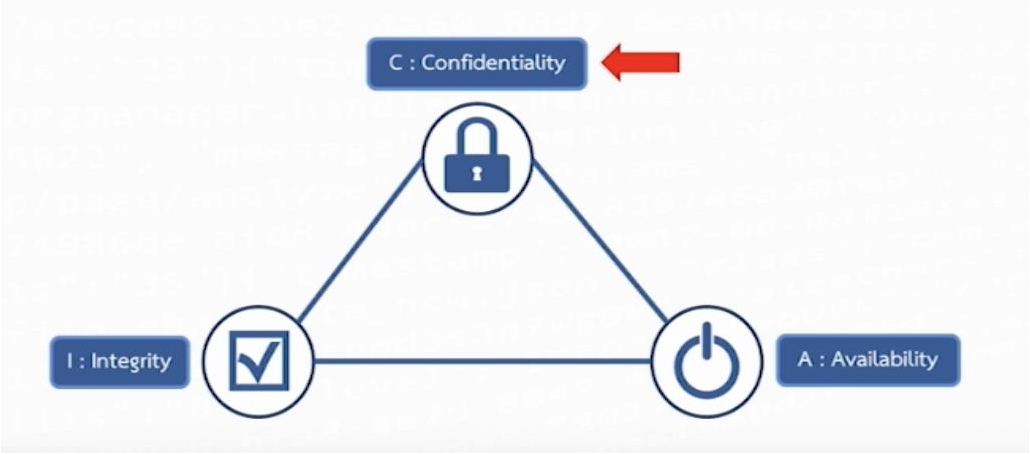



**Confidentiality หรือ การรักษาความลับของข้อมูล** คือ การกำหนดสิทธิในการเข้าถึงข้อมูลให้กับผู้ที่มีสิทธิ์เข้าถึงข้อมูลนั้นตามระดับความลับที่กำหนดไว้ สำหรับข้อมูลแต่ละประเภทจะมีความลับที่แตกต่างกันและผู้ที่มีสิทธิ์เข้าถึงข้อมูลนั้นจะต้องได้รับการอนุญาตตามความจำเป็น

**ตัวอย่างการจัดประเภทความลับของข้อมูล:**

- **ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท**
  - **ระดับความลับ**: ความลับสูงสุด
  - **ผู้ที่สามารถเข้าถึงได้**: ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- **เบอร์โทรของพนักงานในบริษัท**
  - **ระดับความลับ**: ข้อมูลภายใน

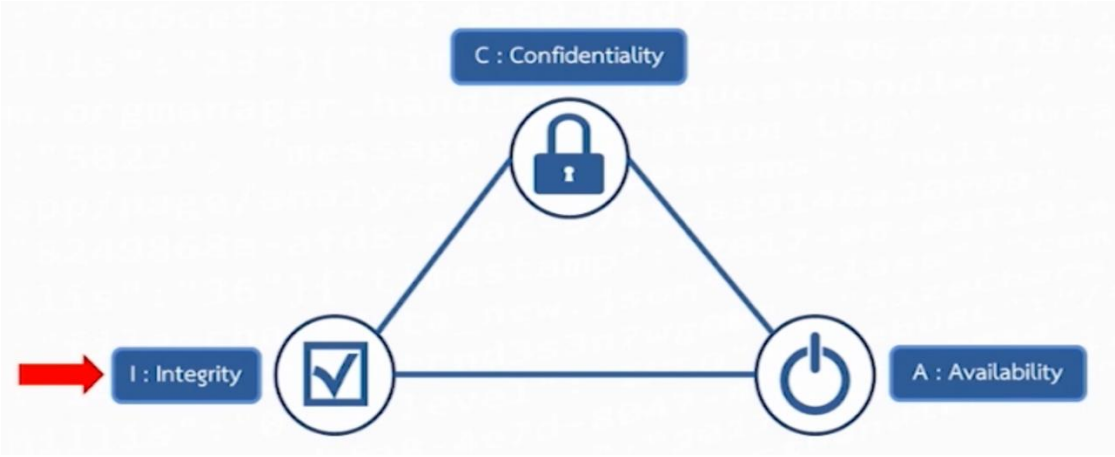
- **ผู้ที่สามารถเข้าถึงได้**: พนักงานบริษัททุกคน




**Integrity หรือ การรักษาความถูกต้องของข้อมูล** คือ การกำหนดสิทธิในการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง การรักษาความถูกต้องของข้อมูลหมายถึงการป้องกันการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตและการตรวจสอบให้แน่ใจว่าข้อมูลยังคงถูกต้องและเชื่อถือได้

**ตัวอย่างการรักษาความถูกต้องของข้อมูล:**

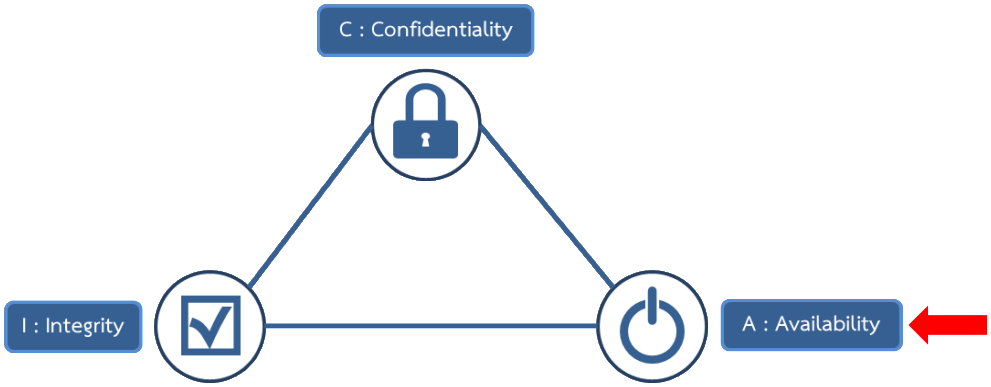
- **ข้อมูลของธนาคารด้านการเงิน**
  - **ตัวอย่าง**: ข้อมูลบัญชีธนาคาร
  - **คำอธิบาย**: ข้อมูลทางการเงินต้องได้รับการรักษาความถูกต้องเพื่อป้องกันการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตและรักษาความถูกต้องของข้อมูลบัญชี
- **ข้อมูลที่อยู่บนระบบคอมพิวเตอร์**
  - **ตัวอย่าง**: ข้อมูลที่อยู่ในฐานข้อมูลหรือไฟล์ต่าง ๆ
  - **คำอธิบาย**: ข้อมูลในระบบคอมพิวเตอร์ต้องได้รับการป้องกันจากการแก้ไขหรือการทำลายที่ไม่ได้รับอนุญาต เพื่อให้ข้อมูลยังคงมีความถูกต้องและไม่ผิดพลาด




**Availability หรือ ความพร้อมใช้งานของข้อมูล** คือ การรับประกันว่าข้อมูลจะพร้อมให้เข้าถึงและใช้งานได้ตลอดเวลา การรักษาความพร้อมใช้งานของข้อมูลหมายถึงการป้องกันไม่ให้ข้อมูลหรือระบบถูกปิดใช้งาน หรือการทำให้ข้อมูลสามารถเข้าถึงได้เมื่อจำเป็น เพื่อรักษาความต่อเนื่องในการให้บริการข้อมูล

**ตัวอย่างการรักษาความพร้อมใช้งานของข้อมูล:**

- **ข้อมูลของธนาคารด้านการเงิน**
    - **ตัวอย่าง**: ข้อมูลบัญชีธนาคาร
    - **คำอธิบาย**: ข้อมูลบัญชีธนาคารต้องสามารถเข้าถึงได้ตลอดเวลาเพื่อให้บริการลูกค้าได้อย่างต่อเนื่องและไม่ขัดข้อง
- **ข้อมูลที่อยู่บนระบบคอมพิวเตอร์**
    - **ตัวอย่าง**: ข้อมูลที่อยู่ในฐานข้อมูลหรือระบบต่าง ๆ
    - **คำอธิบาย**: ข้อมูลในระบบคอมพิวเตอร์ต้องมีความพร้อมใช้งานตลอดเวลา เพื่อให้การดำเนินงานหรือบริการที่เกี่ยวข้องกับข้อมูลนั้น ๆ ไม่หยุดชะงัก




**รูปแบบภัยคุกคามของ Cybersecurity**

**1. Malware** คือ ซอฟต์แวร์หรือโค้ดที่ถูกสร้างขึ้นเพื่อทำลายหรือเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เมื่อถูกติดตั้งหรือเปิดใช้งาน Malware สามารถเข้าถึงทรัพยากรของระบบและแชร์ข้อมูลไปยังเครื่องอื่นในเครือข่ายได้ ประเภทของ Malware รวมถึง:

- ไวรัส (Virus)
- เวิร์ม (Worms)
- โทรจัน (Trojans)

**2. Web-based attacks** คือ การโจมตีผ่านเว็บไซต์ โดยการแฮ็กเว็บไซต์ที่มีช่องโหว่และใส่โค้ดที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์นั้นจะถูกนำไปยังเว็บไซต์ที่มี Malware เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware เว็บไซต์ที่ถูกแฮ็กส่วนใหญ่เป็นเว็บไซต์ประเภท CMS (Content Management System)

**3. Phishing** คือ การหลอกลวงเพื่อขโมยข้อมูลส่วนตัว เช่น Username และ Password ผ่านช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ social media

**4. Web application attacks** คือ การโจมตีเว็บไซต์โดยใช้ช่องโหว่ เช่น:

- Code ของเว็บไซต์ (เช่น CMS)
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยม:

- Cross-Site Scripting
- SQL Injection
- Path Traversal

ศึกษาวิธีป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

**5. Spam** คือ การส่งข้อมูลหรือโฆษณาจำนวนมากไปยังผู้รับโดยไม่ได้รับอนุญาต ผ่านช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ social media เพื่อก่อกวนหรือสร้างความรำคาญ

**6. DDoS** คือ การโจมตีเว็บไซต์, ระบบบริการ หรือเครือข่าย โดยใช้เครื่องโจมตีจำนวนมากยิงพร้อมกัน เพื่อทำให้ระบบไม่สามารถใช้งานได้หรือระบบล่ม

**7. Data breach** คือ การรั่วไหลหรือขโมยข้อมูลจากเว็บไซต์, แอปพลิเคชัน หรือระบบบริการ โดยที่เจ้าของข้อมูลไม่ทราบ ผู้โจมตีอาจนำข้อมูลไปขายหรือเรียกค่าไถ่

ผลกระทบ:

- ข้อมูลส่วนตัวหรือองค์กรถูกเผยแพร่
- อาจมีการเรียกค่าไถ่ข้อมูล
- ส่งผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

**8. Insider threat** คือ ภัยที่เกิดจากบุคลากรภายในองค์กร ซึ่งอาจเกิดจากความตั้งใจหรือไม่ตั้งใจ โดยใช้ช่องทางการใช้งานปกติ เช่น คอมพิวเตอร์หรือสมาร์ทโฟนของบริษัท

วิธีการป้องกัน: นำหลักการ Zero Trust มาใช้ภายในองค์กร

**9. Botnets** คือ โปรแกรมที่ผู้ไม่ประสงค์ดีติดตั้งในคอมพิวเตอร์หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งโจมตีหรือดำเนินการบางอย่าง โดยเหยื่อมักไม่ทราบว่ามี Botnets ติดตั้งอยู่ เนื่องจากโปรแกรมจะทำงานเมื่อได้รับคำสั่งจากผู้ผลิตเท่านั้น

**10. Ransomware** คือ มัลแวร์ที่ล็อคไฟล์ในคอมพิวเตอร์โดยการเข้ารหัส ทำให้ไม่สามารถใช้งานไฟล์ได้ และเรียกค่าไถ่เพื่อปลดล็อคไฟล์

**วิธีการป้องกัน**:

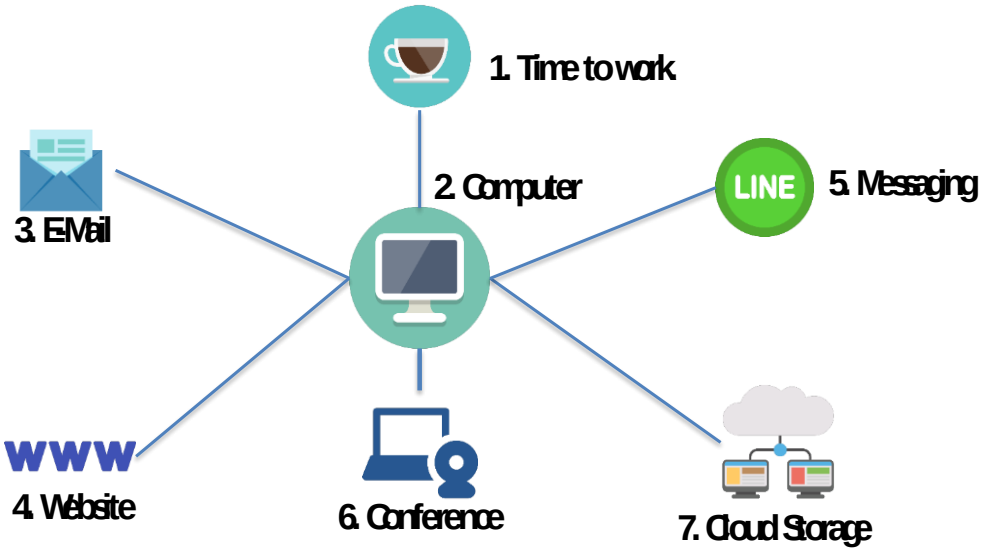
- สำรองข้อมูลเป็นประจำ
- ติดตั้งและอัปเดต Anti-Malware
- ระมัดระวังในการเปิดไฟล์ที่ได้รับมา

**11. Cryptojacking** คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

**ความตระหนักรู้ด้าน Cybersecurity**

**ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน**

**วันทำงาน**




**Computer**

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยของคอมพิวเตอร์

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti-Malware และมีการอัปเดตอย่างสม่ำเสมอ
4. มีการอัปเดต Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการอัปเดต Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดี และไม่ควรบอก Password แก่ผู้อื่น

**Password**

การใช้ Password ที่ดี คือ

1. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)
2. มีความยาวของ Password อย่างน้อย 8 ตัวอักษร
3. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์
4. มีการเปลี่ยน Password อย่างสม่ำเสมอ
5. ใช้ Multi-Factor Authentication ในกรณีที่สามารถใช้งานได้
6. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
7. ไม่ควรบอก Password แก่ผู้อื่น

**E-mail**

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
2. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
3. ไม่คลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค
4. เรื่องที่มีความสำคัญ ก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

**Website**

**สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยในการใช้งานเว็บไซต์**

1. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
2. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser
3. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
4. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
5. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
6. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัว ควรใช้งาน Browser ในโหมด Safe Web Browsing
7. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

**Messaging**

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยในการใช้งาน Messaging

1. ไม่ควรบันทึก Password ไว้ที่โปรแกรม
2. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
3. มีความตระหนักก่อนเปิด Link หรือไฟล์ต่างๆ ที่ได้รับมา
4. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

เพิ่มเติม

- ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

**Fake News**

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

1. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
2. ระบุที่มาของข่าวไม่ได้

3. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
4. สำนวนการเขียนออกแนวการโฆษณา

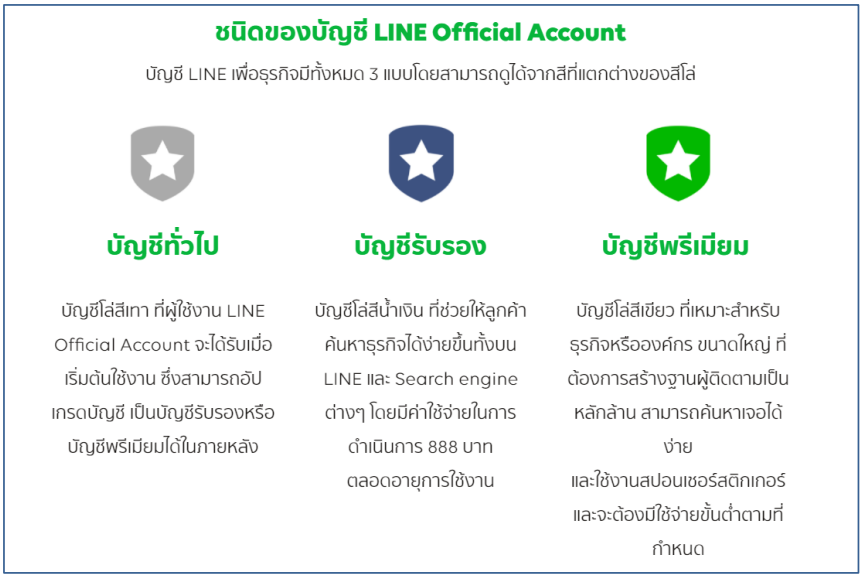




ที่มา https://www.antifakenewscenter.com

LINE Official Account

LINE Official Account คือบัญชีทางการสำหรับธุรกิจที่ช่วยให้ร้านค้าสามารถสร้างฐานผู้ติดตามอย่างไม่จำกัดจำนวน เพื่อส่งข้อมูลทางการตลาด โปรโมชั่นพิเศษ รวมถึงสื่อสารแบบรายบุคคลกับลูกค้าของคุณ






ที่มา https://lineforbusiness.com/th/service/line-oa-features

2. ไนการประชุมควรมีแต่ผู้ทีเกียวข้องเท่านัน
3. แชร์เอกสารต่างๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้
5. อัปเดตเวอร์ชันของโปรแกรม Conference อย่างสม่ำเสมอ

เพิ่มเติม:

- ควรขออนุญาตผู้เข้าร่วมประชุมก่อนที่จะบันทึกภาพและเสียงในการประชุม

## Cloud Storage

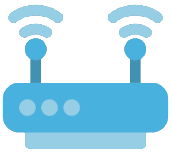
สรุปข้อควรปฏิบัติเพื่อความปลอดภัยในการใช้ Cloud Storage

1. แยกผู้ใช้งาน (User) สำหรับการใช้งานของแต่ละบุคคล
2. กำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
3. ปิดการเข้าถึงไฟล์หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
4. ติดตั้ง Anti-Malware และอัปเดตอย่างสม่ำเสมอ
5. อัปเดตเวอร์ชันของโปรแกรมอย่างสม่ำเสมอ
6. ตั้งรหัสผ่านที่ดีและไม่บอกรหัสผ่านแก่ผู้อื่น

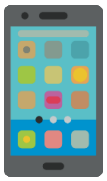
**ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน**

**วันพักผ่อน**

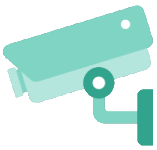
**1. Computer**



**3. Internet Connection**



**2. Mobile**



**4. IoT Devices**

## Computer

สรุปข้อควรปฏิบัติเพื่อความปลอดภัยในการใช้คอมพิวเตอร์:

1. แยกผู้ใช้งาน (User) สำหรับการใช้งานของแต่ละบุคคล
2. Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ติดตั้ง Anti-Malware และอัปเดตอย่างสม่ำเสมอ
4. อัปเดต Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. อัปเดตเวอร์ชันของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่จดรหัสผ่านและติดรหัสผ่านไว้ที่หน้าจอ
7. ใช้รหัสผ่านที่ดีและไม่บอกรหัสผ่านแก่ผู้อื่น

## Free WIFI

สรุปข้อควรปฏิบัติเพื่อความปลอดภัยในการใช้ Free WIFI

1. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
2. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

**Mobile**

สรุปข้อควรปฏิบัติเพื่อความปลอดภัยในการใช้มือถือ

1. เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
2. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
3. กำหนด Application permission ให้เหมาะสม
4. อัปเดต Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. อัปเดตเวอร์ชันของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

**Internet Connection**

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัยของการเชื่อมต่ออินเทอร์เน็ต:

1. เปลี่ยนรหัสผ่านเริ่มต้นของเราเตอร์ที่มาจากโรงงาน
2. เปลี่ยน SSID และรหัสผ่านของ Wi-Fi ที่กำหนดมาจากผู้ให้บริการ
3. กำหนดผู้ที่สามารถเข้าใช้งานอินเทอร์เน็ตเท่าที่จำเป็น

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

**ประโยชน์ที่ได้รับ**

1. มีความตระหนักรู้และรับรู้ถึงภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นในปัจจุบัน
2. มีความรู้เกี่ยวกับภัยคุกคามไซเบอร์ประเภทต่างๆ และสามารถเข้าใจแนวทางการป้องกันและแก้ไขเบื้องต้นได้ สามารถนำความรู้ที่ได้รับไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน เพื่อเพิ่มความปลอดภัยในการใช้งานเทคโนโลยี

(ลงนาม).....

(นางสาวทัชชา จันทกลม)

ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ

(ลงนาม).....

(นางจันทร์จิรา ศิริสุวรรณ์)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินจันทบุรี