

## แบบรายงานผลการพัฒนาความรู้ของข้าราชการ

รอบการประเมินที่ ๑/๒๕๖๙

ตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๘ – ๓๑ มีนาคม ๒๕๖๙

ประจำปีงบประมาณ ๒๕๖๙

ชื่อ-นามสกุล : นางสาวทัศนีย์ กุณณะ ตำแหน่ง นักวิชาการเกษตรชำนาญการ

สังกัด : สถานีพัฒนาที่ดินสิงห์บุรี สำนักงานพัฒนาที่ดินเขต ๑

วิธีการพัฒนาอบรมผ่านหลักสูตรออนไลน์ (TDGA e-Learning) สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

วันที่พัฒนา ๑๗ กุมภาพันธ์ ๒๕๖๙ สถานที่ สถานีพัฒนาที่ดินสิงห์บุรี

หัวข้อการพัฒนา : การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

วิทยากร/ผู้ให้ความรู้ : คุณพลากร ลาภอลงกรณ์ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

### วัตถุประสงค์การเรียนรู้

๑. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆและแนวทางป้องกันแก้ไข
๓. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

### สรุปสาระสำคัญ

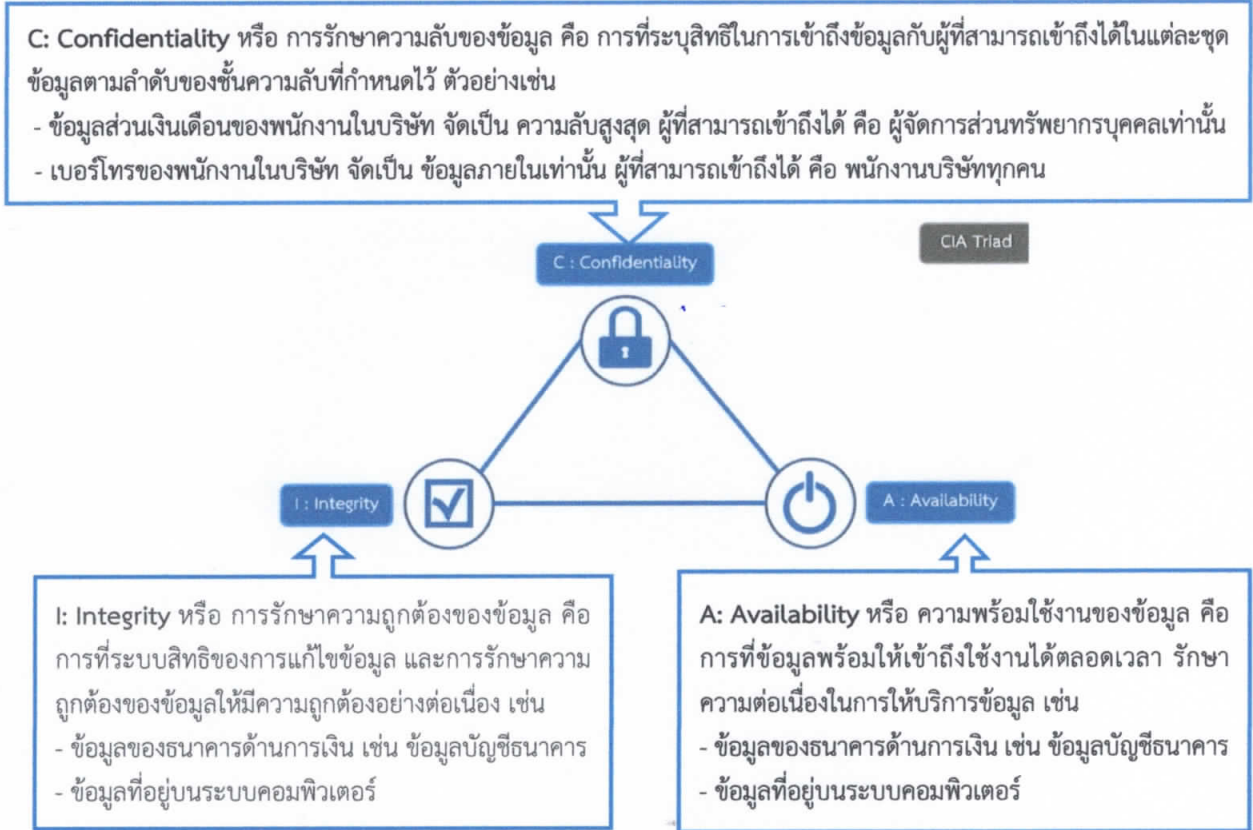
๑. Cybersecurity (ความปลอดภัยทางไซเบอร์) คือ การนำเทคโนโลยี, กระบวนการและวิธีการปฏิบัติมาใช้เพื่อ ปกป้องระบบ, เครือข่าย, อุปกรณ์และข้อมูลจากการโจมตี การเข้าถึงโดยไม่ได้รับอนุญาตหรือความเสียหายที่เกิดขึ้นทางดิจิทัล ในปัจจุบันหน่วยงานภาครัฐและภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลาย และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

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

## ๒. ความรู้พื้นฐานของ Cybersecurity พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

CIA Triad หรือ CIA Model



## ๓. รูปแบบภัยคุกคามของ Cybersecurity องค์กรของฝั่งยุโรปที่ดูแลเรื่องภัยคุกคามทางไซเบอร์ ENISA ได้สรุป ๑๕ ภัยคุกคามที่เกิดขึ้นในปี ๒๐๒๐ ดังนี้



- Malware
- Web-based attacks
- Phishing
- Web application attacks
- Spam
- DDoS
- Data breach
- Insider threat
- Botnets
- Ransomware
- Cryptojacking

ที่มา : <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-๒๐๒๐-list-of-top-๑๕-threats>

**Malware** คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ ต่างๆ โดยมีพฤติกรรมแตกต่างกันตามที่ไม่ประสงค์ที่ทำการผลิตออกมา ชื่อเรียก Malware นั้น ครอบคลุมถึง

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

**Web-based attacks** คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้ เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

**Phishing** คือ วิธีการโจมตีเหยื่อผ่านช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

**Web application attack** คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้ Cross-Site Scripting, SQL injection และ Path Traversal

สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

**Spam** คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาต ไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

**DDos (Distributed Denial of Service)** คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการหรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์ที่ทำให้เว็บไซต์, ระบบการให้บริการ ระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

**Data Breach** คือ เกิดการรั่วไหลของข้อมูลที่เกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัวหรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร.

**Inside threat** คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้น ซึ่ง Inside threat เป็นภัยประเภทที่มีความรุนแรง เนื่องจากภายในองค์กรอาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย

วิธีการป้องกัน นำหลักการ Zero Trust มาใช้ภายในองค์กร Zero Trust เป็นคอนเซ็ปต์การจัดการซีเคียวริตี้ สมัยใหม่ ที่หลายองค์กรได้นำมาใช้ ตั้งแต่การตรวจสอบผู้เข้าระบบทุกครั้ง การให้สิทธิ์ที่น้อยที่สุดหรือเท่าที่จำเป็นกับผู้ใช้งาน

**Botnets หรือ Robot Network** คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามี Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

**Ransomware** คือ Malware ประเภทหนึ่งที่ถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อกไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อกไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อกไฟล์ เพื่อให้ไฟล์ที่อยู่ในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา ควรมีความระมัดระวังก่อนที่จะทำการเปิด

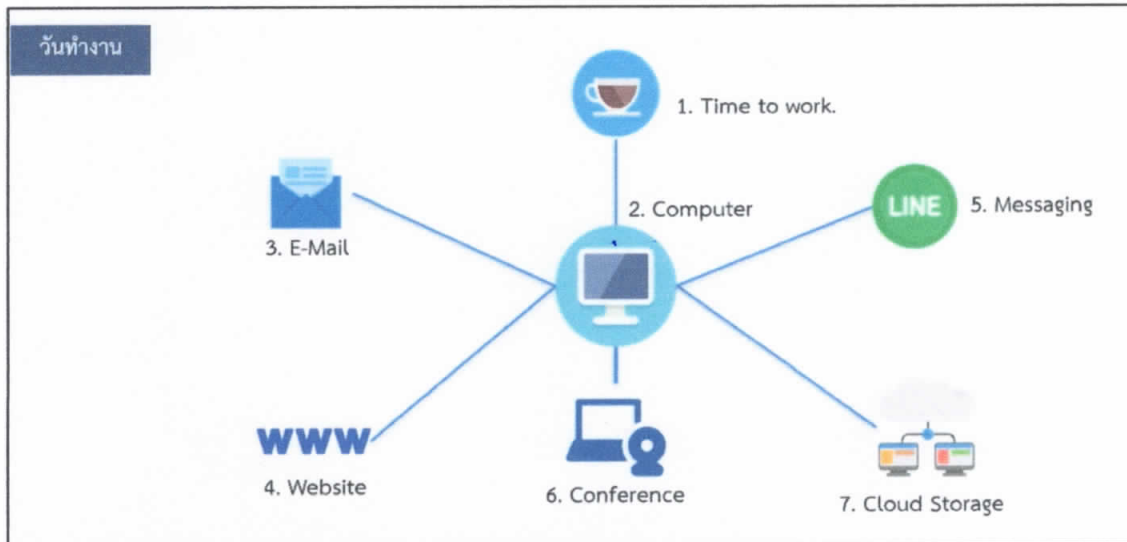
**Cryptocurrency** คือเหรียญดิจิทัล ซึ่งเหรียญดิจิทัลจะมีการประมวลผลตลอดเวลา ซึ่งในการประมวลผลจำเป็นที่จะต้องใช้ในส่วนของ CPU หรือ GPU หรือการ์ดจอบนเครื่องคอมพิวเตอร์ทำการประมวลผล หลังจากประมวลผลเสร็จแล้วเรียบร้อยแล้วก็จะส่งกลับไปเป็นส่วนกองส่วนกลางของเหรียญนั้นๆ เพื่อที่จะได้รับค่าตอบแทนในการประมวลผล

เครื่องที่ติด Cryptojacking จะเห็นว่าบางที CPU หรือ GPU เราขึ้นไปถึง ๑๐๐ เปอร์เซ็นต์โดยที่เรา ยังไม่ได้ใช้งานอะไรเลยให้ลองเช็คดูอาจจะเกิดจาก Cryptojacking



#### ๔. ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน สามารถแยกประเภทช่วงเวลา ดังนี้

๔.๑ วันทำงาน สิ่งที่เราใช้เป็นประจำต้องมีความตระหนักรู้ในการใช้และปฏิบัติเพื่อความปลอดภัย ดังรายละเอียดต่อไปนี้



#### **Computer** สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

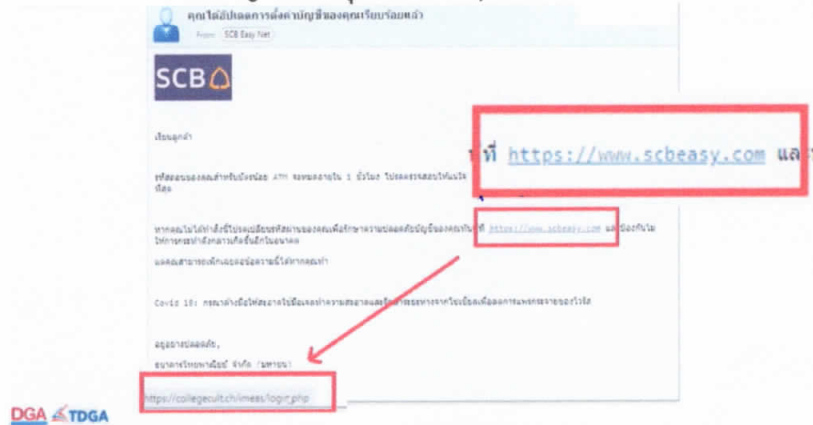
๑. ควรมีการแยก user ใช้งานกันของแต่ละบุคคล
๒. ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
๔. มีการอัปเดต Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
๖. ไม่ควรจด password และติด password ไว้ที่หน้าจอ
๗. มีการใช้ password ที่ดีและไม่ควรบอก password แก่ผู้อื่น

#### **Password** การใช้ Password ที่ดี คือ

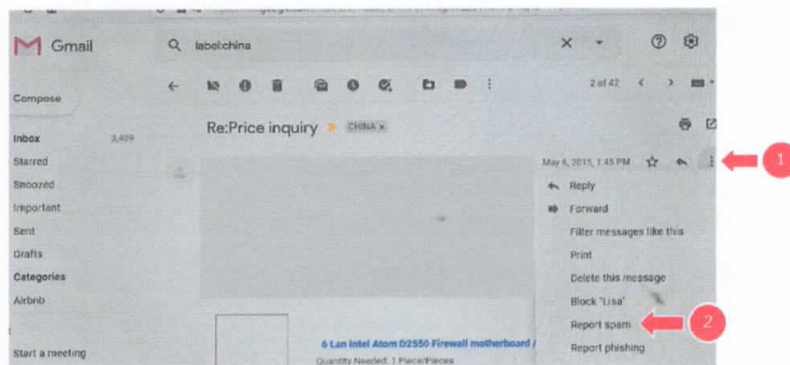
๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ
๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร
๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด และหมายเลขโทรศัพท์
๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ
๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
๗. ไม่ควรบอก Password แก่ผู้อื่น

**E-mail** สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

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



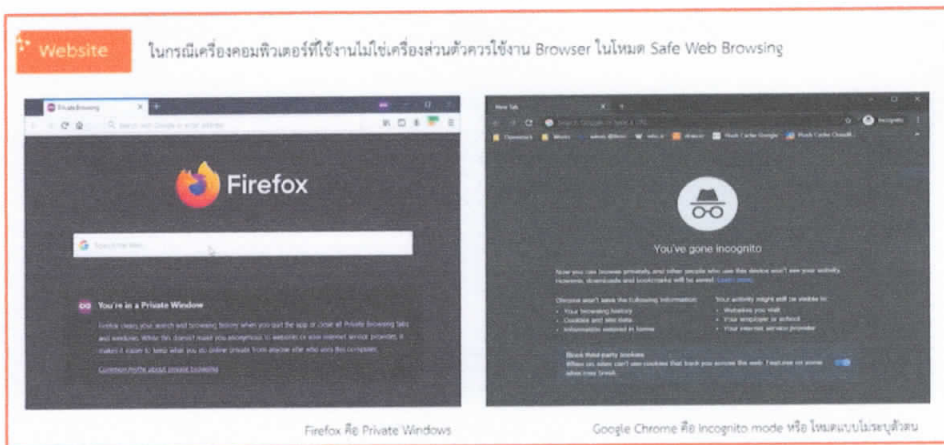
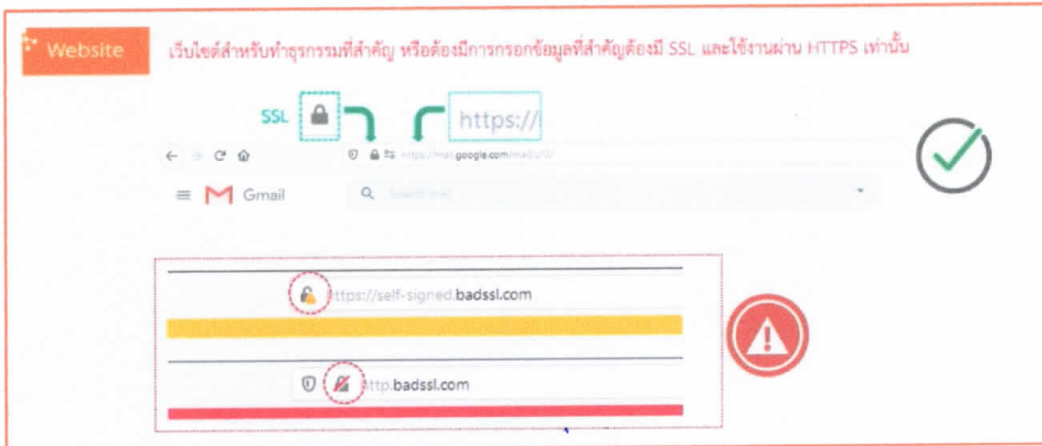
การตรวจเช็ค โดยการนำเมาส์วางที่ลิงก์ จะปรากฏเว็บไซต์ด้านล่างแล้วนำไปตรวจสอบว่าเป็นเว็บไซต์ที่ถูกต้อง



Gmail-Report Spam Mail กรณีเจอ E-mail ที่น่าสงสัย

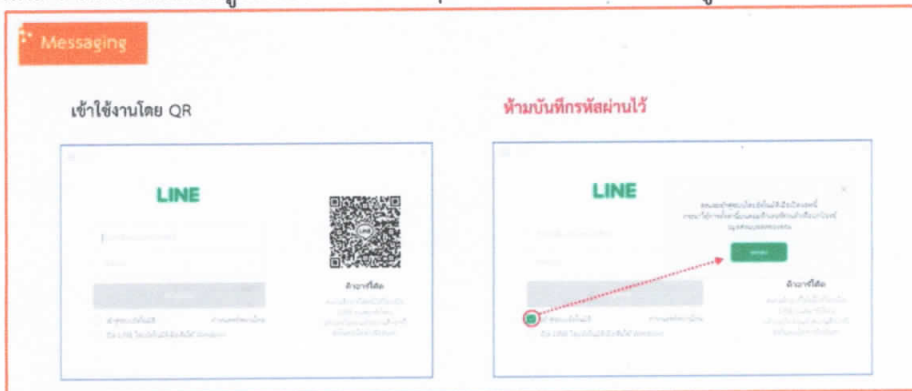
**Website** สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

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. ควรมีการอัปเดตเวอร์ชันของ Browser อย่างสม่ำเสมอ
๖. ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing
๗. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ



### Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรบันทึก password ไว้ที่โปรแกรม
  2. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
  3. มีความระหนังก่อนเปิดลิงค์หรือไฟล์ต่างๆที่ได้รับมา
  4. มีการอัปเดตเวอร์ชันของโปรแกรมอย่างสม่ำเสมอ
- เพิ่มเติม : ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆโดยไม่ทราบที่มาของข้อมูล





**Fake News** หรือ ข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวปลอม ที่นำมาเผยแพร่ นั้นมีความน่าเชื่อถือจึงทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น วิธีการสังเกตข่าวปลอม

๑. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
๒. ระบุที่มาของข่าวไม่ได้
๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
๔. สำนวนการเขียนออกแนวการโฆษณา



ที่มา: <http://www.antifakenewscenter.com>

**Line Official Account** ชนิดของบัญชี Line Official Account สามารถแบ่งได้ ดังนี้

ชนิดของบัญชี LINE Official Account		
บัญชี LINE เพื่อธุรกิจมีทั้งหมด 3 แบบโดยสามารถดูได้จากสีที่แตกต่างของโลโก้		
		
<b>บัญชีทั่วไป</b>	<b>บัญชีรับรอง</b>	<b>บัญชีพรีเมียม</b>
บัญชีโลโก้ที่ผู้ใช้งาน LINE Official Account จะได้รับเมื่อเริ่มต้นใช้งาน ซึ่งสามารถอัปเดตบัญชี เป็นบัญชีรับรองหรือบัญชีพรีเมียมได้ในภายหลัง	บัญชีโลโก้สีน้ำเงิน ที่ช่วยให้ลูกค้าค้นหาธุรกิจได้ง่ายขึ้นทั้งบน LINE และ Search engine ต่างๆ โดยมีค่าใช้จ่ายในการดำเนินการ 888 บาท ตลอดอายุการใช้งาน	บัญชีโลโก้สีเขียว ที่เหมาะสำหรับธุรกิจหรือองค์กร ขนาดใหญ่ ที่ต้องการสร้างฐานผู้ติดตามเป็นหลักล้าน สามารถค้นหาเจอได้ง่าย และใช้งานสปอนเซอร์สติกเกอร์ และจะต้องมีค่าใช้จ่ายขั้นต่ำตามที่กำหนด

ที่มา: <http://www.lineforbusiness.com/th/service/line-oa-features>

**Conference** สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

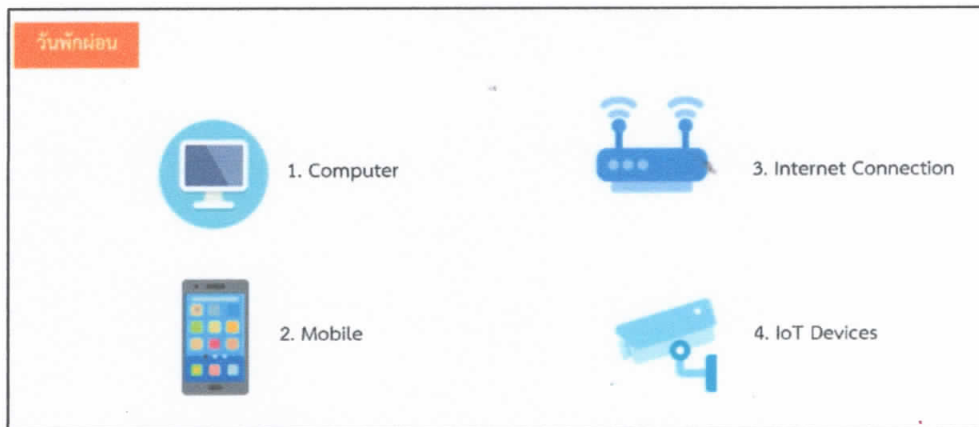
๑. ใช้สถานที่ที่เหมาะสมกับการ Conference
๒. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
๓. แชนแนลเอกสารต่างๆ อย่างระมัดระวัง
๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
๕. มีการอัปเดตเวอร์ชันของโปรแกรม Conference อย่างสม่ำเสมอ

เพิ่มเติม : ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

**Cloud Storage** สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. แยก User ในการใช้งานของแต่ละบุคคล
๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
๔. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ
๕. มีการอัปเดตเวอร์ชันของโปรแกรมอย่างสม่ำเสมอ
๖. มีการตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น

๔.๒ วันพักผ่อน สิ่งที่เราต้องมีความตระหนักรู้ในการใช้และปฏิบัติเพื่อความปลอดภัย ดังรายละเอียดต่อไปนี้



**Computer** ควรปฏิบัติเหมือนที่ใช้สำนักงานในวันทำงานเพื่อความปลอดภัย

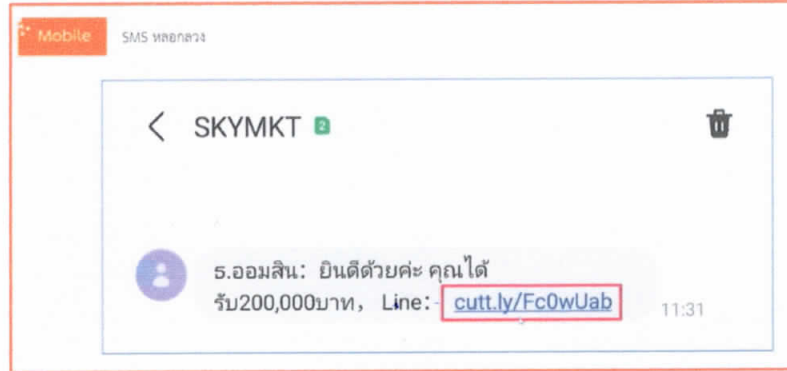
**Free WIFI** สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรใช้งาน wifi ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
๒. หลีกเลี่ยงการใช้งาน wifi ที่ไม่รู้ที่มาในการให้บริการ

**Mobile** สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปิดการใช้งาน PIN/Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
๒. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
๓. กำหนด Application permission ให้เหมาะสม

๔. มีการอัปเดต Patch ระบบปฏิบัติการ (OS) อย่างเหมาะสม
๕. มีการอัปเดตเวอร์ชันของโปรแกรมบนเครื่องอย่างสม่ำเสมอ



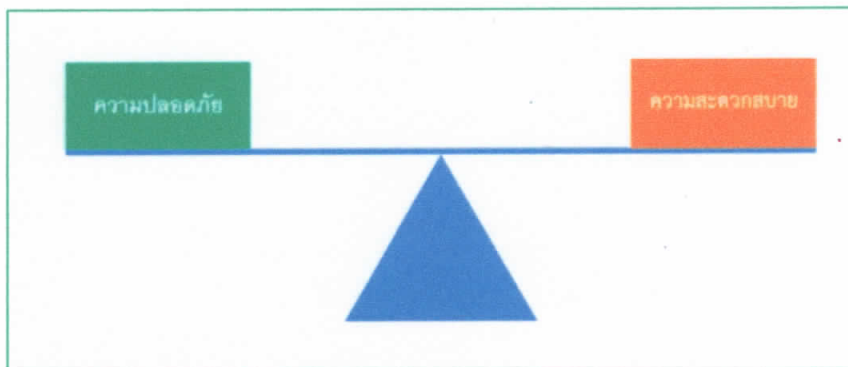
ไม่ควรคลิกลิงก์ SMS ที่ต้องสงสัย

#### Internet Connection สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
๒. เปลี่ยน SSID และรหัสผ่านของ wifi ที่กำหนดมาจากผู้ให้บริการ
๓. กำหนดผู้ที่สามารถเข้าใช้งานอินเทอร์เน็ตเท่าที่จำเป็น

**IoT Devices** คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงาน ร่วมกับระบบต่างๆ หรือ แอปพลิเคชันต่างๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย


๑. เปลี่ยน Default Password ที่มาจากโรงงาน
๒. ควรมีการอัปเดตเฟิร์มแวร์ให้เป็นเวอร์ชันล่าสุด
๓. ใช้ application ที่ใช้ในการคอนโทรลกับอุปกรณ์ต่างๆ ให้เป็นเวอร์ชันล่าสุด

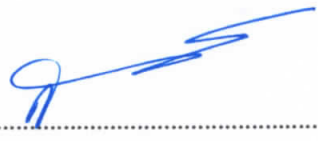


สรุป: การสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ เห็นได้ว่าเราต้องพยายามถ่วงน้ำหนักในส่วนในเรื่องความปลอดภัยและความสะดวกสบายให้เกิดความสมดุลดังภาพ เพื่อให้การใช้เทคโนโลยีและการเข้าถึงอุปกรณ์ต่างๆ ในชีวิตประจำวัน มีความปลอดภัยมากที่สุด

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๑. ได้ตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒. มีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆและแนวทางป้องกันแก้ไข
๓. สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

  
ลงนาม.....  
(นางสาวทัศนีย์ กุณณะ)  
นักวิชาการเกษตรชำนาญการ

  
ลงนาม.....  
(นางสาวกัญญาภัทร พอสม)  
ผู้อำนวยการสถานีพัฒนาที่ดินสิงห์บุรี

# ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ทศนีย์ กุณณะ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน  
การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์  
(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล  
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)  
ให้ ณ วันที่ 17 กุมภาพันธ์ 2569

( นางไอรดา เหลืองวิไล )

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

