

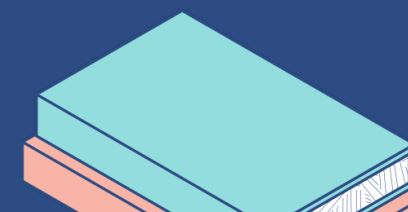
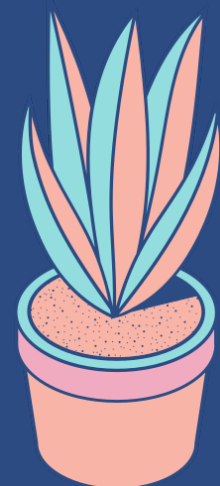


ปริญญาครุศาสตร์อุตสาหกรรม มหาบัณฑิต (ค.อ.ม.)
สาขาวิชา เทคโนโลยีคอมพิวเตอร์
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



อาจารย์ธนาวิทย์ สีหาราช

แผนกวิชาไฟฟ้า วิทยาลัยเทคนิคกาญจนาภิเษกอุดรธานี





ปริญญาครุศาสตรบัณฑิต (ค.อ.ม.)

สาขาวิชา คอมพิวเตอร์และเทคโนโลยีสารสนเทศ

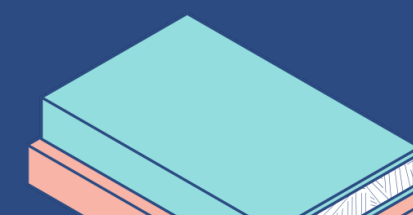
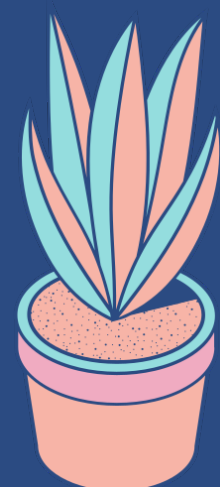
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี



อาจารย์วรัท วรรณเกษมสุข

แผนกวิชาเทคโนโลยีสารสนเทศ

วิทยาลัยเทคนิคกาญจนาภิเษกอุตรธานี



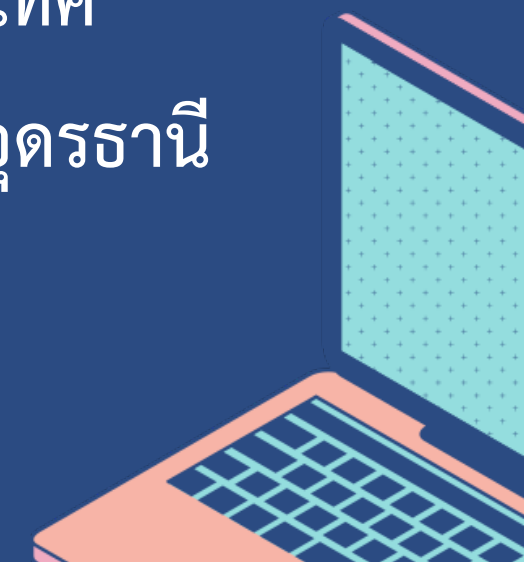
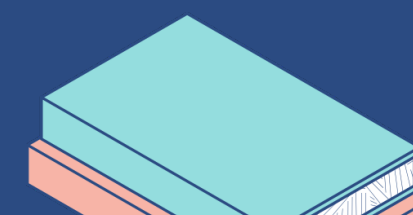
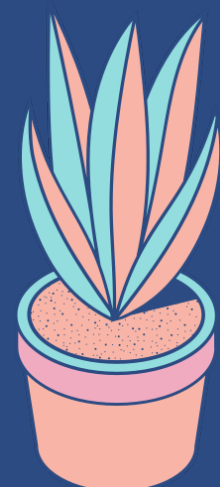


ปริญญาครุศาสตรบัณฑิต (ค.อ.ม.)
สาขาวิชา คอมพิวเตอร์และเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี



อาจารย์มานิชญ์ แก้วก่า

แผนกวิชาเทคโนโลยีสารสนเทศ
วิทยาลัยเทคนิคกาญจนาภิเษกอุดรธานี





บทที่ 4 ความมั่นคงปลอดภัยยุคดิจิทัล

หัวข้อ

- ความหมายของการรักษาความมั่นคงปลอดภัยสารสนเทศ
- องค์ประกอบด้านการรักษาความมั่นคงปลอดภัย

สารสนเทศ

- ภัยคุกคามการรักษาความมั่นคงปลอดภัยสารสนเทศ
- ความมั่นคง(SEcurity) ความเป็นส่วนตัว(PRIVACY)

และ การทิ้งรอยเท้าดิจิทัล(DIGITAL FOOTPRINT)ไว้ใน
โลกออนไลน์



บทที่ 4 ความมั่นคงปลอดภัยยุคดิจิทัล

หัวข้อ

- การพิสูจน์บุคคล (IDENTIFICATION AND AUTHENTICATION)
- การกำหนดสิทธิการเข้าถึงข้อมูล
- วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ
- การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม
- การกู้คืนข้อมูลสารสนเทศ
- ข้อปฏิบัติที่ดีในการป้องกันตนเองจากภัยคุกคาม



ความมั่นคงปลอดภัยยุคดิจิทัล



ความมั่นคง ปลอดภัย ยุคดิจิทัล

คือ การเข้าใจความรู้พื้นฐานทั่วไปของ ความ
ปลอดภัยบนโลกอินเทอร์เน็ต โดย จะมีอันตราย
ที่มาจากผู้ไม่ประสงค์ดีในโลก อินเทอร์เน็ต
เครือข่ายสังคม ออนไลน์ ได้อย่างถูกต้องและ
ปลอดภัย เพื่อ การหลีกเลี่ยงภัยคุกคาม และ
รับมือกับภัยอันตรายในโลกดิจิทัล



ความมั่นคงปลอดภัย และความเป็นส่วนตัว ทางดิจิทัล (Digital Security and Privacy)

เป็นศาสตร์ที่ว่าด้วยการสงวนรักษาไว้ซึ่งความ
ลับความครบถ้วนถูกต้องความพร้อมใช้ของ
ข้อมูลที่มีความสำคัญและการปกป้องข้อมูล
ส่วนตัวในโลกออนไลน์โดยอาศัยวิธีการตรวจ
สอบและ ประเมินความเสี่ยงของข้อมูลและ
ระบบที่สำคัญ และข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ
การใช้งานดิจิทัล



ความมั่นคงปลอดภัย
และความเป็นส่วนตัว
ทางดิจิทัล (Digital
Security and
Privacy)

แก้ไขช่องโหว่รวมถึงภัยคุกคามที่ทำให้เกิด
ความเสี่ยงต่อชีวิต ทรัพย์สินข้อมูลที่สำคัญ
ข้อมูลส่วนบุคคลระบบและอุปกรณ์ดิจิทัลของผู้
ใช้งานจากการกระทำโดยผู้ ไม่ประสงค์ดีการ
กระทำที่ผิดพลาดของผู้ใช้งานหรือภัยธรรมชาติ

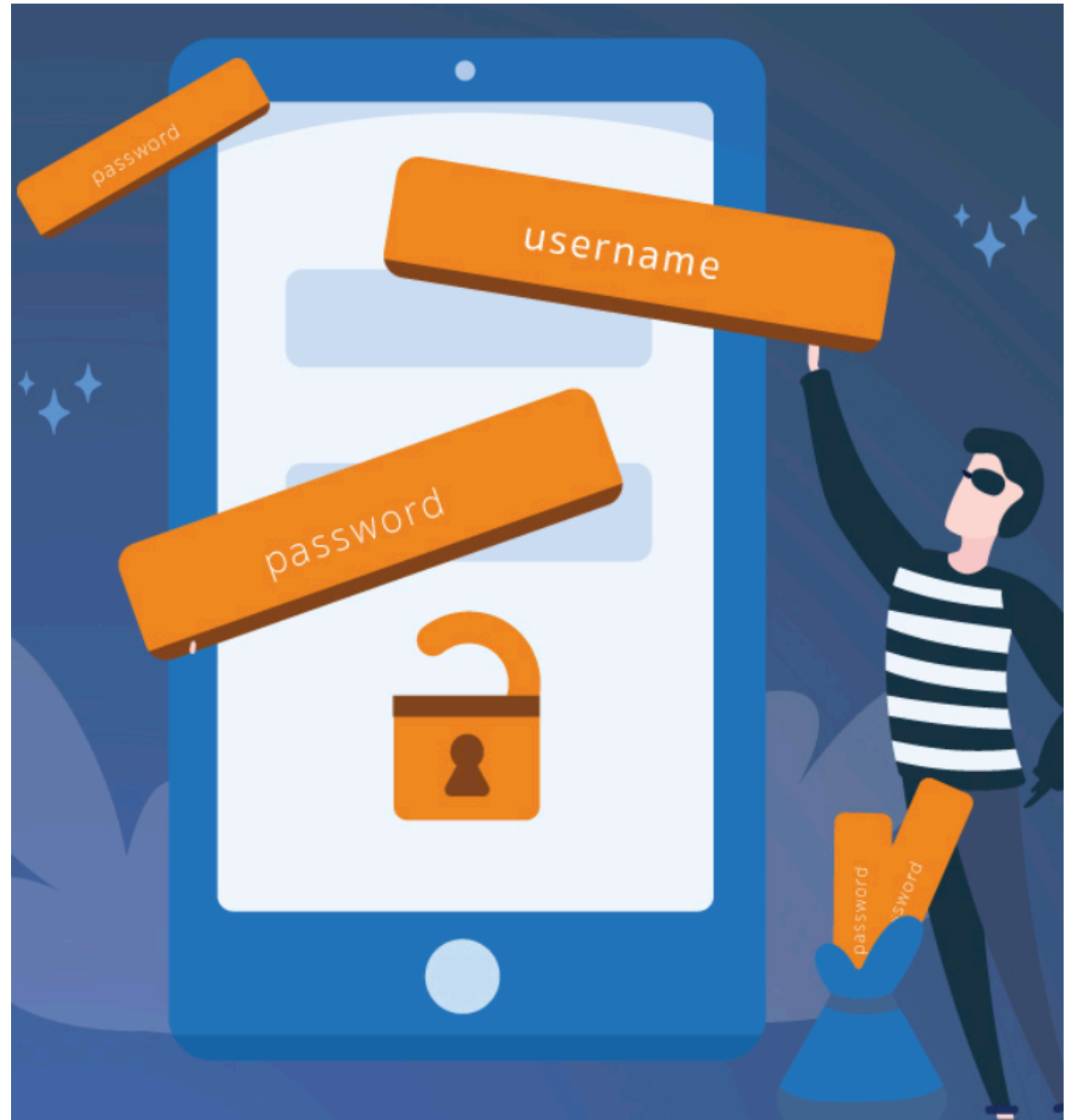


องค์ประกอบด้านการรักษาความมั่นคงปลอดภัย

สารสนเทศ



องค์ประกอบด้าน การรักษาความ มั่นคงปลอดภัย สารสนเทศ





หลักสำคัญของการ รักษาความมั่นคง ปลอดภัยสารสนเทศ

การปกป้องทรัพย์สินสารสนเทศตามสภาพ
ความเสี่ยงขององค์กร การสร้างความ
ตระหนักรู้เกี่ยวกับความจำเป็น และความ
สำคัญในการรักษาความมั่นคงปลอดภัย
สารสนเทศ

หลักสำคัญของการ รักษาความมั่นคง ปลอดภัยสารสนเทศ

การกำหนดความรับผิดชอบ และนโยบาย
สำหรับการรักษาความมั่นคงปลอดภัย
สารสนเทศ ความต่อเนื่องในการให้บริการข้อมูล
สารสนเทศ ระบบ และทรัพยากรสารสนเทศ
พร้อมทั้งประสิทธิผลของมาตรการควบคุม



การด้านการบริหารจัดการ
(Administrative security)

องค์ประกอบด้านการรักษาความมั่นคง
ปลอดภัยสารสนเทศ

มาตรการด้านเทคนิค
(Technical security)

มาตรการทางกายภาพ
(Physical security)



องค์ประกอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

1. การรักษาความลับ (Confidentiality)

ข้อมูล สารสนเทศ เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์ หรือได้รับอนุญาตเท่านั้น จะต้องไม่มีการเปิดเผยโดยมิชอบ หรือโดยบุคคลที่ไม่มีสิทธิ์ หรือไม่ได้รับอนุญาต มาตรการที่นำมาใช้ เช่น การจำแนก หรือจัดชั้นข้อมูล (Data/information classification) การตั้งค่าน์รหัสไฟล์/แฟ้มข้อมูล (Password)



องค์ประกอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

2. การรักษาความถูกต้อง ครบถ้วน (Integrity)

ข้อมูล สารสนเทศ มีความถูกต้อง จะมีการแก้ไข
เปลี่ยนแปลง ได้เฉพาะผู้ที่มีสิทธิ์หรือได้รับอนุญาต
เท่านั้น มาตรการที่นำมาใช้ เช่น การจัดการสิทธิ์
(access rights)



องค์ประกอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

3. สภาพความพร้อมใช้ (Availability)

ข้อมูล สารสนเทศ มีความพร้อมในการใช้งานอยู่เสมอ สามารถเข้าถึงได้เมื่อต้องการ เฉพาะผู้มีสิทธิ์ หรือได้รับอนุญาต มาตรการที่นำมาใช้ เช่น การควบคุมการเข้าถึง (Access control)



คุณสมบัติและองค์ประกอบอื่นที่เกี่ยวข้องด้านความมั่นคง ปลอดภัยสารสนเทศ



คุณสมบัติและองค์ประกอบอื่นที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ

ยืนยันตัวตน

ระบบขอข้อมูลของท่านในระบบเดิม กรุณา
เลือกช่องทางในการยืนยันตัวตน

เลขประจำตัว * (เลขประจำตัวประชาชน)

3210987654321

เลือกช่องทางในการยืนยันตัวตน *

☒ อีเมล xxx@gmail.com

☐ เบอร์โทรศัพท์มือถือ 092849-xxxx

ยืนยันตัวตน

หากไม่สามารถยืนยันตัวตนตามข้อมูลด้านบนได้
▶ ส่งอีเมลแจ้งเตือนให้เจ้าหน้าที่

การยืนยันความถูกต้องแท้จริง (Authenticity):

คุณลักษณะเฉพาะเพื่อยืนยัน

ความถูกต้องแท้จริงถึงตัวตนผู้ใช้งาน

คุณสมบัติและองค์ประกอบอื่นที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ



การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation): วิธีการที่ผู้ส่ง และผู้รับข้อความ จะไม่สามารถปฏิเสธการส่งหรือการรับข้อความนั้น ได้ หากได้ดำเนินการนั้นไปแล้ว

คุณสมบัติและองค์ประกอบอื่นที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ

Accountability): ความรับผิดชอบที่สามารถ
ตรวจสอบได้





ภัยคุกคามการรักษาความมั่นคงปลอดภัยสารสนเทศ

ภัยคุกคามการรักษาความมั่นคงปลอดภัยสารสนเทศ

ภัยคุกคามทางไซเบอร์ หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมีขอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยตรายที่ใกล้จะถึง

ทั้งนี้ ลักษณะของภัยคุกคามทางไซเบอร์ (อ้างอิงตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)



ภัยคุกคามการรักษาความมั่นคงปลอดภัยสารสนเทศ

ลักษณะของภัยคุกคามทางไซเบอร์ แบ่ง
ออกเป็น 3 ระดับ ดังนี้
(อ้างอิงตาม พ.ร.บ. การรักษาความ
มั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)



ภัยคุกคามการรักษาความมั่นคงปลอดภัยสารสนเทศ

ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง

ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัย
สำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของ
หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ
(CII) หรือการให้บริการของรัฐด้อยประสิทธิภาพลง



ภัยคุกคามการรักษาความมั่นคงปลอดภัยสารสนเทศ

ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญ
ของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์
หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตี
โครงสร้างพื้นฐานสำคัญของประเทศ



ภัยคุกคามการรักษาความมั่นคงปลอดภัยสารสนเทศ

ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

การโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์ หรือ โครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงาน หรือให้บริการได้



ภัยคุกคามการรักษาความมั่นคงปลอดภัยสารสนเทศ

ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ

1. เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบ

คอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้น
กว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบ
รุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ
ในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐ
หรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่
ให้กับประชาชนล้มเหลวทั้งระบบ จนไม่สามารถควบคุมการ
ทำงานส่วนกลางของระบบคอมพิวเตอร์ของได้



ภัยคุกคามการรักษาความมั่นคงปลอดภัยสารสนเทศ

ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ

2. เป็นภัยคุกคามทางไซเบอร์อันกระทบ หรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศ หรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบ หรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วน เพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย





ความมั่นคง(SEcurity) ความเป็นส่วนตัว(PriVacy)
และ การทิ้งรอยเท้าดิจิทัล(DiGital FootPrint)
ไว้ในโลกออนไลน์

ความมั่นคงปลอดภัยของข้อมูล
สารสนเทศ
Information Security

การปกป้องทรัพย์สินสารสนเทศตาม
สภาพความเสี่ยงขององค์กร การสร้าง
ความตระหนักรู้เกี่ยวกับความจำเป็น
และความสำคัญในการรักษาความมั่นคง
ปลอดภัยสารสนเทศ

ความเป็นส่วนตัว(Privacy)

ความสำคัญของความเป็นส่วนตัว

ปัจจุบันมนุษย์มีการพัฒนาและสร้างเทคโนโลยีเพื่ออำนวยความสะดวก และแก้ปัญหาที่เกิดขึ้นในชีวิตประจำวัน เทคโนโลยีที่พบมีการนำคอมพิวเตอร์มาช่วยในหลาย ๆ ด้าน โดยเฉพาะอย่างยิ่งด้านการสื่อสาร มีการเก็บข้อมูล ประมวลผลและแสดงข้อมูลบนโลกออนไลน์ ทุกคนสามารถค้นหาข้อมูลต่าง ๆ ได้ง่ายดาย บางคนเลือกใช้ข้อมูลที่ดี แต่บางคนนำข้อมูลไปใช้ในทางที่ผิดหลักคุณธรรมจริยธรรม สิ่งเหล่านี้ก่อให้เกิดความวุ่นวายหรือเกิดอาชญากรรมในสังคมได้

ความเป็นส่วนตัว (Information Privacy) เป็นสิทธิในการเป็นเจ้าของและควบคุมข้อมูลของตนเองในการเปิดเผยหรือเผยแพร่ข้อมูลใด ๆ ให้กับผู้อื่น



ความเป็นส่วนตัว (Information Privacy)

หมายถึง สิทธิที่เจ้าของสามารถที่จะ
ควบคุมข้อมูลของตนเองในการเปิดเผย
ให้กับผู้อื่น เช่น การเข้าไปดูข้อความใน
จดหมายอิเล็กทรอนิกส์ และการบันทึก
ข้อมูลในเครื่องคอมพิวเตอร์ และตัวอย่าง
พฤติกรรมที่ผิดจริยธรรม เช่น การติดตาม
ความเคลื่อนไหวของบุคคล การใช้ข้อมูล
ของลูกค้าจากแหล่งต่าง ๆ เพื่อผล
ประโยชน์ในการขยายตลาด



ความถูกต้อง (Information Accuracy)



หมายถึง ความถูกต้องของการใช้คอมพิวเตอร์เพื่อการรวบรวม จัดเก็บ และเรียกใช้ข้อมูลนั้น ในการจัดทำข้อมูลและสารสนเทศควรได้รับการ ตรวจสอบความถูกต้องก่อนที่จะนำเข้าฐานข้อมูล รวมถึงการปรับปรุง ข้อมูลให้มีความทันสมัยอยู่เสมอ

ความเป็นเจ้าของ (Information Property)

หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สิน ซึ่ง
อาจเป็นทรัพย์สินทั่วไปที่ จับต้องได้และจับต้องไม่
ได้ เช่น คอมพิวเตอร์ รถยนต์ บทเพลง โปรแกรม
คอมพิวเตอร์ แต่สามารถถ่ายทอดและบันทึกลงใน
สื่อต่าง ๆ ได้ เช่น สิ่งพิมพ์ เทป ซีดีรอม ในการคัด
ลอกผลงานนั้น ๆ จะต้องคำนึงถึงสิทธิที่ได้รับว่ามี
สิทธิในระดับใด



การเข้าถึงข้อมูล (Data Accessibility)

การเข้าใช้งานโปรแกรมหรือระบบ
คอมพิวเตอร์จะมีการกำหนดสิทธิ
ตาม ระดับของผู้ใช้งาน เพื่อเป็นการ
ป้องกันการเข้าไปดำเนินการต่าง ๆ
เป็นการรักษาความลับของข้อมูล



อะไรบ้างที่แฮกเกอร์ต้องการ
เมื่อเข้าถึงข้อมูลของเหยื่อ ?

- ชื่อผู้ใช้และรหัสผ่าน
- การเรียกดูกิจกรรม เช่น การไลก์ หรือการแชร์
- ประวัติการค้นหาของคุณ
- วันเกิด
- เลขบัตรประชาชน
- ข้อมูลบน โปรไฟล์ โซเชียลมีเดีย
- เพจที่คุณติดตามหรือ ได้ตอบ
- คำร้องออนไลน์ที่คุณเคยลงชื่อไว้
- ประวัติทางการแพทย์



การทิ้งรอยเท้าดิจิทัล(DIGITAL FOOTPRINT) ไว้ในโลกออนไลน์



ร่องรอยดิจิทัล (Digital footprint)

คือ ร่องรอยการกระทำต่าง ๆ ที่ฝังไว้และติดตามได้ เมื่อผู้ใช้งานสื่อดิจิทัลหรืออินเทอร์เน็ต ได้กระทำการใดๆ ในโลกดิจิทัล เช่น การใช้งานกล้องดิจิทัล สมาร์ทโฟน แท็บเล็ต และคอมพิวเตอร์ รอยเท้าดิจิทัลจะบันทึกข้อมูลของผู้ใช้งาน คือชื่อ และข้อมูลส่วนตัว เช่น วันเกิด ที่อยู่ รอยเท้าดิจิทัล สามารถบอกให้ผู้อื่นทราบถึงสิ่งที่เราชอบ สิ่งที่น่าสนใจ และสิ่งที่เราอยากทำ ข้อมูลบางอย่างเป็นเรื่อง ที่เราพอที่จะทราบว่าเราได้ทิ้งร่องรอยไว้ ในขณะที่บางอย่างเราไม่เคยทราบมาก่อนเลยว่าได้ถูก บันทึกไว้ รอยเท้าดิจิทัล



ร่องรอยดิจิทัล (Digital footprint)

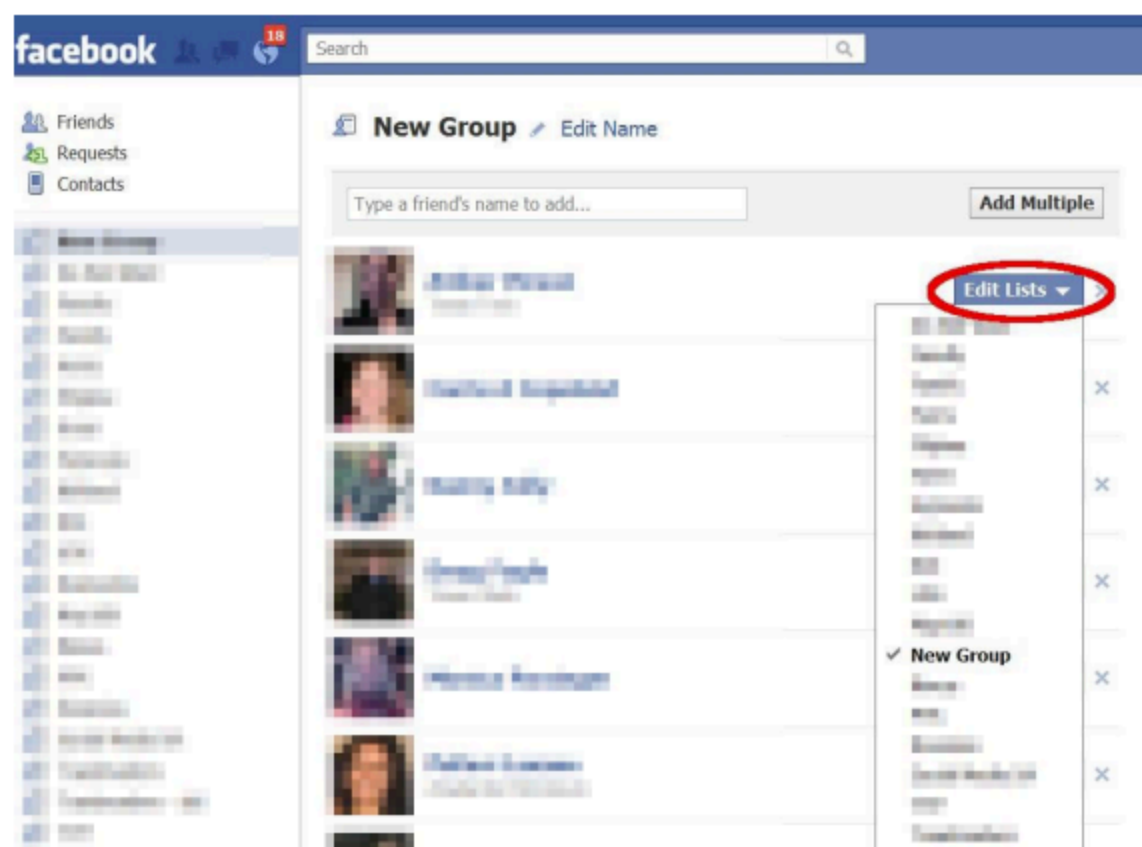


คือ ร่องรอยเท้าดิจิทัลมี 2 ประเภทคือ

1. Active Digital Footprint
2. Passive Digital Footprint



ร่องรอยดิจิทัล (Digital footprint)



- ภาพหรือข้อมูลส่วนตัว เช่น หมายเลขโทรศัพท์ ที่อยู่ หมายเลขบัตรประชาชน
- การดำเนินชีวิต และ การเป็นอยู่ของเรา
- ภาพกับเพื่อน กลุ่มต่าง ๆ
- ความสัมพันธ์กับคนต่าง ๆ ยกตัวอย่างเช่น เพื่อนใน Facebook (เพื่อนร่วมงาน เจ้านาย)

ร่องรอยดิจิทัล (Digital footprint)

หลายเหตุผลที่กระทำก่อให้เกิด Digital Footprint



- ไม่เห็นเป็นอะไร Facebook , Instagram
- เป็นพื้นที่ส่วนตัว
- ไม่ใช่คนดัง ไม่ใช่ดารา ไม่มีใครสนใจหรอก
- แค่อยากระบายอะไรบ้าง



ร่องรอยดิจิทัล (Digital footprint)

ดังนั้นคิดให้ดีก่อนที่จะ
Post



อันตรายของการทิ้ง Digital Footprint

- ทดสอบค้นหาชื่อตัวเอง
- ข้อมูลมีโอกาสโดนทำสำเนาไปนับไม่ถ้วน
- อยู่ในมือผู้ไม่หวังดี
- เสียภาพพจน์ และ ภาพลักษณ์ โดยไม่อาจแก้ไขได้

ร่องรอยดิจิทัล (Digital footprint)



รอยเท้าดิจิทัล

1. Active Digital Footprints

รอยเท้าดิจิทัลที่ผู้ใช้งานเจตนาบันทึกไว้ในโลกออนไลน์ เช่น



สิ่งที่เราพูดหรือโพสต์
ลงในอีเมลหรือในสื่อ
สังคมออนไลน์



สิ่งที่เรากดไลค์
รีทวีต หรือแชร์



ที่ตั้งสถานที่
ที่เราอยู่หรือเคยไป



ร่องรอยดิจิทัล (Digital footprint)

ร่องรอยดิจิทัล ที่ผู้ใช้
เจตนาบันทึก
(Active Digital
Footprints)

ร่องรอยดิจิทัล ของผู้ใช้งานที่เจตนาบันทึกไว้ในโลกออนไลน์ ข้อมูลที่เราตั้งใจเปิดเผยโดยที่รู้ตัว เช่น อีเมล เบอร์โทร ชื่อ โปรไฟล์ เฟซบุ๊ก หรือสิ่งที่เราตั้งใจโพสต์ลงในโซเชียลมีเดีย เช่น สิ่งที่เราพูดหรือโพสต์ รูปที่เราเคยลง สิ่งที่เรากดไลก์ รีทวิต หรือแชร์ ที่ตั้งสถานที่ที่เราอยู่หรือเคยไป

ร่องรอยดิจิทัล (Digital footprint)

รอยเท้าดิจิทัล

2. Passive Digital Footprints

รอยเท้าดิจิทัลที่ผู้ใช้งานไม่มีเจตนาบันทึกเอาไว้ในโลกออนไลน์ เช่น



สิ่งที่เรา
เคยคลิกเข้าไป



ประวัติการ
ค้นหาในโลก
ออนไลน์



การซื้อสินค้า
ออนไลน์
ของเรา



IP address
ของเรา



การเปิดระบบ
GPS ของเรา



ร่องรอยดิจิทัล (Digital footprint)

ร่องรอยดิจิทัล ที่ผู้ใช้
ไม่เจตนาบันทึก
(Passive Digital
Footprints)

ร่องรอยดิจิทัล ของผู้ใช้งานที่ไม่มีเจตนาบันทึกเอาไว้ในโลกออนไลน์ หรือข้อมูลแบบที่ไม่ได้ตั้งใจหรือไม่ได้รู้ตัว เช่น IP Address หรือ Search History ต่าง ๆ ที่เราถูกจัดเก็บเอาไว้ สิ่งที่เราเคยคลิกเข้าไป การซื้อสินค้าออนไลน์ของเรา การเปิดระบบ GPS เป็นต้น

ร่องรอยดิจิทัล (Digital footprint)

DIGITAL FOOTPRINT



ยิ่งทิ้งรอยเท้ามากเท่าไร

ยิ่งระบุตัวตนเรามากเท่านั้น



**รู้จัก Digital Footprint ก่อนสาย
ทำลายอนาคตโดยไม่รู้ตัว**



CYBER ELITE

แนวโน้มด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ

สำหรับปี 2024 โดย Gartner



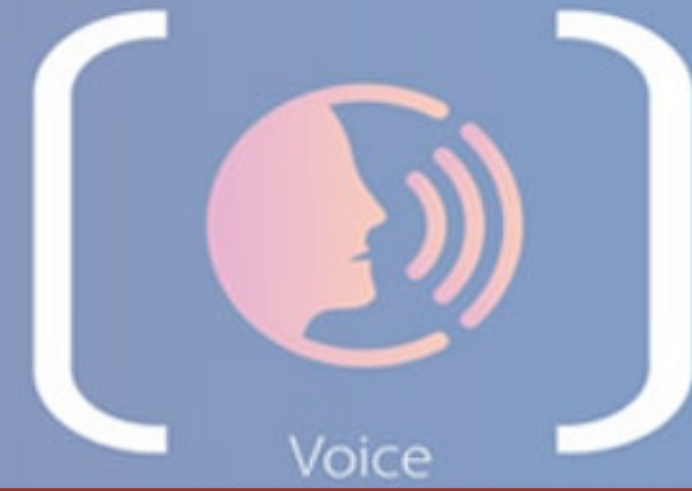
แนวโน้มความปลอดภัยดิจิทัล 2524

ในปัจจุบัน ต้องเผชิญกับภัยคุกคาม และความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ทวีความรุนแรงมากขึ้น ท่ามกลางสภาพแวดล้อมที่เทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว นำมาซึ่ง โอกาสและความท้าทายใหม่ๆ ที่องค์กรจำเป็นต้องรับมือ เช่น **Generative AI** ที่มีบทบาทในการเปลี่ยนแปลงโลกดิจิทัลไปอย่างรวดเร็ว เนื่องจากความก้าวหน้าของเทคโนโลยีที่สามารถสร้างสรรค์ผลงานต่างๆ ออกมาได้หลากหลายเช่น ข้อความ รูปภาพ เสียง และสื่อมัลติมีเดีย นอกจากนี้ยังมีปัจจัยภายนอกอื่นๆ โดย Gartner สรุปแนวโน้มด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญสำหรับปี 2024

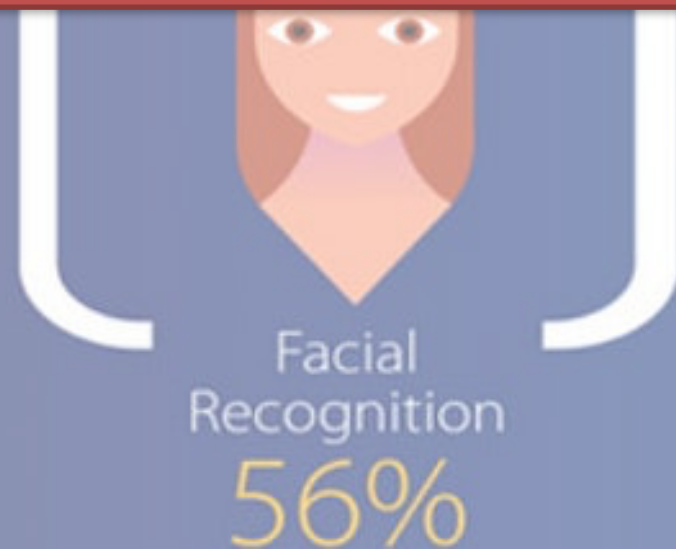
ภัยจากเทคโนโลยี AI จึงอันตราย



1. การบิดเบือนสังคมด้วย Algorithms ของ AI
2. การใช้ AI เพื่อเฝ้าจับตาความเคลื่อนไหวในสังคม
3. จริยธรรมของมนุษย์ที่อาจเสื่อมทรามลงเพราะ AI
4. การสร้างอาวุธร้ายแรงที่ควบคุมโดย AI
5. ความเสี่ยงที่อาจนำไปสู่วิกฤตการเงินครั้งใหญ่



การพิสูจน์บุคคล(Identification and Authentication)





การพิสูจน์บุคคล(Identification and Authentication)

ในยุคปัจจุบันเป็นยุคของข้อมูลข่าวสาร เป็นโลกของการเก็บรักษาข้อมูลให้ปลอดภัย เพราะฉะนั้นจึงเป็นสิ่งสำคัญกับตัวบุคคลและองค์กร เพราะข้อมูลบางอย่างของทั้งตัวบุคคลและองค์กรมีความสำคัญและไม่สามารถเปิดเผยต่อบุคคลภายนอกได้

เช่น ข้อมูลและความปลอดภัยของระบบคอมพิวเตอร์ขององค์กร หรือข้อมูลส่วนตัวของบุคคล เช่น ข้อมูลบัตร ATM, บัตรเครดิต หรือรหัสส่วนตัวสำหรับการเข้าสู่ข้อมูลภายในคอมพิวเตอร์ต่าง ๆ

2-Step Verification

A text message with your code has been sent to: (***) ***-**95

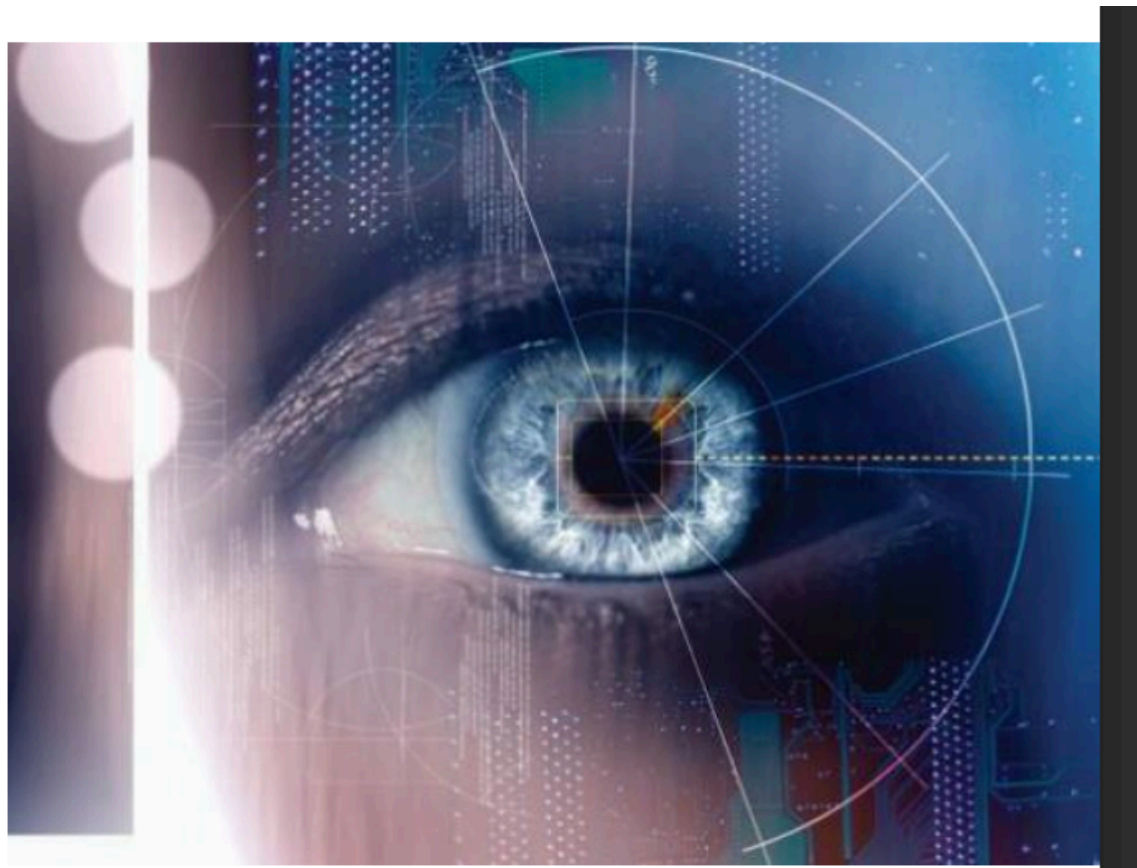
123456

Verify

☐ Don't ask for codes again on this computer



การพิสูจน์บุคคล(Identification and Authentication)



การพิสูจน์ตัวตนจึงมีความสำคัญ เนื่องจาก
ว่าการที่บุคคลใดจะเข้าสู่ระบบได้ จำเป็นต้องได้
รับอนุญาตหรือได้รับการยืนยันว่าเป็นบุคคลคน
นั้นจริง จึงจะเข้าสู่ข้อมูลหรือระบบส่วนตัวนั้นได้
ดังนั้นความปลอดภัยของข้อมูลจึงขึ้นอยู่กับการ
ยืนยันตัวตนที่แท้จริง



การพิสูจน์บุคคล (Identification and Authentication)

การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

- * **การระบุตัวตน (Identification)** คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น

ชื่อผู้ใช้ (Username)

- * **การพิสูจน์ตัวตน (Authentication)** คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็น

บุคคลที่กล่าวอ้างจริง



ประเภทของการพิสูจน์ตัวตน (Authentication Types)

ส่วนประกอบพื้นฐานของการพิสูจน์ตัวตนสมบูรณ์แบ่งได้เป็น 3 ส่วน คือ

- 1) **การพิสูจน์ตัวตน (Authentication)** คือส่วนที่สำคัญที่สุดเพราะเป็นขั้นตอนแรกของการเข้าใช้ระบบ ผู้ใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ การพิสูจน์ตัวตนเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง
- 2) **การกำหนดสิทธิ์ (Authorization)** คือข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง
- 3) **การบันทึกการใช้งาน (Accountability)** คือการบันทึกรายละเอียดของการใช้ระบบ และรวมถึงข้อมูลต่างๆ ที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบจะได้ตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้เปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง



ประเภทของการพิสูจน์ตัวตน (Authentication Types)

ส่วนประกอบพื้นฐานของการพิสูจน์ตัวตนสมบูรณ์แบ่งได้เป็น 3 ส่วน คือ

- 1) **การพิสูจน์ตัวตน (Authentication)** คือส่วนที่สำคัญที่สุดเพราะเป็นขั้นตอนแรกของการเข้าใช้ระบบ ผู้ใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ การพิสูจน์ตัวตนเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง
- 2) **การกำหนดสิทธิ์ (Authorization)** คือข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง
- 3) **การบันทึกการใช้งาน (Accountability)** คือการบันทึกรายละเอียดของการใช้ระบบ และรวมถึงข้อมูลต่างๆ ที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบจะได้ตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้เปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง



การพิสูจน์บุคคล(Identification and Authentication)

1. ไม่มีการพิสูจน์ตัวตน

ตามหลักการแล้วการพิสูจน์ตัวตนไม่มีความจำเป็น
ถ้าเงื่อนไขต่อไปนี้เป็นจริง

- * ข้อมูลเหล่านั้นเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้ หรือ

- * ข้อมูลข่าวสารหรือแหล่งของข้อมูลนั้น ๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

ชนิดของการพิสูจน์ตัวตน



การพิสูจน์บุคคล(Identification and Authentication)

2. การพิสูจน์ตัวตนโดยใช้รหัสผ่าน

รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย
รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบ แต่
ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมาก
พอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์
หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่
ง่ายเกินไป และวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัส
ผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

ชนิดของการพิสูจน์ตัวตน





การพิสูจน์บุคคล(Identification and Authentication)

3. การพิสูจน์ตัวตนโดยใช้ PIN

PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านการธนาคาร เช่น บัตร ATM และบัตรเครดิตต่าง ๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่น ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

ชนิดของการพิสูจน์ตัวตน





การพิสูจน์บุคคล (Identification and Authentication)

4. การพิสูจน์ตัวตนโดยใช้ Password

Authenticators หรือ Tokens

Authenticator หรือ Token เป็นฮาร์ดแวร์ พิเศษที่ใช้สร้าง รหัสผ่านซึ่งเปลี่ยนแปลงได้ (Dynamic Password) ในขณะที่กำลังเข้าสู่ ระบบเครือข่าย

ชนิดของการพิสูจน์ตัวตน





การพิสูจน์บุคคล(Identification and Authentication)

5. การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว

One-Time Password (OTP) ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำ ๆ กัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบ

ชนิดของการพิสูจน์ตัวตน





การพิสูจน์บุคคล(Identification and Authentication)

6. การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจ

สาธารณะ

เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่ยอมรับใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่า การเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัส ทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล

ชนิดของการพิสูจน์ตัวตน





การพิสูจน์บุคคล(Identification and Authentication)

7. การพิสูจน์ตัวตนโดยใช้ลายเซ็น

อิเล็กทรอนิกส์ (Digital Signature)

เป็นการนำหลักการของการทำงานของระบบ
การเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการ
พิสูจน์ตัวตนมาประยุกต์ใช้ ระบบของลาย
เซ็นดิจิทัล

ชนิดของการพิสูจน์ตัวตน





การพิสูจน์บุคคล(Identification and Authentication)

8. การพิสูจน์ตัวตนโดยใช้การถาม-ตอบ

เป็นวิธีการพิสูจน์ตัวตนโดยใช้การถาม-ตอบ เมื่อผู้ใช้เข้ามาในระบบแล้ว ระบบจะแน่ใจได้อย่างไรว่าผู้ใช้คนนั้น เป็นคนที่ได้รับอนุญาตให้เข้ามาใช้ระบบได้จริง การใช้ชื่อผู้ใช้และรหัสผ่าน ในปัจจุบันนี้ไม่มีความปลอดภัยเพียงพอต่อการเข้าใช้ระบบ เนื่องจากความรู้และวิทยาการที่ก้าวหน้า ทำให้เกิดผู้ที่ต้องการจะเข้ามาละเมิดระบบต่าง ๆ มากขึ้น ทำให้ชื่อผู้ใช้และรหัสผ่านอาจจะถูกลักลอบดักข้อมูลระหว่างการสื่อสารกันได้

ชนิดของการพิสูจน์ตัวตน





การกำหนดสิทธิการเข้าถึงข้อมูล



การกำหนดสิทธิ์ การเข้าถึงข้อมูล

การกำหนดสิทธิ์การเข้าถึงข้อมูล

หมายถึง การควบคุมการเข้าถึงข้อมูลของผู้ใช้งาน ผ่านการกำหนดรหัสผ่าน หรือการปิดสิทธิ์ไม่ให้ผู้ใช้งานเห็นข้อมูลนั้นๆ การกำหนดขึ้นอยู่กับระดับความสำคัญและหน้าที่การทำงานของแต่ละบุคคล





การกำหนดสิทธิ์ (Authorization)

หลักการสิทธิน้อยที่สุด Principle of Least Privilege

สามารถใช้ปรับปรุงความปลอดภัยของระบบคอมพิวเตอร์ นี่เป็นเรื่องพื้นฐานแต่สำคัญมาก ที่มักถูกมองข้ามหลักการนี้คือ ผู้ใช้ จะต้องมีระดับต่ำที่สุดของสิทธิตามความต้องการเพื่อกระทำงานตามที่มอบหมาย



ใครเข้าถึงข้อมูลของผู้ใช้งาน ในสื่อสังคมออนไลน์ได้บ้าง



1. องค์กรซึ่งต้องการรวบรวมข้อมูลส่วนตัวของผู้ใช้งานที่ได้รับอนุญาตตามกฎหมาย

- บริษัทขายสินค้าและบริการซึ่งสนใจข้อมูลส่วนตัวของผู้ใช้งาน เพื่อที่จะเลือกกลุ่ม เป้าหมายได้ตรงกับสินค้าและบริการของบริษัท
- ผู้พัฒนาซอฟต์แวร์ที่ร่วมมือกับสื่อสังคมออนไลน์ เพื่อที่จะพัฒนาแอปที่ตรงกับ ความต้องการของผู้ใช้งาน



ใครเข้าถึงข้อมูลของผู้ใช้งาน ในสื่อสังคมออนไลน์ได้บ้าง



2. บุคคลซึ่งต้องการรวบรวมข้อมูลส่วนตัว ของผู้ใช้งานที่ไม่ได้รับอนุญาตตามกฎหมาย

- มิจฉาชีพที่มุ่งโจรกรรมอัตลักษณ์ของผู้ใช้งานโดยการรวบรวมสิ่งที่ผู้ใช้งานโพสต์ และสิ่งที่คนอื่นโพสต์เกี่ยวกับผู้ใช้งาน
- ผู้ไม่หวังดีในโลกไซเบอร์อื่นๆ เช่น ผู้ที่หวังจะคุกคามผู้ใช้งาน หรือต้องการที่จะเจาะ ระบบ หรือปล่อยไวรัสคอมพิวเตอร์





ใครเข้าถึงข้อมูลของผู้ใช้งาน ในสื่อสังคมออนไลน์ได้บ้าง



3. โฆษณาที่เลือกกลุ่มเป้าหมายตามพฤติกรรมการใช้สื่อออนไลน์

สื่อสังคมออนไลน์ ที่ให้บริการโดยไม่ได้เก็บค่าสมาชิกจากผู้ใช้งานจะมีรายได้จากการขาย

โฆษณาที่ ขึ้นบนหน้าฟีดของสื่อสังคมออนไลน์ (behavior advertising)

สื่อสังคมออนไลน์ จะเก็บข้อมูลของผู้ใช้งานที่มีแนวโน้มและศักยภาพในการการซื้อสินค้าและบริการ บริษัทผู้ผลิตยินดีที่จะได้ข้อมูลเหล่านี้เพื่อจะได้เข้าถึงกลุ่มเป้าหมาย ในขณะที่ผู้ใช้งานอาจจะรู้สึกสะดวกที่ได้เห็นโฆษณาที่ตรงกับความสนใจของตนเองขณะที่ใช้ สื่อสังคมออนไลน์นั้นๆ



ใครเข้าถึงข้อมูลของผู้ใช้งาน ในสื่อสังคมออนไลน์ได้บ้าง



4. แอปพลิเคชันภายนอก (Third-party applications) บนเครือข่ายสังคมออนไลน์

แอปเหล่านี้ คือ โปรแกรมที่สามารถเชื่อมต่อกับสื่อสังคมออนไลน์ แต่ไม่ได้เป็นส่วนหนึ่งของสื่อสังคมออนไลน์ โดยมีรูปแบบต่างๆ เช่น

- เกมที่ผู้ใช้จะเล่นกับรายชื่อผู้ติดต่อ
- โพลหรือคำถามออนไลน์
- ซอฟต์แวร์ที่ยินยอมให้ผู้ใช้งานโพสต์ลงสื่อสังคมออนไลน์โดยผ่านแอปพลิเคชันในมือถือ



วิธีการ และผลกระทบของ
ภัยในรูปแบบต่าง ๆ



วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ

การเข้ารหัสข้อมูล

HTTPS ย่อมาจาก Hypertext Transfer Protocol

Secure หรือ Hypertext

Transfer Protocol Over SSL(Secure Socket Layer)

เป็นการทำงานเหมือนกับ HTTP ธรรมดาแต่ทำอยู่บน

SSL เพื่อให้เกิดความปลอดภัยในการส่งข้อมูลมากยิ่งขึ้น มีรูปแบบดังนี้





วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ

มัลแวร์ (malware – malicious software)

WPA2 คือเทคโนโลยีการรักษาความปลอดภัยที่ปกป้อง

เครือข่าย Wi-Fi ของคุณโดยการเข้ารหัสการจราจรบน

เครือข่าย

นอกจากนี้ ยังทำให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงเครือข่าย

ได้ยากขึ้น





วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ

มัลแวร์ (malware – malicious software)

คือโปรแกรมที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อ
เครื่องคอมพิวเตอร์และเพื่อมาล้วงข้อมูลสำคัญไป
จากผู้ใช้งานคอมพิวเตอร์





Malware มีกี่ชนิด

วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ

มัลแวร์มีอยู่หลายชนิดด้วยกัน ซึ่งสามารถแบ่งออกเป็น 6 ชนิดด้วยกันคือ

1. ไวรัส (Virus) เป็นโปรแกรมที่ติดต่อกับไฟล์หนึ่งไปสู่อีกไฟล์หนึ่งได้ และสามารถส่งผ่านไฟล์ด้วยการแนบไวรัสไปกับไฟล์ที่เราส่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งได้ โดยไวรัสจะทำการทำลายทั้งฮาร์ดแวร์และซอฟต์แวร์ในเครื่องพร้อมกับไฟล์ที่ไวรัสแฝงตัวเองเพื่อแพร่กระจายไปสู่เครื่องอื่นๆด้วย



Malware มีกี่ชนิด

วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ

2. เวิร์ม (Worm) สามารถที่จะแพร่ขยายตัวเอง โดยที่ไม่ต้องมีโปรแกรมอื่นในการแพร่กระจาย ก็ได้เช่นกันเป้าหมายของเวิร์มจะจ้องทำลาย ระบบเครือข่าย และขยายการแพร่กระจายไปยัง คอมพิวเตอร์ตัวอื่นๆ โดยการส่งอีเมลหรือช่อง โหว่ของระบบปฏิบัติการ



Malware มีกี่ชนิด

วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ

3. โทรจัน (Trojan Horse)

เป้าหมายของมัลแวร์ตัวนี้จะค่อย ๆ จ้องทำลายระบบและเปิดช่องโหว่ให้กับผู้ไม่หวังดีเข้ามาทำลายระบบและควบคุมจากระยะไกล และไม่แพร่กระจายไปยังไฟล์อื่น ๆ



วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ



Malware มีกี่ชนิด

4. สपाายแวร์ (Spyware)

จะไม่แพร่กระจายไปยังไฟล์อื่น ๆ เหมือนกับโทร
จัน โดยเป้าหมายของสपाายแวร์นั้น
จ้องที่จะรบกวนและละเมิดความเป็นส่วนตัวของ
ผู้ใช้.



Malware มีกี่ชนิด

วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ

5. Hybrid Malware/Blended Threats

เป็นมัลแวร์ที่อันตรายมากเพราะรวมความ

สามารถของ ไวรัส เวิร์ม โทรจัน สปายแวร์ เข้าไว้
ด้วยกัน.



การหลอกลวง (Scam)

วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ

เล่ห์อุบาย แผนการร้าย คำนี้อหากอยู่ในวงการ
ออนไลน์ จะใช้เรียกพฤติกรรม ที่มีเจตนา
หลอกลวง ให้เสียทรัพย์ ให้เสียข้อมูล ตัวอย่าง
การหลอกลวงทางอินเทอร์เน็ต เช่น Email
Scams Phishing Scam เป็นต้น



การโจมตีแบบวิศวกรรมสังคม (Social Engineering)

วิธีการ และผลกระทบของภัยในรูปแบบต่าง ๆ

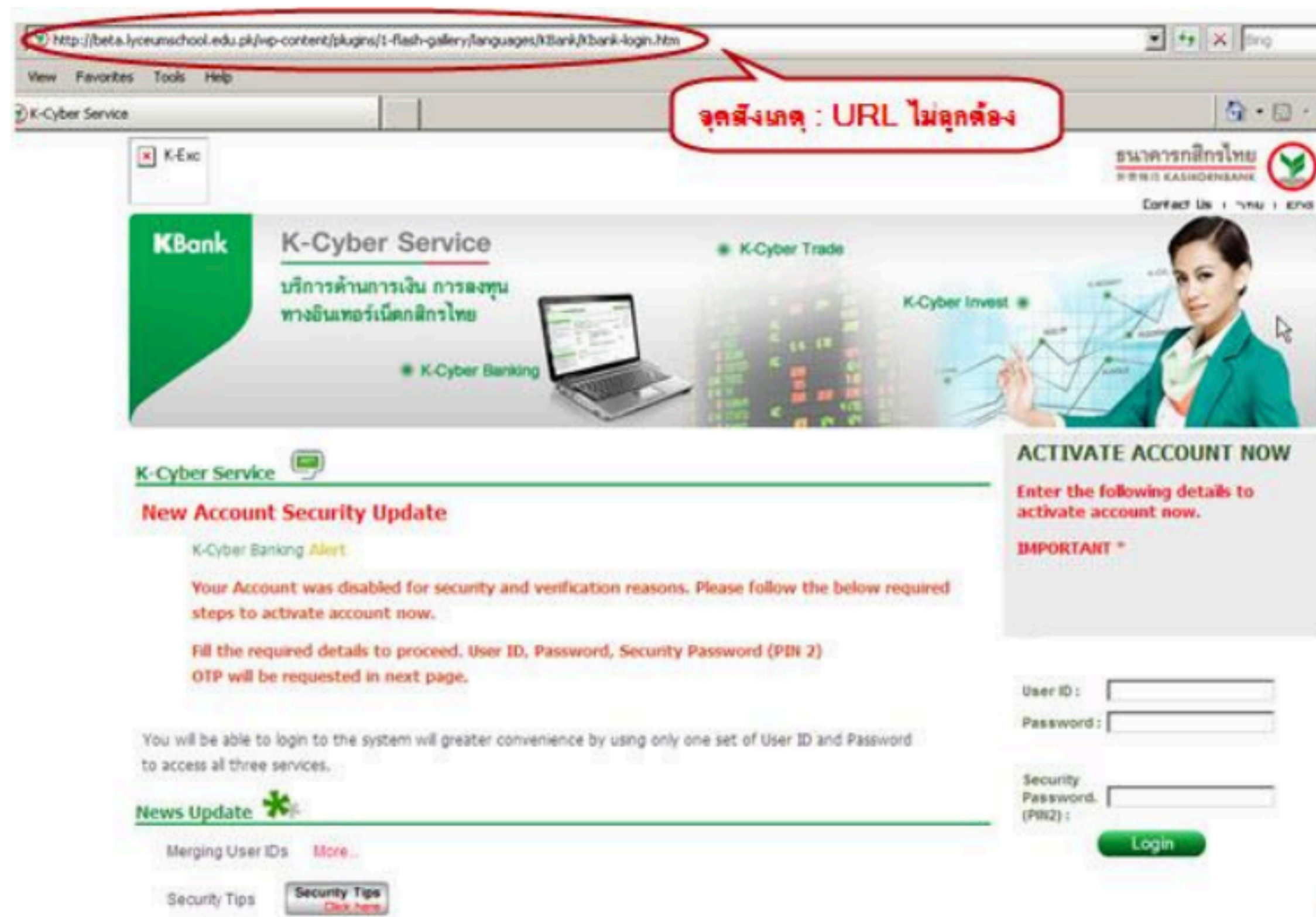
Phishing คือคำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูลเช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น ในบทความนี้จะเน้นในเรื่องของ Phishing ที่มีจุดมุ่งหมายเพื่อหลอกลวงทางการเงิน เนื่องจากจะทำให้ผู้อ่านมองเห็นผลกระทบได้ง่าย



การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม



ตัวอย่าง การ Phishing





การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม



Mobile Security and Privacy

ความเป็นส่วนตัวและความปลอดภัยบนมือถือซึ่งในยุคปัจจุบันเราใช้อุปกรณ์ประเภทเคลื่อนที่ได้ จัดเก็บข้อมูลสำคัญมากขึ้น อาทิเช่น รายชื่อผู้ติดต่อ รูปภาพ ภาพเคลื่อนไหว รวมทั้งเอกสารสำคัญเรื่องงานไว้บนอุปกรณ์ประเภทเคลื่อนที่มากขึ้น



การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม



Mobile Security and Privacy

- การเก็บข้อมูลสำคัญ
- เกิดอะไรขึ้นถ้าโทรศัพท์เคลื่อนที่หาย
- การส่งตำแหน่งที่อยู่ของอุปกรณ์ไปยังเครื่องแม่ข่ายตลอดเวลา
- การสำรองข้อมูลบนมือถือ
- เอกสารงานสำคัญบนโทรศัพท์เคลื่อนที่



รหัสผ่านที่ดี

การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม

- ใช้รหัสเดียวกันหมด รหัสเดียวกันสามารถเข้าถึงได้หมด
- ไม่มีการเปลี่ยนรหัสผ่าน
- คาดเดาง่ายเช่น 1234567
- ประกอบด้วยข้อมูลบุคคล เช่น วันเกิด เบอร์โทร
- ใช้คำมีความหมาย เช่น ชื่อเล่น love happy
- ใช้ตัวพิมพ์ทั้งหมด ไม่มีตัวเลขหรือตัวอักษรผสม



การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม



รหัสผ่านที่ไม่ควรตั้ง

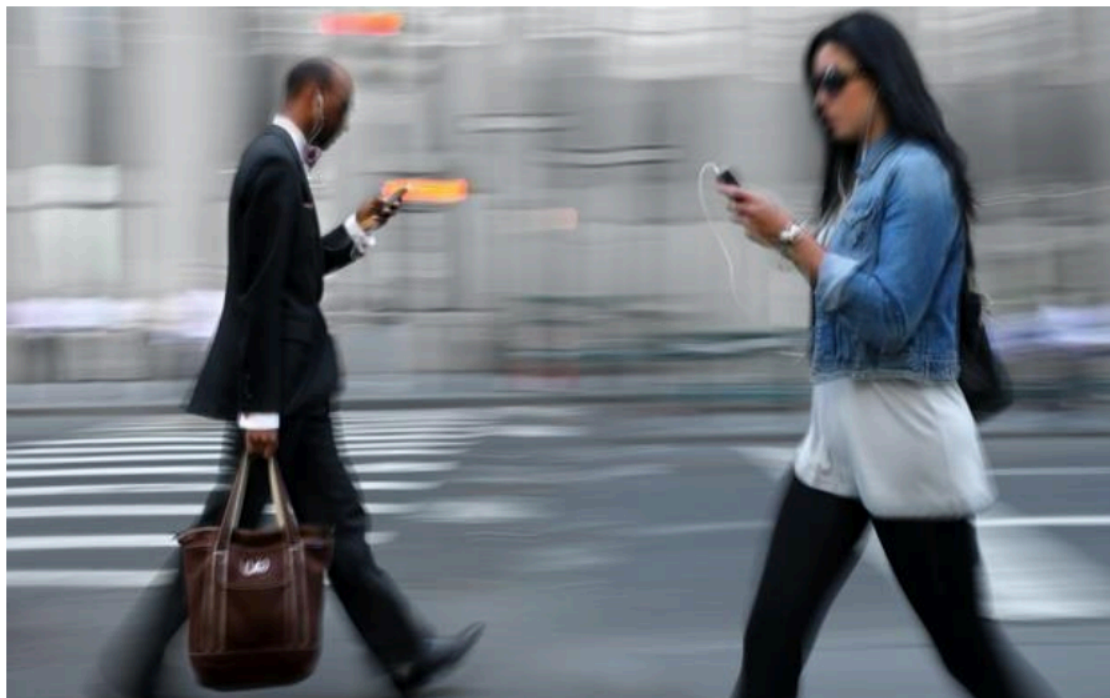
- ใช้รหัสผ่านที่ยาว (อย่างน้อย 7 ตัว)
- ใช้ตัวอักษรตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก ตัวเลข
- รวมทั้งสัญลักษณ์ต่างๆ ประกอบกัน
- ใช้สัญลักษณ์อย่างน้อยหนึ่งตัวในตำแหน่งที่ 2 – 6
- ใช้ตัวอักษรที่แตกต่างกันอย่างน้อย 4 ตัว (อย่าใช้ตัวอักษรซ้ำกัน) ใช้ตัวเลขและตัวอักษรแบบสุ่ม



พฤติกรรมเสี่ยง เมื่อใช้
อุปกรณ์ในที่สาธารณะ

การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกรั้วคุกคาม

- เชื่อมกับไวไฟที่ไม่ได้เข้ารหัส
- ไม่ระวังว่ามีผู้อื่นแอบฟังบทสนทนาอยู่
- ไม่ระวังผู้อื่นแอบหน้าจอ
- ไม่ระวังรอบตัว



การหลอกลวงออนไลน์ (Fraud)

การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม

- มิจฉาชีพจะติดต่อหาเหยื่อที่กำลังต้องการสินค้า
- สร้างความเชื่อถือด้วยภาพสินค้า และหลักฐานปลอมเพื่อระบุด่วน
- หวานล่อมให้เหยื่อยอมโอนเงินค่าสินค้า หากเหยื่อรู้สึกว่าราคาถูกจนผิดปกติ หรือ รู้สึกไม่ไว้วางใจ มิจฉาชีพก็จะพยายามพูดโกหกเพื่อตอบข้อสงสัยของเหยื่อ
- ส่งสินค้าปลอมให้เหยื่อ หรือในกรณีที่แย่ที่สุด คือไม่ส่งสินค้าใดๆ ให้เลย
- ปิดช่องทางการสื่อสาร และลบหนีลบข้อมูลทุกอย่างทิ้ง
- เปลี่ยนชื่อ หลักฐาน เริ่มวงจรหลอกลวงใหม่

การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม



การหลอกลวงออนไลน์ (Fraud)

การหลอกลวงขอหมายเลขบัตรเครดิต เพื่อนำไปลักลอบใช้ทุกวันนี้ด้วยโลกอินเทอร์เน็ตที่เข้ามาในบ้านเราและมีเครือข่ายที่ครอบคลุมมากขึ้นเรื่อยๆ ทำให้คนยุคใหม่ที่เคยซื้อของต่างๆ ได้ง่ายขึ้นผ่านระบบออนไลน์ โดยไม่ต้องออกไปข้างนอกให้เสียเวลา เพียงแค่สั่งซื้อสินค้าที่เราสนใจและจ่ายผ่านทางบัตรเครดิตเท่านั้นเราก็จะได้สินค้าส่งตรงถึงบ้าน แต่โลกออนไลน์ก็เต็มไปด้วยการหลอกลวงเพื่อเอาเงินของเรา จึงต้องระวังอย่างมากเมื่อใช้บัตรเครดิตซื้อของออนไลน์ ในปัจจุบัน

การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม

5ข้อควรระวังเมื่อ ใช้บัตรเครดิตซื้อของออนไลน์



การหลอกลวงออนไลน์ (Fraud)

- อย่าให้หมายเลขบัตรผ่านทางอีเมลล์
- ตรวจสอบความน่าเชื่อถือของร้านค้าเสมอ
- แน่ใจว่าเว็บไซต์ต่างๆปลอดภัยสำหรับคุณ
- เช็ดยอดหนี้ในบัตรเครดิตอย่างละเอียด
- ไม่มีการส่งลิงค์หรือส่งข้อมูลสำคัญทางอีเมลล์



การหลอกลวงออนไลน์ (Fraud)

การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม

อันตรายจากการใช้Wifi สาธารณะ

ความไม่ปลอดภัยที่เป็นไปได้ เมื่อคุณเข้าใช้ฟรี wifi network, การ hack wireless มีรูปแบบไหนบ้าง และวิธีการป้องกันตนเอง เพื่อป้องกันจากการถูก hack บนเครือข่าย ฟรี wifinetwork



อันตรายจากการใช้Wifi สาธารณะ

การปฏิบัติเพื่อป้องกัน และลดความเสี่ยงต่อการถูกภัยคุกคาม

รูปแบบ การ hack บนเครือข่าย Wireless

- **Sniffing** เป็นการใช้โปรแกรมในการดักจับ packets ที่ผ่านไปมาบนเครือข่ายไวเลสที่ไม่มีความปลอดภัย (ฟรี wifi network)
- **Sidejacking** เป็นเทคนิคในการดักจับ cookie sessions เพื่อ login เข้าใช้ account facebook ของคุณ เป็นต้น โดยไม่ต้องใช้username หรือ รหัสผ่าน
- **Evil Twin/Honeypot** เทคนิคในการสร้าง access point ปลอมขึ้นมา เพื่อหลอกให้คุณเข้าใช้ โดยตั้งชื่อ access point ให้เหมือนกับเครือข่ายไวเลส ที่คุณใช้อยู่ประจำ หลังจากนั้น จะใช้ โปรแกรม hack password หรือ โปรแกรมดักจับข้อมูล เพื่อเก็บข้อมูลการใช้งานอินเทอร์เน็ต

ความสำคัญของการสำรองข้อมูล
และการกู้คืนระบบ



๕๔
การกู้คืนข้อมูลสารสนเทศ



ความสำคัญของ การสำรองข้อมูล และการกู้คืนระบบ การสำรองข้อมูล (Backup)

1) การป้องกันข้อมูลสูญหาย การสำรองข้อมูลเป็นกระบวนการที่สำคัญเพื่อป้องกันการสูญหายของข้อมูลที่เกิดจากเหตุการณ์ไม่คาดคิด เช่น การโจมตีทางไซเบอร์ ฮาร์ดแวร์เสียหาย หรือข้อผิดพลาดของมนุษย์ การมีข้อมูลสำรองช่วยให้สามารถกู้คืนข้อมูลได้ในกรณีที่ข้อมูลต้นฉบับสูญหายหรือเสียหาย



ความสำคัญของ
การสำรองข้อมูล
และการกู้คืนระบบ
การสำรองข้อมูล (Backup)

2) การป้องกันการโจมตีทางไซเบอร์การโจมตีทางไซเบอร์ เช่น Ransomware สามารถทำให้ข้อมูลถูกเข้ารหัสและไม่สามารถเข้าถึงได้ การมีข้อมูลสำรองที่ไม่ได้เชื่อมต่อกับระบบหลักจะช่วยให้สามารถกู้คืนข้อมูลได้โดยไม่ต้องจ่ายค่าไถ่ให้แฮกเกอร์



ความสำคัญของ
การสำรองข้อมูล
และการกู้คืนระบบ
การสำรองข้อมูล (Backup)

3) การป้องกันการเสียหายของฮาร์ดแวร์ฮาร์ดไดรฟ์
และอุปกรณ์เก็บข้อมูลอื่น ๆ มีโอกาสเสียหายได้ การ
สำรองข้อมูลช่วยป้องกันการเสียหายที่เกิดจาก
ฮาร์ดแวร์เสียหาย ทำให้สามารถเรียกคืนข้อมูลได้ทันที



ความสำคัญของ
การสำรองข้อมูล
และการกู้คืนระบบ
การสำรองข้อมูล (Backup)

4) การสำรองข้อมูลตามระยะเวลาการสำรองข้อมูล
อย่างต่อเนื่องหรือแบบอัตโนมัติช่วยให้มีข้อมูลที่
อัปเดตอยู่เสมอ ทำให้ลดความเสี่ยงในการสูญหายของ
ข้อมูลที่สำคัญ



การกู้คืนระบบ (Disaster Recovery)

1) ความสามารถในการกู้คืนระบบอย่างรวดเร็วการกู้คืนระบบคือกระบวนการที่ทำให้ระบบสามารถกลับมาทำงานได้อย่างรวดเร็วหลังจากเกิดเหตุการณ์ที่ทำให้ระบบล้มเหลว การมีแผนการกู้คืนระบบช่วยให้ธุรกิจสามารถดำเนินการต่อไปได้โดยมีการหยุดชะงักน้อยที่สุด

การกู้คืนข้อมูลสารสนเทศ

การกู้คืนระบบ (Disaster Recovery)





การกู้คืนระบบ (Disaster Recovery)

2) การลดความเสียหายทางธุรกิจการหยุดทำงาน
ของระบบสามารถทำให้ธุรกิจสูญเสียนายได้และลูกค้า
การกู้คืนระบบที่มีประสิทธิภาพช่วยลดความเสียหายที่
เกิดขึ้นและช่วยให้ธุรกิจกลับมาทำงานได้ในเวลาที่
รวดเร็ว





การกู้คืนระบบ (Disaster Recovery)

3) การรักษาความต่อเนื่องทางธุรกิจแผนการกู้คืนระบบที่ดีเป็นส่วนหนึ่งของการวางแผนความต่อเนื่องทางธุรกิจ (Business Continuity Planning - BCP) ทำให้ธุรกิจสามารถดำเนินการต่อไปได้แม้ในสถานการณ์ที่ยากลำบาก

การกู้คืนข้อมูลสารสนเทศ





การกู้คืนระบบ (Disaster Recovery)

การกู้คืนข้อมูลสารสนเทศ

4) การป้องกันการสูญเสียชีวิตข้อมูลในระยะยาวการกู้คืนระบบที่มีประสิทธิภาพช่วยป้องกันการสูญเสียชีวิตข้อมูลในระยะยาว และช่วยให้สามารถกู้คืนข้อมูลได้ตามต้องการ





การกู้คืนระบบ (Disaster Recovery)

การกู้คืนข้อมูลสารสนเทศ

4) การป้องกันการสูญเสียชีวิตข้อมูลในระยะยาวการกู้คืนระบบที่มีประสิทธิภาพช่วยป้องกันการสูญเสียชีวิตข้อมูลในระยะยาว และช่วยให้สามารถกู้คืนข้อมูลได้ตามต้องการ



คาถากันภัยมีจนาชั้น

ไม่รับ

ไม่ดูย

ไม่คลิก

ไม่เชื่อ

ไม่รับ

ไม่โอน

ข้อปฏิบัติที่ดีในการป้องกันตนเองจากภัยคุกคาม





5 วิธีป้องกันภัย คุกคามทางออนไลน์

ข้อปฏิบัติที่ดีในการป้องกันตนเองจากภัยคุกคาม

การสื่อสารทางออนไลน์แม้จะช่วยให้ชีวิตเราง่ายขึ้น
แต่ก็มีข้อควรระวังเช่นกัน เพราะหากปล่อยให้ข้อมูล
ส่วนตัวตกไปอยู่กับผู้ไม่ประสงค์ดี ก็อาจทำให้ข้อมูล
ของเราไม่ปลอดภัย วันนี้ทางศูนย์จึงขอแนะนำ 5 วิธี
ป้องกันไม่ให้ถูกโจรกรรมข้อมูล



5 วิธีป้องกันภัย คุกคามทางออนไลน์

ข้อปฏิบัติที่ดีในการป้องกันตนเองจากภัยคุกคาม

1. ไม่เชื่อ ไม่บอก ไม่กรอกข้อมูลส่วนตัวที่สำคัญบนโลกออนไลน์
2. ไม่ดาวน์โหลดแอปหรือโปรแกรมที่ไม่น่าเชื่อถือ
3. ไม่ใช้ wifi สาธารณะทำธุรกรรมการเงิน เพราะเสี่ยงถูกล้วงข้อมูล
4. ตั้งรหัสผ่านให้คาดเดายาก และเปลี่ยนเป็นระยะ เช่น ทุก 3 หรือ 6 เดือน
5. ออกจากระบบทุกครั้งเมื่อเลิกใช้งาน



คำถาม



งานกลุ่ม