



การเสริมสร้างความตระหนักรู้ ในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ

สำนักงานพัฒนาชุมชนจังหวัดยะลา



ข้อแนะนำวิธีสำรองข้อมูลเพื่อป้องกัน มัลแวร์เรียกค่าไถ่หรือข้อมูลสูญหาย

ควรมีการสำรองข้อมูลอยู่เป็นประจำเพื่อป้องกันข้อมูลสูญหายเนื่องจาก



ฮาร์ดดิสก์
เสียหาย



เครื่องติด
มัลแวร์



เฟลอปดิสก์
โดยไม่ตั้งใจ



แก้ไขไฟล์
ผิดพลาด

คาถา สำรองข้อมูลให้ปลอดภัย (ทำตัวเอง)



1 ใช้บริการ **Backup and Restore**
ที่มากับระบบปฏิบัติการ

2 สำรองข้อมูลกับอุปกรณ์ภายนอก
ได้มากกว่า 1 ชุด



3 **เข้ารหัสลับ**ข้อมูลที่สำรอง
เช่น โปรแกรม Bitlocker ที่มากับ
ระบบปฏิบัติการวินโดวส์

4 สำรองข้อมูลบน **Cloud**
ก็เสี่ยงไม่น้อย ฉะนั้นเลือก
ไฟล์ที่ส่งไปเก็บให้ดี



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม



ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

<https://www.etcha.or.th/>

แบ็กอัปข้อมูลไว้ก่อน เพราะถ้าหายไป เสียเงินเท่าไร... ก็อาจไม่ได้คืนมา

สำหรับ
SMEs

รู้มั๊ย? **363%**
คือสถิติที่เพิ่มขึ้นช่วง Q2 ปี 61 - Q2 ปี 62

การโจมตีภาคธุรกิจด้วยมัลแวร์เรียกค่าไถ่

ซึ่งจะล็อกข้อมูลในเครื่อง เช่น เอกสาร รูปภาพ ทำให้เปิดใช้งานไม่ได้เพื่อเรียกค่าไถ่
และแม้จ่ายค่าไถ่ไปแล้วก็**ไม่ได้รับประกัน**ว่าจะได้ข้อมูลนั้นคืนมา

แบ็กอัปแบบไหน...ถามใจเธอดู?



บริการ Cloud เช่น Google Drive, Dropbox, OneDrive

อุปกรณ์เก็บข้อมูลแบบพกพา
เช่น DVD, ฮาร์ดดิสก์, Flash Drive

พิมพ์เป็นกระดาษ

NAS (Network-attached storage)



ใช้งานฟรี เข้าที่ไหนก็ได้
แบ็กอัปอัตโนมัติได้

ใช้งาน เก็บรักษาในที่ปลอดภัย
พกติดตัวได้

ไม่ขึ้นต่อฮาร์ดแวร์
ป้องกันการถูกเจาะข้อมูล

เก็บข้อมูลจากคอมพิวเตอร์หลายเครื่อง
พร้อมกันได้ แบ็กอัปอัตโนมัติได้



ต้องมีอินเทอร์เน็ต มีความเสี่ยงปิดบริการ

มีโอกาสสูญหายหรือเสียหาย

จัดการยาก ไม่ต่อสิ่งแวดล้อม

ต้องติดตั้งและดูแลระบบ ราคาสูง
มีโอกาสเสียหาย



(1) : <https://www.thaicert.or.th/newsbite/2019-08-15-01.html>

NAS (Network-attached storage)

*คือ อุปกรณ์ที่ให้บริการเก็บและแชร์ข้อมูลแก่เครื่องของผู้ใช้งานในเครือข่ายเดียวกัน

ข้อมูลเพิ่มเติม ศึกษาได้ที่
www.thaicert.or.th / www.etchda.or.th



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

GO
DIGITAL
with
ETDA

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

<https://www.etchda.or.th/>

9 เทคนิคใช้อุปกรณ์ไอทีอย่างปลอดภัย

เมื่อเดินทางไปเจรจาธุรกิจที่ต่างประเทศ



การนำอุปกรณ์ไปติดต่อธุรกิจในบางประเทศที่เข้มงวดทางกฎหมาย ด้านความมั่นคงปลอดภัยทางไซเบอร์ ควรมีการเตรียมพร้อมในหลาย ๆ ด้าน **เพื่อปกป้องข้อมูลสำคัญทางธุรกิจไม่ให้รั่วไหล**



ป้องกันข้อมูลสูญหาย หรือ เสียหาย



ป้องกันการถูกขโมยข้อมูล



ป้องกันการถูกดักจับข้อมูล

1 สำรองข้อมูลเฉพาะที่ต้องใช้ในแฟลชไดรฟ์หรือ SD Card

2 อัปเดตซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด

3 ไม่เชื่อมต่อ Wi-Fi สาธารณะ หากจำเป็นต้องใช้ ควรเชื่อมต่อผ่าน VPN

4 ระมัดระวังตัวเอง และหมั่นสังเกตท่าทีของคนรอบข้างอยู่เสมอ

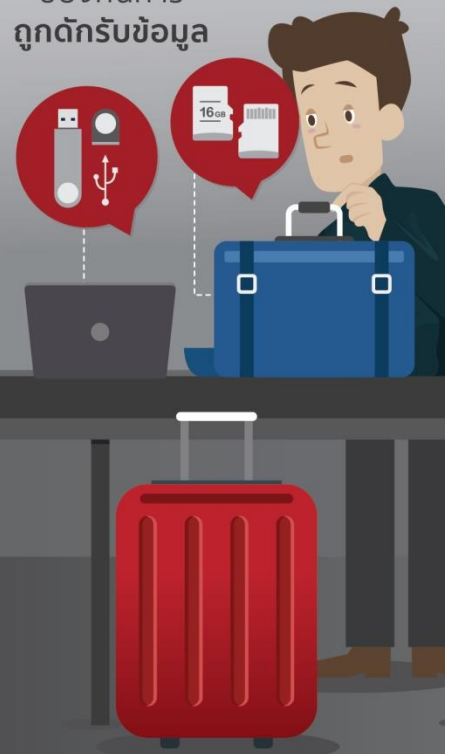
5 เข้ารหัสลับข้อมูลทุกอุปกรณ์ และไฟล์ที่สำคัญด้วยรหัสผ่านที่คาดเดายาก

6 เชื่อมต่อเว็บไซต์ผ่าน HTTPS หรือเว็บไซต์ที่เปิดใช้งานการยืนยันตัวตนแบบสองขั้นตอน

7 ไม่วางอุปกรณ์ไอทีทิ้งไว้โดยไม่มีคนดูแล

8 ใช้เทปปิดบังกล้องเว็บแคม หรือใช้ฟิล์ม ป้องกันการแอบมองหน้าจอ

9 ใช้คอมพิวเตอร์สำหรับยืนยันใช้งานชั่วคราว ที่มีเฉพาะข้อมูลสำคัญเกี่ยวกับงานในขณะนั้น



คลิกเปลี่ยนชีวิต ระวังสัณนิตก่อนติดมัลแวร์

หลาย ๆ คนอาจเคยคลิกเข้าไปดูข่าวหรือเล่น quiz ใน Facebook แล้วเกิดเหตุร้ายขึ้นผู้ใช้แอปสเปดัลประหลาด ทำให้คุณอับอาย บางคนถึงกับปิดบัญชีผู้ใช้ไปเพราะติดมัลแวร์ แล้วจะมีวิธีในการรับมือปัญหานี้อย่างไรกันดี

ติดมัลแวร์ ได้อย่างไร?

โพสต์ต่างๆ ที่ชวนคลิกให้เข้าไปดูเพื่อหลอกให้ติดมัลแวร์



Quiz

ลิงก์ควิช

แพนงตัวมาในรูปแบบแอป / Quizปลอม



ลิงก์แปลก ๆ ที่แชร์มาจากเพื่อน

ลิงก์จากเพื่อนในช่องแชตและหน้าวอลล์เพื่อน



เพจแชร์ข่าวและคลิป

ลิงก์ข่าวปลอมหรือคลิปลามก

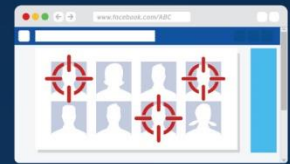
ติดแล้ว เกิดอะไรบ้าง?



โพสต์ข้อความต่าง ๆ ลงในกลุ่มหรือหน้าวอลล์ของคุณโดยไม่รู้ตัว



อาจถูกขโมยข้อมูลส่วนตัว



เพื่อนของคุณอาจติดมัลแวร์ต่อจากคุณ

ติดแล้ว แก้อย่างไร?



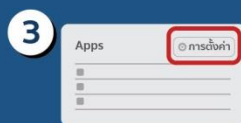
เพิ่มมาตรการความปลอดภัย!
ควรเปลี่ยนรหัสผ่านบัญชีผู้ใช้งาน



ไปที่ APPS แถบด้านซ้าย



คลิกเพื่อดูแอปเพิ่มเติม



ไปที่ การตั้งค่า



หาแอปที่มีหน้าตาแปลกปลอมแล้วลบออกจากรายการ

เล่นโซเชียลอย่างฉลาด ไม่ตกเป็นทาสพวกมัลแวร์



etda.thailand



ThaiCERT



Thaicert.or.th



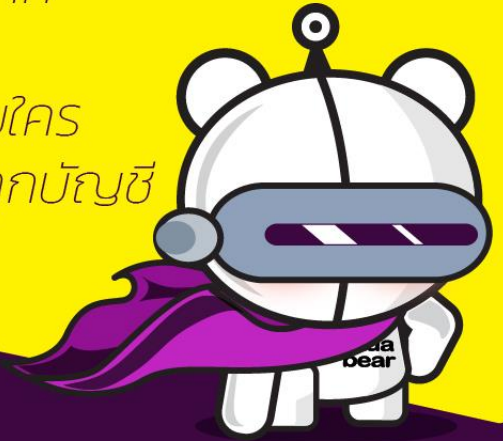
ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

<https://www.etda.or.th/>

PASSWORD

พาสเวิร์ด รหัสผ่าน

ตั้งให้ยาก
จำให้ได้
ไม่แชร์กับใคร
อย่าใช้ซ้ำทุกบัญชี



อย่างน้อย
ควรมี **8 ตัวอักษร**



เดายาก
ไม่เป็นคำจากพจนานุกรม



ไม่ใช่ซ้ำกัน
ในบัญชีต่าง ๆ

112233

ไม่เป็นตัวเลข
หรือตัวอักษรเรียงกัน
หรือซ้ำกัน เช่น abcd1111



ใช้การ**ยืนยัน 2 ขั้นตอน**
หรือหลายขั้นตอน



ไม่ใช่พาสเวิร์ดหรือ
default password
ที่ตั้งค่ามาตั้งแต่แรก



ระวังอีเมลฟิชซิง
หลอกให้เปลี่ยนพาสเวิร์ด
โดยให้คลิกลิงก์



ไม่ใช่ข้อมูลส่วนตัว
เช่น วันเดือนปีเกิด
เบอร์โทร.



พิจารณา**ใช้งาน**
ซอฟต์แวร์ช่วยจัดการ
พาสเวิร์ด



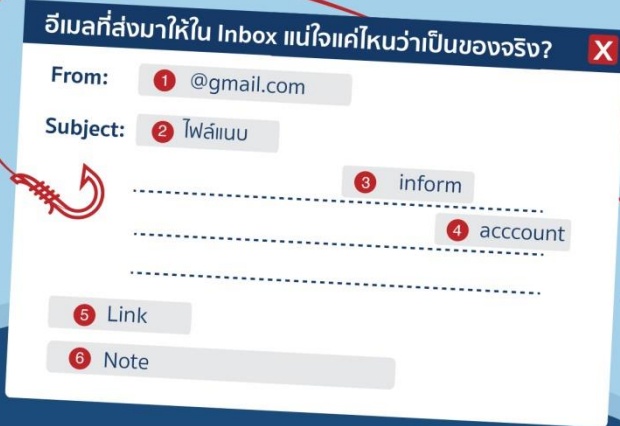
ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

<https://www.eta.or.th/>

จับผิดอีเมลลวงให้ตกเป็นเหยื่อ **ฟิชซิง**

Phishing (ฟิชซิง) คือ

การปลอมแปลงอีเมลให้เหมือนว่าส่งมาจากหน่วยงาน องค์กร หรือสถาบันที่มีชื่อเสียง เพื่อหลอกให้เหยื่อหลงกลใส่ข้อมูลสำคัญส่วนตัว จากนั้น ก็จะนำข้อมูลที่ได้จากเราไปสวมรอยสร้างความเสียหายที่เกี่ยวข้องกับเรื่องเงิน



ลักษณะที่น่าสงสัยของฟิชซิงอีเมล

- 1 อีเมลที่ไม่น่าเชื่อถือ
- 2 มีไฟล์แนบมาด้วยเช่น .zip
- 3 ไม่มีการระบุชื่อ-นามสกุล หรือข้อมูลสำคัญ
- 4 มีคำสะกดผิด
- 5 มีลิงก์ที่น่าสงสัย
- 6 มีข้อความแจ้งเตือนว่า ด่วน หรือสำคัญมาก



บัญชีอีเมลแบบไหนคือเป้าหมาย?



บัญชีอีเมลที่ไม่มีการเคลื่อนไหวเกิน 6 เดือน



บัญชีที่ใช้ล็อกอินหลาย ๆ แอคเคาท์



บัญชีธุรกิจติดต่องานสำคัญ



บัญชีที่ไม่เคยเปลี่ยนรหัสผ่าน

‘คิดก่อนพิมพ์’ ลดโอกาสตกเป็นเหยื่อฟิชซิงได้

ข้อมูลส่วนตัวต่อไปนี้ ควรถูกคิดให้ดีก่อนพิมพ์ลงบนสื่อออนไลน์



เลขบัตรประชาชน



รหัสผ่านอีเมล



รหัสผ่านบัญชีออนไลน์



หมายเลขบัตรเครดิต และรหัส 3 หลักหลังบัตร



etda.thailand



ThaiCERT



Thaicert.or.th



ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

<https://www.etda.or.th/>

แนวทาง รับมือมัลแวร์เรียกค่าไถ่ ransomware สำหรับหน่วยงานของรัฐ



มาตรการพื้นฐานสำหรับเตรียมความพร้อม
ในการรับมือภัยคุกคามทางไซเบอร์

กรณีมัลแวร์เรียกค่าไถ่ สำหรับหน่วยงานของรัฐ

1. จัดทำหรือทบทวนแผนนโยบายและแนวปฏิบัติงาน
2. สำรองข้อมูลที่สำคัญ
3. ควบคุมการเข้าถึงเครือข่าย และระบบสารสนเทศ
4. ประเมินความเสี่ยงด้านระบบสารสนเทศ
5. จัดเก็บบันทึกกิจกรรม (Log) ไปยังพื้นที่จัดเก็บในส่วนกลาง
6. ทบทวน และยกเลิกบริการที่ไม่จำเป็นบนเครื่องให้บริการ
7. กำหนดเจ้าหน้าที่ประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับบริหารกับระดับปฏิบัติการ
8. ให้ความรู้กับผู้ใช้งานในหน่วยงานเกี่ยวกับการป้องกันตนเองจากการติดมัลแวร์เรียกค่าไถ่



แนวทางการดำเนินการรับมือสถานการณ์ กรณีหน่วยงานของรัฐพบความเสียหาย ที่เกิดขึ้นจากมัลแวร์เรียกค่าไถ่

1. ตัดการเชื่อมต่อทางเครือข่าย
2. สำรองข้อมูลที่ยังใช้งานได้อยู่จากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์

หากพบความเสียหาย ที่เกิดขึ้นจากมัลแวร์เรียกค่าไถ่



- แจ้งเหตุไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และไทยเซิร์ต (ทางอีเมล report@thaicert.or.th)
- เปลี่ยนรหัสผ่านที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงรหัสผ่านที่ใช้งานผ่านระบบควบคุมบัญชีผู้ใช้งานทั้งหมด
- ตรวจสอบสายพันธุ์ของมัลแวร์เรียกค่าไถ่โดยอาศัยข้อมูลที่ปรากฏในเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ เช่น บัญชีของไฟล์ที่เปลี่ยนไป ข้อความที่ปรากฏบนหน้าจอ เพื่อประเมินวิธีการแก้ไขปัญหา เช่น การกู้คืนข้อมูล
- หากประสงค์ใช้เครื่องมือถอดรหัสลับข้อมูล ควรทำในสภาพแวดล้อมที่ไม่มีการเชื่อมต่อทางเครือข่าย เพื่อลดความเสี่ยงที่อาจเกิดจากการใช้เครื่องมือดังกล่าว

อ่านรายละเอียดเพิ่มเติมที่นี้



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

GO
DIGITAL
with
ETDA

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

<https://www.eta.or.th/>



พฤติกรรมเสี่ยงใช้งาน LINE

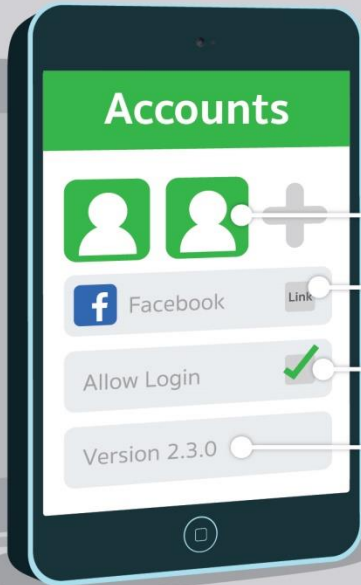
ที่ง่ายต่อการสวมรอยบัญชี

การโดนสวมรอยบัญชี LINE ไม่ใช่เรื่องไกลตัวอีกต่อไป หากคุณมีพฤติกรรมการใช้งานส่วนใหญ่ เข้าข่ายกรณีเหล่านี้

อีเมลที่ใช้ลงทะเบียน
ไม่ใช่อีเมลที่ล็อกอินทุกวัน



ใช้รหัสผ่านที่คาดเดาง่าย



เพิ่มคนที่ไม่รู้จักมาไว้ในรายชื่อ



เชื่อมต่อกับ Facebook ด้วยอีเมล
และรหัสผ่านชุดเดียวกัน

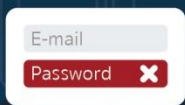


อนุญาตให้ล็อกอินหลาย ๆ อุปกรณ์ได้



ละเลยการอัปเดตซอฟต์แวร์

สัญญาณเตือนว่า กำลังมีใครใช้งานบัญชีคุณอยู่



ล็อกอินไม่ได้
แจ้งว่ารหัสผ่านผิด



พบข้อความแจ้งเตือน
ว่ามีคนอื่นล็อกอิน



เจอข้อความ
ที่เราไม่ได้พิมพ์



ใช้งานอยู่ แล้วบัญชี
เด็งกลับไปที่หน้าล็อกอิน



ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

<https://www.eta.or.th/>

สัญญาณแปลก ๆ จากอุปกรณ์ไอที มีความหมายว่าอะไรบ้างนะ ?



หนึ่งในปัญหาไอทีของคุณ เป็นแบบนี้หรือเปล่า ?



ติดไวรัสหรือมัลแวร์



หน้าจอฟ้า



ฮาร์ดแวร์เสีย



โปรแกรมค้าง



เว็บเพจออนไลน์



มีเสียงแปลก ๆ ขณะใช้งาน

รู้หรือไม่ อาการเหล่านี้ จะไม่เกิดขึ้นแน่ แค่ปรับพฤติกรรมการใช้ใหม่ และทำให้ได้ทุกวัน



ปิดการใช้งาน WiFi ทุกครั้ง เพื่อลดความเสี่ยง จากถูกขโมยข้อมูลทางออนไลน์

ตั้งรหัสผ่าน Login เข้าสู่คอมพิวเตอร์ ก่อนเข้าสู่หน้า desktop



หมั่นอัปเดตซอฟต์แวร์ ให้เป็นเวอร์ชันล่าสุด

ไม่คลิกเว็บไซต์แปลก ๆ หรือคลิก โฆษณาที่ไม่คุ้นเคย

ติดตั้งโปรแกรม แอนติไวรัส ที่ถูกลิขสิทธิ์



ก่อนเน็ตเสิร์จ อย่าลืมลบประวัติการเข้าชม

ตรวจสอบเว็บหรือไฟล์ว่ามีไวรัส โดยอัปโหลดหรือนำลิงก์มาตรวจสอบ ที่เว็บไซต์ virustotal.com

ไม่พินไปต่อ !

หากเบราว์เซอร์แจ้งเตือน เว็บไซต์อันตราย

facebook แฮร์ข้อมูลส่วนตัวมากไปใช้จะดี

ใคร ๆ ก็มองว่า Facebook คือ พื้นที่ส่วนตัว จึงกล้าแฮร์ กล้าโพสต์เรื่องเกี่ยวกับตัวเองหลายอย่าง อาจหลงลืมไปว่า ที่จริงแล้ว มันไม่ได้ปลอดภัยอย่างที่เราคิด ควรเปิดเผยแต่พอเหมาะสมดีกว่า



เพจสาธารณะ

ข้อมูลส่วนตัว
ที่มีจะ **โดนสวมรอยได้** ง่าย



เพจส่วนตัว

ใส่ชื่อที่เป็นทางการ

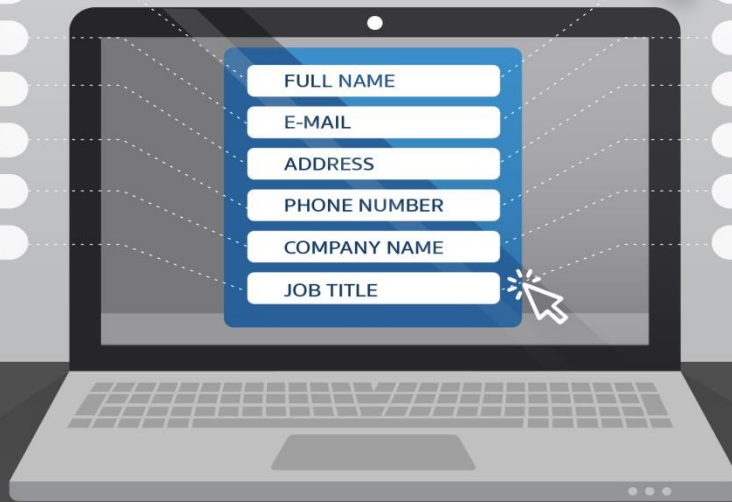
อีเมลหลัก

ที่อยู่สำนักงาน

เบอร์โทรศัพท์

ชื่อบริษัท หรือธุรกิจ

อธิบายเกี่ยวกับองค์กร



ชื่อ-นามสกุลจริง

อีเมล

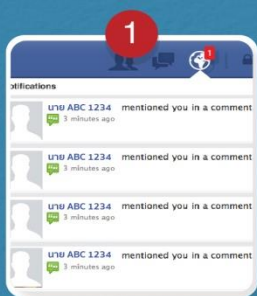
แฮร์บางโอกาสดีกว่า

ไม่ควรระบุลงไป

บริษัทปัจจุบันที่ทำงานอยู่

ตำแหน่งงานปัจจุบัน

อาการที่ Facebook ฟ้องว่า กำลังมีคนกำลังสวมรอยเป็นคุณ



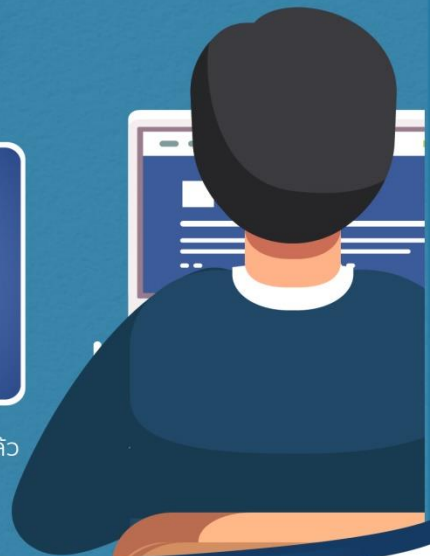
1
แจ้งเตือนข้อความว่า
“มีคนกล่าวถึงคุณในความ
คิดเห็น” ที่คุณไม่ได้โพสต์ต่อ



2
ได้รับ SMS แจ้ง
การล็อกอินที่ไม่ใช่คุณ



3
เปิดหน้า Facebook แล้ว
ให้กลับมาใส่รหัส
ผ่านอีกครั้ง



ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

<https://www.eta.or.th/>

เทคนิคดูแลคอมพิวเตอร์ส่วนตัว ให้ใช้งานปลอดภัย ไม่ถูกขโมยข้อมูล

หลายคนตระหนักดีว่าคอมพิวเตอร์ คือ อุปกรณ์สำคัญ
สำหรับการทำงาน แต่คนส่วนใหญ่กลับมองข้ามเรื่องการหมั่นดูแลตรวจเช็ค
ความผิดปกติ ทำให้นานวันไปคอมพิวเตอร์ที่ใช้เป็นประจำมักเกิดปัญหาบ่อย ๆ



ติดไวรัส



ใช้งานได้ไม่เสถียร



ข้อมูลสำคัญรั่วไหล

มาดูกันว่า **หากจะยืดอายุคอมพิวเตอร์**
ให้ใช้งานได้อย่างปลอดภัยนาน ๆ ควรทำอย่างไรบ้าง?

ควรทำ ทุกวัน



ใช้รหัสผ่านหรือ Pin
เพื่อ Log in ใช้งาน



เริ่มโปรแกรมสแกนไวรัส
ก่อนเริ่มต้นใช้งานโปรแกรมอื่น



ล้างคำค้นหาในเว็บเบราว์เซอร์
ที่ใช้งานในแต่ละวัน



Log Out บัญชีออนไลน์
ทุกบัญชี หลังการใช้งาน

ควรทำ เป็นประจำ

อัปเดตซอฟต์แวร์
ให้อยู่ในเวอร์ชันล่าสุด



ลบโปรแกรม หรือ ซอฟต์แวร์
ที่ไม่จำเป็นต้องใช้งาน



สำรองข้อมูลสำคัญไว้กับ
อุปกรณ์ที่มีความปลอดภัย



ตั้งค่าบัญชีโซเชียล โดยจำกัดสิทธิ์
การเข้าถึง เพื่อความปลอดภัย



จะเกิดอะไรขึ้น ? ...



ถ้า รหัสผ่านอีเมลส่วนตัว
ตกอยู่ในมือผู้ไม่หวังดี



มาดูกันว่า โจรไซเบอร์จะทำอะไรกับบัญชีอีเมลของคุณ



ถูกค้นจดหมาย
ใน Inbox



แอบสอดแนมบัญชี
My Account Info



โดนสวมรอยบัญชี
เพื่อนำข้อมูลไปใช้ต่อ



หาอีเมลยืนยันรหัสผ่าน
ของเพจโซเชียลอื่น ๆ



ชื่อ-นามสกุลจริง



เบอร์โทรศัพท์



ค้นหาอีเมล
ที่มีแนบไฟล์



คอยส่งความ
เคลื่อนไหวบัญชี



อ่านข้อมูลอีเมล
ที่ถูกส่งเข้ามา



ข้อมูลส่วนอื่น ๆ



ส่งเมลแนบไวรัส
ให้เพื่อนที่อยู่ในลิสต์



ส่งจดหมาย
หลอกลวงเงิน

รหัสผ่านอีเมลไม่โดนแฮกแน่ แต่ใส่ไว้วิธีใช้งานที่ปลอดภัย



หมั่นเปลี่ยนรหัสผ่าน
ทุก ๆ 3 เดือน



ตั้งค่าการยืนยันตัวตน
แบบ 2 ขั้นตอน
thcert.co/8dWiQx



ไม่ล็อกอินอีเมล
ด้วย Wi-Fi สาธารณะ



แยกอีเมลเรื่องธุรกิจ
และอีเมลส่วนตัว



etda.thailand



ThaiCERT



Thaicert.or.th



ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

<https://www.eta.or.th/>