การเสริมสร้างความตระหนัก ในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ

สำนักงานพัฒนาชุมชนจังหวัดยะลา

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

แบ็กอัปข้อมูลไว้ก่อน
เพราะถ้าหายไป เสียเงินเท่าไร... ก็อาจไม่ได้คืนมา

สำหรับ SMEs

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

การโจมตีภาคธุรกิจด้วยมัลแวร์เรียกค่าไถ่

ซึ่งจะล็อกข้อมูลในเครื่อง เช่น เอกสาร รูปภาพ ทำให้เปิดใช้งานไม่ได้เพื่อเรียกค่าไถ่
และแม้จ่ายค่าไถ่ไปแล้ว**ก็ไม่ได้รับประกัน**ว่าจะได้ข้อมูลนั้นคืนมา

แบ็กอัปแบบไหน...ถามใจเธอดู?

วิธีเก็บ	ข้อดี	ข้อเสีย
บริการ Cloud เช่น Google Drive, Dropbox, OneDrive	ใช้ง่าย ฟรี เข้าที่ไหนก็ได้ แบ็กอัปอัตโนมัติได้	ต้องมีอินเทอร์เน็ต มีความเสี่ยงปิดบริการ
อุปกรณ์เก็บข้อมูลแบบพกพา เช่น DVD, ฮาร์ดดิสก์, Flash Drive	ใช้ง่าย เก็บรักษาในที่ปลอดภัย พกติดตัวได้	มีโอกาสสูญหายหรือเสียหาย
พิมพ์เป็นกระดาษ	ไม่ขึ้นต่อฮาร์ดแวร์ ป้องกันการถูกเจาะข้อมูล	จัดการยาก ไม่ดีต่อสิ่งแวดล้อม
NAS (Network-attached storage)	เก็บข้อมูลจากคอมพิวเตอร์หลายเครื่อง พร้อมกันได้ แบ็กอัปอัตโนมัติได้	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.etda.or.th

ThaiCERT Thailand Computer Emergency Response Team a member of ETDA
ETDA สพธอ www.etda.or.th
กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม
GO DIGITAL with ETDA

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
https://www.etda.or.th/

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

คลิกเปลี่ยนชีวิต ระวังสักนิดก่อนติดมัลแวร์

หลาย ๆ คนอาจเคยคลิกเข้าไปดูข่าวหรือเล่น quiz ใน Facebook แล้วเกิดเหตุบัญชีผู้ใช้อัปสเตตัสประหลาด ทำให้คุณอับอาย บางคนถึงกับปิดบัญชีผู้ใช้ไปเพราะติดมัลแวร์ แล้วจะมีวิธีในการรับมือปัญหานี้อย่างไรกันดี

ติดมัลแวร์ ได้อย่างไร?

โพสต์ต่างๆ ที่ชวนคลิกให้เข้าไปดูเพื่อหลอกให้ติดมัลแวร์

ลิงก์แปลก ๆ ที่แชร์มาจากเพื่อน
ลิงก์จากเพื่อนในช่องแชตและหน้าวอลล์เพื่อน

ลิงก์ควิซ
แผงตัวมาในรูปแบบแอป / Quiz ปลอม

เพจแชร์ข่าวและคลิป
ลิงก์ข่าวปลอมหรือคลิปลามก

ติดแล้ว เกิดอะไรบ้าง?

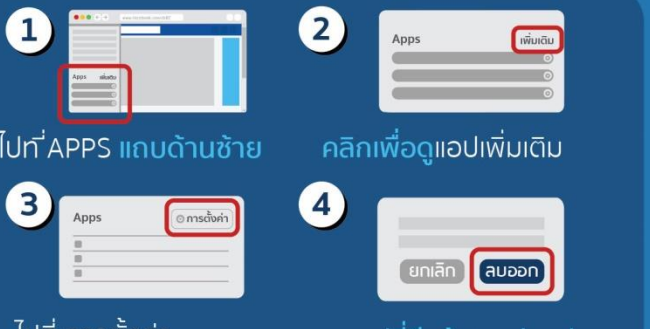
โพสต์ข้อความต่าง ๆ ลงในกลุ่ม
หรือหน้าวอลล์ของคุณโดยไม่รู้ตัว

อาจถูกขโมยข้อมูล
ส่วนตัว

เพื่อนของคุณอาจติดมัลแวร์
ต่อจากคุณ

ติดแล้ว แก้อย่างไร?

เพิ่มมาตรการความปลอดภัย!
ควรเปลี่ยนรหัสผ่านบัญชีผู้ใช้งาน



1. ไปที่ APPS แถบด้านซ้าย
2. คลิกเพื่อดูแอปเพิ่มเติม
3. ไปที่ การตั้งค่า
4. หาแอปที่มีหน้าตาแปลกปลอม แล้วลบออกจากรายการ

เล่นโซเชียลอย่างฉลาด ไม่ตกเป็นทาสพวกมัลแวร์

etda.thailand ThaiCERT Thaicert.or.th

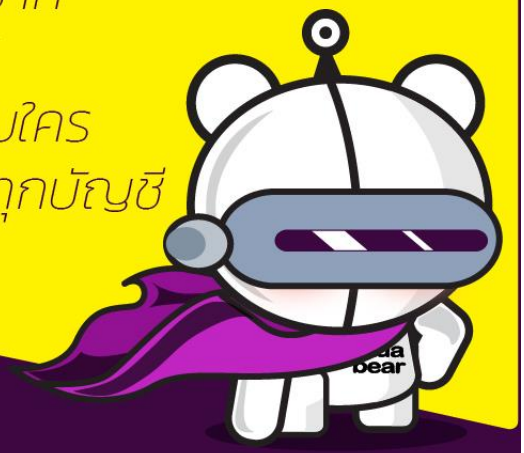
ThaiCERT ETDA ICT

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

PASSWORD
พาสเวิร์ด
รหัสผ่าน

ตั้งให้ยาก
จำให้ได้
ไม่แชร์กับใคร
อย่าใช้ซ้ำทุกบัญชี



••••••••••

อย่างน้อย
ควรมี ***8 ตัวอักษร***

เดายาก
ไม่เป็นคำจากพจนานุกรม

112233

ไม่เป็นตัวเลข
หรือตัวอักษร***เรียงกัน***
หรือซ้ำกัน เช่น abcd1111

ไม่ใช้พาสเวิร์ดหรือ
default password
ที่ตั้งค่ามาตั้งแต่แรก

ไม่ใช้ข้อมูลส่วนตัว
เช่น วันเดือนปีเกิด
เบอร์โทร.

ไม่ใช้ซ้ำกัน
ในบัญชีต่าง ๆ

ใช้การ***ยืนยัน 2 ขั้นตอน***
หรือหลายขั้นตอน

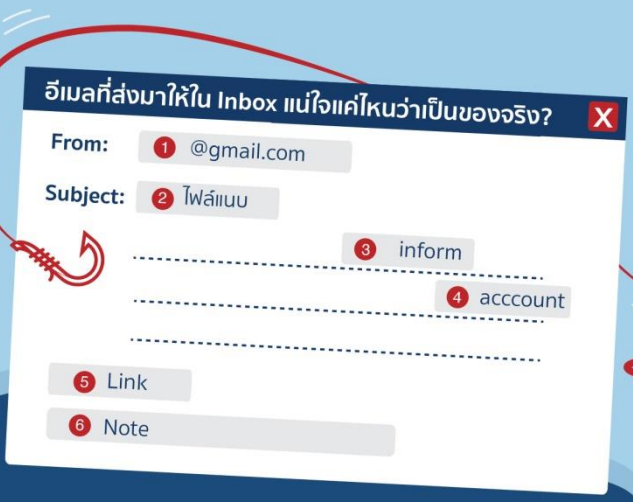
ระวังอีเมลฟิชชิง
หลอกให้เปลี่ยนพาสเวิร์ด
โดยให้คลิกลิงก์

พิจารณา***ใช้งาน***
ซอฟต์แวร์ช่วยจัดการ
พาสเวิร์ด

ThaiCERT Thailand Computer Emergency Response Team a member of ETDA
ETDA สพธอ www.etda.or.th

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
https://www.etda.or.th/

จับผิดอีเมลลวงให้ตกเป็นเหยื่อฟิชชิง



Phishing (ฟิชชิง) คือ

การปลอมแปลงอีเมลให้เหมือนว่าส่งมาจากหน่วยงาน องค์กร หรือสถาบันที่มีชื่อเสียง เพื่อหลอกให้เหยื่อหลงกลใส่ข้อมูลสำคัญส่วนตัว จากนั้น ก็จะนำข้อมูลที่ได้จากเราไปสวมรอยสร้างความเสียหายที่เกี่ยวข้องกับเรื่องเงิน

ลักษณะที่น่าสงสัยของฟิชชิงอีเมล

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

บัญชีเมลแบบไหนคือเป้าหมาย?

- บัญชีเมลที่ไม่มีการเคลื่อนไหวเกิน 6 เดือน
- บัญชีที่ใช้ล็อกอินหลาย ๆ แอคเคาท์
- บัญชีธุรกิจติดต่องานสำคัญ
- บัญชีที่ไม่เคยเปลี่ยนรหัสผ่าน

'คิดก่อนพิมพ์' ลดโอกาสตกเป็นเหยื่อฟิชชิงได้

ข้อมูลส่วนตัวต่อไปนี้ ควรฉุกคิดให้ดีก่อนพิมพ์ลงบนสื่อออนไลน์


เลขบัตรประชาชน


รหัสผ่านอีเมล


รหัสผ่านบัญชีออนไลน์


หมายเลขบัตรเครดิตและรหัส 3 หลักหลังบัตร

etda.thailand ThaiCERT Thaicert.or.th

ThaiCERT ETDA ICT

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

แนวทาง รับมือมัลแวร์เรียกค่าไถ่ ransomware สำหรับหน่วยงานของรัฐ

มาตรการพื้นฐานสำหรับเตรียมความพร้อม ในการรับมือภัยคุกคามทางไซเบอร์

กรณีมัลแวร์เรียกค่าไถ่ สำหรับหน่วยงานของรัฐ

1. **จัดทำหรือทบทวนแนวนโยบาย**และแนวปฏิบัติงาน
2. **สำรองข้อมูลที่สำคัญ**
3. **ควบคุมการเข้าถึงเครือข่าย** และระบบสารสนเทศ
4. **ประเมินความเสี่ยง**ด้านระบบสารสนเทศ
5. จัดเก็บ**บันทึกกิจกรรม (Log) ไปยังพื้นที่จัดเก็บในส่วนกลาง**
6. ทบทวน และ**ยกเลิกบริการที่ไม่จำเป็นบนเครื่องให้บริการ**
7. **กำหนดเจ้าหน้าที่ประสานงาน**ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับบริหารกับระดับปฏิบัติการ
8. ให้ความรู้กับผู้ใช้งานในหน่วยงานเกี่ยวกับการป้องกันตนเองจากการติดมัลแวร์เรียกค่าไถ่

แนวทางการดำเนินการรับมือสถานการณ์

กรณีหน่วยงานของรัฐพบความเสียหาย ที่เกิดขึ้นจากมัลแวร์เรียกค่าไถ่

1. ตัดการเชื่อมต่อทางเครือข่าย
2. สำรองข้อมูลที่ยังใช้งานได้อยู่จากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์

หากพบความเสียหาย ที่เกิดขึ้นจากมัลแวร์เรียกค่าไถ่

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

อ่านรายละเอียดเพิ่มเติมที่นี่

ThaiCERT a member of ETDA | ETDA สพธอ. www.etda.or.th | กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

GO DIGITAL with ETDA

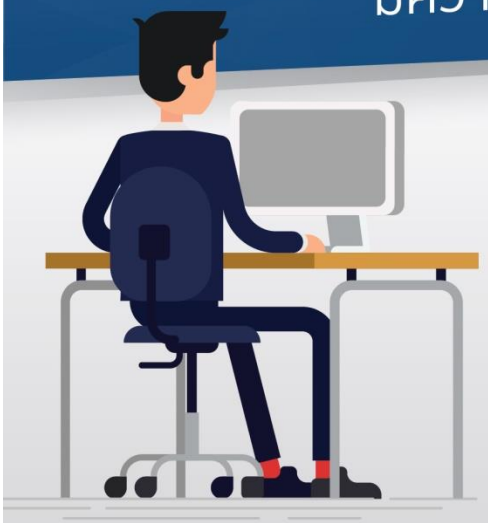
ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

สัญญาณแปลก ๆ จากอุปกรณ์ไอที มีความหมายว่าอะไรบ้างนะ ?



หนึ่งในปัญหาไอทีของคุณ เป็นแบบนี้หรือเปล่า ?

ติดไวรัสหรือมัลแวร์

หน้าจอฟ้า

ฮาร์ดแวร์เสีย

โปรแกรมค้าง

เว็บเพจซ้อนหลายอัน

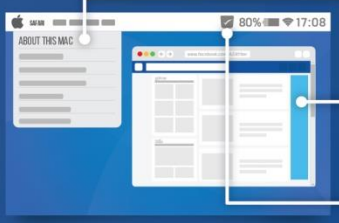
มีเสียงแปลก ๆ ขณะใช้งาน

รู้หรือไม่ อาการเหล่านี้ จะไม่เกิดขึ้นแน่

แค่ปรับพฤติกรรมการใช้ใหม่ และทำให้ได้ทุกวัน

ปิดการใช้งาน WiFi ทุกครั้ง เพื่อลดความเสี่ยงจากถูกขโมยข้อมูลทางออนไลน์

ตั้งรหัสผ่าน Login เข้าสู่คอมพิวเตอร์ก่อนเข้าสู่หน้า desktop



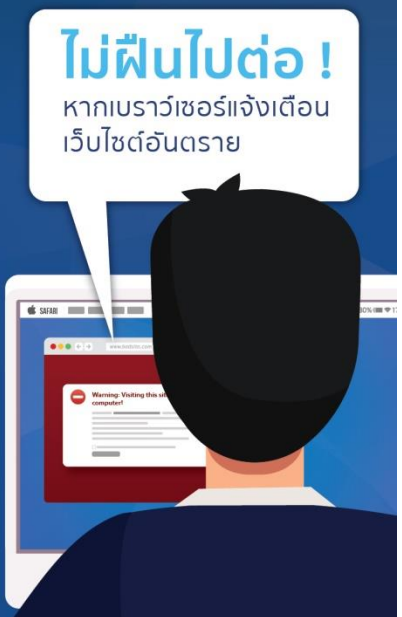
หมั่นอัปเดตซอฟต์แวร์ ให้เป็นเวอร์ชันล่าสุด

ไม่คลิกเว็บไซต์แปลก ๆ หรือคลิกโฆษณาที่ไม่คุ้นเคย

ติดตั้งโปรแกรม แอนติไวรัส ที่ถูกลิขสิทธิ์

ท่องเน็ตเสร็จ **อย่าลืมลบประวัติการเข้าเว็บ**

ตรวจสอบเว็บหรือไฟล์ว่ามีไวรัส
โดยอัปโหลดหรือนำลิงก์มาตรวจสอบที่เว็บไซต์ virustotal.com



etda.thailand ThaiCERT Thaicert.or.th

ThaiCERT ETDA ICT

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

facebook แชร์ข้อมูลส่วนตัวมากไปใช่จะดี

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

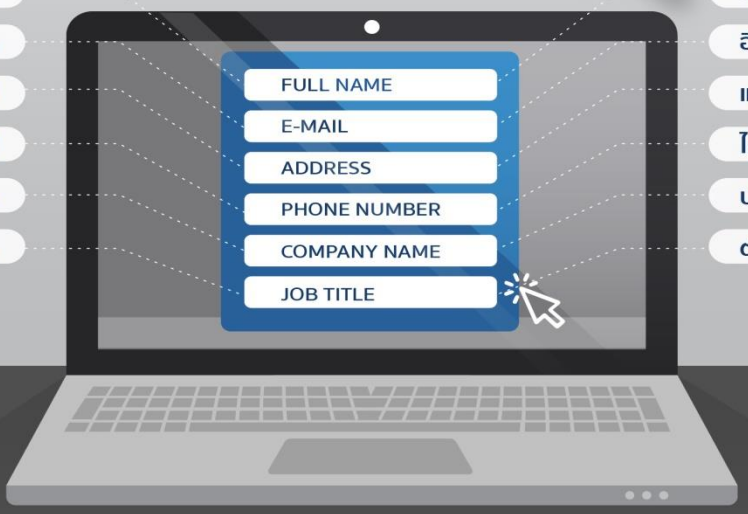
ข้อมูลส่วนตัว ที่มักจะโดนสวมรอยได้ง่าย

เพจสาธารณะ

- ใส่ชื่อที่เป็นทางการ
- อีเมลหลัก
- ที่อยู่สำนักงาน
- เบอร์โทรศัพท์
- ชื่อบริษัท หรือธุรกิจ
- อธิบายเกี่ยวกับองค์กร

เพจส่วนตัว

- ชื่อ-นามสกุลจริง
- อีเมล
- แชร์บางโอกาสดีกว่า
- ไม่ควรระบุลงไป
- บริษัทปัจจุบันที่ทำงานอยู่
- ตำแหน่งงานปัจจุบัน



อาการที่ Facebook ฟ้องว่า กำลังมีคนกำลังสวมรอยเป็นคุณ

แจ้งเตือนข้อความว่า "มีคนกล่าวถึงคุณในความคิดเห็น" ที่คุณไม่ได้โพสต์เอง

ได้รับ SMS แจ้งการล็อกอินที่ไม่ใช่คุณ

เปิดหน้า Facebook แล้วให้กลับมาใส่รหัสผ่านอีกครั้ง

etda.thailand ThaiCERT Thaicert.or.th

ThaiCERT ETDA ICT

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
https://www.etda.or.th/

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

จะเกิดอะไรขึ้น ? ...

ถ้า รหัสผ่านอีเมลส่วนตัว ตกอยู่ในมือผู้ไม่หวังดี

มาดูกันว่า โจรไซเบอร์จะทำอะไรกับบัญชีอีเมลของคุณ

- ถูกค้นจดหมายใน Inbox
- แอบสอดแนมบัญชี My Account Info
- โดนสวมรอยบัญชีเพื่อนำข้อมูลไปใช้ต่อ
- หาอีเมลยืนยันรหัสผ่านของเพจโซเชียลอื่น ๆ
- ชื่อ-นามสกุลจริง
- เบอร์โทรศัพท์
- ค้นหาอีเมลที่มีแนบไฟล์
- คอยส่องความเคลื่อนไหวบัญชี
- อ่านข้อมูลอีเมลที่ถูกส่งเข้ามา
- ข้อมูลส่วนอื่น ๆ
- ส่งเมลแนบไวรัสให้เพื่อนที่อยู่ในลิสต์
- ส่งจดหมายหลอกลวงเงิน

รหัสผ่านอีเมลไม่โดนแฮกแน่ แค่ใส่ใจวิธีใช้งานที่ปลอดภัย

- หมั่นเปลี่ยนรหัสผ่านทุก ๆ 3 เดือน
- ตั้งค่าการยืนยันตัวตนแบบ 2 ขั้นตอน thcert.co/8dWiQx
- ไม่ล็อกอินอีเมลด้วย Wi-Fi สาธารณะ
- แยกอีเมลเรื่องธุรกิจและอีเมลส่วนตัว

etda.thailand ThaiCERT Thaicert.or.th

ThaiCERT ETDA ICT

ที่มา ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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