รายงานการโจมตีทางไซเบอร์ และเหตุการณ์ต่าง ๆ เพื่อให้ออสเตรเลียปลอดภัย

สมัคร

รับบริการแจ้งเตือนฟรีของเราที่
cyber.gov.au

รายงาน

อาชญากรรมทางไซเบอร์ไปที่
REPORTCYBER:
cyber.gov.au/report

ติดต่อ

โทร1300 CYBER1 หรือไปที่
cyber.gov.au
หมายเลขนี้มีไว้สำหรับใช้ภายในออสเตรเลียเท่านั้น

ติดตามเราได้ที่

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. ระวังสแกม

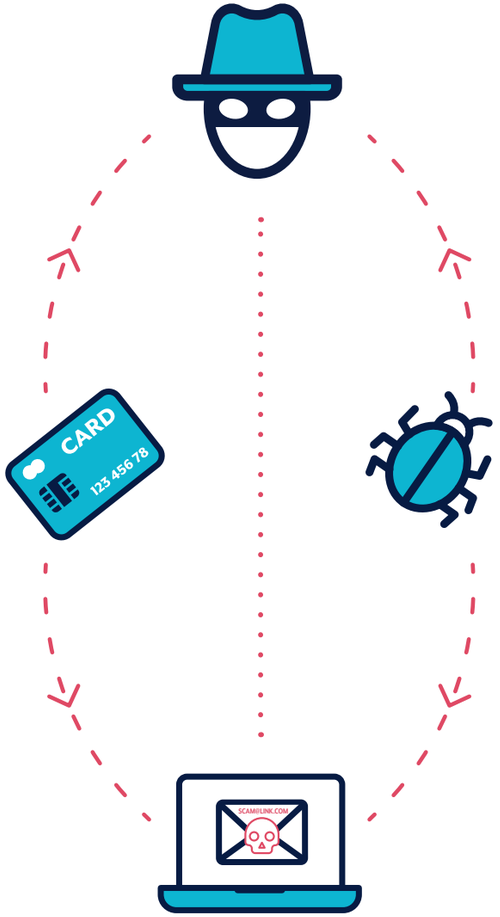
อาชญากรไซเบอร์ใช้อีเมล SMS โทรศัพท์ และโซเชียลมีเดียเพื่อหลอกลวงให้คุณเปิดไฟล์แนบ เยี่ยมชมเว็บไซต์ เปิดเผยรายละเอียดการเข้าสู่ระบบบัญชี เปิดเผยข้อมูลที่ละเอียดอ่อน หรือโอนเงินหรือบัตรของขวัญ ข้อความเหล่านี้ ทำให้ดูเหมือนว่าส่งมาจากบุคคลหรือองค์กรที่คุณคิดว่ารู้จักหรือคุณคิดว่าควรไว้วางใจ

ในการตรวจจับข้อความสแกม ให้หยุดและคิดว่า

- **ผู้มีอำนาจ** มีการอ้างว่า ข้อความนั้นมาจากเจ้าหน้าที่อย่างเป็นทางการหรือไม่?
- **ความเร่งด่วน** คุณได้รับแจ้งว่าคุณมีเวลาจำกัดในการตอบสนองหรือไม่?
- **อารมณ์** ข้อความนั้นทำให้คุณตื่นตระหนก หวาดกลัว มีความหวัง หรืออยากรู้อยากเห็นหรือไม่?
- **ความขาดแคลน** ข้อความนั้นนำเสนอสิ่งที่ขาดแคลนหรือไม่?
- **เหตุการณ์ปัจจุบัน** ข้อความนั้นเกี่ยวข้องกับเรื่องราวของข่าวปัจจุบัน เหตุการณ์สำคัญ หรือช่วงเวลาเฉพาะของปี (เช่น การรายงานภาษี) หรือไม่?

ในการตรวจสอบว่าข้อความนั้นถูกต้องแท้จริงหรือไม่

- ให้กลับไปยังบางสิ่งที่คุณไว้ใจได้ เยี่ยมชมเว็บไซต์ทางการ เข้าสู่ระบบบัญชีของคุณ หรือโทรไปที่หมายเลขโทรศัพท์ที่โฆษณาไว้ อย่าใช้ลิงก์หรือรายละเอียดการติดต่อในข้อความที่คุณได้รับหรือมาทางโทรศัพท์
- ตรวจสอบดูว่าแหล่งที่เป็นทางการนั้นได้แจ้งคุณไว้แล้วหรือไม่ว่า พวกเขาจะไม่ถามคุณเรื่องอะไรบ้าง ตัวอย่างเช่น ธนาคารของคุณอาจแจ้งคุณไว้แล้วว่าพวกเขาจะไม่ถามรหัสผ่านของคุณ



สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจจับข้อความสแกม โปรดดูเอกสารเผยแพร่ชื่อ Detecting Socially Engineered Messages ของศูนย์การรักษาความปลอดภัยทางไซเบอร์ออสเตรเลีย หรือ Australian Cyber Security Center (ACSC) และรับทราบข้อมูลโดยสมัครใช้บริการแจ้งเตือนของ ACSC บนเว็บไซต์ **cyber.gov.au.**

ขั้นตอนง่าย ๆ ในการรักษาความปลอดภัยให้กับอุปกรณ์และบัญชีของคุณ

ลดความเสี่ยงของการตกเป็นเป้าหมายของอาชญากรไซเบอร์โดยทำตามขั้นตอนต่อไปนี้

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. อัปเดตอุปกรณ์ของคุณ

อาชญากรไซเบอร์สามารถแฮก (Hack) เข้าอุปกรณ์โดยใช้จุดอ่อนที่ทราบจากในระบบหรือแอป การอัปเดตเป็นการพัฒนาการรักษาความปลอดภัยให้ดีขึ้ นเพื่อแก้ไขจุดอ่อนเหล่านี้ เปิดการอัปเดตอัตโนมัติเพื่อให้สิ่งนี้ เกิดขึ้ นโดยที่คุณไม่ต้องทำอะไร

เปิดการอัปเดตอัตโนมัติบนอุปกรณ์ทั้งหมดของคุณ

- โทรศัพท์มือถือ
- แล็ปท็อป
- เดสก์ท็อป

ตรวจสอบการอัปเดตเป็นประจำสำหรับ

- แอป
- โปรแกรมต่าง ๆ
- อุปกรณ์อัจฉริยะ

2. เปิดใช้งานการยืนยันตัวตนโดยใช้หลากหลายปัจจัย (MFA)

MFA จะปรับปรุงระบบการรักษาความปลอดภัยของคุณ โดยทำให้อาชญากรไซเบอร์เข้าถึงไฟล์หรือบัญชีของคุณได้ยากขึ้ น

เปิดใช้งาน MFA โดยเริ่มจากบัญชีที่สำคัญที่สุดของคุณก่อน:

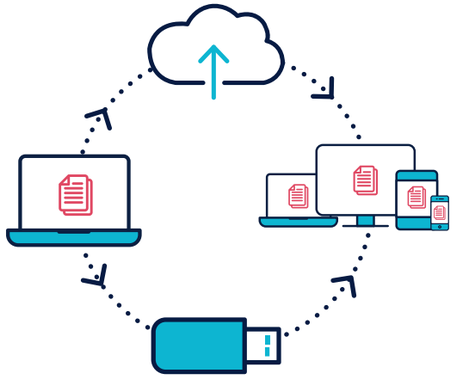
- บัญชีอีเมล
- ธนาคารออนไลน์และบัญชีที่มีรายละเอียดการชำระเงินที่เก็บไว้
- โซเชียลมีเดีย

3. สำรองข้อมูลในอุปกรณ์ของคุณ

การสำรองข้อมูลเป็นการทำสำเนาดิจิทัลของข้อมูลที่จัดเก็บไว้ในอุปกรณ์ของคุณ เช่น ภาพถ่าย เอกสาร วิดีโอ และข้อมูลจากแอปพลิเคชัน ซึ่งสามารถบันทึกลงในอุปกรณ์จัดเก็บข้อมูลภายนอกหรือระบบคลาวด์ (Cloud) ได้ การสำรองข้อมูลหมายความว่าคุณสามารถกู้คืนไฟล์ได้ในกรณีที่อุปกรณ์ของคุณสูญหาย ถูกขโมย หรือเสียหาย

สำรองข้อมูลในอุปกรณ์ของคุณเป็นประจำ

- โทรศัพท์มือถือ
- แล็ปท็อป
- เดสก์ท็อป
- แท็บเล็ต



4. ตั้งค่าข้อความรหัสผ่านที่ปลอดภัย

ในกรณีที่ไม่มี MFA ให้ใช้งาน ข้อความรหัสผ่านที่ปลอดภัยมักจะเป็นสิ่งเดียวที่สามารถปกป้องข้อมูลและบัญชีของคุณจากอาชญากรได้

ข้อความรหัสผ่านใช้คำสุ่มสี่คำขึ้ นไปเพื่อเป็นรหัสผ่านของคุณ เปลี่ยนรหัสผ่านของคุณเป็นข้อความรหัสผ่านโดยตรวจสอบให้แน่ใจว่า

- มีความยาว ยิ่งข้อความรหัสผ่านของคุณยาวเท่าไรก็ยิ่งดีเท่านั้ น ทำให้มีความยาวอย่างน้อย 14 ตัวอักษร
- คาดเดาไม่ได้ ใช้คำที่ไม่เกี่ยวข้องกันผสมกันแบบสุ่ม
- มีเอกลักษณ์ อย่าใช้ข้อความรหัสผ่านซ้ำกันหลายบัญชี