Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

การรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคล

ขั้นตอนแรก

cyber.gov.au

ชุดคู่มือการรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคล

คู่มือการรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคล : ขั้นตอนแรก เป็นคู่มือชุดแรกจากชุดคู่มือสามชุดที่ออกแบบมาเพื่อช่วยให้ชาวออสเตรเลียทั่วไปเข้าใจพื้นฐานของการรักษาความปลอดภัยทางไซเบอร์ เรียนรู้วิธีการที่คุณสามารถดำเนินการเพื่อป้องกันตนเองจากภัยคุกคามทางไซเบอร์ทั่วไป

ขั้นตอนแรก

ขั้นตอนต่อไป

ขั้นตอนขั้นสูง

สารบัญ

คำนำ

การรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคลคืออะไร?

ในโลกที่มีการขับเคลื่อนด้วยเทคโนโลยีเพิ่มมากขึ้นนี้ เราใช้อุปกรณ์และบัญชี ซึ่งมีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ทุกวัน ดังนี้

- อุปกรณ์ของคุณ อาจรวมถึงคอมพิวเตอร์ โทรศัพท์มือถือ แท็บเล็ต และอุปกรณ์เชื่อมต่ออินเทอร์เน็ตชนิดอื่น ๆ
- คุณยังอาจใช้บัญชีออนไลน์สำหรับอีเมล การธนาคาร การจับจ่ายซื้อของ โซเชียลมีเดีย การเล่นเกมหรือพนัน และอื่น ๆ

การรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคลเป็นขั้นตอนต่อเนื่องที่คุณสามารถนำไปใช้เพื่อปกป้องบัญชีและอุปกรณ์ของคุณจากภัยคุกคามทางไซเบอร์ได้

ภัยคุกคามทางไซเบอร์คืออะไร?

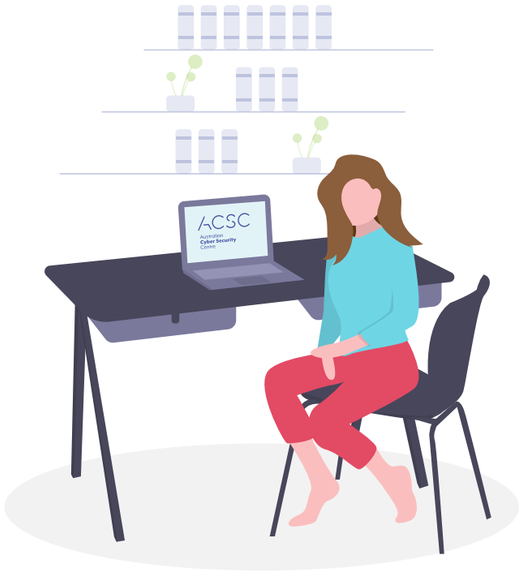
ภัยคุกคามทางไซเบอร์หลัก ๆ ที่ส่งผลกระทบต่อชาวออสเตรเลียทุกวันคือ **สแกม (Scam) และมัลแวร์ (Malware)**

- **มัลแวร์เป็นคำรวม ๆ ที่ใช้อธิบายซอฟต์แวร์ที่เป็นอันตราย** โดยออกแบบมาเพื่อก่อให้เกิดความเสียหาย ซึ่งอาจรวมถึง ไวรัส (Virus) เวิร์ม (Worm) สปายแวร์ (Spyware) โทรจัน (Trojan) และแรนซัมแวร์ (Ransomware) อาชญากรไซเบอร์ใช้มัลแวร์เพื่อขโมยข้อมูลและเงินของคุณ และควบคุมอุปกรณ์และบัญชีของคุณ
- **สแกมเป็นข้อความที่ส่งโดยอาชญากรไซเบอร์** โดยออกแบบมาเพื่อหลอกล่อให้คุณให้ข้อมูลสำคัญ หรือเพื่อเปิดใช้งานมัลแวร์บนอุปกรณ์ของคุณ

การโจมตีเหล่านี้อาจส่งผลกระทบต่อบุคคลเป็นการส่วนตัวและทางด้านการเงินที่มีนัยสำคัญต่อผู้ที่ตกเป็นเหยื่อ การโจมตีเหล่านี้ยังคงเกิดขึ้นด้วยความซับซ้อนและความถี่ที่เพิ่มมากขึ้น

คู่มือนี้จะช่วยปกป้องฉันจากภัยคุกคามทางไซเบอร์ได้อย่างไร?

หากคุณเพิ่งเริ่มเรียนรู้เกี่ยวกับการรักษาความปลอดภัยในโลกไซเบอร์เป็นครั้งแรก หรือกำลังจะอัปเดตตัวเองให้ทันต่อเหตุการณ์ คู่มือนี้เป็นจุดเริ่มต้นที่ดี คู่มือการรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคล: ขั้นตอนแรก เป็นคู่มือฉบับแรกจากชุดคู่มือสามฉบับที่ออกแบบมาเพื่อช่วยให้คุณเข้าใจพื้นฐานของการรักษาความปลอดภัยทางไซเบอร์

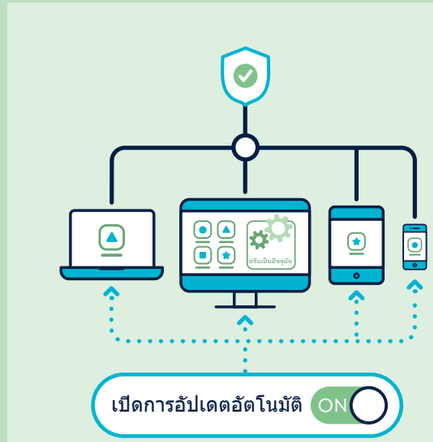


เปิดการอัปเดตอัตโนมัติ

การอัปเดตคืออะไร?

การอัปเดตคือการปรับซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุด (อันได้แก่ โปรแกรม แอป และระบบปฏิบัติการ) ที่คุณได้ติดตั้งบนคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของคุณ

- **การอัปเดตซอฟต์แวร์ช่วยปกป้องอุปกรณ์ของคุณ**ด้วยการแก้ไข ‘bug หรือจุดบกพร่อง’ ของซอฟต์แวร์ (ข้อผิดพลาดในการเข้ารหัสหรือช่องโหว่ต่อความเสี่ยงต่าง ๆ) อาชญากรไซเบอร์และมัลแวร์ สามารถใช้ ‹จุดบกพร่อง› เหล่านี้เพื่อเข้าถึงอุปกรณ์ของคุณและขโมยข้อมูลส่วนบุคคล บัญชีของคุณ ข้อมูลทางการเงินและตัวตนของคุณได้
- **อาชญากรไซเบอร์ค้นพบและมีการใช้ประโยชน์ ‘จุดบกพร่อง› ของซอฟต์แวร์ใหม่ไปในทางที่ผิดอย่างต่อเนื่อง** การอัปเดตซอฟต์แวร์บนอุปกรณ์ของคุณช่วย ปกป้องคุณจากการโจมตีทางไซเบอร์



ฉันจะตั้งค่าการอัปเดตอัตโนมัติได้อย่างไร?

การอัปเดตอัตโนมัติเป็นการตั้งค่าเริ่มต้นหรือ ‹ตั้งค่าแล้วลืมได้› ซึ่งจะติดตั้งอัปเดตใหม่ทันทีที่ออกมา

- เปิดและยืนยันการอัปเดตอัตโนมัติในซอฟต์แวร์และอุปกรณ์ทั้งหมด
- วิธีเปิดการอัปเดตอัตโนมัติอาจแตกต่างกันโดยขึ้นอยู่กับซอฟต์แวร์และอุปกรณ์นั้น ๆ
- ตั้งเวลาที่สะดวกสำหรับการอัปเดตอัตโนมัติหากเป็นไปได้ เช่น เวลาที่คุณหลับหรือไม่ได้ใช้อุปกรณ์ตามปกติ

อุปกรณ์ของคุณจะต้องเปิดทำงาน เสียบอยู่กับปลั๊กไฟ และมีพื้นที่เก็บข้อมูลที่ไม่ได้ใช้งานอยู่

เคล็ดลับ หากคุณได้รับข้อความแจ้งให้อัปเดตซอฟต์แวร์ของอุปกรณ์ คุณควรดำเนินการโดยเร็วที่สุด

คุณสามารถหาดูข้อมูลโดยละเอียดเพิ่มเติมได้เกี่ยวกับวิธีเปิดการอัปเดตอัตโนมัติด้วยการค้นหาคำว่า ‘Updates’ บนเว็บไซต์ cyber.gov.au

จะเกิดอะไรขึ้นหากไม่มีการตั้งค่าการอัปเดตอัตโนมัติ?

หากไม่มีการตั้งค่าการอัปเดตอัตโนมัติ คุณควรตรวจสอบและติดตั้งการอัปเดตใหม่เป็นประจำโดยทำผ่าน ซอฟต์แวร์หรือเมนูการตั้งค่าในอุปกรณ์ของคุณ

จะเกิดอะไรขึ้นหากอุปกรณ์และซอฟต์แวร์รุ่นเก่าของฉันไม่ได้รับการอัพเดตใด ๆ เลย?

หากอุปกรณ์ ระบบปฏิบัติการ หรือซอฟต์แวร์ของคุณเก่าเกินไป ผู้ผลิตหรือผู้พัฒนาอาจไม่ให้การสนับสนุนอีกต่อไป

เมื่อผลิตภัณฑ์มาถึงจุดที่ ‹สิ้นสุดการสนับสนุน (End of support)› ผลิตภัณฑ์จะไม่ได้รับการอัปเดตอีกต่อไป ซึ่งอาจทำให้คุณเสี่ยงต่อการถูกโจมตีทางไซเบอร์ ตัวอย่างของผลิตภัณฑ์ที่สิ้นสุดการสนับสนุน ได้แก่ ระบบปฏิบัติการ Windows 7 และ iPhone 7

หากอุปกรณ์ ระบบปฏิบัติการ หรือซอฟต์แวร์ของคุณถึงจุดสิ้นสุดการสนับสนุน ทาง ACSC ขอแนะนำให้คุณทำการอัปเกรดโดยเร็วที่สุดเพื่อรักษาให้อุปกรณ์ ระบบปฏิบัติการหรือซอฟต์แวร์มีความปลอดภัยไว้

สำหรับข้อมูลเพิ่มเติม ค้นหาคำว่า ‘End of support’ ได้บนเว็บไซต์ cyber.gov.au

การรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคล: ขั้นตอนแรก

เปิดใช้งานการยืนยันตัวตน โดยใช้หลากหลายปัจจัย (MFA)

MFA คืออะไร?

คุณสามารถใช้การยืนยันตัวตนโดยใช้หลากหลายปัจจัย (MFA) เพื่อเพิ่มการรักษาความปลอดภัยของบัญชีที่สำคัญที่สุดของคุณให้ดีขึ้น MFA กำหนดให้คุณสร้างการยืนยันตัวตนตั้งแต่สองประเภทขึ้นไปก่อนที่จะให้สิทธิ์การเข้าถึงบัญชีใด ๆ

- **บางสิ่งที่คุณทราบ** (เช่น เลขรหัสลับส่วนตัว (PIN) รหัสผ่าน หรือข้อความรหัสผ่าน)
- **บางสิ่งที่คุณเป็นเจ้าของ** (เช่น สมาร์ทการ์ด อุปกรณ์สร้างรหัสภายนอก (Physical token) แอปยืนยันตัวตน SMS หรืออีเมล)
- **บางสิ่งที่เป็นตัวคุณ** (เช่น ลายนิ้วมือ ระบบจดจำใบหน้า หรือการสแกนม่านตา)

MFA ทำให้อาชญากรไซเบอร์เข้าถึงบัญชีของคุณได้ยากขึ้น ซึ่งเป็นการเพิ่มระดับความซับซ้อนของการยืนยันตัวตนที่ต้องใช้เวลา ความพยายาม และทรัพยากรเพิ่มขึ้นในการเข้าถึง

ฉันจะเปิดใช้งาน MFA เพื่อปกป้องบัญชีที่สำคัญที่สุดของฉันได้อย่างไร?

ขั้นตอนในการเปิดใช้งาน MFA มีความแตกต่างกันออกไป ขึ้นอยู่กับบัญชี อุปกรณ์ หรือแอปพลิเคชันซอฟต์แวร์ คุณควรเปิดใช้งาน MFA ทันที โดยเริ่มจากบัญชีที่สำคัญ ๆ ของคุณ

- บัญชีการธนาคารและการเงินออนไลน์ทั้งหมด (เช่น ธนาคารของคุณ, PayPal)
- บัญชีอีเมลทั้งหมด (เช่น Gmail, Outlook, Hotmail, Yahoo!)

หากคุณมีบัญชีอีเมลจำนวนมาก ให้จัดลำดับความสำคัญของบัญชีที่เชื่อมโยงกับธนาคารออนไลน์ของคุณหรือบริการที่สำคัญอื่น ๆ ของคุณไว้เป็นลำดับแรก

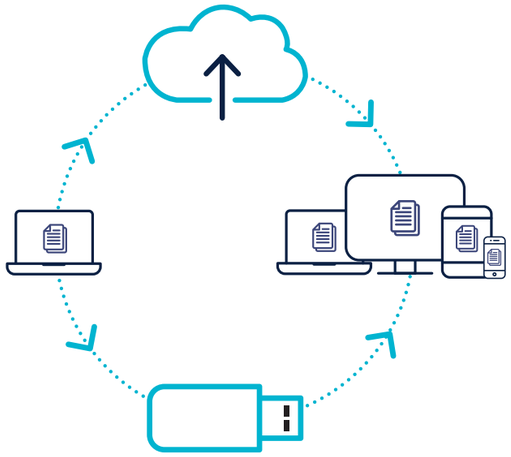
คุณสามารถอ่านเพิ่มเติมได้เกี่ยวกับวิธีเปิดใช้งานการยืนยันตัวตนแบบหลากหลายปัจจัยด้วยการค้นหาคำว่า ‘Multi-factor authentication’ หรือ ‘MFA’ บนเว็บไซต์ cyber.gov.au

สำรองข้อมูลในอุปกรณ์ของคุณเป็นประจำ

การสำรองข้อมูล (Backup) คืออะไร?

การสำรองข้อมูลเป็นการทำสำเนาดิจิทัลข้อมูลของคุณ ซึ่งอาจรวมถึงสิ่งต่าง ๆ เช่น รูปภาพ ข้อมูลหรือบันทึกทางการเงินที่คุณเก็บไว้ในอุปกรณ์จัดเก็บข้อมูลภายนอกหรือบนระบบคลาวด์ (Cloud)

การสำรองข้อมูลของคุณเป็นมาตรการป้องกันล่วงหน้าเพื่อให้สามารถกู้คืนข้อมูลหากสูญหาย ถูกขโมย หรือเสียหายได้



สำรองข้อมูลและไฟล์บนอุปกรณ์ของฉันได้อย่างไร?

คุณควรสำรองไฟล์และอุปกรณ์ของคุณเป็นประจำ ไม่ว่าจะเป็นรายวัน รายสัปดาห์ หรือรายเดือนขึ้นอยู่กับคุณ ส่วนจำนวนครั้งในการสำรองข้อมูลขึ้นอยู่กับจำนวนของ

- ไฟล์ใหม่ที่คุณโหลดลงอุปกรณ์ของคุณ
- การเปลี่ยนแปลงที่คุณทำกับไฟล์

เคล็ดลับ ตรวจสอบการสำรองข้อมูลของคุณเป็นประจำเพื่อให้คุณคุ้นเคยกับกระบวนการกู้คืน ตรวจสอบให้แน่ใจเสมอว่าการสำรองข้อมูลของคุณทำงานได้อย่างถูกต้อง

คุณสามารถดูข้อมูลโดยละเอียดเพิ่มเติมเกี่ยวกับวิธีการสำรองข้อมูลได้ด้วยการค้นหาคำว่า ‘Backups’ บนเว็บไซต์ cyber.gov.au

ใช้ข้อความรหัสผ่านเพื่อรักษาความปลอดภัยบัญชีสำคัญของคุณ

การยืนยันตัวตนโดยใช้หลากหลายปัจจัย (MFA) เป็นหนึ่งในวิธีที่มีประสิทธิภาพที่สุดในการปกป้องบัญชีของคุณจากอาชญากรไซเบอร์ **หากไม่มี MFA** ข้อความรหัสผ่านที่รัดกุมเป็นเอกลักษณ์ไม่ซ้ำใครสามารถปกป้องบัญชีของคุณได้ดีกว่าเมื่อเทียบกับรหัสผ่านธรรมดา

ข้อความรหัสผ่าน (Passphrase) คืออะไร?

ข้อความรหัสผ่านใช้คำสุ่มตั้งแต่สี่คำขึ้นไปเป็นรหัสผ่านของคุณ

ตัวอย่าง เช่น ‘crystal onion clay pretzel’

- **ข้อความรหัสผ่านช่วยรักษาความปลอดภัยได้ดีกว่า** รหัสผ่านธรรมดาง่าย ๆ
- **ข้อความรหัสผ่านนั้นยากสำหรับอาชญากรไซเบอร์**ที่จะมาถอดรหัส แต่**ง่ายสำหรับคุณ**ที่จะจดจำ

ฉันจะสร้างข้อความรหัสผ่านได้อย่างไร?

คุณควรสร้างข้อความรหัสผ่านที่

- **ยาว** มีความยาวอย่างน้อย 14 ตัวอักษร โดยใช้คำสุ่มตั้งแต่สี่คำขึ้นไป ยิ่งข้อความรหัสผ่านของคุณยาวเท่าไรก็ยิ่งปลอดภัยมากขึ้นเท่านั้น
- **คาดเดาไม่ได้** ใช้คำสุ่มที่ไม่เกี่ยวข้องกันตั้งแต่สี่คำขึ้นไป อย่าใช้ข้อความ คำคม หรือเนื้อเพลงที่เป็นที่รู้จักดี
- **เป็นเอกลักษณ์ไม่ซ้ำใคร** อย่าใช้คำเดิม ๆ ซ้ำกันหลายบัญชี

หากเว็บไซต์หรือบริการต้องการรหัสผ่านที่ซับซ้อน รวมถึงสัญลักษณ์ ตัวพิมพ์ใหญ่ หรือตัวเลข คุณสามารถใช้อักษรเหล่านี้กับข้อความรหัสผ่านของคุณได้ ข้อความรหัสผ่านของคุณควรจะยาว คาดเดาไม่ได้และไม่ซ้ำใคร เพื่อให้การรักษาความปลอดภัยที่ดีที่สุด

ฉันควรรักษาความปลอดภัยบัญชีใดด้วยข้อความรหัสผ่าน?

หากบัญชีที่สำคัญที่สุดของคุณไม่ได้รับการปกป้องด้วย MFA ให้เปลี่ยนรหัสผ่านของคุณเป็นข้อความรหัสผ่านที่เป็นเอกลักษณ์ไม่ซ้ำใคร โดยเริ่มจาก

- บัญชีการธนาคารและการเงินออนไลน์
- บัญชีอีเมล

หากคุณมีบัญชีอีเมลจำนวนมาก ให้จัดลำดับความสำคัญของบัญชีที่เชื่อมโยงกับธนาคารออนไลน์หรือบริการที่สำคัญอื่น ๆ ของคุณไว้เป็นลำดับแรก

โดยทั่วไปแล้ว คุณสามารถเปลี่ยนรหัสผ่านของคุณเป็นข้อความรหัสผ่านที่เป็นเอกลักษณ์ไม่ซ้ำใครได้ โดยทำผ่านเมนูการตั้งค่าบัญชีของคุณ

เคล็ดลับ หากคุณมีปัญหาในการจำข้อความรหัสผ่านทั้งหมด ให้พิจารณาใช้แอปจัดการรหัสผ่าน (Password Manager) ด้วยแอปจัดการรหัสผ่าน คุณเพียงต้องจดจำรหัสผ่านตัวเดียวเท่านั้น จากนั้นแอปจัดการรหัสผ่านจะดูแลส่วนที่เหลือเอง ค้นหาคำว่า ‘Password Manager’ บนเว็บไซต์ cyber.gov.au เพื่อขอคำแนะนำเพิ่มเติม

คุณสามารถหาดูข้อมูลโดยละเอียดเพิ่มเติมได้เกี่ยวกับวิธีสร้างข้อความรหัสผ่านที่ปลอดภัยด้วยการค้นหาคำว่า ‘Passphrases’ บนเว็บไซต์ cyber.gov.au

เก็บรักษาอุปกรณ์เคลื่อนที่ของคุณให้ปลอดภัย

ทุกวันนี้ เราใช้งานสมาร์ทโฟนและแท็บเล็ตในชีวิตประจำวัน เราใช้อุปกรณ์เหล่านี้เพื่อเชื่อมต่อ ซื้อของ ทำงาน ทำธุรกรรมธนาคาร ติดตามสมรรถภาพร่างกายของเรา และทำงานหลายร้อยอย่างให้เสร็จสิ้นได้ทุกเมื่อ ทุกสภาพและทุกที่

จะเกิดอะไรขึ้นหากอุปกรณ์เคลื่อนที่ของฉันถูกจู่โจม สูญหาย หรือถูกขโมย?

- อาชญากรไซเบอร์อาจใช้มันเพื่อขโมยเงินหรือตัวตนของคุณ อาชญากรทำเรื่องนี้ได้โดยใช้ข้อมูลที่จัดเก็บไว้ในอุปกรณ์ของคุณ รวมถึงบัญชีบนโซเชียลมีเดียและบัญชีอีเมล
- คุณอาจสูญเสียข้อมูลที่ไม่สามารถทดแทนคืนได้ เช่น รูปภาพ โน้ตบันทึก หรือข้อความ (หากไม่ได้สำรองข้อมูลไว้)
- อาชญากรไซเบอร์อาจใช้หมายเลขโทรศัพท์ของคุณเพื่อไปหลอกลวงผู้อื่น

ฉันจะรักษาความปลอดภัยอุปกรณ์เคลื่อนที่ของฉันได้อย่างไร?

การรักษาความปลอดภัยของอุปกรณ์

- **ปิดล็อก**อุปกรณ์ของคุณด้วยข้อความรหัสผ่าน รหัสผ่านเลขรหัสลับส่วนตัว (PIN) หรือเลขรหัสผ่าน ทำให้คาดเดาได้ยาก การใช้วันเกิดและการล็อกแบบลากเส้น (Pattern Lock) ของคุณง่ายเกินไปสำหรับอาชญากรไซเบอร์ที่จะคาดคะเนได้ ใช้ข้อความรหัสผ่านเพื่อการรักษาความปลอดภัยสูงสุด (ดูหน้า 6) คุณยังอาจพิจารณาใช้ระบบจดจำใบหน้า (Facial Recognition) หรือลายนิ้วมือเพื่อปลดล็อกอุปกรณ์ของคุณ
- **ตรวจสอบให้แน่ใจว่า** อุปกรณ์ของคุณได้รับการตั้งค่าให้ล็อกโดยอัตโนมัติหลังจากเวลาไม่ใช้งานเพียงสั้น ๆ
- **อย่า**ชาร์จอุปกรณ์ของคุณที่สถานีชาร์จสาธารณะและหลีกเลี่ยงการใช้ที่ชาร์จจากบุคคลอื่น
- **ดูแลรักษา**โทรศัพท์ของคุณเหมือนกระเป๋าสตางค์ของคุณ เก็บมันไว้อย่างปลอดภัย และถือติดตัวคุณตลอดเวลา

การรักษาความปลอดภัยของซอฟต์แวร์และแอป

- **ใช้**คุณสมบัติการอัปเดตอัตโนมัติของอุปกรณ์เพื่อติดตั้งอัปเดตแอปพลิเคชันและระบบปฏิบัติการใหม่ทันทีที่มีให้อัปเดต
- **ตั้งค่า**ให้อุปกรณ์ต้องใช้ข้อความรหัสผ่าน/รหัสผ่านก่อนติดตั้งแอปพลิเคชัน นอกจากนี้ ยังสามารถใช้ระบบควบคุมโดยผู้ปกครอง (Parental Controls) เพื่อจุดประสงค์นี้ได้
- **ตรวจสอบ**การอนุญาตที่เกี่ยวข้องกับความเป็นส่วนตัวอย่างรอบคอบก่อนติดตั้งแอปใหม่บนอุปกรณ์ของคุณ โดยเฉพาะอย่างยิ่งแอปที่แจกให้ฟรี ติดตั้งแอปจากผู้จำหน่ายที่มีชื่อเสียงเชื่อถือได้เท่านั้น

การรักษาความปลอดภัยของข้อมูล

- **เปิดใช้งาน**ฟังก์ชั่นล็อกและการล้างข้อมูลจากระยะไกลหากอุปกรณ์ของคุณรองรับฟังก์ชั่นนี้
- **ตรวจสอบให้แน่ใจว่า** คุณลบข้อมูลส่วนบุคคลจากอุปกรณ์ของคุณให้หมดจดก่อนที่จะขายหรือกำจัดอุปกรณ์ทิ้งไป

การรักษาความปลอดภัยในการเชื่อมต่อ

- **ปิด** Bluetooth และ Wi-Fi ในเวลาที่คุณไม่ได้ใช้งาน
- **ตรวจสอบให้แน่ใจว่า**คุณไม่ได้ตั้งค่าให้มือถือเชื่อมต่อกับเครือข่าย Wi-Fi ใหม่อย่างอัตโนมัติ

คุณสามารถหาดูข้อมูลโดยละเอียดเพิ่มเติมได้เกี่ยวกับวิธีรักษาโทรศัพท์มือถือของคุณให้ปลอดภัย ด้วยการค้นหาคำว่า 'Secure your mobile phone' บนเว็บไซต์ cyber.gov.au

การรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคล: ขั้นตอนแรก

พัฒนาแนวความคิดด้านการรักษาความปลอดภัยทางไซเบอร์ของคุณ

การรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคลไม่ได้เป็นเพียงการเปลี่ยนการตั้งค่าเท่านั้น แต่ยังเกี่ยวกับการเปลี่ยนแปลงความคิดและพฤติกรรมของคุณด้วย

ระวังสแกมหรือการหลอกลวงทางไซเบอร์

เป็นที่รู้กันว่าอาชญากรไซเบอร์ใช้อีเมล ข้อความ โซเชียลมีเดีย หรือโทรศัพท์เพื่อพยายามหลอกลวงชาวออสเตรเลีย พวกเขาอาจแสร้งทำเป็นบุคคลหรือองค์กรที่คุณคิดว่ารู้จักหรือคิดว่าคุณควรไว้วางใจ

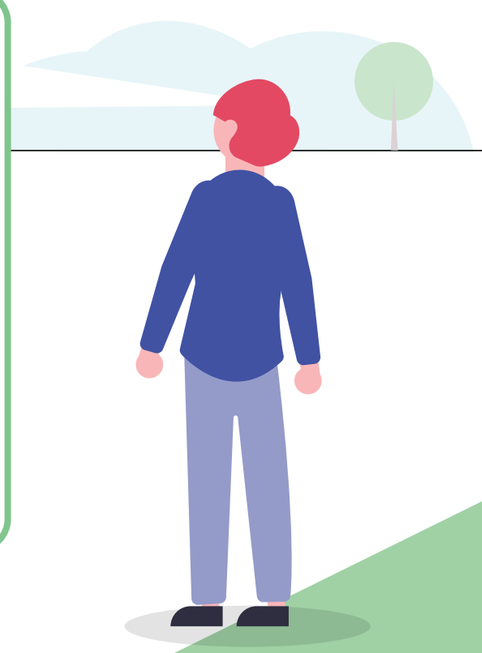
ข้อความและโทรศัพท์จากพวกเขาพยายามจะหลอกให้คุณดำเนินการอะไรบางอย่าง เช่น

- เปิดเผยรายละเอียดบัญชีธนาคาร รหัสผ่าน และหมายเลขบัตรเครดิต
- ให้การเข้าถึงคอมพิวเตอร์ของคุณจากระยะไกล
- การเปิดไฟล์แนบซึ่งอาจมีมัลแวร์
- การส่งเงินหรือบัตรของขวัญ

ฉันจะรู้ได้อย่างไรว่าเป็นข้อความสแกม?

อาจเป็นเรื่องยากที่จะรับรู้ได้ว่าข้อความใดเป็นสแกม อาชญากรไซเบอร์มักใช้วิธีการบางอย่างเพื่อหลอกลวงคุณ ข้อความของพวกเขาอาจรวมถึง

- **ผู้มีอำนาจ** มีการอ้างว่าข้อความนั้นมาจากเจ้าหน้าที่อย่างเป็นทางการหรือไม่ เช่น ธนาคารของคุณ?
- **ความเร่งด่วน** คุณได้รับแจ้งว่าคุณมีปัญหาหรือเวลาจำกัดในการตอบสนองหรือชำระเงินหรือไม่?
- **อารมณ์** ข้อความนั้นทำให้คุณตื่นตระหนก มีความหวัง หรืออยากรู้อยากเห็นหรือไม่?
- **ความขาดแคลน** ข้อความนั้นนำเสนอสิ่งที่ขาดแคลนหรือมีการสัญญาว่าจะให้ข้อเสนอที่ดีแก่คุณหรือไม่?
- **เหตุการณ์ปัจจุบัน** ข้อความนั้นเกี่ยวข้องกับเรื่องราวในข่าวปัจจุบันหรือเหตุการณ์สำคัญหรือไม่?



เรียนรู้วิธีสังเกตข้อความฟิชชิ่งหรือสแกมด้วยการค้นหาคำว่า 'Learn the basics' บนเว็บไซต์ cyber.gov.au

ฉันควรทำอย่างไรหากได้รับข้อความสแกม?

หากคุณได้รับข้อความหรือโทรศัพท์สแกม คุณควรเพิกเฉยลบ หรือรายงานไปที่ Scamwatch ของ ACCC ที่ scamwatch.gov.au

คุณยังสามารถติดต่อสายด่วน Cyber Security Hotline ของ ACSC ได้ที่หมายเลข **1300 CYBER1** (1300 292 371) หากคุณกังวลเกี่ยวกับความปลอดภัยทางไซเบอร์ของคุณ

หากคุณรู้ตัวว่าถูกสแกมและคิดว่าบัญชีธนาคาร บัตรเครดิต หรือบัตรเดบิตของคุณอาจตกอยู่ในความเสี่ยง โปรดติดต่อสถาบันการเงินของคุณทันที สถาบันเหล่านั้นอาจสามารถปิดบัญชีหรือระงับธุรกรรมให้คุณได้

จะเกิดอะไรขึ้นหากฉันไม่แน่ใจว่าข้อความนั้นเป็นสแกมหรือไม่?

หากคุณคิดว่าข้อความหรือโทรศัพท์นั้นอาจมาจากองค์กรที่คุณไว้วางใจจริง ๆ (เช่น ธนาคารของคุณ) ให้หาวิธีติดต่อกลับที่เชื่อถือได้ ค้นหาเว็บไซต์ที่เป็นทางการ โทรไปหมายเลขโทรศัพท์ที่โฆษณาไว้หรือไปที่หน้าร้านหรือสาขา อย่าใช้ลิงก์หรือรายละเอียดการติดต่อในข้อความที่คุณได้รับหรือมาทางโทรศัพท์ เนื่องจากอาจเป็นการหลอกลวงได้

หากคุณคิดว่าได้ตกเป็นเหยื่ออาชญากรรมทางไซเบอร์แล้ว สามารถรายงานผ่าน ReportCyber ของ ACSC ที่ cyber.gov.au/report หรือโทรสายด่วน Cyber Security Hotline ที่ 1300 CYBER1 (1300 292 371)

คุณยังสามารถติดตามเรื่องราวล่าสุดเกี่ยวกับภัยคุกคามไซเบอร์ได้โดยสมัครใช้บริการแจ้งเตือนฟรีของ ACSC ค้นหาคำว่า 'Subscribe to the ACSC alert service' บนเว็บไซต์ cyber.gov.au เราจะส่งการแจ้งเตือนถึงคุณเมื่อเราพบภัยคุกคามทางไซเบอร์ใหม่ ๆ

การรักษาความปลอดภัยทางไซเบอร์ส่วนบุคคล: ขั้นตอนแรก

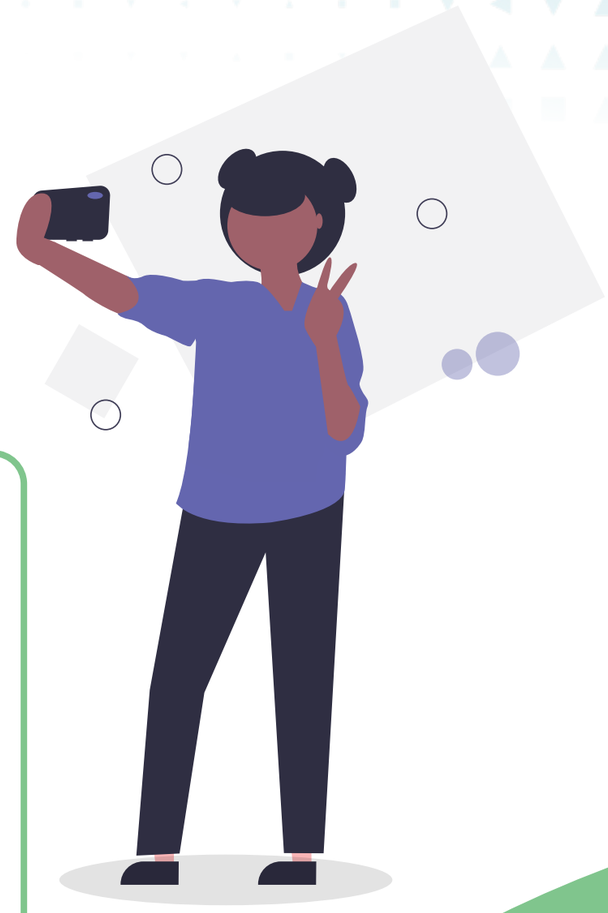
หยุดคิดก่อนแชร์บนโซเชียลมีเดีย

อาชญากรไซเบอร์สามารถใช้ข้อมูลที่คุณโพสต์แบบสาธารณะในบัญชีโซเชียลมีเดียของคุณในการหลอกลวงและการโจมตีทางไซเบอร์

โปรดจำไว้ว่าข้อมูลบนอินเทอร์เน็ตเป็นสิ่งถาวร และคุณไม่สามารถลบสิ่งที่โพสต์ออกไปแล้วได้ทั้งหมด

คุณจะหยุดคิดก่อนโพสต์ได้ยังไง?

- **ลองคิดดู** อาชญากรไซเบอร์จะใช้ข้อมูลนี้เพื่อจู่โจมฉันหรือบัญชีของฉันได้อย่างไร?
- **ลองคิดดู** ฉันจะยินดีแสดงข้อมูลหรือรูปภาพนี้ให้คนแปลกหน้าดูแบบออฟไลน์หรือไม่?



ข้อมูลใดที่ฉันควรหลีกเลี่ยงไม่แชร์?

หลีกเลี่ยงการแชร์ข้อมูล (รวมถึงภาพถ่าย) ทางออนไลน์ที่อาชญากรไซเบอร์สามารถใช้เพื่อระบุตัวตนของคุณ หลอกลวงคุณผ่านการสแกม หรือคาดเดาคำถามในการกู้คืนบัญชี (Account Recovery) ของคุณ ซึ่งอาจรวมถึง

- สถานที่เกิดและวันเดือนปีเกิด
- ที่อยู่และหมายเลขโทรศัพท์
- นายจ้างและประวัติการทำงาน
- โรงเรียนเก่าของคุณ
- ข้อมูลส่วนบุคคลอื่นใดที่สามารถใช้เพื่อทำให้คุณตกเป็นเหยื่อได้

รายการตรวจสอบโดยสรุป

คุณทำทุกอย่างตามคู่มือนี้แล้วหรือไม่?

ใช้รายการตรวจสอบที่มีประโยชน์นี้เพื่อติดตามความคืบหน้าของคุณ

- **ฉันเปิดการอัปเดตอัตโนมัติในอุปกรณ์ทั้งหมดของฉันแล้ว**
  - คอมพิวเตอร์ (เดสก์ท็อปและแล็ปท็อป)
  - โทรศัพท์มือถือ
  - แท็บเล็ต
- **ฉันได้เปิดใช้งานการยืนยันตัวตนโดยใช้หลากหลายปัจจัย ในบัญชีที่สำคัญที่สุดของฉันแล้ว**
  - บัญชีการธนาคารและการเงินทางออนไลน์ทั้งหมดของฉัน (เช่น บัญชีธนาคาร บัญชี PayPal)
  - บัญชีอีเมลทั้งหมดของฉัน (เช่น Gmail, Outlook, Hotmail, Yahoo!)
- **ฉันสำรองข้อมูลในอุปกรณ์ของฉันเป็นประจำ**
  - คอมพิวเตอร์ (เดสก์ท็อปและแล็ปท็อป)
  - โทรศัพท์มือถือ
  - แท็บเล็ต
- **ฉันใช้ข้อความรหัสผ่านที่เป็นเอกลักษณ์ไม่ซ้ำใครกับบัญชีที่สำคัญที่สุดของฉัน ซึ่งไม่ได้รับการปกป้องโดย MFA**
  - บัญชีการธนาคารและการเงินออนไลน์
  - บัญชีอีเมล
- **ฉันให้การรักษาความปลอดภัยกับอุปกรณ์เคลื่อนที่ของฉันแล้ว**
  - แล็ปท็อป
  - โทรศัพท์มือถือ
  - แท็บเล็ต
- **ฉันใช้แนวความคิดด้านการรักษาความปลอดภัยทางไซเบอร์ทุกวัน**
  - ฉันสามารถจำแนกข้อความที่เป็นสแกมหลอกลวงได้
  - ฉันรู้ว่าต้องทำอย่างไรหากได้รับข้อความสแกม
  - ฉันรู้วิธีตรวจสอบว่าข้อความที่ได้รับเป็นสแกมหรือไม่ถ้าฉันไม่แน่ใจ
  - ฉันคิดก่อนคลิกลิงก์และก่อนเปิดไฟล์ที่แนบมาด้วย
  - ฉันคิดก่อนแชร์อะไรบนโซเชียลมีเดีย
- **ฉันรู้ว่าจะขอความช่วยเหลือได้ที่ไหนหากตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์หรือเหยื่อสแกม**

อภิธานศัพท์

การกู้คืนบัญชี (Account recovery)
กระบวนการที่ใช้ชุดคำถามหรือวิธีการยืนยันอื่น ๆ เพื่อกู้คืนหรือเข้าถึงบัญชีได้อีกครั้ง หรือเพื่อเปลี่ยนข้อความรหัสผ่าน/รหัสผ่านของบัญชีหนึ่ง ๆ

มัลแวร์ (Malware)
ซอฟต์แวร์ที่ไม่ประสงค์ดี ทำขึ้นมาเพื่อเข้าถึงและควบคุมคอมพิวเตอร์ของผู้ใช้โดยไม่ได้รับอนุญาต เข้าถึงเพื่อขโมยข้อมูล และขัดขวางหรือปิดการใช้งานเครือข่าย

แอป (App)
เรียกอีกอย่างว่าแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ แอปเป็นคำศัพท์สำหรับซอฟต์แวร์ที่ใช้กับสมาร์ทโฟนหรือแท็บเล็ตโดยทั่วไป

ไฟล์แนบ (Attachment)
ไฟล์ที่ส่งไปพร้อมกับข้อความอีเมล

ระบบปฏิบัติการ (Operating system)
ซอฟต์แวร์ที่ติดตั้งบนฮาร์ดไดรฟ์ของคอมพิวเตอร์ที่ช่วยให้ฮาร์ดแวร์คอมพิวเตอร์สื่อสารและใช้งานกับโปรแกรมคอมพิวเตอร์ได้ ตัวอย่าง เช่น ไมโครซอฟต์วินโดว์ (Microsoft Windows) แอปเปิลแมคโอเอส (Apple macOS) ไอโอเอส (iOS) แอนดรอยด์ (Android)

อุปกรณ์สร้างรหัสภายนอก (Physical token)
อุปกรณ์ทางกายภาพขนาดเล็กที่มักร้อยกับพวกกุญแจได้ ซึ่งสามารถสร้างรหัสความปลอดภัยที่นำไปยืนยันตัวตนของผู้ใช้คอมพิวเตอร์ที่ใช้ MFA ได้

แอปยืนยันตัวตน (Authenticator app)
แอปที่ใช้ในการยืนยันตัวตนของผู้ใช้คอมพิวเตอร์เพื่ออนุญาตการเข้าถึงโดยผ่านการยืนยันตัวตนโดยใช้หลากหลายปัจจัย (MFA)

คลาวด์ (Cloud)
เครือข่ายของเซิร์ฟเวอร์ระยะไกลที่ให้พื้นที่การจัดเก็บและกระจายข้อมูล รวมถึงกำลังการประมวลผลขนาดใหญ่

การเข้าถึงระยะไกล (Remote access)
เข้าถึงและควบคุมอุปกรณ์และเครือข่ายจากทำเลที่อยู่นอกสถานที่

อาชญากรไซเบอร์ (Cybercriminal)
บุคคลใดก็ตามที่เข้าถึงระบบคอมพิวเตอร์หรือบัญชีโดยมิชอบเพื่อสร้างความเสียหายหรือขโมยข้อมูล

อุปกรณ์ (Device)
คอมพิวเตอร์หรืออุปกรณ์สื่อสาร ตัวอย่างเช่น คอมพิวเตอร์แล็ปท็อป โทรศัพท์มือถือ หรือแท็บเล็ต

ซอฟต์แวร์ (Software)
โดยทั่วไปเรียกว่าโปรแกรม ซึ่งเป็นชุดคำสั่งที่ช่วยให้ผู้ใช้งานสามารถโต้ตอบกับคอมพิวเตอร์ ฮาร์ดแวร์ หรือทำงานต่าง ๆ ได้

สิ้นสุดการสนับสนุน (End of support)
สิ้นสุดการสนับสนุนหมายถึง สถานการณ์ที่บริษัทยุติการสนับสนุนผลิตภัณฑ์หรือบริการของตน โดยทั่วไปมักจะเป็นสถานการณ์ที่บริษัทออกผลิตภัณฑ์ฮาร์ดแวร์และซอฟต์แวร์เวอร์ชันใหม่และจะสิ้นสุดการสนับสนุนเวอร์ชันก่อนหน้า

สำหรับข้อมูลเพิ่มเติมหรือรายงานเหตุการณ์ที่เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ ติดต่อเราที่
cyber.gov.au | 1300 CYBER1 (1300 292 371)
หมายเลขนี้มีไว้สำหรับใช้ภายในออสเตรเลียเท่านั้น

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre