ข้อแนะนำในการรักษาความปลอดภัยอุปกรณ์ Internet of Things ของคุณ

ศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลีย (Australian Cyber Security Centre) ได้พัฒนาข้อมูลชุดนี้ขึ้นเพื่อช่วยให้ชุมชนสามารถเลือกซื้อและใช้งานอุปกรณ์ Internet of Things (IoT) ได้อย่างปลอดภัย อุปกรณ์ IoT คือสิ่งของที่เราใช้ในชีวิตประจำวันซึ่งมีการเพิ่มความสามารถในการเชื่อมต่ออินเทอร์เน็ตเข้าไป ตัวอย่างของอุปกรณ์ IoT ได้แก่ อุปกรณ์ใช้เฝ้าดูลูกน้อยในห้องเด็ก อากาศยานไร้คนขับหรือโดรน กล้องวงจรปิด โทรทัศน์อัจฉริยะ และอุปกรณ์แปลงไฟฟ้าหรืออินเวอร์เตอร์พลังงานแสงอาทิตย์ อุปกรณ์ IoT ภายในบ้านและธุรกิจมักใช้งานผ่านเครือข่าย Wi-Fi หรือเครือข่ายเซลลูลาร์ในการเชื่อมต่อกับอินเทอร์เน็ต เช่น 4G หรือ 5G

อุปกรณ์ IoT จำนวนมากที่พบได้ทั่วไปในบ้านและธุรกิจของออสเตรเลียไม่ได้ออกแบบมาโดยคำนึงถึงความปลอดภัยเป็นหลัก ซึ่งส่งผลให้อุปกรณ์เหล่านี้มีความเสี่ยงต่อการถูกบุกรุกผ่านทางอินเทอร์เน็ต เหตุการณ์ลักษณะนี้อาจเปิดโอกาสให้อาชญากรไซเบอร์เข้าถึงอุปกรณ์และข้อมูลส่วนบุคคลของคุณโดยไม่ได้รับอนุญาต เพื่อนำไปใช้ในทางที่ไม่ประสงค์ดี

ก่อนซื้ออุปกรณ์ IoT ใด ๆ

การศึกษาข้อมูลเกี่ยวกับอุปกรณ์ก่อนตัดสินใจซื้อเป็นสิ่งสำคัญ เนื่องจากผู้ผลิตแต่ละรายมีระดับมาตรฐานความปลอดภัยที่แตกต่างกัน ก่อนซื้ออุปกรณ์ ควรเปรียบเทียบอุปกรณ์ที่คล้ายคลึงกันจากผู้ผลิตรายอื่น ๆ สิ่งที่ควรพิจารณา ได้แก่

1. **อุปกรณ์นี้ผลิตโดยบริษัทที่มีชื่อเสียงและน่าเชื่อถือ และมีจำหน่ายในร้านค้าที่มีชื่อเสียงและน่าเชื่อถือหรือไม่?** บริษัทที่มีชื่อเสียงและน่าเชื่อถือมีแนวโน้มที่จะผลิตอุปกรณ์โดยคำนึงถึงความปลอดภัยมากกว่า ร้านค้าที่มีชื่อเสียงและน่าเชื่อถือมีแนวโน้มที่จะจำหน่ายเฉพาะอุปกรณ์จากบริษัทที่มีชื่อเสียงและน่าเชื่อถือเท่านั้น รวมทั้งมีการควบคุมห่วงโซ่อุปทานที่เข้มงวดมากกว่า เพื่อให้มั่นใจว่าอุปกรณ์จะส่งถึงมือลูกค้าในสภาพที่ตรงตามที่ผู้ผลิตตั้งใจไว้

2. **เป็นไปได้ไหมที่จะเปลี่ยนรหัสผ่าน?** การเปลี่ยนรหัสผ่านเป็นสิ่งที่ดีเสมอ อย่างไรก็ตาม หากอุปกรณ์ที่จัดส่งมามีรหัสผ่านที่ตั้งโดยค่าเริ่มต้นที่ไม่ปลอดภัย การเปลี่ยนรหัสผ่านจะมีความสำคัญมากขึ้น อุปกรณ์ที่มีความปลอดภัยดีควรมีรหัสผ่านที่ไม่ซ้ำกัน ทายไม่ถูก มีความซับซ้อน และเดายาก เพราะรหัสผ่านที่ตั้งโดยค่าเริ่มต้นที่ไม่ปลอดภัยเป็นช่องทางที่ง่ายที่สุดในการโจมตีอุปกรณ์

3. **ผู้ผลิตมีการอัปเดตซอฟต์แวร์หรือไม่?** เป็นสิ่งสำคัญที่บริษัทจะต้องมีการอัปเดตซอฟแวร์เพื่อแก้ไขช่องโหว่ของอุปกรณ์เมื่อมีการค้นพบ ตัวอย่างเช่น หากซอฟต์แวร์บนอุปกรณ์มีช่องโหว่เป็นที่รู้จักกันอยู่แล้ว หรือแฮกเกอร์มีการพัฒนาวิธีใหม่ ๆ ในการบุกรุกระบบอุปกรณ์ของคุณ การอัปเดตจึงเป็นสิ่งจำเป็นเพื่อแก้ไขปัญหาเหล่านี้

4. **อุปกรณ์จะเก็บรวบรวมข้อมูลอะไรบ้าง และข้อมูลเหล่านั้นจะถูกแชร์ให้กับใครบ้าง?** ข้อมูลที่เกี่ยวกับว่าข้อมูลใดจะถูกเก็บรวบรวมและนำไปใช้งานอย่างไร ควรมีให้อ่านได้โดยง่ายบนเว็บไซต์ของผู้ผลิตหรือในนโยบายความเป็นส่วนตัวของผู้ผลิต สิ่งสำคัญคือต้องพิจารณาอยู่เสมอว่า ข้อมูลใดบ้างที่จะเก็บรวบรวมโดยแอปพลิเคชันออนไลน์หรือแอปพลิเคชันในอุปกรณ์เคลื่อนที่

5. **อุปกรณ์ทำเฉพาะสิ่งที่คุณต้องการให้มันทำหรือไม่?** การซื้ออุปกรณ์ที่ทำงานได้มากกว่าที่คุณต้องการ รวมถึงการเชื่อมต่ออินเทอร์เน็ต อาจทำให้ความปลอดภัยของคุณลดลง ความสามารถของอุปกรณ์ที่คุณไม่ใช้งานอาจเพิ่มความเสี่ยงต่อการถูกโจมตี โดยที่คุณไม่ได้รับประโยชน์ใด ๆ เลย

อุปกรณ์ IoT

โปรดคำนึงถึงคำถามง่าย ๆ สองสามข้อขณะตั้งค่าอุปกรณ์ของคุณ เพื่อช่วยให้เครือข่ายและข้อมูลของคุณปลอดภัยยิ่งขึ้น

1. **อุปกรณ์นี้จำเป็นต้องเชื่อมต่อกับอินเทอร์เน็ตหรือไม่?** เพียงเพราะอุปกรณ์สามารถเชื่อมต่ออินเทอร์เน็ตได้ ไม่ได้หมายความว่าควรเชื่อมต่อเสมอไป อุปกรณ์ที่ไม่ได้เชื่อมต่อกับอินเทอร์เน็ตมีโอกาสถูกบุกรุกได้น้อยกว่ามาก หากคุณไม่ได้ใช้งานฟีเจอร์ต่าง ๆ ที่ต้องเชื่อมต่อกับอินเทอร์เน็ต คุณควรพิจารณาว่าจำเป็นต้องเชื่อมต่ออุปกรณ์นั้นกับอินเทอร์เน็ตหรือไม่

2. **อุปกรณ์นั้นอยู่ในตำแหน่งที่ปลอดภัยหรือไม่?** หากไม่จำเป็นต้องติดตั้งอุปกรณ์นั้นในพื้นที่ที่ไม่ปลอดภัย การติดตั้งไว้ในตำแหน่งที่ปลอดภัยสามารถช่วยลดความเสี่ยงจากการถูกบุกรุกทางกายภาพได้

3. **ฉันต้องเปลี่ยนชื่อผู้ใช้และรหัสผ่านที่ตั้งโดยค่าเริ่มต้นหรือไม่?** การใช้รหัสผ่าน (Password) หรือวลีรหัสผ่าน (Passphrase) ที่รัดกุมเป็นสิ่งสำคัญอย่างยิ่ง หากอุปกรณ์ของคุณไม่ได้ส่งมาพร้อมกับรหัสผ่านที่ไม่ซ้ำกัน ทายไม่ถูก มีความซับซ้อน และเดายาก คุณจำเป็นต้องเปลี่ยนรหัสผ่านนั้น ชื่อผู้ใช้และรหัสผ่านที่ตั้งโดยค่าเริ่มต้นมักถูกเก็บรวบรวมและเผยแพร่ทางออนไลน์ ซึ่งทำให้อุปกรณ์ของคุณเสี่ยงต่อการถูกโจมตีมากขึ้น

4. **เครือข่าย Wi-Fi ของฉันตั้งค่ามาอย่างปลอดภัยหรือไม่ และเครือข่ายนั้นมีรหัสผ่านที่ปลอดภัยหรือไม่?** รักษาความปลอดภัยเครือข่าย Wi-Fi และเราเตอร์ของคุณ เพื่อทำให้ผู้โจมตีเข้าถึงอุปกรณ์และเครือข่ายของคุณได้ยากขึ้น

ทำเพิ่มอีกนิดเพื่อความปลอดภัยอีกขั้น

ตั้งค่าเครือข่าย Wi-Fi เพิ่มเติมบนเราเตอร์ของคุณสำหรับใช้งานกับอุปกรณ์ IoT โดยเฉพาะ โดยฟีเจอร์นี้อาจเรียกว่าเครือข่าย 'สำหรับแขก' บนอุปกรณ์เราเตอร์ Wi-Fi ของคุณ หากอุปกรณ์ IoT ของคุณไม่จำเป็นต้องสื่อสารกันเอง ให้เปิดการใช้งานของฟีเจอร์ 'แยกอุปกรณ์ลูกข่าย' (Client isolation) การแยกอุปกรณ์ IoT ออกจากข้อมูลสำคัญของคุณจะช่วยให้มั่นใจได้ว่า หากอุปกรณ์ IoT เครื่องหนึ่งถูกบุกรุก ผู้ไม่ประสงค์ดีจะไม่สามารถเข้าถึงอุปกรณ์หรือข้อมูลอื่นของคุณได้

5. **คุณปิดการใช้งานฟีเจอร์ของอุปกรณ์ที่ไม่จำเป็นแล้วหรือยัง?** หากอุปกรณ์ของคุณมีฟีเจอร์ที่ไม่ต้องการใช้งานหรือไม่จำเป็น (เช่น กล้องหรือไมโครโฟน) ควรปิดการใช้งานฟีเจอร์เหล่านั้นหากเป็นไปได้

ทำเพิ่มอีกนิดเพื่อความปลอดภัยอีกขั้น

มองหาการกำหนดตั้งค่าที่ระบุถึงการเปิดใช้งานการเข้าถึงจากระยะไกล (Remote access) ไปยังอินเทอร์เฟซที่ใช้จัดการอุปกรณ์ผ่านหน้าเว็บจากเครือข่ายภายใน (Local LAN) หรือเครือข่ายภายนอก/อินเทอร์เน็ต (WAN/internet) ตรวจสอบให้แน่ใจว่ามีการตั้งค่าไว้ที่เครือข่ายภายในเท่านั้น เว้นแต่คุณเองจำเป็นต้องใช้งานจากระยะไกล

การดูแลรักษาอุปกรณ์ IoT

มีสิ่งสำคัญบางอย่างที่ควรจำไว้หลังจากที่คุณตั้งค่าและเริ่มใช้งานอุปกรณ์ IoT แล้ว ซึ่งรวมถึง

1. **รีบูต (Reboot) อุปกรณ์ของคุณเป็นประจำ** หากอุปกรณ์เริ่มทำงานช้าลงหรือไม่สามารถใช้งานได้ อาจเป็นไปได้ว่ามีไวรัสอยู่ในอุปกรณ์ IoT มัลแวร์ส่วนใหญ่มักถูกเก็บไว้ในหน่วยความจำ และสามารถลบออกได้ง่ายด้วยการรีบูตอุปกรณ์ นั่นคือ การปิดแล้วเปิดเครื่องใหม่ หากอุปกรณ์ยังคงทำงานช้าหรือไม่สามารถใช้งานได้หลังจากรีบูต ลองทำการรีเซ็ตเป็นค่าเริ่มต้นจากโรงงาน อย่างไรก็ตาม ควรระวังว่าการทำเช่นนี้อาจลบข้อมูลผู้ใช้และการตั้งค่าส่วนตัวของคุณออกไปทั้งหมด

2. **อัปเดตอุปกรณ์อย่างสม่ำเสมอ** อุปกรณ์บางชนิดจะอัปเดตเองโดยอัตโนมัติ สำหรับอุปกรณ์ที่ไม่อัปเดตเองโดยอัตโนมัติ ให้ตรวจสอบกับผู้ผลิตเป็นประจำและติดตั้งการอัปเดตเมื่อมีการเปิดให้ใช้งาน เมื่อไม่มีการอัปเดตสำหรับอุปกรณ์ของคุณอีกต่อไป ควรพิจารณาเปลี่ยนเป็นอุปกรณ์รุ่นใหม่ที่ยังให้การอัปเดตอยู่ อุปกรณ์ที่ไม่ได้รับการอัปเดตด้านความปลอดภัยจะไม่ได้รับการปกป้องหากมีการค้นพบช่องโหว่ใหม่ ๆ และอุปกรณ์เหล่านี้อาจกลายเป็นความเสี่ยงต่อเครือข่าย ความเป็นส่วนตัว และข้อมูลของคุณ

3. **ปิดอุปกรณ์ของคุณเมื่อไม่ใช้งาน** การปล่อยให้อุปกรณ์ที่ไม่ได้ใช้งานและไม่มีการเฝ้าดูเปิดเครื่องอยู่และเชื่อมต่อกับเครือข่าย Wi-Fi ของคุณเป็นเวลานานนั้น อาจเพิ่มโอกาสที่อุปกรณ์ของคุณจะถูกโจมตีมากขึ้น ตัวเลือกหนึ่งในการทำอัปเดตโดยอัตโนมัติคือการใช้ปลั๊กไฟที่ตั้งเวลาได้ เพื่อจ่ายไฟให้กับอุปกรณ์เฉพาะในช่วงเวลาที่กำหนดไว้เท่านั้น

4. **เฝ้าระวังการใช้งานอินเทอร์เน็ตรายเดือนหรือค่าใช้จ่ายที่เพิ่มขึ้นอย่างผิดปกติ** การใช้งานอินเทอร์เน็ตหรือค่าใช้จ่ายที่เพิ่มขึ้นอย่างผิดปกติอาจบ่งชี้ว่าอุปกรณ์ของคุณถูกบุกรุกแล้ว เว้นแต่กรณีที่แผนก IT ภายในธุรกิจของคุณจะทำการตรวจสอบ คุณควรทำการรีเซ็ตอุปกรณ์เป็นค่าเริ่มต้นจากโรงงาน (แต่อย่าลืมว่าการทำเช่นนี้อาจลบข้อมูลผู้ใช้และการตั้งค่าส่วนตัวของคุณออกไปทั้งหมด) จากนั้นจึงเปลี่ยนรหัสผ่านใหม่

การกำจัดอุปกรณ์ IoT

การกำจัดอุปกรณ์ (ไม่ว่าจะเป็นการทิ้งหรือขายต่อ) อาจทำให้ผู้อื่นสามารถเข้าถึงข้อมูลส่วนตัวหรือข้อมูลของคุณได้อย่างง่ายดาย วิธีป้องกันเรื่องนี้ได้แก่

1. **ลบข้อมูลและข้อมูลส่วนตัวทั้งหมด** ผู้ผลิตอุปกรณ์ควรให้วิธีลบข้อมูลและข้อมูลส่วนตัวของคุณออกจากทั้งตัวอุปกรณ์และแอปพลิเคชันที่เกี่ยวข้อง การลบข้อมูลส่วนตัวของคุณจะช่วยให้มั่นใจว่าไม่มีใครสามารถเข้าถึงข้อมูลเหล่านั้นได้หลังจากที่คุณได้กำจัดอุปกรณ์ไปแล้ว ลบบัญชีออนไลน์ของคุณหากไม่จำเป็นต้องใช้งานร่วมกับอุปกรณ์ IoT อีกต่อไป

2. **ทำการรีเซ็ตอุปกรณ์เป็นค่าเริ่มต้นจากโรงงาน** การรีเซ็ตอุปกรณ์เป็นค่าเริ่มต้นจากโรงงานถูกออกแบบมาเพื่อลบข้อมูลที่จัดเก็บไว้ในหน่วยความจำภายในและรีเซ็ตรหัสผ่าน ชื่อผู้ใช้ และการตั้งค่าต่าง ๆ กลับไปเป็นค่าเริ่มต้น ตรวจสอบคู่มือการใช้งานของอุปกรณ์หรือเว็บไซต์ของผู้ผลิตเพื่อดูข้อมูลเกี่ยวกับวิธีการรีเซ็ตอุปกรณ์เป็นค่าเริ่มต้นจากโรงงาน

3. **ยกเลิกการเชื่อมต่ออุปกรณ์ออกจากโทรศัพท์มือถือและอุปกรณ์อื่น ๆ** การกำจัดอุปกรณ์ที่ยังสามารถเข้าถึงอุปกรณ์อื่น ๆ เข้าถึงเครือข่าย หรือบัญชีออนไลน์ของคุณอยู่ ยังมีความเป็นไปได้ที่ผู้อื่นจะเข้าถึงข้อมูลของคุณได้ ให้แน่ใจได้ว่าคุณได้ตรวจสอบอุปกรณ์อื่น ๆ และได้ยกเลิกการจับคู่ออกจากอุปกรณ์ที่คุณจะกำจัดแล้ว ยกเลิกสิทธิ์การเข้าถึงของแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ที่ไม่จำเป็นต้องใช้งานแล้ว

4. **ถอดสื่อบันทึกข้อมูลที่ถอดออกได้ (เช่น แฟลชไดรฟ์ USB การ์ดหน่วยความจำ ฯลฯ) ที่เชื่อมต่อกับอุปกรณ์ออกให้หมด** สื่อบันทึกข้อมูลที่ถอดออกได้อาจยังเก็บข้อมูลส่วนตัวที่ไม่ได้ถูกลบในระหว่างการรีเซ็ตเป็นค่าเริ่มต้นจากโรงงาน จึงควรถอดออกทำลายทิ้ง และกำจัดแยกต่างหากจากตัวอุปกรณ์

ความช่วยเหลือ

ติดต่อศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลีย (Australian Cyber Security Centre) ของหน่วยข่าวกรองสัญญาณออสเตรเลีย (Australian Signals Directorate) ทางอีเมลที่ asd.assist@defence.gov.au หรือโทรสายด่วนได้ตลอด 24 ชั่วโมงทุกวันสำหรับความช่วยเหลือเร่งด่วนที่ **1300 CYBER1 (1300 292 371)**

แจ้งเหตุอาชญากรรมไซเบอร์ไปยัง ReportCyber ได้ที่ www.cyber.gov.au/report

ติดต่อ IDCARE ทางเว็บไซต์ได้ที่ www.idcare.org หากคุณประสบปัญหาการโจรกรรมอัตลักษณ์บุคคล

เยี่ยมชมเว็บไซต์ www.cyber.gov.au เพื่อขอรับคำแนะนำสำหรับคุณและครอบครัว สมัครรับบริการแจ้งเตือนฟรีจาก ACSC เพื่อรับข้อมูลเกี่ยวกับภัยคุกคามทางออนไลน์ล่าสุด

มาร่วมกันทำให้ออสเตรเลียเป็นสถานที่ที่ปลอดภัยที่สุดในการเชื่อมต่อแบบออนไลน์

สำหรับคำแนะนำเกี่ยวกับความปลอดภัยทางไซเบอร์ เยี่ยมชมเว็บไซต์ www.cyber.gov.au

ข้อจำกัดความรับผิดชอบ

เนื้อหาในคู่มือนี้มีลักษณะทั่วไปและไม่ควรยึดถือว่าเป็นคำแนะนำทางกฎหมายหรือเป็นที่พึ่งสำหรับความช่วยเหลือในสถานการณ์เฉพาะหรือสถานการณ์ฉุกเฉินใด ๆ ในเรื่องที่สำคัญใด ๆ คุณควรขอคำแนะนำจากผู้เชี่ยวชาญอิสระที่เหมาะสมกับสถานการณ์ของคุณเอง

เครือรัฐจะไม่รับผิดชอบหรือมีส่วนรับผิดต่อความเสียหาย การสูญเสีย หรือค่าใช้จ่ายที่เกิดขึ้นจากการพึ่งพาข้อมูลที่มีอยู่ในคู่มือนี้

สงวนลิขสิทธิ์

สำหรับข้อมูลเพิ่มเติมหรือรายงานเหตุการณ์ที่เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ ติดต่อเราที่

เว็บไซต์ cyber.gov.au | โทร 1300 CYBER1 (1300 292 371)

หมายเลขนี้มีไว้สำหรับใช้ภายในออสเตรเลียเท่านั้น

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre