# 15 วิธีเพิ่มความปลอดภัยให้กับระบบ IoT

- อุปกรณ์ต่างๆ ที่ควบคุมหรือสั่งการผ่านทางการเชื่อมต่ออินเทอร์เน็ต กลายเป็นเทคโนโลยีที่ช่วยเพิ่มความสะดวกสบายให้แก่มนุษย์ เปลี่ยนจากบ้านธรรมดา ๆ เป็น Smart Home ได้อย่างง่ายๆ เช่น Smart TV, CCTV & Home Security System, Smart Refrigerator, Thermostat ระบบควบคุมไฟฟ้า ฯลฯ ซึ่งเรียกว่า Internet of Things (IoT) แต่ใช่ว่าจะปลอดภัยเสมอไป อุปกรณ์บางประเภทไม่มีมาตรการรักษาความปลอดภัยที่เพียงพอ เสี่ยงต่อการถูกแฮกเกอร์โจมตีได้ เช่น ถูกโขมยข้อมูลส่วนบุคคล ถูกสอดแนม หรือ อาจทำให้อุปกรณ์และเครือข่ายใช้งานไม่ได้อีกต่อไปเลยก็ได้

# สาเหตุหลัก ๆ ที่เสี่ยงต่อการถูกโจมตี

- 1. อุปกรณ์ไม่ได้มีมาตรการรักษาความปลอดภัยที่เพียงพอ
- 2. อุปกรณ์ไม่ได้ทำการอัปเดตแพทช์อย่างสม่ำเสมอ
- 3. ใช้รหัสผ่าน Default มาตลอด โดยไม่ยอมเปลี่ยน Username , Password

- 1. เปลี่ยนชื่อ Router
- 2. เลือกวิธีการเข้ารหัสที่รัดกุมสำหรับ Wi-Fi
- 3. แยกเครือข่าย Wi-Fi สำหรับ Visitors โดยเฉพาะ
- 4. เปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นทันที
- 5. ใช้รหัสผ่านที่รัดกุมสำหรับเครือข่าย Wi-Fi และบัญชีอุปกรณ์ IoT
- 6. ตรวจสอบการตั้งค่าเริ่มต้นของอุปกรณ์ IoT
- 7. ปิด Features ที่ไม่ได้ใช้งาน
- 8. Disconnect อุปกรณ์บางชนิดเมื่อไม่ได้ใช้งาน

- 9. Update Firmware สม่ำเสมอ
- 10. Upgrade อุปกรณ์ IoT ให้ทันสมัย
- 11. เปิดใช้งานการยืนยันตนแบบสองปัจจัย (2FA)
- 12. หลีกเลี่ยงเครือข่าย Wi-Fi สาธารณะ
- 13. Disable การเปิดใช้ Universal Plug-and-Play (UPnP) ใน Router
- 14. ดูแลมือถือให้ปลอดภัยอยู่เสมอ
- 5. ระวังผลกระทบจากไฟฟ้าดับชั่วขณะ

# 1. เปลี่ยนชื่อ Router

- ปกติผู้ผลิตจะใช้ยี่ห้อหรือรุ่นของ Router เป็นชื่อเริ่มต้นมาจากโรงงาน ผู้ใช้ควรเปลี่ยนเป็นชื่อที่ไม่สามารถระบุยี่ห้อหรือรุ่นของ Router ได้ เพื่อทำให้ยากสำหรับมิจฉาชีพที่คิดจะลักลอบเข้าสู่ระบบ นอกจากนี้อย่าตั้งชื่อที่มีส่วนเกี่ยวข้องกับผู้ใช้เอง เช่น ชื่อเล่น เลขที่บ้าน หรือข้อมูลใด ๆ ที่สามารถระบุตัวตนได้

# 2. เลือกวิธีการเข้ารหัสที่รัดกุมสำหรับ Wi-Fi

- เมื่อตั้งค่าใน Router ควรเลือกวิธีการเข้ารหัส WPA2 เป็นอย่างน้อย ซึ่งในปัจจุบันมีวิธีการเข้ารหัสแบบใหม่ WPA3 ซึ่งทำให้แฮกเกอร์คาดเดารหัสผ่านได้ยากขึ้นกว่าเดิม

# 3. แยกเครือข่าย Wi-Fi สำหรับ Visitors โดยเฉพาะ

- หากมีเพื่อนและญาติมาที่บ้าน ควรสร้างเครือข่ายอีกวงหนึ่งแยกออกผู้ใช้เหล่านั้นออกจากเครือข่ายของเจ้าของบ้านที่ผูกไว้กับอุปกรณ์ IoT เพื่อความปลอดภัยยิ่งขึ้น

# 4. เปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นทันที

- ชื่อผู้ใช้งานพร้อมรหัสผ่านเริ่มต้น (Default Username / Password) ที่มาพร้อมกับอุปกรณ์เป็นข้อมูลที่ผู้ผลิตพิมพ์ไว้ในคู่มือ ซึ่งใคร ๆ ก็เข้าถึงได้จึงรวมถึงแฮกเกอร์ด้วยเช่นกัน หลังจากแกะกล่องจึงควรรีบเปลี่ยนชื่อและรหัสผ่านใหม่ทันที

# 5. ใช้รหัสผ่านที่รัดกุมสำหรับเครือข่าย Wi-Fi และบัญชีอุปกรณ์ IoT

- หลีกเลี่ยงคำหรือรหัสผ่านที่สามารถคาดเดาได้ง่าย เช่น “password” หรือ “123456” โดยต้องตั้งรหัสผ่านที่ซับซ้อน ซึ่งควรคละไปด้วยตัวอักษรใหญ่-เล็ก ตัวเลขและสัญลักษณ์ ไม่ควรใช้รหัสผ่านที่ซ้ำกันในแต่ละบัญชี นอกจากนี้อาจเลือกใช้โปรแกรมจัดการรหัสผ่าน (Password Manager) เพื่อความปลอดภัยที่สะดวกยิ่งขึ้น

# 6. ตรวจสอบการตั้งค่าเริ่มต้นของอุปกรณ์ IoT

- ควรศึกษาการตั้งค่าเริ่มต้นของอุปกรณ์ หากพบว่าการตั้งค่าเริ่มต้นบางอย่างทำให้เกิดความเสี่ยงด้านความปลอดภัยและความเป็นส่วนตัว เช่น การเก็บและ Track ข้อมูลพฤติกรรมส่วนตัวของผู้ใช้มากเกินไป ก็ควรปรับการตั้งค่านั้น

# 7. ปิด Features ที่ไม่ได้ใช้งาน

- อุปกรณ์ IoT มาพร้อมกับ Features ที่เพิ่มความสะดวกในการควบคุมการใช้งาน เช่น Remote Access ซึ่งมักจะเปิดใช้งานเป็นค่าเริ่มต้น ควร Disable หรือตั้ง Off ไว้หากไม่ได้ใช้งาน

# 8. Disconnect อุปกรณ์บางชนิดเมื่อไม่ได้ใช้งาน

- อุปกรณ์ IoT บางชนิดจำเป็นที่จะต้องใช้การเชื่อมต่ออินเทอร์เน็ตตลอดเวลา เช่น ระบบควบคุมไฟฟ้าภายในบ้าน แต่อุปกรณ์ที่มีไมโครโฟนและกล้องวิดีโอ ควร Disconnect จากเครือข่ายทันทีหลังเลิกใช้งาน ไม่จำเป็นต้องเชื่อมต่อตลอดเวลา เพื่อลดความเสี่ยงจากการถูกสอดแนมจากแฮกเกอร์

# 9. Update Firmware สม่ำเสมอ

- ควรตั้งค่าเปิดให้อัปเดท Firmware หรือ Patch แบบอัตโนมัติ (ถ้ามี) เนื่องจากผู้ผลิตมักแก้ไขข้อบกพร่องด้านความปลอดภัยออกมาเป็นระยะ ๆ ตามสถานการณ์ช่องโหว่ที่เกิดขึ้น

# 10. Upgrade อุปกรณ์ IoT ให้ทันสมัย

- นอกจากการ Update Firmware ของอุปกรณ์แล้ว ผู้ใช้ควรพิจารณา Upgrade ตัวอุปกรณ์ด้วย เช่น กรณีที่อุปกรณ์รุ่นเก่า ๆ อาจไม่รองรับ Software เวอร์ชันปัจจุบัน หรืออุปกรณ์รุ่นใหม่ที่มี Features ด้านความปลอดภัยที่ดีกว่าเดิม

# 11. เปิดใช้งานการยืนยันตนแบบสองปัจจัย (2FA)

- เพื่อความปลอดภัยที่มากขึ้นควรเปิด 2FA เพราะเมื่อมีกรณีรหัสผ่านของผู้ใช้ถูกขโมย แฮกเกอร์จะไม่สามารถเข้าสู่บัญชีของอุปกรณ์ได้ หากไม่ได้รับการยืนยันจากปัจจัยที่ 2 ไม่ว่าจะเป็น SMS หรือ Application ของเจ้าของ Account

# 12. หลีกเลี่ยงเครือข่าย Wi-Fi สาธารณะ

- อุปกรณ์ IoT บางชนิดอาจถูกพกพาติดตัวไปกับผู้ใช้เมื่อออกนอกบ้าน แต่ไม่ควรเชื่อมอินเทอร์เน็ตผ่าน Wi-Fi สาธารณะ แต่หากจำเป็นจริง ๆ ให้เชื่อมผ่าน VPN อีกชั้นหนึ่งเพื่อความปลอดภัยและความเป็นส่วนตัว

# 13. Disable การเปิดใช้ Universal Plug-and-Play (UPnP) ใน Router

- อุปกรณ์ที่ใช้ Universal Plug and Play (UPnP) จัดเป็นอุปกรณ์ที่มีช่องโหว่มากที่สุดเนื่องจากโปรโตคอลนี้ อนุญาตให้อุปกรณ์ IoT เปิดพอร์ตในการเชื่อมต่อกับอินเทอร์เน็ตภายนอกโดยอัตโนมัติ แฮกเกอร์ใช้ช่องโหว่ UPnP ในการการโจมตี แนะนำให้ Disable หรือ Deactivate การใช้งานนี้ดีกว่า

# 14. ดูแลมือถือให้ปลอดภัยอยู่เสมอ

- สำหรับผู้ใช้ส่วนใหญ่ มือถือก็ไม่ต่างกับห้องควบคุมอุปกรณ์ IoT ดังนั้นผู้ใช้ควรระมัดระวังอย่าให้มือถือหาย หรือถูกขโมย ควรสำรองข้อมูลไปยังบัญชีออนไลน์ไว้เสมอ ตั้งค่าติดตามตำแหน่งอุปกรณ์เพื่อทำการ Lock และ Reset จากระยะไกล ควรตั้งค่า PIN ที่ซับซ้อนเพื่อการเข้าถึงข้อมูลในมือถือจากผู้อื่นได้ยากขึ้น

# 15. ระวังผลกระทบจากไฟฟ้าดับชั่วขณะ

- ตรวจสอบให้แน่ใจว่าในกรณีที่ไฟดับซึ่งส่งผลให้ฮาร์ดแวร์ IoT บางตัวหยุดทำงานชั่วคราวหรือ Reboot จะไม่ส่งผลกระทบด้านความปลอดภัย หรือต้องตั้งค่าใด ๆ ใหม่ทุกครั้ง

# อ้างอิงที่มา:


- https://us.norton.com/internetsecurity-iot-smart-home-security-core.html
- https://www.lifehack.org/353418/10-essential-security-tips-for-your-internet-things
- https://www.techopedia.com/6-tips-for-securing-an-iot-device/2/33720
- https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-6