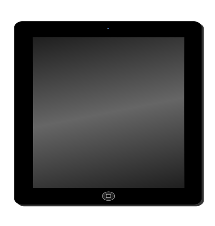
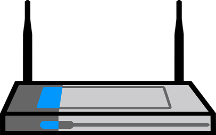
**Wireless Network Compromised**

**Wireless/Wi-Fi** ลักษณะของการใช้อุปกรณ์ด้านสื่อสารโทรคมนาคม แปลตรงตัวว่าไร้สาย ฉะนั้นอุปกรณ์อะไรก็ตามที่ติดต่อสื่อสารกันโยไม่ใช้สายสัญญาณถือว่าอุปกรณ์นั้นเป็น Wireless เหมือนกันเพราะฉะนั้นจะเรียก Wi-Fi ก็ได้

**Wi-Fi** เป็นเทคโนโลยีเครือข่ายไร้สายที่อนุญาตให้อุปกรณ์ต่าง ๆ เช่นคอมพิวเตอร์ (แล็ปท็อป และ เดสก์ท็อป) อุปกรณ์มือถือ (สมาร์ทโฟนและอุปกรณ์สวมใส่) และอุปกรณ์อื่น ๆ (เครื่องพิมพ์และกล้องวิดีโอ) เชื่อมต่อกับอินเทอร์เน็ต จะช่วยให้อุปกรณ์เหล่านี้ และอื่น ๆ อีกมากมายแลกเปลี่ยนข้อมูลซึ่งกันและกันสร้างเครือข่าย การเชื่อมต่ออินเทอร์เน็ตเกิดขึ้นผ่านเราเตอร์ไร้สาย เมื่อคุณเข้าถึง Wi-Fi คุณกำลังเชื่อมต่อกับเราเตอร์ไร้สายที่อนุญาตให้อุปกรณ์ที่รองรับ Wi-Fi ของคุณเชื่อมต่อกับอินเทอร์เน็ต

**WPA/WPA2** เทคโนโลยีการรักษาความปลอดภัยที่ปกป้องเครือข่าย Wi-Fi ของคุณโดยการเข้ารหัสการจราจรบนเครือข่าย นอกจากนี้ ยังทำให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงเครือข่ายได้ยากขึ้น

**การทำงานของ WI-FI** ในด้านเทคนิคมาตรฐาน IEEE 802.11 จะกำหนดโปรโตคอลที่เปิดใช้งานการสื่อสารกับอุปกรณ์ไร้สายที่เปิดใช้งาน Wi-Fi ในปัจจุบันรวมถึงเราเตอร์ไร้สายและจุดเชื่อมต่อไร้สาย จุดเชื่อมต่อไร้สายรองรับมาตรฐาน IEEE ที่แตกต่างกัน แต่ละมาตรฐานคือการแก้ไขที่ได้รับการยอมรับเมื่อเวลาผ่านไป มาตรฐานทำงานกับความถี่ที่แตกต่างส่งแบนด์วิดท์ที่แตกต่างกันและรองรับจำนวนช่องสัญญาณที่แตกต่างกัน

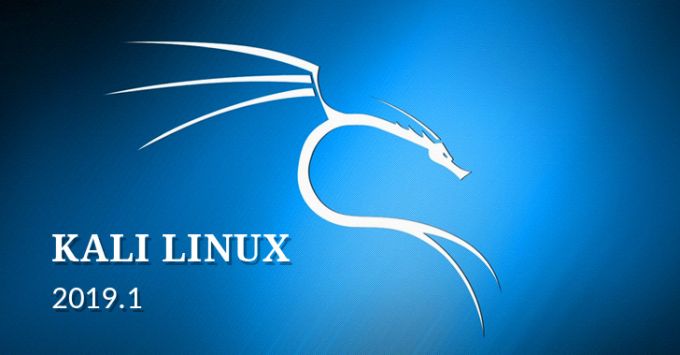


**รูปแบบการให้บริการเครือข่ายไร้สาย มี 2 รูปแบบ**

1. บริการในพื้นที่สาธารณะ (Public Wireless Network) ส่วนใหญ่จะเป็นผู้ให้บริการที่มีความเชี่ยวชาญและมีความรู้เฉพาะที่เกี่ยวกับการให้บริการเครือข่ายไร้สายอยู่แล้ว เช่น True WiFi, 3BB Hotspot, TOT Wi-Fi ซึ่งการขอใช้บริการส่วนใหญ่จำเป็นต้องเปิดให้บริการโดยการลงทะเบียนรับเอกสารข้อมูลการยืนยันตัวตน เช่น ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเข้าใช้งาน
2. บริการในพื้นที่ส่วนตัว (Private Wireless Network) เช่น ในบริเวณบ้าน หรือในบริเวณสำนักงานเล็ก ๆ และการใช้งานจะครอบคลุมพื้นที่การใช้งานในระยะใกล้

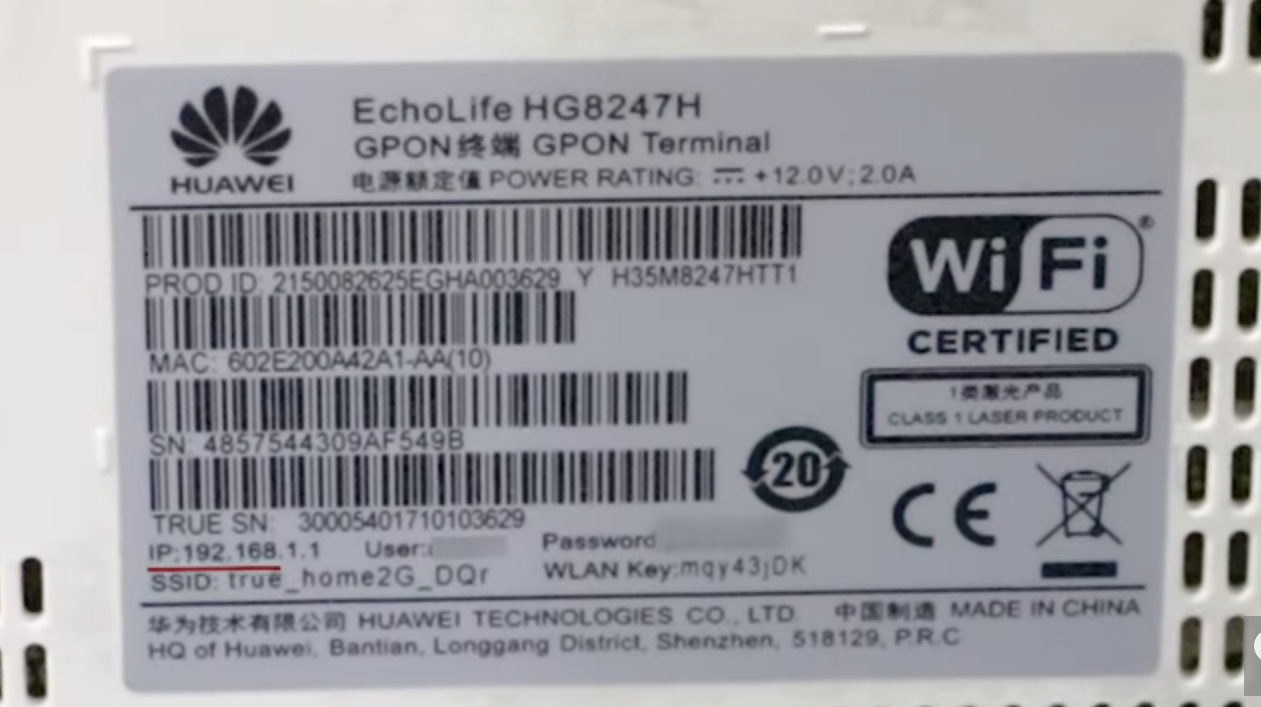
**ช่องโหว่ Wi-Fi** Router Wi-Fi หลายยี่ห้อมักใช้ชิพคอมพิวเตอร์ราคาถูกซึ่งแฮคเกอร์แคทีเดียวก็ได้รหัสผ่าน นักวิจัยด้านความปลอดภัยรายงานว่าชิพคอมพิวเตอร์ยอดนิยมที่ใช้ในเร้าท์เตอร์มักจะใช้วิธีสร้างตัวเลขแบบสุ่ม “random number generator” ล่าสุดค้นพบว่าวิธีนี้ไม่ได้สุ่มตัวเลขแบบที่ควรจะเป็น เราท์เตอร์บางยี่ห้อนั้นมักง่ายใช้ตัวเลข “0” เป็นประจำ เพื่อขโมยรหัสผ่านของ Wi-Fi router สิ่งที่แฮคเกอร์ต้องทำก็คือ รู้ว่าเร้าเตอร์นั้นเป็นรุ่นอะไรก่อน หลังจากนั้นต้องรู้ว่าตัวเลขต่อไปคืออะไรแล้วส่งตัวเลขนี้กลับไปยังเร้าท์เตอร์ ทีนี้แฮคเกอร์ก็จะได้ PIN code และรหัสผ่าน Wi-Fi ต่อจากนั้นก็สามารถล็อกอินเข้าเครือข่ายเพื่อดักขโมยข้อมูลที่ส่งระหว่างเร้าเตอร์และอุปกรณ์ เร้าเตอร์ที่ได้รับผลกระทบก็คือเครื่องที่ใช้มาตรฐานความปลอดภัยแบบ WPS ที่หลาย ๆ ยี่ห้อนิยมใช้กัน

**โปรแกรมแฮก Wi-Fi Kali Linux** คือ โอเอสลินุกซ์แบบหนึ่ง พัฒนาขึ้นมาเพื่อจุดประสงค์ทางด้านตรวจสอบความปลอดภัยของระบบเครือข่าย โดยภายในจะมีคำสั่งต่าง ๆ ที่เกี่ยวข้องกับการทำงานและตรวจสอบระบบที่จำเป็นไว้ทั้งหมด รวมทั้งสามารถดักสัญญาณไวร์เลส ดับจับแพ็กเกจ หรือ Sniffer ได้ นั่นจึงทำให้แฮกเกอร์ประยุกต์ใช้ Kali Linux ในการแฮกไวร์เลสแลนที่เข้ารหัสผ่านแบบ WPA หรือ WPA2 ได้ด้วยเช่นกัน

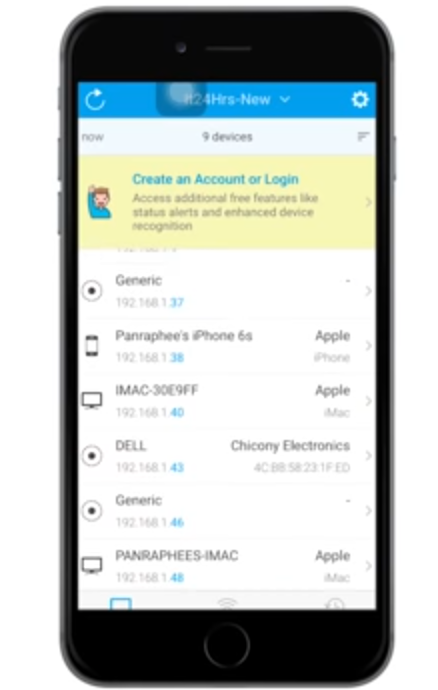


**การป้องกัน**

1. เปิด Web Browser แล้วก็พิมพ์หมายเลข IP ของ Router ลงไปอย่างเช่น 192.168.1.1 จากนั้นก็คลิกเข้าหน้าตั้งค่า Router ก็จะดูได้เลยว่าตอนนี้มีจำนวนเครื่องที่เชื่อมต่ออยู่กับเรามีกี่เครื่อง เครื่องไหนบ้าง อุปกรณ์ขึ้นน่าสงสัยเป็นแขกไม่ได้รับเชิญหรือเปล่าแต่ว่าเราเตอร์



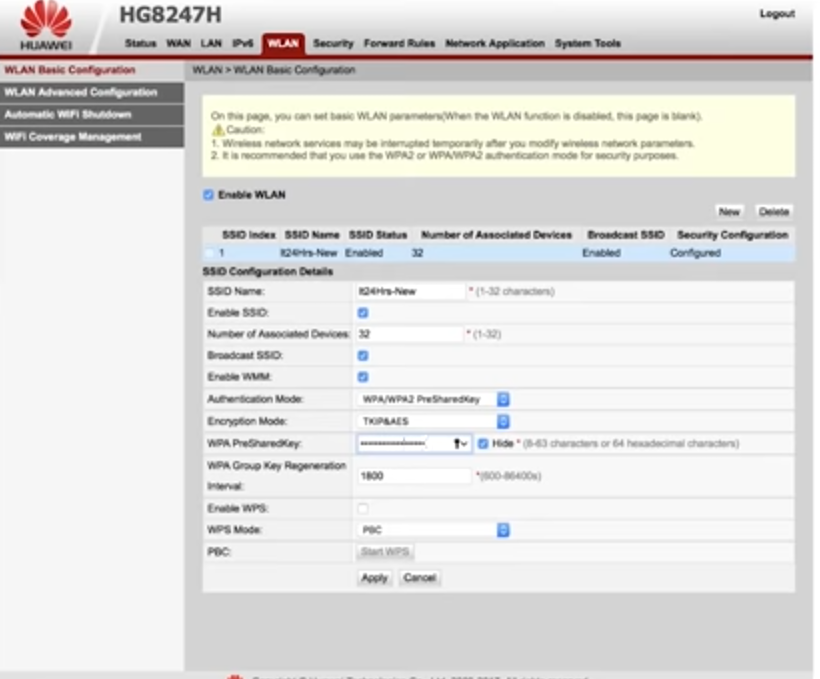
1. เปิด App มือถือดูก็ได้ finished work Today ว่ามีใครบ้างที่เชื่อมต่อใช้ WiFi เดียวกันกับเราอยู่ใช้ได้ทั้ง iOS และ Android เป็น App ที่ช่วยค้นหาอุปกรณ์ที่มีการเชื่อมต่ออยู่ในระบบเครือข่ายทั้งหมด



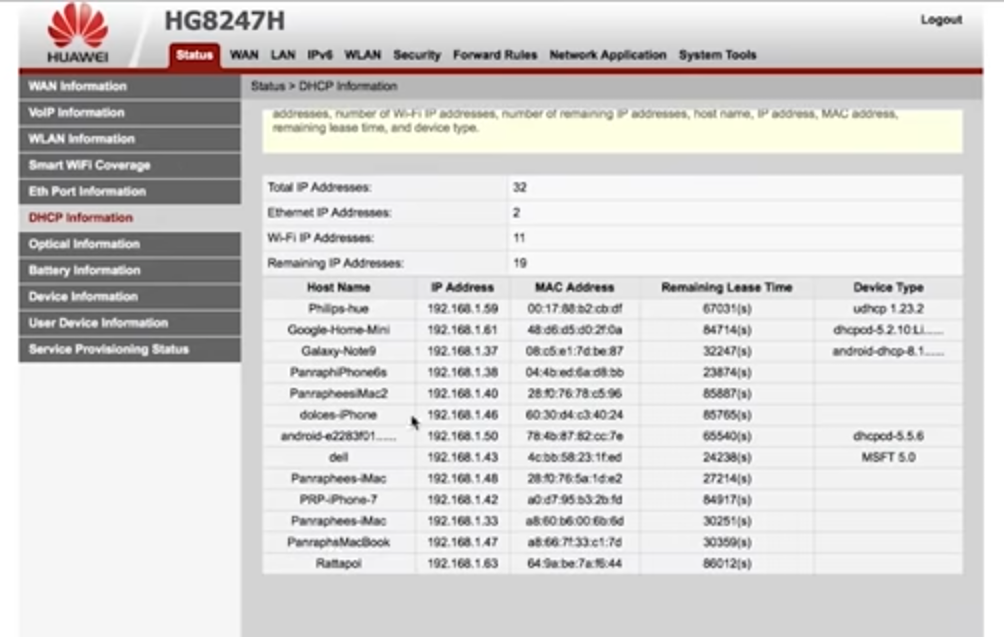
1. พยายามติดตั้งอุปกรณ์ Router ไว้กลางบ้านไกล ๆ หน้าต่าง ไม่ให้ใกล้หน้าต่างสัญญาณก็ไม่มีไปถึงคนอื่น



1. การตั้งรหัสสำหรับเข้าใช้ WiFi ใครอยากจะเชื่อมต่อ WiFi ก็ต้องรู้รหัส ใส่รหัสไม่ถูก ก็เข้าไม่ได้ ต้องเข้าไปตั้งค่า Router ของเราโดยเปิดเว็บบราวเซอร์ขึ้นมาแล้วก็พิมพ์หมายเลข IP Router 192.168.1.1 ซึ่งแต่ละเครื่องหมายเลขบัญชีก็อาจจะแตกต่างกันไป จากนั้นก็ทำการ login เข้าสู่หน้าการตั้งค่า Router แล้วก็ทำการตั้งรหัสผ่าน



1. ปิดซ่อน wireless ไม่ให้มีใครเห็น ป้องกันคนข้างบ้านหรือคนทั่วไปเห็น wi-fi





**ผิดตามมาตรา** ดังนั้นจะมีความผิดตาม ม.5 "ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้น มิได้มีไว้สำหรับตน..." พิจารณาองค์ประกอบ คือการเข้าถึงโดยมิชอบ กฎหมายไม่ได้ใช้คำว่าโดยทุจริตเหมือนกฎหมายอาญา แต่ถ้าจะแปลให้สอดคล้องกับเจตนารมณ์ และองค์ประกอบสุดท้าย "มาตรการนั้นมิได้มีไว้สำหรับตน" น่าจะต้องดูว่าได้รับอนุญาตจากเจ้าของหรือไม่ ถ้าได้รับอนุญาตก็เป็นการเข้าถึงโดยชอบ ถ้าเขาแจกรหัสให้ลูกค้า แล้วคุณเป็นลูกค้า แม้ต่อมาเดินออกจากร้านแล้ว ยังเล่นได้อยู่ ก็ไม่น่าจะผิดนะ การเข้าไปก่อกวนหรือไม่ ไม่ใช่ประเด็น เพราะไม่ใช่องค์ประกอบความผิดตามมาตรานี้ สังเกต ม.11 "อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข" แบบนี้จึงต้องมีพฤติการณ์ประกอบการกระทำ