www.ez-admin.com

ศูนย์อบรมสำหรับผู้ต้องการก้าวสู่อาชีพผู้ดูแลระบบ เครือข่ายคอมพิวเตอร์ โดยเรียนรู้จากการปฏิบัติงานจริง

“เราจะทำเรื่องยากให้เข้าใจง่ายด้วยสิ่งเหล่านี้”

- จัดอบรมเป็นกลุ่มเล็กๆ เพื่อให้การเรียนการสอนเกิดประสิทธิภาพสูงสุด
- เน้นเนื้อหาที่นำไปใช้งานได้จริง ถ่ายทอดให้ผู้เรียนเข้าใจได้ง่าย
- จัดทำคู่มือที่อ่านง่าย ทำตามได้ เพื่อให้ผู้เรียนนำไปต่อยอดหลังจากอบรม
- บริการอบรมซ้ำ เพื่อให้ผู้เรียนได้ทบทวนความรู้ให้เข้าใจได้ชัดเจนมากขึ้น

บริการเสริมที่น่าสนใจ : บริการติดตั้งระบบเครือข่ายคอมพิวเตอร์ ระบบ WiFi Hotspot ด้วย MikroTik บริการดูแลระบบเครือข่าย บริการติดตั้งระบบ Thin Client หรือ Zero Client คลิกดูรายละเอียดได้ที่ service.ez-admin.com

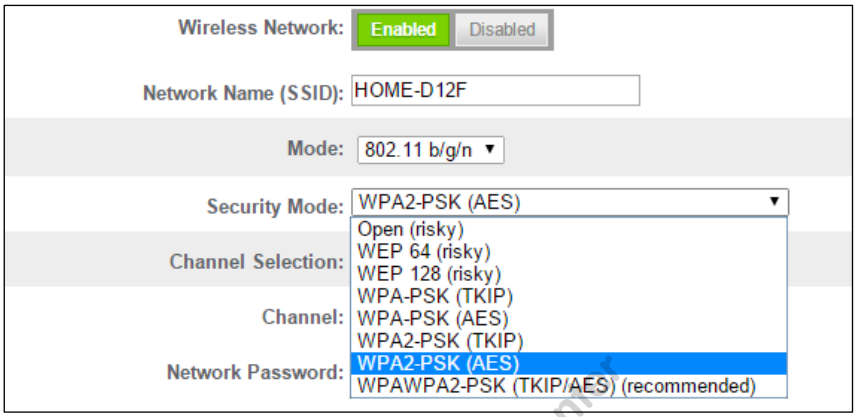
ชี้ชัด!!! ความปลอดภัยและการเข้ารหัสของ Wi-Fi เลือกแบบไหนดี

หลายคนคงสับสนไม่น้อยเวลาที่กำหนดค่าการเข้ารหัสที่ตัว Access Point เพราะมีตัวเลือกมากมาย เช่น WEP, WPA, WPA2-TKIP, WPA2-AES หรือ Open ดังนั้นบทความนี้จะชี้ชัดกันเลยว่าการเข้ารหัสแบบไหนที่ปลอดภัยและให้ประสิทธิภาพในการทำงานมากที่สุด

ทำไมต้องเข้ารหัส?

การเข้ารหัสเชื่อมต่อ Access Point เพื่อป้องกันไม่ให้บุคคลอื่นสามารถเชื่อมต่อเข้ามาในระบบเครือข่ายของเราโดยไม่ได้รับอนุญาต ไม่อย่างนั้นคลื่นไร้สายที่แพร่กระจายออกมาจาก Access Point ของเราอาจทำให้ผู้ไม่หวังดีเชื่อมต่อเข้ามาที่ Access Point แล้วโจมตีการทำงานระบบเครือข่ายของเราได้โดยง่าย รวมถึงยังสามารถดักจับข้อมูลสำคัญ และเข้าใช้งานอินเทอร์เน็ตแบบผิดกฎหมายแล้วโยนความผิดมาที่เราได้

ดังนั้นการเข้ารหัสจึงเป็นสิ่งสำคัญเมื่อเราเปิดใช้งาน Access Point แต่การเลือกมาตรฐานการเข้ารหัสที่ไม่เหมาะสมก็อาจมีผลกระทบกับการใช้งาน Wi-Fi ของเรา ดังนั้นการทำความเข้าใจกับตัวเลือกต่างๆ ในระดับหนึ่ง ย่อมเป็นสิ่งที่เราควรทำ เพื่อให้สามารถตัดสินใจเลือกค่าที่เหมาะสมได้ด้วยตัวของเราเอง



รู้จักกับเทคโนโลยีความปลอดภัยของ Wi-Fi

ใน Router หรือ Access Point จะมีตัวเลือกเทคโนโลยีความปลอดภัยของระบบไร้สายและการเข้ารหัสอยู่หลายคำสั่ง แต่โดยส่วนใหญ่ที่พบเห็นได้ในหลายๆ ยี่ห้อ มีดังนี้

- Open : เปิดการใช้งาน Wi-Fi โดยไม่มีการเข้ารหัสใดๆ เราไม่ควรเลือกคำสั่งนี้ เพราะนั่นหมายถึงใครก็สามารถเชื่อมต่อเข้ามาในระบบเครือข่ายของเราได้ หรือใช้งานอินเทอร์เน็ตของเราเพื่อไปทำสิ่งที่ผิดกฎหมาย
- WEP 64 หรือ WEP 128 : เป็นเทคโนโลยีความปลอดภัยของระบบไร้สายโดยใช้โปรโตคอล WEP (Wired Equivalent Privacy) แบบเก่า แม้ WEB 128 จะปรับปรุงให้ใช้ขนาดคีย์ในการเข้ารหัสที่มีความซับซ้อนมากขึ้น แต่ทั้ง 2 มาตรฐานนี้ก็ยังถือว่าไม่มีความปลอดภัยอยู่ดี
- WPA-PSK (TKIP) : เป็นเทคโนโลยีความปลอดภัยของระบบไร้สายโดยใช้โปรโตคอล WPA เวอร์ชั่น 1 (Wi-Fi Protected Access) โดยใช้การเข้ารหัสแบบ TKIP ทำให้มีความปลอดภัยมากกว่า WEP แต่ปัจจุบันการใช้ WPA แบบ TKIP สามารถถูก Hack ได้อย่างรวดเร็วแล้ว
- WPA-PSK (AES) เป็นเทคโนโลยีความปลอดภัยของระบบไร้สายแบบ WPA แต่ใช้การเข้ารหัสแบบ AES ที่เข้ามาแทนที่ TKIP ซึ่งใช้รูปแบบการเข้ารหัสรูปแบบใหม่ที่มีความปลอดภัยมากขึ้น แต่อุปกรณ์ส่วนใหญ่ที่เข้ารหัสแบบ AES มักจะรองรับ WPA2 เท่านั้น ทำให้อาจมีปัญหากับ WPA ที่ใช้การเข้ารหัสแบบ AES
- WPA2-PSK (TKIP) เป็นเทคโนโลยีความปลอดภัยของระบบไร้สายแบบใหม่ที่มาแทน WPA ที่เริ่มจะมีช่องโหว่ให้เจาะมากขึ้นเรื่อยๆ แต่มีจุดด้อยตรงที่ยังใช้การเข้ารหัสแบบ TKIP ซึ่งยังเป็นแบบเก่าอยู่ ทำให้มีความเร็วในการรับส่งข้อมูลที่ช้ากว่า AES เนื่องจากไม่รองรับกับมาตรฐาน Wireless แบบใหม่ เช่น 802.11n หรือ 802.11ac

- WPA2-PSK (AES) เป็น WPA2 ที่ใช้การเข้ารหัสแบบ AES ทำให้มีความปลอดภัยและความเร็วมากกว่ามาตรฐานอื่นๆ เนื่องจากรองรับมาตรฐาน 802.11n/ac แต่อาจมีปัญหากับอุปกรณ์รุ่นเก่าที่ไม่รองรับการเข้ารหัสแบบ AES
- WPA2-PSK (TKIP/AES) เป็น WPA2 ที่ใช้การเข้ารหัสแบบผสมผสาน เพื่อให้รองรับการเชื่อมต่อได้ทั้งกับอุปกรณ์รุ่นเก่าและใหม่ แต่อาจทำให้มีช่องโหว่จะการทำงานของ TKIP ซึ่งสามารถถูกเจาะช่องโหว่ได้ง่าย

ความแตกต่างระหว่าง TKIP และ AES

การเข้ารหัส TKIP และ AES ถูกนำมาใช้ร่วมกับเทคโนโลยีด้านความปลอดภัยของ Wi-Fi แบบ WPA/WPA2 ซึ่งการเข้ารหัสทั้ง 2 แบบนี้มีความแตกต่างกันพอสมควร และจะมีผลต่อการทำงานของเครือข่ายไร้สายของเราอย่างมาก

TKIP เป็นการเข้ารหัสรุ่นเก่าที่นำมาใช้กับ WPA เพื่อแทนที่ WEP ทำให้การทำงานส่วนใหญ่คล้ายกับการเข้ารหัสบน WEP จึงมีปัญหาในเรื่องความปลอดภัยอย่างมาก นอกจากนี้ยังรองรับมาตรฐาน Wireless แบบเก่า คือ b/g เท่านั้น จึงทำงานที่ความเร็วสูงสุดเพียงแค่ 54 Mbps

AES เป็นมาตรฐานการเข้ารหัสแบบใหม่ที่ทำงานร่วมกับ WPA โดยเฉพาะ จึงมีความปลอดภัยสูงจนได้รับการรับรองโดยรัฐบาลสหรัฐ รองรับมาตรฐาน Wireless แบบใหม่ เช่น 802.11n/ac ได้ มีความเร็วในการรับส่งข้อมูลสูงถึง 300 Mbps ขึ้นไป และไม่เพียงแต่ใช้ร่วมกับเครือข่ายไร้สายเท่านั้น ยังสามารถนำไปใช้ร่วมกับ Services อื่นได้อีกด้วย เช่น การเข้ารหัสบน VPN หรือการเข้ารหัสข้อมูลในฮาร์ดดิสก์ แต่อาจมีจุดอ่อนที่อาจถูกเจาะช่องโหว่ด้วยการโจมตีแบบ Brute-Force (สุ่มรหัสผ่านเข้ามาเรื่อยๆ จนกว่าจะถูกต้อง) ซึ่งสามารถป้องกันได้โดยการกำหนดรหัส Passphrase ให้มีความยาวไม่น้อยกว่า 9 ตัว และควรมีอักษรตัวเล็ก, ตัวใหญ่, ตัวเลข และอักขระพิเศษปนเข้าไปด้วย

ชี้ให้ชัด

มาถึงช่วงของการชี้ให้ชัดกันแล้วว่า มาตรฐานการทำงานและการเข้ารหัสแบบไหนดี จึงจะเหมาะสมกับการใช้งานของเรา

หากอุปกรณ์หรือ Access Point ที่เราใช้งานอยู่เป็นอุปกรณ์รุ่นใหม่ ทำให้ไม่ต้องกังวลว่าจะใช้งานร่วมกับมาตรฐานการทำงานหรือการเข้ารหัสแบบใหม่ แนะนำให้เลือกตัวเลือกที่ดีที่สุด ทั้งด้านความปลอดภัยและความเร็วในการรับส่งข้อมูล **ชี้ชัดไปเลยว่าให้เลือก WPA2-AES เท่านั้น**

แต่ถ้าอุปกรณ์หรือเครื่อง Client ที่มาเชื่อมต่อ ส่วนใหญ่เป็นรุ่นกลางหรือเก่า ควรเลือกใช้ค่า WPA2-TKIP ซึ่งจะทำงานร่วมกับอุปกรณ์รุ่นเก่าได้ราบลื่นกว่า แต่ก็ต้องยอมรับกับความเร็วในการรับส่งข้อมูลที่ล่าช้าโดยเฉพาะในปัจจุบันที่ความเร็วของอินเทอร์เน็ตมากขึ้นเรื่อยๆ การใช้ WPA2-TKIP อาจเป็นตัวเลือกที่ล้าสมัยไปแล้ว

ปัจจุบันทั้งมาตรฐาน WEP และ WPA ทั้งแบบ TKIP/AES สามารถถูก Hack ได้ง่าย โดยใช้เวลาเพียงไม่กี่นาทีด้วยเครื่องมือยอดนิยมอย่างเช่น Aircrack **ชี้ชัดให้ยกเลิกการใช้งานทั้ง 2 มาตรฐานนี้ไปเลย**