Wi-Fi สาธารณะ ใช้อย่างไรให้ปลอดภัย

WI-FI ถือเป็นสิ่งสำคัญสำหรับการท่องโลกอินเทอร์เน็ตของผู้ใช้งาน Smart Device และ Computer ที่ชอบการเชื่อมต่อแบบไร้สาย ยิ่งเร็วยิ่งแรงยิ่งตอบโจทย์การใช้งานในยุค 5G ที่กำลังก้าวผ่านอย่างรวดเร็ว ที่สำคัญ **ถ้าใช้งานฟรี จะเป็นที่ถูกตาต้องใจกับผู้ที่เข้าถึงได้อย่างไม่มีขีดจำกัด และนั่นคือประเด็นสำคัญสำหรับบทความนี้ เพราะหลายท่านเมื่อเข้าสู่พื้นที่สาธารณะ จำเป็นต้องใช้งานระบบ internet ผ่านเครือข่ายของโทรศัพท์มือถือซึ่งมีการคิดค่าบริการตามการใช้งานและ package ที่กำหนดไว้ การมี WI-FI ที่เข้าถึงและใช้งานได้ฟรี จึงเป็นการลดภาระค่าใช้จ่ายและสงวนความเร็วอินเทอร์เน็ตไว้ใช้ยามจำเป็นได้อย่างดี** จากประเด็นดังกล่าว จึงเป็นเหตุผลชั้นดีที่ อาชญากรทาง cyber หรือผู้ไม่ประสงค์ดี สามารถใช้ช่องว่างตรงนี้ สร้าง WI-FI ฟรี เพื่อให้เราตกเป็นเหยื่อได้โดยแยบยล ในรูปแบบ FAKE FREE WI-FI

FAKE FREE WI-FI คือการจัดทำ WI-FI ที่เกิดจากเหล่าผู้ไม่ประสงค์ดี โดยจัดทำด้วยการปล่อย WI-FI หรือ Hot Spot จากเครื่องของตนเองในสถานที่ที่ให้บริการ FREE WI-FI แบบสาธารณะที่น่าเชื่อถือ และใช้สิ่งที่เปรียบเสมือนเหยื่อล่อให้ผู้สนใจเข้ามา connect เช่น

การตั้งชื่อให้สอดคล้องหรือใกล้เคียงกับสถานที่หรือชื่อ WI-FI ที่มีอยู่ เช่น ชื่อ WIFI ร้านกาแฟร้านหนึ่ง สมมติชื่อ coffeecup มีการให้บริการ FREE WI-FI ในร้านชื่อ coffeecup-wifi โดยให้ผู้ใช้งานนำรหัสที่ได้จากใบเสร็จไปทำการ login เพื่อใช้งาน ผู้ไม่ประสงค์ดีจะทำการสร้างชื่อของ WI-FI ให้สอดคล้องหรือใกล้เคียง เช่น coffeecup-wifi-free, @coffeecup-free-connect หรือที่นิยมมากที่สุดคือใส่ . หน้าชื่อ WIFI ปลอมที่ตั้งให้เหมือนจริง เช่น .coffeecup-wifi ซึ่งใกล้เคียงกับ coffeecup-wifi มากๆ ทำให้ผู้หลงเชื่อทำการ connect แล้วอาจจะถูกถาม เบอร์โทรศัพท์ หรือทำการ Redirect เปลี่ยนหน้าระบบให้ไปติดตั้งโปรแกรมบางอย่าง, ดึงข้อมูลรหัสผ่าน จากการใช้งานของคุณได้ทันที

การตั้งชื่อเชิญชวนหรือจงใจ ยกตัวอย่างต่อเนื่องจากด้านบน เช่น ชื่อจริงคือ coffeecup-wifi ผู้ไม่ประสงค์ดีจะเปลี่ยนให้เป็น freecoffee-here , free-wifi-1-hour , unlimited-wifi-for-shop เหล่านี้เป็นต้น **ซึ่งจะเร่งเร้าให้ผู้ใช้งานเกิดความต้องการอยากเข้าถึง โดยไม่สนใจความเสี่ยงที่เกิดขึ้น** การจงใจตั้งชื่อจริงเพื่อให้ผู้ใช้เลือกผิด โดยผู้ไม่ประสงค์ดีจะเจตนาใช้ชื่อเดียวกับ Official FREE WI-FI เป็นความเสี่ยงที่ส่งผลกระทบอย่างมากทั้งผู้ใช้งานและผู้เป็นเจ้าของที่แท้จริงจุดนี้ทางผู้ดูแลสถานที่ผู้ให้บริการควรตรวจสอบอยู่เสมอ

การป้องกันตนเองจากการใช้ FREE-WI-FI ในที่สาธารณะ ตรวจสอบการใช้งานและชื่อของ WI-FI ให้ถูกต้องก่อนการ connect เสมอ หากไม่จำเป็น อย่าใช้งาน App หรือข้อมูลที่เกี่ยวข้องกับ การเงิน , สุขภาพ หรือข้อมูลสำคัญที่มีความเสี่ยงต่อการถูกโจรกรรม อย่าเปิด Auto Connect สำหรับการใช้งาน WI-FI ในที่สาธารณะ เพราะอาจเป็นการละเลยการตรวจสอบการใช้งานของคุณได้ **หากเป็นไปได้ “ใช้อินเทอร์เน็ตของตนเองจากเครือข่ายมือถือ” ปลอดภัยกว่าการใช้ WI-FI สาธารณะ**ที่คุณอาจมีความเสี่ยงหากไม่ทำการตรวจสอบอย่างรอบคอบ นอกจากนี้ เมื่อเดินทางไปตามสถานที่ต่าง ๆ สิ่งแรกที่มักจะทำกันคือ

การขอรหัส Wi-Fi เพื่อใช้ฟรี แต่ก็ต้องระวังการใช้ Wi-Fi ที่อาจมีภัยแฝงซ่อนอยู่ วันนี้ทางศูนย์ฯ จึงนำคำแนะนำวิธีใช้ Wi-Fi สาธารณะให้ปลอดภัยมาแชร์ ดังนี้

1. ปิดระบบเชื่อมต่อ Wi-Fi แบบอัตโนมัติ ไม่ควรเปิดเชื่อมต่อ Wi-Fi แบบอัตโนมัติไว้ เพราะระบบอาจไปเชื่อมต่อกับ Wi-Fi ที่ไม่ปลอดภัย เสี่ยงถูกแฮกข้อมูลได้

2. เชื่อมต่อกับ Secured Public Network หรือเครือข่ายสาธารณะที่ปลอดภัย Wi-Fi ปลอม อาจใช้ชื่อคล้ายกับสถานที่ที่ให้บริการ ทำให้เกิดความเข้าใจผิดเผลอไปคลิกลิงก์ได้ จึงควรสังเกตเครือข่ายที่ปลอดภัย เช่น มีการให้สมัครสมาชิกก่อนการล็อกอิน หรือต้องกรอก Password ก่อนเข้าใช้งาน

3. เข้าเว็บไซต์ที่ปลอดภัยควรพิมพ์ URL เว็บไซต์เอง และสังเกตว่า URL เว็บไซต์เป็น HTTPS หรือรูปแม่กุญแจล็อกเพื่อมั่นใจได้ว่ามีการเข้ารหัสข้อมูลป้องกันความปลอดภัยหากมีการดักจับข้อมูลจากแฮกเกอร์

4. ยกเลิกการแชร์ไฟล์ เมื่อเชื่อมต่อ Wi-Fi เครื่องคอมพิวเตอร์ในเครือข่ายเดียวกัน จะสามารถเห็นเครื่องของเราได้ หากเปิดแชร์ไฟล์ไว้ ควรยกเลิกเพื่อป้องกันไม่ให้ผู้ไม่หวังดีเอาข้อมูลเราไปได้ง่าย

5. ไม่บันทึกรหัสผ่าน หรือเข้าสู่ระบบเว็บไซต์อัตโนมัติ เมื่อเปิดหน้าเว็บไซต์ ข้อมูลการเข้าสู่ระบบจะถูกส่งออกทันที หากเราเผลอเชื่อมต่อกับ Wi-Fi ผู้ไม่หวังดี จะทำให้เขาสามารถได้ข้อมูลเข้าสู่ระบบเราได้ทันที

บทสรุป ที่กล่าวมาขั้นต้นเป็นแนวทางการป้องกันตนเองของเราให้ห่างไกลจากการถูกจารกรรมข้อมูลที่จำเป็นต่อการใช้ชีวิตในยุคปัจจุบัน โดยเฉพาะการใช้ WI-FI ที่มีความจำเป็นต่อการจัดการสื่อข้อมูลที่เราสนใจอย่างหลากหลาย โดยในความเป็นจริงแล้วนั้น **การโจมตีส่วนของ WI-FI ของผู้ไม่ประสงค์ดี สามารถทำได้มากกว่าที่กล่าวมาอีกมากมายหลายแบบ บทความนี้จึงอยากขอเป็นส่วนหนึ่งที่จะทำให้ผู้อ่านได้ตระหนักถึงการป้องกันตนเองในยุคดิจิทัล** และสามารถส่งผ่านความปลอดภัยสู่คนที่คุณรักด้วยการส่งต่อข้อมูลดีๆ ในด้านความปลอดภัยนี้ไปด้วยกัน

ผู้จัดทำ/เรียบเรียง : นางสาวณัฏฐนันท์ คงทน / นสม.ชก
หน่วยงาน : ฝ่ายข่าวและรายการ สวท.ปัตตานี
แหล่งที่มา : ศูนย์ต่อต้านข่าวปลอม https://shorturl.asia/Wn9f6
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) https://shorturl.asia/TvQRO