WIFI Password-Stealer

SC362006 Information and Communication Technology Security

ศ. ดร.จักรชัย โสอินทร์

หลักการและเหตุผล

การขโมยรหัสไวไฟ (Wi-Fi Password Theft)
เป็นปัญหาที่กระทบต่อความปลอดภัยและความเป็นส่วนตัวของเจ้าของเครือข่าย อาจนำไปสู่การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การกระทำผิดกฎหมาย และทำให้เครือข่ายช้าลง
เหตุผลที่ควรตระหนักและป้องกันคือ ป้องกันข้อมูลรั่วไหล ลดความเสี่ยงจากการถูกขโมยหรือใช้ในทางมิชอบ ส่งเสริมจริยธรรมทางไซเบอร์และหลีกเลี่ยงปัญหาทางกฎหมาย การสร้างความเข้าใจในเรื่องนี้ช่วยเสริมสร้างสังคมดิจิทัลที่ปลอดภัยและมีจริยธรรม

วัตถุประสงค์

- เพื่อสร้างความตระหนักรู้เกี่ยวกับผลกระทบของการขโมยรหัสไวไฟ
- เพื่อส่งเสริมการป้องกันและรักษาความปลอดภัยของเครือข่ายไวไฟ
- เพื่อให้ความรู้เกี่ยวกับกฎหมายและจริยธรรมในการใช้งานอินเทอร์เน็ต
- เพื่อกระตุ้นให้ผู้ใช้งานอินเทอร์เน็ตปฏิบัติตนอย่างมีความรับผิดชอบ

ขอบเขตการทำงาน

โครงงานนี้มุ่งเน้นการศึกษาช่องโหว่ของเครือข่าย WiFi และการทดสอบการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อวิเคราะห์และประเมินความแข็งแกร่งของมาตรการรักษาความปลอดภัยบนมาตรฐานการเข้ารหัสต่างๆ โดยดำเนินการภายใต้ขอบเขตที่ได้รับอนุญาตและมีจริยธรรม เพื่อเสนอแนวทางในการเสริมสร้างความปลอดภัยของเครือข่ายไร้สายให้มีประสิทธิภาพมากขึ้น

สรุปผลการดำเนินงาน

จากการทดสอบความปลอดภัยของเครือข่าย WiFi ในรูปแบบต่างๆ พบว่าเครือข่ายที่ใช้การเข้ารหัสแบบ WEP มีความเสี่ยงสูงต่อการถูกเจาะระบบ ในขณะที่ WPA2 และ WPA3 มีความปลอดภัยมากขึ้น แต่ยังคงมีช่องโหว่ที่อาจถูกโจมตีผ่านวิธีการทางวิศวกรรมสังคม (Social Engineering) หรือการโจมตีแบบ Evil Twin Attack ได้

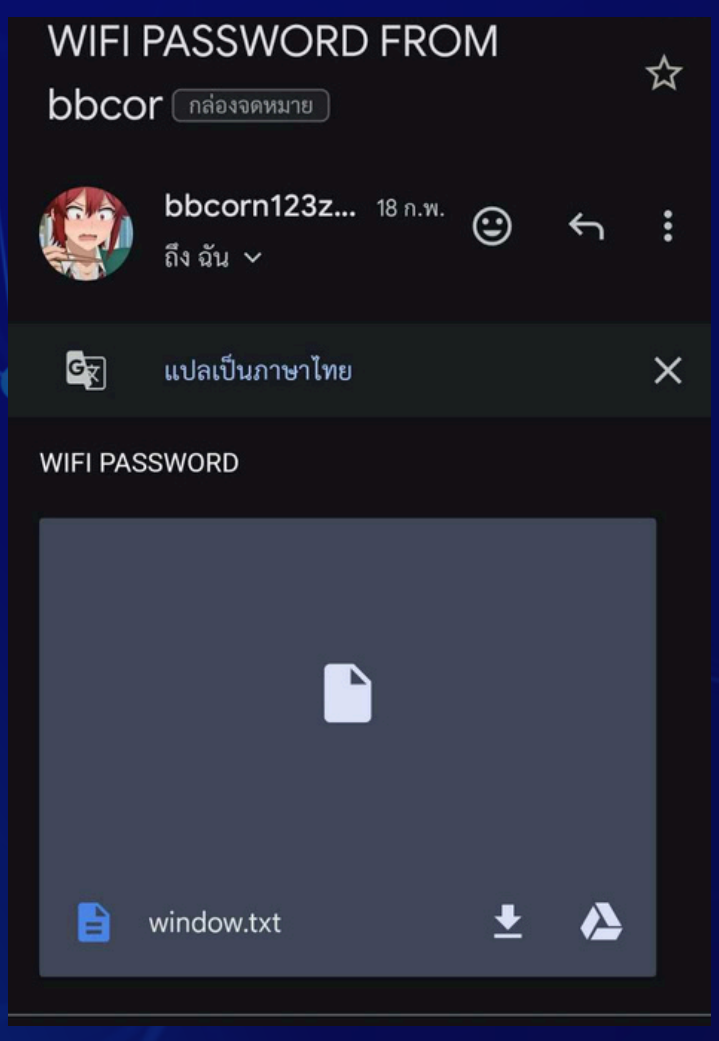
การทดลองนี้ชี้ให้เห็นถึงความสำคัญของการใช้มาตรการป้องกัน

วิธีการใช้งาน

1. เปิดApplication
2. เชื่อมwifi
3. รับe-mail

เครื่องมือที่ใช้

ผลลัพธ์



สมาชิก กลุ่มที่ 11

1.นางสาวกรองกาญจน์ ตรีเมฆ 663380142-3
2.นางสาวปริยากร พละดร 663380170-8
3.นายอโนชา เชยทอง 663380193-6
4.นายทวีพงศ์ เหลืองปฐมชัย 663380486-1
5.นายอรรถนนท์ บุญน้อย 663380500-3