การประเมินความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์โดยการจำลองการกระจายสัญญาณไวไฟสาธารณะ

นายนันทภพ เครือครุ่ย

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

การประเมินความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์โดยการจำลองการกระจายสัญญาณไวไฟสาธารณะ

นายนันทภพ เครือครุ่ย

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

ใบรับรองโครงร่างการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การประเมินความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์โดยการจำลองการกระจายสัญญาณไวไฟสาธารณะ

โดย นายนันทภพ เครือครุ่ย

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณบดีบัณฑิตวิทยาลัย / หัวหน้าภาควิชา

คณะกรรมการสอบการค้นคว้าอิสระ

---------- ประธานกรรมการ

(สุมิตรา นวลมีศรี)

---------- อาจารย์ที่ปรึกษา

(สุนันฑา สดสี)

---------- กรรมการ

(นวพร วิสิฐพงศ์พันธ์)

---------- กรรมการ

(สุนันฑา สดสี)

ชื่อ	: นายนันทภพ เครือครุ่ย
ชื่อการค้นคว้าอิสระ	: การประเมินความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์โดยการจำลองการกระจายสัญญาณไวไฟสาธารณะ
สาขาวิชา	: การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก	: สุนันฑา สดสี
ปีการศึกษา	: 2567

บทคัดย่อ

งานวิจัยนี้มุ่งเน้นไปที่การประเมินความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์โดยจำลองจุดเชื่อมต่อไวไฟสาธารณะที่ตั้งอยู่ในองค์กรด้านการดูแลสุขภาพ งานวิจัยเริ่มต้นด้วยการสำรวจเกี่ยวกับช่องทางปัจจุบันสำหรับการแบ่งปันข้อมูล หรือการรักษาที่ได้รับการสนับสนุนในหมู่บุคลากรทางการแพทย์ ผลสำรวจแสดงให้เห็นว่า แอปพลิเคชันไลน์ ถูกใช้งานบ่อยครั้งสำหรับพวกเขา ต่อมา ตำแหน่งของจุดเชื่อมต่อไวไฟจำลองถูกกำหนด การเฝ้าระวังการใช้งานจุดเชื่อมต่อไวไฟแสดงให้เห็นว่าร้อยละ 82.98 ของผู้เชื่อมต่อมีความเสี่ยง ดังนั้นความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์จึงมีความจำเป็นสำหรับพวกเขา ในงานนี้ ได้มีการดำเนินการฝึกอบรมด้านความมั่งคงปลอดภัยทางไซเบอร์ การจำลองการใช้งานจุดเชื่อมต่อไวไฟครั้งที่สองได้รับการทดสอบ ผลลัพธ์แสดงให้เห็นว่าร้อยละ 8.51 ของบุคลากร เป็นผู้เชื่อมต่อที่มีความเสี่ยง สรุปได้ว่าจำนวนบุคลากรที่ตกอยู่ในความเสี่ยงลดลง แสดงว่าบุคลากรด้านการดูแลสุขภาพจำนวนมากมีความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์แล้ว

(มีจำนวนทั้งสิ้น 66 หน้า)

คำสำคัญ : ความมั่นคงปลอดภัยทางไซเบอร์ ความตระหนักรู้ ภัยคุกคามทางไซเบอร์

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Nanthaphop Kruakrui
Independent Study Title : A Cyber Threat Awareness Assessment by Simulating Public Wi-Fi Hotspots
Major Field : Network and Information Security Management
King Mongkut's University of Technology North Bangkok
Independent Study Advisor : Sunantha Sodsee
Academic Year : 2024

ABSTRACT

This study focused on the cyber threat awareness assessment by simulating the public Wi-Fi hotspots located in the healthcare organizations. The study starts the survey about the current channels for sharing the supported information of treatment among the healthcare staffs. The survey shows that Line community Application is frequently used for them. Next, the positions of the simulated Wi-Fi hotspots are determined. The usage monitoring of Wi-Fi hotspots are shown that 82.98% of users is at risk, then the cyber threat awareness is necessary for them. In this work, the cybersecurity training is conducted. The second simulation of the Wi-Fi hotspots usage is tested, the result shows that only 8.51% of users are at risk. It concludes that the number of risked staffs is decreased, then many healthcare staffs have got the cyber threat awareness.

(Total 66 Pages)

Keywords: Cybersecurity, Awareness, Cyber threat

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงไปได้ด้วยความกรุณา และการสนับสนุนอย่างดียิ่ง จาก ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี อาจารย์ที่ปรึกษาหลักการค้นคว้าอิสระ ที่ได้มอบคำแนะนำพร้อมทั้งเสนอแนะแนวทางการดำเนินงานวิจัยในทุกขั้นตอน ด้วยความเอาใจใส่และเสียสละเวลาเป็นอย่างยิ่ง ผู้วิจัยขอกราบขอบพระคุณอย่างสูงไว้ ณ โอกาสนี้

ขอขอบคุณคณะกรรมการสอบการค้นคว้าอิสระทุกท่าน ที่ได้กรุณาให้คำแนะนำ และข้อคิดเห็นที่เป็นประโยชน์อย่างยิ่ง อันเป็นปัจจัยสำคัญที่ช่วยให้การค้นคว้าอิสระฉบับนี้สมบูรณ์

นอกจากนี้ผู้วิจัยขอขอบคุณ นพ.สมคิด อุดมกิจมงคล ผู้อำนวยการโรงพยาบาล ที่ได้ให้การสนับสนุนด้านทรัพยากรบุคคล และสถานที่สำหรับการดำเนินการค้นคว้าอิสระทำให้สามารถดำเนินการศึกษาจนสำเร็จลุล่วง

ขอขอบคุณผู้จัดการแผนก และเพื่อนร่วมงานทุกท่านที่ได้มอบคำแนะนำในด้านต่างๆ ที่เกี่ยวข้องกับการค้นคว้าอิสระ โดยเฉพาะอย่างยิ่ง นายอรรถวิท เรืองรัตนกุล และนายศิวณัฐ แลวงศ์นิล ที่ได้ให้คำปรึกษาด้านอุปกรณ์ และข้อมูลสนับสนุนรวมถึงช่วยเหลือการดำเนินงานการค้นคว้าอิสระในภาคสนามจนเสร็จสมบูรณ์

ขอขอบคุณ นางสาวพิมพิศา ใจหล้า ได้รับการแต่งตั้งจากทางมหาวิทยาลัย เป็นผู้เชี่ยวชาญร่วมให้ความรู้อบรมเสริมสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ ตลอดจนการให้คำปรึกษา และข้อเสนอแนะต่างๆ

ท้ายที่สุด ผู้วิจัยขอกราบขอบพระคุณ บิดา มารดา ครอบครัว และทุกท่านที่อยู่เบื้องหลังความสำเร็จในครั้งนี้ ที่ได้มอบกำลังใจ และการสนับสนุนในทุกด้านมาโดยตลอด จนทำให้การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงด้วยดี

นันทภพ เครือครุ่ย

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ข
บทคัดย่อภาษาอังกฤษ	ค
กิตติกรรมประกาศ	ง
สารบัญตาราง	ซ
สารบัญภาพ	ฌ
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการวิจัย	3
1.3 ขอบเขตของงานวิจัย	3
1.4 ประโยชน์ที่จะได้รับ	4
1.5 ขั้นตอนในการดำเนินงาน	4
1.6 อุปกรณ์ที่ใช้ในการทำงานวิจัย	5
บทที่ 2 เอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้อง	7
2.1 ความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ Cybersecurity Awareness)	7
2.2 อีวิล ทวิน (Evil Twin Attack)	7
2.3 การเขียนคำสั่งการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) ด้วยภาษา Python บน Visual Studio Code	8
2.4 วิธีตั้งค่า Hotspot บน MikroTik hAP ax²	13
2.5 MikroTik แก้ไขหน้า HotSpot Login	19
2.6 การแก้ไขหน้า Log in Hotspot MikroTik ด้วยภาษา CSS และ JavaScript	25

สารบัญ (ต่อ)

หน้า

2.7 การสร้าง User Account หลายคนพร้อมกันใน MikroTik 29

2.8 การสร้าง app passwords สำหรับ Account ที่ใช้ Google 2FA สำหรับตั้งค่าส่ง Logging Hotspot Report MikroTik 36

2.9 การตั้งค่า Sent Logging to Email Hotspot Report MikroTik 39

2.10 สรุป 42

บทที่ 3 วิธีดำเนินงานวิจัย 43

3.1 ขั้นตอนวิธีการดำเนินงานวิจัย 43

3.2 จัดทำแบบสอบถามการส่งต่อข้อมูลประกอบการรักษาคนไข้ผ่าน Community Application 44

3.3 Monitor การใช้งาน Wi-Fi 52

3.4 ดำเนินการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) 52

3.5 จำลองการโจมตีอีวิล ทวิน ครั้งที่ 1 53

3.6 ดำเนินการส่งเสริมความตระหนักรู้ให้เท่าทันภัยคุกคามทางด้านไซเบอร์ 54

3.7 จำลองการโจมตีอีวิล ทวิน ครั้งที่ 2 56

บทที่ 4 ผลการวิจัย 57

4.1 ผลลัพธ์หลังจากทดสอบครั้งที่ 1 57

4.2 ผลลัพธ์จากการสอบวัดผลหลังการอบรมเสริมสร้างความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ 58

4.3 ผลการตอบแบบสอบถามประเมินความตระหนักรู้หลังการจากอบรม 59

4.4 ผลลัพธ์หลังจากทดสอบครั้งที่ 2 59

บทที่ 5 สรุปผลการวิจัย และข้อเสนอแนะ 61

5.1 สรุปผลการวิจัย 61

สารบัญ (ต่อ)

	หน้า
5.2 ข้อจำกัด	62
บรรณานุกรม	63
ประวัติผู้วิจัย	66

สารบัญตาราง

ตารางที่		หน้า
3-1	จำนวนผู้ตอบแบบสอบถาม	49
3-2	จำนวนการใช้งาน Community Application	50
3-3	การใช้งาน Community Application ส่งต่อข้อมูลประเภทใด	51
3-4	จำนวนความถี่ในการส่งต่อข้อมูลจากการใช้งาน Community Application	51
3-5	จำนวนผู้เชื่อมต่อเข้าใช้งาน Wi-Fi ระยะเวลา 4 สัปดาห์	52
3-6	จำนวนผู้ตอบแบบสอบถามจากการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) 50 คน	53

สารบัญรูปภาพ

ภาพที่		หน้า
2-1	นำเข้าไลบรารี pandas และ numpy นำเข้าโดยใช้คำสั่ง import	8
2-2	การกำหนดเส้นทางไฟล์	8
2-3	การอ่านข้อมูลจากไฟล์ CSV	9
2-4	การสุ่มตัวอย่างข้อมูล	9
2-5	การแสดงผลลัพธ์	9
2-6	ผลลัพธ์ที่ได้จากการ Run Code	10
2-7	นำผลลัพธ์ที่ได้ไปวางบน Excel เพื่อเตรียมข้อมูลสำหรับ Mapping	10
2-8	ตั้งค่าเพิ่มเติมจากข้อ 2.3.7	11
2-9	นำลำดับของข้อมูลที่ได้มา Mapping กับข้อมูลการตอบแบบสอบทั้งหมด	12
2-10	นำลำดับของข้อมูลที่ได้มา Mapping กับข้อมูลการตอบแบบสอบทั้งหมด	12
2-11	ตั้งค่าเมนู IP -> Addresses กดปุ่ม Add แล้วทำการตั้งค่า	13
2-12	ตั้งค่าเมนู IP -> Hotspot หัวข้อ Servers แล้วทำการตั้งค่า	14
2-13	ตั้งค่าเพิ่มเติมจากข้อ 2.4.2	14
2-14	ตั้งค่าเพิ่มเติมจากข้อ 2.4.3	15
2-15	ตั้งค่าเพิ่มเติมจากข้อ 2.4.4	15
2-16	ตั้งค่าเพิ่มเติมจากข้อ 2.4.5	16
2-17	ตั้งค่าเพิ่มเติมจากข้อ 2.4.6	16
2-18	ตั้งค่า User Profiles สำหรับกำหนดการใช้งานของ User	17
2-19	ตั้งค่าเพิ่มเติมจากข้อ 2.4.7	18
2-20	หน้า Login กรณีไม่ได้ใส่ SSL Certificate	18
2-21	ขั้นตอน - แก้ไขหน้าจอ Login ของ Hotspot	19

สารบัญรูปภาพ (ต่อ)

ภาพที่	หน้า
2-22 ดับเบิ้ลคลิกที่โฟล์เดอร์ hotspot เพื่อคลิกทำการ Backup	20
2-23 คลิกขวาที่โฟล์เดอร์ hotspot จากนั้น Download	20
2-24 คลิกขวาที่โฟล์เดอร์ hotspot จากนั้น Download	21
2-25 โฟล์เดอร์ hotspot ทั้งหมดในตัว MikroTik เพื่อทำการแก้ไขตามความต้องการ	21
2-26 ทำการคัดลอกรูปโลโก้ หรือไฟล์ที่ต้องการใส่ในโฟลเดอร์ /hotspot/img	22
2-27 ทำการแก้ไขไฟล์ login.html โดยผ่านโปรแกรม Visual Studio Code	22
2-28 หลังจากทำการแก้ไข login.html เสร็จเรียบร้อย	23
2-29 ทดสอบเชื่อมต่อ Wi-Fi เข้าหน้า Login Hotspot	24
2-30 ทดสอบเชื่อมต่อ Wi-Fi เข้าหน้า Login Hotspot	24
2-31 Code ก่อนการแก้ไข การเชื่อมโยงสไตล์ และภาพพื้นหลัง	25
2-32 Code หลังการแก้ไข การเชื่อมโยงสไตล์ และภาพพื้นหลัง	25
2-33 การตั้งค่า Redirect ไปยัง Website ที่ต้องการ	25
2-34 Code เดิมก่อนการแก้ไขแทรกรูป Logo	26
2-35 Code หลังจากการแก้ไขแทรกรูป Logo	26
2-36 การแทรกคำสั่ง และการจัดรูปแบบ CSS	27
2-37 Event Listener สำหรับ Checkbox	27
2-38 Event Listener สำหรับปุ่ม Submit	28
2-39 Event Listener สำหรับปุ่ม Close ของ Popup	28
2-40 การปิด Popup เมื่อคลิกนอกพื้นที่ Popup	28
2-41 การเพิ่มปุ่ม และฟอร์มเงื่อนไข	29
2-42 เข้า MikroTik ผ่านโปรแกรม Winbox	30

สารบัญรูปภาพ (ต่อ)

ภาพที่	หน้า
2-43 เมนู New Terminal พิมพ์คำสั่ง	30
2-44 ไฟล์ที่ชื่อ user. rsc ในเมนู File	31
2-45 ไฟล์ user.rsc ด้วยโปรแกรมประเภท Text Editor	31
2-46 ลบคำสั่งที่อยู่หลังจากบรรทัด /ip hotspot user	32
2-47 คัดลอกข้อมูลที่เป็น User ID ที่เราได้สร้างไว้	32
2-48 นำข้อมูลของ User จะสร้างใหม่ลงไป	33
2-49 คัดลอกข้อมูลทั้งหมดแล้วนำไปวางในไฟล์ user.rsc	33
2-50 ทำการลากไฟล์ user.rsc มาใส่ในหน้าต่างนี้	34
2-51 พิมพ์คำสั่ง /import user.rsc	35
2-52 หน้าต่าง Hotspot	35
2-53 การตั้งค่าความปลอดภัยสำหรับสร้าง app passwords	36
2-54 รหัสผ่านสำหรับแอป	37
2-55 ยืนยันตัวตน โดยการกรอก Password	37
2-56 ตั้งชื่อแอป	38
2-57 ระบบจะสร้างรหัสผ่านแสดงผ่าน	38
2-58 การตั้งค่า E-mail ไปที่ Tools เลือก E-mail	39
2-59 กรอกข้อมูล Server และ E-mail	39
2-60 การตั้งค่าเพื่อส่ง Logging	40
2-61 การตั้งค่าสร้าง Log Action	40
2-62 กรอกรายละเอียดการตั้งค่า	41
2-63 การตั้งค่าเพื่อกำหนด Logging Rules	41

สารบัญรูปภาพ (ต่อ)

ภาพที่		หน้า
2-64	สร้าง Log Rule	42
2-65	Log เมื่อส่งเข้า E-mail	42
3-1	ขั้นตอนกระบวนการดำเนินงาน (Process Diagram) ส่วนที่ 1	43
3-2	ขั้นตอนกระบวนการดำเนินงาน (Process Diagram) ส่วนที่ 2	44
3-3	รายละเอียดของแบบสอบถามแต่ละส่วน	45
3-4	Department / แผนก	46
3-5	Work Experience / ประสบการณ์การทำงาน	46
3-6	ประเมินการใช้งาน Community Application	47
3-7	ประเมินการส่งต่อข้อมูลโดยผ่านการใช้งาน Community Application	48
3-8	การจัดอบรมให้ความรู้ต่อภัยคุกคามทางไซเบอร์	54
3-9	แบบทดสอบส่งเสริมความตระหนักรู้	55
3-10	เรียนออนไลน์ย้อนหลัง	55
4-1	ผลลัพธ์การวิเคราะห์ครั้งที่ 1 ของ Nurse OPD	57
4-2	ผลลัพธ์การวิเคราะห์ครั้งที่ 1 ของ Nurse IPD	58
4-3	ผลลัพธ์การวิเคราะห์ครั้งที่ 2 ของ Nurse OPD	59

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันการใช้งานเทคโนโลยี (Technology) ร่วมกับการทำงาน และการใช้ชีวิตประจำวันเพิ่มขึ้น หลีกเลี่ยงไม่ได้หากต้องนำเทคโนโลยีเข้ามามีบทบาทในการทำงาน การใช้งานอินเทอร์เน็ต (Internet) ก็เป็นส่วนหนึ่งของการใช้งานเทคโนโลยีในปัจจุบัน เนื่องจากมีการใช้งานอินเทอร์เน็ตอย่างแพร่หลาย และใช้ร่วมกับการทำงานนั้น ในองค์กรสายสุขภาพ อาทิ โรงพยาบาล คลินิก สาธารณสุข ยังคงต้องใช้งานเทคโนโลยีเหล่านี้ ร่วมกับเทคโนโลยีด้านอื่นๆ ปัญหาด้านความมั่นคงปลอดภัยเกี่ยวกับการใช้งานอินเทอร์เน็ต หรือที่เราเรียกกันอย่างแพร่หลาย คือ ความมั่นคงปลอดภัยทางไซเบอร์ ทั้งนี้ World Economic Forum (WEF) เป็นที่รู้จักในเวทีโลกในเรื่องการดำเนินกิจกรรมเพื่อเสนอแนะทิศทางในการกำหนดนโยบายด้านเศรษฐกิจ สังคม และการพัฒนาในระดับระหว่างประเทศ ผ่านเครือข่ายผู้นำภาคการเมือง ธุรกิจ และภาคประชาสังคม ได้เขียนบนความ Healthcare Cyber Attacks are on the rise: Here's why zero trust will prevent care disruptions เมื่อวันที่ 5 พฤษภาคม 2023 บทความกล่าวถึงการวิจัยจาก Check Point Software Technologies ยืนยันแนวโน้มนี้ โดยเผยให้เห็นว่าภาคส่วนการดูแลสุขภาพประสบกับการโจมตีโดยเฉลี่ย 1,684 ครั้งต่อสัปดาห์ในไตรมาสที่ 1 ปี 2566 ซึ่งเพิ่มขึ้น 22% เมื่อเทียบเป็นรายปี นั่นทำให้การดูแลสุขภาพกลายเป็นอุตสาหกรรมที่เป็นเป้าหมายมากเป็นอันดับสามในปี 2566 แซงหน้าการเงิน การประกันภัย และการสื่อสาร [1]

จากที่กล่าวมา หนึ่งในภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ที่น่าสนใจ และมีแนวโน้มที่จะถูกใช้ในการโจมตีทางไซเบอร์ ก็คือ อีวิล ทวิน (Evil Twin) ซึ่งเป็นวิธีการโจมตีของผู้ไม่ประสงค์ดี โดยทำการติดตั้งจุดเข้าใช้งานไวไฟปลอม เมื่อผู้ใช้เชื่อมต่อเข้าใช้งานข้อมูลทั้งหมดจะถูกแชร์กับเครือข่ายผ่านเซิร์ฟเวอร์ ที่ควบคุมโดยผู้ไม่ประสงค์ดี และผู้ใช้จะถูกขโมยข้อมูลจากการเชื่อมต่อไวไฟปลอมนั้น ทั้งนี้ เดลินิวส์ ออนไลน์ ได้มีบทความกล่างถึงความเสี่ยงของการใช้ไวไฟสาธารณะ (Public Wi-Fi) และแนวทางเสริมความปลอดภัย แน่นอนว่าขึ้นชื่อว่าเป็นสาธารณะ หมายความว่าใครก็มีสิทธิ์ที่จะแอบเข้ามาดูการใช้งานของเราได้ ไม่เหมือนอินเทอร์เน็ตส่วนตัว เราจะไม่มีทางรู้เลยว่าเราเป็นเป้าหมายของผู้ไม่ประสงค์ดี หรือไม่ การกรอกข้อมูลส่วนตัว เช่น ชื่อ นามสกุล เลขบัตรประจำตัวประชาชน เพื่อขอเข้าใช้งานอินเทอร์เน็ตนั้นก็มีความเสี่ยงที่ข้อมูลจะถูกดึง และเก็บไว้กับผู้ไม่ประสงค์ดีได้ด้วยเช่นเดียวกัน

โดยในกรณีของการทำธุรกรรมออนไลน์นั้นอาจทำให้คุณหมดตัว หรือโดนสวมรอยกลายเป็นอาชญากรโดยไม่รู้ตัว ดังนั้นเราไม่ควรคิดว่าที่สาธารณะนั้นเป็นที่ปลอดภัยเสมอ ยกตัวอย่างจากอาชญากรระดับโลก Ross Ulbricht เจ้าของ Silk road Dark web นั่งในห้องสมุดสาธารณะตอนถูกจับกุม โดยพวกเราแทบไม่มีทางดูออกได้เลย นอกเหนือจากที่ได้กล่าวมาข้างต้น บางครั้งผู้ไม่ประสงค์ดีอาจใช้วิธีแชร์ Hotspot ของตน และเปลี่ยนชื่อให้น่าเชื่อถือเพื่อหลอกล่อให้คนเข้ามาใช้งาน แอบสอดแทรกมัลแวร์ (Malware) หรือ แรนซัมแวร์ (Ransomware) เข้ามาก็เป็นได้ [2]

จากที่กล่าวมาข้างต้นจะเห็นได้ว่า ภัยทางไซเบอร์ยังคงถือเป็นปัญหาใหม่ และส่งผลกระทบอย่างมาก โดยเฉพาะอย่างยิ่งภัยจากการโจมตีด้วยอีวิล ทวิน (Evil Twin) ซึ่งสามารถสร้างความเสียหายในองค์กรทุกองค์กรไม่เพียงแต่องค์กรสายสุขภาพได้โดยตรงผู้วิจัยจึงได้ทำการศึกษาเกี่ยวกับความตระหนักรู้เท่าทันภัยทางไซเบอร์ (Cybersecurity Awareness) ของบุคลากรในองค์กรสายสุขภาพแห่งหนึ่ง โดยมีขั้นตอน คือ 1) ทางผู้วิจัยจัดทำแบบสอบถามเพื่อประเมินการใช้งาน แอปพลิเคชันชุมชน (Community Application) ในการส่งต่อข้อมูลประกอบการรักษาคนไข้ให้ทางบุคลากรในองค์กรสายสุขภาพให้ข้อมูลผ่านการตอบแบบสอบถาม โดย Community Application ที่ทางผู้วิจัยนำมาใช้ในแบบสอบถามนี้ ประกอบด้วย Line, Messenger, Google Chat, WeChat และ WhatsApp 2) หลังจากได้ข้อมูลจำนวนผู้ตอบแบบสอบถามแล้วทางผู้วิจัยได้ทำการ Monitor การใช้งาน Wi-Fi ภายในองค์กรสายสุขภาพที่ทางผู้วิจัยจะใช้การโจมตีด้วย อีวิล ทวิน เป็นระยะเวลา 4 สัปดาห์ เมื่อได้ข้อมูลแล้วทางผู้วิจัยจะนำมาหาค่าเฉลี่ยคำนวณเพื่อใช้ประกอบการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) จากจำนวนผู้ตอบแบบสอบถาม คิดเป็นร้อยละ 30 ของผู้ตอบแบบสอบถามทั้งหมด 3) ทางผู้วิจัยจำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน ครั้งที่ 1 เพื่อรวบรวมข้อมูลการเชื่อมต่อเข้าใช้งาน Wi-Fi บันทึกข้อมูลการเชื่อมต่อเข้าใช้งาน และความตระหนักรู้ของพนักงานในองค์กรสายสุขภาพ 4) จัดกิจกรรม กระบวนการส่งเสริมความตระหนักรู้ให้บุคลากรเหล่านั้นเพื่อให้รู้เท่าทันภัย ทางไซเบอร์ โดยมีสมมติฐานว่ากระบวนการถ่ายทอดความรู้ที่ดำเนินการไปสามารถให้ผลลัพธ์ที่ดี และสามารถนำไปประยุกต์ใช้ในการยกระดับความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์รูปแบบต่างๆ ในองค์กรอื่นๆ ได้ 5) หลังจากที่ผู้วิจัยส่งเสริมความตระหนักรู้แล้ว ทางผู้วิจัยจะทำการจำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน ครั้งที่ 2 เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน เพื่อรวมรวบข้อมูลการเชื่อมต่อเข้าใช้งาน Wi-Fi บันทึกข้อมูลการเชื่อมต่อเข้าใช้งาน และความตระหนักรู้ของพนักงานในองค์กรสายสุขภาพอีกครั้ง โดยคาดหวังว่าบุคลากรภายในองค์กรสายสุขภาพต้องไม่ตกเป็นเหยื่อการถูกโจมตีจากภัยทางไซเบอร์ หรือลดน้อยลงจากครั้งแรก

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อนำผลการทดสอบ โดยการใช้เทคนิคการจำลองจุดกระจายสัญญาณไวไฟสาธารณะไปใช้ในการประเมินความตระหนักรู้ ทางด้านภัยคุกคามด้านไซเบอร์ ของผู้ใช้อินเทอร์เน็ตภายในองค์กรสายสุขภาพ

1.2.2 เพื่อส่งเสริมความตระหนักรู้ด้านภัยคุกคามทางด้านไซเบอร์ โดยผ่านกิจกรรม และกระบวนการส่งเสริมความตระหนักรู้ให้กับผู้ใช้อินเทอร์เน็ตภายในองค์กรสายสุขภาพ

1.2.3 เพื่อประเมินผลลัพธ์หลังจากผ่านกิจกรรมอบรม ประเมิน และวัดผลให้บุคลากรภายในองค์กรสายสุขภาพสามารถตระหนักรู้ และถือเป็นการป้องกันก่อนเกิดเหตุการณ์การโจมตีทางไซเบอร์ของผู้ไม่ประสงค์ดี

1.3 ขอบเขตของงานวิจัย

1.3.1 ศึกษาค้นคว้าเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ โดยใช้เทคนิคการจำลองจุดกระจายสัญญาณไวไฟสาธารณะ ของผู้ใช้อินเทอร์เน็ตภายในองค์กรสายสุขภาพ

1.3.2 ส่งเสริมความตระหนักรู้ เกี่ยวกับภัยคุกคามทางไซเบอร์ ผ่านกิจกรรม และกระบวนการส่งเสริมความตระหนักรู้ให้กับผู้ใช้อินเทอร์เน็ตในองค์กรสายสุขภาพที่เข้าข่ายเป็นเหยื่ออีวิล ทวิน

1.3.3 เก็บข้อมูลโดยใช้ผลการทดสอบ โดยใช้เทคนิคการการจำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน ของผู้ใช้อินเทอร์เน็ตภายในโรงพยาบาลแห่งหนึ่ง

1.3.4 ประชากร และพื้นที่ในการวิจัยครั้งนี้ คือ บุคลากรผู้ใช้งานอินเทอร์เน็ตภายในโรงพยาบาลแห่งหนึ่ง จำนวน 2 กลุ่ม ประกอบด้วย กลุ่มที่ 1 และกลุ่มที่ 2 รวมทั้งสิ้น 47 คน (โดยจำนวนนับจากผู้ตอบแบบสอบถาม) ซึ่งในปัจจุบันองค์กร ยังไม่เคยพบปัญหาด้านการโจมตีของอีวิล ทวิน ถึงแม้ยังไม่มีการถูกโจมตี แต่เนื่องจากบุคลากรผู้ที่ใช้งานอินเทอร์เน็ตภายในองค์กร ส่วนใหญ่ยังขาดความตระหนักรู้ทางด้านไซเบอร์ อาจเกิดปัญหาจากการถูกโจมตีได้ จึงควรสร้างความตระหนักรู้เพื่อป้องกันก่อนเกิดเหตุการณ์

1.3.5 เครื่องมือที่ใช้สำหรับใช้ในการทดสอบคือ TP-link Router 4G LTE, MikroTik Router hAP ax², Notebook, Sim Card Internet

1.3.6 กิจกรรม และกระบวนการส่งเสริมความตระหนักรู้ให้กับผู้ใช้อินเทอร์เน็ตภายในองค์กรสายสุขภาพ มีดังนี้

1.3.6.1 การจัดอบรมร่วมกับผู้เชี่ยวชาญด้าน Cybersecurity ผู้มีความรู้ความเชี่ยวชาญทางด้านภัยคุกคามทางไซเบอร์ จำนวน 1 ครั้ง

1.3.6.2 เพิ่มช่องทางจากสื่อสาร เรื่องภัยคุกคามทางไซเบอร์ในองค์กร เช่น line Commutation, อีเมล์ขององค์กร เป็นต้น

1.3.7 ประเมินผลลัพท์ที่ได้จากการทำกิจกรรม และกระบวนการถ่ายทอดความรู้ให้กับผู้ใช้อินเทอร์เน็ตในองค์กรสายสุขภาพ หลังจากใช้เทคนิคการจำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน เพื่อเสริมสร้างตระหนักรู้ของผู้ใช้อินเทอร์เน็ตในองค์กรสายสุขภาพ ทดสอบการจำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน ซ้ำอีกครั้ง และนำมาสรุปผลการวิจัย

1.3.8 การออกแบบการทดสอบอีวิล ทวิน และกิจกรรมกระบวนการส่งเสริมความตระหนักรู้ให้กับบุคลากรผู้ใช้อินเทอร์เน็ตภายในองค์กรสายสุขภาพ มีการตรวจสอบจากผู้เชี่ยวชาญด้านภัยคุกคามทางไซเบอร์ และทีมงานผู้เกี่ยวข้องในสายงาน เพื่อให้งานวิจัยได้ผลลัพธ์ที่ถูกต้องสมบูรณ์ และมีประสิทธิภาพในด้านการส่งเสริมความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์

1.4 ประโยชน์ที่จะได้รับ

1.4.1 ส่งเสริมความตระหนักรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ ให้กับพนักงานที่ใช้งานอินเทอร์เน็ตภายในองค์กรสายสุขภาพ

1.4.2 องค์กรสายสุขภาพ หรือบริษัทอื่นๆ สามารถนำงานวิจัยนี้ไปพัฒนาเกี่ยวกับการส่งเสริมความตระหนักรู้ด้านไซเบอร์ให้กับพนักงานที่ใช้งานอินเทอร์เน็ตภายในองค์กร สร้างแผน การป้องกันก่อนเกิดเหตุการณ์การโจมตีทางไซเบอร์ เพื่อเตรียมแผนการรับมือ และพนักงานภายในองค์กรสามารถตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ และรับมือก่อนเกิดเหตุได้

1.5 ขั้นตอนในการดำเนินงาน

1.5.1 จัดทำแบบสอบถามการใช้งาน Community Application ในการส่งต่อข้อมูลประกอบการรักษาคนไข้ และส่งให้บุคลากรในองค์กรสายสุขภาพตอบแบบสอบถาม

1.5.2 Monitor จำนวนผู้ใช้งาน Wi-Fi เป็นระยะเวลา 4 สัปดาห์ เพื่อหาค่าเฉลี่ยในการเลือกใช้วิธีการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) สำหรับการสุ่มจากจำนวนผู้ตอบแบบสอบถาม คิดเป็นร้อยละ 30 ของผู้ตอบแบบสอบถามทั้งหมด

1.5.3 สรุปข้อมูลจากจำนวนผู้ตอบแบบสอบถามเพื่อกำหนดแผนก เพื่อใช้สำหรับทำการทดสอบการโจมตีอีวิล ทวิน

1.5.3 ศึกษากระบวนการโจมตีทางไซเบอร์ของอีวิล ทวิน

1.5.4 ศึกษาเครื่องมือในการใช้โจมตีทางไซเบอร์ของอีวิลทวิน

1.5.5 ดำเนินการจัดเตรียมเครื่องมือ และสำรวจจุดติดตั้งสัญญาณไวไฟ

1.5.6 จำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน และรวบรวมข้อมูล ครั้งที่ 1

1.5.7 จัดกิจกรรมอบรมส่งเสริมสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ และสอบวัดประเมินผลลัพธ์หลังจากอบรมส่งเสริมสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

1.5.8 จำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน และรวบรวมข้อมูล ครั้งที่ 2

1.5.9 สรุปผลการรวบรวม และวิเคราะห์ข้อมูลจากการทดสอบจำลองจุดกระจายสัญญาณไวไฟ ครั้งที่ 1 และครั้งที่ 2

1.6 อุปกรณ์ที่ใช้ในการทำงานวิจัย

1.6.1 ฮาร์ดแวร์ (Hardware)

- TP-link Router 4G LTE
- MikroTik Router hAP ax²
- Sim Card Internet
- Notebook Dell G3
- Adapter Power
- สาย LAN

1.6.2 ซอฟต์แวร์ (Software)

- ระบบปฏิบัติการ Windows 11 64-bit
- MikroTik RouterOS, Level4
- TP-link Web Setting
- Visual Studio Code

- ภาษา HTML
- ภาษา CSS
- ภาษา JavaScript
- ภาษา Python
  - Library pandas
  - Library numpy
- winbox64
- Power BI Desktop
- Microsoft Excel 2016
- Notepad++

บทที่ 2

เอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

กระบวนการของการวิจัยในหัวข้อ การจำลองจุดกระจายสัญญาณไวไฟสาธารณะภายในองค์กร เพื่อนำไปใช้ในการประเมินความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ ของกลุ่มผู้ใช้งานอินเทอร์เน็ตภายในองค์กรสายสุขสภาพ ทางผู้วิจัยได้ศึกษาบทความ, เอกสาร, ทฤษฎี และงานวิจัยที่เกี่ยวข้องเพื่อเป็นแนวทางในการดำเนินการวิจัย ดังต่อไปนี้

2.1 ความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness)

Cybersecurity Awareness คือ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมุ่งเน้นให้บุคลากรในองค์กรเข้าใจถึงภัยคุกคามทางไซเบอร์ ความเสี่ยงที่อาจเกิดขึ้น และแนวทางปฏิบัติที่ดีที่สุดในการปกป้องข้อมูลทั้งในระดับบุคคล และองค์กร การตระหนักรู้ด้านความปลอดภัยนี้เปรียบเสมือนเกราะป้องกันที่ช่วยให้องค์กรสามารถป้องกันภัยคุกคามในปัจจุบันและอนาคตได้อย่างมีประสิทธิภาพ

Cybersecurity Awareness ไม่ได้หมายถึงเพียงการรู้จักเทคโนโลยีหรือกฎระเบียบด้านความปลอดภัยเท่านั้น แต่ยังรวมถึงการให้ทุกคนในองค์กรมีความเข้าใจเกี่ยวกับภัยคุกคาม และสามารถตอบสนองได้อย่างเหมาะสม โดยการสร้างความตระหนักรู้สามารถทำได้ผ่านการฝึกอบรม (Security Awareness Training) และการทดสอบความรู้ เพื่อให้มั่นใจว่าบุคลากรมีทักษะในการป้องกันและตอบสนองต่อภัยคุกคามไซเบอร์ได้อย่างถูกต้อง [3]

2.2 อีวิล ทวิน (Evil Twin Attack)

Evil Twin Attack เป็นรูปแบบของการโจมตีทางไซเบอร์ที่เกี่ยวข้องกับเครือข่าย Wi-Fi สาธารณะ โดยผู้โจมตีจะสร้างจุดเชื่อมต่อ Wi-Fi ปลอม (Evil Twin) ที่มีชื่อคล้ายหรือเหมือนกับจุดเชื่อมต่อที่ถูกต้อง เมื่อผู้ใช้ตั้งใจ หรือเผลอเชื่อมต่อกับเครือข่ายปลอมนี้ ข้อมูลทั้งหมดที่ส่งผ่านเครือข่ายจะถูกดักจับโดยผู้โจมตี ซึ่งอาจนำไปสู่การขโมยข้อมูลสำคัญ เช่น รหัสผ่าน ข้อมูลบัญชีธนาคาร หรือข้อมูลทางธุรกิจ การโจมตีนี้สามารถทำได้ง่ายด้วยอุปกรณ์ทั่วไป เช่น สมาร์ทโฟน (Smart Phone) หรือแล็ปท็อป (Laptop) ที่ติดตั้งซอฟต์แวร์ (Software) ที่เหมาะสม Evil Twin Attack มักเกิดขึ้นในพื้นที่ที่มีเครือข่าย Wi-Fi สาธารณะ เช่น ร้านกาแฟ สนามบิน หรือโรงแรม ซึ่งมักมีระบบความปลอดภัยต่ำ ทำให้ข้อมูลของผู้ใช้งานตกอยู่ในความเสี่ยง [4]

2.3 การเขียนคำสั่งการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) ด้วยภาษา Python บน Visual Studio Code

ใช้ภาษา Python ร่วมกับไลบรารี pandas และ numpy เพื่ออ่าน และประมวลผลข้อมูลจากไฟล์ CSV ที่ระบุใน file_path โดย pandas ออกแบบมาเพื่อให้จัดการและวิเคราะห์ข้อมูลได้ง่าย โดยเฉพาะข้อมูลในรูปแบบตาราง (คล้ายกับการทำงานกับสเปรดชีต เช่น Microsoft Excel หรือ Google Sheets) และ numpy เป็นไลบรารีพื้นฐานสำหรับการคำนวณทางคณิตศาสตร์ใน Python โดยเฉพาะการจัดการกับอาร์เรย์หลายมิติ และการคำนวณเชิงตัวเลขที่มีประสิทธิภาพสูง อธิบายขั้นตอนการทำงานของ Code ดังนี้

2.3.1 นำเข้าไลบรารี pandas และ numpy นำเข้าโดยใช้คำสั่ง import ดังภาพที่ 2-1

```
import pandas as pd
import numpy as np
```

ภาพที่ 2-1 นำเข้าไลบรารี pandas และ numpy นำเข้าโดยใช้คำสั่ง import

2.3.2 การกำหนดเส้นทางไฟล์ กำหนดเส้นทางไปยังไฟล์ .CSV ที่ต้องการอ่านโดยใช้ตัวแปร file_path = r”_” ตัวอักษร r ข้างหน้าสตริงบอก Python ว่านี่คือ "raw string" ซึ่งจะช่วยให้สตริงถูกตีความตรงตามตัวอักษร (โดยไม่สนใจอักขระพิเศษเช่น \n, \t) ดังภาพที่ 2-2

```
file_path = r"C:\Users\PrinH\Downloads\แบบสอบถามการส่งต่อข้อมูลประกอบการรักษาใน.csv"
```

ภาพที่ 2-2 การกำหนดเส้นทางไฟล์

2.3.3 การอ่านข้อมูลจากไฟล์ CSV ใช้ pandas ในการอ่านไฟล์ CSV และสร้าง DataFrame จากข้อมูล ดังภาพที่ 2-3

```
data = pd.read_csv(file_path)
```

ภาพที่ 2-3 การอ่านข้อมูลจากไฟล์ CSV

2.3.4 การสุ่มตัวอย่างข้อมูล ใช้ฟังก์ชัน .sample() ของ DataFrame เพื่อสุ่มตัวอย่างข้อมูล 50 ตัวอย่างจาก DataFrame data โดย n = จำนวนตัวอย่างที่ต้องการสุ่ม และ random_state=1 ทำให้การสุ่มมีความ สม่ำเสมอทุกครั้งในการ Run ดังภาพที่ 2-4

```
sample_data = data.sample(n=50, random_state=1)
```

ภาพที่ 2-4 การสุ่มตัวอย่างข้อมูล

2.3.5 การแสดงผลลัพธ์ ใช้ฟังก์ชัน print() เพื่อแสดงข้อมูลตัวอย่างที่สุ่มมา ดังภาพที่ 2-5

```
print(sample_data)
```

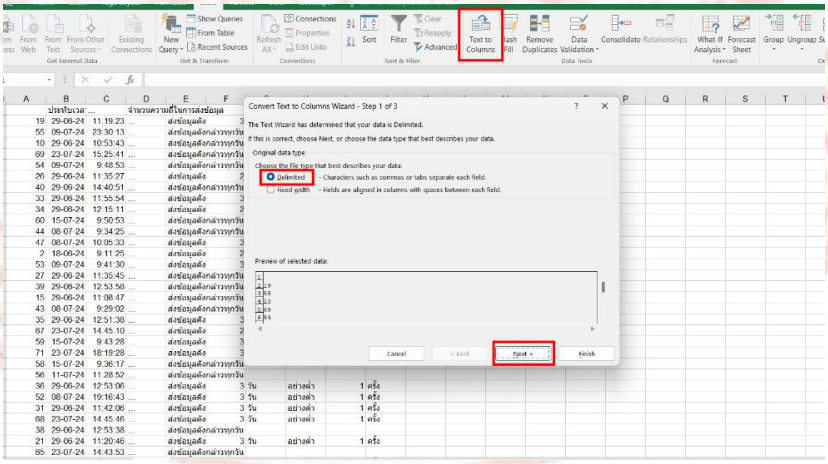
ภาพที่ 2-5 การแสดงผลลัพธ์

2.3.6 ผลลัพธ์ที่ได้จากการ Run Code ดังภาพที่ 2-6

	ประทับเวลา	...	จำนวนความถี่ในการส่งข้อมูล
19	29/6/2024, 11:19:23	...	ส่งข้อมูลดังกล่าวมากกว่า 3 วัน อย่างต่ำ 1 ครั้ง
55	9/7/2024, 23:30:13	...	ส่งข้อมูลดังกล่าวทุกวัน
10	29/6/2024, 10:53:43	...	ส่งข้อมูลดังกล่าวทุกวัน
69	23/7/2024, 15:25:41	...	ส่งข้อมูลดังกล่าวทุกวัน
54	9/7/2024, 9:48:53	...	ส่งข้อมูลดังกล่าวทุกวัน
26	29/6/2024, 11:35:27	...	ส่งข้อมูลดังกล่าว 2 วัน อย่างต่ำ 1 ครั้ง
40	29/6/2024, 14:40:51	...	ส่งข้อมูลดังกล่าวทุกวัน
33	29/6/2024, 11:55:54	...	ส่งข้อมูลดังกล่าวมากกว่า 3 วัน อย่างต่ำ 1 ครั้ง
34	29/6/2024, 12:15:11	...	ส่งข้อมูลดังกล่าว 2 วัน อย่างต่ำ 1 ครั้ง
60	15/7/2024, 9:50:53	...	ส่งข้อมูลดังกล่าวทุกวัน
44	8/7/2024, 9:34:25	...	ส่งข้อมูลดังกล่าวทุกวัน
47	8/7/2024, 10:05:33	...	ส่งข้อมูลดังกล่าวมากกว่า 3 วัน อย่างต่ำ 1 ครั้ง
2	18/6/2024, 9:11:25	...	ส่งข้อมูลดังกล่าว 2 วัน อย่างต่ำ 1 ครั้ง
53	9/7/2024, 9:41:30	...	ส่งข้อมูลดังกล่าวมากกว่า 3 วัน อย่างต่ำ 1 ครั้ง
27	29/6/2024, 11:35:45	...	ส่งข้อมูลดังกล่าวทุกวัน
39	29/6/2024, 12:53:58	...	ส่งข้อมูลดังกล่าวทุกวัน
15	29/6/2024, 11:08:47	...	ส่งข้อมูลดังกล่าวทุกวัน

ภาพที่ 2-6 ผลลัพธ์ที่ได้จากการ Run Code

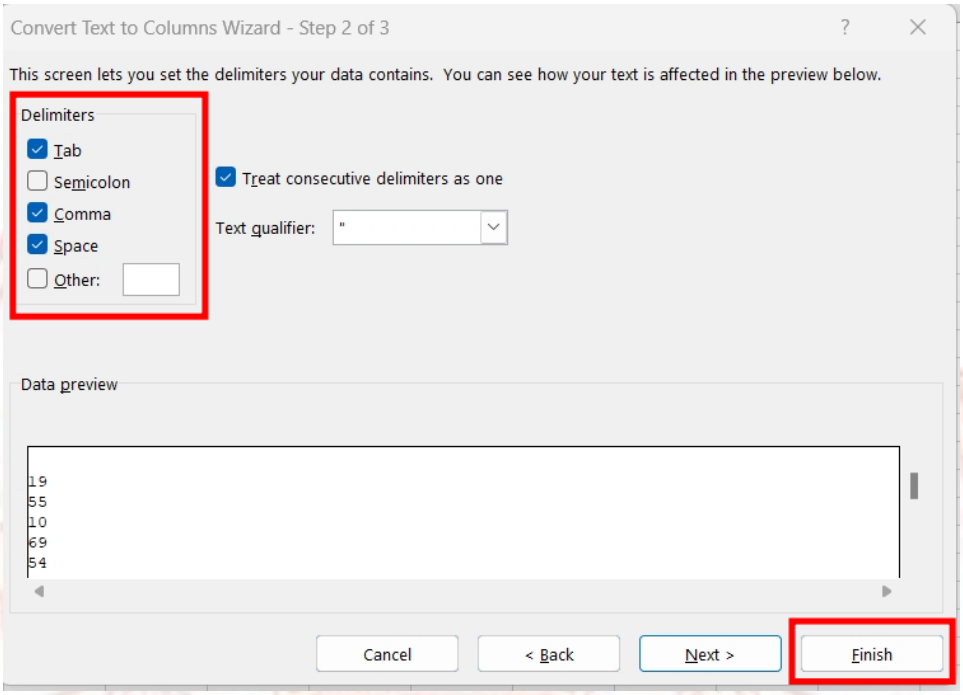
2.3.7 นำผลลัพธ์ที่ได้ไปวางบน Excel เพื่อเตรียมข้อมูลสำหรับ Mapping นำข้อมูลที่ได้จากการ Run Code มาวางบน Excel และ Textto Columns เลือก Delimited จากนั้นกด Next ดังภาพที่ 2-7



ภาพที่ 2-7 นำผลลัพธ์ที่ได้ไปวางบน Excel เพื่อเตรียมข้อมูลสำหรับ Mapping

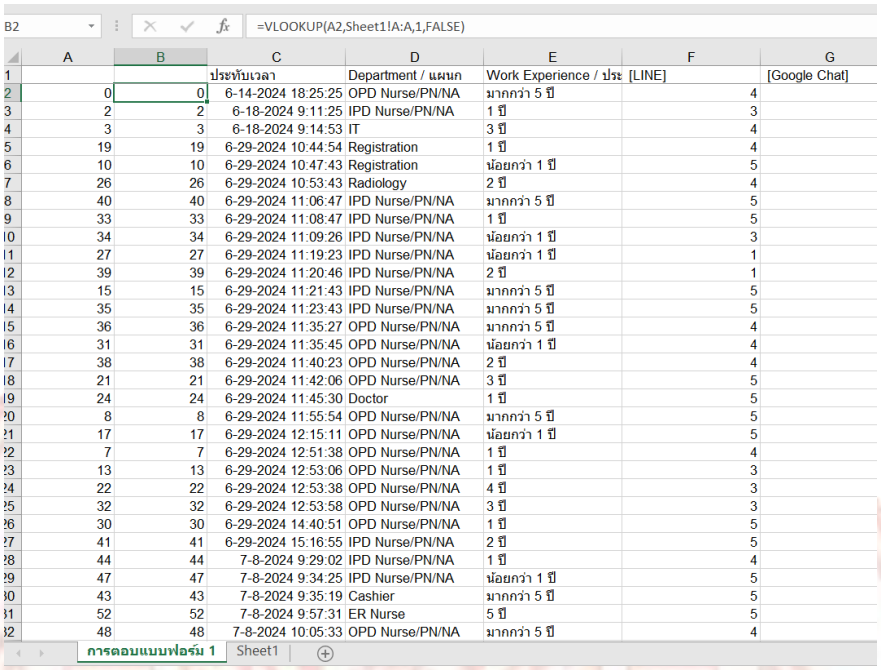
2.3.8 ตั้งค่าเพิ่มเติมจากข้อ 2.3.7 ให้ทำการเลือก check box กำหนดค่า Delimiters ที่ Tab, Comma, Space และ Treat consecutive delimiters as one จากนั้นกด Finish เพื่อให้ Excel

ทำการ Convert Text to Columns ตามค่าที่กำหนดไว้จากการเลือกกำหนด checkbox จากที่กล่าวไว้ข้างต้น ซึ่งแสดงดังภาพที่ 2-8



ภาพที่ 2-8 ตั้งค่าเพิ่มเติมจากข้อ 2.3.7

2.3.9 จากนั้นให้นำลำดับของข้อมูลที่ได้มา จับคู่ (Mapping) กับข้อมูลที่ได้รับจากการตอบแบบสอบการส่งต่อข้อมูลประกอบการรักษาผ่าน Community Application ทั้งหมด เมื่อได้ข้อมูลที่ได้จากการสุ่ม และลำดับของข้อมูลแล้วให้ใช้สูตร Vlookup บน Excel เพื่อ Mapping ข้อมูลเพื่อตรวจสอบความถูกต้อง และนำข้อมูลไปวิเคราะห์ต่อสำหรับกำหนดแผนกที่ใช้สำหรับทดสอบการติดตั้ง Hotspot Wi-Fi บนโปรแกรม (Program) Power BI Desktop เป็นเครื่องมือในการวิเคราะห์ข้อมูลธุรกิจ (Business Analytics Tool) และสร้างรายงาน Dashboard โดยแสดงข้อมูลเป็นตารางและกราฟพายเพื่อให้สามารถตรวจสอบ และแยกข้อมูลที่ต้องการนำมาใช้งานได้อย่างถูกต้อง และชัดเจน โดยจากที่กล่าวมาข้างต้นจะแสดงดังภาพที่ 2-9 และภาพที่ 2-10 ตามลำดับ

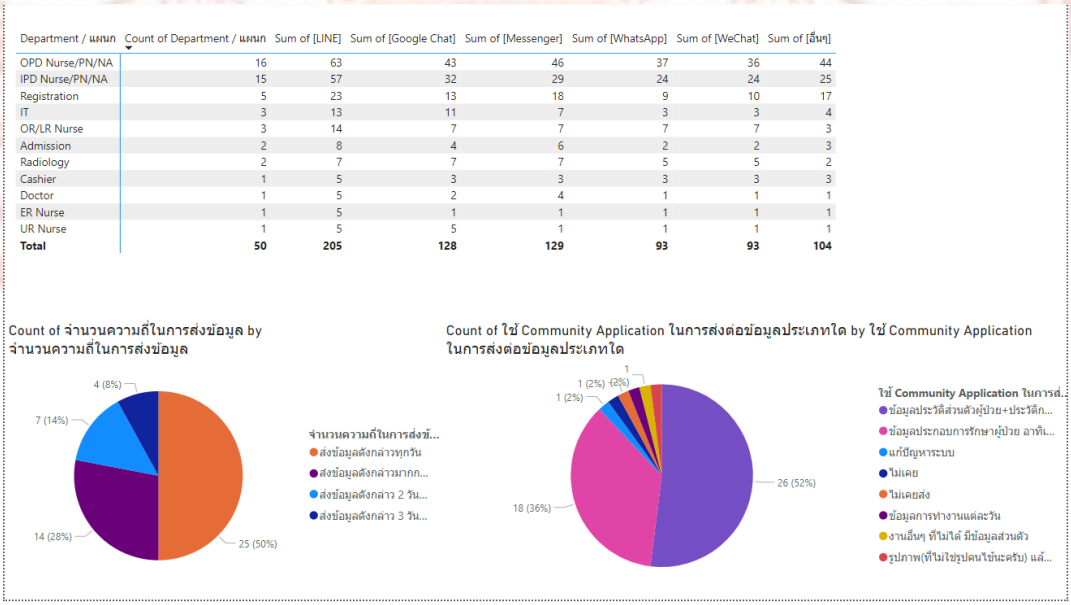


B2 =VLOOKUP(A2,Sheet1!A:A,1,FALSE)

	A	B	C	D	E	F	G
1			ประทับเวลา	Department / แผนก	Work Experience / ประ	[LINE]	[Google Chat]
2	0	0	6-14-2024 18:25:25	OPD Nurse/PN/NA	มากกว่า 5 ปี	4	
3	2	2	6-18-2024 9:11:25	IPD Nurse/PN/NA	1 ปี	3	
4	3	3	6-18-2024 9:14:53	IT	3 ปี	4	
5	19	19	6-29-2024 10:44:54	Registration	1 ปี	4	
6	10	10	6-29-2024 10:47:43	Registration	น้อยกว่า 1 ปี	5	
7	26	26	6-29-2024 10:53:43	Radiology	2 ปี	4	
8	40	40	6-29-2024 11:06:47	IPD Nurse/PN/NA	มากกว่า 5 ปี	5	
9	33	33	6-29-2024 11:08:47	IPD Nurse/PN/NA	1 ปี	5	
10	34	34	6-29-2024 11:09:26	IPD Nurse/PN/NA	น้อยกว่า 1 ปี	3	
11	27	27	6-29-2024 11:19:23	IPD Nurse/PN/NA	น้อยกว่า 1 ปี	1	
12	39	39	6-29-2024 11:20:46	IPD Nurse/PN/NA	2 ปี	1	
13	15	15	6-29-2024 11:21:43	IPD Nurse/PN/NA	มากกว่า 5 ปี	5	
14	35	35	6-29-2024 11:23:43	IPD Nurse/PN/NA	มากกว่า 5 ปี	5	
15	36	36	6-29-2024 11:35:27	OPD Nurse/PN/NA	มากกว่า 5 ปี	4	
16	31	31	6-29-2024 11:35:45	OPD Nurse/PN/NA	น้อยกว่า 1 ปี	4	
17	38	38	6-29-2024 11:40:23	OPD Nurse/PN/NA	2 ปี	4	
18	21	21	6-29-2024 11:42:06	OPD Nurse/PN/NA	3 ปี	5	
19	24	24	6-29-2024 11:45:30	Doctor	1 ปี	5	
20	8	8	6-29-2024 11:55:54	OPD Nurse/PN/NA	มากกว่า 5 ปี	5	
21	17	17	6-29-2024 12:15:11	OPD Nurse/PN/NA	น้อยกว่า 1 ปี	5	
22	7	7	6-29-2024 12:51:38	OPD Nurse/PN/NA	1 ปี	4	
23	13	13	6-29-2024 12:53:06	OPD Nurse/PN/NA	1 ปี	3	
24	22	22	6-29-2024 12:53:38	OPD Nurse/PN/NA	4 ปี	3	
25	32	32	6-29-2024 12:53:58	OPD Nurse/PN/NA	3 ปี	3	
26	30	30	6-29-2024 14:40:51	OPD Nurse/PN/NA	1 ปี	5	
27	41	41	6-29-2024 15:16:55	IPD Nurse/PN/NA	2 ปี	5	
28	44	44	7-8-2024 9:29:02	IPD Nurse/PN/NA	1 ปี	4	
29	47	47	7-8-2024 9:34:25	IPD Nurse/PN/NA	น้อยกว่า 1 ปี	5	
30	43	43	7-8-2024 9:35:19	Cashier	มากกว่า 5 ปี	5	
31	52	52	7-8-2024 9:57:31	ER Nurse	5 ปี	5	
32	48	48	7-8-2024 10:05:33	OPD Nurse/PN/NA	มากกว่า 5 ปี	4	

การตอบแบบฟอร์ม 1 | Sheet1

ภาพที่ 2-9 นำลำดับของข้อมูลที่ได้มา Mapping กับข้อมูลการตอบแบบสอบทั้งหมด



Department / แผนก	Count of Department / แผนก	Sum of [LINE]	Sum of [Google Chat]	Sum of [Messenger]	Sum of [WhatsApp]	Sum of [WeChat]	Sum of [อื่นๆ]
OPD Nurse/PN/NA	16	63	43	46	37	36	44
IPD Nurse/PN/NA	15	57	32	29	24	24	25
Registration	5	23	13	18	9	10	17
IT	3	13	11	7	3	3	4
OR/LR Nurse	3	14	7	7	7	7	3
Admission	2	8	4	6	2	2	3
Radiology	2	7	7	7	5	5	2
Cashier	1	5	3	3	3	3	3
Doctor	1	5	2	4	1	1	1
ER Nurse	1	5	1	1	1	1	1
UR Nurse	1	5	5	1	1	1	1
Total	**50**	**205**	**128**	**129**	**93**	**93**	**104**

Count of จำนวนความถี่ในการส่งข้อมูล by จำนวนความถี่ในการส่งข้อมูล

Count of ใช้ Community Application ในการส่งต่อข้อมูลประเภทใด by ใช้ Community Application ในการส่งต่อข้อมูลประเภทใด

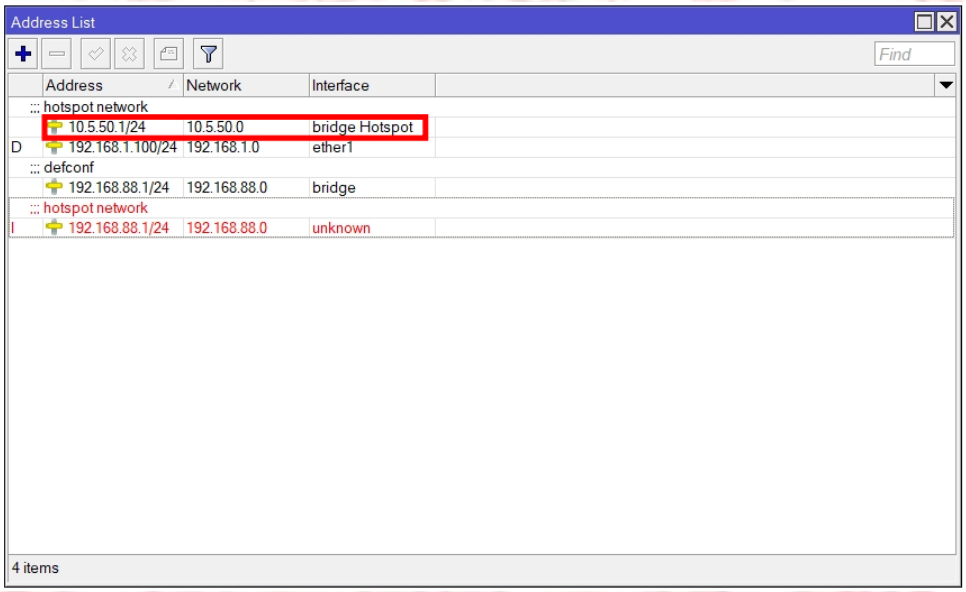
ภาพที่ 2-10 นำลำดับของข้อมูลที่ได้มา Mapping กับข้อมูลการตอบแบบสอบทั้งหมด

2.4 วิธีตั้งค่า Hotspot บน MikroTik hAP ax²

การตั้งค่า Hotspot สำหรับการเตรียมอุปกรณ์กระจายสัญญาณไวไฟก่อนติดตั้งตามจุดติดตั้งที่กำหนดไว้ เพื่อเก็บรวบรวมข้อมูลการเชื่อมต่อใช้งาน

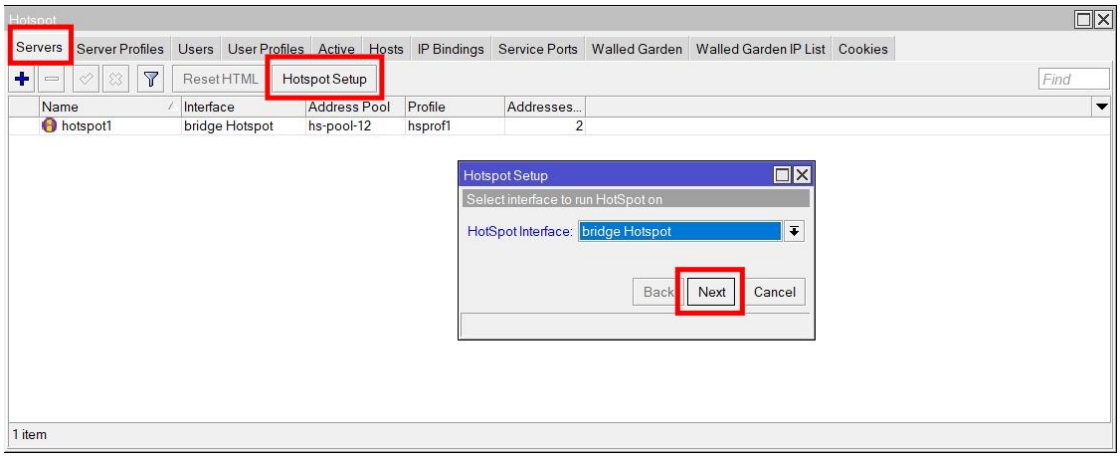
2.4.1 ตั้งค่าเมนู IP -> Addresses กดปุ่ม Add แล้วทำการตั้งค่า ดังภาพที่ 2-11

- Address : 10.5.50.1/24
- Network : 10.5.50.0
- Interface : bridge Hotspot



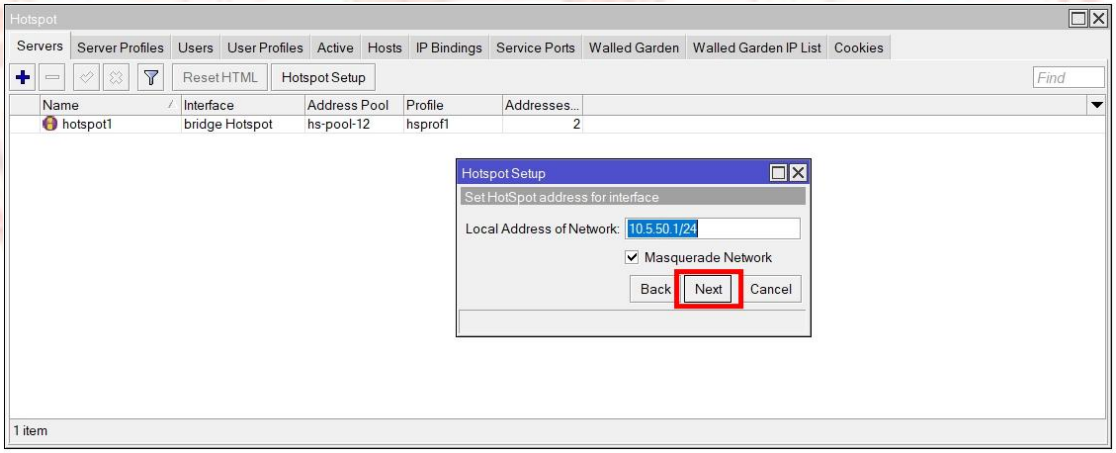
ภาพที่ 2-11 ตั้งค่าเมนู IP -> Addresses กดปุ่ม Add แล้วทำการตั้งค่า

2.4.2 ตั้งค่าเมนู IP -> Hotspot หัวข้อ Servers แล้วทำการตั้งค่าดังภาพที่ 2-12 กดุปุ่ม Hotspot Setup Hotspot Interface : bridge Hotspot เมื่อเสร็จแล้วกดปุ่ม Next



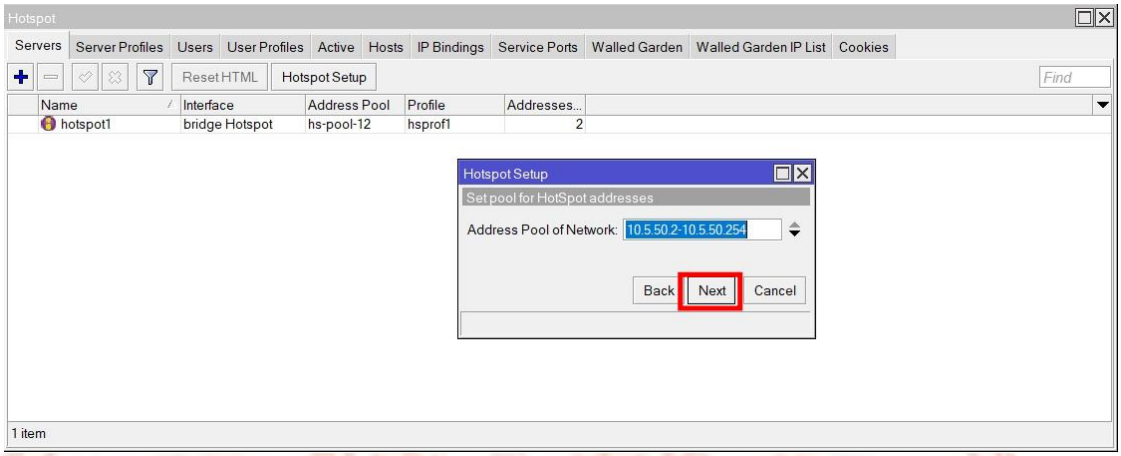
ภาพที่ 2-12 ตั้งค่าเมนู IP -> Hotspot หัวข้อ Servers แล้วทำการตั้งค่า

2.4.3 ตั้งค่าเพิ่มเติมจากข้อ 2.4.2 ทำการตรวจสอบ Local Address of Network กดปุ่ม Next เมื่อตรวจสอบเรียบร้อยแล้ว ดังภาพที่ 2-13



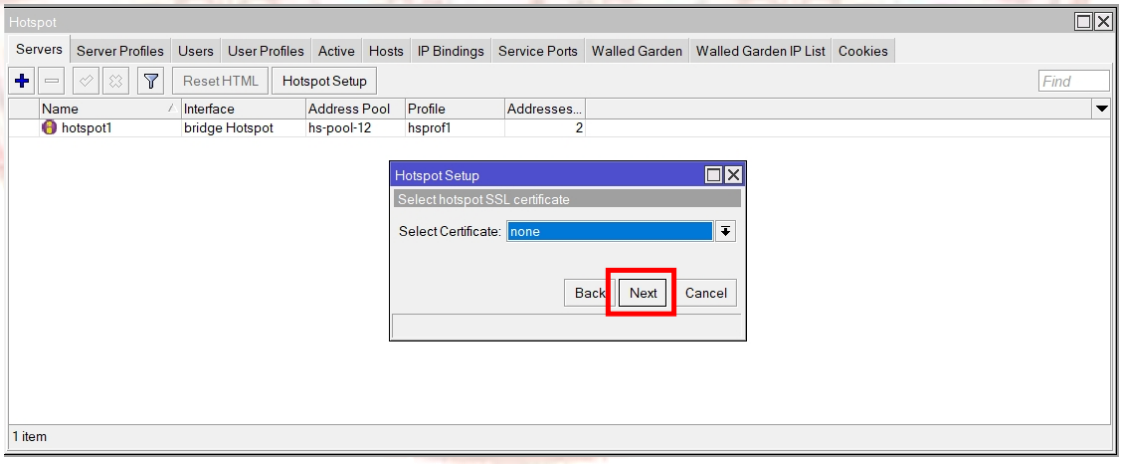
ภาพที่ 2-13 ตั้งค่าเพิ่มเติมจากข้อ 2.4.2

2.4.4 ตั้งค่าเพิ่มเติมจากข้อ 2.4.3 ทำการตรวจสอบ Address Pool of Network กดปุ่ม Next เมื่อตรวจสอบเรียบร้อยแล้ว ดังภาพที่ 2-14



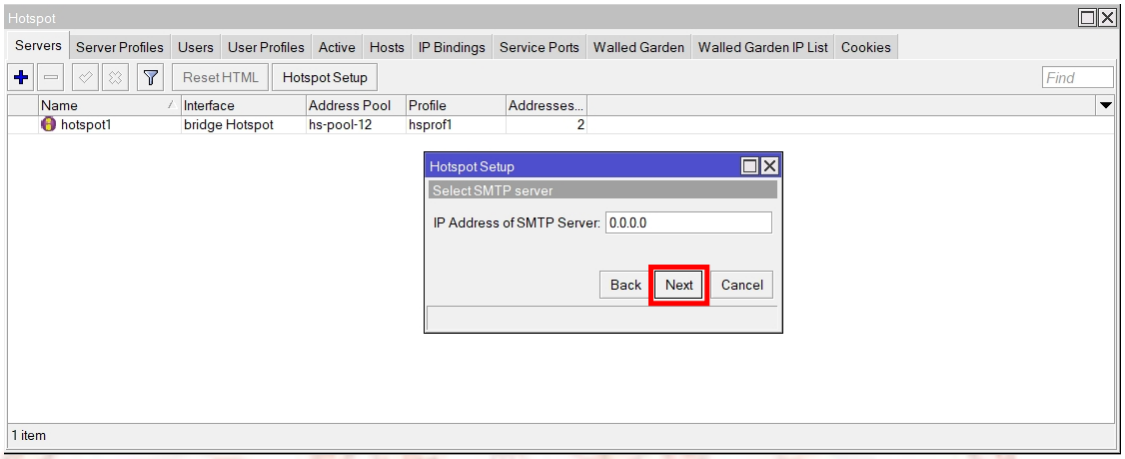
ภาพที่ 2-14 ตั้งค่าเพิ่มเติมจากข้อ 2.4.3

2.4.5 ตั้งค่าเพิ่มตามจากข้อ 2.4.4 Select Certificate : none (กรณียังไม่มี Certificate) กดปุ่ม Next เมื่อตรวจสอบเรียบร้อยแล้ว ดังภาพที่ 2-15



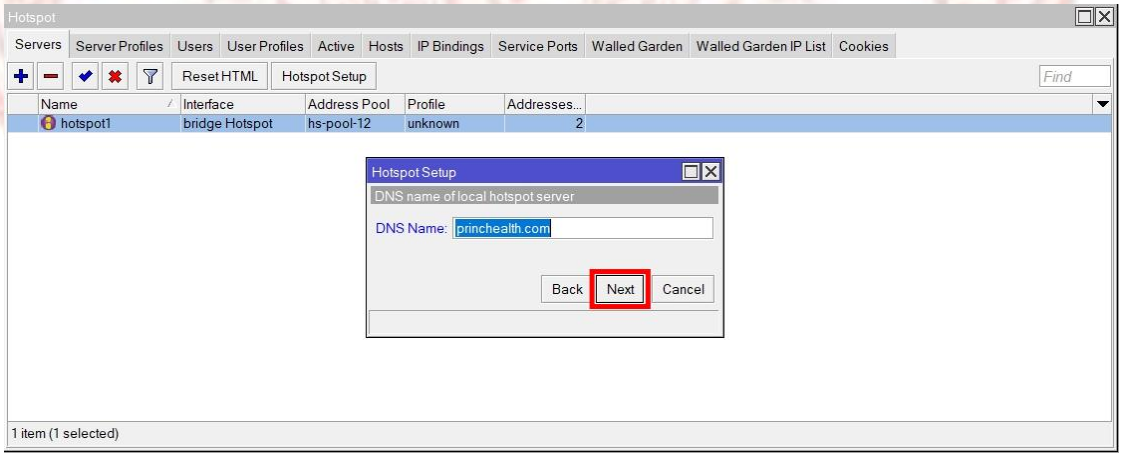
ภาพที่ 2-15 ตั้งค่าเพิ่มเติมจากข้อ 2.4.4

2.4.6 ตั้งค่าเพิ่มตามจากข้อ 2.4.5 IP Address of SMTP Server : 0.0.0.0 (ใส่ไว้ถ้ากรณีไม่มี SMTP Server) กดปุ่ม Next เมื่อกำหนดเรียบร้อยแล้ว ดังภาพที่ 2-16



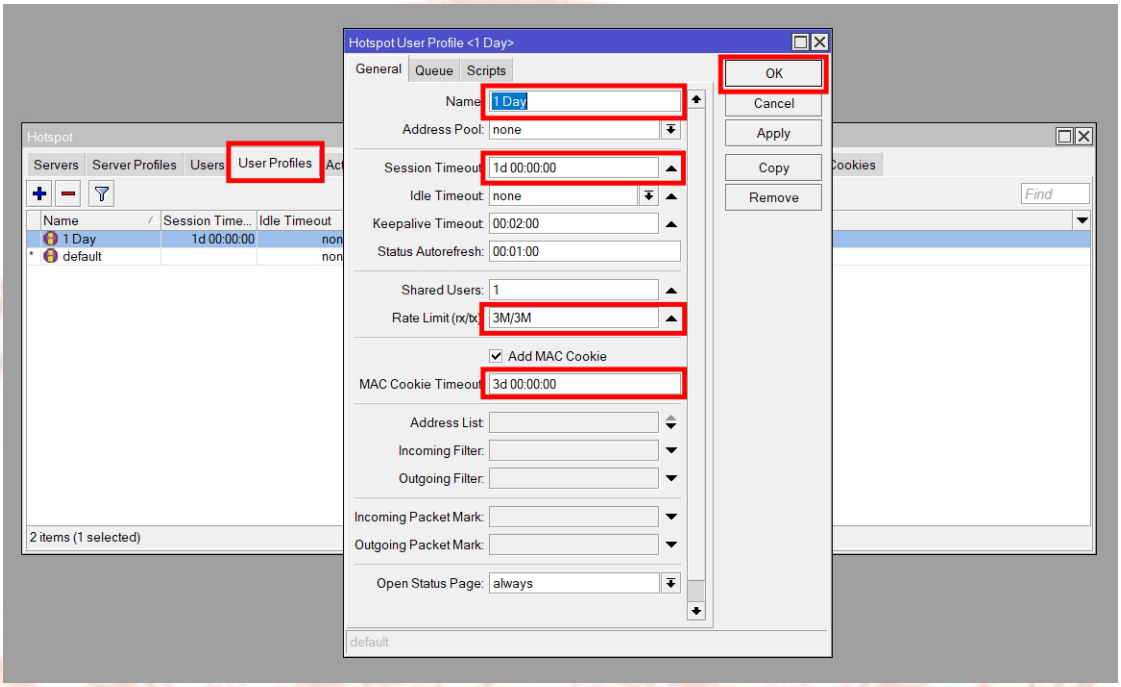
ภาพที่ 2-16 ตั้งค่าเพิ่มเติมจากข้อ 2.4.5

2.4.7 ตั้งค่าเพิ่มเติมจากข้อ 2.4.6 DNS Name : ใส่ชื่อ DNS Name ของเราโดยกำหนดขึ้นเอง (DNS Name ต้องตรงกับ SSL Certificate ที่จะเอามาใส่) กดปุ่ม Next เมื่อกำหนดค่าเรียบร้อยแล้ว ดังภาพที่ 2-17



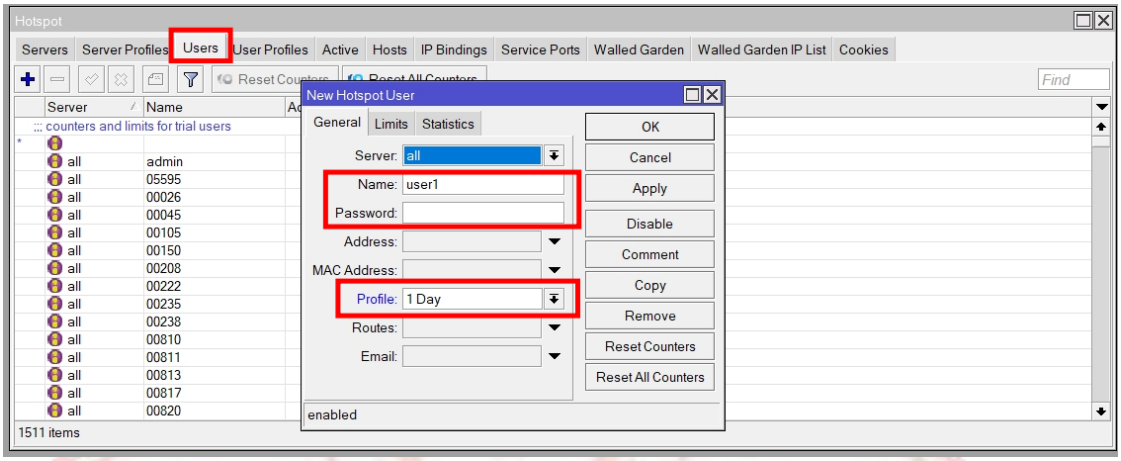
ภาพที่ 2-17 ตั้งค่าเพิ่มเติมจากข้อ 2.4.6

2.4.8 ตั้งค่า User Profiles สำหรับกำหนดการใช้งานของ User สร้าง User Profiles เพื่อกำหนด Name, Session Timeout, Rate Limit (rx/tx) และ MAC Cookie Timeout จากนั้นการปุ่ม OK ดังภาพที่ 2-18



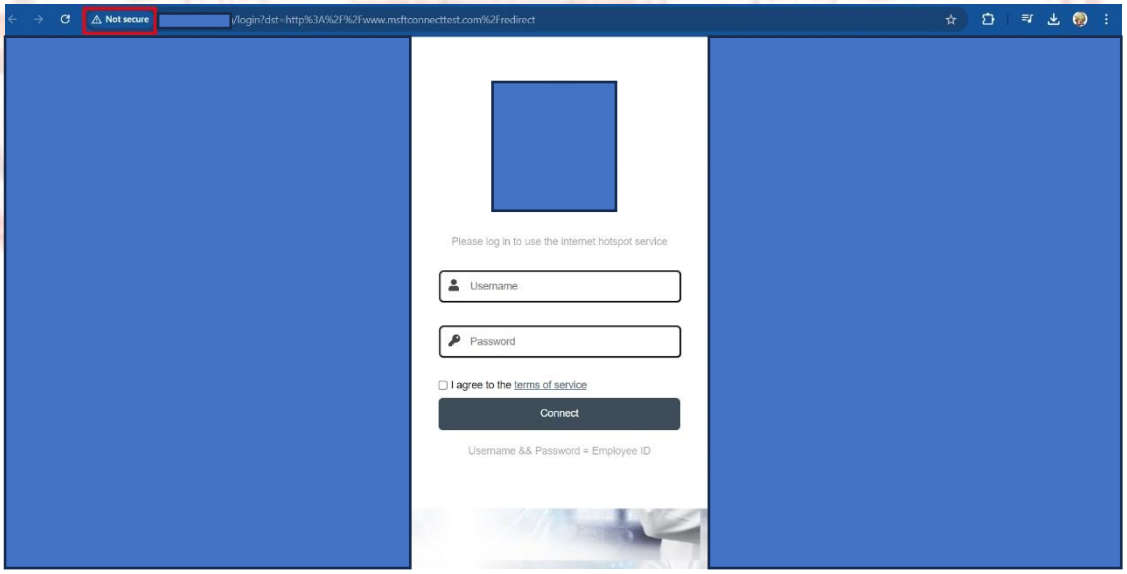
ภาพที่ 2-18 ตั้งค่า User Profiles สำหรับกำหนดการใช้งานของ User

2.4.9 ตั้งค่า User สำหรับใช้งาน Hotspot หลังจากตั้งค่า Hotspot Server เรียบร้อยให้สร้าง Users Name Hotspot User : กำหนด User สำหรับ Login Hotspot Password for the User : กำหนด Password สำหรับ User ที่ใช้ Login Hotspot กำหนด Profile ที่สร้างจาก User Profiles จากนั้นกดปุ่ม OK เมื่อกำหนดค่าเรียบร้อยแล้ว ดังภาพที่ 2-19



ภาพที่ 2-19 ตั้งค่าเพิ่มเติมจากข้อ 2.4.7

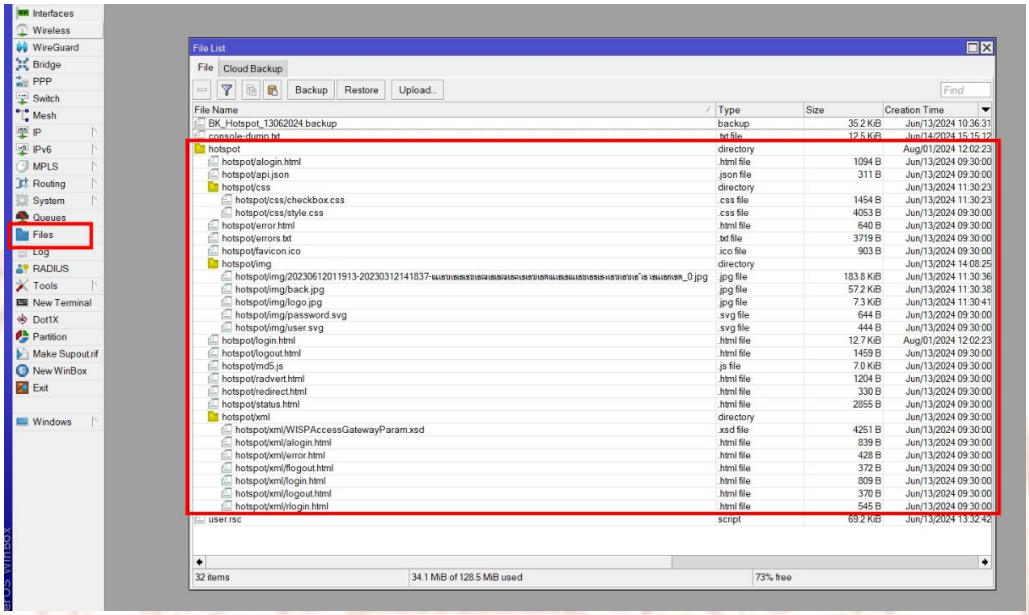
2.4.10 หน้า Login กรณีไม่ได้ใส่ SSL Certificate เมื่อทำการเชื่อมต่อ Hotspot หน้า Login จะขึ้นไม่ปลอดภัย ดังภาพที่ 2-20



ภาพที่ 2-20 หน้า Login กรณีไม่ได้ใส่ SSL Certificate

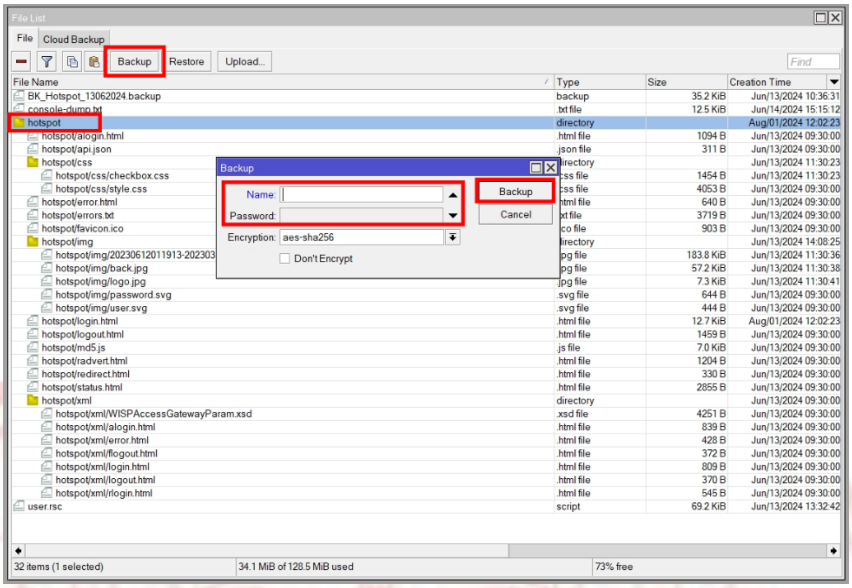
2.5 MikroTik แก้ไขหน้า HotSpot Login

2.5.1 ขั้นตอน - แก้ไขหน้าจอ Login ของ Hotspot เข้าเมนู IP > File ดังภาพที่ 2-21



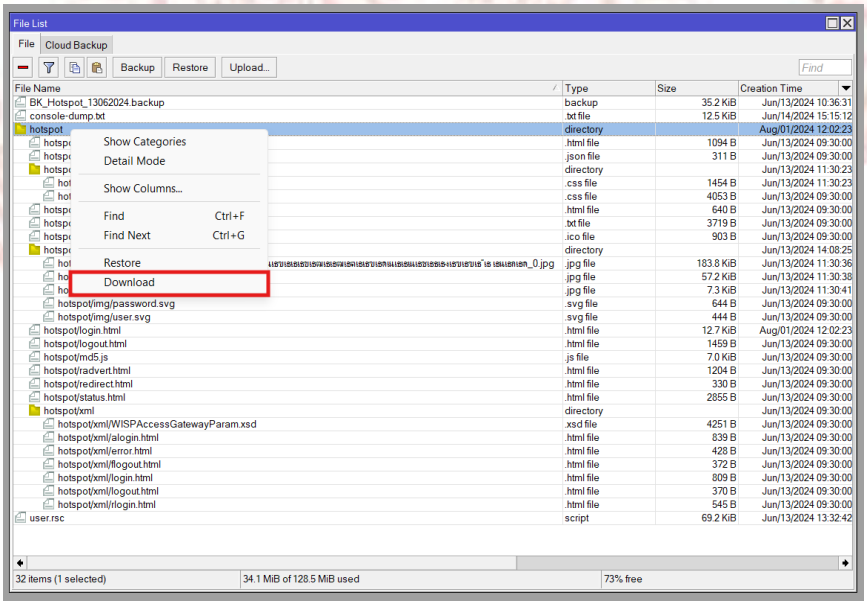
ภาพที่ 2-21 ขั้นตอน - แก้ไขหน้าจอ Login ของ Hotspot

2.5.2 ดับเบิ้ลคลิกที่โฟล์เดอร์ hotspot เพื่อคลิกทำการ Backup เลือก Folder hotspot จากนั้นกด Backup สามารถกำหนด Name, Password, Encrytion จากนั้นกดปุ่ม OK เพื่อยืนยัน ดังภาพที่ 2-22

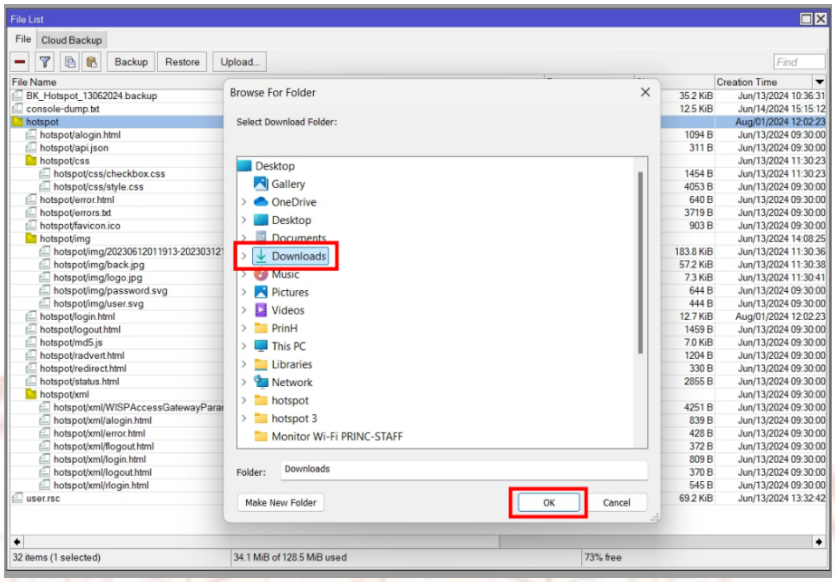


ภาพที่ 2-22 ดับเบิ้ลคลิกที่โฟล์เดอร์ hotspot เพื่อคลิกทำการ Backup

2.5.3 คลิกขวาที่โฟล์เดอร์ hotspot จากนั้น Download Folder hotspot ดังภาพที่ 2-23 และเลือก location ที่ต้องการบันทึก File จากนั้นกดปุ่ม OK เพื่อบันทึกการตั้งค่า ดังภาพที่ 2-24

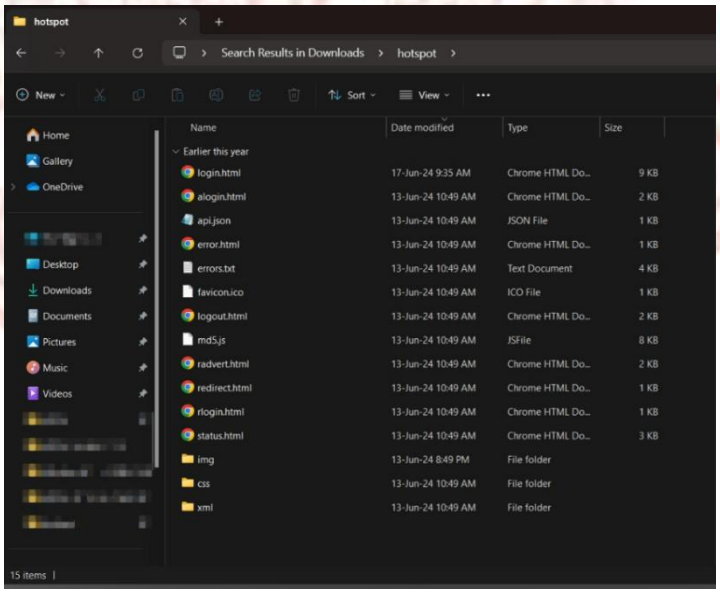


ภาพที่ 2-23 คลิกขวาที่โฟล์เดอร์ hotspot จากนั้น Download



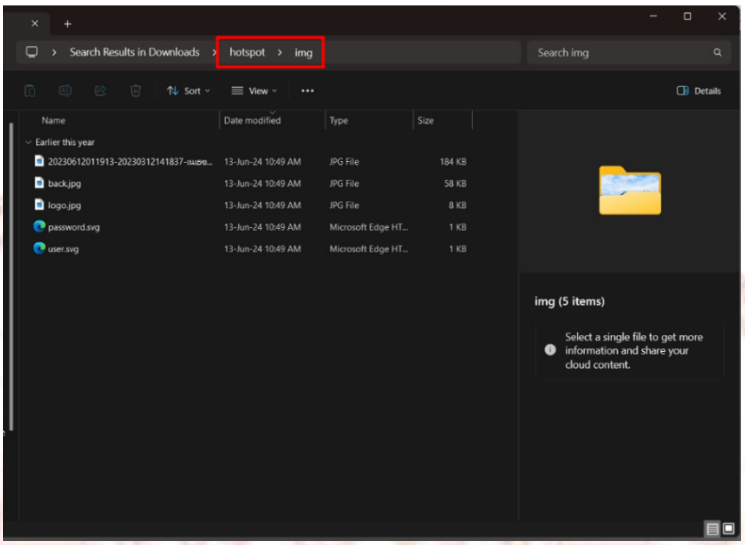
ภาพที่ 2-24 คลิกขวาที่โฟล์เดอร์ hotspot จากนั้น Download

2.5.4 จะได้โฟล์เดอร์ hotspot ทั้งหมดในตัว MikroTik ออกมา เพื่อทำการแก้ไขตามความต้องการ ดังภาพที่ 2-25



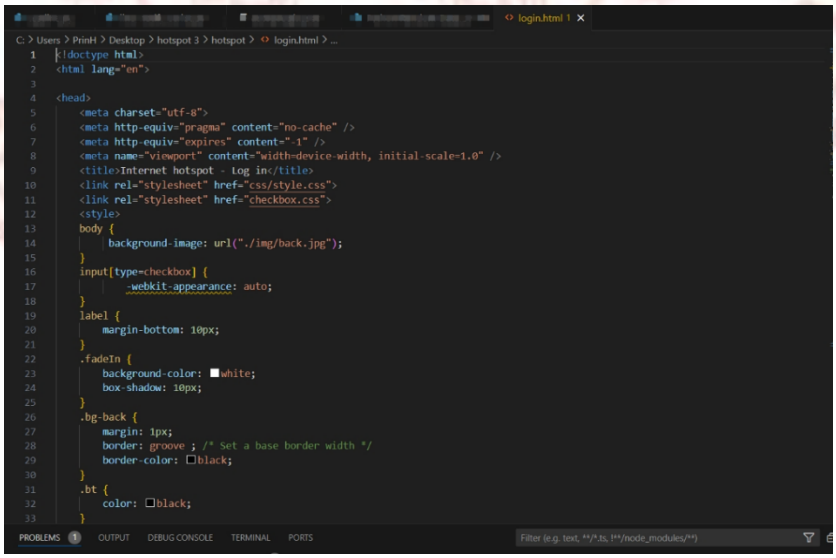
ภาพที่ 2-25 โฟล์เดอร์ hotspot ทั้งหมดในตัว MikroTik เพื่อทำการแก้ไขตามความต้องการ

2.5.5 ทำการคัดลอกรูปโลโก้ หรือไฟล์ที่ต้องการใส่ในโฟลเดอร์ /hotspot/img ดังภาพที่ 2-26



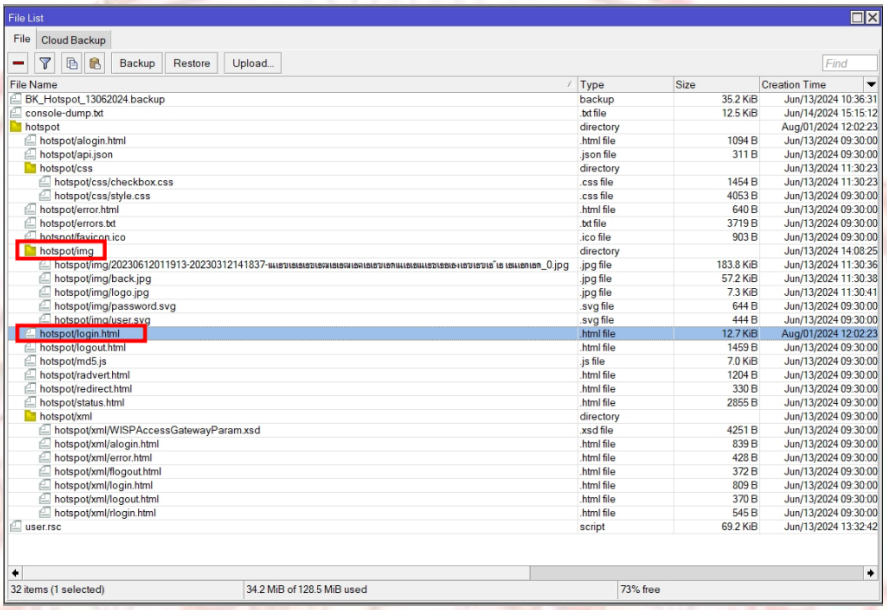
ภาพที่ 2-26 ทำการคัดลอกรูปโลโก้ หรือไฟล์ที่ต้องการใส่ในโฟลเดอร์ /hotspot/img

2.5.6 ทำการแก้ไขไฟล์ login.html โดยผ่านโปรแกรม Visual Studio Code ภาพที่ 2-27



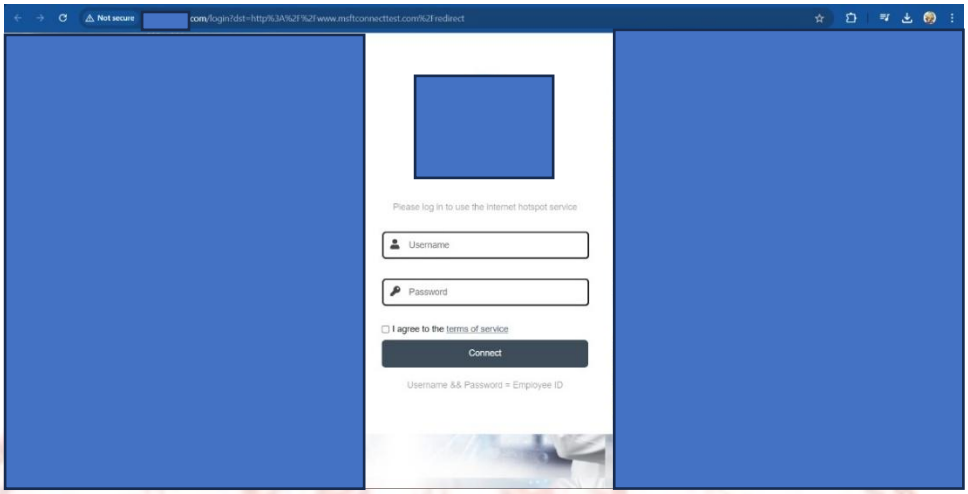
ภาพที่ 2-27 ทำการแก้ไขไฟล์ login.html โดยผ่านโปรแกรม Visual Studio Code

2.5.7 หลังจากทำการแก้ไข login.html เสร็จเรียบร้อย เข้ามาในส่วนของ Winbox แล้วทำการวางทับ File login.html เดิมใน MikroTik และเพิ่ม File Image ใน Folder hotspot/img ดังภาพที่ 2-28

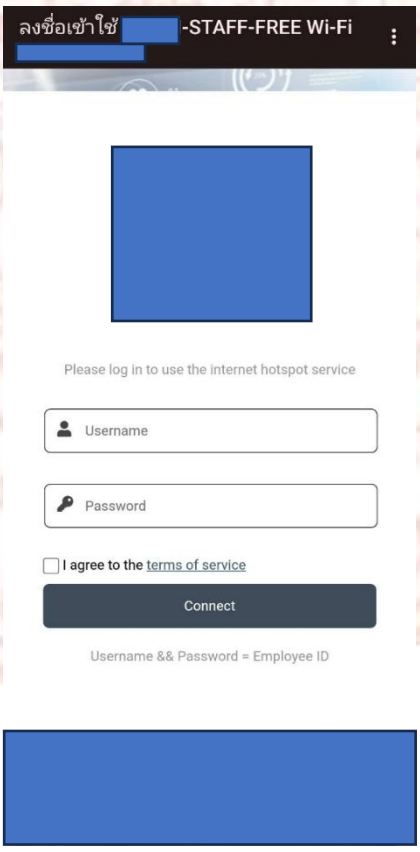


ภาพที่ 2-28 หลังจากทำการแก้ไข login.html เสร็จเรียบร้อย

2.5.8 ทดสอบเชื่อมต่อ Wi-Fi เข้าหน้า Login Hotspot แสดงผลบน Web Browser ดังภาพที่ 2-29 และแสดงผลบน Smart Phone Android ดังภาพที่ 2-30



ภาพที่ 2-29 ทดสอบเชื่อมต่อ Wi-Fi เข้าหน้า Login Hotspot



ภาพที่ 2-30 ทดสอบเชื่อมต่อ Wi-Fi เข้าหน้า Login Hotspot

2.6 การแก้ไขหน้า Log in Hotspot MikroTik ด้วยภาษา CSS และ JavaScript

หลังจากตั้งค่า Hotspot บนอุปกรณ์ MikroTik ระบบจะ Generate Folder Hotspot ให้ Download ลงเครื่องคอมพิวเตอร์เพื่อทำการแก้ไขหน้า login.html โดยทำตามขั้นตอนจากข้อ 2.5

2.6.1 การเชื่อมโยงสไตล์ และภาพพื้นหลัง Code ก่อนการแก้ไขเพิ่มเติมแสดงดังภาพที่ 2-31 และ Code หลังจากการแก้ไข โดยตั้งค่าให้เชื่อมโยงสไตล์ และภาพพื้นหลังที่ต้องการปรับแก้ไขแสดงดังภาพที่ 2-32

```
<link rel="stylesheet" href="css/style.css">
```

ภาพที่ 2-31 Code ก่อนการแก้ไข การเชื่อมโยงสไตล์ และภาพพื้นหลัง

```
<link rel="stylesheet" href="css/style.css">
<link rel="stylesheet" href="checkbox.css">
<style>
body {
    background-image: url("./img/back.jpg");
}
```

ภาพที่ 2-32 Code หลังการแก้ไข การเชื่อมโยงสไตล์ และภาพพื้นหลัง

2.6.2 การตั้งค่า Redirect ไปยัง Website ที่ต้องการ เมื่อทำการ Log in จะ Redirect ไปยัง Website ที่ต้องการ โดยนำ Link Website ไปวาง ดังแสดงภาพที่ 2-33

```
$(if chap-id)
<form name="sendin" action="$(link-login-only)" method="post" style="display:none">
    <input type="hidden" name="username" />
    <input type="hidden" name="password" />
    <input type="hidden" name="dst" value="https://w[redacted].com/" />
    <input type="hidden" name="popup" value="true" />
</form>
```

ภาพที่ 2-33 การตั้งค่า Redirect ไปยัง Website ที่ต้องการ

2.6.3 การแทรกรูปภาพ Logo Code ก่อนการแก้ไขเพิ่มเติมแสดงดังภาพที่ 2-34 และ Code หลังจากการแก้ไข โดยตั้งค่าให้แทรกรูปภาพโลโก้ที่ต้องการปรับแก้ไขแสดงดังภาพที่ 2-35

```
<img class="logo" src="logo.png" width="Auto"  />
```

ภาพที่ 2-34 Code เดิมก่อนการแก้ไขแทรกรูป Logo

```
<img src="img/logo.jpg" class="logo"  data-name="Layer1" alt="logo">
```

ภาพที่ 2-35 Code หลังจากการแก้ไขแทรกรูป Logo

2.6.4 การแทรกคำสั่ง และการจัดรูปแบบ CSS ที่ปรับแต่งเพิ่มเติม แสดงดังภาพที่ 2-36

- background-color: white; ตั้งค่าสีพื้นหลังขององค์ประกอบเป็นสีขาว
- box-shadow: 10px; สร้างเงาให้กับกล่องขององค์ประกอบ ความยาว และขนาดของเงาคือ 10 พิกเซล
- margin: 1px; กำหนดระยะขอบภายนอกขององค์ประกอบเป็น 1 พิกเซล
- border: groove; กำหนดรูปแบบเส้นขอบเป็นแบบ groove
- border-color: black; กำหนดสีของเส้นขอบเป็นสีดำ
- color: black; กำหนดสีข้อความขององค์ประกอบเป็นสีดำ

```css
.fadeIn {
    background-color: white;
    box-shadow: 10px;
}
.bg-back {
    margin: 1px;
    border: groove ; /* Set a base border width */
    border-color: black;
}
.bt {
    color: black;
}
```

ภาพที่ 2-36 การแทรกคำสั่ง และการจัดรูปแบบ CSS

2.6.5 ฟังก์ชั่น JavaScript เพื่อจัดการกับการตรวจสอบเงื่อนไข และการแสดงป๊อปอัปฟังก์ชันที่ควบคุมการทำงานของ checkbox ปุ่ม submit และ popup message บนหน้าเว็บ โดยมีการเปลี่ยนแปลงการ แสดงผลตามสถานะของ checkbox

2.6.5.1 Event Listener สำหรับ checkbox เมื่อ checkbox มีการเปลี่ยนแปลง (checked หรือ unchecked) ฟังก์ชันนี้จะทำการเปิดหรือปิดใช้งานปุ่ม submit และแสดง popup message หาก checkbox ถูก checked และแสดงข้อความเตือนถ้าไม่ได้ถูก checked แสดงดังภาพที่ 2-37

```javascript
document.getElementById('my-checkbox').addEventListener('change', function() {
var submitButton = document.getElementById('submit-button');
var message = document.getElementById('message');
var popup = document.getElementById('popup');
var popupMessage = document.getElementById('popup-message');

if (this.checked) {
    submitButton.disabled = false;
    message.textContent = '';
    submitButton.style.cursor = 'pointer'; // Change cursor to pointer when enabled
    popup.style.display = 'block';
} else {
    submitButton.disabled = true;
    message.textContent = 'You must agree to the terms and conditions to submit.';
    message.style.color = 'red';
    submitButton.style.cursor = 'not-allowed'; // Change cursor to not-allowed when disabled

}
});
```

ภาพที่ 2-37 Event Listener สำหรับ Checkbox

2.6.5.2 Event Listener สำหรับปุ่ม submit เมื่อคลิกปุ่ม submit จะมีการแสดงข้อความว่า "Form submitted successfully!" พร้อมเปลี่ยนสีข้อความเป็นสีเขียวเพื่อแสดงสถานะสีแสดงดังภาพที่ 2-38

```
document.getElementById('submit-button').addEventListener('click', function() {
    var message = document.getElementById('message');
    message.textContent = 'Form submitted successfully!';
    message.style.color = 'green';
});
```

ภาพที่ 2-38 Event Listener สำหรับปุ่ม Submit

2.6.5.3 Event Listener สำหรับปุ่ม Close ของ Popup เมื่อคลิกปุ่ม close ของ popup จะทำการปิด popup แสดงดังภาพที่ 2-39

```
document.querySelector('.close').addEventListener('click', function() {
document.getElementById('popup').style.display = 'none';
 });
```

ภาพที่ 2-39 Event Listener สำหรับปุ่ม Close ของ Popup

2.6.5.4 การปิด popup เมื่อคลิกนอกพื้นที่ popup เมื่อคลิกนอกพื้นที่ popup จะทำการปิด popup แสดงดังภาพที่ 2-40

```
window.addEventListener('click', function(event) {
    var popup = document.getElementById('popup');
    if (event.target == popup) {
        popup.style.display = 'none';
    }
});
```

ภาพที่ 2-40 การปิด Popup เมื่อคลิกนอกพื้นที่ Popup

2.6.6 การเพิ่มปุ่ม และฟอร์มเงื่อนไข

- label องค์ประกอบนี้ใช้ในการสร้างกลุ่มขององค์ประกอบฟอร์มที่มีข้อความอธิบายอยู่ข้างๆ

- input type="checkbox" สร้างกล่องเลือก (checkbox) ที่มี id เป็น my-checkbox

- span ใช้เพื่อแสดงข้อความ "I agree to the terms of service" โดยที่ "terms of service" เป็นลิงก์ที่เรียกฟังก์ชัน showTerms() เมื่อคลิก

- สร้างปุ่ม submit ที่มี id เป็น submit-button และมีข้อความว่า "Connect" ปุ่มนี้ถูกปิดใช้งาน (disabled)

- สร้างองค์ประกอบ p ที่มี id เป็น message และคลาส message ใช้สำหรับแสดงข้อความแจ้งเตือน โดยแสดงดังภาพที่ 2-41

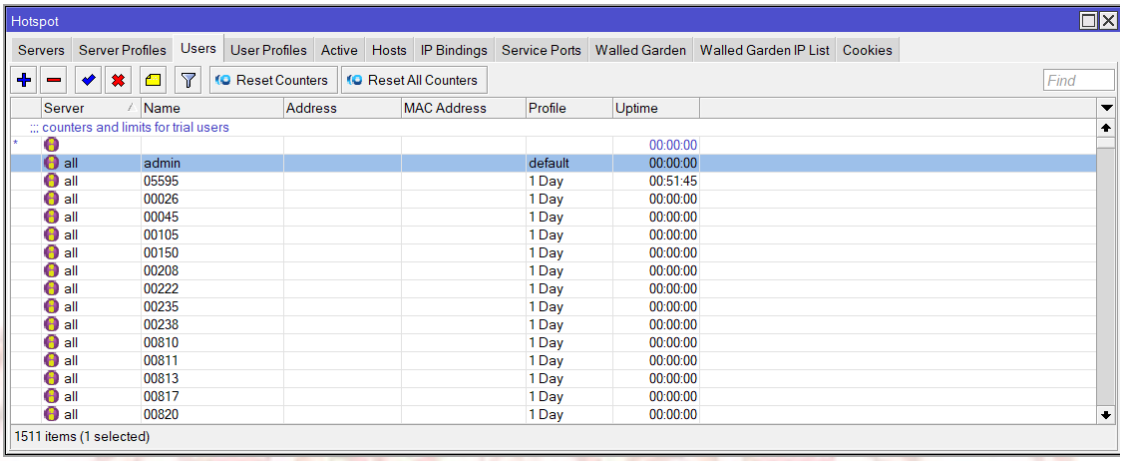
```
<label class="container">
    <input type="checkbox" id="my-checkbox"/>
    <span>I agree to the <a href="#" onclick="showTerms(); return false;">terms of service</a></span>
</label>
<input type="submit" id="submit-button" value="Connect" disabled/>
<p id="message" class="message"></p>
```

ภาพที่ 2-41 การเพิ่มปุ่ม และฟอร์มเงื่อนไข

2.7 การสร้าง User Account หลายคนพร้อมกันใน MikroTik

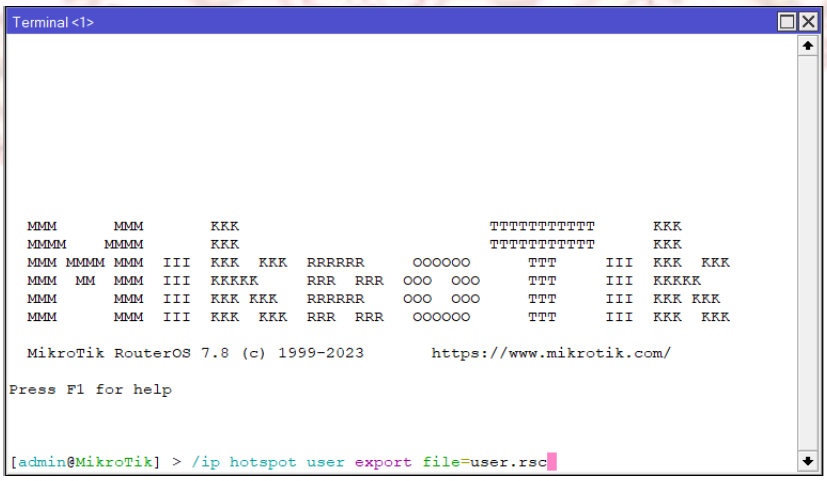
การใช้งาน Hotspot, VPN หรือระบบยืนยันตัวต่างๆ อาจต้องมีการเพิ่ม User ใน MikroTik ครั้งละหลายๆ Users พร้อมกัน ในการใช้โปรแกรม Winbox จะสามารถเพิ่มได้เพียงครั้งละ User เท่านั้น แต่สามารถเพิ่มได้ครั้งละหลายๆ User โดยการ Import File ที่มีรายชื่อเข้าไปใน MikroTik โดยมีขั้นตอนดังนี้

2.7.1 เข้า MikroTik ผ่านโปรแกรม Winbox ไปที่เมนู IP เลือก Hotspot แล้วกำหนดค่าต่างๆ ของ Users ที่ต้องการก่อน ดังภาพที่ 2-42 กำหนด Profile 1 Day ให้กับ User

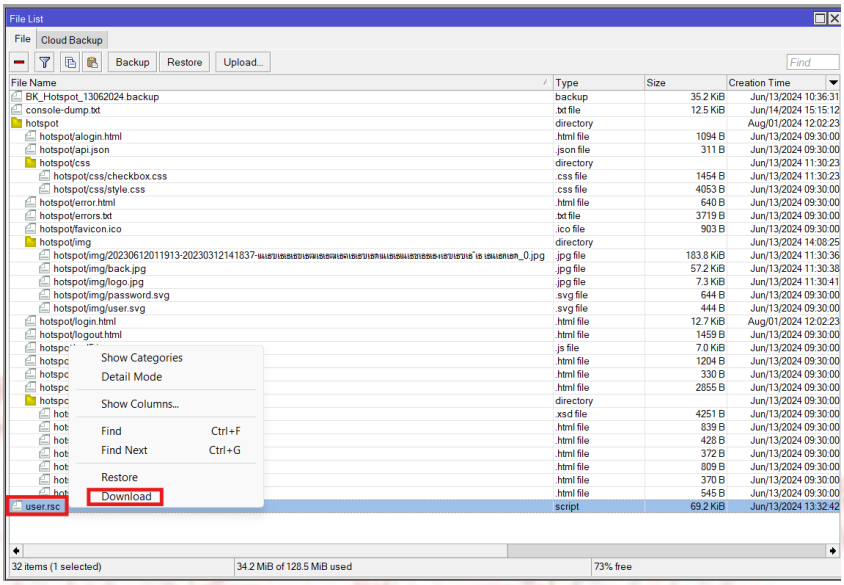


ภาพที่ 2-42 เข้า MikroTik ผ่านโปรแกรม Winbox

2.7.2 ไปที่เมนู New Terminal พิมพ์คำสั่ง /ip hotspot user export file=user.rsc ดังภาพที่ 2-43 จะได้ไฟล์ที่ชื่อ user. rsc ในเมนู File ให้ทำการคลิกขวาเพื่อ Download ไว้ที่เครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่ออยู่ ดังภาพที่ 2-44

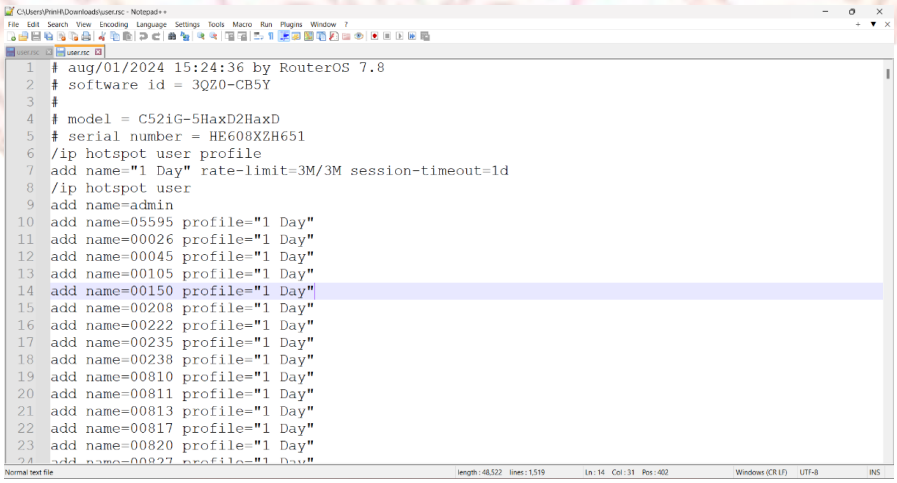


ภาพที่ 2-43 เมนู New Terminal พิมพ์คำสั่ง

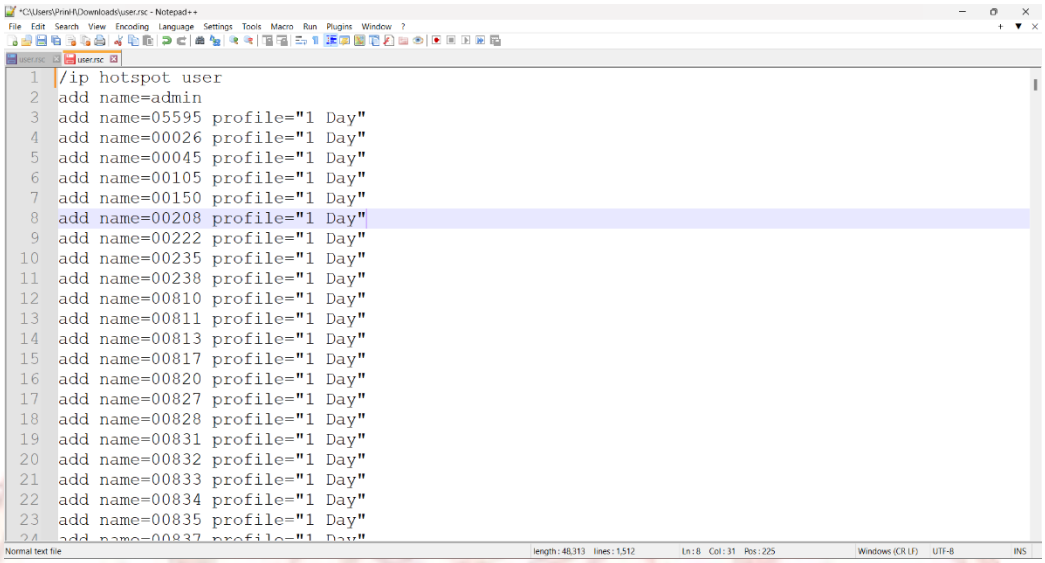


ภาพที่ 2-44 ไฟล์ที่ชื่อ user. rsc ในเมนู File

2.7.3 เปิดไฟล์ user.rsc ด้วยโปรแกรมประเภท Notepad++ ดังภาพที่ 2-45 จะลบส่วนข้างบนออก หรือจะแก้แค่ส่วนล่างที่อยู่หลังจากบรรทัด /ip hotspot user นี้ก็ได้ โดยเปลี่ยนช่องว่างธรรมดาไปเป็นช่องว่างด้วยปุ่ม Tab (ให้ลบ ช่องว่างออกแล้ว กดปุ่ม Tab แทน 1 ครั้ง) ทำแบบนี้ทุกช่อง และสำหรับข้อมูลของแต่ละ User ต้องอยู่ในบรรทัดเดียวกัน ดังภาพที่ 2-46

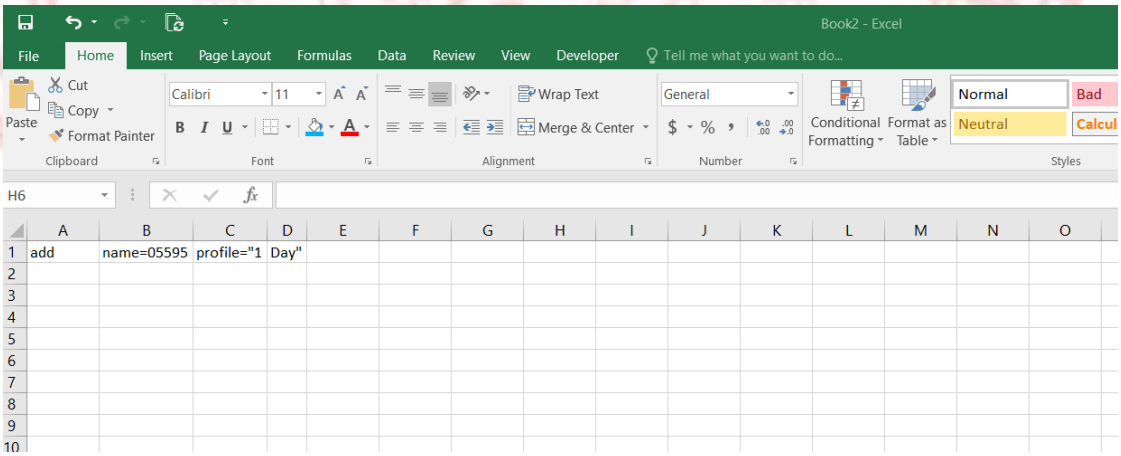


ภาพที่ 2-45 ไฟล์ user.rsc ด้วยโปรแกรมประเภท Text Editor



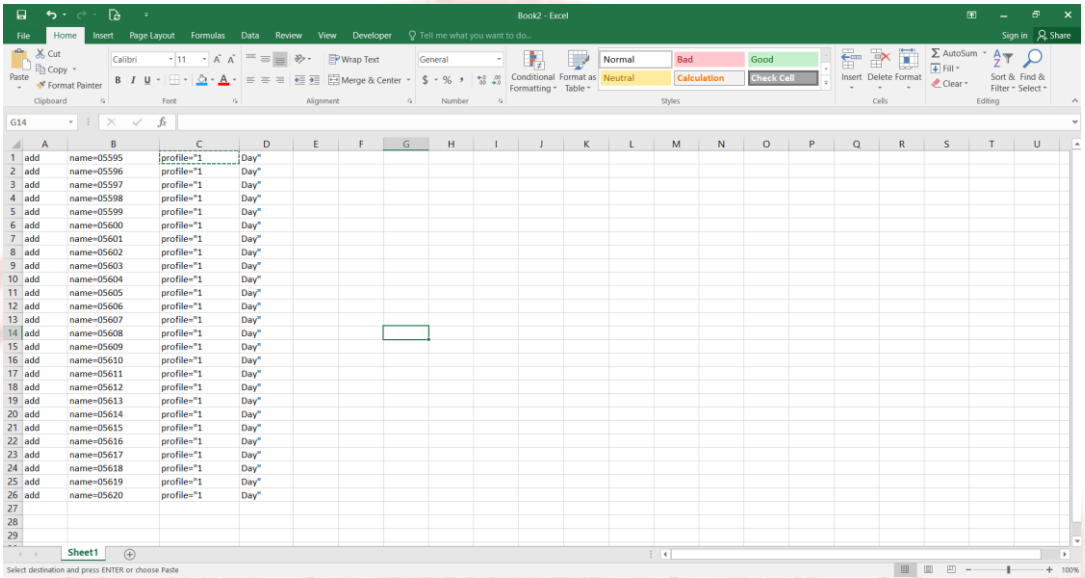
ภาพที่ 2-46 ลบคำสั่งที่อยู่หลังจากบรรทัด /ip hotspot user

2.7.4 คัดลอกข้อมูลที่เป็น User ID ที่เราได้สร้างไว้ จากนั้นเปิดโปรแกรม Microsoft Excel วางข้อมูลที่ เราได้คัดลอกไว้ลงไป ข้อมูลก็จะไปอยู่ ตามช่องในตารางพอดี ดังภาพที่ 2-47

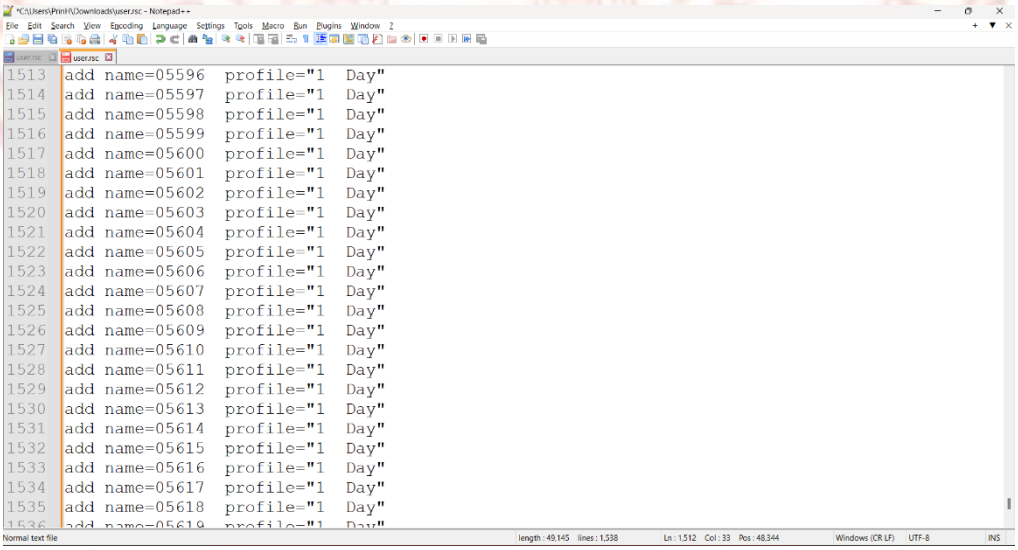


ภาพที่ 2-47 คัดลอกข้อมูลที่เป็น User ID ที่เราได้สร้างไว้

จากนั้นถ้าต้องการเพิ่มยูสเซอร์ ก็สามารถนำข้อมูลของยูสเซอร์ที่จะสร้างใหม่ลงไป โดยให้อิงจากแบบฟอร์มเดิม จากนั้นให้คัดลอกข้อมูลทั้งหมดแล้วนำไปวางในไฟล์ user.rsc จากนั้น Save เพื่อบันทึกข้อมูล ดังภาพที่ 2-48 และภาพที่ 2-49

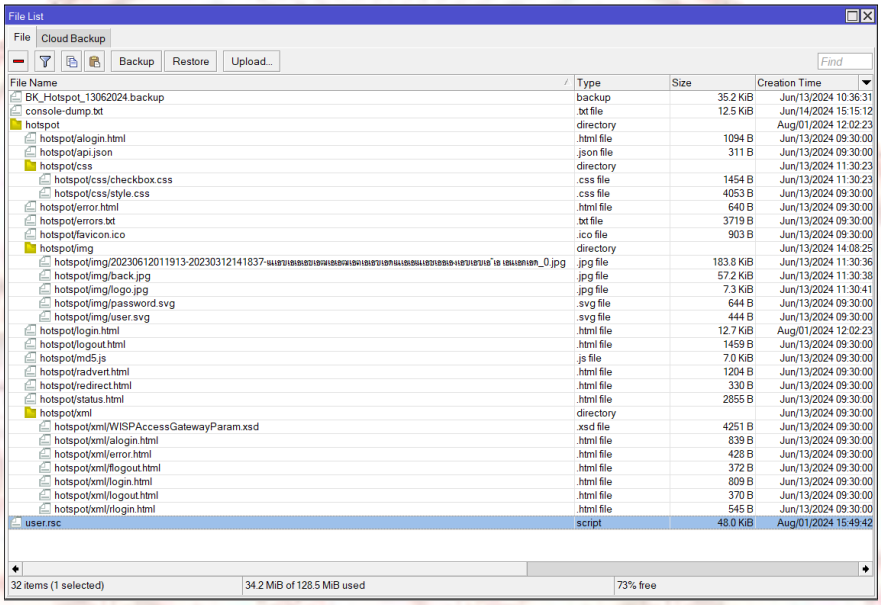


ภาพที่ 2-48 นำข้อมูลของ User จะสร้างใหม่ลงไป



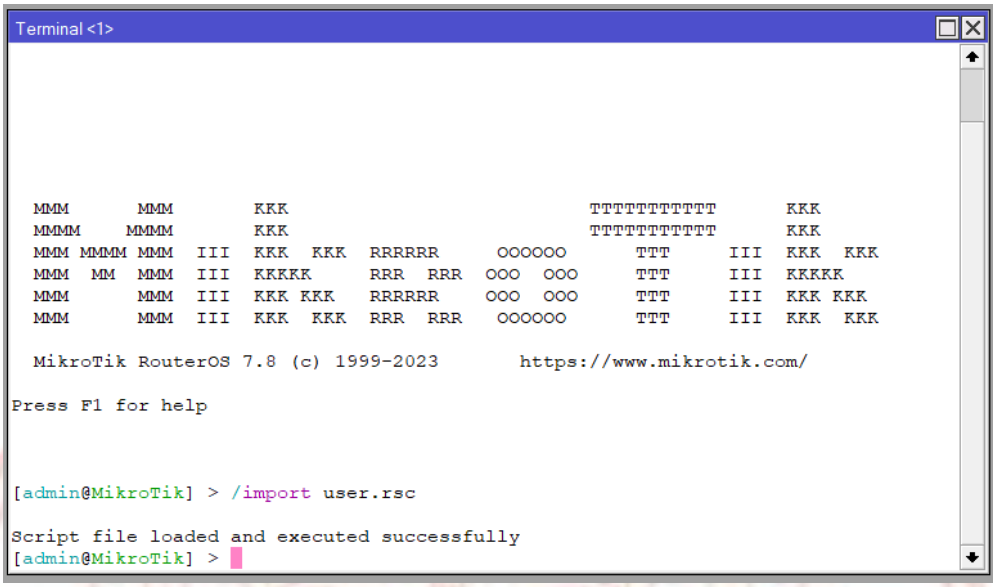
ภาพที่ 2-49 คัดลอกข้อมูลทั้งหมดแล้วนำไปวางในไฟล์ user.rsc

2.7.5 กลับมาที่โปรแกรม Winbox เลือกคำสั่ง New Terminal ให้ทำการลากไฟล์ user.rsc มาใส่ในหน้าต่างนี้ ตัวไฟล์จะไปปรากฏ และ Save ทับไฟล์เดิมที่อยู่ในเมนูคำสั่ง Files (ลองสังเกตขนาดของไฟล์ user.rsc จะมีจำนวนเพิ่มมากขึ้นกว่าตอนแรกที่นำออกไป) ถึงตรงนี้ถ้าใน Hotspot มี User ตรงกับไฟล์ที่นำเข้ามาให้ ไปลบยูสเซอร์ที่ Tab Users ออกก่อน ไม่เช่นนั้นจะทำขั้นตอนต่อไปไม่ได้ ดังภาพที่ 2-50



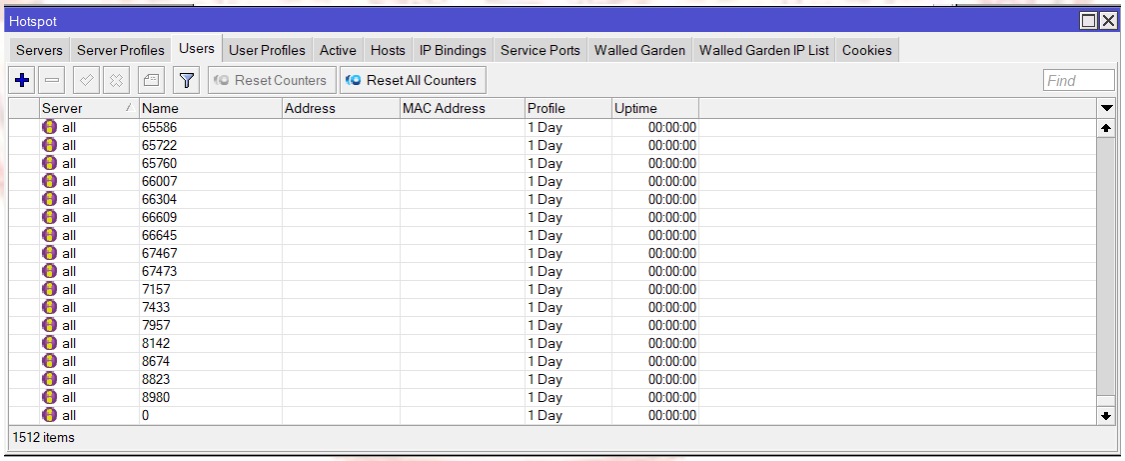
ภาพที่ 2-50 ทำการลากไฟล์ user.rsc มาใส่ในหน้าต่างนี้

2.7.6 กลับมาที่หน้าต่างคำสั่ง New Terminal พิมพ์คำสั่ง /import user.rsc แล้วกดปุ่ม Enter ถ้าทำถูกขั้นตอน จะปรากฏข้อความ “Script file loaded and executed successfully” ดังภาพที่ 2-51



ภาพที่ 2-51 พิมพ์คำสั่ง /import user.rsc

2.7.7 ตรวจสอบหน้าต่าง Hotspot Tab Users จะปรากฏ User ที่เราได้สร้างไว้ ดังภาพที่ 2-52

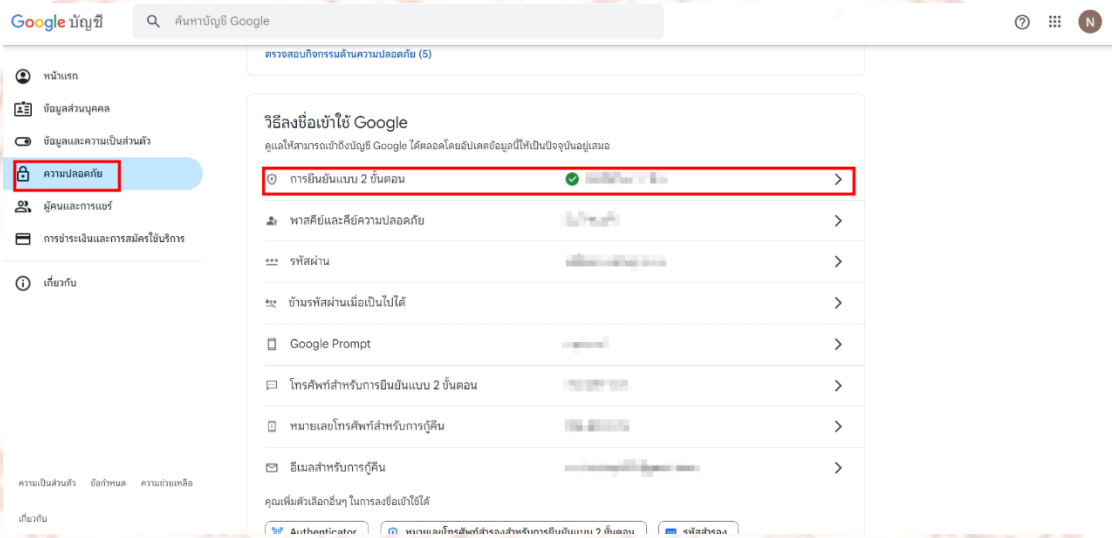


ภาพที่ 2-52 หน้าต่าง Hotspot

2.8 การสร้าง app passwords สำหรับ Account ที่ใช้ Google 2FA สำหรับตั้งค่าส่ง Logging Hotspot Report MikroTik

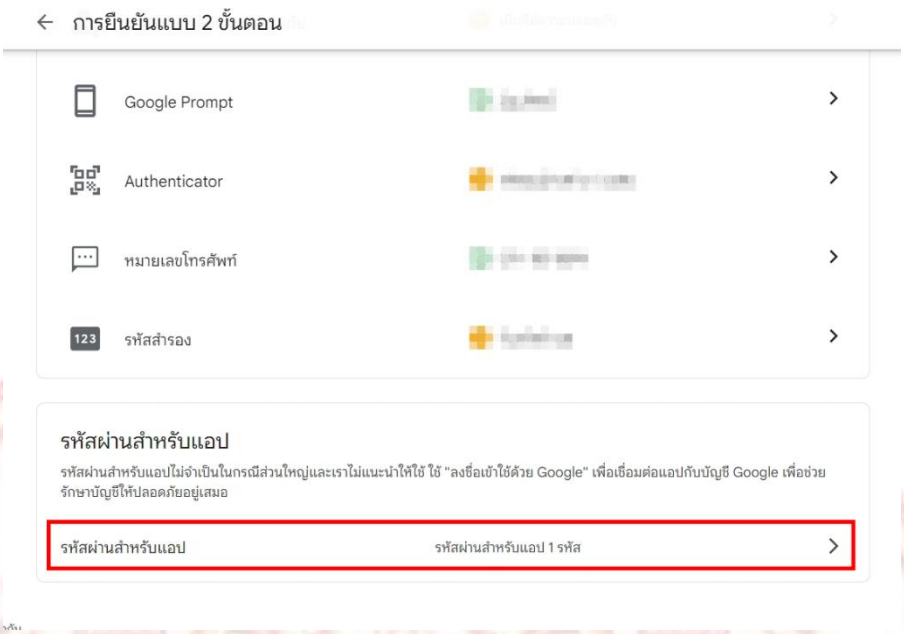
เนื่องจากก่อนการตั้งค่าให้อุปกรณ์ MikroTik ให้ส่ง Logging Report เข้า E-mail ต้องทำการตั้งค่าความปลอดภัยก่อน โดยการสร้าง app passwords สำหรับอุปกรณ์ Mikrotik โดยเฉพาะ

2.8.1 การตั้งค่าความปลอดภัยสำหรับสร้าง app passwords เข้าไปที่การตั้งค่าเลือกความปลอดภัย และการยืนยันแบบ 2 ขั้นตอนดังภาพที่ 2-53

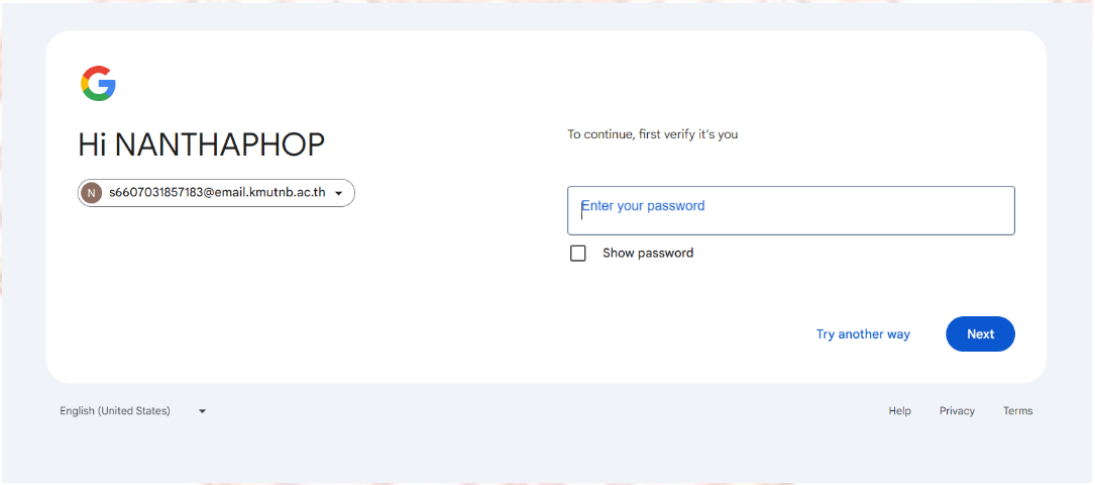


ภาพที่ 2-53 การตั้งค่าความปลอดภัยสำหรับสร้าง app passwords

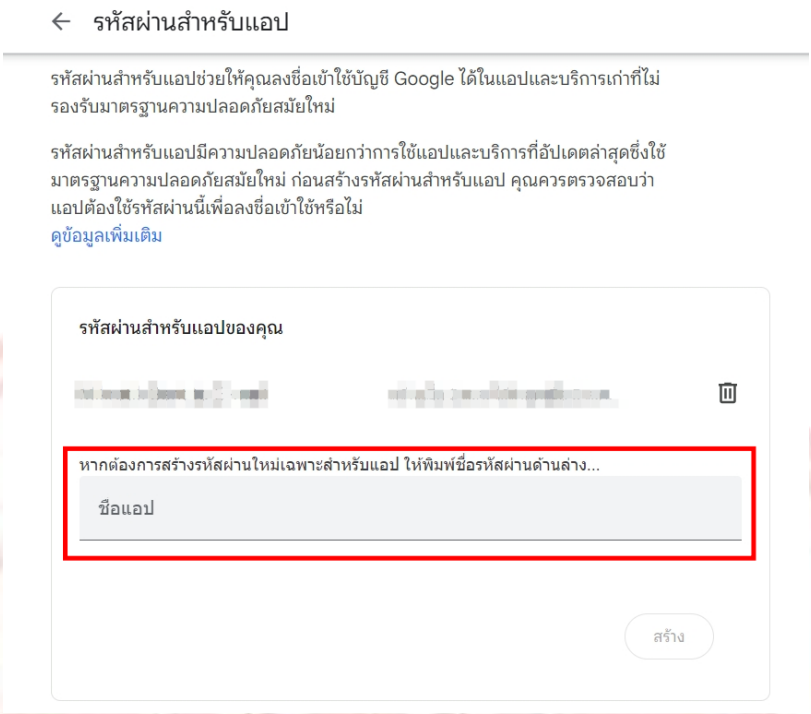
2.8.2 การตั้งค่ายืนยันตัวตน 2 ขั้นตอน หลังจากเข้าที่การยืนยันตัวตน 2 ขั้นตอน ให้เข้าไปที่รหัสผ่านสำหรับแอปแสดงดังภาพที่ 2-54 ทาง Google จะให้ยืนยันตัวตน โดยการกรอก Password ของ E-mail ที่ต้องการสร้าง app passwords แสดงดังภาพที่ 2-55 จากนั้นให้ตั้งชื่อแอป เพื่อนำรหัสผ่านไปใช้กับแอปที่ต้องการแสดงดังภาพที่ 2-56 ระบบจะสร้างรหัสผ่านแสดงผ่านแสดงดังภาพที่ 2-57 ให้นำรหัสผ่านที่ได้ไปตั้งค่าในอุปกรณ์ MikroTik ซึ่งจะอธิบายในข้อ 2.9



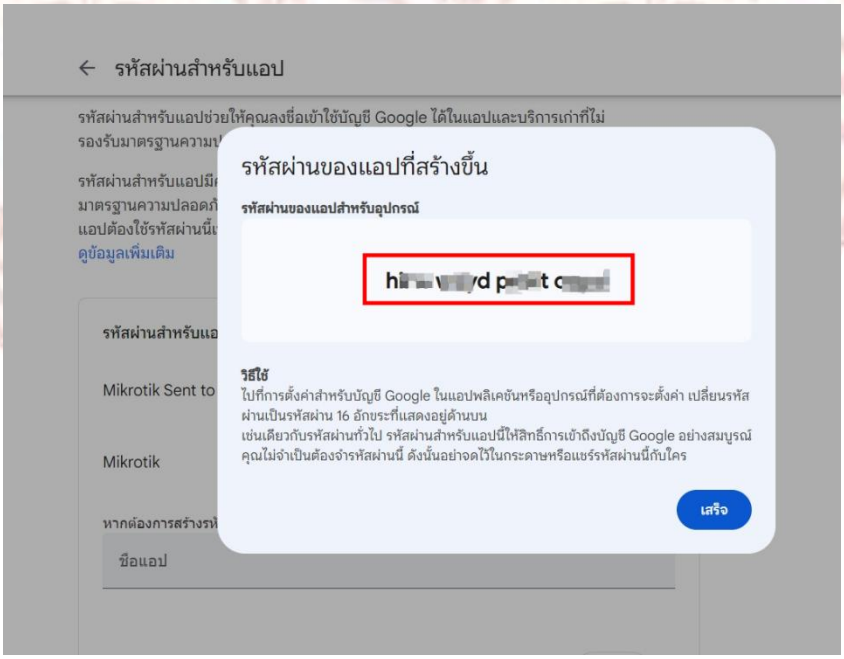
ภาพที่ 2-54 รหัสผ่านสำหรับแอป



ภาพที่ 2-55 ยืนยันตัวตน โดยการกรอก Password



ภาพที่ 2-56 ตั้งชื่อแอป

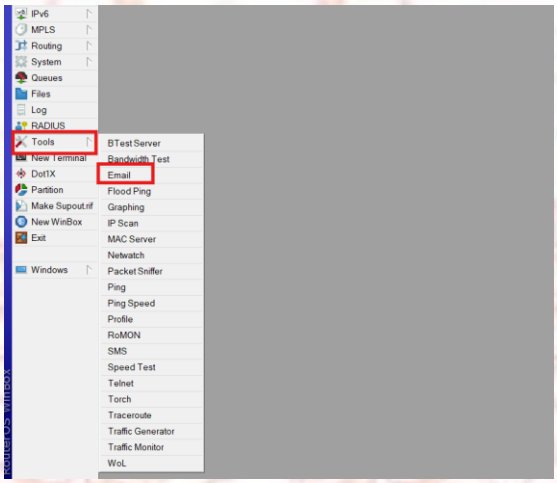


ภาพที่ 2-57 ระบบจะสร้างรหัสผ่านแสดงผ่าน

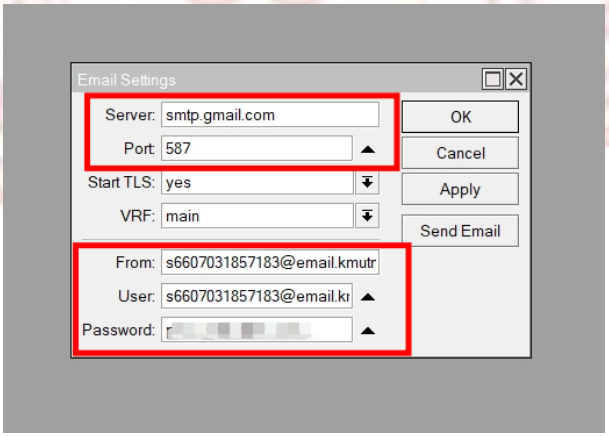
2.9 การตั้งค่า Sent Logging to Email Hotspot Report MikroTik

การตั้งค่าเพื่อให้อุปกรณ์ MikroTik ส่ง Logging Hotspot Report เข้า E-mail เมื่อมีผู้ใช้งาน Hotspot ผ่าน Wi-Fi ของอุปกรณ์ MikroTIk

2.9.1 การตั้งค่า E-mail ไปที่ Tools เลือก E-mail แสดงดังภาพที่ 2-58 จากนั้นนำ Server และ Port ของ gmail มาใส่รวมถึงใส่ E-mail ที่ช่อง From User และในส่วนของ Password จากข้อ 2.8.2 ในใส่เพื่อให้สามารถส่ง E-mail ได้แสดงดังภาพที่ 2-59

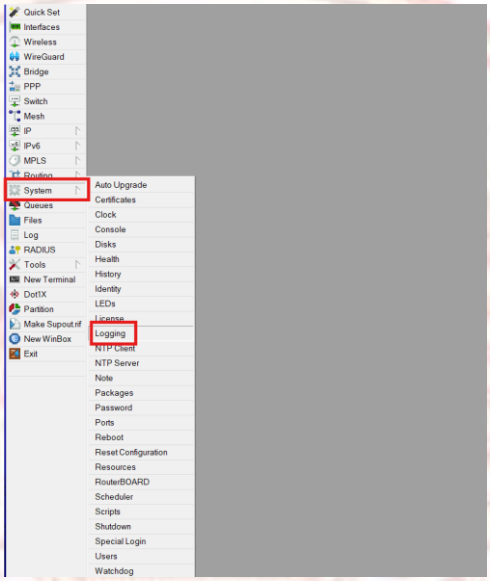


ภาพที่ 2-58 การตั้งค่า E-mail ไปที่ Tools เลือก E-mail

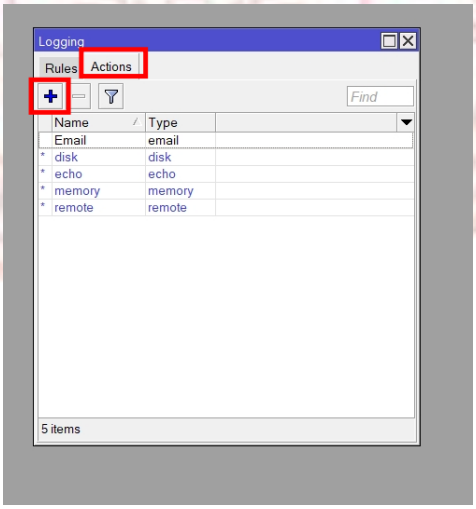


ภาพที่ 2-59 กรอกข้อมูล Server และ E-mail

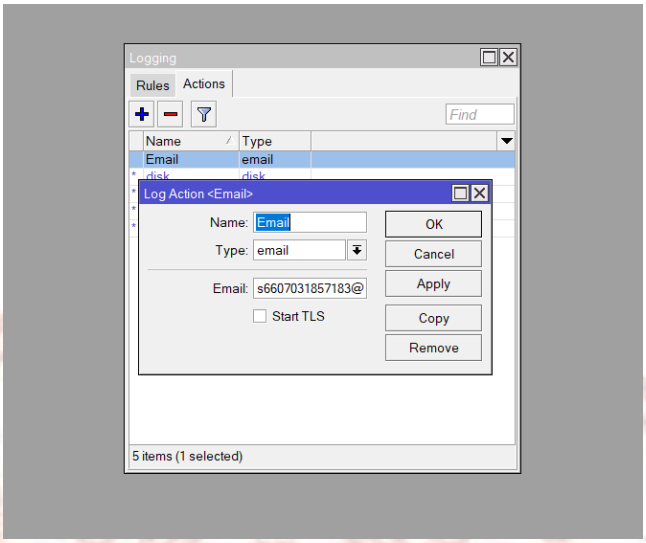
2.9.2 ตั้งค่า Logging Actions บนอุปกรณ์ MikroTik การตั้งค่าเพื่อส่ง Logging เข้า System เลือก Logging แสดงดังภาพที่ 2-60 จากนั้นเลือก Actions กดปุ่มบวกเพื่อสร้าง Log Action แสดงดังภาพที่ 2-61 ในที่นี้สร้าง E-mail ให้ตั้งชื่อ (Name) เลือกประเภท (Type) และกรอกที่อยู่ E-mail ที่ต้องการแสดงดังภาพที่ 2-62



ภาพที่ 2-60 การตั้งค่าเพื่อส่ง Logging

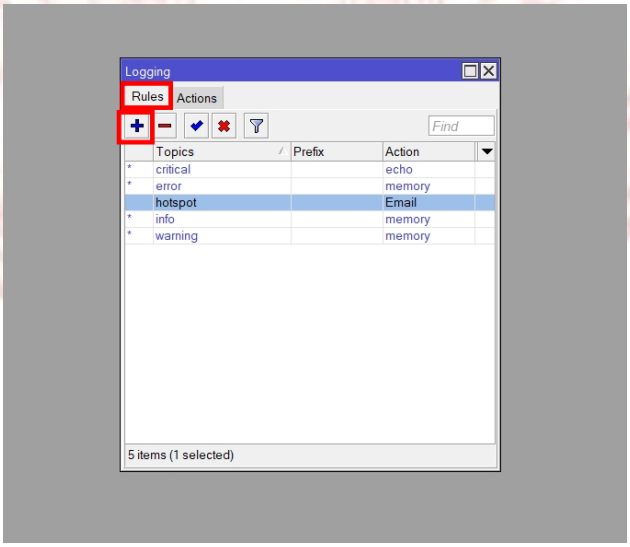


ภาพที่ 2-61 การตั้งค่าสร้าง Log Action

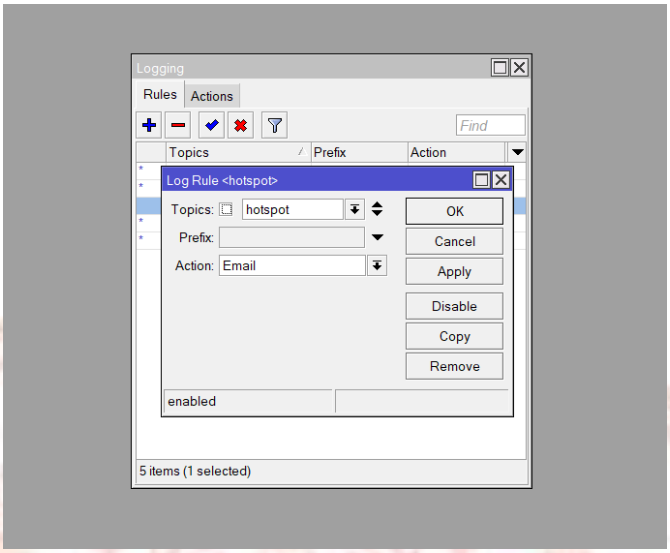


ภาพที่ 2-62 กรอกรายละเอียดการตั้งค่า

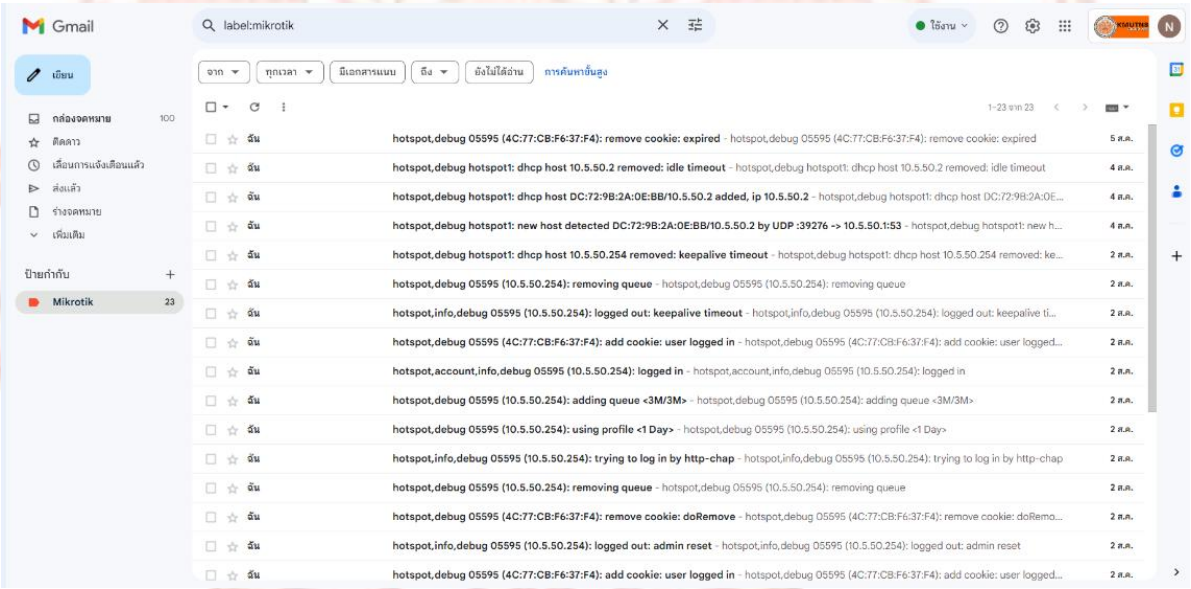
2.9.2 ตั้งค่า Logging Rules บนอุปกรณ์ MikroTik การตั้งค่าเพื่อกำหนด Logging Rules ไปที่ Rules จากนั้นกดปุ่มบวก แสดงดังภาพที่ 2-63 จากนั้นเลือก Topics เป็น Hotspot และ Action เป็น Email ตามที่สร้างไว้ในข้อ 2.8.1 แสดงดังภาพที่ 2-64 เมื่อมีการเชื่อมต่อเข้าใช้งาน Hotspot Log จะถูกส่งเข้า E-mail โดยอัตโนมัติแสดงดังภาพที่ 2-65



ภาพที่ 2-63 การตั้งค่าเพื่อกำหนด Logging Rules



ภาพที่ 2-64 สร้าง Log Rule



ภาพที่ 2-65 Log เมื่อส่งเข้า E-mail

2.10 สรุป

จากข้อมูลข้างต้นที่กล่าวมาในบทที่ 2 เป็นการนำเสนอการตั้งค่าอุปกรณ์ ทฤษฎี และงานวิจัยที่เกี่ยวข้อง ทั้งนี้ผู้วิจัยจะนำเสนอกระบวนการวิธีการดำเนินการวิจัยในบทที่ 3 ในลำดับต่อไป

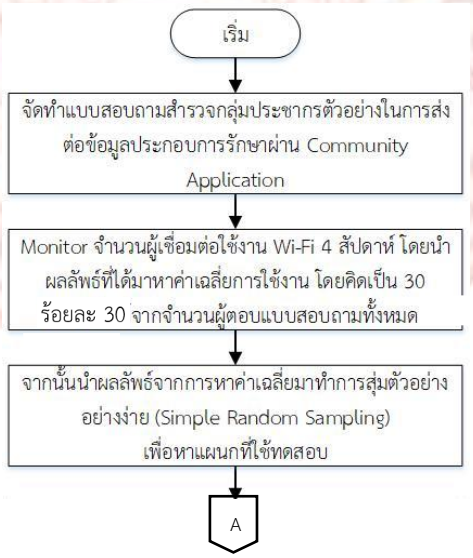
บทที่ 3

วิธีดำเนินงานวิจัย

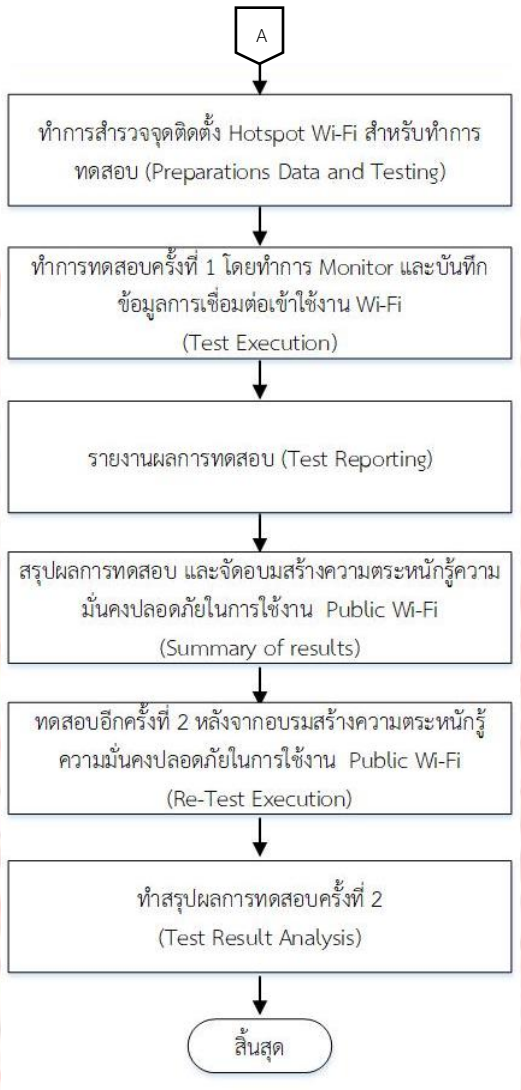
การค้นคว้าอิสระนี้ได้รับการอนุมัติการเข้าถึงข้อมูลเบื้องต้น โดยไม่มีการระเมิดกฎหมาย PDPA ของผู้ป่วย หรือบุคลากรแต่อย่างใด มีวิธีการดำเนินการวิจัยที่มุ่งเน้นการเสริมสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ โดยใช้การจำลองการโจมตีทางไซเบอร์รูปแบบหนึ่ง คือ อีวิล ทวิน ทางผู้วิจัยได้ดำเนินการจำลองการทดสอบด้วยอีวิล ทวิน ในโรงพยาบาลแห่งหนึ่ง ซึ่งในการทดสอบดังกล่าว ผู้ทดสอบได้ดำเนินการทดสอบในรูปแบบที่เรียกว่า ไซเบอร์ดริลล์ (Cyber Drill) โดยใช้เทคนิคการจำลองการโจมตีด้วยอีวิล ทวิน ซึ่งแบ่งการจำลองการทดสอบ ออกเป็น 2 ครั้ง โดยหลังจากทดสอบครั้งที่ 1 จะจัดให้มีกิจกรรม และกระบวนการส่งเสริมความตระหนักรู้เกี่ยวกับภัยคุกคามทางด้านไซเบอร์หลังจากอบรม จัดให้ทำแบบทดสอบวัดผลประเมินความเข้าใจ และรวบรวมข้อมูลการจำลองการทดสอบครั้งที่ 1 เรียบร้อยแล้ว จะดำเนินการทดสอบครั้งที่ 2 เพื่อคาดหวัง และประเมินผลลัพธ์ที่ดีขึ้นจากการทดสอบครั้งที่ 1 ซึ่งจากที่กล่าวมาข้างต้นทางผู้วิจัยมีวิธีการดำเนินการวิจัยดังภาพที่ 3-1และภาพที่ 3-2

3.1 ขั้นตอนกระบวนการดำเนินงาน (Process Diagram)

แสดงดังภาพที่ 3-1 และภาพที่ 3-2



ภาพที่ 3-1 ขั้นตอนกระบวนการดำเนินงาน (Process Diagram) ส่วนที่ 1



ภาพที่ 3-2 ขั้นตอนกระบวนการดำเนินงาน (Process Diagram) ส่วนที่ 2

จากภาพที่ 3-1 และภาพที่ 3-2 วิธีการดำเนินงานวิจัยในแต่ละขั้นตอนดังต่อไปนี้

3.2 จัดทำแบบสอบถามการส่งต่อข้อมูลประกอบการรักษาคนไข้ผ่าน Community Application

นำส่งแบบสอบถามให้กลุ่มประชากรตัวอย่างที่ทางผู้วิจัยจะทำการทดสอบ โดยจัดทำแบบสอบถามเพื่อให้สามารถกำหนดกลุ่มประชากรที่ใช้ในการทดสอบในการส่งต่อข้อมูลประกอบการรักษาคนไข้ผ่านทาง Community Application โดย Community Application ที่ทางผู้วิจัย

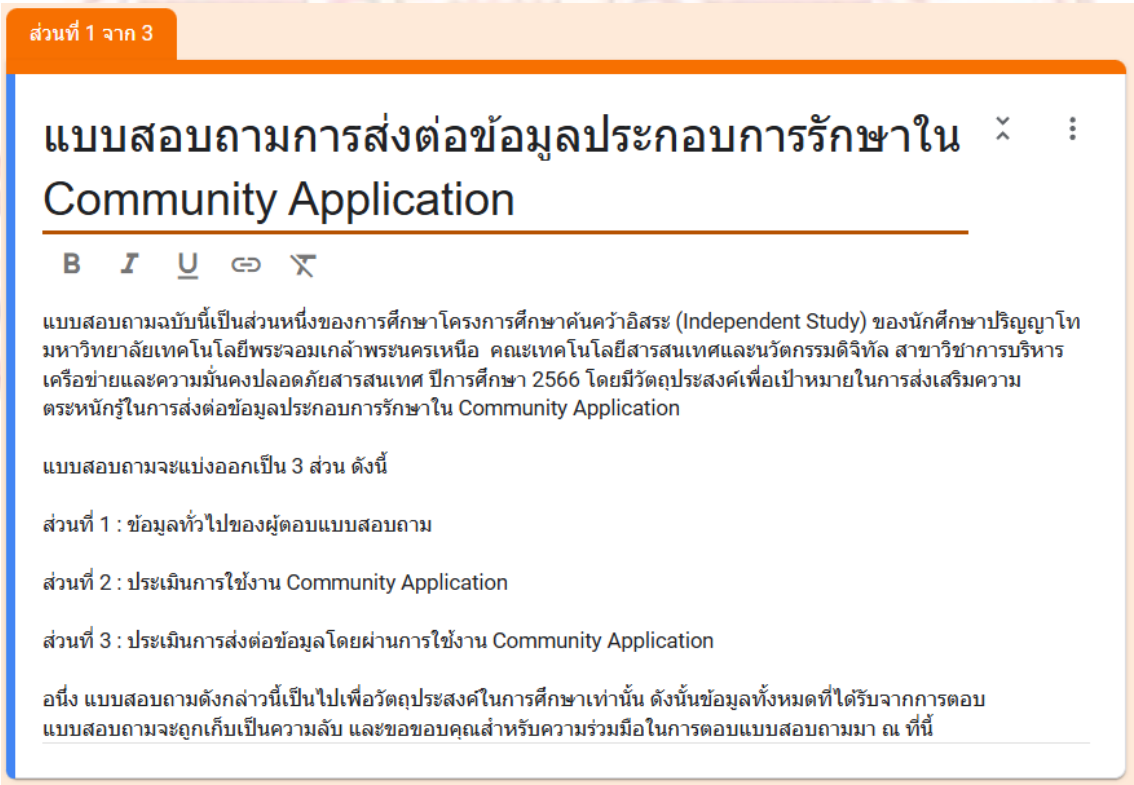
นำมาใช้ในแบบสอบถามนี้ ประกอบด้วย Line, Messenger, Google Chat, WeChat, WhatsApp และอื่นๆ โปดระบุเพิ่มเติม ซึ่งแบบสอบถามแบ่งออกเป็น 3 ส่วน

ส่วนที่ 1 : ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ส่วนที่ 2 : ประเมินการใช้งาน Community Application

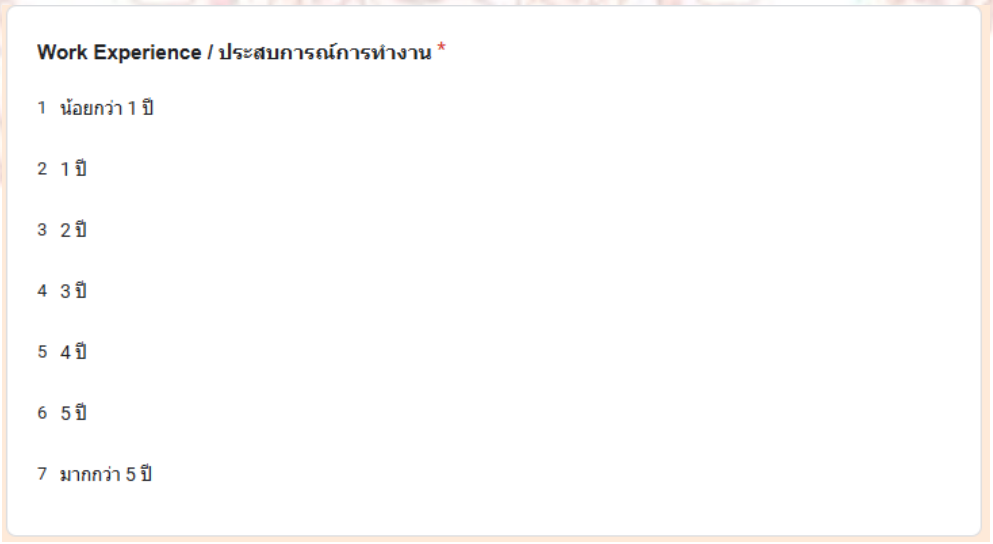
ส่วนที่ 3 : ประเมินการส่งต่อข้อมูลโดยผ่านการใช้งาน Community Application

3.2.1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ได้แก่ หัวข้อแบบสอบถาม ชี้แจงรายละเอียดของแบบสอบถามแต่ละส่วนพร้อมแจ้งให้ทราบถึงจุดประสงค์ของการตอบแบบสอบถามให้งานวิจัย แบบสอบถามการส่งต่อข้อมูลประกอบการรักษาผ่าน Community Application นั้นในส่วนของข้อมูลทั่วไปของผู้ตอบแบบสอบถามจะประกอบไปด้วย แผนกทั้ง 16 แผนก และประสบการณ์การทำงาน 1-5 ปี และมากกว่า 5 ปีขึ้นไป โดยแบบสอบถามการส่งต่อข้อมูลประกอบการรักษาผ่าน Community Application แสดงดังภาพที่ 3-3 ภาพที่ 3-4 และภาพที่ 3-5 ตามลำดับ



ภาพที่ 3-3 รายละเอียดของแบบสอบถามแต่ละส่วน

ภาพที่ 3-4 Department / แผนก



ภาพที่ 3-5 Work Experience / ประสบการณ์การทำงาน

3.2.2 ประเมินการใช้งาน Community Application จำนวน 5 Application ได้แก่ Line, Google Chat, WhatsApp, Messenger, WeChat และอื่นๆ โปรดระบุ เพิ่มเติมนอกเหนือจากที่กำหนดไว้ โดยมีหลักเกณฑ์การประเมินการใช้งาน Community Application ดังนี้

1 คะแนน หมายถึง น้อยที่สุด

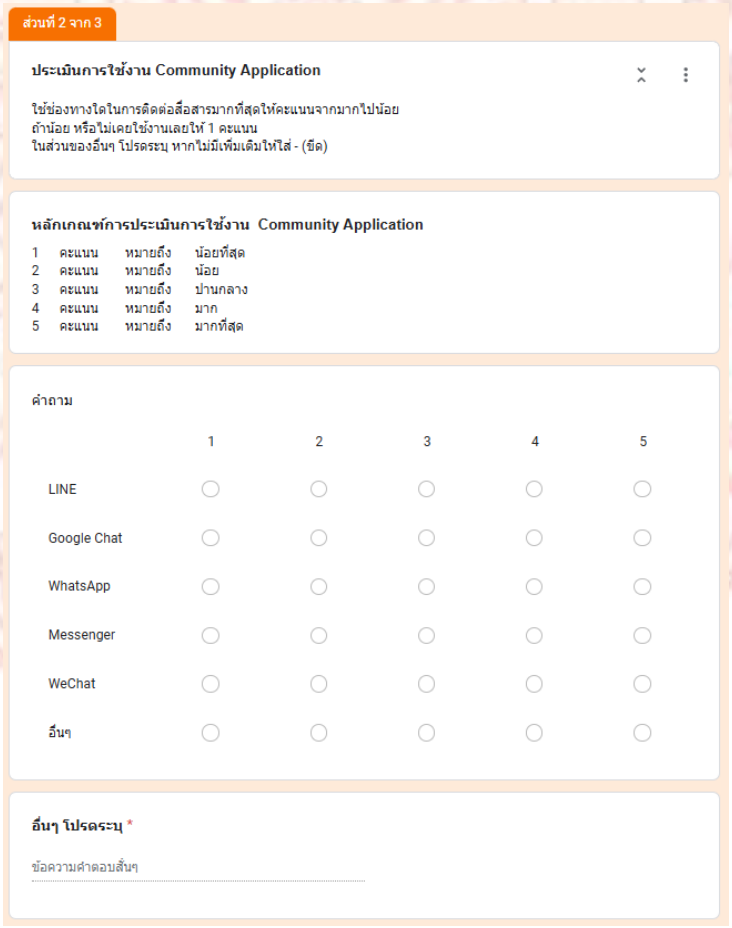
2 คะแนน หมายถึง น้อย

3 คะแนน หมายถึง ปานกลาง

4 คะแนน หมายถึง มาก

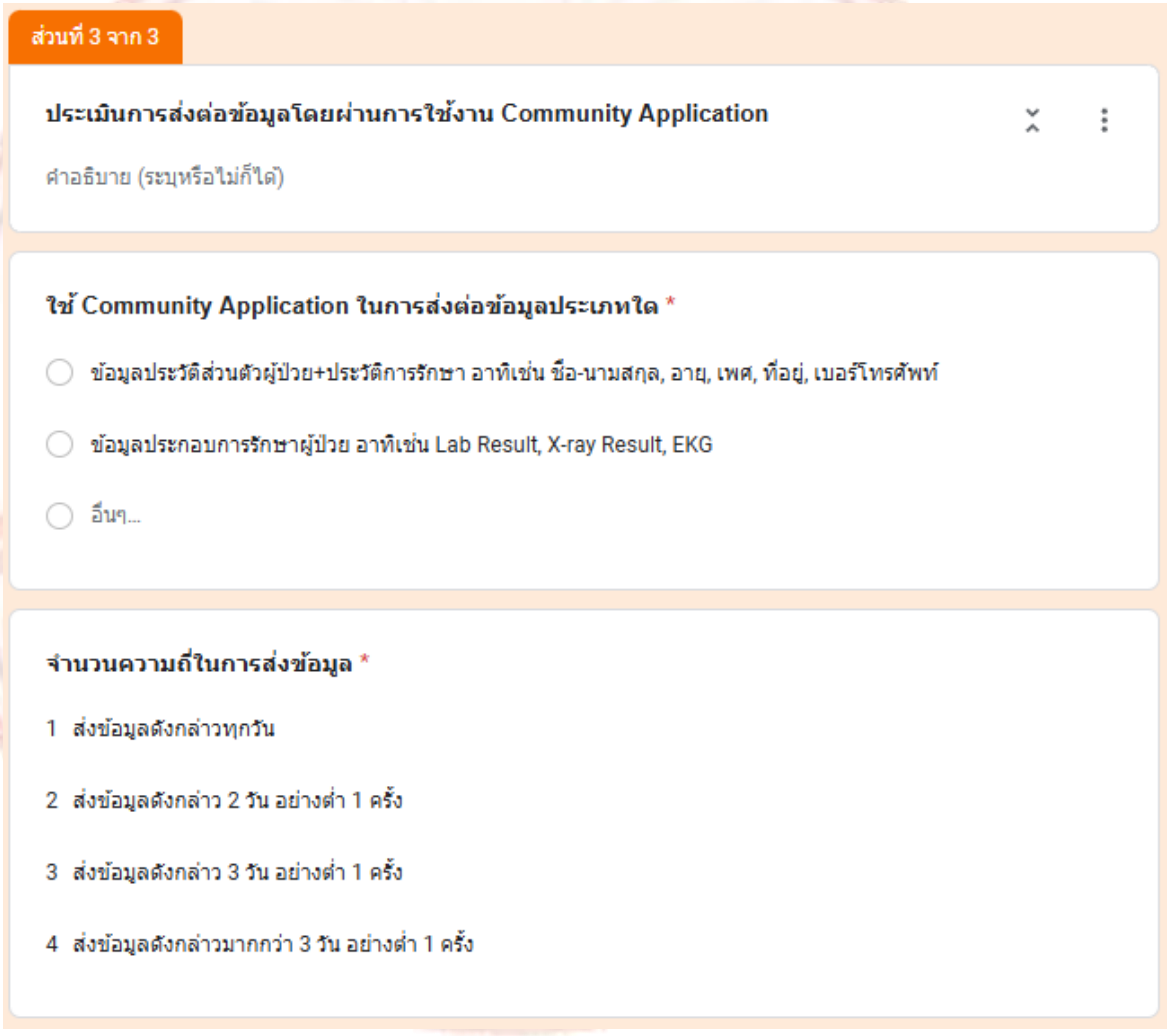
5 คะแนน หมายถึง มากที่สุด

ซึ่งคะแนนบอกถึงการใช้งานจากมากที่สุดไปน้อยที่สุด ใช้คะแนนในการบอกปริมาณการใช้งาน โดยรายละเอียดแสดงดังภาพที่ 3-6



ภาพที่ 3-6 ประเมินการใช้งาน Community Application

3.2.3 ประเมินการส่งต่อข้อมูลโดยผ่านการใช้งาน Community Application แบ่งประเภทของข้อมูลที่ส่งต่อ ได้แก่ ข้อมูลประวัติส่วนตัวผู้ป่วย+ประวัติการรักษา อาทิเช่น ชื่อ-นามสกุล อายุ เพศ ที่อยู่ เบอร์โทรศัพท์ ข้อมูลประกอบการรักษาผู้ป่วย อาทิเช่น Lab Result, X-ray Result, EKG และ อื่นๆ โปรดระบุ จำนวนความถี่ในการส่งต่อข้อมูล แบ่งเป็น 4 ระดับ ได้แก่ ส่งข้อมูลดังกล่าวทุกวัน ส่งข้อมูลดังกล่าว 2 วัน อย่างต่ำ 1 ครั้ง ส่งข้อมูลดังกล่าว 3 วัน อย่างต่ำ 1 ครั้ง และส่งข้อมูลดังกล่าวมากกว่า 3 วัน อย่างต่ำ 1 ครั้ง แสดงดังภาพที่ 3-7



ภาพที่ 3-7 ประเมินการส่งต่อข้อมูลโดยผ่านการใช้งาน Community Application

3.2.4 สรุปผลการตอบแบบสอบถามเพื่อประเมินการส่งต่อข้อมูลโดยผ่านการใช้งาน Community Application ของทางโรงพยาบาล ซึ่งมีแผนกร่วมตอบแบบสอบถามทั้งหมด 13 แผนก จากทั้ง 16 แผนก ตามรายละเอียดส่วนที่ 1 ของแบบสอบถามการส่งต่อข้อมูลประกอบการรักษาผ่าน Community Application โดยได้ข้อมูลแสดงดังตารางที่ 3-1

ตารางที่ 3-1 จำนวนผู้ตอบแบบสอบถาม

ลำดับ	แผนก	จำนวนผู้ตอบแบบสอบถามแต่ละแผนก
1	OPD Nurse/PN/NA	25
2	IPD Nurse/PN/NA	22
3	Registration	7
4	IT	4
5	Radiology	4
6	OR/LR Nurse	3
7	Admission	2
8	Cashier	1
9	Doctor	1
10	ER Nurse	1
11	Laboratory	1
12	Physical therapy	1
13	UR Nurse	1
	รวม	73

จากตารางที่ 3-1 พบว่า ผู้ตอบแบบสอบถามการส่งต่อข้อมูลประกอบการรักษาผ่าน Community Application ทั้งหมด 13 แผนก คิดเป็นจำนวนผู้ตอบแบบสอบถามการส่งต่อข้อมูลประกอบการรักษาผ่าน Community Application ทั้งหมด 73 คน ทางผู้วิจัยจึงขอใช้จำนวนทั้งหมดจากผู้ตอบแบบสอบถามการส่งต่อข้อมูลประกอบการรักษาผ่าน Community Application ในการนำมาวิเคราะห์เพื่อหาแผนกสำหรับติดตั้งจุดกระจายสัญญาณ Wi-Fi สำหรับหาบุคลากรผู้เข้าข่ายตกเป็นเหยื่อของอีวิล ทวิน ในลำดับต่อไป

ตารางที่ 3-2 จำนวนการใช้งาน Community Application

ลำดับ	แผนก	Google Chat	LINE	Messenger	WeChat	WhatsApp	อื่นๆ
1	OPD Nurse/PN/NA	67	99	65	52	55	63
2	IPD Nurse/PN/NA	51	79	47	38	41	36
3	Registration	19	31	25	15	16	19
4	IT	16	18	11	4	4	5
5	Radiology	11	17	13	7	7	4
6	OR/LR Nurse	7	14	7	7	7	3
7	Admission	4	8	6	2	2	3
8	Cashier	3	5	3	3	3	3
9	Doctor	2	5	4	1	1	1
10	ER Nurse	1	5	1	1	1	1
11	Laboratory	3	4	5	2	1	1
12	Physical therapy	1	5	1	1	1	1
13	UR Nurse	5	5	1	1	1	1
	รวม	190	295	189	134	140	141

จากตารางที่ 3-2 จะเห็นได้ว่า Community Application ที่นิยมใช้งานจำนวนมากในการส่งต่อข้อมูล คือ LINE รองลงมาเป็น Google Chat และ Community Application อื่นๆ ตามลำดับ จะเห็นได้ว่า Community Application มีบทบาท และเป็นเครื่องมือใช้สำหรับการส่งต่อข้อมูลเพื่อติดต่อสื่อสาร

ตารางที่ 3-3 การใช้งาน Community Application ส่งต่อข้อมูลประเภทใด

ลำดับ	ประเภทของข้อมูล	จำนวน
1	ข้อมูลประวัติส่วนตัวผู้ป่วย+ประวัติการรักษา	35
2	ข้อมูลประกอบการรักษาผู้ป่วย	28
3	อื่นๆ	10
	รวม	73

จากตารางที่ 3-3 จะเห็นได้ว่า การส่งต่อข้อมูลผ่าน Community Application จะส่งต่อข้อมูลประวัติส่วนตัวผู้ป่วย+ประวัติการรักษา และข้อมูลประกอบการรักษาผู้ป่วย เป็นจำนวนมากซึ่งข้อมูลที่ใช้ส่งต่อใน Community Application เกี่ยวข้องกับผู้ป่วยมากที่สุด

ตารางที่ 3-4 จำนวนความถี่ในการส่งต่อข้อมูลจากการใช้งาน Community Application

ลำดับ	ความถี่ในการส่งข้อมูล	จำนวน
1	ส่งข้อมูลดังกล่าวทุกวัน	38
2	ส่งข้อมูลดังกล่าว 2 วัน อย่างต่ำ 1 ครั้ง	11
3	ส่งข้อมูลดังกล่าว 3 วัน อย่างต่ำ 1 ครั้ง	18
4	ส่งข้อมูลดังกล่าวมากกว่า 3 วัน อย่างต่ำ 1 ครั้ง	6
	รวม	73

จากตารางที่ 3-4 จะเห็นได้ว่า การส่งต่อข้อมูลผ่าน Community Application จะส่งต่อข้อมูลดังกล่าวทุกวันเป็นจำนวนมาก จากจำนวนของผู้ตอบแบบสอบถามทั้งหมด

3.3 ดำเนินการตรวจเช็คเฝ้าระวัง (Monitor) การใช้งาน Wi-Fi

ในระหว่างเก็บรวบรวมผลจากการตอบแบบสอบถาม ทางผู้วิจัยได้ดำเนินการ Monitor การใช้งาน Wi-Fi ในปัจจุบันของบุคลากรภายในองค์กร โดยจะทำการบันทึกจำนวนผู้เชื่อมต่อ Wi-Fi เป็นระยะ 4 สัปดาห์ เพื่อหาค่าเฉลี่ยของผู้เชื่อมต่อทั้งหมด

ตารางที่ 3-5 จำนวนผู้เชื่อมต่อเข้าใช้งาน Wi-Fi ระยะเวลา 4 สัปดาห์

สัปดาห์ที่	จำนวนผู้เชื่อมต่อ
1	161
2	175
3	160
4	177

จากนั้นทางผู้วิจัยจะนำค่าเฉลี่ยที่ได้มาคำนวณเพื่อใช้วิธีการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) จากจำนวนผู้ตอบแบบสอบถามทั้งหมดจากข้อ 3.1 หาค่าเฉลี่ยการ Monitor ใช้งาน Wi-Fi จำนวน 4 สัปดาห์ คิดเป็นร้อยละ 30 ของ 168.25 เท่ากับ 50.475 คิดเป็นจำนวน 50 คน ของผู้ตอบแบบสอบถาม เมื่อได้จำนวนจากการสุ่มแล้วจะได้แผนกที่เป็นกลุ่มเป้าหมายซึ่งทั้ง 2 กลุ่มนี้เป็นการสุ่มตัวอย่างอย่างง่าย (Random Selection) สำหรับทำการทดสอบการครั้งที่ 1 และครั้งที่ 2 ตามลำดับ

3.4 ดำเนินการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling)

เมื่อได้จำนวนผลการตอบแบบสอบถามที่ 50 คน นำมาสุ่มด้วยทฤษฎีการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) จากผู้ตอบแบบสอบถามทั้งหมด 73 คน จะได้แผนกที่ใช้ในการทดสอบจุดติดตั้ง Wi-Fi ในครั้งที่ 1 และครั้งที่ 2 ตามลำดับ ซึ่งกระบวนการ และวิธีการที่ใช้แสดงในบทที่ 2 ข้อ 2.3 การเขียนคำสั่งการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) ด้วยภาษา Python บน Visual Studio Code

ตารางที่ 3-6 จำนวนผู้ตอบแบบสอบถามจากการสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) 50 คน

ลำดับ	แผนก	จำนวนผู้ตอบแบบสอบถามแต่ละแผนก
1	OPD Nurse/PN/NA	16
2	IPD Nurse/PN/NA	15
3	Registration	5
4	IT	3
5	Radiology	2
6	OR/LR Nurse	3
7	Admission	2
8	Cashier	1
9	Doctor	1
10	ER Nurse	1
11	UR Nurse	1
	รวม	50

จากตารางที่ 3-6 จะได้แผนกที่ตอบแบบสอบถาม และมีการส่งต่อข้อมูลมากที่สุด คือ Nurse OPD และ Nurse IPD ตามลำดับ ทางผู้วิจัยจึงใช้ทั้ง 2 แผนกข้างต้น ในการทดสอบการจำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน

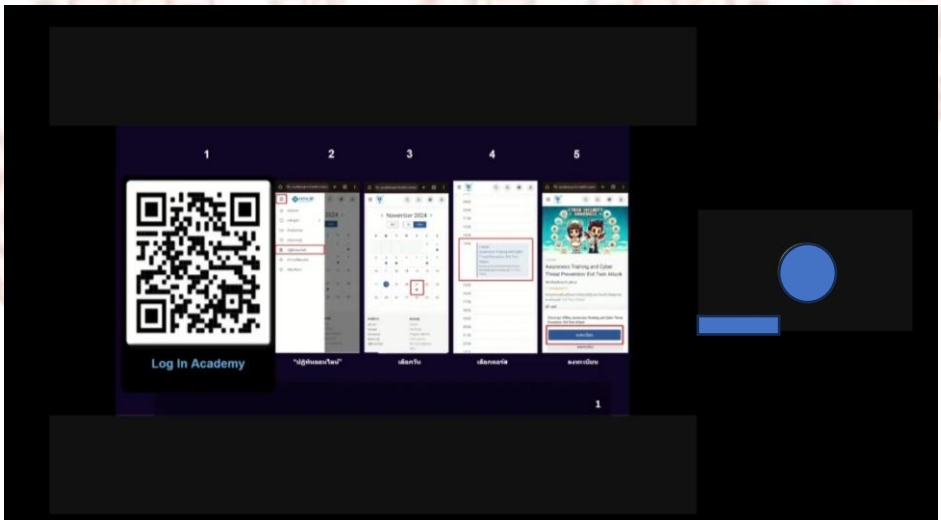
3.5 การจำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน ครั้งที่ 1

ทางผู้วิจัยได้ดำเนินการสร้าง SSID Wi-Fi จำลองซึ่งมีลักษณะคล้ายกับ SSID Wi-Fi จริงขององค์กร เมื่อใดผู้เชื่อมต่อภายในองค์กร Log in สมบูรณ์โดยผ่านหน้า Log in Hotspot จะถือว่าเข้าข่ายตกเป็นเหยื่อของอีวิล ทวิน โดยจำนวนกลุ่มเป้าหมาย Nurse OPD และ Nurse IPD จากผู้ตอบแบบทดสอบทั้งหมด จำนวน 47 คน ซึ่งมีทั้งพนักงานหญิง และชาย ที่มีอายุระหว่าง 22-55 ปี จากนั้นจึงนำผลการศึกษาที่ได้ ไปวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่อของอีวิล ทวิน ตามเกณฑ์ และสรุปผลการทดสอบครั้งที่ 1 พบว่ากลุ่มเป้าหมายทั้ง 2 กลุ่มมีการเชื่อมต่อใช้งานเป็นจำนวนมาก และมีความตระหนักถึงการใช้งาน Wi-Fi ที่ค่อนข้างน้อยมาก

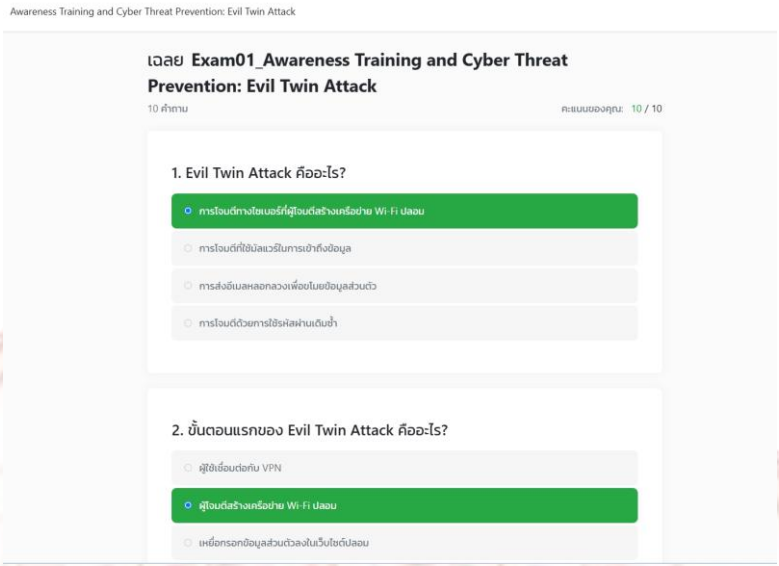
3.6 ดำเนินการส่งเสริมความตระหนักรู้ให้เท่าทันภัยคุกคามทางด้านไซเบอร์

กลุ่มเป้าหมายได้แก่บุคลากรสายสุขภาพที่เข้าข่ายตกเป็นเหยื่อของอีวิล ทวิน ตามเกณฑ์ ซึ่งประกอบด้วย

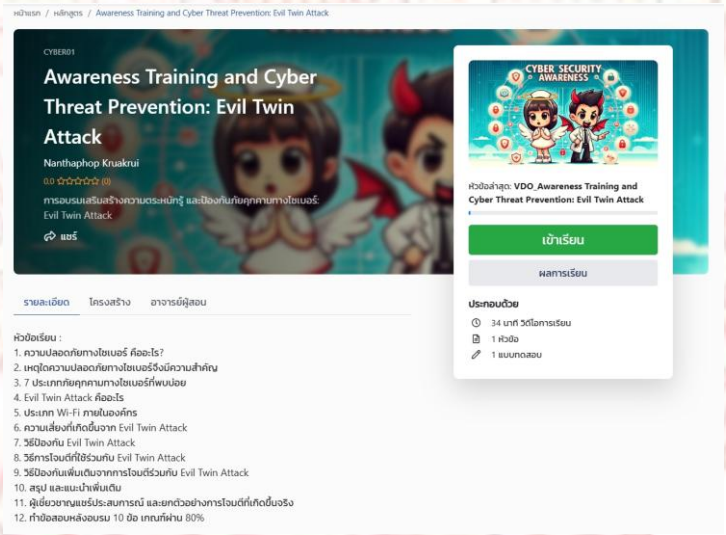
3.6.1 การจัดกิจกรรมส่งเสริมความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ซึ่งมีกิจกรรมหลายอย่าง เช่น การสื่อสารให้ความรู้กับพนักงานผ่าน Line, อีเมล์ขององค์กร และการจัดอบรมให้ความรู้ต่อภัยคุกคามทางไซเบอร์ที่พบบ่อย รวมถึงมุ่งเน้นในส่วนของการโจมตีทางไซเบอร์ด้วยอีวิล ทวิน วิธีการทำงานของ อีวิล ทวิน, ประเภท Wi-Fi ภายในองค์กร, ความเสี่ยงที่เกิดขึ้นจาก อีวิล ทวิน, วิธีป้องกัน อีวิล ทวิน, วิธีการโจมตีที่ใช้ร่วมกับอีวิล ทวิน และวิธีป้องกันเพิ่มเติมจากการโจมตีร่วมกับอีวิล ทวิน, ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจริงจากประสบการณ์ของผู้เชี่ยวชาญตามภาพที่ 3-8 ทำแบบทดสอบหลังจากอบรบส่งเสริมความตระหนักรู้ตามภาพที่ 3-9 และสามารถเรียนออนไลน์ย้อนหลังได้ตามภาพที่ 3-10 ซึ่งมีกิจกรรมหลายอย่าง เช่น การสื่อสารให้ความรู้กับพนักงานผ่าน Line, อีเมล์ขององค์กร และการจัดอบรมให้ความรู้ต่อภัยคุกคามทางไซเบอร์ด้วยการโจมตีอีวิล ทวิน และในหัวข้อภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจริงจากประสบการณ์ของผู้เชี่ยวชาญ และเปิดโอกาสให้บุคลากรภายในองค์กรสายสุขภาพซักถามข้อสงสัยกับผู้เชี่ยวชาญได้อย่างใกล้ชิด ทำแบบทดสอบวัดผลหลังจากอบรบส่งเสริมความตระหนักรู้ และทำแบบสอบถามประเมินความเข้าใจหลังจากอบรมเสริมสร้างความตระหนักรู้ต่อภัยคุกคาทางไซเบอร์



ภาพที่ 3-8 การจัดอบรมให้ความรู้ต่อภัยคุกคามทางไซเบอร์



ภาพที่ 3-9 แบบทดสอบส่งเสริมความตระหนักรู้



ภาพที่ 3-10 เรียนออนไลน์ย้อนหลัง

3.7 การจำลอง SSID Wi-Fi เพื่อวิเคราะห์หาบุคลากรที่เข้าข่ายตกเป็นเหยื่ออีวิล ทวิน ครั้งที่ 2

ใช้หลักการ และกลุ่มประชากรเดียวกันกับการทดสอบครั้งที่ 1 ซึ่งทางผู้วิจัยคาดหวังให้ผลการศึกษาวิเคราะห์มีผลที่ดีกว่าการจำลองทดสอบในครั้งที่ 1 คือ กลุ่มประชากรต้องใช้งานเฉพาะ Wi-Fi ที่องค์กรจัดไว้ให้ใช้งาน และในส่วนของอีวิล ทวินต้องมีการเชื่อมต่อเข้าใช้งาน Wi-Fi น้อยลงหรือไม่มีการเชื่อมต่อเข้าใช้งาน Wi-Fi อีกเลย

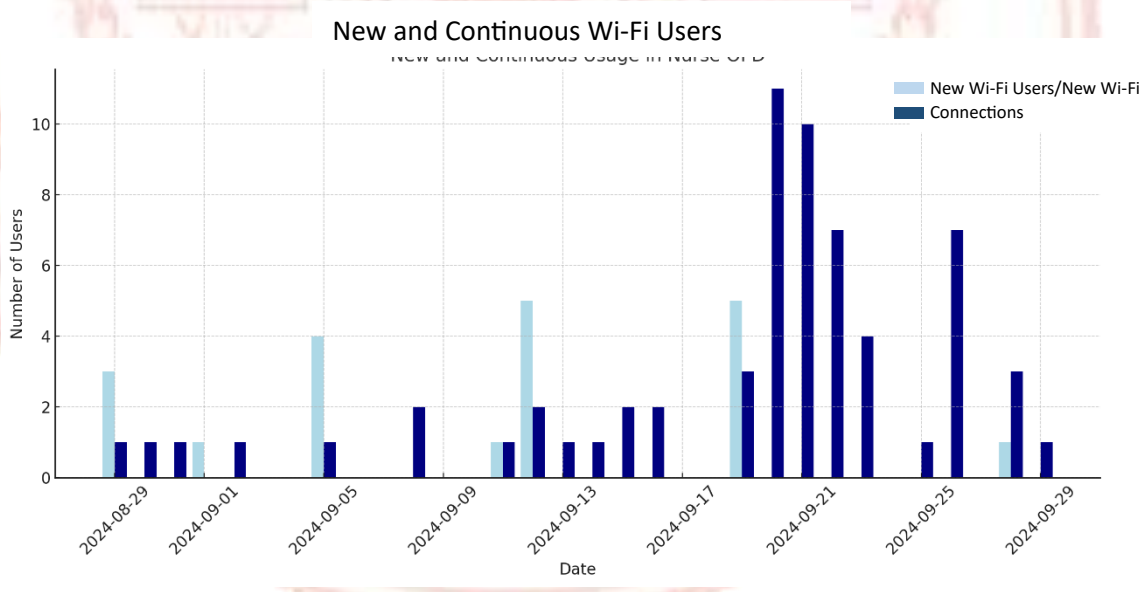
บทที่ 4

ผลการวิจัย

บทนี้จะแสดงผลลัพธ์จากการวิเคราะห์ครั้งที่ 1 และครั้งที่ 2 เปรียบเทียบก่อน และหลังการอบรบเสริมสร้างความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ ทางผู้วิจัยจะขออธิบายผลการวิจัยดังต่อไปนี้

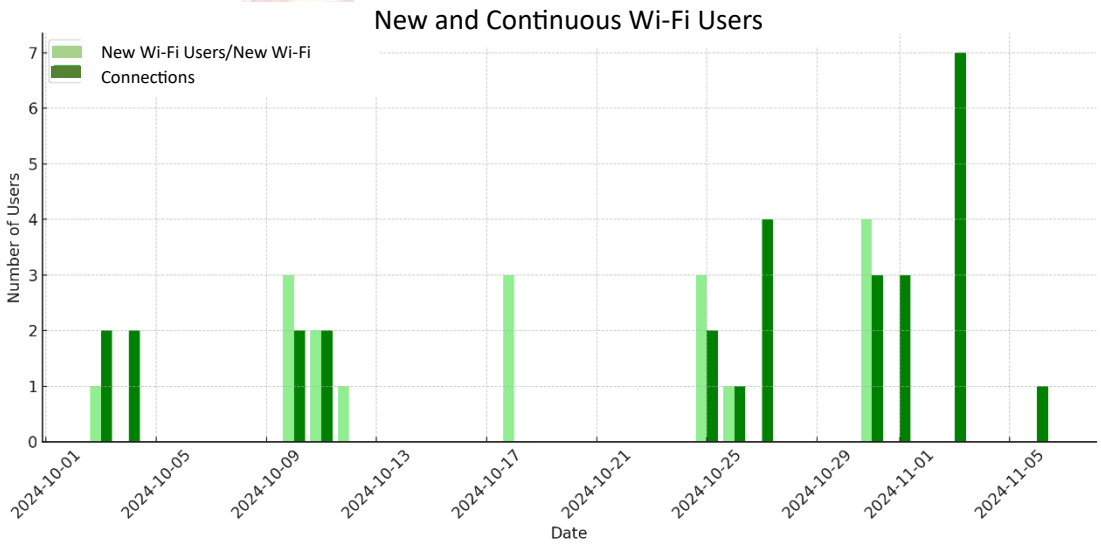
4.1 ผลลัพธ์หลังจากทดสอบครั้งที่ 1

4.1.1 ผลลัพธ์การวิเคราะห์ของ Nurse OPD จะเห็นได้ว่ามีผู้เชื่อมต่อใหม่ใช้งานอย่างต่อเนื่องสม่ำเสมอ โดยพิจารณากราฟแท่งสีฟ้าอ่อน แสดงถึงผู้เชื่อมต่อใหม่ทำการเชื่อมต่อเข้าใช้งาน Wi-Fi และสีน้ำเงินแสดงถึงผู้เชื่อมต่อ Wi-Fi ใช้งานอย่างสม่ำเสมอหลังจากทำการเชื่อมต่อใช้งาน Wi-Fi ดังภาพที่ 4-1



ภาพที่ 4-1 ผลลัพธ์การวิเคราะห์ครั้งที่ 1 ของ Nurse OPD

4.1.2 ผลลัพธ์การวิเคราะห์ของ Nurse IPD จะเห็นได้ว่ามีผู้เชื่อมต่อใหม่ใช้งานอย่างต่อเนื่องสม่ำเสมอ โดยพิจารณากราฟแท่งสีเขียวอ่อน แสดงถึงผู้เชื่อมต่อใหม่ทำการเชื่อมต่อเข้าใช้งาน Wi-Fi และสีเขียวเข้ม แสดงถึงผู้เชื่อมต่อ Wi-Fi ใช้งานอย่างสม่ำเสมอหลังจากทำการเชื่อมต่อใช้งาน Wi-Fi ดังภาพที่ 4-2



ภาพที่ 4-2 ผลลัพธ์การวิเคราะห์ครั้งที่ 1 ของ Nurse IPD

4.2 ผลลัพธ์จากการสอบวัดผลหลังการอบรมเสริมสร้างความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์

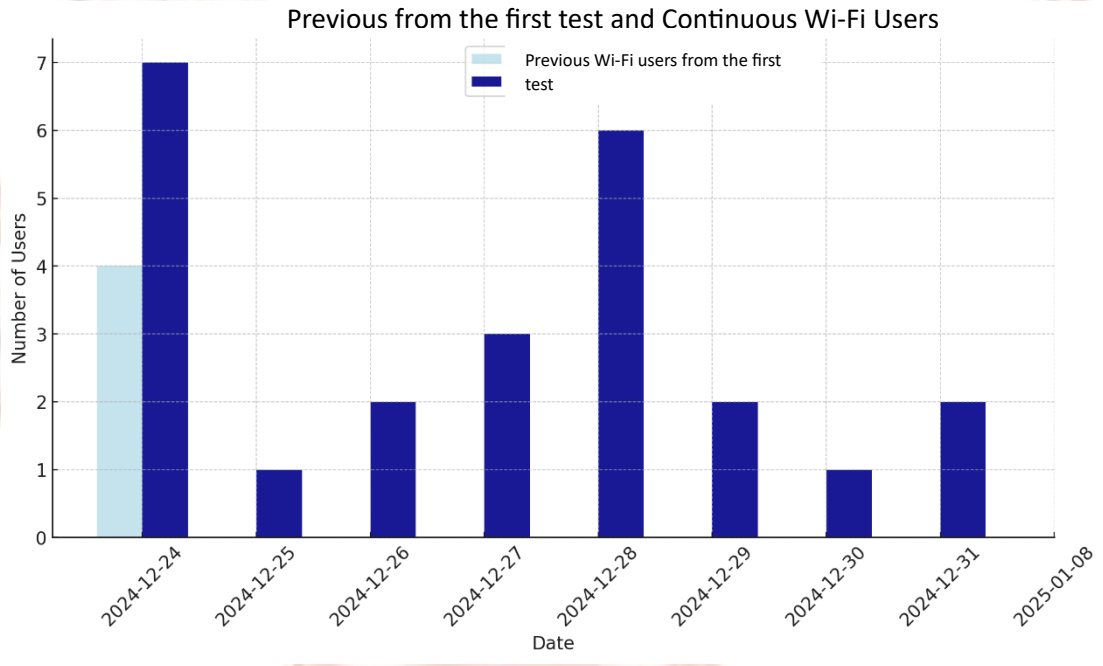
พบว่าหลังจากอบรมเสริมสร้างความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ และทำแบบทดสอบเพื่อวัดผลการอบรมจากผู้เข้าอบรมทั้งหมด 74 คน แบ่งเป็นผู้สอบผ่าน 65 คน ไม่ผ่าน 9 คน ความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ โดยหลีกเลี่ยงการส่งต่อข้อมูลประกอบการรักษาผ่านทาง Line Application และ Community Application อื่นๆ หากไม่ได้เชื่อมต่อกับเครือข่ายที่ทางองค์กรไม่ได้จัดสรรไว้ให้ใช้งาน และเครือข่ายที่ไม่ปลอดภัย หรือคาดว่ามีความเสี่ยงอย่างเด็ดขาด

4.3 ผลการตอบแบบสอบถามประเมินความตระหนักรู้หลังการจากอบรม

โดยคำถามระบุว่าท่านจะคำนึงถึงภัยคุกคามทางไซเบอร์ และหลีกเลี่ยงการส่งต่อข้อมูลประกอบการรักษาผ่านทาง Line Application ในกรณีที่ไม่ได้เชื่อมต่อ Wi-Fi ที่ปลอดภัย หรือไม่ คิดเป็นร้อยละ 85.37 ของผู้ตอบแบบสอบถามทั้งหมด

4.4 ผลลัพธ์หลังจากทดสอบครั้งที่ 2

4.4.1 ผลลัพธ์การวิเคราะห์ของ Nurse OPD จะเห็นได้ว่ามีผู้เชื่อมต่อ Wi-Fi จากการทดสอบครั้งที่ 1 ใช้งานอย่างต่อเนื่องสม่ำเสมอลดลงจากการทดสอบครั้งที่ 1 อย่างเห็นได้ชัดถึงผลลัพธ์จากการอบรม โดยสีฟ้าอ่อน แสดงถึงผู้เชื่อมต่อใช้งาน Wi-Fi เดิมจากการทดสอบครั้งที่ 1 และสีน้ำเงินแสดงถึงผู้เชื่อมต่อ Wi-Fi ใช้งานอย่างสม่ำเสมอหลังจากทำการเชื่อมต่อใช้งาน Wi-Fi ดังภาพที่ 4-3



ภาพที่ 4-3 ผลลัพธ์การวิเคราะห์ครั้งที่ 2 ของ Nurse OPD

4.4.2 ผลลัพธ์การวิเคราะห์ของ Nurse IPD พบว่าไม่มีผู้เชื่อมต่อ Wi-Fi จากการทดสอบครั้งที่ 1 เข้าเชื่อมต่อใช้งาน Wi-Fi คิดเป็นร้อยละ 100 ของ Nurse IPD ทั้งหมด ไม่มีผู้เชื่อมต่อ Wi-Fi รายเดิมเข้าข่ายตกเป็นเหยื่อ อีวิล ทวิน เลยหลังจากได้รับการอบรมเสริมสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์

บทที่ 5

สรุปผลการวิจัย และข้อจำกัด

5.1 สรุปผลการวิจัย

งานวิจัยค้นคว้าอิสระนี้ดำเนินการวิจัยเรื่อง การจำลองจุดกระจายสัญญาณไวไฟสาธารณะเพื่อประเมินความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในองค์กรสายสุขภาพ โดยวิเคราะห์ความเสี่ยงด้วยอีวิล ทวิน และการอบรมเสริมสร้างความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ นั้นมีวัตถุประสงค์หลักเพื่อที่จะช่วยลดความเสี่ยงต่อการถูกโจมตีจากภัยคุกคามทางไซเบอร์ในองค์กรสายสุขภาพ และเป็นประโยชน์ต่อองค์กรอื่นๆ หรือในลักษณะแบบเดียวกัน ทำให้เพิ่มจำนวนผู้ทราบถึงผลกระทบต่อภัยคุกคาม และทราบแนวทางการป้องกันตนเองเพิ่มมากขึ้น ผลที่ได้รับตามมา สามารถจัดทำแผนอบรมและพัฒนาบุคลากรในองค์กร สามารถนำข้อมูลที่ได้รับจากการทดสอบในการทำวิจัยครั้งนี้ใช้อ้างอิงและเป็นแนวทางในการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ได้ในอนาคตข้างหน้า

ผลการติดตั้ง Wi-Fi ก่อนการอบรมเสริมสร้างความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ โดยจำนวนกลุ่มเป้าหมายเชื่อมต่อ Wi-Fi ได้แก่ แผนก Nurse OPD จำนวน 21 คน และ Nurse IPD จำนวน 18 คน จากผู้ตอบแบบทดสอบทั้งหมด จำนวน 47 คน พบว่ามีผู้เชื่อมต่อทั้งในแผนก Nurse OPD และ Nurse IPD เชื่อมต่อ Wi-Fi จำลองนี้อย่างต่อเนื่อง แสดงให้เห็นถึงความเสี่ยงที่บุคลากรอาจตกเป็นเหยื่อของการโจมตีทางไซเบอร์ และหลังจากอบรมเสริมสร้างความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ พบว่าจำนวนผู้ใช้งานที่เชื่อมต่อ Wi-Fi จำลองลดลงอย่างมาก โดยแผนก Nurse OPD มีผู้เชื่อมต่อเดิมจากการทดสอบครั้งที่ 1 จำนวน 4 คน และ Nurse IPD ไม่พบผู้เชื่อมต่อเลย แสดงให้เห็นว่าการอบรมมีประสิทธิภาพในการลดความเสี่ยงต่อภัยคุกคามทางไซเบอร์

สรุปการอบรมเสริมสร้างความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ โดยมีผู้เข้ารับการอบรม 74 คน มีผู้สอบผ่านการวัดผล 65 คน และไม่ผ่าน 9 คน ผู้ตอบแบบสอบถามส่วนใหญ่ร้อยละ 85.37 แสดงความตระหนักถึงภัยคุกคามทางไซเบอร์ และจะหลีกเลี่ยงการส่งต่อข้อมูลผ่านแอปพลิเคชัน เมื่อไม่ได้เชื่อมต่อ Wi-Fi ที่ปลอดภัย ผลการตอบแบบสอบถาม และการทดสอบบ่งชี้ว่าหลังจากการอบรมผู้เข้ารับการอบรมมีความระมัดระวังตัวในการเชื่อมต่อกับสัญญาณ Wi-Fi มากขึ้น

ทั้งนี้ผลจากการศึกษาค้นคว้าอิสระนี้ได้รับการนำไปประยุกต์ใช้ในการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) สำหรับองค์กร ซึ่งมีจุดประสงค์หลักเพื่อเพิ่มความพร้อมในการเผชิญกับภัยคุกคามทางไซเบอร์ โดยแผนนี้ครอบคลุมการกำหนดนโยบาย และเป้าหมายของการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น การระบุ และจัดตั้งทีมตอบสนองต่อเหตุการณ์ (Incident

Response Team) พร้อมด้วยการกำหนดบทบาท และความรับผิดชอบของสมาชิกในทีม การจัดเตรียมเครื่องมือ ทรัพยากร และช่องทางการสื่อสารที่จำเป็นสำหรับการดำเนินงาน

โดยสรุปแล้ว ผลจากการศึกษาค้นคว้าอิสระนี้สามารถนำไปใช้ในการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และก่อให้เกิดประโยชน์อย่างแท้จริงต่อองค์กรในการเตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์

5.2 ข้อจำกัด

เนื่องจากองค์กรที่ทำการศึกษาเป็นองค์กรที่เกี่ยวข้องกับด้านสุขภาพ จึงมีข้อจำกัดในกระบวนการดำเนินงานและการขออนุมัติ เนื่องจากข้อมูลที่เกี่ยวข้องส่วนใหญ่เป็นข้อมูลที่มีความละเอียดอ่อน (Sensitive Data) และข้อมูลที่เป็นความลับ (Confidential Data) ซึ่งจำเป็นต้องปฏิบัติตามกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เป็นต้น

ด้วยเหตุนี้ การทดสอบในงานวิจัยนี้จึงถูกจำกัดอยู่เพียงการเก็บข้อมูลการเข้าใช้งานระบบ (Log in) เท่านั้น โดยไม่ได้มีการเก็บข้อมูลในส่วนของประวัติการใช้งานอินเทอร์เน็ต การรับ หรือส่งข้อมูลการสื่อสารผ่านแอปพลิเคชันชุมชน (Community Application) แต่อย่างใด

บรรณานุกรม

1. Itai Greenberg. (2023). [ออนไลน์]. **Healthcare cyber attacks are on the rise: Here's why zero trust will prevent care disruptions** สืบค้นจาก https://www.weforum.org/agenda/2023/05/cyber-attacks-on-healthcare-rise-zero-trust/
2. Anonymous. (2023). [ออนไลน์]. **ความเสี่ยงของการใช้ Public WiFi และแนวทางเสริมความปลอดภัย** สืบค้นจาก https://www.dailynews.co.th/news/2763175/
3. SOSECURE. (n.d.). [ออนไลน์]. **Cybersecurity Awareness รู้ทันภัยก่อนตกเป็นเหยื่อ** สืบค้นจาก https://www.sosecure.co.th/th/activity/cybersecurity-awareness
4. Kaspersky. (n.d.). [ออนไลน์]. **Evil twin attacks and how to prevent them**. สืบค้นจาก https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks
5. เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี. **ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร.** วารสารวิชาการไทยวิจัยและการจัดการรัฐประศาสนศาสตร์มหาบัณฑิตมหาวิทยาลัยธุรกิจบัณฑิตย์. ปีที่ 3 ฉบับที่ 2, (2565) **:** 1-6.
6. สุธาเทพ รุณเรศ. **ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร.** การศึกษาค้นคว้าอิสระวิทยาศาสตรมหาบัณฑิต สาขาวิชานโยบายและการบริหารเทคโนโลยีสารสนเทศวิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์, 2561.
7. Imran Hossain, Md Mahmudul Hasan, Syed Faisal Hasan, Md. Rezaul Karim. **A study of security awareness in Dhaka city using a portable WiFi pentesting device.** Bangladesh : 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), 2019
8. Andre Esser and Carlos Serrao. **Wi-Fi Network Testing Using an Integrated Evil-Twin Framework**. Spain : 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, 2018.
9. Felicia Sonola. **Hidden Cyber Security Risks: Why you Should Exercise Caution When Using Public Wi-Fi**. United Kingdom : Department of computer science Bournemouth university, 2022.
10. Serin F. **Public Wi-Fi: The Untold Story**. India : Department of Computer Science Al Azhar College of Arts and Sciences, 2021

บรรณานุกรม (ต่อ)

11. วัชรเมธน์ ศรีเนธิโรทัย. (n.d.). [ออนไลน์]. **การสร้าง App password สำหรับแอคเค้าที่ใช้ Google 2FA**. สืบค้นจากhttps://select2web.com/creating-google-app-password/
12. Lunodzo Mwinuka, Abel Agghey, Shubi F. Kaijage, Jema David Ndibwile. **FakeAP Detector: An Android-Based Client-Side Application for Detecting Wi-Fi Hotspot Spoofing**. Tanzania : School of Computation and Communication Science and Engineering, The Nelson Mandela African Institution of Science and Technology, Information Security and Communication Technology, Kamili Technologies Ltd.. Rwanda : College of Engineering, Carnegie Mellon University Africa, 2022
13. Said Abdul Ahad Ahadi, Elyas Baray, Nitin Rakesh, et al. **Public Wi-Fi security threat evil twin attack detection based on signal variant and hop count**. India : PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE AND COMPUTING APPLICATIONS-21 (ICCICA-21), 2022.
14. David Maimon, Scott Jacques & Robert C. Perkins, C. Jordan Howell. **Situational awareness and public Wi-Fi users' self-protective behaviors**. United Kingdom : Department of Criminal Justice and Criminology Georgia State University, Department of Criminal Justice, The University of Texas at El Paso, 2020
15. Codecademy Team. (n.d.). [ออนไลน์]. **Introduction to Pandas and NumPy**. สืบค้นจาก https://www.codecademy.com/article/introduction-to-numpy-and-pandas
16. Kurtis Pykes. (2023). [ออนไลน์]**. pandas read csv() Tutorial: Importing Data**. สืบค้นจาก https://www.datacamp.com/tutorial/pandas-read-csv
17. kartikaybhutani. (2020). [ออนไลน์]**. Python | Pandas Dataframe.sample()**. สืบค้นจาก https://www.geeksforgeeks.org/python-pandas-dataframe-sample
18. ซิสทูยู ออนไลน์. (2017). [ออนไลน์]. **คู่มือการติดตั้ง MikroTik แก้ไขหน้าHotSpot Login ตามต้องการด้วยตัวเอง**. สืบค้นจาก https://www.sys2u.online/XPERT_TOPIC68_how-to-config-setup-customized-MikroTik-hotspot-login-page--MikroTik.html
19. Adam Hayes. (2023). [ออนไลน์]. **Simple Random Sampling: 6 Basic Steps With Examples**. สืบค้นจาก https://www.investopedia.com/terms/s/simple-random-sample.asp

บรรณานุกรม (ต่อ)

20. admins. (2020). [ออนไลน์]. **สร้าง User Account หลายคนพร้อมกันเข้าไปใน MikroTik.** สืบค้นจาก https://ez-genius.com/%e0%b8%aa%e0%b8%a3%e0%b9%89%e0%b8%b2%e0%b8%87-user-%e0%b8%ab%e0%b8%a5%e0%b8%b%e0%b8%a2%e0%b8%84%e0%b8%99-MikroTik

21. SYED JAHANZAIB. (2011). [ออนไลน์]. **Mikrotik Hotspot Quick Setup Guide + Tips n Tricks for Hotspot !**. สืบค้นจาก https://aacable.wordpress.com/tag/mikrotik-howto-redirect-user-to-your-selected-site-after-succesful-login

22. TKSJa. (2018). [ออนไลน์]. **MikroTik Tutorial 71 - Send Emails for specific log event**. สืบค้นจากhttps://www.youtube.com/watch?v=fRQfnzo_p9Y&list=PLCvN_Pl1BlxhobZO5FSNyis281JbocVH

ประวัติผู้เขียน

ชื่อ	นายนันทภพ เครือครุ่ย
ชื่อการค้นคว้าอิสระ	การประเมินความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์โดยการจำลองการกระจายสัญญาณไวไฟสาธารณะ
สาขาวิชา	การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
ประวัติ	ประวัติการศึกษา
	สำเร็จการศึกษาระดับปริญญาตรี วิทยาศาสตรบัณฑิต คณะวิทยาศาสตร์ สาขาวิทยาการคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ปีการศึกษา 2561
	ประวัติการทำงาน
	ปฏิบัติงานในตำแหน่ง HIS Master Data Management พ.ศ. 2566 – ปัจจุบัน
	ปฏิบัติงานในตำแหน่ง Application Specialist (HIS and Clinical Process) พ.ศ. 2564 - 2566
	ปฏิบัติงานในตำแหน่ง Application Support พ.ศ. 2562 - 2564
	ปฏิบัติงานในตำแหน่ง Service Support พ.ศ. 2562
	ปฏิบัติงานในตำแหน่ง System Staff พ.ศ. 2561 - 2562